

KASPERSKY

Kaspersky Endpoint Security 10 для Linux (для защиты конфиденциальной информации)

Руководство администратора

Версия программы: 10.0.0.3458

Уважаемый пользователь!

Спасибо, что доверяете нам. Мы надеемся, что этот документ поможет вам в работе и ответит на большинство возникающих вопросов.

Внимание! Права на этот документ являются собственностью АО "Лаборатория Касперского" (далее также "Лаборатория Касперского") и защищены законодательством Российской Федерации об авторском праве и международными договорами. За незаконное копирование и распространение документа и его отдельных частей нарушитель несет гражданскую, административную или уголовную ответственность в соответствии с применимым законодательством.

Копирование в любой форме, распространение, в том числе в переводе, любых материалов возможны только с письменного разрешения "Лаборатории Касперского".

Документ и связанные с ним графические изображения могут быть использованы только в информационных, некоммерческих или личных целях.

Документ может быть изменен без предварительного уведомления.

За содержание, качество, актуальность и достоверность используемых в документе материалов, права на которые принадлежат другим правообладателям, а также за возможный ущерб, связанный с использованием этих материалов, "Лаборатория Касперского" ответственности не несет.

Дата редакции документа: 17.11.2017

Обозначение документа: 643.46856491.00054-05 90 01

© АО "Лаборатория Касперского", 2017.

<http://www.kaspersky.ru>

<https://help.kaspersky.com>

<http://support.kaspersky.ru>

Содержание

Об этом документе	9
В этом документе	9
Условные обозначения	12
Источники информации о программе	14
Источники для самостоятельного поиска информации	14
Обсуждение программ "Лаборатории Касперского" на форуме	16
Kaspersky Endpoint Security	17
О Kaspersky Endpoint Security	17
Что нового	19
Комплект поставки	19
Аппаратные и программные требования	20
Установка и удаление программы	24
Процедура установки программы	24
Об установке Kaspersky Endpoint Security	24
Установка пакета Kaspersky Endpoint Security	25
Обновление параметров Kaspersky Endpoint Security	25
Установка Агента администрирования	26
Установка Kaspersky Endpoint Security с помощью Kaspersky Security Center	26
Подготовка программы к работе	27
О первоначальной настройке Kaspersky Endpoint Security	27
Мастер первоначальной настройки Kaspersky Endpoint Security	27
Шаг 1. Выбор языкового стандарта	28
Шаг 2. Просмотр текста Лицензионного соглашения	28
Шаг 3. Участие в Kaspersky Security Network	29
Шаг 4. Определение типа перехватчика файловых операций	29
Шаг 5. Настройка параметров прокси-сервера	30
Шаг 6. Загрузка антивирусных баз Kaspersky Endpoint Security	31
Шаг 7. Включение автоматического обновления антивирусных баз	31
Шаг 8. Активация программы	32

Автоматический режим первоначальной настройки Kaspersky Endpoint Security	32
Запуск первоначальной настройки Kaspersky Endpoint Security в автоматическом режиме	32
Параметры конфигурационного файла первоначальной настройки Kaspersky Endpoint Security	33
Настройка параметров Агента администрирования	35
Настройка разрешающих правил в системе SELinux	36
Настройка разрешающих правил в системе AppArmor	37
Обновление файла модуля правил	38
Удаление программы	39
Локальное удаление Kaspersky Endpoint Security	39
Удаление Kaspersky Endpoint Security через Kaspersky Security Center	39
Лицензирование программы	40
О Лицензионном соглашении	40
О лицензии	41
О лицензионном сертификате	42
О коде активации	42
О ключе	43
О файле ключа	43
О подписке	44
О предоставлении данных	45
Запуск и остановка программы	48
Управление задачами Kaspersky Endpoint Security	49
О задачах Kaspersky Endpoint Security	49
Просмотр списка задач Kaspersky Endpoint Security	51
Создание задачи	51
Запуск и остановка задачи	51
Удаление задачи	51
Приостановка и возобновление задачи	52
Настройка расписания задачи	52
Просмотр состояния задачи	53
Обновление баз и модулей программы	54
Об обновлении баз и модулей программы	54

Об источниках обновлений	55
Настройка параметров обновления	56
Создание задачи обновления.....	56
Выбор источника обновлений.....	57
Использование прокси-сервера при доступе к источникам обновлений.....	58
Откат обновления баз	59
Копирование обновлений.....	59
Постоянная защита и проверка по требованию	60
О постоянной защите	61
О проверке по требованию	63
О зараженных файлах.....	65
Создание пользовательской задачи проверки по требованию	65
Формирование области защиты и области проверки	66
Об эвристическом анализе	68
Включение и настройка эвристического анализатора	68
Исключение объектов из областей защиты и проверки по требованию	70
Исключение объектов из области защиты или области проверки.....	70
Исключение объектов по названию обнаруженной угрозы	71
Выбор режима постоянной защиты.....	72
Выбор действий программы над зараженными объектами.....	74
Выборочная проверка файлов и директорий (Scan_File)	75
Проверка загрузочных секторов	75
Проверка памяти процессов	76
Сокращение времени проверки.....	76
Особенности проверки символических и жестких ссылок	78
Настройка совместной работы: Антивирус Касперского для Linux Mail Server...	79
Работа с резервным хранилищем	80
О резервном хранилище	80
Просмотр идентификаторов объектов в резервном хранилище.....	81
О восстановлении объектов из резервного хранилища	81
Восстановление объектов из резервного хранилища.....	82
Удаление объектов из резервного хранилища.....	83

Настройка уведомлений о событиях	84
Участие в Kaspersky Security Network.....	85
Об участии в Kaspersky Security Network	85
Включение и выключение использования Kaspersky Security Network.....	87
Проверка подключения к Kaspersky Security Network	88
Дополнительная защита с использованием Kaspersky Security Network	89
Управление программой через Kaspersky Security Center.....	90
Об управлении Kaspersky Endpoint Security с помощью Kaspersky Security Center.....	91
Запуск и остановка Kaspersky Endpoint Security на клиентском компьютере.....	92
Настройка параметров Kaspersky Endpoint Security	93
Просмотр состояния защиты компьютера	95
Просмотр параметров Kaspersky Endpoint Security.....	96
Управление задачами	97
О задачах для Kaspersky Endpoint Security	98
Создание локальной задачи.....	99
Создание групповой задачи.....	100
Создание задачи для набора компьютеров	101
Запуск, остановка, приостановка и возобновление выполнения задачи вручную	101
Изменение параметров задачи	103
Управление политиками.....	106
О политиках	106
Создание политики.....	108
Изменение параметров политики.....	108
Просмотр сообщений пользователей в хранилище событий Kaspersky Security Center.....	109
Проверка соединения с Сервером администрирования вручную. Утилита klnagchk	110
Подключение к Серверу администрирования вручную. Утилита klmover	112
Обращение в Службу технической поддержки.....	114
Способы получения технической поддержки	114
Техническая поддержка по телефону	115
Техническая поддержка через Kaspersky CompanyAccount	115

Приложения.....	117
Параметры конфигурационных файлов.....	117
Правила редактирования конфигурационных файлов Kaspersky Endpoint Security	117
Общие параметры Kaspersky Endpoint Security	119
Параметры задачи постоянной защиты и задач проверки по требованию... 123	
Общие параметры задачи постоянной защиты и задач проверки по требованию	124
[ScanScope.item_#]	133
[ExcludedFromScanScope.item_#]	135
Параметры задач проверки загрузочных секторов и задач проверки памяти процессов.....	136
Параметры задач обновления и задач копирования обновлений.....	140
Общие параметры задач обновления и задач копирования обновлений. 140	
[CustomSources.item_#]	143
Параметры резервного хранилища.....	144
Команды управления Kaspersky Endpoint Security из командной строки.....	145
Об управлении Kaspersky Endpoint Security из командной строки.....	145
Вывод справки о командах Kaspersky Endpoint Security.....	150
Включение вывода событий	151
Быстрая проверка файлов и директорий.....	151
Просмотр информации о программе	152
Команды управления параметрами Kaspersky Endpoint Security и задачами.....	153
Получение общих параметров Kaspersky Endpoint Security.....	153
Изменение общих параметров Kaspersky Endpoint Security	155
Параметры расписания задачи	156
Команды управления задачами Kaspersky Endpoint Security	159
Создание задачи	159
Удаление задачи	160
Запуск задачи	161
Остановка задачи	162
Приостановка задачи	163
Возобновление задачи.....	164
Просмотр состояния задачи	165
Просмотр списка задач Kaspersky Endpoint Security	166

Получение параметров задачи	167
Изменение параметров задачи	168
Команды управления ключами	170
Добавление активного ключа	171
Добавление дополнительного ключа.....	171
Удаление активного ключа	172
Удаление дополнительного ключа.....	172
Ввод дополнительного кода активации	173
Команды управления резервным хранилищем.....	173
Получение информации об объектах в хранилище.....	173
Восстановление объектов из хранилища	174
Коды возврата командной строки.....	175
АО "Лаборатория Касперского"	176
Информация о стороннем коде	178
Уведомления о товарных знаках	179
Глоссарий	180
Предметный указатель	188

Об этом документе

Руководство администратора «Kaspersky Endpoint Security 10 для Linux (для защиты конфиденциальной информации)» (далее «Kaspersky Endpoint Security») адресовано специалистам, которые осуществляют установку и администрирование Kaspersky Endpoint Security, и специалистам, которые осуществляют техническую поддержку организаций, использующих Kaspersky Endpoint Security.

Вы можете применять информацию в этом руководстве для выполнения следующих задач:

- подготовка к установке, установка и активация Kaspersky Endpoint Security;
- настройка и использование Kaspersky Endpoint Security.

Также из этого руководства вы можете узнать об источниках информации о программе и способах получения технической поддержки.

В этом разделе

В этом документе	9
Условные обозначения	12

В этом документе

Это руководство содержит следующие разделы.

Источники информации о программе (см. стр. [14](#))

Этот раздел содержит описание источников информации о программе.

Kaspersky Endpoint Security (см. стр. [17](#))

Этот раздел содержит описание возможностей программы, а также краткую информацию о функциях и компонентах программы. Вы узнаете о том, из чего состоит комплект поставки и какие услуги доступны зарегистрированным пользователям программы.

Установка и удаление программы (см. стр. [24](#))

Этот раздел содержит информацию о том, как установить Kaspersky Endpoint Security на компьютер, как выполнить первоначальную настройку программы, а также о том, как удалить программу с компьютера.

Лицензирование программы (см. стр. [40](#))

Этот раздел содержит информацию об основных понятиях, связанных с лицензированием программы.

Запуск и остановка программы (см. стр. [48](#))

Этот раздел содержит информацию о том, как запускать, перезапускать и завершать работу программы из командной строки.

Управление задачами Kaspersky Endpoint Security (см. стр. [49](#))

Этот раздел содержит информацию о типах задач Kaspersky Endpoint Security и инструкции о том, как управлять задачами.

Обновление баз и модулей программы (см. стр. [54](#))

Этот раздел содержит информацию об обновлении антивирусных баз и модулей программы (далее также "обновления") и инструкции о том, как настроить параметры обновления.

Постоянная защита и проверка по требованию (см. стр. [60](#))

Этот раздел содержит информацию о задачах постоянной защиты и проверки по требованию, а также инструкции о том, как настроить параметры этих задач.

Работа с резервным хранилищем (см. стр. [80](#))

Этот раздел содержит инструкции о том, как настроить параметры резервного хранилища, и информацию о том, какие действия можно выполнять над объектами в резервном хранилище.

Участие в Kaspersky Security Network (см. стр. [85](#))

Этот раздел содержит информацию об участии в Kaspersky Security Network и инструкции о том, как включить и выключить использование Kaspersky Security Network.

Управление программой через Kaspersky Security Center (см. стр. [90](#))

Этот раздел содержит информацию об управлении Kaspersky Endpoint Security с помощью Kaspersky Security Center.

Обращение в Службу технической поддержки (см. стр. [114](#))

Этот раздел содержит информацию о способах и условиях получения технической поддержки.

Приложения (см. стр. [117](#))

Этот раздел содержит информацию о параметрах конфигурационных файлов, командах управления Kaspersky Endpoint Security из командной строки, а также коды возврата командной строки.

АО "Лаборатория Касперского" (см. стр. [176](#))

Этот раздел содержит информацию об АО "Лаборатория Касперского".

Информация о стороннем коде (см. стр. [178](#))

Этот раздел содержит информацию о стороннем коде.

Уведомления о товарных знаках (см. стр. [179](#))

Этот раздел содержит информацию о товарных знаках, упомянутых в документе.

Глоссарий (см. стр. [180](#))

Этот раздел содержит список терминов, которые встречаются в тексте документа, а также определения этих терминов.

Предметный указатель

Этот раздел позволяет быстро найти необходимые сведения в документе.

Условные обозначения

В этом документе используются условные обозначения (см. таблицу ниже).

Таблица 1. Условные обозначения

Пример текста	Описание условного обозначения
Обратите внимание на то, что...	Предупреждения выделены красным цветом и заключены в рамку. Предупреждения содержат информацию о действиях, которые могут иметь нежелательные последствия.
Рекомендуется использовать...	Примечания заключены в рамку. Примечания содержат дополнительную и справочную информацию.
Пример: ...	Примеры приведены в блоках на голубом фоне под заголовком "Пример".
<i>Обновление</i> – это... Возникает событие <i>Базы устарели</i> .	Курсивом выделены следующие элементы текста: <ul style="list-style-type: none">• новые термины;• названия статусов и событий программы.
Нажмите на клавишу ENTER . Нажмите комбинацию клавиш ALT+F4 .	Названия клавиш клавиатуры выделены полужирным шрифтом и прописными буквами. Названия клавиш, соединенные знаком + (плюс), означают комбинацию клавиш. Такие клавиши требуется нажимать одновременно.
Нажмите на кнопку Включить .	Названия элементов интерфейса программы, например, полей ввода, пунктов меню, кнопок, выделены полужирным шрифтом.

Пример текста	Описание условного обозначения
<p>► <i>Чтобы настроить расписание задачи, выполните следующие действия:</i></p>	<p>Вводные фразы инструкций выделены курсивом и значком "стрелка".</p>
<p>В командной строке введите текст <code>help</code></p> <p>Появится следующее сообщение:</p> <p>Укажите дату в формате ДД:ММ:ГГ.</p>	<p>Специальным стилем выделены следующие типы текста:</p> <ul style="list-style-type: none"> • текст командной строки; • текст сообщений, выводимых программой на экран; • данные, которые требуется ввести с клавиатуры.
<p><Имя пользователя></p>	<p>Переменные заключены в угловые скобки. Вместо переменной требуется подставить соответствующее ей значение, опустив угловые скобки.</p>

Источники информации о программе

Этот раздел содержит описание источников информации о программе.

Вы можете выбрать наиболее удобный источник информации в зависимости от важности и срочности вопроса.

В этом разделе

Источники для самостоятельного поиска информации	14
Обсуждение программ "Лаборатории Касперского" на форуме.....	16

Источники для самостоятельного поиска информации

Вы можете использовать следующие источники для самостоятельного поиска информации о Kaspersky Endpoint Security:

- страница Kaspersky Endpoint Security на веб-сайте "Лаборатории Касперского";
- страница Kaspersky Endpoint Security на веб-сайте Службы технической поддержки (База знаний);
- документация.

Если вы не нашли решения возникшей проблемы самостоятельно, обратитесь в Службу технической поддержки "Лаборатории Касперского" (см. раздел "Обращение в Службу технической поддержки" на стр. [114](#)).

Для использования источников информации на веб-сайтах требуется подключение к интернету.

Страница Kaspersky Endpoint Security на веб-сайте "Лаборатории Касперского"

На странице Kaspersky Endpoint Security (<http://www.kaspersky.ru/business-security/endpoint-linux>) вы можете получить общую информацию о программе, ее возможностях и особенностях работы.

Страница Kaspersky Endpoint Security содержит ссылку на интернет-магазин. В нем вы можете приобрести программу или продлить право пользования программой.

Страница Kaspersky Endpoint Security в Базе знаний

База знаний – это раздел веб-сайта Службы технической поддержки.

На странице Kaspersky Endpoint Security в Базе знаний (<http://support.kaspersky.ru/kes10linux>) вы найдете статьи, которые содержат полезную информацию, рекомендации и ответы на часто задаваемые вопросы о приобретении, установке и использовании программы.

Статьи Базы знаний могут отвечать на вопросы, которые относятся не только к Kaspersky Endpoint Security, но и к другим программам "Лаборатории Касперского". Статьи Базы знаний также могут содержать новости Службы технической поддержки.

Документация

В состав документации к программе входят файлы руководства администратора.

В руководстве администратора вы можете найти информацию для выполнения следующих задач:

- подготовка к установке, установка и активация Kaspersky Endpoint Security;
- настройка и использование Kaspersky Endpoint Security;
- удаленное управление Kaspersky Endpoint Security через Kaspersky Security Center.

Обсуждение программ "Лаборатории Касперского" на форуме

Если ваш вопрос не требует срочного ответа, вы можете обсудить его со специалистами "Лаборатории Касперского" и с другими пользователями на нашем форуме (<http://forum.kaspersky.com>).

На форуме вы можете просматривать опубликованные темы, добавлять свои комментарии, создавать новые темы для обсуждения.

Kaspersky Endpoint Security

Этот раздел содержит описание функций, компонентов и комплекта поставки Kaspersky Endpoint Security, перечень аппаратных и программных требований Kaspersky Endpoint Security.

В этом разделе

О Kaspersky Endpoint Security	17
Что нового	19
Комплект поставки	19
Аппаратные и программные требования	20

О Kaspersky Endpoint Security

Kaspersky Endpoint Security обеспечивает защиту компьютеров под управлением операционных систем Linux® от вредоносных программ. Угрозы могут проникать в систему через сетевые каналы передачи данных или со съемных дисков.

Программа позволяет:

- Проверять объекты файловой системы, расположенные на локальных дисках компьютера, а также смонтированные и разделяемые ресурсы, доступ к которым предоставляется по протоколам SMB и NFS.

Программа проверяет объекты файловой системы как в режиме реального времени с помощью задачи постоянной защиты, так и по команде с помощью задач проверки по требованию.

- Проверять загрузочные секторы с помощью задачи проверки загрузочных секторов.
- Проверять память процессов с помощью задачи проверки памяти процессов.

- Обнаруживать зараженные объекты.

Kaspersky Endpoint Security оценивает объект как зараженный, если в объекте обнаружен код известного вируса.

- Обезвреживать обнаруженные в файлах угрозы.

В зависимости от типа угрозы программа автоматически подбирает действие, которое требуется выполнить для нейтрализации угрозы.

- Сохранять резервные копии файлов перед лечением или удалением и восстанавливать файлы из резервных копий.
- Управлять задачами и настраивать их параметры.

Вы можете управлять задачей постоянной защиты, задачами проверки по требованию, проверки загрузочных секторов, проверки памяти процессов, обновления, задачами отката обновлений и копирования обновлений.

- Добавлять ключи, активировать программу с помощью кодов активации, использовать программу по подписке.
- Уведомлять администратора о событиях, произошедших во время работы Kaspersky Endpoint Security.
- Обновлять базы Kaspersky Endpoint Security с серверов обновлений «Лаборатории Касперского», через Сервер администрирования или из указанного пользователем источника по расписанию и по требованию.

Программа использует антивирусные базы для обнаружения и лечения зараженных файлов. Kaspersky Endpoint Security анализирует каждый файл во время проверки на наличие угроз: код файла сравнивается с кодом, характерным для той или иной угрозы.

- Управлять Kaspersky Endpoint Security следующими способами:
 - с помощью команд управления программой из командной строки;
 - через Kaspersky Security Center.

Что нового

В Kaspersky Endpoint Security появились следующие возможности:

- Добавлена поддержка Kaspersky Security Network.
- Добавлена поддержка Kaspersky Private Security Network при использовании Kaspersky Security Center.
- Добавлена возможность использования Kaspersky Endpoint Security по подписке.
- Добавлена поддержка сервиса активации 2.0.
- Добавлена возможность проверки памяти процессов.
- Добавлена возможность проверки загрузочных секторов.
- Добавлены новые команды для облегчения управления Kaspersky Endpoint Security.
- Добавлена поддержка технологии fanotify.
- Добавлена возможность проверки файлов непривилегированными пользователями.

Комплект поставки

В комплект поставки входит дистрибутив Kaspersky Endpoint Security, содержащий следующие файлы:

- `kesl-10.0.0-<номер сборки>.i386.rpm`, `kesl_10.0.0-<номер сборки>_i386.deb`

Содержат основные файлы Kaspersky Endpoint Security. Пакеты могут быть установлены на 32-битные операционные системы в соответствии с типом пакетного менеджера.

- `kesl-10.0.0-<номер сборки>.x86_64.rpm`, `kesl_10.0.0-<номер сборки>_amd64.deb`

Содержат основные файлы Kaspersky Endpoint Security. Пакеты могут быть установлены на 64-битные операционные системы в соответствии с типом пакетного менеджера.

- kesi.zip

Содержит файлы, используемые в процедуре удаленной установки Kaspersky Endpoint Security с помощью Kaspersky Security Center.

- klnagent-<номер сборки>.i386.rpm, klnagent_<номер сборки>_i386.deb

Содержат Агент Администрирования (утилиту связи Kaspersky Endpoint Security с Kaspersky Security Center).

- klnagent-rpm.tar.gz, klnagent-deb.tar.gz

Содержат файлы klnagent.kpd и ainstall.sh, используемые в процедуре удаленной установки Агента Администрирования с помощью Kaspersky Security Center.

- Файл ksn_license.<ID языка>, с помощью которого вы можете ознакомиться с условиями участия в Kaspersky Security Network.
- Файл license.<ID языка>, с помощью которого вы можете ознакомиться с Лицензионным соглашением. В Лицензионном соглашении указано, на каких условиях вы можете пользоваться программой.

Аппаратные и программные требования

Для функционирования Kaspersky Endpoint Security компьютер должен удовлетворять следующим требованиям.

Минимальные общие требования:

- процессор Core™ 2 Duo 1.86 GHz или выше;
- 1 GB оперативной памяти для 32-битных операционных систем;
- 2 GB оперативной памяти для 64-битных операционных систем;
- раздел подкачки не менее 1 GB;
- 1 GB свободного места на жестком диске.

Программные требования:

- Поддерживаемые 32-битные операционные системы:
 - Red Hat® Enterprise Linux® 6.7;
 - Red Hat Enterprise Linux 6.8;
 - CentOS-6.7;
 - CentOS-6.8;
 - Ubuntu Server 14.04 LTS;
 - Ubuntu Server 16.04 LTS;
 - Ubuntu Server 16.10 LTS;
 - Debian GNU/Linux 7.10;
 - Debian GNU/Linux 7.11;
 - Debian GNU/Linux 8.6;
 - Debian GNU/Linux 8.7;
 - Альт Линукс СПТ 8.0.

- Поддерживаемые 64-битные операционные системы:
 - Red Hat Enterprise Linux 6.7;
 - Red Hat Enterprise Linux 6.8;
 - Red Hat Enterprise Linux 7.2;
 - Red Hat Enterprise Linux 7.3;
 - CentOS-6.7;
 - CentOS-6.8;
 - CentOS-7.2;
 - CentOS-7.3;

- Ubuntu Server 14.04 LTS;
- Ubuntu Server 16.04 LTS;
- Ubuntu Server 16.10 LTS;
- Debian GNU/Linux 7.10;
- Debian GNU/Linux 7.11;
- Debian GNU/Linux 8.6;
- Debian GNU/Linux 8.7;
- openSUSE 42.2;
- Novell OES11 SP3;
- Novell OES2015 SP1;
- Oracle Linux 7.3;
- Альт Линукс СПТ 8.0;
- Astra Linux SE 1.5 – только при отключенном механизме мандатного разграничения доступа и отключенном механизме создания замкнутой программной среды, вариант ядра без PAX.
- Интерпретатор языка Perl версии 5.10 или выше.
- Установленная утилита which.
- Установленные пакеты для компиляции программ (gcc, binutils, glibc, glibc-devel, make, ld).
- Исходный код ядра операционной системы – для компиляции модулей Kaspersky Endpoint Security на операционных системах, не поддерживающих технологию fanotify.
- Kaspersky Endpoint Security 10 для Linux совместим с Kaspersky Security Center 10 SP1 и Kaspersky Security Center 10 SP2.
- Для работы плагина управления Kaspersky Endpoint Security должен быть установлен Microsoft® Visual C++ 2015 Redistributable Update 3 RC.

- До установки Агента администрирования должны быть установлены следующие модули:
 - Модуль `libc6-i386` должен быть установлен на 64-битные версии Debian и Ubuntu.
 - Модуль `glibc.i686` должен быть установлен на Red Hat Enterprise Linux 7 и выше, CentOS 7 и выше, Oracle Linux 7 и выше.
 - Модуль `glibc-32bit` должен быть установлен на openSUSE 42.2 и SUSE Linux Enterprise Server 11 SP4.

Установка и удаление программы

Этот раздел содержит пошаговые инструкции по установке и удалению Kaspersky Endpoint Security.

В этом разделе

Процедура установки программы	24
Подготовка программы к работе	27
Удаление программы	39

Процедура установки программы

Этот раздел содержит инструкции о том, как установить пакет установки (далее "пакет") Kaspersky Endpoint Security и Агента администрирования.

Об установке Kaspersky Endpoint Security

Kaspersky Endpoint Security распространяется в пакетах форматов DEB и RPM.

Для работы с Kaspersky Endpoint Security вам требуется выполнить следующие операции:

1. установить пакет Kaspersky Endpoint Security;
2. запустить скрипт обновления параметров;
3. установить пакет Агента администрирования и плагин управления Kaspersky Endpoint Security, если вы планируете управлять Kaspersky Endpoint Security с помощью Kaspersky Security Center.

Установка пакета Kaspersky Endpoint Security

Kaspersky Endpoint Security распространяется в пакетах форматов DEB и RPM.

- ▶ Чтобы установить Kaspersky Endpoint Security из пакета формата RPM на 32-битную операционную систему, выполните следующую команду:

```
# rpm -i kesi-10.0.0-<номер сборки>.i386.rpm
```

- ▶ Чтобы установить Kaspersky Endpoint Security из пакета формата RPM на 64-битную операционную систему, выполните следующую команду:

```
# rpm -i kesi-10.0.0-<номер сборки>.x86_64.rpm
```

- ▶ Чтобы установить Kaspersky Endpoint Security из пакета формата DEB на 32-битную операционную систему, выполните следующую команду:

```
# dpkg -i kesi-10.0.0-<номер сборки>_i386.deb
```

- ▶ Чтобы установить Kaspersky Endpoint Security из пакета формата DEB на 64-битную операционную систему, выполните следующую команду:

```
# dpkg -i kesi_10.0.0-<номер сборки>_amd64.deb
```

Обновление параметров Kaspersky Endpoint Security

После установки Kaspersky Endpoint Security требуется запустить скрипт послеустановочной настройки Kaspersky Endpoint Security. Скрипт послеустановочной настройки Kaspersky Endpoint Security входит в пакет Kaspersky Endpoint Security.

- ▶ Чтобы запустить скрипт послеустановочной настройки Kaspersky Endpoint Security, выполните следующую команду:

```
# /opt/kaspersky/kesi/bin/kesi-setup.pl
```

Скрипт послеустановочной настройки по шагам запрашивает значения параметров Kaspersky Endpoint Security (см. раздел "О первоначальной настройке Kaspersky Endpoint Security" на стр. [27](#)).

