System Center

Endpoint Protection для Mac

Инструкция по установке и руководство пользователя

Microsoft

Содержание

System Center Endpoint Protection

В результате роста популярности операционных систем на основе Unix создатели вредоносных программ стали активнее разрабатывать вирусы для платформы Mac. System Center Endpoint Protection обеспечивает мощную и эффективную защиту от угроз, причем в том числе может обнаруживать и угрозы для Windows, защищая пользователей компьютеров Mac при взаимодействии с пользователями Windows и наоборот. Хотя вредоносные программы для Windows не представляют непосредственной угрозы для компьютеров Mac, их деактивация на компьютере под управлением Mac позволяет предотвратить заражение других компьютеров с системой Windows по локальной сети или через Интернет.

Системные требования

Для оптимальной работы System Center Endpoint Protection система должна отвечать перечисленным ниже аппаратным и программным требованиям.

System Center Endpoint Protection:

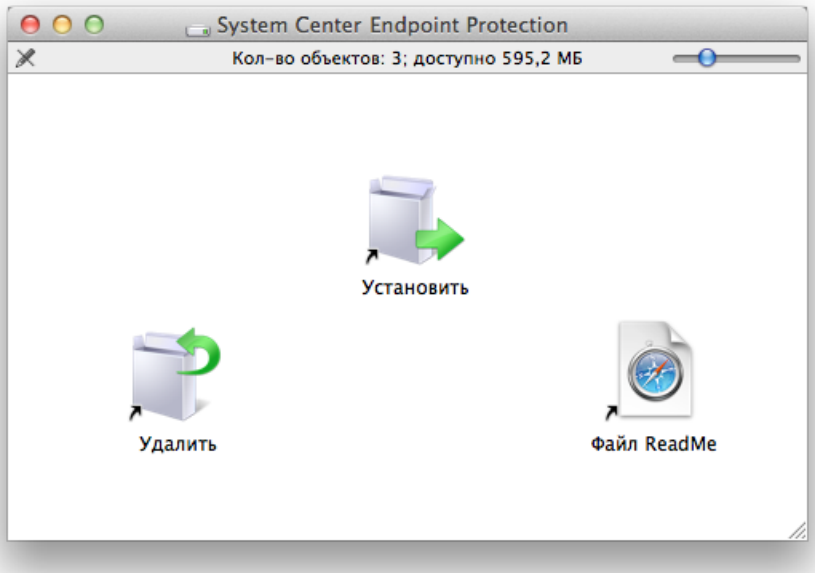
	Системные требования
Архитектура процессора	32-разрядная или 64-разрядная Intel®
Операционная система	Mac OS X 10.6 или более поздней версии
Память	512 Мб
Свободное место	100 МБ

Установка

Прежде чем приступать к процессу установки, нужно закрыть все открытые программы. В System Center Endpoint Protection есть компоненты, которые могут конфликтовать с другими установленными программами защиты от вирусов при их наличии. Настоятельно рекомендуется удалить любые другие программы защиты от вирусов, чтобы предотвратить возможные проблемы. Установить System Center Endpoint Protection можно с установочного компакт- или DVD-диска или с помощью файла, загруженного с нашего веб-сайта.

Для запуска мастера установки выполните одно из перечисленных далее действий.

- Если установка выполняется с компакт- или DVD-диска, вставьте его в дисковод, откройте на рабочем столе или в окне Finder и дважды щелкните значок **Установить**.
- Если установка выполняется с помощью загруженного файла, откройте его и дважды щелкните значок **Установить**.



Запустите установочный файл, и мастер установки поможет установить приложение. После принятия лицензионного соглашения и прочтения заявления о конфиденциальности можно выбрать один из указанных ниже типов установки.

- Обычная 4
- Выборочная 4

Обычная установка

В режиме обычной установки используются параметры конфигурации, подходящие для большинства пользователей. Эти параметры обеспечивают максимальную защиту и высокую производительность системы. Обычная установка — это вариант по умолчанию; при отсутствии особых требований не следует выбирать другой способ.

После выбора обычного режима установки настройте **обнаружение потенциально нежелательных приложений**. Потенциально нежелательные приложения не обязательно являются вредоносными, но часто негативно влияют на работу операционной системы. Такие приложения часто поставляются в пакете с другими программами, и их установку бывает трудно заметить при установке всего пакета. Хотя при установке таких приложений обычно на экран выводится уведомление, они вполне могут быть установлены без согласия пользователя.

После установки System Center Endpoint Protection следует выполнить сканирование компьютера на предмет наличия вредоносного кода. В главном окне программы выберите пункт **Сканирование ПК**, а затем — **Сканирование Smart**. Дополнительные сведения о сканировании ПК по требованию см. в разделе Сканирование ПК по требованию 11.

Выборочная установка

Режим выборочной установки предназначен для опытных пользователей, которые хотят изменить дополнительные параметры в ходе установки.