Обновление предыдущей версии программы до Kaspersky Endpoint Security 10 для Linux не поддерживается. Вам необходимо удалить предыдущую версию программы и установить Kaspersky Endpoint Security.

Установка Агента администрирования

Установка Агента администрирования требуется, если вы планируете управлять Kaspersky Endpoint Security с помощью Kaspersky Security Center.

Запускать процесс установки Агента администрирования требуется с root-правами.

- ▶ Чтобы установить Агент администрирования из пакета формата RPM на 32-битную или 64-битную операционную систему, выполните следующую команду:

```
# rpm -i klnagent-<номер сборки>.i386.rpm
```

- ▶ Чтобы установить Агент администрирования из пакета формата DEB на 32-битную операционную систему, выполните следующую команду:

```
# dpkg -i klnagent_<номер сборки>_i386.deb
```

- ▶ Чтобы установить Агент администрирования из пакета формата DEB на 64-битную операционную систему, выполните следующую команду:

```
# dpkg -i --force-architecture klnagent_<номер сборки>_i386.deb
```

После установки пакета запустите скрипт послеустановочной настройки Kaspersky Endpoint Security, выполнив следующую команду:

```
/opt/kaspersky/klnagent/lib/bin/setup/postinstall.pl
```

Установка Kaspersky Endpoint Security с помощью Kaspersky Security Center

Вы можете установить Kaspersky Endpoint Security на компьютер с помощью Kaspersky Security Center.

Подробнее об этом типе установки программы вы можете прочитать в *Руководстве администратора для Kaspersky Security Center*.

Подготовка программы к работе

Этот раздел содержит инструкции о первоначальной настройке Kaspersky Endpoint Security.

О первоначальной настройке Kaspersky Endpoint Security

По завершении установки Kaspersky Endpoint Security на компьютер вам нужно выполнить первоначальную настройку Kaspersky Endpoint Security.

Если вы не выполнили процедуру первоначальной настройки Kaspersky Endpoint Security, антивирусная защита компьютера не будет работать.

Процесс первоначальной настройки представляет собой последовательность шагов. Эта процедура реализована в виде скрипта послеустановочной настройки. Скрипт послеустановочной настройки необходимо запустить с root-правами после завершения установки пакета Kaspersky Endpoint Security.

Мастер первоначальной настройки Kaspersky Endpoint Security

- ▶ Чтобы запустить скрипт первоначальной настройки Kaspersky Endpoint Security вручную, выполните следующую команду:

```
# /opt/kaspersky/kesl/bin/kesl-setup.pl
```

В этом разделе

Шаг 1. Выбор языкового стандарта	28
Шаг 2. Просмотр текста Лицензионного соглашения	28
Шаг 3. Участие в Kaspersky Security Network	29
Шаг 4. Определение типа перехватчика файловых операций	29

Шаг 5. Настройка параметров прокси-сервера.....	30
Шаг 6. Загрузка антивирусных баз Kaspersky Endpoint Security.....	31
Шаг 7. Включение автоматического обновления антивирусных баз	31
Шаг 8. Активация программы	32

Шаг 1. Выбор языкового стандарта

На этом шаге вам нужно задать обозначение языкового стандарта, который будет использоваться при работе Kaspersky Endpoint Security.

Вы можете задать языковой стандарт в формате, определенном в RFC 3066.

- ▶ *Чтобы получить полный список обозначений языковых стандартов, выполните следующую команду:*

```
# locale -a
```

По умолчанию программа предлагает использовать языковой стандарт, установленный для root.

Шаг 2. Просмотр текста Лицензионного соглашения

На этом шаге вам нужно принять или отклонить условия Лицензионного соглашения.

Вы можете просмотреть текст с помощью утилиты `less`. Для перемещения по тексту используйте клавиши управления курсором или клавиши **B** (для перемещения назад на один экран) и **F** (для перемещения вперед на один экран). Для получения справки используйте клавишу **H**. Для завершения просмотра используйте клавишу **Q**.

После выхода из режима просмотра введите одно из следующих значений:

- `yes` (или `y`), если вы согласны с условиями Лицензионного соглашения;

- no (или n), если вы не согласны с условиями Лицензионного соглашения.

Если вы не согласны с условиями Лицензионного соглашения, программа прерывает процесс настройки Kaspersky Endpoint Security.

Шаг 3. Участие в Kaspersky Security Network

На этом шаге вам нужно принять или отклонить условия Положения о Kaspersky Security Network. Файл с текстом Положения о Kaspersky Security Network расположен в директории `/opt/kaspersky/kesl/doc/ksn_license.<ID языка>`.

Введите одно из следующих значений:

- yes (или y), если вы согласны с условиями Положения о Kaspersky Security Network;
- no (или n), если вы не согласны с условиями Положения о Kaspersky Security Network.

Отказ от участия в Kaspersky Security Network не прерывает процесс установки Kaspersky Endpoint Security. Вы можете включить или выключить использование Kaspersky Security Network в любой момент (см. раздел "Включение и выключение использования Kaspersky Security Network" на стр. [87](#)).

Шаг 4. Определение типа перехватчика файловых операций

На этом этапе определяется тип перехватчика файловых операций для используемой операционной системы. Для операционных систем, не поддерживающих технологию fanotify, будет запущена компиляция модуля ядра. Модуль ядра требуется для работы задачи постоянной защиты.

Для компиляции модуля ядра требуется наличие файла `System.map-<версия ядра>` в директории `/boot`.

Если скрипт обнаруживает исходные коды ядра операционной системы в директории по умолчанию, программа будет использовать путь к этой директории. В противном случае вам нужно указать путь к исходным кодам ядра.

Если в процессе компиляции модуля ядра не обнаружены необходимые пакеты, Kaspersky Endpoint Security пытается скачать их самостоятельно. Если скачать пакеты не удастся, выводится сообщение об ошибке.

Вы можете выполнить компиляцию модуля ядра позже, после завершения первоначальной настройки Kaspersky Endpoint Security.

Шаг 5. Настройка параметров прокси-сервера

На этом шаге вам нужно указать параметры прокси-сервера, если вы используете прокси-сервер для доступа в интернет. Подключение к интернету требуется для загрузки антивирусных баз Kaspersky Endpoint Security с серверов обновлений (см. раздел "Шаг 6. Загрузка антивирусных баз Kaspersky Endpoint Security" на стр. [31](#)).

► *Чтобы настроить параметры прокси-сервера, выполните одно из следующих действий:*

- Если при подключении к интернету вы используете прокси-сервер, укажите адрес прокси-сервера в одном из следующих форматов:
 - IP_адрес_прокси_сервера:порт, если при подключении к прокси-серверу не требуется аутентификация;
 - имя_пользователя:пароль@IP_адрес_прокси_сервера:порт, если при подключении к прокси-серверу требуется аутентификация;
- Если при подключении к интернету вы не используете прокси-сервер, введите ответ no.

По умолчанию программа предлагает ответ no.

Вы можете настроить параметры прокси-сервера без использования скрипта первоначальной настройки (см. раздел "Использование прокси-сервера при доступе к источникам обновлений" на стр. [58](#)).

Шаг 6. Загрузка антивирусных баз Kaspersky Endpoint Security

На этом шаге вы можете загрузить на компьютер антивирусные базы Kaspersky Endpoint Security. Антивирусные базы содержат описания сигнатур угроз и методов борьбы с ними. Kaspersky Endpoint Security использует эти записи при поиске и обезвреживании угроз. Вирусные аналитики "Лаборатории Касперского" регулярно пополняют записи о новых угрозах.

Чтобы загрузить антивирусные базы Kaspersky Endpoint Security на компьютер, вам нужно ввести ответ `yes`.

Введите `no`, если вы хотите отказаться от немедленной загрузки антивирусных баз.

По умолчанию предлагается ответ `yes`.

Программа будет обеспечивать антивирусную защиту компьютера только после загрузки антивирусных баз Kaspersky Endpoint Security.

Вы можете запустить задачу обновления антивирусных баз Kaspersky Endpoint Security без использования скрипта первоначальной настройки (см. раздел "Обновление баз и модулей программы" на стр. [54](#)).

Шаг 7. Включение автоматического обновления антивирусных баз

На этом шаге вы можете включить автоматическое обновление антивирусных баз.

Введите ответ `yes`, чтобы включить автоматическое обновление антивирусных баз. По умолчанию Kaspersky Endpoint Security проверяет наличие обновлений для антивирусных баз каждые 60 минут. Если обновления есть, Kaspersky Endpoint Security загружает обновленные антивирусные базы.

Введите ответ `no`, если вы не хотите, чтобы Kaspersky Endpoint Security автоматически обновлял антивирусные базы.

Вы можете включить автоматическое обновление антивирусных баз без помощи скрипта первоначальной настройки, управляя расписанием задачи обновления (см. раздел "Изменение параметров расписания задачи" на стр. [157](#)).

Шаг 8. Активация программы

На этом шаге вам нужно активировать программу с помощью кода активации или файла ключа.

Чтобы активировать программу с помощью кода активации, вам нужно ввести код активации.

Чтобы активировать программу с помощью файла ключа, вам нужно указать полный путь к файлу ключа.

Если код активации или файл ключа не указаны, программа будет активирована с помощью пробного ключа на один месяц.

Вы можете установить файл ключа без использования скрипта первоначальной настройки (см. раздел "Команды управления ключами" на стр. [170](#)).

Автоматический режим первоначальной настройки Kaspersky Endpoint Security

Вы можете выполнить первоначальную настройку Kaspersky Endpoint Security в автоматическом режиме. Программа установит значения параметров, указанные в конфигурационном файле первоначальной настройки.

Запуск первоначальной настройки Kaspersky Endpoint Security в автоматическом режиме

► Чтобы запустить первоначальную настройку Kaspersky Endpoint Security в автоматическом режиме, выполните следующую команду:

```
/opt/kaspersky/kes1/bin/kes1-setup.pl --autoinstall=<полный путь к конфигурационному файлу первоначальной настройки>
```


Параметры конфигурационного файла первоначальной настройки Kaspersky Endpoint Security

Конфигурационный файл первоначальной настройки Kaspersky Endpoint Security содержит параметры, приведенные в таблице ниже.

Таблица 2. Параметры конфигурационного файла первоначальной настройки Kaspersky Endpoint Security

Параметр	Описание	Возможные значения
EULA_AGREED	Обязательный параметр. Согласие с условиями Лицензионного соглашения	yes – согласие с условиями Лицензионного соглашения необходимо для продолжения процедуры установки программы
USE_KSN	Согласие с Положением о Kaspersky Security Network	yes – принять Положение о Kaspersky Security Network no – не принимать Положение о Kaspersky Security Network
SERVICE_LOCALE	Языковой стандарт, используемый при работе Kaspersky Endpoint Security	Языковой стандарт в формате, определенном в RFC 3066
INSTALL_LICENSE	Код активации или файл ключа	

Параметр	Описание	Возможные значения
UPDATER_SOURCE	Источник обновлений	<ul style="list-style-type: none"> • <code>SCServer</code> – использовать в качестве источника обновлений Сервер администрирования Kaspersky Security Center; • <code>KLServers</code> – использовать в качестве источника обновлений серверы "Лаборатории Касперского"; • адрес источника обновлений.
PROXY_SERVER	Адрес прокси-сервера, используемого для подключения к интернету	<ul style="list-style-type: none"> • адрес прокси-сервера; • <code>no</code> – не использовать прокси-сервер.
UPDATE_EXECUTE	Запуск задачи обновления баз во время процедуры настройки	<ul style="list-style-type: none"> • <code>yes</code> – запускать задачу обновления; • <code>no</code> – не запускать задачу обновления.
KERNEL_SRCS_INSTALL	Автоматический запуск компиляции модуля ядра	<ul style="list-style-type: none"> • <code>yes</code> – компилировать модуль ядра; • <code>no</code> – не компилировать модуль ядра.

Если вы хотите изменить параметры в конфигурационном файле первоначальной настройки Kaspersky Endpoint Security, вводите значения параметров в формате `имя параметра=значение_параметра` (программа не обрабатывает пробелы между именем параметра и его значением).

Настройка параметров Агента администрирования

Если вы планируете управлять Kaspersky Endpoint Security с помощью Kaspersky Security Center, вам нужно настроить параметры Агента администрирования.

► Чтобы настроить параметры Агента администрирования, выполните следующие действия:

1. Выполните команду:

```
# /opt/kaspersky/klnagent/lib/bin/setup/postinstall.pl
```

2. Укажите DNS-имя или IP-адрес Сервера администрирования.

3. Укажите номер порта Сервера администрирования

По умолчанию используется порт 14000.

4. Если вы хотите использовать SSL-соединение, укажите номер SSL-порта Сервера администрирования.

По умолчанию используется порт 13000.

5. Выполните одно из следующих действий:

- Введите `yes`, если вы хотите использовать SSL-соединение;
- Введите `no`, если вы не хотите использовать SSL-соединение.

По умолчанию SSL-соединение включено.

Для получения подробной информации о настройке Агента администрирования обратитесь к *Руководству администратора Kaspersky Security Center*.

Настройка разрешающих правил в системе SELinux

- ▶ Чтобы создать модуль SELinux с правилами, необходимыми для работы Kaspersky Endpoint Security, выполните следующие действия:

1. Переведите SELinux в разрешающий режим:

- Если SELinux был активирован, выполните следующую команду:

```
# setenforce Permissive
```

- Если SELinux был выключен, в конфигурационном файле `/etc/selinux/config` задайте значение параметра `SELINUX=permissive` и перезагрузите операционную систему.

2. Запустите следующие задачи:

- задачу постоянной защиты:

```
/opt/kaspersky/kesl/bin/kesl-control --start-t 1
```

- задачу проверки памяти процессов:

```
/opt/kaspersky/kesl/bin/kesl-control --start-t 4 -W
```

- задачу проверки загрузочных секторов:

```
/opt/kaspersky/kesl/bin/kesl-control --start-t 5 -W
```

3. Создайте модуль правил на основе блокирующих записей:

```
grep kesl /var/log/audit/audit.log | audit2allow -M kesl
```

Убедитесь, что созданный список содержит только правила, относящиеся к Kaspersky Endpoint Security.

4. Загрузите полученный модуль правил:

```
# semodule -i kesl.pp
```

5. Переведите SELinux в принудительный режим:

```
# setenforce Enforcing
```

В случае появления новых audit-сообщений, связанных с Kaspersky Endpoint Security, следует обновлять файл модуля правил (см. раздел "Обновление файла модуля правил" на стр. [38](#)).

Дополнительную информацию вы можете найти в документации для используемой операционной системы.

Настройка разрешающих правил в системе AppArmor

► Чтобы обновить профили AppArmor, необходимые для работы Kaspersky Endpoint Security, выполните следующие действия:

1. Убедитесь, что модуль AppArmor загружен одним из следующих способов:

- `systemctl status apparmor`
- `/etc/init.d/apparmor status`

2. Создайте профиль Kaspersky Endpoint Security:

a. В первой консоли выполните команды:

```
cd /etc/apparmor.d
aa-genprof /opt/kaspersky/kesl/libexec/kesl
```

b. Во второй консоли запустите следующие задачи:

- задачу постоянной защиты:

```
/opt/kaspersky/kesl/bin/kesl-control --start-t 1
```

- задачу проверки памяти процессов:

```
/opt/kaspersky/kesl/bin/kesl-control --start-t 4 -W
```

- задачу проверки загрузочных секторов:

```
opt/kaspersky/kesl/bin/kesl-control --start-t 5 -W
```

- задачу обновления:

```
/opt/kaspersky/kesl/bin/kesl-control --start-t 6 -W
```

с. В первой консоли нажмите **S**. После завершения сканирования событий нажмите **F**.

3. Переведите созданный профиль Kaspersky Endpoint Security в режим показа сообщений:

```
aa-complain opt.kaspersky.kesl.libexec.kesl
```

4. Через несколько дней работы программы обновите профиль, запустив команду:

```
aa-logprof
```

Укажите разрешения `Allow` или `Glob` на все файлы, которые Kaspersky Endpoint Security использовал в течение этого периода.

5. Переводите профиль Kaspersky Endpoint Security в блокирующий режим:

```
aa-enforce opt.kaspersky.kesl.libexec.kesl
```

В случае появления новых audit-сообщений, связанных с Kaspersky Endpoint Security, следует обновлять файл модуля правил (см. раздел "Обновление файла модуля правил" на стр. [38](#)).

Дополнительную информацию вы можете найти в документации для используемой операционной системы.

Обновление файла модуля правил

Установите пакет `poliscoreutils-python` перед использованием утилиты `audit2allow`.

► Чтобы обновить файл модуля правил, выполните следующие команды:

```
# audit2allow -l -M kesl -i /var/log/audit/audit.log
```

```
# semodule -u kesl.pp
```

Удаление программы

Этот раздел содержит инструкции о том, как удалить Kaspersky Endpoint Security локально или через Kaspersky Security Center.

Локальное удаление Kaspersky Endpoint Security

В процессе удаления программы все задачи Kaspersky Endpoint Security будут остановлены.

- ▶ Чтобы удалить Kaspersky Endpoint Security, установленный из пакета формата RPM, выполните следующую команду:

```
# rpm -e kesl
```

- ▶ Чтобы удалить Kaspersky Endpoint Security, установленный из пакета формата DEB, выполните следующую команду:

```
# dpkg -r kesl
```

- ▶ Чтобы удалить Агент администрирования, установленный из пакета формата RPM, выполните следующую команду:

```
# rpm -e klnagent
```

- ▶ Чтобы удалить Агент администрирования, установленный из пакета формата DEB, выполните следующую команду:

```
# dpkg -r klnagent
```

Программа автоматически выполняет процедуру удаления. По завершении программа выводит сообщение о результатах удаления.

Удаление Kaspersky Endpoint Security через Kaspersky Security Center

Вы можете удалить Kaspersky Endpoint Security через Kaspersky Security Center. Для этого вам нужно создать и запустить задачу удаления Kaspersky Endpoint Security.

Подробнее о создании и запуске задачи удаления Kaspersky Endpoint Security вы можете прочитать в *Руководстве администратора для Kaspersky Security Center*.

Лицензирование программы

Этот раздел содержит информацию об основных понятиях, связанных с лицензированием программы.

В этом разделе

О Лицензионном соглашении.....	40
О лицензии.....	41
О лицензионном сертификате	42
О коде активации	42
О ключе	43
О файле ключа	43
О подписке	44
О предоставлении данных	45

О Лицензионном соглашении

Лицензионное соглашение – это юридическое соглашение между вами и АО "Лаборатория Касперского", в котором указано, на каких условиях вы можете использовать программу.

Внимательно ознакомьтесь с условиями Лицензионного соглашения перед началом работы с программой.

Вы можете ознакомиться с условиями Лицензионного соглашения следующими способами:

- Во время установки Kaspersky Endpoint Security.
- Прочитав документ license.txt. Этот документ включен в комплект поставки программы.

Вы принимаете условия Лицензионного соглашения, подтверждая свое согласие с текстом Лицензионного соглашения во время установки программы. Если вы не согласны с условиями Лицензионного соглашения, вы должны прервать установку программы и не должны использовать программу.

О лицензии

Лицензия – это ограниченное по времени право на использование программы, предоставляемое вам на основе Лицензионного соглашения.

Лицензия включает в себя право на получение следующих видов услуг:

- использование программы в соответствии с условиями Лицензионного соглашения;
- получение технической поддержки.

Объем предоставляемых услуг и срок использования программы зависят от типа лицензии, по которой была активирована программа.

Предусмотрены следующие типы лицензий:

- *Пробная* – бесплатная лицензия, предназначенная для ознакомления с программой.

Пробная лицензия имеет небольшой срок действия. По истечении срока действия пробной лицензии Kaspersky Endpoint Security прекращает выполнять все свои функции. Чтобы продолжить использование программы, вам нужно приобрести коммерческую лицензию.

Вы можете активировать программу по пробной лицензии только один раз.

- *Коммерческая* – платная лицензия, предоставляемая при приобретении программы.

По истечении срока действия коммерческой лицензии программа продолжает работу, но с ограниченной функциональностью (например, недоступно обновление баз Kaspersky Endpoint Security). Чтобы продолжить использование Kaspersky Endpoint Security в режиме полной функциональности, вам нужно продлить срок действия коммерческой лицензии.

Рекомендуется продлевать срок действия лицензии не позднее даты его окончания, чтобы обеспечить максимальную защиту от угроз компьютерной безопасности.

О лицензионном сертификате

Лицензионный сертификат – это документ, который передается вам вместе с файлом ключа или кодом активации.

В Лицензионном сертификате содержится следующая информация о предоставляемой лицензии:

- номер заказа;
- информация о пользователе, которому предоставляется лицензия;
- информация о программе, которую можно активировать по предоставляемой лицензии;
- ограничение на количество единиц лицензирования (например, устройств, на которых можно использовать программу по предоставляемой лицензии);
- дата начала срока действия лицензии;
- дата окончания срока действия лицензии или срок действия лицензии;
- тип лицензии.

О коде активации

Код активации – это уникальная последовательность из двадцати латинских букв и цифр. Вы вводите код активации, чтобы добавить ключ, активирующий Kaspersky Endpoint Security. Вы получаете код активации по указанному вами адресу электронной почты после приобретения Kaspersky Endpoint Security или после заказа пробной версии Kaspersky Endpoint Security.

Чтобы активировать программу с помощью кода активации, требуется доступ в интернет для подключения к серверам активации "Лаборатории Касперского".

Если код активации был потерян после активации программы, вы можете восстановить код активации. Вам может потребоваться код активации, например, для регистрации в Kaspersky CompanyAccount. Для восстановления кода активации требуется обратиться в Службу технической поддержки "Лаборатории Касперского" (см. раздел "Способы получения технической поддержки" на стр. [114](#)).

О ключе

Ключ – последовательность бит, с помощью которой вы можете активировать и затем использовать программу в соответствии с условиями Лицензионного соглашения. Ключ создается специалистами "Лаборатории Касперского".

Вы можете добавить ключ в программу одним из следующих способов: применить *файл ключа* или ввести *код активации*. Ключ отображается в интерфейсе программы в виде уникальной буквенно-цифровой последовательности, после того как вы добавили его в программу.

Ключ может быть заблокирован "Лабораторией Касперского", если условия Лицензионного соглашения нарушены. Если ключ заблокирован, для работы программы требуется добавить другой ключ.

Ключ может быть активным и дополнительным.

Активный ключ – ключ, используемый в текущий момент для работы программы. В качестве активного может быть добавлен ключ для пробной или коммерческой лицензии. В программе не может быть больше одного активного ключа.

Дополнительный ключ – ключ, подтверждающий право на использование программы, но не используемый в текущий момент. Дополнительный ключ автоматически становится активным, когда заканчивается срок действия лицензии, связанной с текущим активным ключом. Дополнительный ключ может быть добавлен только при наличии активного ключа.

Ключ для пробной лицензии может быть добавлен только в качестве активного ключа. Ключ для пробной лицензии не может быть добавлен в качестве дополнительного ключа.

О файле ключа

Файл ключа – это файл с расширением key, который вам предоставляет "Лаборатория Касперского". Файл ключа предназначен для добавления ключа, активирующего программу.

Вы получаете файл ключа по указанному вами адресу электронной почты после приобретения Kaspersky Endpoint Security или после заказа пробной версии Kaspersky Endpoint Security.

Чтобы активировать программу с помощью файла ключа, не требуется подключение к серверам активации "Лаборатории Касперского".

Если файл ключа был случайно удален, вы можете его восстановить. Файл ключа может потребоваться вам, например, для регистрации в Kaspersky CompanyAccount.

Для восстановления файла ключа вам нужно выполнить одно из следующих действий:

- Обратиться в Службу технической поддержки (<http://support.kaspersky.ru>).
- Получить файл ключа на веб-сайте "Лаборатории Касперского" (<https://activation.kaspersky.com/ru/>) на основе имеющегося кода активации.

О подписке

Подписка на Kaspersky Endpoint Security – это заказ на использование программы с выбранными параметрами (дата окончания подписки, количество защищаемых устройств). Подписку на Kaspersky Endpoint Security можно зарегистрировать у поставщика услуг (например, у интернет-провайдера). Подписку можно продлевать вручную или в автоматическом режиме или отказаться от нее. Управление подпиской доступно на веб-сайте поставщика услуг.

Подписка может быть ограниченной (например, на один год) или неограниченной (без даты окончания). Для продолжения работы Kaspersky Endpoint Security после окончания ограниченной подписки ее требуется продлевать. Неограниченная подписка продлевается автоматически при условии своевременного внесения предоплаты поставщику услуг.

Если подписка ограничена, по ее истечении может предоставляться буферный период для продления подписки, в течение которого функциональность программы сохраняется. Наличие и длительность буферного периода определяет поставщик услуг.

Чтобы использовать Kaspersky Endpoint Security по подписке, требуется применить код активации, предоставленный поставщиком услуг. После применения кода активации устанавливается активный ключ, определяющий лицензию на использование программы по подписке. При этом дополнительный ключ может быть установлен только с помощью кода активации и не может быть установлен с помощью файла ключа или по подписке.

Функциональность программы, доступная по подписке, может соответствовать функциональности программы для следующих видов коммерческой лицензии: Стандартная, Kaspersky Business Space Security, Kaspersky Enterprise Space Security. Лицензии этих видов предназначены для защиты файловых серверов, рабочих станций и мобильных устройств, позволяют использовать компоненты контроля на рабочих станциях и мобильных устройствах.

В зависимости от поставщика услуг, набор возможных действий для управления подпиской может различаться. Поставщик услуг может не предоставлять буферный период для продления подписки, в течение которого функциональность программы сохраняется.

Коды активации, приобретенные по подписке, не могут быть использованы для активации предыдущих версий Kaspersky Endpoint Security.

О предоставлении данных

Принимая условия Лицензионного соглашения, вы соглашаетесь передавать в автоматическом режиме следующую информацию:

- информацию, связанную с активацией программы по активационному коду;
- статистику об использовании задачи постоянной защиты и задач проверки по требованию;
- идентификатор программы;
- версию программы;
- идентификатор компьютера, на котором установлена программа;
- название и версию используемой операционной системы (включая названия и версии установленных обновлений).

Принимая условия Положения о Kaspersky Security Network, вы дополнительно соглашаетесь передавать в автоматическом режиме следующую информацию:

- информацию о дате и длительности установки программы на компьютере;
- идентификатор партнера, у которого приобретена лицензия;
- тип установки программы на компьютере (первичная установка);
- данные об установленной на компьютере операционной системе (в том числе название, тип и разрядность);
- информацию о запускаемых на компьютере приложениях;
- хеш (MD5) исполняемого файла и количество запусков файла с момента последнего предоставления информации;
- полный путь на компьютере к исполняемому файлу;
- идентификатор наличия у файла действительной электронно-цифровой подписи;
- идентификатор, указывающий один из стандартных путей в системе расположения запускаемого файла;
- хеш (MD5) и категория, к которой отнесен проверяемый объект (по версии правообладателя);
- идентификатор источника категоризации;
- информацию о производителе (vendor name) объекта и идентификатор получения информации о производителе;
- версию проверяемого объекта;
- информацию о версии используемых программой баз категоризации файлов и идентификатор использованной записи базы при проверке;
- идентификатор компонента программы, запросившего категорию объекта.

Полученная информация защищается "Лабораторией Касперского" в соответствии с установленными законом требованиями и действующими правилами "Лаборатории Касперского".