После выбора этого режима будет предложено настроить параметры **прокси-сервера**. Если используется прокси-сервер, можно указать его параметры, установив флажок **Я использую прокси-сервер**. Введите IP-адрес или URL-адрес прокси-сервера в поле **Адрес**. В соответствующем поле укажите порт, по которому прокси-сервер принимает запросы на соединение (по умолчанию 3128). Если прокси-сервер требует аутентификации, введите правильные **имя пользователя** и **пароль**, которые

необходимы для доступа к нему. Если прокси-сервер не используется, установите флажок **Я не использую прокси-сервер**. Если вы не уверены в выборе, можно использовать текущие системные параметры, установив флажок **Системные настройки (рекомендуется)**.

На следующем этапе можно **определить пользователей с правами**, которые смогут изменять конфигурацию программы. Для того чтобы наделить пользователей правами, выберите их в списке в левой части окна и нажмите кнопку **Добавить**. Чтобы отобразить всех системных пользователей, установите флажок **Показывать всех пользователей**.

Следующим этапом установки является настройка **обнаружения потенциально нежелательных приложений**. Потенциально нежелательные приложения не обязательно являются вредоносными, но часто негативно влияют на работу операционной системы. Такие приложения часто поставляются в пакете с другими программами, и их установку бывает трудно заметить при установке всего пакета. Хотя при установке таких приложений обычно на экран выводится уведомление, они вполне могут быть установлены без согласия пользователя.

После установки System Center Endpoint Protection следует выполнить сканирование компьютера на предмет наличия вредоносного кода. В главном окне программы выберите пункт **Сканирование ПК**, а затем — **Сканирование Smart**. Дополнительные сведения о сканировании ПК по требованию см. в разделе Сканирование ПК по требованию 11.

Удаление программы

Удалить System Center Endpoint Protection с компьютера можно одним из описанных ниже способов.

- Вставьте установочный компакт- или DVD-диск с программой System Center Endpoint Protection в дисковод, откройте его на рабочем столе или в окне Finder и дважды щелкните значок **Удалить**.
- Откройте установочный файл System Center Endpoint Protection (*DMG*-файл) и дважды щелкните значок **Удалить**.
- Запустите программу **Finder**, откройте папку **Программы** на жестком диске, нажмите клавишу CTRL и щелкните значок System Center Endpoint Protection, а затем выберите команду **Показать содержимое пакета**. Откройте папку **Contents > Helpers** и дважды щелкните значок **Uninstaller**.

Руководство для начинающих

В этом разделе приводятся общие сведения о программном обеспечении System Center Endpoint Protection и его основных параметрах.

Интерфейс пользователя

Главное окно System Center Endpoint Protection разделено на две основные части. Основное окно справа содержит информацию, относящуюся к параметру, выбранному в главном меню слева.

Ниже описаны пункты главного меню.

- **Состояние защиты**: этот пункт предоставляет информацию о состоянии защиты System Center Endpoint Protection. Если активирован **расширенный режим**, отображается подменю **Статистика**.
- **Сканирование ПК**: этот пункт позволяет настроить и запустить сканирование ПК по требованию.
- **Обновление**: выводит на экран информацию об обновлениях базы данных сигнатур вирусов.
- **Настройка**: этот пункт позволяет настроить уровень безопасности компьютера. Если активирован **расширенный режим**, отображается подменю **Защита от вирусов и шпионских программ**.
- **Служебные программы**: этот пункт предоставляет доступ к **файлам журнала**, **карантину** и **планировщику**. Он отображается только в **расширенном режиме**.
- **Справка**: с помощью этого пункта можно получить информацию о программе и доступ к файлам справки.