"Лаборатория Касперского" использует полученную информацию только в обезличенном виде и в виде данных общей статистики. Данные общей статистики формируются автоматически из исходной полученной информации и не содержат персональных и иных конфиденциальных данных. Исходная полученная информация уничтожается по мере накопления (один раз в год). Данные общей статистики хранятся бессрочно.

Более подробную информацию о получении, обработке, хранении и уничтожении информации об использовании программы после принятия Лицензионного соглашения вы можете узнать, прочитав его текст, и на веб-сайте «Лаборатории Касперского» (<http://www.kaspersky.ru/privacy>). Файл license.txt с текстом Лицензионного соглашения входит в комплект поставки программы.

Запуск и остановка программы

По умолчанию Kaspersky Endpoint Security запускается автоматически при запуске операционной системы (на уровнях выполнения по умолчанию, принятых для каждой операционной системы). Kaspersky Endpoint Security запускает все служебные задачи, а также пользовательские задачи, в параметрах расписания которых задан режим запуска PS.

Если вы остановите Kaspersky Endpoint Security, все выполняющиеся задачи будут прерваны. После повторного запуска Kaspersky Endpoint Security прерванные пользовательские задачи не будут автоматически возобновлены. Только те пользовательские задачи, в параметрах расписания которых задан режим запуска PS, будут запущены снова.

- ▶ *Чтобы запустить Kaspersky Endpoint Security, выполните следующую команду:*

```
/etc/init.d/kesl-supervisor start
```

- ▶ *Чтобы остановить Kaspersky Endpoint Security, выполните следующую команду:*

```
/etc/init.d/kesl-supervisor stop
```

- ▶ *Чтобы перезапустить Kaspersky Endpoint Security, выполните следующую команду:*

```
/etc/init.d/kesl-supervisor restart
```

- ▶ *Чтобы вывести статус Kaspersky Endpoint Security, выполните следующую команду:*

```
/etc/init.d/kesl-supervisor status
```

- ▶ *Чтобы запустить Kaspersky Endpoint Security в systemd-системе, выполните следующую команду:*

```
systemctl start kesl-supervisor
```

- ▶ *Чтобы остановить Kaspersky Endpoint Security в systemd-системе, выполните следующую команду:*

```
systemctl stop kesl-supervisor
```

- ▶ *Чтобы перезапустить Kaspersky Endpoint Security в systemd-системе, выполните следующую команду:*

```
systemctl restart kesl-supervisor
```

- ▶ *Чтобы вывести статус Kaspersky Endpoint Security в systemd-системе, выполните следующую команду:*

```
systemctl status kesl-supervisor
```

Управление задачами Kaspersky Endpoint Security

Этот раздел содержит информацию о типах задач Kaspersky Endpoint Security и инструкции о том, как управлять задачами.

В этом разделе

О задачах Kaspersky Endpoint Security	49
Просмотр списка задач Kaspersky Endpoint Security	51
Создание задачи	51
Запуск и остановка задачи	51
Удаление задачи	51
Приостановка и возобновление задачи	52
Настройка расписания задачи	52
Просмотр состояния задачи	53

О задачах Kaspersky Endpoint Security

Вы можете управлять работой программы Kaspersky Endpoint Security с помощью задач как локально на компьютерах (с помощью командной строки или конфигурационных файлов), так и централизованно через Kaspersky Security Center (см. раздел «Управление программой через Kaspersky Security Center» на стр. [90](#)).

Для работы с Kaspersky Endpoint Security существует два типа задач:

- *Предустановленная задача* – задача, которая создается во время установки программы. Вы не можете создавать или удалять предустановленные задачи, но вы можете изменять параметры этих задач.

- *Пользовательская задача* – задача, которую вы можете создавать или удалять самостоятельно.

Вы можете управлять следующими задачами:

- **File_Monitoring** – задача постоянной защиты (ID=1, тип – OAS);
- **Scan_My_Computer** – задача проверки по требованию (ID=2, тип – ODS);
- **Scan_File** – задача выборочной проверки (ID=3, тип – ODS). По умолчанию параметры этой задачи совпадают с параметрами задачи Scan_My_Computer;
- **Boot_Scan** – задача проверки загрузочных секторов (ID=4, тип – BootScan);
- **Memory_Scan** – задача проверки системной памяти (ID=5, тип – MemoryScan);
- **Update** – задача обновления (ID=6, тип – Update);
- **Rollback** – задача отката обновлений (ID=7, тип – Rollback). В этой задаче нет параметров. Вы можете только управлять этой задачей;
- **Retranslate** – задача копирования обновлений (ID=8, тип – Retranslate).
- **License** – задача, реализующая сервер лицензий (ID=9, тип – License);
- **Backup** – задача, управляющая резервным хранилищем (ID=10, тип – Backup).

Вы можете выполнять следующие действия над задачами:

- запускать и останавливать задачи;
- создавать и удалять задачи (только для пользовательских задач);
- изменять параметры задач.

ID – номер задачи, который Kaspersky Endpoint Security присваивает задаче при ее создании.

Просмотр списка задач Kaspersky Endpoint Security

- ▶ Чтобы просмотреть список задач Kaspersky Endpoint Security, выполните следующую команду:

```
/opt/kaspersky/kesl/bin/kesl-control --get-task-list
```

Создание задачи

Вы можете создавать задачи.

- ▶ Чтобы создать задачу, выполните следующую команду:

```
/opt/kaspersky/kesl/bin/kesl-control --create-task <имя задачи>  
--type <тип задачи>
```

Запуск и остановка задачи

Вы можете запускать и останавливать только задачи типов OAS, ODS, BootScan, MemoryScan, Rollback, Retranslate и Update.

Вы не можете запускать и останавливать задачи типов Backup и License.

- ▶ Чтобы запустить задачу, выполните следующую команду:

```
/opt/kaspersky/kesl/bin/kesl-control  
--start-task <ID_задачи>|<имя_задачи>
```

- ▶ Чтобы остановить задачу, выполните следующую команду:

```
/opt/kaspersky/kesl/bin/kesl-control  
--stop-task <ID задачи>|<имя задачи>
```

Удаление задачи

Вы можете удалять задачи, которые вы создали (пользовательские задачи).

- ▶ Чтобы удалить задачу, выполните следующую команду:

```
/opt/kaspersky/kesl/bin/kesl-control  
--delete-task <ID задачи>|<имя задачи>
```

Приостановка и возобновление задачи

Вы можете приостанавливать и возобновлять выполнение задач типов ODS, BootScan, MemoryScan, Rollback, Retranslate и Update.

- ▶ *Чтобы приостановить задачу, выполните команду:*

```
/opt/kaspersky/kesl/bin/kesl-control  
--suspend-task <ID задачи>|<имя задачи>
```

После выполнения команды выполнение задачи приостанавливается.

- ▶ *Чтобы возобновить задачу, выполните команду:*

```
/opt/kaspersky/kesl/bin/kesl-control  
--resume-task <ID задачи>|<имя задачи>
```

После выполнения команды выполнение задачи возобновляется.

Настройка расписания задачи

- ▶ *Чтобы настроить расписание задачи, выполните следующие действия:*

1. Сохраните параметры расписания задачи в конфигурационный файл с помощью следующей команды:

```
/opt/kaspersky/kesl/bin/kesl-control  
--get-schedule <ID задачи>|<имя задачи> --file <полный путь к файлу>
```

2. Откройте конфигурационный файл для редактирования.
3. Задайте параметры расписания.
4. Сохраните изменения в конфигурационном файле.
5. Импортируйте параметры расписания в задачу с помощью следующей команды:

```
/opt/kaspersky/kesl/bin/kesl-control --set-schedule  
<ID задачи>|<имя задачи> --file <полный путь к файлу>
```

См. также

Просмотр состояния задачи	53
---------------------------------	--------------------

Просмотр состояния задачи

Вы можете просматривать состояние задачи.

Задачи Kaspersky Endpoint Security могут находиться в одном из следующих состояний:

- **Started** – выполняется;
- **Starting** – запускается;
- **Stopped** – остановлена;
- **Stopping** – останавливается;
- **Suspended** – приостановлена;
- **Suspending** – приостанавливается;
- **Resumed** – возобновлена;
- **Resuming** – возобновляется.

► Чтобы просмотреть состояние задачи, выполните команду:

```
/opt/kaspersky/kesl/bin/kesl-control  
--get-task-state <ID задачи>|<имя задачи>
```

Обновление баз и модулей программы

Этот раздел содержит информацию об обновлении баз и модулей программы и инструкции о том, как настраивать параметры обновления.

В этом разделе

Об обновлении баз и модулей программы	54
Об источниках обновлений.....	55
Настройка параметров обновления.....	56
Откат обновления баз.....	59
Копирование обновлений	59

Об обновлении баз и модулей программы

В течение срока действия лицензии вы можете получать обновления баз и модулей Kaspersky Endpoint Security. Базы представляют собой файлы с записями. Эти записи содержат информацию о контрольных участках кода угроз и алгоритмы лечения объектов, в которых содержатся эти угрозы.

Вирусные аналитики "Лаборатории Касперского" ежедневно обнаруживают множество новых угроз. Они создают для этих угроз идентифицирующие записи и включают их в обновления баз. *Обновление баз* представляет собой один или несколько файлов с такими записями. Чтобы свести риск заражения сервера к минимуму, рекомендуется регулярно получать обновления баз.

Обновление баз программы

Во время установки Kaspersky Endpoint Security получает актуальные базы с одного из HTTP-серверов обновлений "Лаборатории Касперского". Если для обновления используется предустановленная задача с параметрами по умолчанию (ID=6), Kaspersky Endpoint Security обновляет базы с периодичностью один раз в 60 минут. Вы можете изменять параметры предустановленной задачи обновления баз и модулей программы и создавать пользовательские задачи обновления.

Kaspersky Endpoint Security продолжает использовать предыдущую установленную версию баз, если загрузка обновлений баз прерывается или завершается с ошибкой.

По умолчанию программа записывает в журнал событие *Базы устарели* (AVBasesAreOutOfDate), если последние установленные обновления баз были опубликованы на сервере "Лаборатории Касперского" более недели назад. Если базы не обновляются в течение двух недель, Kaspersky Endpoint Security записывает в журнал событие *Базы сильно устарели* (AVBasesAreTotallyOutOfDate).

Об источниках обновлений

Источник обновлений – это ресурс, содержащий обновления баз и модулей программы Kaspersky Endpoint Security. Источником обновлений могут быть FTP- или HTTP-серверы (например, Kaspersky Security Center, серверы обновлений «Лаборатории Касперского»), локальные или сетевые директории, примонтированные пользователем.

В предустановленной задаче обновления по умолчанию в качестве источника обновлений выбраны серверы обновлений "Лаборатории Касперского". На серверах обновлений выкладываются обновления баз и программных модулей для многих программ "Лаборатории Касперского". Обновления загружаются по протоколам HTTP.

Если по каким-то причинам вы не можете использовать в качестве источника обновлений серверы обновлений "Лаборатории Касперского", вы можете получать обновления из *пользовательского источника обновлений* – указанной вами локальной или сетевой директории (SMB / NFS), примонтированной пользователем, или FTP- или HTTP-сервера. Вы можете указать пользовательский источник обновлений в конфигурационном файле задачи обновления.

Настройка параметров обновления

Вы можете настраивать следующие параметры обновления:

- источник обновлений (см. раздел "Выбор источника обновлений" на стр. [57](#));
- включать / выключать использование прокси-сервера, если вы используете прокси-сервер для подключения к интернету (см. раздел "Использование прокси-сервера при доступе к источникам обновлений" на стр. [58](#)).

Параметры обновления содержатся в конфигурационном файле, который использует задача обновления. Структура конфигурационного файла, подробное описание используемых параметров и их возможных значений содержатся в разделе Параметры задач обновления (см. раздел "Параметры задач обновления и задач копирования обновлений" на стр. [140](#)).

Создание задачи обновления

Для получения обновлений вы можете создать задачу обновления с параметрами по умолчанию или с заданным вами набором параметров.

- *Чтобы создать задачу обновления с параметрами по умолчанию, выполните команду:*

```
/opt/kaspersky/kesl/bin/kesl-control --create-task <имя задачи>  
--type Update
```

Созданная задача автоматически работает с параметрами по умолчанию (см. раздел "Параметры задач обновления и задач копирования обновлений" на стр. [140](#)).

- *Чтобы создать задачу обновления с заданным набором параметров, выполните следующие действия:*

1. Создайте конфигурационный файл (см. стр. [117](#)) с параметрами, которые вы хотите установить в задаче обновления.
2. Выполните команду:

```
/opt/kaspersky/kesl/bin/kesl-control --create-task <имя задачи>  
--type Update --file <имя конфигурационного файла>
```

Созданная задача автоматически работает с параметрами, заданными в конфигурационном файле.

Выбор источника обновлений

► Чтобы выбрать источник обновлений, выполните следующие действия:

1. Сохраните параметры задачи обновления в конфигурационном файле с помощью следующей команды:

```
/opt/kaspersky/kesl/bin/kesl-control --get-settings 6  
--file <полный путь к файлу>
```

2. Откройте созданный конфигурационный файл для редактирования. Укажите значение параметра `SourceType`:

- `KLServers` – чтобы загружать обновления с серверов обновлений "Лаборатории Касперского";
- `SCServer` – чтобы загружать обновления с Сервера администрирования Kaspersky Security Center;
- `Custom` – чтобы загружать обновления из пользовательского (указанного вами) источника.

Пример:

```
SourceType="KLServers"
```

Для пользовательского источника обновлений настройте дополнительные параметры в секции `[CustomSources.item_#]` (см. стр. [143](#)):

- `URL` – адрес HTTP-сервера или директории, которая является источником обновлений.
 - `Enabled` – состояние источника обновлений (`Yes` – источник обновлений используется, `No` – источник обновлений не используется). Если вы выбрали значение параметра `Enabled=No`, программа не использует источник обновлений, указанный параметром `URL`.
3. Настройте дополнительные параметры обновления (не обязательно).

4. Сохраните изменения в конфигурационном файле.
5. Импортируйте параметры из конфигурационного файла в задачу обновления с помощью следующей команды:

```
/opt/kaspersky/kesl/bin/kesl-control --set-settings 6  
--file <полный путь к файлу>
```

Kaspersky Endpoint Security применяет новые значения параметров задачи обновления немедленно.

Использование прокси-сервера при доступе к источникам обновлений

► Чтобы включить использование прокси-сервера при доступе к источникам обновлений, выполните следующие действия:

1. Сохраните параметры задачи обновления в конфигурационном файле с помощью следующей команды:

```
/opt/kaspersky/kesl/bin/kesl-control --get-settings 6  
--file <полный путь к файлу>
```

2. Откройте созданный конфигурационный файл для редактирования. Укажите источник обновлений:

- Чтобы использовать прокси-сервер при доступе к серверам обновлений "Лаборатории Касперского", укажите `IgnoreProxySettingsForKLServers=No`.
- Чтобы использовать прокси-сервер при доступе к пользовательским источникам обновлений, укажите `IgnoreProxySettingsForCustomSources=No`.

3. Сохраните изменения в конфигурационном файле.
4. Импортируйте параметры из конфигурационного файла в задачу обновления с помощью следующей команды:

```
/opt/kaspersky/kesl/bin/kesl-control --set-settings 6  
--file <полный путь к файлу>
```

Откат обновления баз

- ▶ Чтобы откатить обновления антивирусных баз, выполните команду:

```
/opt/kaspersky/kesl/bin/kesl-control --start-task Rollback
```

В результате программа запустит предустановленную задачу отката обновления баз. Выполнение задачи отката обновления баз возможно, если ранее было выполнено не менее двух успешных обновлений антивирусных баз.

Копирование обновлений

Для копирования обновлений вы можете создать задачу копирования обновлений с параметрами по умолчанию или с заданным вами набором параметров.

- ▶ Чтобы создать задачу копирования обновлений с параметрами по умолчанию, выполните команду:

```
/opt/kaspersky/kesl/bin/kesl-control --create-task <имя задачи>  
--type Retranslate
```

Созданная задача автоматически работает с параметрами по умолчанию (см. раздел "Параметры задач обновления и задач копирования обновлений" на стр. [140](#)).

- ▶ Чтобы создать задачу копирования обновлений с заданным набором параметров, выполните следующие действия:

1. Создайте конфигурационный файл (см. стр. [117](#)) с параметрами, которые вы хотите установить в задаче копирования обновлений.
2. Выполните команду:

```
/opt/kaspersky/kesl/bin/kesl-control --create-task <имя задачи>  
--type Retranslate --file <имя конфигурационного файла>
```

Созданная задача автоматически работает с параметрами, заданными в конфигурационном файле.

Постоянная защита и проверка по требованию

Этот раздел содержит информацию о том, как Kaspersky Endpoint Security защищает и проверяет серверы. Постоянная защита и проверка по требованию выполняются с помощью предустановленных и пользовательских задач. Раздел содержит инструкции о том, как создавать и настраивать задачи постоянной защиты и проверки по требованию:

- формировать области защиты и области проверки, а также исключения из этих областей;
- выбирать действия программы с зараженными объектами;
- настраивать продолжительность проверки и другие параметры.

В этом разделе

О постоянной защите	61
О проверке по требованию	63
О зараженных файлах	65
Создание пользовательской задачи проверки по требованию	65
Формирование области защиты и области проверки.....	66
Об эвристическом анализе.....	68
Включение и настройка эвристического анализатора	68
Исключение объектов из областей защиты и проверки по требованию	70
Выбор режима постоянной защиты	72
Выбор действий программы над зараженными объектами.....	74
Выборочная проверка файлов и директорий (Scan_File)	75

Проверка загрузочных секторов.....	75
Проверка памяти процессов.....	76
Сокращение времени проверки	76
Особенности проверки символических и жестких ссылок	78
Настройка совместной работы: Антивирус Касперского для Linux Mail Server.....	79

О постоянной защите

Постоянная защита позволяет избежать заражения файловой системы компьютера. Задача постоянной защиты создается с параметрами по умолчанию при установке Kaspersky Endpoint Security на компьютер. По умолчанию задача постоянной защиты запускается автоматически при старте Kaspersky Endpoint Security. Задача постоянно находится в оперативной памяти компьютера и проверяет все открываемые, сохраняемые и запускаемые файлы. Вы можете останавливать и запускать ее.

Вы не можете создавать пользовательские задачи постоянной защиты. Вы можете изменять параметры предустановленной задачи постоянной защиты.

Параметры постоянной защиты содержатся в конфигурационном файле, который использует задача постоянной защиты. Структура конфигурационного файла, подробное описание используемых параметров и их возможных значений содержатся в разделе "Параметры задачи постоянной защиты и задач проверки по требованию" (см. стр. [123](#)).

По умолчанию задача постоянной защиты работает со следующими параметрами:

- `ScanArchived=No` – не проверять архивы.
- `ScanSfxArchived=No` – не проверять самораспаковывающиеся архивы (self-extracting archives).
- `ScanMailBases=No` – не проверять почтовые базы.

- `ScanPlainMail=No` – не проверять сообщения электронной почты в текстовом формате (plain text).
- `UseTimeLimit=Yes` – включить применение параметра `TimeLimit`.
- `TimeLimit=60` – установить максимальную продолжительность проверки объекта 60 секунд.
- `UseSizeLimit=No` – отключить применение параметра `SizeLimit`.
- `SizeLimit=0` – проверять объекты любого размера.
- `FirstAction=Recommended` – установить `Recommended` (рекомендуемое) как первое действие над зараженным объектом.
- `SecondAction=Block` – установить `Block` (блокировать) как второе действие над зараженным объектом.
- `UseExcludeMasks=No` – не исключать объекты из области защиты по маскам.
- `UseExcludeThreats=No` – не исключать объекты из области защиты по названию угрозы.
- `ReportCleanObjects=No` – не записывать в журнал информацию о незараженных объектах.
- `ReportPackedObjects=No` – не записывать в журнал информацию о проверке объектов в составе упакованных файлов.
- `ReportUnprocessedObjects=No` – не записывать в журнал информацию о непроверенных объектах.
- `UseAnalyzer=Yes` – включить использование эвристического анализатора.
- `HeuristicLevel=Recommended` – установить рекомендуемый уровень эвристического анализа.
- `UseIChecker=Yes` – использовать технологию `iChecker™`.

- `ScanByAccessType=SmartCheck` – применять интеллектуальный режим (`SmartCheck`) проверки объектов в зависимости от типа доступа к ним.
- `[ScanScope.item_0000]` – секция, содержащая параметры для формирования области защиты.
- `AreaDesc=All objects` – описание области защиты (все объекты).
- `UseScanArea=Yes` – проверять указанную область.
- `Path=/` – проверять все локальные директории компьютера; проверять директории, смонтированные с помощью SMB и NFS.
- `AreaMask.item_0000=*` – проверять все объекты в области защиты.

О проверке по требованию

Проверка по требованию – это однократная полная или выборочная проверка файлов на компьютере, которую Kaspersky Endpoint Security. Kaspersky Endpoint Security может выполнять одновременно несколько задач проверки по требованию.

В Kaspersky Endpoint Security по умолчанию создана одна предустановленная задача проверки по требованию – полная проверка. Программа проверяет все объекты, расположенные на локальных дисках компьютера, а также все смонтированные и разделяемые объекты, доступ к которым предоставляется по протоколам Samba и NFS, с рекомендуемыми параметрами безопасности.

Вы можете создавать пользовательские задачи проверки по требованию самостоятельно.

Также в Kaspersky Endpoint Security по умолчанию создана предустановленная задача выборочной проверки.

Параметры проверки по требованию содержатся в конфигурационном файле, который использует задача проверки по требованию. Структура конфигурационного файла, подробное описание используемых параметров и их возможных значений содержатся в разделе "Параметры задачи постоянной защиты и задач проверки по требованию" (см. стр. [123](#)).

По умолчанию задача проверки по требованию работает со следующими параметрами:

- `ScanArchived=Yes` – проверять архивы.
- `ScanSfxArchived=Yes` – проверять самораспаковывающиеся архивы (self-extracting archives).
- `ScanMailBases=No` – не проверять почтовые базы.
- `ScanPlainMail=No` – не проверять сообщения электронной почты в текстовом формате (plain text).
- `UseTimeLimit=No` – выключить применение параметра `TimeLimit`.
- `TimeLimit=0` – не устанавливать максимальную продолжительность проверки объекта.
- `UseSizeLimit=No` – отключить применение параметра `SizeLimit`.
- `SizeLimit=0` – не устанавливать максимальный размер проверяемого объекта.
- `FirstAction=Recommended` – установить `Recommended` (рекомендуемое) как первое действие над зараженным объектом.
- `SecondAction=Skip` – установить `Skip` (пропускать) как второе действие над зараженным объектом.
- `UseExcludeMasks=No` – не исключать объекты из области проверки по маскам.
- `UseExcludeThreats=No` – не исключать объекты из области проверки по названию угрозы.
- `ReportCleanObjects=No` – не записывать в журнал информацию о незараженных объектах.
- `ReportPackedObjects=No` – не записывать в журнал информацию о проверке объектов в составе упакованных файлов.
- `ReportUnprocessedObjects=No` – не записывать в журнал информацию о непроверенных объектах.

- `UseAnalyzer=Yes` – включить использование эвристического анализатора.
- `HeuristicLevel=Recommended` – установить рекомендуемый уровень эвристического анализа.
- `UseIChecker=Yes` – использовать технологию iChecker.
- `[ScanScope.item_0000]` – секция, содержащая параметры для формирования области проверки.
- `AreaDesc=All objects` – описание области проверки (все объекты).
- `UseScanArea=Yes` – проверять указанную область.
- `Path=/` – проверять все локальные директории компьютера; проверять директории, смонтированные с помощью SMB и NFS.
- `AreaMask.item_0000=*` – проверять все объекты в области проверки.

О зараженных файлах

При проверке файлов Kaspersky Endpoint Security использует антивирусные базы. Базы содержат файлы с фрагментами кода угроз и алгоритмы лечения объектов, в которых содержатся эти угрозы. Антивирусные базы позволяют обнаруживать в проверяемых файлах известные угрозы.

Если в файле содержится код, который полностью совпадает с кодом известной угрозы, Kaspersky Endpoint Security присваивает файлу статус *Зараженный*.

Создание пользовательской задачи проверки по требованию

- Чтобы создать задачу проверки по требованию с параметрами по умолчанию, выполните следующую команду:

```
/opt/kaspersky/kes1/bin/kes1-control --create-task <имя задачи>
--type ODS
```

В результате выполнения команды будет создана новая задача проверки по требованию с параметрами предустановленной задачи полной проверки.

► *Чтобы создать задачу с собственным конфигурационным файлом, выполните следующие действия:*

1. Создайте конфигурационный файл с параметрами (см. стр. [117](#)), которые вы хотите установить в задаче проверки по требованию.
2. Выполните следующую команду:

```
/opt/kaspersky/kesl/bin/kesl-control --create-task <имя задачи>  
--type ODS --file <имя конфигурационного файла>
```

В результате будет создана новая задача проверки по требованию с параметрами, заданными в конфигурационном файле.

Формирование области защиты и области проверки

Совокупность открываемых, изменяемых и сохраняемых объектов, которые проверяет задача постоянной защиты во время работы, называется *областью защиты*. Область защиты указывается в конфигурационном файле задачи постоянной защиты.

По умолчанию задача постоянной защиты проверяет все открываемые, изменяемые и сохраняемые объекты, находящиеся на локальных дисках компьютера, а также все смонтированные и разделяемые объекты, доступ к которым предоставляется по протоколам SMB и NFS.

Совокупность объектов файловой системы компьютера, которые проверяет задача проверки по требованию, называется *областью проверки*. Область проверки указывается в конфигурационном файле задачи проверки. Область проверки предустановленной задачи проверки по требованию – все объекты, находящиеся на локальных дисках компьютера, а также все смонтированные и разделяемые объекты, доступ к которым предоставляется по протоколам SMB и NFS.

Вы можете изменять области защиты и области проверки в предустановленных и пользовательских задачах.

Kaspersky Endpoint Security проверяет объекты в указанных областях в том порядке, в каком эти области пронумерованы в конфигурационном файле задачи.

► Чтобы добавить объекты для проверки в область защиты или область проверки, выполните следующие действия:

1. Сохраните параметры задачи постоянной защиты или задачи проверки по требованию в конфигурационном файле с помощью следующей команды:

```
/opt/kaspersky/kesl/bin/kesl-control --get-settings <ID задачи>  
--file <полный путь к файлу>
```

2. Откройте созданный конфигурационный файл для редактирования.
3. Добавьте в созданный файл секцию [ScanScope.item_#]. В секции укажите значения следующих параметров:
 - AreaMask, задающий маску имен объектов для проверки;
 - AreaDesc, задающий название области защиты или область проверки.
 - Path, задающий путь к проверяемым объектам.
 - UseScanArea, включающий проверку области защиты или области проверки в задаче.

Пример:

```
AreaMask.item_0000=*exe – проверять все объекты с расширением exe.  
AreaMask.item_0001=*doc – проверять все объекты с расширением doc.
```

4. Сохраните изменения в конфигурационном файле.
5. Импортируйте параметры из конфигурационного файла в задачу постоянной защиты или в задачу проверки по требованию с помощью следующей команды:

```
/opt/kaspersky/kesl/bin/kesl-control --set-settings <ID задачи>  
--file <полный путь к файлу>
```

В результате во время выполнения задачи постоянной защиты или проверки по требованию Kaspersky Endpoint Security будет проверять объекты, по умолчанию входящие в область постоянной защиты или проверки по требованию.

Об эвристическом анализе

Каждый день появляются вредоносные объекты, записи о которых еще не попали в антивирусные базы. Чтобы обнаруживать в файлах такие вредоносные объекты, Kaspersky Endpoint Security использует *эвристический анализатор*.

Эвристический анализ позволяет программе распознавать новые угрозы еще до того, как они станут известны вирусным аналитикам. Вы можете задать уровень эвристического анализа. Уровень эвристического анализа обеспечивает баланс между тщательностью поиска угроз, степенью загрузки ресурсов операционной системы и длительностью проверки. Чем выше установленный уровень эвристического анализа, тем больше ресурсов потребует проверка и больше времени займет.

Вы можете выбрать уровень эвристического анализа в зависимости от ваших требований к безопасности и скорости файлового обмена на компьютере:

- **Light (Поверхностный)** – наименее тщательная проверка, минимальная загрузка системы;
- **Medium (Средний)** – средний уровень эвристического анализа, сбалансированная загрузка системы;
- **Deep (Глубокий)** – наиболее тщательная проверка, максимальная загрузка системы;
- **Recommended (Рекомендуемый)** – рекомендуемое специалистами "Лаборатории Касперского" значение.

По умолчанию эвристический анализатор включен для задач постоянной защиты и проверки по требованию со значением `Recommended`.

Включение и настройка эвристического анализатора

В предустановленных задачах постоянной защиты и проверки по требованию эвристический анализатор по умолчанию включен. Уровень эвристического анализа по умолчанию: рекомендованный. Если вы используете задачи постоянной защиты и проверки

по требованию с вашими собственными наборами параметров, вам может потребоваться включить или выключить эвристический анализатор и настроить уровень эвристического анализа.

► *Чтобы включить эвристический анализатор и настроить уровень эвристического анализа, выполните следующие действия:*

1. Сохраните параметры задачи постоянной защиты или задачи проверки по требованию в конфигурационном файле с помощью следующей команды:

```
/opt/kaspersky/kesl/bin/kesl-control --get-settings <ID задачи>  
--file <полный путь к файлу>
```

2. Откройте созданный конфигурационный файл для редактирования.
3. Задайте значение `Yes` для параметра `UseAnalyzer`, чтобы включить эвристический анализатор.

Чтобы выключить эвристический анализатор, для параметра `UseAnalyzer` нужно задать значение `No`.

4. Задайте одно из следующих значений для параметра `HeuristicLevel`:

- `Recommended` – чтобы использовать рекомендованный уровень эвристического анализа;
- `Deep` – чтобы использовать высокий уровень эвристического анализа;
- `Medium` – чтобы использовать средний уровень эвристического анализа;
- `Light` – чтобы использовать низкий уровень эвристического анализа.

5. Сохраните изменения в конфигурационном файле.
6. Импортируйте параметры из конфигурационного файла в задачу постоянной защиты или в задачу проверки по требованию с помощью следующей команды:

```
/opt/kaspersky/kesl/bin/kesl-control --set-settings <ID задачи>  
--file <полный путь к файлу>
```

Исключение объектов из областей защиты и проверки по требованию

По умолчанию задачи постоянной защиты и проверки по требованию проверяют все объекты в области защиты и области проверки. Вы можете исключать некоторые объекты из области защиты и области проверки.

Исключение объектов из области защиты или области проверки

Вы можете формировать *глобальную область исключения*. Объекты в этой области исключаются из области защиты или из всех областей проверки, заданных в задаче постоянной защиты или в задаче проверки по требованию.

► *Чтобы сформировать глобальную область исключения, выполните следующие действия:*

1. Сохраните параметры задачи постоянной защиты или задачи проверки по требованию в конфигурационном файле с помощью следующей команды:

```
/opt/kaspersky/kesl/bin/kesl-control --get-settings <ID задачи>
--file <полный путь к файлу>
```

2. Откройте созданный конфигурационный файл для редактирования.
3. Добавьте в созданный конфигурационный файл секцию [ExcludedFromScanScope.item_#] (см. стр. [135](#)).
4. В секции [ExcludedFromScanScope.item_#] укажите значения следующих параметров:
 - AreaDesc, задает уникальное имя области исключения.
 - UseScanArea, указывает, будет ли Kaspersky Endpoint Security исключать область из проверки во время выполнения задачи.
 - Path, задает путь к объектам, исключаемым из проверки.

С помощью масок в формате командной оболочки вы можете задавать шаблон имени файла для исключения из области защиты или проверки по требованию.

5. Сохраните изменения в конфигурационном файле.
6. Импортируйте параметры из конфигурационного файла в задачу постоянной защиты или в задачу проверки по требованию с помощью следующей команды:

```
/opt/kaspersky/kesl/bin/kesl-control --set-settings <ID задачи>  
--file <полный путь к файлу>
```

Исключение объектов по названию обнаруженной угрозы

Когда Kaspersky Endpoint Security обнаруживает зараженный файл, программа обрабатывает его: выполняет над ним заданное действие (см. раздел "Выбор действий программы над зараженными объектами" на стр. [74](#)). Если вы считаете этот файл безопасным для компьютера, вы можете исключить его из проверки по названию обнаруженной угрозы. В этом случае Kaspersky Endpoint Security признает обнаруженные объекты безопасными и не обрабатывает их.

Полное название угрозы, обнаруженной в файле, содержит следующую информацию:

<класс объекта>:<тип объекта>.<краткое название операционной системы>.<имя объекта>.<код модификации объекта>. Например: **not-a-virus:NetTool.Linux.SynScan.a**.

Вы можете найти полное название типа угрозы, обнаруженной в файле, в журнале Kaspersky Endpoint Security и на веб-сайте Вирусной энциклопедии (<http://www.securelist.ru>).

При задании шаблонов названий обнаруживаемых объектов вы можете использовать маски в формате командной оболочки.

► *Чтобы исключить объекты из области защиты или области проверки по названию обнаруженной угрозы, выполните следующие действия:*

1. Сохраните параметры задачи постоянной защиты или задачи проверки по требованию в конфигурационном файле с помощью следующей команды:

```
/opt/kaspersky/kesl/bin/kesl-control --get-settings <ID задачи>  
--file <полный путь к файлу>
```

2. Откройте созданный конфигурационный файл для редактирования.
3. Присвойте значение `Yes` параметру `UseExcludeThreats`.
4. Задайте шаблон названия угроз с помощью параметра `ExcludeThreats`.

Чтобы задать несколько шаблонов названий угроз, повторите значение параметра `ExcludeThreats` нужное число раз с указанием порядкового номера `item_#`.

Пример:

```
ExcludeThreats.item_0000=EICAR-Test-*
```

```
ExcludeThreats.item_0001=?rojan.Linux
```

5. Сохраните изменения в конфигурационном файле.
6. Импортируйте параметры из конфигурационного файла в задачу постоянной защиты или в задачу проверки по требованию с помощью следующей команды:

```
/opt/kaspersky/kesl/bin/kesl-control --set-settings <ID задачи>  
--file <полный путь к файлу>
```

Выбор режима постоянной защиты

Выбор режима защиты объектов доступен только для задачи постоянной защиты (см. раздел "О постоянной защите" на стр. [61](#)).

Режим постоянной защиты определяет, при каком типе доступа к файлам Kaspersky Endpoint Security будет их проверять.

Вы можете выбрать один из режимов постоянной защиты:

- *Интеллектуальный режим защиты*: Kaspersky Endpoint Security проверяет файл при попытке открытия и проверяет его повторно при попытке закрытия, если файл

был изменен. Если какой-либо процесс многократно обращается к файлу в течение некоторого времени и изменяет его, Kaspersky Endpoint Security повторно проверяет файл только при последней попытке закрытия файла этим процессом.

- *Режим защиты при попытке открытия и изменения файла:* Kaspersky Endpoint Security проверяет файл при попытке открытия и проверяет его повторно при попытке закрытия, если файл был изменен.
- *Режим защиты при попытке открытия файла:* Kaspersky Endpoint Security проверяет файл при попытке открыть его на чтение, выполнение или изменение.

► *Чтобы выбрать режим постоянной защиты объектов, выполните следующие действия:*

1. Сохраните параметры задачи постоянной защиты в конфигурационном файле с помощью следующей команды:

```
/opt/kaspersky/kesl/bin/kesl-control --get-settings <ID задачи>  
--file <полный путь к файлу>
```

2. Откройте созданный конфигурационный файл для редактирования.

3. Присвойте параметру `ScanByAccessType` одно из следующих значений:

- `SmartCheck` – чтобы включить интеллектуальный режим защиты.
- `OpenAndModify` – чтобы включить режим защиты при попытке открытия и изменения файла.
- `Open` – чтобы включить режим защиты при попытке открытия файла.

4. Сохраните изменения в конфигурационном файле.

5. Импортируйте параметры из конфигурационного файла в задачу постоянной защиты с помощью следующей команды:

```
/opt/kaspersky/kesl/bin/kesl-control --set-settings <ID задачи>  
--file <полный путь к файлу>
```

Выбор действий программы над зараженными объектами

При обнаружении *зараженных* объектов (см. раздел "О зараженных файлах" на стр. [65](#)) Kaspersky Endpoint Security обрабатывает их: выполняет действия, указанные в задаче постоянной защиты или проверки по требованию. Kaspersky Endpoint Security может лечить, удалять, блокировать (для задачи постоянной защиты) или пропускать объекты (для задачи проверки по требованию).

Вы можете задать два действия Kaspersky Endpoint Security с зараженными объектами: первое действие (выполняется первоначально) и второе действие (выполняется, если первое действие выполнить не удалось).

► *Чтобы задать действия над зараженными объектами, выполните следующие действия:*

1. Сохраните параметры задачи постоянной защиты или задачи проверки по требованию в конфигурационном файле с помощью следующей команды:

```
/opt/kaspersky/kesl/bin/kesl-control --get-settings <ID задачи>  
--file <полный путь к файлу>
```

2. Откройте созданный конфигурационный файл для редактирования.

3. Задайте значения следующих параметров:

- `FirstAction` – первое действие над объектом;
- `SecondAction` – второе действие над объектом.

4. Сохраните изменения в конфигурационном файле.

5. Импортируйте параметры из конфигурационного файла в задачу постоянной защиты или в задачу проверки по требованию с помощью следующей команды:

```
/opt/kaspersky/kesl/bin/kesl-control --set-settings <ID задачи>  
--file <полный путь к файлу>
```

Выборочная проверка файлов и директорий (Scan_File)

Kaspersky Endpoint Security позволяет быстро проверять файлы и директории без необходимости формировать область проверки (см. раздел "Формирование области защиты и области проверки" на стр. [66](#)).

Вы можете задавать шаблоны имен проверяемых файлов с помощью масок в формате командной оболочки. В этом случае Kaspersky Endpoint Security проверяет только файлы из области защиты, описанные с помощью масок в формате командной оболочки.

По умолчанию Kaspersky Endpoint Security запускает проверку файлов и директорий с помощью команды `--scan-file` с параметрами по умолчанию, заданными для задачи проверки по требованию (см. раздел "О проверке по требованию" на стр. [63](#)).

► *Чтобы запустить выборочную проверку файлов и директорий, выполните одну из следующих команд:*

- Если вы хотите проверить один файл или директорию, выполните команду:

```
/opt/kaspersky/kesl/bin/kesl-control --scan-file <путь к файлу  
или директории>
```

- Если вы хотите проверить несколько файлов или директорий, выполните команду:

```
/opt/kaspersky/kesl/bin/kesl-control --scan-file <путь к файлу или  
директории> <путь к файлу или директории> и т.д.
```

Проверка загрузочных секторов

Kaspersky Endpoint Security позволяет проверять загрузочные секторы без необходимости формировать область проверки (см. раздел "Формирование области защиты и области проверки" на стр. [66](#)).

► *Чтобы проверить загрузочные секторы, запустите предустановленную задачу проверки загрузочных секторов (ID=4):*

```
/opt/kaspersky/kesl/bin/kesl-control --start-task 4
```

Проверка памяти процессов

Kaspersky Endpoint Security позволяет проверять память процессов без необходимости формировать область проверки (см. раздел "Формирование области защиты и области проверки" на стр. [66](#)).

- ▶ Чтобы проверить память процессов, запустите предустановленную задачу проверки памяти процессов (ID=5):

```
/opt/kaspersky/kesl/bin/kesl-control --start-task 5
```

Сокращение времени проверки

При необходимости вы можете сократить время проверки объектов следующими способами:

- Ограничить длительность проверки объекта. По истечении заданного времени Kaspersky Endpoint Security прекращает проверку объекта.
- Ограничить максимальный размер проверяемого объекта. Во время проверки Kaspersky Endpoint Security пропускает объекты, размер которых превышает заданный.

Ограничения по длительности проверки и размеру объекта применяются только при проверке составных объектов (например, архивов или баз данных).

- ▶ Чтобы ограничить длительность проверки составного объекта, выполните следующие действия:

1. Сохраните параметры задачи постоянной защиты или задачи проверки по требованию в конфигурационном файле с помощью следующей команды:

```
/opt/kaspersky/kesl/bin/kesl-control --get-settings <ID задачи>  
--file <полный путь к файлу>
```

2. Откройте созданный конфигурационный файл для редактирования.

3. Задайте следующие значения параметров:

- значение Yes для параметра UseTimeLimit;
- максимальное время проверки составного объекта (в секундах) для параметра TimeLimit.

Пример:

```
UseTimeLimit=Yes
```

```
TimeLimit=120
```

4. Сохраните изменения в конфигурационном файле.
5. Импортируйте параметры из конфигурационного файла в задачу постоянной защиты или задачу проверки по требованию с помощью следующей команды:

```
/opt/kaspersky/kesl/bin/kesl-control --set-settings <ID задачи>  
--file <полный путь к файлу>
```

► **Чтобы ограничить максимальный размер проверяемого составного объекта, выполните следующие действия:**

1. Сохраните параметры задачи постоянной защиты или задачи проверки по требованию в конфигурационном файле с помощью следующей команды:

```
/opt/kaspersky/kesl/bin/kesl-control --get-settings <ID задачи>  
--file <полный путь к файлу>
```

2. Откройте созданный конфигурационный файл для редактирования.
3. Задайте следующие значения параметров:
 - значение `Yes` для параметра `UseSizeLimit`;
 - максимальный размер проверяемого составного объекта (в мегабайтах) для параметра `SizeLimit`.

Пример:

```
UseSizeLimit=Yes
```

```
SizeLimit=10
```

4. Сохраните изменения в конфигурационном файле.

5. Импортируйте параметры из конфигурационного файла в задачу постоянной защиты или задачу проверки по требованию с помощью следующей команды:

```
/opt/kaspersky/kesl/bin/kesl-control --set-settings <ID задачи>  
--file <полный путь к файлу>
```

Особенности проверки символических и жестких ссылок

Kaspersky Endpoint Security позволяет проверять символические и жесткие ссылки на файлы.

Проверка символических ссылок

Kaspersky Endpoint Security проверяет символические ссылки только если файл, на который ссылается символическая ссылка, входит в область защиты задачи постоянной защиты или в область проверки задачи проверки по требованию.

Если файл, обращение к которому происходит по символической ссылке, не входит в область защиты или в область проверки задачи, программа не проверяет этот файл. Если такой файл содержит вредоносный код, безопасность компьютера окажется под угрозой.

Проверка жестких ссылок

Когда Kaspersky Endpoint Security обрабатывает файл, у которого больше одной жесткой ссылки, программа выбирает действие в зависимости от заданного действия над объектами:

- Если выбрано действие **Выполнять рекомендуемое действие** (Recommended) Kaspersky Endpoint Security автоматически подбирает и выполняет действие над объектом на основе данных об опасности обнаруженной в объекте угрозы и возможности его лечения.
- Если выбрано действие **Удалять** (Remove), Kaspersky Endpoint Security удаляет обрабатываемую жесткую ссылку. Остальные жесткие ссылки на этот файл обработаны не будут.

- Если выбрано действие **Лечить** (Cure), Kaspersky Endpoint Security лечит исходный файл. Если лечение невозможно, программа удаляет жесткую ссылку и создает вместо нее копию исходного файла с именем удаленной жесткой ссылки.

Когда вы восстанавливаете файл с жесткой ссылкой из резервного хранилища, Kaspersky Endpoint Security создает копию исходного файла с именем жесткой ссылки, которая была помещена в резервное хранилище. Связи с остальными жесткими ссылками на исходный файл восстановлены не будут.

Настройка совместной работы: Антивирус Касперского для Linux Mail Server

► Чтобы настроить совместную работу Kaspersky Endpoint Security 10 с Антивирусом Касперского для Linux Mail Server, выполните следующие действия:

1. Сохраните параметры задачи постоянной защиты в конфигурационном файле с помощью следующей команды:

```
/opt/kaspersky/kesl/bin/kesl-control --get-settings 1  
--file <полный путь к файлу>
```

2. Откройте созданный конфигурационный файл для редактирования.

3. Добавьте в созданный файл следующую секцию:

```
[ExcludedFromScanScope.item_#]  
Path=</var/opt/kaspersky/klms>
```

4. Повторите указанную выше секцию для всех почтовых агентов, интегрированных с Антивирусом Касперского для Linux Mail Server.

5. Для исключения из проверки временной директории фильтров и служб Антивируса Касперского для Linux Mail Server добавьте в созданный файл следующую секцию:

```
[ExcludedFromScanScope.item_#]  
Path=/tmp/klmstmp
```

6. Сохраните изменения в конфигурационном файле.

7. Импортируйте параметры из конфигурационного файла в задачу постоянной защиты с помощью следующей команды:

```
/opt/kaspersky/kesl/bin/kesl-control --set-settings 1  
--file <полный путь к файлу>
```

Работа с резервным хранилищем

Перед лечением или удалением зараженных объектов Kaspersky Endpoint Security сохраняет копии этих объектов в резервном хранилище.

Если зараженный объект является частью составного объекта, Kaspersky Endpoint Security сохраняет составной объект в резервном хранилище полностью. Например, если Kaspersky Endpoint Security признает зараженным один объект в составе почтовой базы, перед лечением Kaspersky Endpoint Security сохраняет в резервном хранилище копию всей почтовой базы.

Этот раздел содержит инструкции по работе с объектами в резервном хранилище.

В этом разделе

О резервном хранилище	80
Просмотр идентификаторов объектов в резервном хранилище.....	81
О восстановлении объектов из резервного хранилища	81
Восстановление объектов из резервного хранилища.....	82
Удаление объектов из резервного хранилища	83

См. также

Команды управления резервным хранилищем	173
Параметры резервного хранилища	144

О резервном хранилище

Резервное хранилище – это список резервных копий файлов, которые были удалены или изменены в процессе лечения. *Резервная копия* – копия файла, которая создается при первом лечении или удалении этого файла. Резервные копии файлов хранятся в специальном формате и не представляют опасности.

Иногда при лечении файлов не удается сохранить их целостность. Если вылеченный файл содержал важную информацию, которая в результате лечения стала полностью или частично недоступна, пользователь может попытаться восстановить файл из его вылеченной копии в папку исходного размещения файла.

Просмотр идентификаторов объектов в резервном хранилище

При помещении объекта в резервное хранилище Kaspersky Endpoint Security присваивает ему числовой идентификатор. Идентификатор используется для действий с объектом, например, при восстановлении (см. стр. [82](#)) или удалении (см. стр. [83](#)) объекта из резервного хранилища.

- Чтобы просмотреть идентификаторы объектов в резервном хранилище, выполните команду:

```
/opt/kaspersky/kesl/bin/kesl-control -B --query
```

Идентификатор объекта отображается в строке `ObjectId`.

См. также

| Получение информации об объектах в хранилище [173](#)

О восстановлении объектов из резервного хранилища

Kaspersky Endpoint Security хранит объекты в резервном хранилище в зашифрованном виде, чтобы предохранить защищаемый сервер от их возможного вредоносного действия.

Вы можете восстанавливать объекты из резервного хранилища. Восстановление объектов может потребоваться в следующих случаях:

- При лечении зараженного файла Kaspersky Endpoint Security не удалось сохранить его целостность, и в результате информация в файле стала недоступной.
- Вы считаете объект безопасным для сервера и хотите его использовать.

Вы можете исключить объект из проверки, чтобы программа не обнаруживала его при последующих проверках. Для этого вам нужно исключить объект по имени или по названию обнаруженной угрозы в задаче постоянной защиты, а также по имени или по названию обнаруженной угрозы в задачах проверки по требованию.

Восстановление зараженных объектов может привести к заражению компьютера.

При восстановлении из резервного хранилища вы можете сохранить файл под другим именем.

См. также

Восстановление объектов из хранилища.....[174](#)

Восстановление объектов из резервного хранилища

► Чтобы восстановить объект из резервного хранилища, выполните одно из следующих действий:

- Чтобы восстановить объект с исходным именем и в исходное местоположение, выполните команду:

```
/opt/kaspersky/kesl/bin/kesl-control --restore <ID объекта>
```

где ID объекта – идентификатор объекта в резервном хранилище.

- Чтобы восстановить объект с новым именем в указанную директорию, выполните команду:

```
/opt/kaspersky/kesl/bin/kesl-control --restore <ID объекта>  
--file <имя файла и путь к нему>
```

Если указанная директория не существует, Kaspersky Endpoint Security создает ее.

Удаление объектов из резервного хранилища

- ▶ Чтобы удалить один объект из резервного хранилища, выполните следующую команду:

```
/opt/kaspersky/kesl/bin/kesl-control -B --mass-remove --query "ObjectId == 'ID объекта>'"
```

- ▶ Чтобы удалить несколько объектов из резервного хранилища, выполните следующую команду:

```
/opt/kaspersky/kesl/bin/kesl-control -B --mass-remove --query "<поле><оператор сравнения> '<значение>' [and <поле> <оператор сравнения> '<значение>' ]* ]"
```

- ▶ Чтобы удалить все объекты из резервного хранилища, выполните одну из следующих команд:

```
/opt/kaspersky/kesl/bin/kesl-control -B --mass-remove
```

или

```
/opt/kaspersky/kesl/bin/kesl-control -B --mass-remove --query
```

Настройка уведомлений о событиях

Во время работы Kaspersky Endpoint Security возникают события, отражающие изменение состояния антивирусной защиты сервера и состояния Kaspersky Endpoint Security в целом. Если вы управляете программой через Kaspersky Security Center, вы можете настроить уведомление администратора об этих событиях по электронной почте.

Подробнее о настройке уведомлений о событиях вы можете прочитать в *Руководстве администратора для Kaspersky Security Center*.

Участие в Kaspersky Security Network

Этот раздел содержит информацию об участии в Kaspersky Security Network и инструкции о том, как включить и выключить использование Kaspersky Security Network.

В этом разделе

Об участии в Kaspersky Security Network	85
Включение и выключение использования Kaspersky Security Network.....	87
Проверка подключения к Kaspersky Security Network	88
Дополнительная защита с использованием Kaspersky Security Network	89

Об участии в Kaspersky Security Network

Чтобы повысить эффективность защиты компьютера пользователя, Kaspersky Endpoint Security использует данные, полученные от пользователей во всем мире. Для получения этих данных предназначена сеть *Kaspersky Security Network*.

Kaspersky Security Network (KSN) – это инфраструктура облачных служб, предоставляющая доступ к оперативной базе знаний "Лаборатории Касперского" о репутации файлов, интернет-ресурсов и программного обеспечения. Использование данных Kaspersky Security Network обеспечивает более высокую скорость реакции Kaspersky Endpoint Security на неизвестные угрозы, повышает эффективность работы некоторых компонентов защиты, а также снижает вероятность ложных срабатываний.

В зависимости от расположения инфраструктуры различают Глобальный KSN (инфраструктура расположена на серверах "Лаборатории Касперского") и Локальный KSN (инфраструктура расположена на сторонних серверах, например, внутри сети интернет-провайдера).

После изменения лицензии для использования Локального KSN требуется предоставить поставщику услуг информацию о новом ключе. В противном случае обмен информацией с Локальным KSN будет невозможен из-за ошибки аутентификации.

Участие пользователей в KSN позволяет "Лаборатории Касперского" оперативно получать информацию о типах и источниках угроз, разрабатывать способы нейтрализации угроз, уменьшать количество ложных срабатываний компонентов программы.

Во время использования KSN программа автоматически отправляет в KSN статистическую информацию, полученную в результате своей работы. Также программа может отправлять в "Лабораторию Касперского" для дополнительной проверки файлы (или части файлов), которые злоумышленники могут использовать для нанесения вреда компьютеру или данным.

Сбор, обработка и хранение персональных данных пользователя не производится. Более подробную информацию об отправке в "Лабораторию Касперского", хранении и уничтожении статистической информации, полученной во время использования KSN, вы можете прочитать в Положении о Kaspersky Security Network и на веб-сайте "Лаборатории Касперского" (<http://www.kaspersky.ru/privacy>). Файл с текстом Положения о Kaspersky Security Network входит в комплект поставки программы.

Компьютеры пользователей, работающие под управлением Сервера администрирования Kaspersky Security Center, могут взаимодействовать с KSN при помощи службы KSN Proxy.

Служба KSN Proxy предоставляет следующие возможности:

- Компьютер пользователя может выполнять запросы к KSN и передавать в KSN информацию, даже если он не имеет прямого доступа к интернету.
- Служба KSN Proxy кеширует обработанные данные, снижая тем самым нагрузку на канал во внешнюю сеть и ускоряя получение компьютером пользователя запрошенной информации.

Подробнее о службе KSN Proxy вы можете прочитать в *Руководстве администратора для Kaspersky Security Center*.

Настройка параметров использования службы KSN Proxy доступна в свойствах политики *Kaspersky Security Center* (см. раздел "Управление политиками" на стр. [106](#)).

Участие в Kaspersky Security Network является добровольным. Программа предлагает участвовать в KSN во время установки. Начать или прекратить использование KSN можно в любой момент.

Включение и выключение использования Kaspersky Security Network

- ▶ *Чтобы включить использование Kaspersky Security Network, выполните следующую команду:*

```
kesl-control --set-app-settings UseKSN=Yes
```

- ▶ *Чтобы выключить использование Kaspersky Security Network, выполните следующую команду:*

```
kesl-control --set-app-settings UseKSN=No
```

- ▶ *Чтобы включить или выключить использование Kaspersky Security Network с помощью конфигурационного файла, выполните следующую команду:*

```
kesl-control --set-app-settings --file <имя конфигурационного файла>
```

Если Kaspersky Endpoint Security, установленный на компьютере, работает под политикой, назначенной в Kaspersky Security Center, изменить значение параметра `UseKSN` можно только с помощью Kaspersky Security Center.

Если Kaspersky Endpoint Security, установленный на компьютере, выходит из-под политики, устанавливается значение параметра `UseKSN=No`.

Файл с текстом Положения о Kaspersky Security Network расположен в директории `/opt/kaspersky/kesl/doc/ksn_license.<ID языка>`.

Проверка подключения к Kaspersky Security Network

- ▶ Чтобы проверить подключение к Kaspersky Security Network, выполните следующую команду:

```
kesl-control --app-info
```

В строке `KSN state` отображается статус подключения к Kaspersky Security Network:

- Если отображается статус `On`, Kaspersky Endpoint Security подключен к Kaspersky Security Network.
- Если отображается статус `Off`, Kaspersky Endpoint Security не подключен к Kaspersky Security Network.

Подключение к Kaspersky Security Network может отсутствовать по следующим причинам:

- Ваш компьютер не подключен к интернету.
- Вы не участвуете в Kaspersky Security Network.
- Программа не активирована или срок действия лицензии истек.
- Выявлены проблемы, связанные с ключом. Например, ключ попал в черный список ключей.