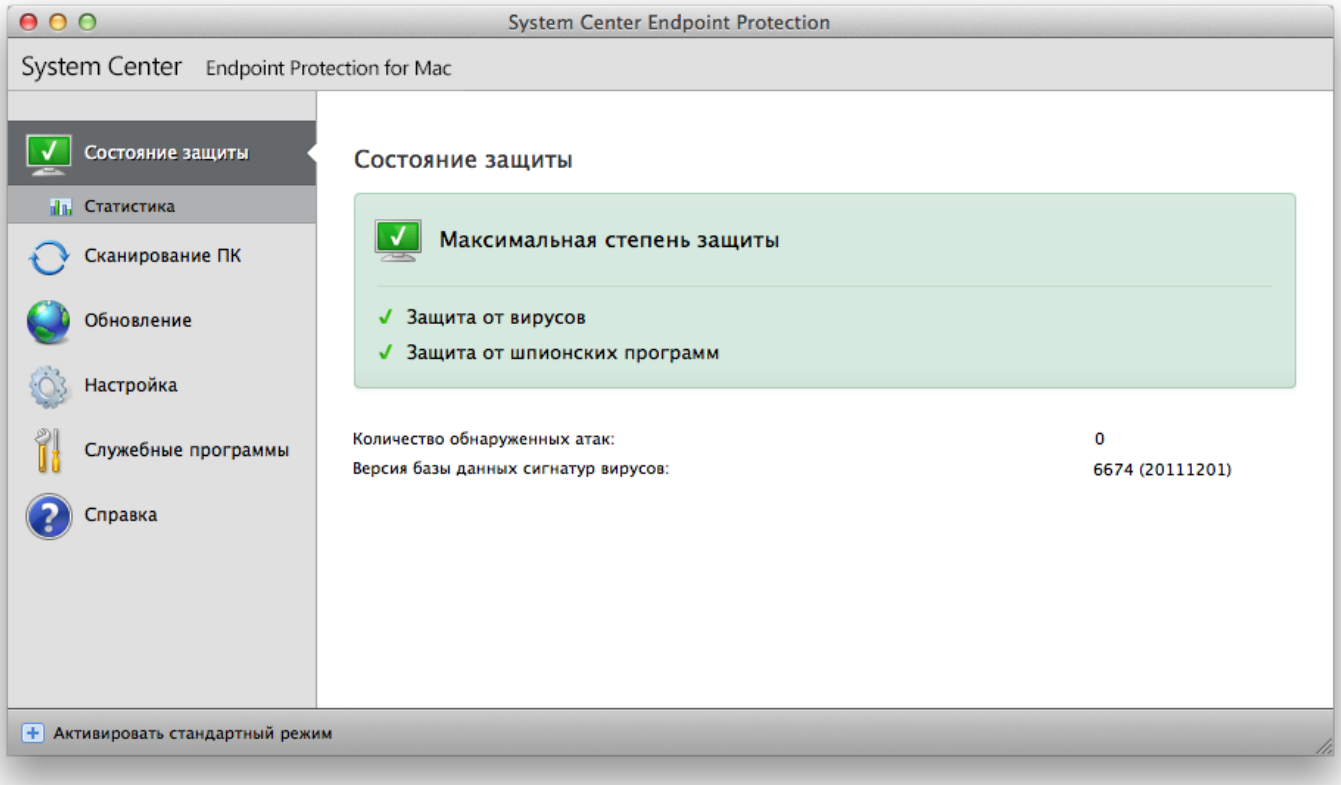
Интерфейс System Center Endpoint Protection позволяет переключаться между стандартным и расширенным режимами. Стандартный режим предоставляет доступ к функциям, необходимым для выполнения обычных операций. Расширенные функции при этом недоступны. Для переключения между режимами используйте значок **+** рядом с пунктом **Активировать расширенный режим** или **Активировать стандартный режим** в левом нижнем углу главного окна программы или нажмите cmd+M.

При переключении в расширенный режим в главном меню появляется пункт **Служебные программы**. Он позволяет воспользоваться подменю **Файлы журнала**, **Карантин** и **Планировщик**.

ПРИМЕЧАНИЕ. Далее в этом руководстве все указания относятся к **расширенному режиму**.