Дополнительная защита с использованием Kaspersky Security Network

«Лаборатория Касперского» предоставляет дополнительный уровень защиты с использованием Kaspersky Security Network. Этот способ защиты нацелен на эффективную борьбу против постоянных угроз повышенной сложности и угроз нулевого дня. Объединенные с Kaspersky Endpoint Security облачные технологии и экспертные знания вирусных аналитиков «Лаборатории Касперского» обеспечивают мощную защиту против сложнейших угроз в сети.

Более подробную информацию о дополнительной защите в Kaspersky Endpoint Security вы можете найти на веб-сайте «Лаборатории Касперского».

Управление программой через Kaspersky Security Center

Этот раздел содержит информацию об управлении программой Kaspersky Endpoint Security через Kaspersky Security Center. Описание приведено для Kaspersky Security Center SP2.

В этом разделе

Об управлении Kaspersky Endpoint Security с помощью Kaspersky Security Center	91
Запуск и остановка Kaspersky Endpoint Security на клиентском компьютере.....	92
Настройка параметров Kaspersky Endpoint Security.....	93
Просмотр состояния защиты компьютера	95
Просмотр параметров Kaspersky Endpoint Security.....	96
Управление задачами.....	97
Управление политиками	106
Просмотр сообщений пользователей в хранилище событий Kaspersky Security Center ...	109
Проверка соединения с Сервером администрирования вручную. Утилита klnagchk.....	110
Подключение к Серверу администрирования вручную. Утилита klmover	112

Об управлении Kaspersky Endpoint Security с помощью Kaspersky Security Center

Kaspersky Security Center позволяет удаленно устанавливать и удалять, запускать и останавливать Kaspersky Endpoint Security, настраивать параметры работы программы, запускать задачи на управляемых компьютерах.

Управление программой через Kaspersky Security Center осуществляется с помощью плагина управления Kaspersky Endpoint Security.

Перед установкой плагина управления Kaspersky Endpoint Security необходимо убедиться, что установлены Kaspersky Security Center и Redist C++ 2015 (Microsoft Visual C++ 2015 Redistributable).

Вы можете выполнять следующие действия в Консоли администрирования Kaspersky Security Center:

- просматривать состояние защиты компьютеров;
- настраивать общие параметры защиты компьютеров;
- управлять политиками;
- управлять задачами:
 - добавления ключей;
 - копирования обновлений;
 - обновления;
 - отката обновления баз;
 - проверки загрузочных секторов;
 - проверки памяти процессов;
 - проверки по требованию.

Запуск и остановка Kaspersky Endpoint Security на клиентском компьютере

► Чтобы запустить или остановить Kaspersky Endpoint Security на клиентском компьютере, выполните следующие действия:

1. Откройте Консоль администрирования Kaspersky Security Center.
2. В папке **Управляемые устройства** дерева Консоли администрирования Kaspersky Security Center откройте папку с названием группы администрирования, в состав которой входит нужный вам компьютер.
3. В рабочей области выберите закладку **Устройства**.
4. В списке управляемых устройств выберите компьютер, на котором вы хотите запустить или остановить программу.
5. По правой клавише мыши откройте контекстное меню компьютера. Выберите пункт **Свойства**.


Откроется окно свойств компьютера.

6. В окне свойств компьютера выберите раздел **Программы**.

Справа в окне свойств компьютера отобразится список программ "Лаборатории Касперского", установленных на компьютере.


7. Выберите программу Kaspersky Endpoint Security 10 для Linux.

8. Выполните следующие действия:

- Если вы хотите запустить программу, справа от списка программ "Лаборатории Касперского" нажмите на кнопку  или выполните следующие действия:

- а. По правой клавише мыши откройте контекстное меню программы Kaspersky Endpoint Security 10 для Linux и выберите пункт **Свойства** или нажмите на кнопку **Свойства**, расположенную под списком программ «Лаборатории Касперского».

Откроется окно **Параметры программы Kaspersky Endpoint Security 10 для Linux** на закладке **Общие**.

- b. Нажмите на кнопку **Запустить**.
- Если вы хотите остановить работу программы, справа от списка программ "Лаборатории Касперского" нажмите на кнопку  или выполните следующие действия:
 - a. По правой клавише мыши откройте контекстное меню программы Kaspersky Endpoint Security 10 для Linux и выберите пункт **Свойства** или нажмите на кнопку **Свойства**, расположенную под списком программ.

Откроется окно **Параметры программы Kaspersky Endpoint Security 10 для Linux** на закладке **Общие**.

- b. Нажмите на кнопку **Остановить**.

Настройка параметров Kaspersky Endpoint Security

► *Чтобы настроить параметры Kaspersky Endpoint Security, выполните следующие действия:*

1. Откройте Консоль администрирования Kaspersky Security Center.
2. В папке **Управляемые устройства** дерева консоли администрирования Kaspersky Security Center откройте папку с названием группы администрирования, в состав которой входит нужный вам компьютер.
3. В рабочей области выберите закладку **Устройства**.
4. В списке клиентских компьютеров выберите компьютер, для которого вы хотите настроить параметры Kaspersky Endpoint Security.
5. По правой клавише мыши откройте контекстное меню компьютера. Выберите пункт **Свойства**.

Откроется окно свойств компьютера.

6. В окне свойств компьютера выберите раздел **Программы**.

Справа в окне свойств компьютера отобразится список программ "Лаборатории Касперского", установленных на компьютере.

7. Выберите программу Kaspersky Endpoint Security 10 для Linux.

8. По правой клавише мыши откройте контекстное меню программы Kaspersky Endpoint Security 10 для Linux. Выберите пункт **Свойства**.

Откроется окно **Параметры программы "Kaspersky Endpoint Security 10 для Linux"**.

9. В разделе **Дополнительные параметры** настройте параметры работы Kaspersky Endpoint Security, а также параметры отчетов и хранилищ.

Остальные разделы окна **Параметры программы "Kaspersky Endpoint Security 10 для Linux"** стандартны для программы Kaspersky Security Center, их описание вы можете прочитать в *Руководстве администратора для Kaspersky Security Center*.

Если для программы создана политика, в которой запрещено изменение некоторых параметров, то во время настройки параметров программы их изменение недоступно.

10. В окне **Параметры программы "Kaspersky Endpoint Security 10 для Linux"** нажмите на кнопку **ОК**, чтобы сохранить внесенные изменения.

Просмотр состояния защиты компьютера

► Чтобы просмотреть состояние защиты компьютера, выполните следующие действия:

1. В дереве Консоли администрирования Kaspersky Security Center разверните узел **Управляемые устройства** и выберите группу, к которой принадлежит защищаемый компьютер.
2. В рабочей области выберите закладку **Устройства**.
3. По правой клавише мыши откройте контекстное меню защищаемого компьютера и выберите пункт **Свойства**.
4. В окне **Свойства** выберите закладку **Защита**.

На закладке **Защита** отображается следующая информация о защищаемом компьютере:

- **Статус компьютера** – информация об антивирусной безопасности защищаемого компьютера, например, *Базы устарели*, *Срок действия лицензии истек*;
- **Статус постоянной защиты** – состояние постоянной защиты, например, *Выполняется*, *Остановлена*, *Приостановлена*;
- **Последняя проверка по требованию** – дата и время последнего выполнения задачи проверки по требованию;
- **Обнаружено вирусов** – общее количество вредоносных программ, обнаруженных на защищаемом компьютере (счетчик обнаруженных угроз) с момента установки Kaspersky Endpoint Security или с момента сброса счетчика. Чтобы сбросить счетчик, нажмите на кнопку **Обнулить**;
- **Количество невылеченных объектов** – количество зараженных объектов, которые Kaspersky Endpoint Security не удалось вылечить.

Просмотр параметров Kaspersky Endpoint Security

► Чтобы просмотреть параметры Kaspersky Endpoint Security, выполните следующие действия:

1. В дереве Консоли администрирования Kaspersky Security Center разверните узел **Управляемые устройства** и выберите группу, к которой принадлежит защищаемый компьютер.
2. В рабочей области выберите закладку **Устройства**.
3. По правой клавише мыши откройте контекстное меню защищаемого компьютера и выберите пункт **Свойства**.
4. В окне **Свойства: <Имя компьютера>** выберите раздел **Программы**.
5. В разделе **Программы** выберите **Kaspersky Endpoint Security 10 для Linux** в списке установленных программ и в контекстном меню программы выберите пункт **Свойства**.

В результате откроется окно **Параметры программы Kaspersky Endpoint Security 10 для Linux** в разделе **Общие**.

В окне **Параметры программы Kaspersky Endpoint Security 10 для Linux** отображается следующая информация о Kaspersky Endpoint Security:

Раздел **Общие**

- **Номер версии** – номер версии Kaspersky Endpoint Security;
- **Установлено** – дата и время установки Kaspersky Endpoint Security на защищаемом компьютере;
- **Текущее состояние** – состояние постоянной защиты, например, *Выполняется*, *Приостановлена*;
- **Последнее обновление ПО** – дата и время последнего обновления программных модулей Kaspersky Endpoint Security;

- **Установленные обновления** – список программных модулей, для которых установлены обновления;
- **Базы программы** – дата и время последнего обновления антивирусных баз, а также количество записей в базах.

Раздел **Ключи**

- **Тип лицензии** – тип лицензии, *коммерческая* или *пробная*;
- **Дата активации** (поле доступно только для активного ключа) – дата добавления активного ключа;
- **Дата окончания срока** (поле доступно только для активного ключа) – дата окончания срока действия активного ключа;
- **Срок действия** – количество дней, в течение которых действует ключ;
- **Ограничение** – количество компьютеров, на которых вы можете использовать ключ.

Раздел **События**

В этом разделе вы можете просмотреть события, которые Kaspersky Endpoint Security сохраняет в хранилище событий.

Раздел **Дополнительно**

В этом разделе вы можете просмотреть информацию о плагине управления программой.

Управление задачами

Этот раздел содержит информацию об управлении задачами для Kaspersky Endpoint Security.

Подробнее о методике управления задачами через Kaspersky Security Center вы можете прочитать в *Руководстве администратора для Kaspersky Security Center*.

О задачах для Kaspersky Endpoint Security

Kaspersky Security Center управляет работой Kaspersky Endpoint Security, установленной на компьютерах, с помощью задач. Задачи реализуют основные функции управления, например, добавление ключа, проверку объектов, обновление баз и модулей программы.

При работе с Kaspersky Endpoint Security через Kaspersky Security Center вы можете создавать следующие типы задач:

- локальные задачи, определенные для отдельного компьютера;
- групповые задачи, определенные для компьютеров, входящих в группы администрирования;
- задачи для наборов компьютеров, не входящих в группы администрирования.

Задачи для наборов компьютеров, не входящих в группы администрирования, выполняются только для указанных в параметрах задачи компьютеров. Если в набор компьютеров, для которого сформирована задача, добавлены новые компьютеры, то для них эта задача не выполняется. В этом случае вам необходимо создать новую задачу или изменить параметры уже существующей задачи.

Вы можете создавать задачи следующих типов:

- **Обновление.** В процессе выполнения задачи Kaspersky Endpoint Security обновляет антивирусные базы в соответствии с установленными параметрами обновления.
- **Откат обновления.** В процессе выполнения задачи Kaspersky Endpoint Security откатывает последнее обновление антивирусных баз.
- **Копирование обновлений.** В процессе выполнения задачи Kaspersky Endpoint Security скачивает антивирусные базы в указанную директорию, не устанавливая их.
- **Проверка по требованию.** В процессе выполнения задачи Kaspersky Endpoint Security проверяет на вирусы и другие программы, представляющие угрозу, области компьютера, указанные в параметрах задачи.

- **Проверка загрузочных секторов.** В процессе выполнения задачи Kaspersky Endpoint Security проверяет загрузочные секторы компьютера.
- **Проверка системной памяти.** В процессе выполнения задачи Kaspersky Endpoint Security проверяет системную память компьютера.
- **Добавление ключа.** В процессе выполнения задачи Kaspersky Endpoint Security добавляет ключ, в том числе дополнительный, для активации программы.

Вы можете выполнять следующие действия над задачами:

- запускать, останавливать, приостанавливать и возобновлять выполнение задач;
- создавать новые задачи;
- изменять параметры задач.

Права на доступ к параметрам задач Kaspersky Endpoint Security (чтение, изменение, выполнение) задаются для каждого пользователя, имеющего доступ к Серверу администрирования Kaspersky Security Center, через параметры доступа к функциональным областям Kaspersky Endpoint Security. Для настройки прав доступа к параметрам функциональных областей Kaspersky Endpoint Security перейдите в раздел **Безопасность** окна свойств Сервера администрирования Kaspersky Security Center.

Общая информация о задачах в Kaspersky Security Center приводится в *Руководстве администратора для Kaspersky Security Center*.

Создание локальной задачи

► Чтобы создать локальную задачу, выполните следующие действия:

1. Откройте Консоль администрирования Kaspersky Security Center.
2. В папке **Управляемые устройства** дерева Консоли администрирования Kaspersky Security Center откройте папку с названием группы администрирования, в состав которой входит нужный вам компьютер.
3. В рабочей области выберите закладку **Устройства**.

4. В списке клиентских компьютеров выберите компьютер, для которого вы хотите создать локальную задачу.

5. По правой клавише мыши откройте контекстное меню компьютера. Выберите пункт **Свойства**.

Откроется окно свойств компьютера.

6. Выберите раздел **Задачи**.

7. Нажмите на кнопку **Добавить**.

Запустится мастер создания задачи.

8. Следуйте указаниям мастера создания задачи.

Создание групповой задачи

► Чтобы создать групповую задачу, выполните следующие действия:

1. Откройте Консоль администрирования Kaspersky Security Center.

2. Откройте папку **Управляемые устройства** дерева Консоли администрирования Kaspersky Security Center.

3. В рабочей области выберите закладку **Задачи**.

4. Выполните одно из следующих действий:

- Нажмите на кнопку **Создать задачу**.
- Выберите пункт **Создать** → **Задачу** в контекстном меню Kaspersky Security Center.

Запустится мастер создания задачи.

5. Следуйте указаниям мастера создания задачи.

Создание задачи для набора компьютеров

► Чтобы создать задачу для набора компьютеров, выполните следующие действия:

1. Откройте Консоль администрирования Kaspersky Security Center.
2. Откройте папку **Задачи для наборов устройств** дерева Консоли администрирования Kaspersky Security Center.
3. Выполните одно из следующих действий:
 - Нажмите на кнопку **Создать задачу**.
 - Выберите пункт **Создать** → **Задачу** в контекстном меню Kaspersky Security Center.Запустится мастер создания задачи.
4. Следуйте указаниям мастера создания задачи.

Запуск, остановка, приостановка и возобновление выполнения задачи вручную

Если на компьютере запущена программа Kaspersky Endpoint Security (см. раздел "Запуск и остановка Kaspersky Endpoint Security на клиентском компьютере" на стр. [92](#)), вы можете запустить / остановить / приостановить / возобновить выполнение задачи на этом компьютере через Kaspersky Security Center. Если программа Kaspersky Endpoint Security остановлена, выполнение запущенных задач прекращается, а управлять запуском, остановкой, приостановкой и возобновлением задач через Kaspersky Security Center становится невозможным.

► Чтобы запустить / остановить / приостановить / возобновить выполнение локальной задачи, выполните следующие действия:

1. Откройте Консоль администрирования Kaspersky Security Center.
2. В папке **Управляемые устройства** дерева Консоли администрирования Kaspersky Security Center откройте папку с названием группы администрирования, в состав которой входит нужный вам компьютер.

3. В рабочей области выберите закладку **Устройства**.
4. В списке клиентских компьютеров выберите компьютер, на котором вы хотите запустить / остановить / приостановить / возобновить выполнение локальной задачи.
5. Выберите пункт **Свойства** в контекстном меню компьютера.



Откроется окно свойств компьютера.

6. Выберите раздел **Задачи**.

В правой части окна отобразится список локальных задач.

7. Выберите локальную задачу, выполнение которой вы хотите запустить / остановить / приостановить / возобновить.

8. Выполните одно из следующих действий:

- По правой клавише мыши откройте контекстное меню локальной задачи. Выберите пункт **Запустить / Остановить / Приостановить / Возобновить**.
- Нажмите на кнопку  или  справа от списка локальных задач, чтобы запустить или остановить локальную задачу.
- Нажмите на кнопку **Свойства** под списком локальных задач. Откроется окно **Свойства задачи <Название задачи>**. Далее на закладке **Общие** окна **Свойства задачи <Название задачи>** нажмите на кнопку **Запустить / Остановить / Приостановить / Возобновить**.

► Чтобы запустить / остановить / приостановить / возобновить выполнение групповой задачи, выполните следующие действия:



1. Откройте Консоль администрирования Kaspersky Security Center.
2. В папке **Управляемые компьютеры** дерева консоли откройте папку с названием группы администрирования, для которой вы хотите запустить / остановить / приостановить / возобновить выполнение групповой задачи.
3. В рабочей области выберите закладку **Задачи**.

В правой части окна отобразится список групповых задач.

4. В списке групповых задач выберите групповую задачу, выполнение которой вы хотите запустить / остановить / приостановить / возобновить.

5. Выполните одно из следующих действий:

- По правой клавише мыши откройте контекстное меню групповой задачи. Выберите пункт **Запустить / Остановить / Приостановить / Возобновить**.

- Нажмите на кнопку  /  справа от списка групповых задач, чтобы запустить или остановить групповую задачу.

► *Чтобы запустить / остановить / приостановить / возобновить выполнение задачи для набора компьютеров, выполните следующие действия:*



1. Откройте Консоль администрирования Kaspersky Security Center.

2. В папке **Задачи для наборов компьютеров** дерева консоли выберите задачу для набора компьютеров, выполнение которой вы хотите запустить / остановить / приостановить / возобновить.

3. Выполните одно из следующих действий:

- По правой клавише мыши откройте контекстное меню задачи для набора компьютеров.

Выберите пункт **Запустить / Остановить / Приостановить / Возобновить**.

- Нажмите на кнопку  /  справа от списка задач для наборов компьютеров, чтобы запустить или остановить задачу для набора компьютеров.

Изменение параметров задачи

► *Чтобы изменить параметры локальной задачи, выполните следующие действия:*

1. Откройте Консоль администрирования Kaspersky Security Center.

2. В папке **Управляемые устройства** дерева Консоли администрирования Kaspersky Security Center откройте папку с названием группы администрирования, в состав которой входит нужный вам компьютер.

3. В рабочей области выберите закладку **Компьютеры**.
4. В списке клиентских компьютеров выберите компьютер, для которого вы хотите настроить параметры программы.
5. Выполните одно из следующих действий:
 - По правой клавише мыши откройте контекстное меню компьютера. Выберите пункт **Свойства**.
 - В меню **Действия** выберите пункт **Свойства компьютера**.

Откроется окно свойств компьютера.

6. Выберите раздел **Задачи**.

В правой части окна отобразится список локальных задач.

7. Выберите в списке локальных задач нужную локальную задачу.

8. Выполните одно из следующих действий:

- По правой клавише мыши откройте контекстное меню задачи. Выберите пункт **Свойства**.
- Нажмите на кнопку **Свойства**.

Откроется окно **Свойства: <Название локальной задачи>**.

9. В окне **Свойства: <Название локальной задачи>** выберите раздел **Параметры**.

10. Измените параметры локальной задачи.

11. В окне **Свойства: <Название локальной задачи>** нажмите на кнопку **ОК**, чтобы сохранить внесенные изменения.

► *Чтобы изменить параметры групповой задачи, выполните следующие действия:*

1. Откройте Консоль администрирования Kaspersky Security Center.
2. В папке **Управляемые компьютеры** откройте папку с названием нужной группы администрирования.

3. В рабочей области выберите закладку **Задачи**.

В нижней части панели задач отобразится список групповых задач.

4. Выберите в списке групповых задач нужную групповую задачу.

5. Выполните одно из следующих действий:

- По правой клавише мыши откройте контекстное меню задачи. Выберите пункт **Свойства**.
- Нажмите на кнопку **Изменить параметры задачи**, которая находится справа от списка групповых задач.

Откроется окно **Свойства: <Название групповой задачи>**.

6. В окне **Свойства: <Название групповой задачи>** выберите раздел **Параметры**.

7. Измените параметры групповой задачи.

8. В окне **Свойства: <Название групповой задачи>** нажмите на кнопку **ОК**, чтобы сохранить внесенные изменения.

► *Чтобы изменить параметры задачи для набора компьютеров, выполните следующие действия:*

1. Откройте Консоль администрирования Kaspersky Security Center.

2. В папке **Задачи для наборов компьютеров** дерева консоли выберите задачу для набора компьютеров, параметры которой вы хотите изменить.

3. Выполните одно из следующих действий:

- По правой клавише мыши откройте контекстное меню задачи для набора компьютеров. Выберите пункт **Свойства**.
- Нажмите на кнопку **Изменить параметры задачи**, которая находится справа от списка задач для наборов компьютеров.

Откроется окно **Свойства: <Название задачи для набора компьютеров>**.

4. В окне **Свойства: <Название задачи для набора компьютеров>** выберите раздел **Параметры**.
5. Измените параметры задачи для набора компьютеров.
6. В окне **Свойства: <Название задачи для набора компьютеров>** нажмите на кнопку **ОК**, чтобы сохранить внесенные изменения.

Все разделы окна свойств задач, кроме раздела **Параметры**, стандартны для программы Kaspersky Security Center. Их подробное описание вы можете прочитать в *Руководстве администратора для Kaspersky Security Center*. Раздел **Параметры** содержит специфические параметры Kaspersky Endpoint Security 10, его содержимое варьируется в зависимости от выбранного типа и вида задачи.

Управление политиками


Этот раздел содержит информацию о создании и настройке политик для Kaspersky Endpoint Security. Более подробную информацию о концепции управления программой Kaspersky Endpoint Security при помощи политик Kaspersky Security Center вы можете прочитать в *Руководстве администратора для Kaspersky Security Center*.

О политиках

При помощи политик вы можете установить одинаковые значения параметров работы программы Kaspersky Endpoint Security для всех клиентских компьютеров, входящих в состав группы администрирования.

Вы можете локально изменять значения параметров, заданные политикой, для отдельных компьютеров в группе администрирования при помощи Kaspersky Endpoint Security. Вы можете изменять локально только те параметры, изменение которых не запрещено политикой.

Возможность изменять параметр программы на клиентском компьютере определяется статусом «замка» у параметра в политике:

- Если параметр закрыт "замком" () , это означает, что вы не можете изменить значение параметра локально. Для всех клиентских компьютеров группы администрирования используется значение параметра, заданное политикой.
- Если параметр не закрыт "замком" () , это означает, что вы можете изменить значение параметра локально. Для всех клиентских компьютеров группы администрирования используются значения параметра, установленные локально. Значение параметра, установленное в политике, не применяется.

Локальные параметры программы изменяются в соответствии с параметрами политики после первого применения политики.

С помощью политик вы можете настраивать параметры задачи постоянной защиты Kaspersky Endpoint Security.

Права на доступ к параметрам политики (чтение, изменение, выполнение) задаются для каждого пользователя, имеющего доступ к Серверу администрирования Kaspersky Security Center, и отдельно для каждой функциональной области Kaspersky Endpoint Security. Для настройки прав доступа к параметрам политики перейдите в раздел **Безопасность** окна свойств Сервера администрирования Kaspersky Security Center.

Вы можете выполнять следующие действия над политикой:

- Создавать политику.
- Изменять параметры политики.

Если учетная запись пользователя, под которой вы осуществили доступ к Серверу администрирования, не имеет прав на изменение параметров отдельных функциональных областей, то параметры этих функциональных областей недоступны для изменения.

- Удалять политику.
- Изменять состояние политики.

Информацию о работе с политиками, не касающуюся взаимодействия с Kaspersky Endpoint Security, вы можете прочитать в *Руководстве администратора для Kaspersky Security Center*.

Создание политики

► Чтобы создать политику, выполните следующие действия:

1. Откройте Консоль администрирования Kaspersky Security Center.
2. Выполните одно из следующих действий:
 - Выберите папку **Управляемые компьютеры** дерева консоли, если вы хотите создать политику для всех управляемых программой Kaspersky Security Center компьютеров.
 - В папке **Управляемые компьютеры** дерева консоли выберите папку с названием группы администрирования, в состав которой входят интересующие вас компьютеры.
3. В рабочей области выберите закладку **Политики**.
4. Выполните одно из следующих действий:
 - Нажмите на кнопку **Создать политику**.
 - По правой клавише мыши откройте контекстное меню. Выберите пункт **Создать → Политику**.

Запустится мастер создания политики.
5. Следуйте указаниям мастера создания политики.

Изменение параметров политики

► Чтобы изменить параметры политики, выполните следующие действия:

1. Откройте Консоль администрирования Kaspersky Security Center.
2. В папке **Управляемые компьютеры** дерева консоли откройте папку с названием нужной группы администрирования, для которой вы хотите изменить параметры политики.

3. В рабочей области выберите закладку **Политики**.
4. Выберите нужную политику.
5. Выполните одно из следующих действий:
 - По правой клавише мыши вызовите контекстное меню политики. Выберите пункт **Свойства**.
 - Нажмите на кнопку **Изменить политику**, которая находится справа от списка политик.

Откроется окно **Свойства: <Название политики>**.

Параметры политики для Kaspersky Endpoint Security 10 включают в себя параметры задач и параметры программы. В разделах **Защита** и **Контроль** окна **Свойства: <Название политики>** представлены параметры задач, а в разделе **Дополнительные параметры** представлены параметры программы.

6. Измените параметры политики.
7. В окне **Свойства: <Название политики>** нажмите на кнопку **ОК**, чтобы сохранить внесенные изменения.

Просмотр сообщений пользователей в хранилище событий Kaspersky Security Center

Kaspersky Endpoint Security предоставляет пользователям локальной сети организации, на компьютерах которых установлена программа, возможность отправлять сообщения администратору.

Возможны два способа доставки сообщения администратору от пользователя:

- В виде события в хранилище событий Kaspersky Security Center. Событие пользователя передается в хранилище событий Kaspersky Security Center,

если программа Kaspersky Endpoint Security, установленная на компьютере пользователя, работает под активной политикой.

- В виде сообщения электронной почты. Информация пользователя передается в виде сообщения электронной почты, если программа Kaspersky Endpoint Security, установленная на компьютере пользователя, работает не под политикой или под мобильной политикой.
- Чтобы просмотреть сообщение пользователя в хранилище событий Kaspersky Security Center, выполните следующие действия:

1. Откройте Консоль администрирования Kaspersky Security Center.
2. Откройте папку **Отчеты и уведомления \ События \ Предупреждения** дерева консоли.

В рабочей области Kaspersky Security Center отображается список всех событий-предупреждений, в том числе и сообщений администратору, приходящих от пользователей локальной сети организации. Рабочая область Kaspersky Security Center располагается справа от дерева консоли.

3. Выберите в списке событий сообщение администратору.
4. Откройте свойства события одним из следующих способов:
 - Дважды нажмите левой клавишей мыши по событию в списке событий.
 - По правой клавише мыши откройте контекстное меню события. В контекстное меню события выберите пункт **Свойства**.
 - Нажмите на кнопку **Открыть свойства события** справа от списка событий.

Проверка соединения с Сервером администрирования вручную. Утилита klnagchk

В комплект поставки Агента администрирования входит утилита *klnagchk*, предназначенная для проверки соединения с Сервером администрирования.

После установки Агента администрирования утилита располагается в директории `/opt/kaspersky/klnagent/bin` и при запуске в зависимости от используемых ключей выполняет следующие действия:

- выводит на экран или заносит в файл журнала событий значения параметров подключения установленного на клиентском компьютере Агента администрирования к Серверу администрирования;
- записывает в файл журнала событий статистику 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.

Синтаксис утилиты:

```
klnagchk [-logfile <имя файла>] [-sp] [-savecert <путь к файлу сертификата>] [-restart]
```

Описание ключей:

- `-logfile <имя файла>` – записать значения параметров подключения Агента администрирования к Серверу и результаты выполнения утилиты в файл журнала; по умолчанию информация сохраняется в файле `stdout.tx`; если ключ не используется, параметры, результаты и сообщения об ошибках выводятся на экран.
- `-sp` – вывести пароль для аутентификации пользователя на прокси-сервере; параметр используется, если подключение к Серверу администрирования осуществляется через прокси-сервер.
- `-savecert <имя файла>` – сохранить сертификат для аутентификации доступа к Серверу администрирования в указанном файле.
- `-restart` – перезапустить Агент администрирования после завершения утилиты.

Подключение к Серверу администрирования вручную. Утилита *klmover*

В комплект поставки Агента администрирования входит утилита *klmover*, предназначенная для управления подключением к Серверу администрирования.

После установки Агента администрирования утилита располагается в директории `/opt/kaspersky/klagent/bin` и при запуске в зависимости от используемых ключей выполняет следующие действия:

- подключает Агент администрирования к Серверу администрирования с указанными параметрами;
- записывает результаты выполнения операции в файл журнала событий или выводит их на экран.

Синтаксис утилиты:

```
klmover [-logfile <имя файла>] {-address <адрес сервера>} [-pn <номер порта>] [-ps <номер SSL-порта>] [-noss1] [-cert <путь к файлу сертификата>] [-silent] [-dupfix]
```

Описание ключей:

- `-logfile <имя файла>` – записать результаты выполнения утилиты в указанный файл; если ключ не используется, результаты и сообщения об ошибках выводятся на `stdout`.
- `-address <адрес сервера>` – адрес Сервера администрирования для подключения; в качестве адреса может быть указан IP-адрес, NetBIOS или DNS-имя компьютера.
- `-pn <номер порта>` – номер порта, по которому будет осуществляться незащищенное подключение к Серверу администрирования; по умолчанию используется порт 14000.
- `-ps <номер SSL-порта>` – номер SSL-порта, по которому будет осуществляться защищенное подключение к Серверу администрирования с использованием протокола SSL. По умолчанию это порт 13000.

- `-noss1` – использовать незащищенное подключение к Серверу администрирования; если ключ не указан, подключение Агента к Серверу осуществляется по защищенному SSL-протоколу.
- `-cert` <путь к файлу сертификата> – использовать указанный файл сертификата для аутентификации доступа к новому Серверу администрирования. Если ключ не используется, Агент администрирования получит сертификат при первом подключении к Серверу администрирования.
- `-silent` – запустить утилиту на выполнение в неинтерактивном режиме; использование ключа может быть полезно, например, при запуске утилиты из сценария запуска при регистрации пользователя.
- `-dupfix` – данный ключ используется в случае, если установка Агента администрирования была выполнена не традиционным способом, с использованием дистрибутива, а, например, путем восстановления из образа диска.

Обращение в Службу технической поддержки

Этот раздел содержит информацию о способах и условиях получения технической поддержки.

В этом разделе

Способы получения технической поддержки.....	114
Техническая поддержка по телефону	115
Техническая поддержка через Kaspersky CompanyAccount	115

Способы получения технической поддержки

Если вы не нашли решения вашей проблемы в документации или других источниках информации о программе (см. раздел "Источники информации о программе" на стр. [14](#)), рекомендуется обратиться в Службу технической поддержки. Сотрудники Службы технической поддержки ответят на ваши вопросы об установке и использовании программы.

Техническая поддержка предоставляется только пользователям, которые приобрели коммерческую лицензию на использование программы. Пользователям, которые получили пробную лицензию, техническая поддержка не предоставляется.

Перед обращением в Службу технической поддержки ознакомьтесь с правилами предоставления технической поддержки (<http://support.kaspersky.ru/support/rules>).

Вы можете связаться со специалистами Службы технической поддержки одним из следующих способов:

- позвонить в Службу технической поддержки по телефону (<http://support.kaspersky.ru/support/contacts>);
- отправить запрос в Службу технической поддержки "Лаборатории Касперского" с портала Kaspersky CompanyAccount (<https://companyaccount.kaspersky.com>).

Техническая поддержка по телефону

В большинстве регионов по всему миру вы можете позвонить специалистам Службы технической поддержки. Вы можете найти информацию о способах получения технической поддержки в вашем регионе и контакты Службы технической поддержки на веб-сайте Службы технической поддержки "Лаборатории Касперского" (<http://support.kaspersky.ru/support/contacts>).

Перед обращением в Службу технической поддержки ознакомьтесь с правилами предоставления технической поддержки (<http://support.kaspersky.ru/support/rules>).

Техническая поддержка через Kaspersky CompanyAccount

Kaspersky CompanyAccount (<https://companyaccount.kaspersky.com>) – это портал для организаций, использующих программы "Лаборатории Касперского". Портал Kaspersky CompanyAccount предназначен для взаимодействия пользователей со специалистами "Лаборатории Касперского" с помощью электронных запросов. На портале Kaspersky CompanyAccount можно отслеживать статус обработки электронных запросов специалистами "Лаборатории Касперского" и хранить историю электронных запросов.

Вы можете зарегистрировать всех сотрудников вашей организации в рамках одной учетной записи Kaspersky CompanyAccount. Одна учетная запись позволяет вам централизованно управлять электронными запросами от зарегистрированных сотрудников в "Лабораторию Касперского", а также управлять правами этих сотрудников в Kaspersky CompanyAccount.

Портал Kaspersky CompanyAccount доступен на следующих языках:

- английском;
- испанском;
- итальянском;
- немецком;
- польском;
- португальском;
- русском;
- французском;
- японском.

Вы можете узнать больше о Kaspersky CompanyAccount на веб-сайте Службы технической поддержки (http://support.kaspersky.ru/faq/companyaccount_help).

Приложения

Этот раздел содержит информацию, которая дополняет основной текст документа.

В этом разделе

Параметры конфигурационных файлов.....	117
Команды управления Kaspersky Endpoint Security из командной строки	145
Коды возврата командной строки	175

Параметры конфигурационных файлов

В этом разделе описаны структуры и параметры конфигурационных файлов Kaspersky Endpoint Security в формате INI, а также правила редактирования конфигурационных файлов.

Правила редактирования конфигурационных файлов Kaspersky Endpoint Security

При редактировании конфигурационного файла соблюдайте следующие правила:

- В конфигурационном файле необходимо указать все обязательные параметры. Указать отдельные параметры задачи вы можете используя безфайловый способ задания параметров из командной строки.
- Если параметр принадлежит к какой-либо секции, помещайте его только в этой секции. В пределах одной секции вы можете помещать параметры в любом порядке.
- Закрывайте имена секций в квадратные скобки [].
- Вводите значения параметров в формате **имя параметра=значение** (пробелы между именем параметра и его значением не обрабатываются).

Пример:

```
[ScanScope.item_0000]  
AreaDesc=Home  
AreaMask.item_0000=*doc  
Path=/home
```

Символы "пробел" и "табуляция" игнорируются перед первой кавычкой и после последней кавычки строкового значения, а также в начале и в конце строкового значения, не заключенного в кавычки.

- Если вам нужно указать несколько значений параметра, повторите параметр столько раз, сколько значений вы хотите указать.

Пример:

```
AreaMask.item_0000=*xml  
AreaMask.item_0001=*doc
```

- Соблюдайте регистр при вводе значений параметров следующих типов:
 - имена (маски) проверяемых объектов и объектов исключения;
 - названия (маски) угроз;

При вводе остальных значений параметров соблюдать регистр не требуется.

- Указывайте значения параметров булевского типа следующим образом: Yes – No.
- Закрывайте в кавычки строковые значения, содержащие символ "пробел" (например, имена файлов и директорий, пути к ним; выражения, содержащие дату и время в формате "ГГГГ-ММ-ДД ЧЧ:ММ:СС").

Пример:

```
AreaDesc="Проверка почтовых баз"
```

Остальные значения вы можете вводить как в кавычках, так и без них.

Одиночная кавычка в начале или в конце строки считается ошибкой.

Общие параметры Kaspersky Endpoint Security

После изменения общих параметров Kaspersky Endpoint Security перезапустите программу.

Общие параметры конфигурационного файла имеют следующие значения:

SambaConfigPath

Директория, в которой хранится конфигурационный файл Samba. Конфигурационный файл Samba нужен для обеспечения работы значений `AllShared` или `Shared:SMB` для опции `Path`.

По умолчанию указана стандартная директория конфигурационного файла Samba на компьютере.

Значение по умолчанию: `/etc/samba/smb.conf`.

NfsExportPath

Директория, в которой хранится конфигурационный файл NFS. Конфигурационный файл NFS нужен для обеспечения работы значений `AllShared` или `Shared:NFS` для опции `Path`.

По умолчанию указана стандартная директория конфигурационного файла NFS на компьютере.

Значение по умолчанию: `/etc/exports`.

TraceFolder

Директория, в которой Kaspersky Endpoint Security сохраняет файлы журнала трассировки.

Если вы указываете другую директорию, убедитесь, что она разрешена на чтение и запись для учетной записи, с правами которой работает Kaspersky Endpoint Security.

Значение по умолчанию: `/var/log/kaspersky/kesl`.

TraceLevel

Уровень детализации журнала трассировки.

Возможные значения:

`Detailed` – наиболее детализированный журнал трассировки;

`NotDetailed` – журнал трассировки содержит оповещения об ошибках;

`None` – не создает журнал трассировки.

Значение по умолчанию: `None`.

BlockFilesGreaterMaxFileNamePath

Блокирование доступа к файлам, длина полного пути к которым превышает заданное значение параметра, в байтах.

Если длина полного пути к проверяемому файлу превышает значение этого параметра, задачи проверки по требованию пропускают такой файл при проверке.

Возможные значения: 4096 – 33554432.

Значение по умолчанию: 16384.

DetectOtherObjects

Включает / выключает обнаружение легальных программ, которые могут быть использованы злоумышленником для нанесения вреда компьютеру или данным пользователя.

Возможные значения:

Yes – включать обнаружение легальных программ, которые могут быть использованы злоумышленником для нанесения вреда компьютеру или данным пользователя;

No – выключать обнаружение легальных программ, которые могут быть использованы злоумышленником для нанесения вреда компьютеру или данным пользователя.

Значение по умолчанию: *No*.

UseKSN

Включает / выключает участие в Kaspersky Security Network.

Возможные значения:

Yes – включить участие в Kaspersky Security Network;

No – выключить участие в Kaspersky Security Network.

Значение по умолчанию: *No*.

UseProxy

Включает / выключает использование прокси для Kaspersky Security Network, активации программы и обновлений.

Возможные значения:

Yes – включить использование прокси;

No – выключить использование прокси.

Значение по умолчанию: *No*.

ProxyServer

Параметры прокси-сервера в формате [user[:password]@]host[:port].

MaxEventsNumber

Максимальное количество событий, которые будет хранить Kaspersky Endpoint Security. При превышении заданного количества событий Kaspersky Endpoint Security удаляет наиболее давние события.

Значение по умолчанию: 500000.

LimitNumberOfScanFileTasks

Максимальное количество задач типа `Scan_File`, которые непривилегированный пользователь может запустить на компьютере одновременно. Этот параметр не ограничивает количество задач, которые запускает пользователь с root-правами. Если задано значение 0, непривилегированный пользователь не может запускать задачи типа `Scan_File`.

Возможные значения: 0 – 4294967295.

Значение по умолчанию: 0.

UseSysLog

Включает / выключает запись информации о событиях в syslog.

Yes – включить запись информации о событиях в syslog;

No – выключить запись информации о событиях в syslog.

Значение по умолчанию: No.

EventsStoragePath

Файл базы данных, в которой Kaspersky Endpoint Security сохраняет информацию о событиях.

Значение по умолчанию: `/var/opt/kaspersky/kes1/events.db`.

См. также

Параметры задачи постоянной защиты и задач проверки по требованию	123
Правила редактирования конфигурационных файлов Kaspersky Endpoint Security	117

Параметры задачи постоянной защиты и задач проверки по требованию

Вы можете настраивать работу задач постоянной защиты и проверки по требованию, изменяя параметры в конфигурационных файлах этих задач.

Чтобы изменить задачу, нужно выполнить следующую последовательность действий:

1. Экспортируйте параметры задачи в конфигурационный файл (см. стр. [167](#)).
2. В конфигурационном файле измените параметры задачи в соответствии со своими требованиями (см. стр. [117](#)).
3. Импортируйте в задачу конфигурационный файл с измененными параметрами (см. стр. [168](#)).

В этом разделе описаны секции и параметры конфигурационных файлов задачи постоянной защиты и задач проверки по требованию.

Структура конфигурационного ini-файла задачи постоянной защиты и задачи проверки по требованию

Конфигурационный файл задачи постоянной защиты и задачи проверки по требованию состоит из отдельных параметров и секций. Секции конфигурационного файла описывают области проверки и области исключения, используемые Kaspersky Endpoint Security во время выполнения задачи постоянной защиты и задач проверки по требованию.

Конфигурационный файл задачи постоянной защиты и задач проверки по требованию содержит следующие секции:

[ScanScope.item_#]

В этой секции вы можете указать название области проверки. С помощью параметров этой секции вы можете сформировать область проверки.

Эта секция является обязательной.

[ExcludedFromScanScope.item_#] (см. стр. [135](#))

В этой секции вы можете указать область исключения из проверки.

Эта секция не является обязательной.

Если вы хотите указать несколько областей проверки или исключений, задайте несколько секций [ScanScope.item_#] и секций [ExcludedFromScanScope.item_#] (только в задачах постоянной защиты).

Kaspersky Endpoint Security обрабатывает области в порядке, указанном в идентификаторе секции.

Общие параметры задачи постоянной защиты и задач проверки по требованию

Конфигурационные файлы задачи постоянной защиты и задач проверки по требованию содержат следующие параметры:

ScanArchived

Включение / отключение проверки архивов (включая самораспаковывающиеся архивы SFX). Kaspersky Endpoint Security обнаруживает угрозы в архивах, но не лечит их.

Возможные значения:

Yes – проверять архивы;

No – не проверять архивы.

Значения по умолчанию:

в задаче постоянной защиты – No;

в задаче проверки по требованию – Yes.

ScanSfxArchived

Включение / отключение проверки только самораспаковывающихся архивов (архивов, имеющих в своем составе исполняемый модуль-распаковщик, self-extracting archives).

Возможные значения:

Yes – проверять самораспаковывающиеся архивы;

No – не проверять самораспаковывающиеся архивы.

Значения по умолчанию:

в задаче постоянной защиты – No;

в задаче проверки по требованию – Yes.

ScanMailBases

Включение / отключение проверки почтовых баз Microsoft Outlook®, Outlook Express, The Bat! и других почтовых клиентов.

Возможные значения:

Yes – проверять файлы почтовых баз;

No – не проверять файлы почтовых баз.

Значение по умолчанию: No.

ScanPlainMail

Включение / отключение проверки сообщений электронной почты в текстовом формате (plain text).

Возможные значения:

Yes – проверять сообщения электронной почты в текстовом формате;

No – не проверять сообщения электронной почты в текстовом формате.

Значение по умолчанию: No.

ScanPacked

Включение / отключение проверки исполняемых файлов, упакованных программами-упаковщиками двоичного кода (например, UPX или ASPack). Составные объекты этого типа чаще других содержат угрозы.

Возможные значения:

Yes – проверять упакованные файлы;

No – не проверять упакованные файлы.

Значение по умолчанию: Yes.

UseSizeLimit

Включение / отключение применения параметра `SizeLimit` (максимальный размер проверяемого объекта).

Возможные значения:

`Yes` – применять параметр `SizeLimit`;

`No` – не применять параметр `SizeLimit`.

Значение по умолчанию: `No`.

SizeLimit

Задаёт максимальный размер проверяемого объекта (в мегабайтах). Если размер проверяемого объекта превышает указанное значение, Kaspersky Endpoint Security пропускает объект.

Этот параметр применяется совместно с параметром `UseSizeLimit`.

Возможные значения: `0` – `999 999`. `0` – Kaspersky Endpoint Security проверяет объекты любого размера.

Значение по умолчанию: `0`.

UseTimeLimit

Включение / отключение применения параметра `TimeLimit` (максимальная продолжительность проверки объекта).

Возможные значения:

`Yes` – применять параметр `TimeLimit`;

`No` – не применять параметр `TimeLimit`.

Значения по умолчанию:

в задаче постоянной защиты – `Yes`;

в задаче проверки по требованию – `No`.

TimeLimit

Задаёт максимальную продолжительность проверки объекта (в секундах). Kaspersky Endpoint Security прекращает проверку объекта, если она выполняется дольше, чем указано значением этого параметра.

Этот параметр применяется совместно с параметром `UseTimeLimit`.

Возможные значения: 0 – 9999. 0 – продолжительность проверки объектов не ограничена.

Значение по умолчанию: 0.

FirstAction

Выбор первого действия Kaspersky Endpoint Security над заражёнными объектами.

В задачах постоянной защиты, перед тем как выполнить выбранное вами действие, Kaspersky Endpoint Security блокирует доступ к объекту для программы, которая к нему обратилась.

Возможные значения:

`Cure` (лечить) – Kaspersky Endpoint Security пытается вылечить объект, сохранив копию объекта в резервном хранилище. Если лечение невозможно (например, тип объекта или тип угрозы в объекте не предполагает лечения), Kaspersky Endpoint Security оставляет объект неизменным. Если первым действием выбрано `Cure`, рекомендуется задать второе действие в параметре `SecondAction`.

`Remove` (удалять) – Kaspersky Endpoint Security удаляет заражённый объект, предварительно создав его резервную копию.

`Recommended` (выполнять рекомендуемое действие) – Kaspersky Endpoint Security автоматически выбирает и выполняет действие над объектом на основе данных об обнаруженной в объекте угрозе. Например, Kaspersky Endpoint Security сразу удаляет троянские программы, так как они не заражают другие файлы и поэтому не предполагают лечения.

`Block` (блокировать) – Kaspersky Endpoint Security блокирует доступ к зараженному объекту. Информация о зараженном объекте сохраняется в журнале.

Значение используется только в задаче постоянной защиты.

`Skip` (пропускать) – Kaspersky Endpoint Security не пытается вылечить или удалить зараженный объект. Информация о зараженном объекте сохраняется в журнале.

Значение используется только в задачах проверки по требованию.

Значение по умолчанию: `Recommended`.

SecondAction

Выбор второго действия Kaspersky Endpoint Security над зараженными объектами. Kaspersky Endpoint Security выполняет второе действие, если не удалось выполнить первое действие.

Значения параметра `SecondAction` такие же, как значения параметра `FirstAction`.

Если в качестве первого действия выбрано `Block` (для задачи постоянной защиты) / `Skip` (для задачи проверки по требованию) или `Remove`, то второе действие указывать не нужно. В остальных случаях рекомендуется указывать два действия. Если вы не указали второе действие, Kaspersky Endpoint Security в качестве второго действия применяет `Block` (для задачи постоянной защиты) / `Skip` (для задачи проверки по требованию).

Значение по умолчанию: `Block` (для задачи постоянной защиты) / `Skip` (для задачи проверки по требованию).

UseExcludeMasks

Включает / отключает исключение из проверки объектов, указанных параметром `ExcludeMasks`.

Возможные значения:

`Yes` – исключать объекты, указанные параметром `ExcludeMasks`;

`No` – не исключать объекты, указанные параметром `ExcludeMasks`.

Значение по умолчанию: `No`.

ExcludeMasks

Исключает из проверки объекты по именам или маскам. С помощью этого параметра вы можете исключать из указанной области проверки отдельный файл по имени или несколько файлов, используя маски в формате командной оболочки.

Значение по умолчанию: не задано.

Пример:

```
UseExcludeMasks=Yes
```

```
ExcludeMasks.item_0000=eicar1.*
```

```
ExcludeMasks.item_0001=eicar2.*
```

UseExcludeThreats

Включает или отключает исключение из проверки объектов с угрозами, указанными параметром `ExcludeThreats`.

Возможные значения:

`Yes` – исключать из проверки объекты, которые содержат угрозы, указанные параметром `ExcludeThreats`;

`No` – не исключать из проверки объекты, которые содержат угрозы, указанные параметром `ExcludeThreats`.

Значение по умолчанию: `No`.

ExcludeThreats

Исключает из проверки объекты по названиям обнаруженных в объектах угроз. Перед тем как указать значения этого параметра, убедитесь, что включен параметр UseExcludeThreats.

Чтобы исключить из проверки один объект, укажите полное название угрозы, обнаруженной в этом объекте, – строку-заключение Kaspersky Endpoint Security о том, что объект является зараженным.

Например, вы используете одну из утилит для получения информации о сети. Для того чтобы Kaspersky Endpoint Security не блокировал ее, добавьте полное название угрозы в ней в список угроз, исключаемых из проверки.

Вы можете найти полное название угрозы, обнаруженной в объекте, в журнале Kaspersky Endpoint Security. Вы также можете найти полное название угрозы на веб-сайте Вирусной энциклопедии (<http://www.securelist.ru>). Чтобы найти название угрозы, введите название программы в поле **Поиск**.

Значение параметра чувствительно к регистру.

Значение по умолчанию: не задано.

Примеры:

```
UseExcludeThreats=Yes
```

```
ExcludeThreats.item_0000=EICAR-Test-*
```

```
ExcludeThreats.item_0001=?rojan.Linux
```

ReportCleanObjects

Включает / отключает запись в журнал информации о проверенных объектах, которые Kaspersky Endpoint Security признал незараженными.

Вы можете включить этот параметр, например, чтобы убедиться в том, что какой-либо объект был проверен Kaspersky Endpoint Security.

Возможные значения:

Yes – записывать в журнал информацию о незараженных объектах;

No – не записывать в журнал информацию о незараженных объектах.

Значение по умолчанию: *No*.

ReportPackedObjects

Включает / отключает запись в журнал информации о проверенных объектах, которые являются частью составных объектов.

Вы можете включить этот параметр, например, чтобы убедиться в том, что какой-либо объект в составе архива был проверен Kaspersky Endpoint Security.

Возможные значения:

Yes – записывать в журнал информацию о проверке объектов в составе архивов;

No – не записывать в журнал информацию о проверке объектов в составе архивов.

Значение по умолчанию: *No*.

ReportUnprocessedObjects

Включает / отключает запись в журнал информации о непроверенных объектах.

Возможные значения:

Yes – записывать в журнал информацию о непроверенных объектах;

No – не записывать в журнал информацию о непроверенных объектах.

Значение по умолчанию: *No*.

UseAnalyzer

Включает / отключает эвристический анализатор.

Возможные значения:

`Yes` – включить эвристический анализатор;

`No` – отключить эвристический анализатор.

Значение по умолчанию: `Yes`.

HeuristicLevel

Уровень эвристического анализа.

Возможные значения:

`Light` – наименее тщательная проверка, минимальная загрузка системы;

`Medium` – средний уровень эвристического анализа, сбалансированная загрузка системы;

`Deep` – наиболее тщательная проверка, максимальная загрузка системы;

`Recommended` – рекомендуемое значение.

Значение по умолчанию: `Recommended`.

UselChecker

Включает / отключает использование технологии iChecker.

Возможные значения:

`Yes` – включить использование технологии iChecker;

`No` – отключить использование технологии iChecker.

Значение по умолчанию: `Yes`.

ScanByAccessType

С помощью этого параметра вы можете задать режим постоянной защиты. Параметр `ScanByAccessType` применяется только в задачах постоянной защиты.

Возможные значения:

`SmartCheck` – проверять файл при попытке открытия, и проверять файл повторно при попытке закрытия, если файл был изменен. Если процесс во время своей работы многократно обращается к файлу в течение некоторого времени и изменяет его, повторно проверять файл только при последней попытке закрытия файла этим процессом.

`OpenAndModify` – проверять файл при попытке открытия и проверять его повторно при попытке закрытия, если файл был изменен.

`Open` – проверять файл при попытке открытия как на чтение, так и на выполнение или изменение.

Значение по умолчанию: `SmartCheck`.

[ScanScope.item_#]

В секции [ScanScope.item_#] содержатся следующие параметры:

AreaDesc

Описание области проверки; содержит дополнительную информацию об области проверки. Максимальная длина строки, задаваемой этим параметром, равна 4096 символов.

Значение по умолчанию: `All objects`.

Пример:

```
AreaDesc="Проверка почтовых баз"
```

UseScanArea

Этот параметр включает / отключает проверку указанной области. Для выполнения задачи необходимо включить проверку хотя бы одной области.

Возможные значения:

Yes – проверять указанную область;

No – не проверять указанную область.

Значение по умолчанию: Yes.

AreaMask

С помощью этого параметра вы можете ограничивать область проверки.

В области проверки Kaspersky Endpoint Security проверяет только файлы, указанные помощью масок в формате командной оболочки.

Если параметр не указан, Kaspersky Endpoint Security проверяет все объекты в области проверки. Вы можете указать несколько значений этого параметра.

Значение по умолчанию: * (проверять все объекты).

Пример:

```
AreaMask=*doc
```

Path

С помощью этого параметра вы можете указать путь к проверяемым объектам.

Значение параметра Path состоит из двух элементов: <тип файловой системы>:<протокол доступа>. Также он может содержать путь к директории в локальной файловой системе.

Возможные значения:

<путь к локальной директории> – проверять объекты в указанной директории;

Shared:NFS – проверять ресурсы файловой системы компьютера, предоставленные для доступа по протоколу NFS;

`Shared:SMB` – проверять ресурсы файловой системы компьютера, предоставленные для доступа по протоколу SMB;

`AllRemoteMounted` – проверять все удаленные директории, смонтированные на компьютере с помощью протоколов SMB и NFS;

`AllShared` – проверять все ресурсы файловой системы компьютера, предоставленные для доступа по протоколам SMB и NFS.

[ExcludedFromScanScope.item_#]

В секции [ExcludedFromScanScope.item_#] содержатся следующие параметры:

AreaDesc

Описание области исключения из проверки. Содержит дополнительную информацию об области исключения.

Значение по умолчанию: не задано.

Пример:

```
AreaDesc="Исключение разделенных SAMBA"
```

UseScanArea

Этот параметр включает / исключает проверку указанной области.

Возможные значения:

`Yes` – исключать указанную область;

`No` – не исключать указанную область.

Значение по умолчанию: `Yes`.

Path

С помощью этого параметра вы можете указать путь к исключаемым объектам.

Значение параметра `Path` состоит из двух элементов: `<тип файловой системы>:<протокол доступа>`. Также он может содержать путь к директории в локальной файловой системе.

Возможные значения:

`<путь к локальной директории>` – исключать из проверки объекты в указанной директории;

`Shared:NFS` – исключать из проверки ресурсы файловой системы компьютера, предоставленные для доступа по протоколу NFS;

`Shared:SMB` – исключать из проверки ресурсы файловой системы компьютера, предоставленные для доступа по протоколу Samba;

`AllRemoteMounted` – исключать из проверки все удаленные директории, смонтированные на компьютере с помощью протоколов SMB и NFS;

`AllShared` – исключать из проверки все ресурсы файловой системы компьютера, предоставленные для доступа по протоколам SMB и NFS.