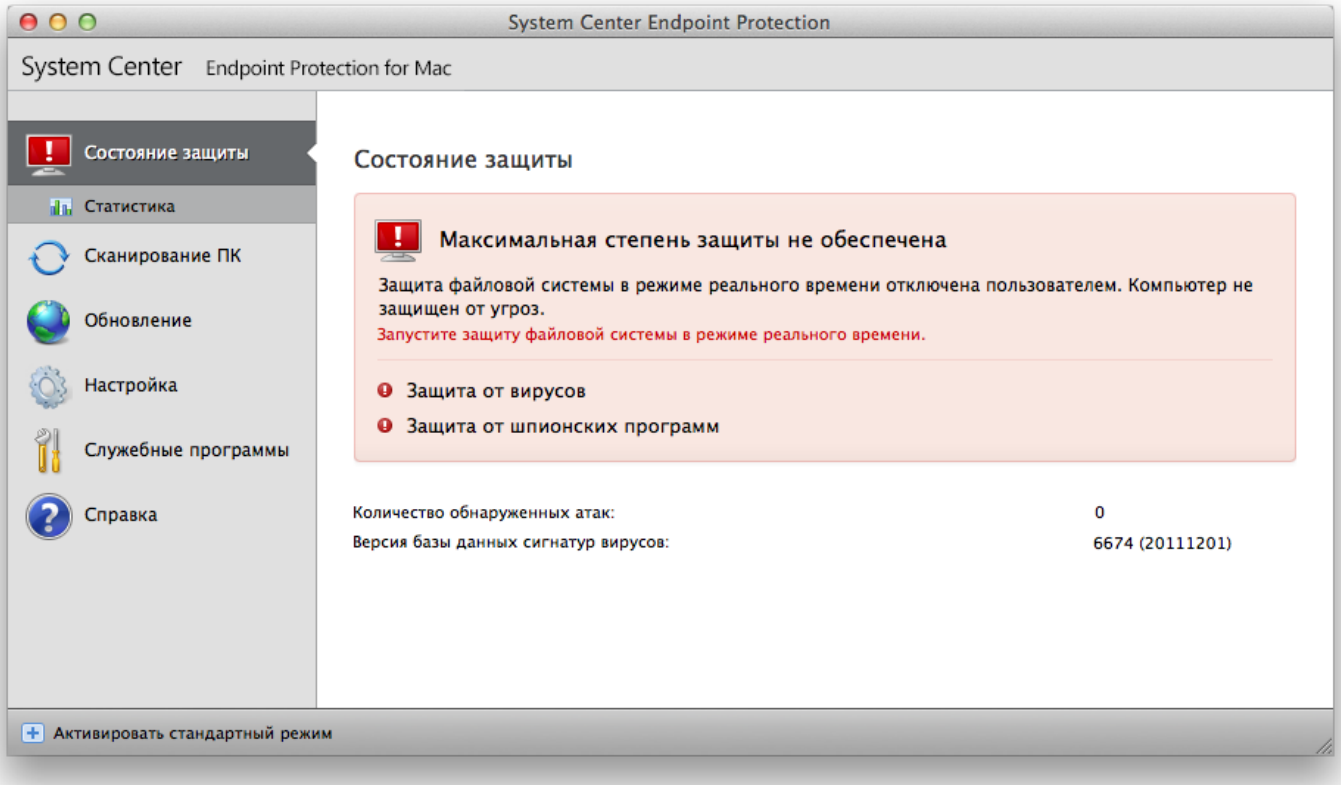
Проверка работоспособности системы

Для того чтобы просмотреть **состояние защиты**, выберите соответствующий пункт в главном меню. В главном окне появится сводная информация о работе System Center Endpoint Protection, а также подменю **статистики**. Откройте это подменю, чтобы просмотреть более подробные сведения и статистическую информацию о сканировании ПК. Окно «Статистика» доступно только в расширенном режиме.



Действия, которые следует выполнить, если программа не работает надлежащим образом

Если включенные модули работают правильно, они обозначаются зеленой галочкой. Если же нет, появляется красный восклицательный знак или оранжевый значок уведомления, а в верхней части окна выводятся дополнительные сведения об этом модуле. Кроме того, предлагается решение проблемы для данного модуля. Для того чтобы изменить состояние отдельного модуля, выберите в главном меню пункт **Настройка** и щелкните мышью нужный модуль.



Работа с System Center Endpoint Protection

Защита от вирусов и шпионских программ

Эта система обеспечивает защиту от вредоносных атак, изменяя файлы, потенциально представляющие угрозу. При обнаружении вредоносного кода модуль защиты от вирусов обезвреживает его, блокируя его выполнение, а затем очищая, удаляя или помещая на карантин.

Защита файловой системы в режиме реального времени

Функция защиты файловой системы в режиме реального времени контролирует все события в системе, относящиеся к защите от вирусов. Все файлы сканируются на наличие злонамеренного кода в момент их открытия, создания или запуска. Защита файловой системы в режиме реального времени запускается при загрузке операционной системы.

Настройка защиты в режиме реального времени

Защита файловой системы в режиме реального времени проверяет все типы носителей и запускает сканирование при различных событиях. Защита файловой системы в режиме реального времени может быть разной для вновь создаваемых и уже существующих файлов. При обработке новых файлов могут быть применены углубленные способы контроля.

По умолчанию защита в режиме реального времени запускается при загрузке системы и обеспечивает постоянное сканирование. В особых случаях (например, при возникновении конфликта с другим модулем сканирования в режиме реального времени) работу защиты в режиме реального времени можно прервать, нажав значок System Center Endpoint Protection, расположенный в строке меню (в верхней части экрана) и выбрав пункт меню **Отключить защиту файловой системы в режиме реального времени**. Также работу защиты в режиме реального времени можно прервать из главного окна программы (**Настройка** > **Защита от вирусов и шпионских программ** > **Отключить**).

Чтобы изменить дополнительные параметры защиты в режиме реального времени, воспользуйтесь пунктами меню **Настройка** > **Ввести настройки приложения...** > **Защита** > **Защита в режиме реального времени** и нажмите кнопку **Настройка...** рядом с пунктом **Расширенные параметры** (описание приведено в разделе Расширенные параметры сканирования 9).

Сканировать при (сканирование при определенных условиях)

По умолчанию все файлы сканируются при **открытии**, **создании** и **выполнении**. Рекомендуется не изменять параметры по умолчанию, поскольку они обеспечивают максимальную защиту компьютера в режиме реального времени.

Расширенные параметры сканирования

В этом окне можно определить типы объектов, которые будут сканироваться модулем сканирования, включить или отключить **расширенную эвристику**, а также изменить параметры для работы с архивами и файловым кэшем.

Изменять значения по умолчанию в разделе **Параметры сканирования архивов по умолчанию** не рекомендуется. Исключениями могут быть те случаи, когда требуется устранить определенную проблему, поскольку увеличение значений по вложенности архивов может снизить производительность системы.

Можно включить или отключить сканирование с применением расширенной эвристики по отдельности для запускаемых, создаваемых или изменяемых файлов, установив флажок **Расширенная эвристика** в соответствующих разделах параметров модуля.

Для того чтобы свести к минимуму влияние на производительность компьютера при использовании защиты в режиме реального времени, можно задать размер кэша оптимизации. Эта функция активна, если установить флажок **Включить очистку файлового кэша**. Если же он снят, все файлы сканируются каждый раз при доступе к ним. Файлы не будут сканироваться повторно после кэширования, если они не были изменены, пока не превышен указанный размер кэша. Файлы сканируются повторно сразу после каждого обновления базы данных сигнатур вирусов.

Для того чтобы включить или отключить эту функцию, используйте флажок **Включить очистку файлового кэша**. Для задания количества кэшируемых файлов введите нужное значение в поле ввода **Размер кэша**.

В окне **Настройка модуля** можно настроить дополнительные параметры сканирования, например можно определить типы **объектов**, которые необходимо сканировать, используемые **параметры** и уровень **очистки**, а также указать **расширения** и **ограничения** размера файлов для защиты в режиме реального времени. Окно настройки модуля можно открыть, нажав кнопку **Настройка** рядом с элементом **Модуль** в окне расширенных параметров. Дополнительные сведения о параметрах модуля см. в разделе Настройка параметров модуля 14.

Исключения из сканирования

В этом разделе можно исключить определенные файлы и папки из сканирования.

- **Путь** — путь к исключаемым файлам и папкам.
- **Угроза**: если рядом с исключаемым файлом указано имя угрозы, файл не сканируется только на предмет этой угрозы, а не в принципе. То есть если файл окажется заражен другой вредоносной программой, модуль защиты от вирусов ее обнаружит.
- **Добавить...**: команда, исключающая объекты из сканирования. Введите путь к объекту (допускается использование подстановочных знаков * и ?) либо выберите файл или папку в древовидной структуре.
- **Изменить...**: команда, позволяющая изменить выделенные записи.
- **Удалить**: команда, удаляющая выделенные записи.
- **По умолчанию**: команда, отменяющая все исключения.

Изменение конфигурации защиты в режиме реального времени

Защита в режиме реального времени является наиболее важным элементом обеспечения безопасности системы. Изменять параметры модуля защиты в режиме реального времени следует с осторожностью. Рекомендуется делать это только в особых случаях, например при возникновении конфликтов с какими-либо приложениями или модулями сканирования в режиме реального времени других программ защиты от вирусов.

После установки System Center Endpoint Protection все параметры оптимизированы для максимальной защиты системы. Чтобы восстановить параметры по умолчанию, нажмите кнопку **По умолчанию** в левом нижнем углу окна **Защита в режиме реального времени** (диалоговое окно **Настройка** > **Ввести настройки приложения...** > **Защита** > **Защита в режиме реального времени**).

Проверка защиты в режиме реального времени

Чтобы убедиться в том, что защита в режиме реального времени работает и обнаруживает вирусы, воспользуйтесь тестовым файлом eicar.com. Это специальный безвредный файл, обнаруживаемый всеми программами защиты от вирусов. Он создан институтом EICAR (Европейский институт антивирусных компьютерных исследований) для тестирования функциональности программ защиты от вирусов.

Чтобы удаленно проверить состояние защиты в режиме реального времени, подключитесь к клиентскому компьютеру с помощью **терминала**, а затем выполните следующую команду:
`/Applications/.scep/Contents/MacOS/scep_daemon --status`

Отобразится следующее состояние модуля сканирования в режиме реального времени: `RTPStatus=Enabled` или `RTPStatus=Disabled`.

При использовании терминала также могут отображаться следующие сведения:

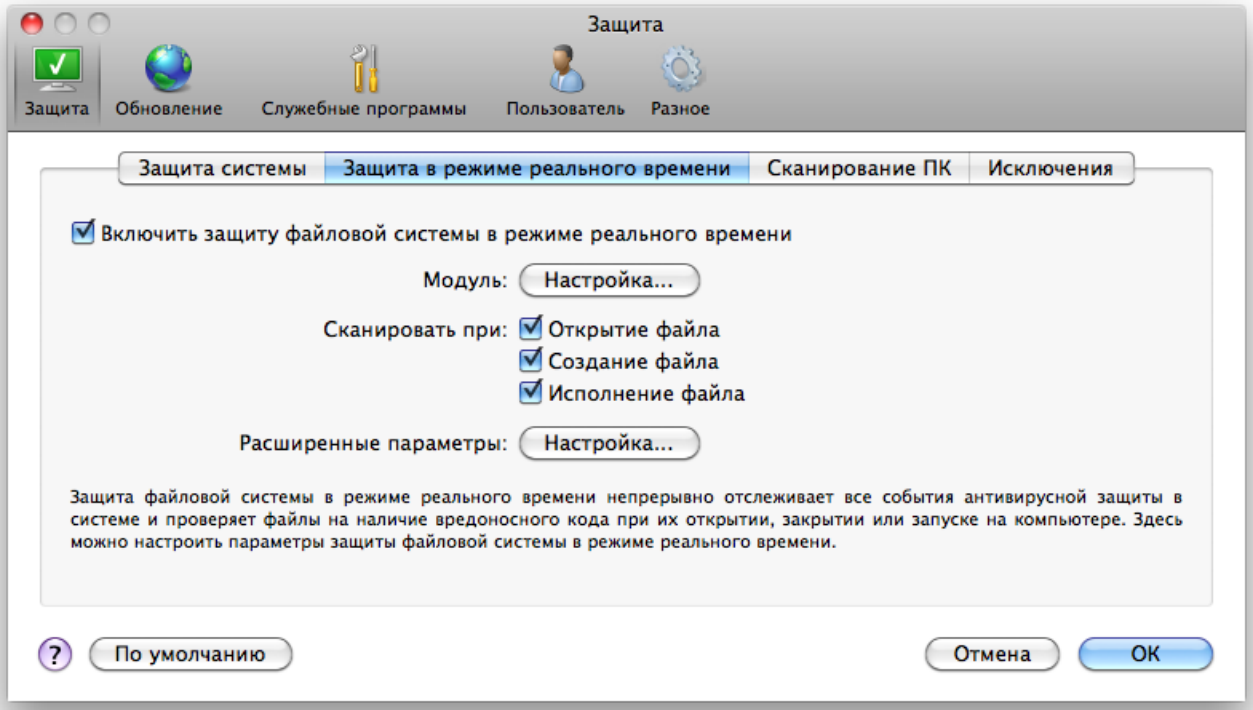
- установленная на клиентском компьютере версия программы System Center Endpoint Protection;
- дата и версия базы данных сигнатур вирусов;
- путь к серверу обновлений.