Параметры задач проверки загрузочных секторов и задач проверки памяти процессов

Вы можете настраивать работу задач проверки загрузочных секторов и задач проверки памяти процессов, изменяя параметры в конфигурационных файлах этих задач.

Параметры конфигурационных файлов имеют следующие значения:

UseExcludeMasks

Параметр не используется в задаче проверки памяти процессов.

Включает / отключает исключение из проверки объектов, указанных параметром `ExcludeMasks`.

Возможные значения:

`Yes` – исключать объекты, указанные параметром `ExcludeMasks`;

`No` – не исключать объекты, указанные параметром `ExcludeMasks`.

Значение по умолчанию: `No`.

ExcludeMasks

Параметр не используется в задаче проверки памяти процессов.

Исключает из проверки объекты по именам или маскам. С помощью этого параметра вы можете исключать из указанной области проверки отдельный файл по имени или несколько файлов, используя маски в формате командной оболочки.

Значение по умолчанию: не задано.

UseExcludeThreats

Включает или отключает исключение из проверки объектов с угрозами, указанными параметром `ExcludeThreats`.

Возможные значения:

`Yes` – исключать из проверки объекты, которые содержат угрозы, указанные параметром `ExcludeThreats`;

`No` – не исключать из проверки объекты, которые содержат угрозы, указанные параметром `ExcludeThreats`.

Значение по умолчанию: `No`.

ExcludeThreats

Исключает из проверки объекты по названиям обнаруженных в объектах угроз. Перед тем как указать значения этого параметра, убедитесь, что включен параметр `UseExcludeThreats`.

Чтобы исключить из проверки один объект, укажите полное название угрозы, обнаруженной в этом объекте, – строку-заключение Kaspersky Endpoint Security о том, что объект является зараженным.

Например, вы используете одну из утилит для получения информации о сети. Для того чтобы Kaspersky Endpoint Security не блокировал ее, добавьте полное название угрозы в ней в список угроз, исключаемых из проверки.

Вы можете найти полное название угрозы, обнаруженной в объекте, в журнале Kaspersky Endpoint Security. Вы также можете найти полное название угрозы на веб-сайте Вирусной энциклопедии (<http://www.securelist.ru>). Чтобы найти название угрозы, введите название программы в поле **Поиск**.

Значение параметра чувствительно к регистру.

Значение по умолчанию: не задано.

ReportCleanObjects

Включает / отключает запись в журнал информации о проверенных объектах, которые Kaspersky Endpoint Security признал незараженными.

Вы можете включить этот параметр, например, чтобы убедиться в том, что какой-либо объект был проверен Kaspersky Endpoint Security.

Возможные значения:

Yes – записывать в журнал информацию о незараженных объектах;

No – не записывать в журнал информацию о незараженных объектах.

Значение по умолчанию: No.

UseAnalyzer

Параметр не используется в задаче проверки памяти процессов.

Включает / отключает эвристический анализатор.

Возможные значения:

Yes – включить эвристический анализатор;

No – отключить эвристический анализатор.

Значение по умолчанию: Yes.

HeuristicLevel

Параметр не используется в задаче проверки памяти процессов.

Уровень эвристического анализа.

Возможные значения:

Light – наименее тщательная проверка, минимальная загрузка системы;

Medium – средний уровень эвристического анализа, сбалансированная загрузка системы;

Deep – наиболее тщательная проверка, максимальная загрузка системы;

Recommended – рекомендуемое значение.

Значение по умолчанию: Recommended.

Action

Выбор действия Kaspersky Endpoint Security над зараженными объектами.

Возможные значения:

Cure (лечить) – Kaspersky Endpoint Security пытается вылечить объект, сохранив копию объекта в резервном хранилище. Если лечение невозможно (например, тип объекта или тип угрозы в объекте не предполагает лечения), Kaspersky Endpoint Security оставляет объект неизменным.

Skip (пропускать) – Kaspersky Endpoint Security не пытается вылечить или удалить зараженный объект. Информация о зараженном объекте сохраняется в журнале.

Значение по умолчанию: Cure.

Параметры задач обновления и задач копирования обновлений

Вы можете настраивать работу задач обновления и задач копирования обновлений, изменяя параметры в конфигурационных файлах этих задач.

Конфигурационный файл задач обновления и задач копирования обновлений состоит из отдельных параметров и секции `[CustomSources.item_#]`. В этой секции вы можете настроить параметры пользовательских источников обновлений. Если вы хотите указать несколько пользовательских источников обновления, вам нужно описать каждый из источников в отдельной секции `[CustomSources.item_#]`. Kaspersky Endpoint Security будет использовать эти параметры при обращении к пользовательским источникам обновления. Эта секция не является обязательной.

Общие параметры задач обновления и задач копирования обновлений

Конфигурационные файлы задач обновления и задач копирования обновлений содержат следующие параметры:

SourceType

С помощью этого параметра вы можете выбрать источник, из которого Kaspersky Endpoint Security будет получать обновления.

Возможные значения:

`KLServers` – Kaspersky Endpoint Security получает обновления с одного из серверов обновлений "Лаборатории Касперского". Обновления загружаются по протоколу HTTP.

`SCServer` – Kaspersky Endpoint Security загружает обновления на защищаемый компьютер с установленного в локальной сети Сервера администрирования Kaspersky Security Center. Вы можете выбрать этот источник обновления, если вы используете программу Kaspersky Security Center для централизованного управления антивирусной защитой компьютеров в вашей организации.

Custom – Kaspersky Endpoint Security загружает обновления из пользовательского источника, указанного в секции [CustomSources.item_#] (см. раздел "[CustomSources.item_#]" на стр. [143](#)). Вы можете указывать директории HTTP-серверов, директории на любом смонтированном устройстве защищаемого компьютера, включая директории на удаленных компьютерах, смонтированные по протоколам Samba или NFS.

Значение по умолчанию: KLServers.

UseKLServersWhenUnavailable

С помощью этого параметра вы можете настроить обращение Kaspersky Endpoint Security к серверам обновлений "Лаборатории Касперского" в случае если все пользовательские источники недоступны.

Возможные значения:

Yes – Kaspersky Endpoint Security обращается к серверам обновлений "Лаборатории Касперского", если все пользовательские источники обновлений недоступны;

No – Kaspersky Endpoint Security не обращается к серверам обновлений "Лаборатории Касперского", если все пользовательские источники обновлений недоступны.

Значение по умолчанию: Yes.

IgnoreProxySettingsForKLServers

С помощью этого параметра вы можете настроить использование прокси-сервера для соединения с серверами обновлений "Лаборатории Касперского".

Возможные значения:

Yes – Kaspersky Endpoint Security не использует прокси-сервер для соединения с серверами обновлений "Лаборатории Касперского";

No – Kaspersky Endpoint Security использует прокси-сервер для соединения с серверами обновлений "Лаборатории Касперского".

Значение по умолчанию: No.

IgnoreProxySettingsForCustomSources

С помощью этого параметра вы можете настроить использование прокси-сервера для соединения с пользовательскими источниками обновлений. Вам нужно включить этот параметр, если для соединения с каким-либо из пользовательских HTTP-серверов обновлений требуется доступ к прокси-серверу.

Возможные значения:

Yes – Kaspersky Endpoint Security не использует прокси-сервер для соединения с пользовательскими источниками обновлений;

No – Kaspersky Endpoint Security использует прокси-сервер для соединения с пользовательскими источниками обновлений.

Значение по умолчанию: **No**.

ConnectionTimeout

С помощью этого параметра вы можете указать время ожидания (в секундах) ответа от источника обновлений – HTTP-сервера при соединении с ним. Если в течение указанного промежутка времени от источника обновлений не приходит ответ, Kaspersky Endpoint Security обращается к другому указанному источнику обновлений.

Вы можете указывать только целые числа в диапазоне от 0 до 120.

Значение по умолчанию: **10**.

RetranslationFolder

Параметр доступен только для задач копирования обновлений.

С помощью этого параметра вы можете указать директорию, в которую будут копироваться обновления. Если указанная директория не существует, Kaspersky Endpoint Security создает ее во время выполнения задачи копирования обновлений.

[CustomSources.item_#]

Секция [CustomSources.item_#] содержит следующие параметры:

URL

С помощью этого параметра вы можете указать адрес пользовательского источника обновлений в локальной сети или в интернете.

Значение по умолчанию: не задано.

Примеры:

URL=http://example.com/bases/ – адрес HTTP-сервера, на котором помещается директория с обновлениями.

URL=/home/bases/ – директория на защищаемом компьютере, в которой содержатся базы программы.

Enabled

С помощью этого параметра вы можете включить или отключить использование источника обновлений, указанного в параметре URL. Для выполнения задачи необходимо, чтобы использование хотя бы одного источника обновлений было включено.

Возможные значения:

Yes – Kaspersky Endpoint Security использует источник обновления;

No – Kaspersky Endpoint Security не использует источник обновления.

Значение по умолчанию: не задано.

Пример:

Enabled=Yes

Параметры резервного хранилища

Вы можете настраивать работу задач для резервного хранилища, изменяя следующие параметры в конфигурационных файлах этих задач.

BackupFolder

Путь к директории резервного хранилища. Вы можете указать собственную директорию резервного хранилища, отличную от директории, установленной по умолчанию.

Для резервного хранилища вы можете использовать директории на любых устройствах компьютера. Не рекомендуется указывать директории, расположенные на удаленных компьютерах, например, смонтированных по протоколам Samba и NFS.

Kaspersky Endpoint Security начинает помещать объекты в указанную директорию после того, как вы импортируете параметры из файла в задачу для резервного хранилища и перезапустите Kaspersky Endpoint Security.

Если указанная директория не существует или недоступна, Kaspersky Endpoint Security использует директорию резервного хранилища по умолчанию.

Значение по умолчанию:

```
/var/opt/kaspersky/kes1/objects-backup/
```

BackupSizeLimit

Максимальный размер резервного хранилища.

При достижении максимального размера резервного хранилища Kaspersky Endpoint Security удаляет наиболее давние объекты.

Возможные значения: 0 – 999 999 (в мегабайтах).

Чтобы снять ограничение на размер резервного хранилища, укажите значение 0.

Значение по умолчанию: 0.

DaysToLive

Время хранения объектов в резервном хранилище (в днях).

Чтобы снять ограничение на время хранения объектов в резервном хранилище, укажите значение 0.

Значение по умолчанию: 90.

Команды управления Kaspersky Endpoint Security из командной строки

Этот раздел содержит информацию о командах управления Kaspersky Endpoint Security из командной строки.

Об управлении Kaspersky Endpoint Security из командной строки

Вы можете менять значения параметров Kaspersky Endpoint Security

При вводе команд Kaspersky Endpoint Security применяйте следующие правила:

- Соблюдайте регистр.
- Разделяйте ключи символом "пробел".
- Используя полное название команды или ключа, вводите значение через символ "равно" (=).

Пример:

Указать значение параметра URL для пользовательского источника обновлений для задачи обновления (ID=6) из командной строки:

```
/opt/kaspersky/kesl/bin/kesl-control --set-settings 6 SourceType=Custom  
CustomSources.item_0000.URL=http://site.domain/path  
CustomSources.item_0000.Enabled=Yes
```

Вывод справки о командах Kaspersky Endpoint Security

`--help`

Выводит справку о командах Kaspersky Endpoint Security.

Вывод событий Kaspersky Endpoint Security

`-W`

Включает вывод событий Kaspersky Endpoint Security.

Команды управления параметрами Kaspersky Endpoint Security и задачами

`-T`

Префикс; указывает на то, что команда принадлежит к группе команд управления параметрами Kaspersky Endpoint Security / управления задачами (необязательный).

`[-S] --app-info`

Выводит общую информацию о Kaspersky Endpoint Security.

`[-T] --get-app-settings --file <имя и директория файла>`

Возвращает общие параметры Kaspersky Endpoint Security.

`[-T] --set-app-settings --file <имя и директория файла>`

Устанавливает общие параметры Kaspersky Endpoint Security.

`[-T] --get-task-list`

Возвращает список существующих задач Kaspersky Endpoint Security.

`[-T] --get-task-state <ID задачи>|<имя задачи>`

Выводит состояние указанной задачи.

`[-T] --create-task <имя задачи> --type <тип задачи>
--file <имя и директория файла>`

Создает задачу указанного типа; импортирует в задачу параметры из указанного конфигурационного файла.

```
[-T] --delete-task <ID задачи>|<имя задачи>
```

Удаляет задачу.

```
[-T] --start-task <ID задачи>|<имя задачи> [-W] [--progress]
[--file <имя и директория файла>]
```

Запускает задачу.

```
[-T] --stop-task <ID задачи>|<имя задачи>
```

Останавливает задачу.

```
[-T] --suspend-task <ID задачи>|<имя задачи>
```

Приостанавливает задачу.

```
[-T] --resume-task <ID задачи>|<имя задачи>
```

Возобновляет задачу.

```
[-T] --get-settings <ID задачи>|<имя задачи>
--file <имя_и_директория_файла>
```

Выводит параметры задачи.

```
[-T] --set-settings <ID задачи>|<имя задачи> [<параметры>]
[--file <имя и директория файла>] [--add-path <путь>]
[--del-path <путь>] [--add-exclusion <исключение>]
[--del-exclusion <исключение>]
```

Устанавливает параметры задачи.

```
[-T] --scan-file <путь> [--action <действие>]
```

Создает и запускает временную задачу Scan_File.

Команды управления ключами

-L

Префикс; указывает на то, что команда принадлежит к группе команд управления ключами.

```
[-L] --install-active-key <код активации>|<файл ключа>
```

Добавляет активный ключ.

```
[-L] --install-additional-key <код активации>|<файл ключа>
```

Добавляет дополнительный ключ.

```
[-L] --revoke-active-key
```

Удаляет активный ключ.

```
[-L] --revoke-additional-key
```

Удаляет дополнительный ключ.

```
[-L] --query
```

Выводит информацию о ключе.

Команды управления резервным хранилищем

-B

Префикс; указывает на то, что команда принадлежит к группе команд управления резервным хранилищем.

```
[-B] --mass-remove --query
```

Очищает резервное хранилище, полностью или выборочно.

```
[-B] --query --limit --offset
```

Выводит информацию об объектах в резервном хранилище.

```
--limit
```

Максимальное количество объектов, о которых выводится информация.

```
--offset
```

Количество записей, на которое следует отступить от начала выборки.

```
[-B] --restore <ID объекта> --file <имя и директория файла>
```

Восстанавливает объект из резервного хранилища.

Команды управления журналом событий

-E

Префикс; указывает на то, что команда принадлежит к группе команд управления журналом событий.

```
[-E] --query --limit --offset --file <имя и директория файла> --db
```

Максимальное количество событий, о которых выводится информация.

--query

Выводит информацию о событиях по фильтру из журнала событий или указанного файла ротации.

--offset

Количество записей, на которое следует отступить от начала выборки.

--db

Имя файла базы данных.

Команды управления расписанием задач

```
[-T] --set-schedule <ID задачи>|<имя задачи>
```

```
--file <имя и директория файла>
```

Устанавливает параметры расписания задачи / импортирует их в задачу из конфигурационного файла.

```
[-T] --get-schedule <ID задачи>|<имя задачи>
```

```
--file <имя и директория файла>
```

Выводит параметры расписания задачи.

```
RuleType=Once|Monthly|Weekly|Daily|Hourly|Minutely|Manual|PS|BR
```

Расписание запуска задачи.

PS – запускать задачу после запуска Kaspersky Endpoint Security.

BR – запускать задачу после обновления антивирусных баз.

```
StartTime=[year/month/month_day] [hh]:[mm]:[ss];  
[<month_day>|<week_day>]; [<period>]
```

Время запуска задачи.

```
RandomInterval=<мин.>
```

Интервал запуска задачи, если несколько задач запущены одновременно (в минутах).

```
ExecuteTimeLimit=<мин.>
```

Ограничение времени выполнения задачи (в минутах).

```
RunMissedStartRules
```

Включает / выключает запуск пропущенной задачи после запуска Kaspersky Endpoint Security.

Вывод справки о командах Kaspersky Endpoint Security

Команда `kesl-control` с ключом `--help` <набор команд Kaspersky Endpoint Security> выводит справку о командах Kaspersky Endpoint Security.

Синтаксис команды

```
kesl-control --help [<набор команд Kaspersky Endpoint Security>]
```

<набор команд Kaspersky Endpoint Security>

Возможные значения:

[`-T`] – команды управления задачами и общими параметрами Kaspersky Endpoint Security;

[`-L`] – команды управления ключами;

[`-B`] – команды управления резервным хранилищем;

[`-E`] – команды управления событиями Kaspersky Endpoint Security.

Включение вывода событий

Команда `-W` включает режим вывода событий Kaspersky Endpoint Security. Вы можете использовать эту команду как отдельно, чтобы выводить все события Kaspersky Endpoint Security, как и совместно с командой `--start-task` (запустить задачу (см. раздел "Запуск и остановка задачи" на стр. [51](#))), чтобы выводить только события о выполняемой задаче. Вы можете использовать `--query` с флагом `-W` для вывода только определенных событий.

Команда возвращает название события и дополнительную информацию о событии.

Синтаксис команды

```
kesl-control -W
```

Примеры:

Включить режим вывода событий Kaspersky Endpoint Security:

```
/opt/kaspersky/kesl/bin/kesl-control -W
```

Быстрая проверка файлов и директорий

Команда `--scan-file` создает и запускает временную задачу `Scan_File`. Kaspersky Endpoint Security удаляет задачу после ее завершения или после перезапуска программы.

Синтаксис команды

```
kesl-control --scan-file <путь к файлу или директории> [ <путь к файлу или директории> ... ] --action <действие>
```

Описание аргументов и ключей

```
--scan-file <путь к файлу или директории>
```

Имя файла или директории, которые будут быстро проверены Kaspersky Endpoint Security. Вы можете добавить до 100 файлов или директорий для проверки.

```
--action <действие>
```

Необязательный ключ.

Возможные значения:

Recommended – выполнять рекомендуемое действие;

Cure – лечить;

Remove – удалять;

Skip – пропускать.

Значение по умолчанию: Skip.

Просмотр информации о программе

Команда `--app-info` выводит информацию о Kaspersky Endpoint Security.

Синтаксис команды

```
kesl-control [-S] --app-info
```

Результат выполнения команды

Name

Название Kaspersky Endpoint Security.

License status

Состояние лицензии.

License expiration date

Дата окончания срока действия лицензии.

Backup state

Количество объектов в резервном хранилище.

Backup usage space

Объем резервного хранилища.

Scan_My_Computer last run date

Время последнего запуска задачи Scan_My_Computer.

Anti-virus databases loaded

Отображает, загружены ли антивирусные базы.

Anti-virus databases date

Время последней загрузки антивирусных баз.

Anti-virus databases records

Количество записей в антивирусных базах.

Protection status

Состояние защиты компьютера.

KSN state

Статус подключения к Kaspersky Security Network.

Команды управления параметрами Kaspersky Endpoint Security и задачами

Этот раздел содержит информацию о командах управления параметрами Kaspersky Endpoint Security и задачами.

Получение общих параметров Kaspersky Endpoint Security

Команда `--get-app-settings` выводит общие параметры Kaspersky Endpoint Security. Используя эту команду, вы также можете получить общие параметры Kaspersky Endpoint Security, заданные с помощью ключей команды.

Вы можете использовать эту команду для изменения общих параметров Kaspersky Endpoint Security, установленного на компьютере:

1. Сохраните общие параметры Kaspersky Endpoint Security в конфигурационном файле с помощью команды `--get-app-settings`.

2. Откройте созданный конфигурационный файл, измените нужные параметры и сохраните изменения.
3. Импортируйте параметры из конфигурационного файла в Kaspersky Endpoint Security с помощью команды `--set-app-settings`. Kaspersky Endpoint Security применит новые значения параметров после того, как вы остановите и снова запустите Kaspersky Endpoint Security.

Вы можете использовать созданный конфигурационный файл для импорта параметров в Kaspersky Endpoint Security, установленный на другом компьютере.

Синтаксис команды

```
kesl-control [-T] --get-app-settings [--file <имя конфигурационного файла>] kesl-control [-T] --get-app-settings [<название параметра>]
```

Аргументы и ключи

```
--file <имя конфигурационного файла>
```

Имя конфигурационного файла, в котором будут сохранены параметры Kaspersky Endpoint Security. Если вы укажете имя файла, не указав пути к нему, файл будет создан в текущей директории. Если файл с указанным именем уже существует по указанному пути, он будет перезаписан. Если указанная директория отсутствует на диске, конфигурационный файл не будет создан.

Примеры:

Экспортировать общие параметры Kaspersky Endpoint Security в файл с именем `kesl_config.ini`. Сохранить созданный файл в текущей директории:

```
/opt/kaspersky/kesl/bin/kesl-control --get-app-settings --file kesl_config.ini
```

Вывести значение параметра `TraceLevel`:

```
/opt/kaspersky/kesl/bin/kesl-control --get-app-settings TraceLevel
```

Изменение общих параметров Kaspersky Endpoint Security

Команда `--set-app-settings` устанавливает с помощью ключей команды или импортирует из указанного конфигурационного файла общие параметры Kaspersky Endpoint Security.

Вы можете использовать эту команду для изменения общих параметров Kaspersky Endpoint Security:

1. Сохраните общие параметры Kaspersky Endpoint Security в конфигурационном файле с помощью команды `--get-app-settings`.
2. Откройте созданный конфигурационный файл, измените нужные параметры и сохраните изменения.
3. Импортируйте параметры из конфигурационного файла в Kaspersky Endpoint Security с помощью команды `--set-app-settings`. Kaspersky Endpoint Security применит новые значения параметров после того, как вы остановите и снова запустите Kaspersky Endpoint Security с помощью команд `--stop-app` и `--start-app` или с помощью команды `--restart-app`.

Синтаксис команды

```
kesl-control [-T] --set-app-settings --file <имя конфигурационного файла>  
kesl-control [-T] --set-app-settings <название параметра>=<значение параметра> <название параметра>=<значение параметра>
```

Аргументы и ключи

```
--file <имя конфигурационного файла>
```

Имя конфигурационного файла, параметры из которого будут импортированы в Kaspersky Endpoint Security; включает полный путь к файлу.

Примеры:

Импортировать в Kaspersky Endpoint Security общие параметры из конфигурационного файла с именем `/home/test/kav_config.ini`:

```
/opt/kaspersky/kesl/bin/kesl-control --set-app-settings --file  
/home/test/kav_config.ini
```

Установить уровень детализации в журнале трассировки "Важные события":

```
/opt/kaspersky/kesl/bin/kesl-control --set-app-settings  
TraceLevel=Warning
```

Параметры расписания задачи

Этот раздел содержит информацию о командах для управления расписанием задачи.

Получение параметров расписания задачи

Команда `--get-schedule` выводит параметры расписания задачи. Используя эту команду, вы также можете получить параметры расписания задачи, заданные с помощью ключей команды.

Вы можете использовать эту команду для изменения расписания задачи:

1. Сохраните параметры расписания в конфигурационном файле с помощью команды `--get-schedule`.
2. Откройте созданный конфигурационный файл, измените нужные параметры и сохраните изменения.
3. Импортируйте параметры из конфигурационного файла в Kaspersky Endpoint Security с помощью команды `--set-schedule`. Kaspersky Endpoint Security применит новые значения параметров расписания немедленно.

Синтаксис команды

```
kesl-control [-T] --get-schedule <ID задачи>|<имя задачи> [--file <имя  
конфигурационного файла>]
```

```
kesl-control [-T] --get-schedule <ID задачи>|<имя задачи> <название  
параметра>
```

Аргументы и ключи

<ID задачи>

Идентификационный номер задачи в Kaspersky Endpoint Security.

<имя задачи>

Имя задачи.

--file <имя конфигурационного файла>

Имя конфигурационного файла, в котором будут сохранены параметры расписания. Если вы укажете имя файла, не указав пути к нему, файл будет создан в текущей директории. Если файл с указанным именем уже существует по указанному пути, он будет перезаписан. Если указанная директория отсутствует на диске, конфигурационный файл не будет создан.

Примеры:

Сохранить параметры Kaspersky Endpoint Security в файле с именем on_demand_schedule.ini. Сохранить созданный файл в текущей директории:

```
/opt/kaspersky/kesl/bin/kesl-control --get-schedule 9 --file on_demand_schedule.ini
```

Вывести значение параметра RuleType расписания задачи постоянной защиты:

```
/opt/kaspersky/kesl/bin/kesl-control --get-schedule 9 RuleType
```

Изменение параметров расписания задачи

Команда `--set-schedule` устанавливает с помощью ключей команды или импортирует из указанного конфигурационного файла параметры расписания задачи.

Вы можете использовать эту команду для изменения параметров Kaspersky Endpoint Security:

1. Сохраните параметры расписания в конфигурационном файле с помощью команды `--get-schedule`.

2. Откройте созданный конфигурационный файл, измените нужные параметры и сохраните изменения.
3. Импортируйте параметры из конфигурационного файла в Kaspersky Endpoint Security с помощью команды `-T --set-schedule`. Kaspersky Endpoint Security применит новые значения параметров расписания немедленно.

Синтаксис команды

```
kesl-control --set-schedule <ID задачи>|<имя задачи> --file <имя конфигурационного файла>
```

```
kesl-control --set-schedule <ID задачи>|<имя задачи> <название параметра>=<значение параметра> <название параметра>=<значение параметра>
```

Аргументы и ключи

<ID задачи>

Идентификационный номер задачи в Kaspersky Endpoint Security.

<имя задачи>

Имя задачи.

`--file <имя конфигурационного файла>`

Имя конфигурационного файла, параметры расписания из которого будут импортированы в задачу; включает полный путь к файлу.

Пример:

Импортировать в задачу с ID=9 параметры расписания из конфигурационного файла с именем `/home/test/on_demand_schedule.ini`:

```
/opt/kaspersky/kesl/bin/kesl-control --set-schedule 9 --file /home/test/on_demand_schedule.ini
```

Команды управления задачами Kaspersky Endpoint Security

Этот раздел содержит информацию о командах управления задачами Kaspersky Endpoint Security.

Создание задачи

Команда `--create-task` создает задачу обновления или проверки по требованию. Команда импортирует в задачу параметры из указанного конфигурационного файла и выводит идентификационный номер созданной задачи.

Синтаксис команды

```
kesl-control [-T] --create-task <имя задачи> --type <тип задачи> [--file  
<имя конфигурационного файла>]
```

Описание и возможные значения аргументов и ключей

`--create-task <имя задачи>`

Присвоить задаче имя.

Имя задачи должно начинаться с буквы латинского алфавита и должно быть уникальным. Имя задачи может содержать неограниченное количество ASCII-символов.

`--type <тип задачи>`

Обязательный ключ.

Указать тип создаваемой задачи. О возможных значениях можно прочитать в разделе о задачах Kaspersky Endpoint Security (см. раздел "О задачах Kaspersky Endpoint Security" на стр. [49](#)).

`--file <имя конфигурационного файла>`

Необязательный ключ.

Указать полный путь к существующему конфигурационному файлу.

Kaspersky Endpoint Security импортирует в задачу параметры, описанные в этом конфигурационном файле.

Пример:

Создать задачу проверки по требованию с именем Fridayscan. Импортировать в задачу параметры из конфигурационного файла /home/test/config_kesscanner.ini:

```
/opt/kaspersky/kesl/bin/kesl-control --create-task Fridayscan --type  
ODS --file /home/test/config_kesscanner.ini
```

Удаление задачи

Команда `--delete-task` удаляет задачу Kaspersky Endpoint Security с указанным идентификационным номером или именем.