ПРИМЕЧАНИЕ. Использование терминала рекомендовано только для опытных пользователей.

Действия, которые следует выполнить, если модуль защиты в режиме реального времени не работает

В этом разделе описаны проблемы, которые могут возникнуть при защите в режиме реального времени, и способы их устранения.

Защита в режиме реального времени отключена
Если защита в режиме реального времени была случайно отключена пользователем, ее нужно включить. Для того чтобы повторно активировать защиту в режиме реального времени, перейдите на страницу **Настройка** > **Защита от вирусов и шпионских программ** и щелкните ссылку **Включить защиту в режиме реального времени** справа в главном окне приложения. Либо защиту файловой системы в режиме реального времени можно включить в диалоговом окне расширенных параметров в разделе **Защита** > **Защита в режиме реального времени**, установив флажок **Включить защиту файловой системы в режиме реального времени**.



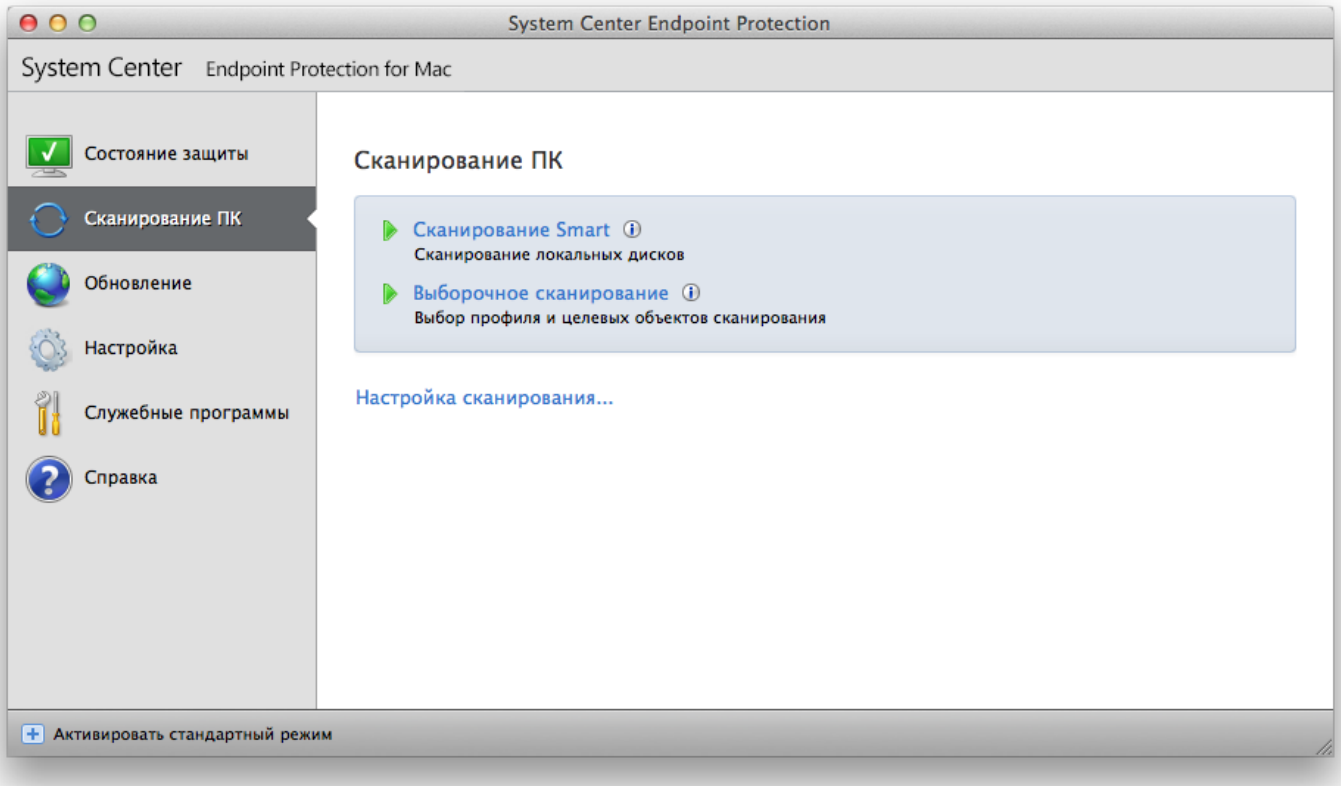
Функция защиты в режиме реального времени не обнаруживает и не очищает заражения
Убедитесь, что на компьютере не установлены другие программы защиты от вирусов. При одновременной работе двух систем защиты в режиме реального времени могут возникать конфликты. Рекомендуется удалить все другие программы защиты от вирусов.

Защита в режиме реального времени не запускается
Если защита в режиме реального времени не инициализируется при запуске системы, это может быть вызвано конфликтом с другими программами. В этом случае обратитесь за консультацией к специалистам службы поддержки клиентов.

Сканирование ПК по требованию

При обнаружении симптомов возможного заражения компьютера (необычное поведение и т. п.) запустите сканирование ПК, воспользовавшись командами **Сканирование ПК** > **Сканирование Smart**. Для обеспечения максимальной защиты сканирование ПК следует выполнять регулярно, а не только при подозрении на заражение. Регулярное сканирование позволяет обнаружить заражения, не обнаруженные модулем сканирования в режиме реального времени при их записи на диск. Это может произойти, если в момент заражения модуль сканирования в режиме реального времени был отключен или использовалась устаревшая база данных сигнатур вирусов.

Рекомендуется запускать сканирование ПК по требованию хотя бы раз в месяц. Можно сконфигурировать сканирование в качестве запланированной задачи в разделе **Служебные программы** > **Планировщик**.



Также можно перетаскивать выделенные файлы и папки с рабочего стола или из окна Finder на основной экран System Center Endpoint Protection, значок Dock, значок в строке меню (в верхней части экрана) или значок приложения (в папке */Applications*).

Тип сканирования

Доступны два типа сканирования ПК по требованию. **Сканирование Smart** позволяет быстро просканировать систему без настройки каких-либо параметров. Тип **Выборочное сканирование** позволяет выбрать предопределенный профиль сканирования, а также указать конкретные объекты.

Сканирование Smart

Сканирование Smart позволяет быстро запустить сканирование ПК и очистить зараженные файлы без вмешательства пользователя. Главным преимуществом этого метода является простота использования без детальной настройки параметров сканирования. Функция сканирования Smart проверяет все файлы во всех папках и автоматически очищает или удаляет обнаруженные заражения. При этом автоматически используется уровень очистки по умолчанию. Дополнительные сведения о типах очистки см. в разделе Очистка 15.

Выборочное сканирование

Выборочное сканирование является оптимальным решением в том случае, если нужно указать параметры сканирования (например, объекты и методы сканирования). Преимуществом такого сканирования является возможность детальной настройки параметров. Различные конфигурации можно сохранить в виде пользовательских профилей сканирования, которые полезны, если сканирование с одинаковыми параметрами выполняется регулярно.

Чтобы указать объекты сканирования, выберите пункт **Сканирование ПК** > **Выборочное сканирование** и выделите нужные **объекты сканирования** в древовидной структуре. Объекты сканирования также можно задать более точно, указав пути к папкам и файлам, которые нужно сканировать. Если нужно только выполнить сканирование системы без выполнения дополнительных действий по очистке, установите флажок **Сканировать без очистки**. Кроме того, можно выбрать один из трех уровней очистки в разделе **Настройка...** > **Очистка**.

Пользователям, не имеющим достаточного опыта работы с антивирусными программами, не рекомендуется выполнять выборочное сканирование.