Вы можете удалять пользовательские задачи.

Синтаксис команды

```
kesl-control --delete-task <ID задачи>|<имя задачи>
```

Описание аргументов

<ID задачи>

Идентификационный номер задачи (ID). Чтобы просмотреть идентификационные номера задач Kaspersky Endpoint Security, используйте команду `--get-task-list` (см. стр. [166](#)).

<имя задачи>

Имя задачи.

Пример:

Удалить задачу с ID=20:

```
/opt/kaspersky/kesl/bin/kesl-control --delete-task 20
```


Запуск задачи

Команда `--start-task` запускает задачу с указанным идентификационным номером или именем.

Вы можете запускать задачи типов OAS, ODS, BootScan, MemoryScan, Rollback, Retranslate и Update.

Эта команда может быть использована с ключом `-W`, при этом выводится информация о событиях, возникающих во время выполнения задачи. После завершения задачи отслеживание событий прекращается.

Синтаксис команды

```
kesl-control --start-task <ID задачи>|<имя задачи> --[progress]
```

Описание аргументов и ключей

<ID задачи>

Идентификационный номер задачи (ID). Чтобы просмотреть идентификационные номера задач Kaspersky Endpoint Security, используйте команду `--get-task-list` (см. стр. [166](#)).

<имя задачи>

Имя задачи.

`--progress`

Отображать ход выполнения задачи (кроме задачи постоянной защиты).

Примеры:

Запустить задачу с ID=6:

```
/opt/kaspersky/kesl/bin/kesl-control --start-task 6
```

Запустить задачу с именем UpdateTask1 и отображать информацию о событиях, возникающих во время выполнения задачи:

```
/opt/kaspersky/kesl/bin/kesl-control --start-task UpdateTask1 -W
```

Запустить задачу проверки по требованию и отображать ход выполнения задачи:

```
/opt/kaspersky/kesl/bin/kesl-control --start-task 2 --progress
```

Остановка задачи

Команда `--stop-task` останавливает задачу с указанным идентификационным номером или именем.

Вы можете останавливать задачи всех типов, кроме Backup и License.

Эта команда может быть использована с ключом `-W`, при этом выводится информация о событиях, возникающих во время выполнения задачи. После завершения задачи отслеживание событий прекращается.

Синтаксис команды

```
kesl-control --stop-task <ID задачи>|<имя задачи>
```

Описание аргументов

<ID задачи>

Идентификационный номер задачи (ID). Чтобы просмотреть идентификационные номера задач Kaspersky Endpoint Security, используйте команду `--get-task-list` (см. стр. [166](#)).

<имя задачи>

Имя задачи.

Примеры:

Остановить задачу с ID=6:

```
/opt/kaspersky/kesl/bin/kesl-control --stop-task 6
```

Остановить задачу с именем ODStask и отображать информацию о событиях, возникающих во время выполнения задачи:

```
/opt/kaspersky/kesl/bin/kesl-control --stop-task ODStask -W
```

Приостановка задачи

Команда `--suspend-task` приостанавливает задачу с указанным идентификационным номером или именем.

Вы можете приостанавливать задачи типов Update, Retranslate, Rollback, ODS, BootScan и MemoryScan.

Синтаксис команды

```
kesl-control --suspend-task <ID задачи>|<имя задачи>
```

Описание аргументов

<ID задачи>

Идентификационный номер задачи (ID). Чтобы просмотреть идентификационные номера задач Kaspersky Endpoint Security, используйте команду `--get-task-list` (см. стр. [166](#)).

<имя задачи>

Имя задачи.

Пример:

Приостановить задачу с ID=19:

```
/opt/kaspersky/kesl/bin/kesl-control --suspend-task 19
```

Возобновление задачи

Команда `--resume-task` возобновляет задачу с указанным идентификационным номером или именем, приостановленную с помощью команды `--suspend-task`.

Вы можете возобновлять задачи типов Update, Retranslate, Rollback, ODS, BootScan и MemoryScan.

Синтаксис команды

```
kesl-control --resume-task <ID задачи>|<имя задачи>
```

Описание аргументов

<ID задачи>

Идентификационный номер задачи (ID). Чтобы просмотреть идентификационные номера задач Kaspersky Endpoint Security, используйте команду `--get-task-list` (см. стр. [166](#)).

<имя задачи>

Имя задачи.

Пример:

Возобновить задачу с ID=19:

```
/opt/kaspersky/kesl/bin/kesl-control --resume-task 19
```

Просмотр состояния задачи

Команда `--get-task-state` возвращает состояние указанной задачи.

Синтаксис команды

```
kesl-control --get-task-state <ID задачи>|<имя задачи>
```

Описание аргументов

<ID задачи>

Идентификационный номер задачи (ID). Чтобы просмотреть идентификационные номера задач Kaspersky Endpoint Security, используйте команду `--get-task-list` (см. стр. [166](#)).

<имя задачи>

Имя задачи.

Описание результата выполнения команды

Name

Имя задачи.

Пользователь присваивает имя пользовательской задаче при ее создании. Kaspersky Endpoint Security присваивает имена предустановленным задачам.

ID

Идентификационный номер задачи, который Kaspersky Endpoint Security присваивает задаче при ее создании.

Type

Тип задачи Kaspersky Endpoint Security.

State

Состояние задачи.

Пример:

Просмотреть состояние задачи с ID=1:

```
/opt/kaspersky/kesl/bin/kesl-control --get-task-state 1
```

Пример вывода результата выполнения команды:

```
Name: File_Monitoring
```

```
ID: 1
```

```
Type: OAS
```

```
State: Started
```

Просмотр списка задач Kaspersky Endpoint Security

Команда `--get-task-list` возвращает список существующих задач Kaspersky Endpoint Security.

Синтаксис команды

```
kesl-control --get-task-list
```

Описание результата выполнения команды

Name

Имя задачи.

Пользователь присваивает имя пользовательской задаче при ее создании. Kaspersky Endpoint Security присваивает имена предустановленным задачам.

ID

Идентификационный номер задачи, который Kaspersky Endpoint Security присваивает задаче при ее создании.

Type

Тип задачи Kaspersky Endpoint Security.

State

Состояние задачи.

Получение параметров задачи

Команда `--get-settings` выводит все параметры указанной задачи или ее параметры, заданные с помощью ключей команды.

Вы можете экспортировать параметры задачи в конфигурационный файл на одном компьютере, а импортировать параметры из этого конфигурационного файла в задачу соответствующего типа на другом компьютере.

Синтаксис команды

```
kesl-control --get-settings <ID задачи>|<имя задачи> [--file <имя  
конфигурационного файла>]
```

```
kesl-control --get-settings <ID задачи>|<имя задачи> <название секции INI  
файла>.<название параметра>
```

Описание и возможные значения аргументов и ключей

<ID задачи>

Идентификационный номер задачи.

<имя задачи>

Имя задачи.

`--file <имя конфигурационного файла>`

Имя конфигурационного файла, в котором будут сохранены параметры задачи. Если вы не укажете путь к файлу, файл будет создан в текущей директории. Если файл с указанным именем уже существует по указанному пути, он будет

перезаписан. Если указанная директория отсутствует, конфигурационный файл не будет создан.

Вы можете сохранить конфигурационный файл в формате INI.

Примеры:

Вывести значения параметров задачи проверки по требованию:

```
/opt/kaspersky/kesl/bin/kesl-control --get-settings 2
```

Экспортировать параметры задачи с проверки по требованию в файл `/home/test/configkesscanner.ini`:

```
/opt/kaspersky/kesl/bin/kesl-control --get-settings 2 --file  
/home/test/configkesscanner.ini
```

Экспортировать параметры задачи проверки по требованию в файл `configkesscanner.ini`, расположенный в текущей директории:

```
/opt/kaspersky/kesl/bin/kesl-control --get-settings 2 --file  
configkesscanner.ini
```

Вывести значение параметра `Path`, заданное в задаче проверки по требованию:

```
/opt/kaspersky/kesl/bin/kesl-control --get-settings 2 Path
```

Изменение параметров задачи

Команда `--set-settings` устанавливает параметры задачи с помощью ключей или импортирует параметры в задачу из конфигурационного файла.

Вы можете импортировать параметры из конфигурационного файла в задачи всех типов (пользовательские и предустановленные). Kaspersky Endpoint Security применяет новые значения параметров в задаче постоянной защиты немедленно. В задачах других типов Kaspersky Endpoint Security применяет новые значения параметров при следующем запуске задачи.

Синтаксис команды

```
kesl-control --set-settings <ID задачи>|<имя задачи>} [<параметры>]  
[--file <имя конфигурационного файла>] [--add-path <путь>] [--del-path  
<путь>] [--add-exclusion <путь>] [--del-exclusion <путь>]
```

Описание и возможные значения аргументов и ключей

<ID задачи>

Идентификационный номер задачи (ID). Чтобы просмотреть идентификационные номера задач Kaspersky Endpoint Security, используйте команду `--get-task-list` (см. стр. [166](#)).

<имя задачи>

Имя задачи.

`--file <имя конфигурационного файла>`

Имя конфигурационного файла, параметры из которого будут импортированы в задачу; включает полный путь к файлу.

`--add-path <путь>`

Добавляет в конфигурационный файл задачи секцию `[ScanScope.item_#]` с указанным значением параметра `Path=<путь>` и `UseScanArea=Yes`.

`--del-path <путь>`

Удаляет из конфигурационного файла задачи секцию `[ScanScope.item_#]` для указанного пути.

`--add-exclusion <путь>`

Добавляет в конфигурационный файл задачи секцию `[ExcludedFromScanScope.item_#]` с указанным значением параметра `Path=<путь>` и `UseScanArea=Yes`.

`--del-exclusion <путь>`

Удаляет из конфигурационного файла задачи секцию [ExcludedFromScanScope.item_#] для указанного пути.

Примеры:

Задать значение URL для пользовательского источника обновлений в задаче обновления с ID=6:

```
/opt/kaspersky/kesl/bin/kesl-control --set-settings 6
SourceType=Custom
CustomSources.item_0000.URL=http://site.domain/path
CustomSources.item_0000.Enabled=Yes
```

Добавить в конфигурационный файл задачи проверки по требованию область проверки:

```
/opt/kaspersky/kesl/bin/kesl-control --set-settings 2 --add-path
/home
```

В результате выполнения команды в конфигурационный файл будет добавлена секция:

```
[ScanScope.item_0001]
AreaDesc=
UseScanArea=Yes
Path=/home
AreaMask.item_0000=*
```

Команды управления ключами

Этот раздел содержит инструкции по просмотру информации о лицензиях и по действиям с ключами.

Добавление активного ключа

Команда `--install-active-key` добавляет активный ключ. Подробнее о ключах читайте в разделе "О ключе" (см. раздел "О ключе" на стр. [43](#)).

Синтаксис команды

```
kesl-control [-L] --install-active-key <путь к файлу  
ключа>|<код активации>
```

Аргументы и ключи

<путь к файлу ключа>

Путь к файлу ключа; если файл ключа находится в текущей директории, достаточно указать только имя файла.

Пример:

Добавить ключ из файла `/home/test/00000001.key` в качестве активного:

```
/opt/kaspersky/kesl/bin/kesl-control --install-active-key  
/home/test/00000001.key
```

Добавление дополнительного ключа

Команда `--install-additional-key` добавляет дополнительный ключа. Подробнее о ключах читайте в разделе "О ключе" (см. раздел "О ключе" на стр. [43](#)).

Если активный ключ не установлен, то дополнительный ключ будет установлен как основной.

Синтаксис команды

```
kesl-control [-L] --install-additional-key <путь к файлу ключа>
```

Аргументы и ключи

<путь к файлу ключа>

Путь к файлу ключа; если файл ключа находится в текущей директории, достаточно указать только имя файла.

Пример:

Установить дополнительный ключ из файла /home/test/00000002.key:

```
/opt/kaspersky/kesl/bin/kesl-control --install-additional-key  
/home/test/00000002.key
```

Удаление активного ключа

Команда `--revoke-active-key` удаляет активный ключ.

Синтаксис команды

```
kesl-control [-L] --revoke-active-key
```

Удаление дополнительного ключа

Команда `--revoke-additional-key` удаляет дополнительный ключ.

Синтаксис команды

```
kesl-control [-L] --revoke-additional-key
```

Ввод дополнительного кода активации

Команда `--install-additional-key` вводит дополнительный код активации. Подробнее о кодах активации читайте в разделе "О коде активации" (см. стр. [42](#)).

Синтаксис команды

```
kesl-control [-L] --install-additional-key <код активации>
```

Команды управления резервным хранилищем

Этот раздел содержит информацию о командах управления резервным хранилищем.

Получение информации об объектах в хранилище

Команда `--query` отображает информацию об объектах в резервном хранилище в текущий момент. Вы можете использовать фильтры.

Синтаксис команды

```
kesl-control [-B] --query "<логическое выражение>"  
[--limit=<максимальное количество записей>] [--offset=<отступ  
от начала выборки>]
```

Аргументы и ключи

`"<логическое выражение>"`

Устанавливает фильтр: логическое выражение.

`--limit=<максимальное количество записей>`

Устанавливает фильтр: максимальное количество записей из выборки, которое следует отобразить.

`--offset=<отступ от начала выборки>`

Устанавливает фильтр: количество записей, на которое следует отступить от начала выборки.

Примеры:

Просмотреть информацию об объектах в резервном хранилище, которые содержат слово test в имени файла или пути:

```
/opt/kaspersky/kesl/bin/kesl-control -B --query "FileName like '%test%'"
```

Восстановление объектов из хранилища

Команда `--restore` восстанавливает из резервного хранилища объект с указанным идентификатором.

Дата и время создания файла, восстановленного из резервного хранилища, отличаются от даты и времени создания исходного файла.

Синтаксис команды

```
kesl-control [-B] --restore <идентификатор объекта в резервном хранилище> [--file <имя файла и путь к файлу>]
```

Аргументы и ключи

<идентификатор объекта>

Чтобы получить идентификатор объекта, вы можете использовать команду `-B --query`.

`--file <имя файла>`

Имя, с которым Kaspersky Endpoint Security сохраняет объект при восстановлении. Включает путь к файлу.

Если путь к файлу не указан, Kaspersky Endpoint Security сохраняет файл в текущей директории.

Если указанная директория не существует, Kaspersky Endpoint Security создает ее.

Если ключ не указан, Kaspersky Endpoint Security сохраняет объект в исходном местоположении, в файле с исходным именем.

Примеры:

Восстановить объект с ID=1 в исходном местоположении:

```
/opt/kaspersky/kesl/bin/kesl-control -[B] --restore 1
```

Восстановить объект с ID=1 в текущей директории, в файле с именем restored.exe:

```
/opt/kaspersky/kesl/bin/kesl-control --restore 1 --file restored.exe
```

Восстановить объект с указанием нового имени и местоположения:

```
/opt/kaspersky/kesl/bin/kesl-control --restore 1 --file  
/newpath/newfile
```

Коды возврата командной строки

В этом разделе приведено описание кодов возврата командной строки.

0 – команда / задача выполнена успешно;

1 – общая ошибка в аргументах команды;

2 – ошибка в переданных настройках программы;

64 – Kaspersky Endpoint Security не запущен;

66 – антивирусные базы не загружены (используется только командой `--app-info`);

67 – активация 2.0 завершилась с ошибкой из-за сетевых проблем;

68 – выполнение команды невозможно, так как программа работает под политикой;

128 – неизвестная ошибка;

65 – все остальные ошибки.

АО "Лаборатория Касперского"

"Лаборатория Касперского" – известный в мире производитель систем компьютерной защиты от различных видов угроз, включая защиту от вирусов и других вредоносных программ, нежелательной почты (спама), сетевых и хакерских атак.

В 2008 году "Лаборатория Касперского" вошла в четверку ведущих мировых лидеров рынка программных решений для обеспечения информационной безопасности конечных пользователей (рейтинг "IDC Worldwide Endpoint Security Revenue by Vendor"). В России, по данным IDC, "Лаборатория Касперского" – самый предпочитаемый производитель систем компьютерной защиты для домашних пользователей ("IDC Endpoint Tracker 2014").

"Лаборатория Касперского" основана в России в 1997 году. Сегодня "Лаборатория Касперского" – это международная группа компаний с 38 офисами в 33 странах мира. В компании работает более 3000 квалифицированных специалистов.

Продукты. Продукты "Лаборатории Касперского" защищают как домашние компьютеры, так и компьютерные сети организаций.

Линейка персональных продуктов включает программы, обеспечивающие информационную безопасность настольных компьютеров и ноутбуков, планшетных компьютеров, смартфонов и других мобильных устройств.

Компания предлагает решения и технологии для защиты и контроля рабочих станций и мобильных устройств, виртуальных машин, файловых и веб-серверов, почтовых шлюзов, сетевых экранов. Также в портфеле компании есть специализированные продукты для защиты от DDoS-атак, защиты сред под управлением АСУТП и предотвращения финансового мошенничества. Использование этих решений в сочетании с централизованными средствами управления позволяет построить и эксплуатировать эффективную автоматизированную защиту организации любого размера от компьютерных угроз. Продукты "Лаборатории Касперского" сертифицированы крупными тестовыми лабораториями, совместимы с программным обеспечением многих поставщиков программного обеспечения и оптимизированы для работы на многих аппаратных платформах.

Вирусные аналитики "Лаборатории Касперского" работают круглосуточно. Каждый день они находят сотни тысяч новых компьютерных угроз, создают средства их обнаружения и лечения и включают сигнатуры этих угроз в базы, используемые программами "Лаборатории Касперского".

Технологии. Многие технологии, без которых трудно представить себе современный антивирус, впервые разработаны именно "Лабораторией Касперского". Не случайно программное ядро Антивируса Касперского используют в своих продуктах многие другие разработчики программного обеспечения, среди них: Alcatel-Lucent, Alt-N, Asus, BAE Systems, Blue Coat, Check Point, Cisco Meraki, Clearswift, D-Link, Facebook, General Dynamics, H3C, Juniper Networks, Lenovo, Microsoft, NETGEAR, Openwave Messaging, Parallels, Qualcomm, Samsung, Stormshield, Toshiba, Trustwave, Vertu, ZyXEL. Многие из инновационных технологий компании подтверждены патентами.

Достижения. За годы борьбы с компьютерными угрозами "Лаборатория Касперского" завоевала сотни наград. Например, в 2014 году по итогам испытаний и исследований, проведенных авторитетной австрийской антивирусной лабораторией AV-Comparatives, "Лаборатория Касперского" стала одним из двух лидеров по количеству полученных сертификатов Advanced+, в результате компания была удостоена сертификата Top Rated. Но главная награда "Лаборатории Касперского" – это приверженность пользователей по всему миру. Продукты и технологии компании защищают более 400 миллионов пользователей. Количество организаций, являющихся ее клиентами, превышает 270 тысяч.

Сайт "Лаборатории Касперского": <http://www.kaspersky.ru>

Вирусная энциклопедия: <https://securelist.ru>

Вирусная лаборатория: <http://newvirus.kaspersky.ru> (для проверки подозрительных файлов и сайтов)

Веб-форум "Лаборатории Касперского": <http://forum.kaspersky.com>

Информация о стороннем коде

Информация о стороннем коде содержится в файле `legal_notices.txt`, расположенном в директории установки программы.

Уведомления о товарных знаках

Зарегистрированные товарные знаки и знаки обслуживания являются собственностью их правообладателей.

Core – товарный знак Intel Corporation, зарегистрированный в Соединенных Штатах Америки и в других странах.

Linux – товарный знак Linus Torvalds, зарегистрированный в США и в других странах.

Microsoft, Outlook, Visual C++, Windows – товарные знаки Microsoft Corporation, зарегистрированные в Соединенных Штатах Америки и в других странах.

Novell – товарный знак Novell Inc., зарегистрированный в Соединенных Штатах Америки и в других странах.

Red Hat, Red Hat Enterprise Linux, CentOS – товарные знаки Red Hat Inc., зарегистрированные в Соединенных Штатах Америки и в других странах.

Debian – зарегистрированный товарный знак Software in the Public Interest, Inc.

SUSE – зарегистрированный в США и других странах товарный знак SUSE LLC.

Глоссарий

А

Агент администрирования

Компонент программы Kaspersky Security Center, осуществляющий взаимодействие между Сервером администрирования и программами "Лаборатории Касперского", установленными на конкретном сетевом узле (рабочей станции или сервере). Данный компонент является единым для всех программ "Лаборатории Касперского", работающих в операционной системе Windows®. Для программ, работающих в других операционных системах, предназначены отдельные версии Агента администрирования.

Активный ключ

Ключ, используемый в текущий момент для работы программы.

Антивирусные базы

Базы данных, которые содержат информацию об угрозах компьютерной безопасности, известных "Лаборатории Касперского" на момент выпуска антивирусных баз. Записи в антивирусных базах позволяют обнаруживать в проверяемых объектах вредоносный код. Антивирусные базы формируются специалистами "Лаборатории Касперского" и обновляются каждый час.

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 клиентских устройствах, входящих в состав этой группы администрирования.

Д

Дополнительный ключ

Ключ, подтверждающий право на использование программы, но не используемый в текущий момент.

З

Задача

Функции, выполняемые программой "Лаборатории Касперского", реализованы в виде задач, например: Постоянная защита файлов, Полная проверка устройства, Обновление баз.

Задача для набора устройств

Задача, определенная для набора клиентских устройств из произвольных групп администрирования и выполняемая на них.

Зараженный файл

Файл, внутри которого содержится вредоносный код (при проверке файла был обнаружен код известной программы, представляющей угрозу). Специалисты "Лаборатории

Касперского" не рекомендуют вам работать с такими файлами, поскольку это может привести к заражению вашего компьютера.

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 названию согласно классификации Вирусной энциклопедии. Для каждой задачи могут быть заданы свои исключения.

Источник обновлений

Ресурс, содержащий обновления антивирусных баз программы Kaspersky Endpoint Security. Источником обновлений антивирусных баз могут служить серверы обновлений "Лаборатории Касперского", а также HTTP-, FTP-сервер, локальная или сетевая папка.

К

Код активации

Код, который предоставляет вам "Лаборатория Касперского" при получении пробной лицензии или при приобретении коммерческой лицензии на использование Kaspersky Endpoint Security. Этот код требуется для активации программы.

Код активации представляет собой последовательность из двадцати латинских букв и цифр в формате XXXXX-XXXXX-XXXXX-XXXXX.

Л

Лечение объектов

Способ обработки зараженных объектов, в результате применения которого происходит полное или частичное восстановление данных. Не все зараженные объекты можно вылечить.

Лицензионный сертификат

Документ, который передает вам вместе с файлом ключа или кодом активации "Лаборатория Касперского". Документ содержит информацию о предоставляемой лицензии.

Ложное срабатывание

Ситуация, когда незараженный объект определяется программой "Лаборатории Касперского" как зараженный из-за того, что его код напоминает код вируса.

М

Маска файла

Представление названия и расширения файла общими символами.

Для формирования маски файла можно использовать любые символы, допустимые в названиях файлов, в том числе специальные:

- * – символ, заменяющий нуль или более нуль любых символов;
- ? – символ, заменяющий любой один символ.

Следует иметь в виду, что название и расширение файла всегда пишутся через точку.

О

Обновление

Процедура замены / добавления новых файлов (баз или программных модулей), получаемых с серверов обновлений "Лаборатории Касперского".

П

Параметры задачи

Параметры работы программы, специфичные для каждого типа задач.

Параметры программы

Параметры работы программы, общие для всех типов ее задач и отвечающие за работу программы в целом, например: параметры производительности программы, параметры ведения отчетов, параметры резервного хранилища.

Политика

Политика определяет параметры работы программы и доступ к настройке программы, установленной на компьютерах группы администрирования. Для каждой программы требуется создать свою политику. Вы можете создать неограниченное количество различных политик для программ, установленных на компьютерах в каждой группе администрирования, но в пределах группы администрирования только одна политика может применяться единовременно к каждой программе.

Постоянная 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, обрабатываются в соответствии с параметрами задачи (лечатся, удаляются).

Потенциально заражаемый файл

Файл, который в силу своей структуры или формата может быть использован злоумышленниками в качестве "контейнера" для размещения и распространения вредоносного кода. Как правило, это исполняемые файлы, например, с расширением com, exe, dll и др. Риск внедрения в такие файлы вредоносного кода достаточно высок.

Прокси-сервер

Служба в компьютерных сетях, позволяющая клиентам выполнять косвенные запросы к другим сетевым службам. Сначала клиент подключается к прокси-серверу и запрашивает какой-либо ресурс (например, файл), расположенный на другом сервере. Затем прокси-сервер либо подключается к указанному серверу и получает ресурс у него, либо возвращает ресурс из собственного кеша (в случаях, если прокси имеет свой кеш). В некоторых случаях запрос клиента или ответ сервера может быть изменен прокси-сервером в определенных целях.

Р

Резервное хранилище

Специальное хранилище, предназначенное для сохранения резервных копий файлов, создаваемых перед их первым лечением или удалением.

С

Сервер администрирования

Компонент программы Kaspersky Security Center, осуществляющий функции централизованного хранения информации об установленных в сети организации программах "Лаборатории Касперского" и управления ими.

Сигнатурный анализ

Технология обнаружения угроз, которая использует базы Kaspersky Endpoint Security, содержащие описания известных угроз и методы их устранения. Защита с помощью сигнатурного анализа обеспечивает минимально допустимый уровень безопасности. В соответствии с рекомендациями специалистов "Лаборатории Касперского" этот метод анализа всегда включен.

Состояние защиты

Текущее состояние защиты, характеризующее степень защищенности устройства.

У

Уровень безопасности

Под уровнем безопасности понимается предустановленный набор параметров работы компонента.

Ф

Файл ключа

Файл вида xxxxxxxx.key, который предоставляет вам "Лаборатория Касперского" при получении пробной лицензии или при приобретении коммерческой лицензии на использование Kaspersky Endpoint Security. Файл ключа требуется для активации программы.

Э

Эвристический анализ

Технология обнаружения угроз, которые невозможно определить с помощью текущей версии баз программ "Лаборатории Касперского". Позволяет находить файлы, которые могут содержать неизвестный вирус или новую модификацию известного вируса.

Файлам, в которых во время эвристического анализа обнаружен вредоносный код, присваивается статус *зараженный*.

Эвристический анализатор

Модуль Kaspersky Endpoint Security, выполняющий эвристический анализ.

Предметный указатель

К

Kaspersky Security Network85

Б

Базы программы.....54

З

Задача.....49

 выборочной проверки.....49, 75, 123, 151

 копирования обновлений.....49, 54, 140

 отката обновлений.....49, 54

 постоянной защиты.....49, 61, 123

 проверки загрузочных секторов.....49, 136

 проверки по требованию.....49, 63, 123

 проверки системной памяти.....49, 136

 реализующая сервер лицензий.....49, 145, 170

 управляющая резервным хранилищем.....49, 80, 173

И

Исключения.....70

К

Код активации..... 42

Л

Лицензирование программы 40, 42

Лицензия 41

 код активации 42

 Лицензионное соглашение 40

 файл ключа 43

О

Область защиты..... 61

Область проверки..... 63

Обновление..... 54, 140

П

Проверка

 задачи..... 49, 60, 123

 запуск задачи..... 51

 проверка составных файлов..... 61, 63

 сокращение времени проверки..... 76

Р

Резервное хранилище..... 80, 144, 173

настройка параметров.....	144, 173
удаление объекта.....	173

У

Уведомления.....	84
Управление задачами.....	49, 153

Э

Эвристический анализ.....	68
---------------------------	----