Объекты сканирования

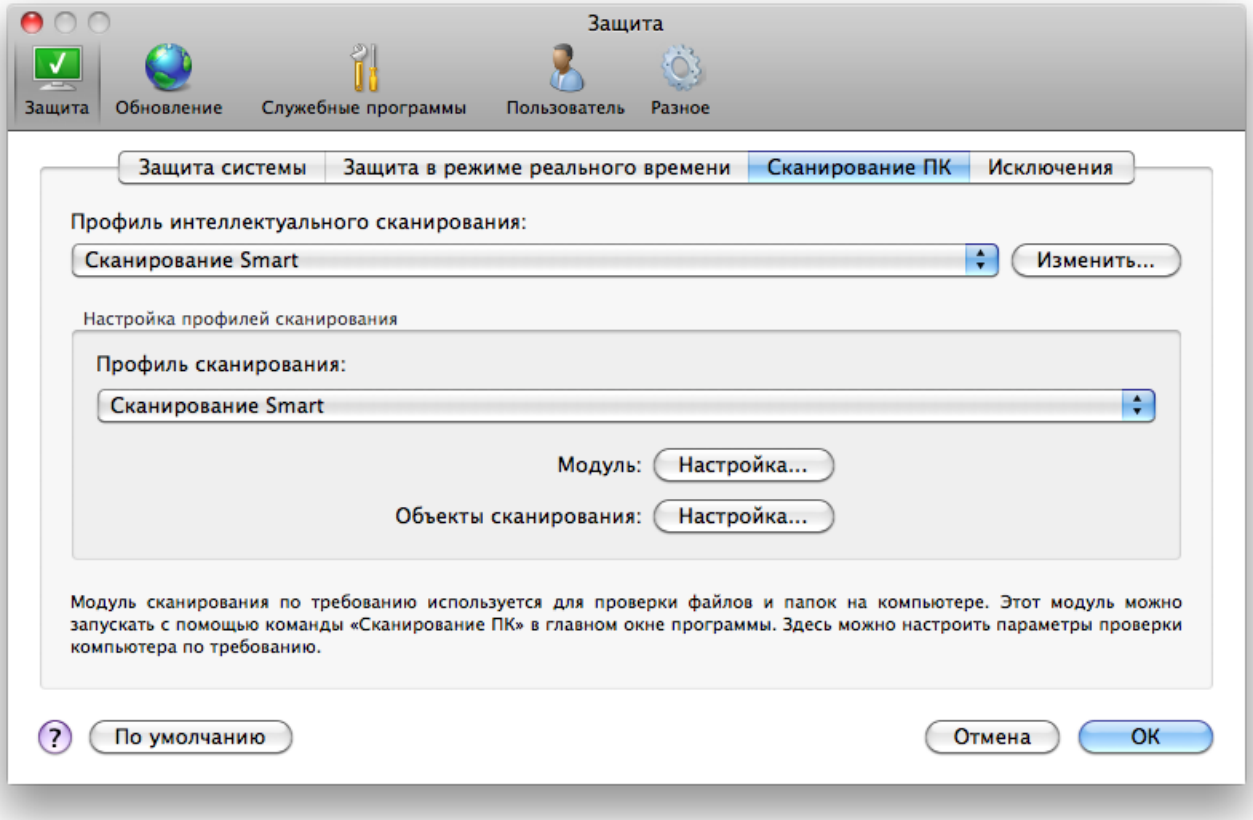
Древовидная структура объектов сканирования позволяет выбрать файлы и папки, которые необходимо просканировать на наличие вирусов. Выбор папок может также осуществляться в соответствии с параметрами профиля.

Объекты сканирования можно определить более точно, введя путь к папкам или файлам, подлежащим сканированию. Выберите объекты сканирования в древовидной структуре, содержащей все доступные на компьютере папки.

Профили сканирования

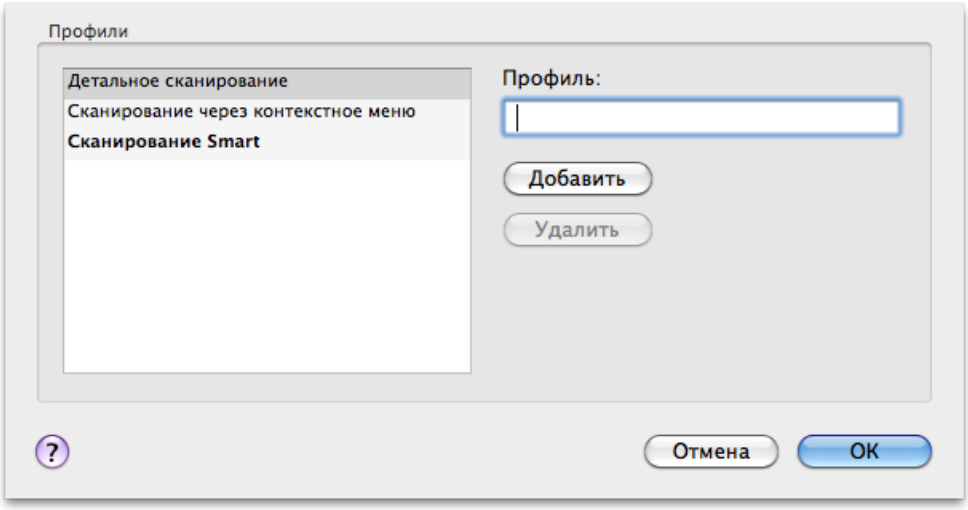
Предпочтительные настройки сканирования можно сохранить для использования в будущем. Рекомендуется создать отдельный профиль для каждого регулярно используемого сканирования (с различными объектами, методами сканирования и прочими параметрами).

Чтобы создать профиль, выберите пункт **Настройка** > **Ввести настройки приложения...** > **Защита** > **Сканирование компьютера** и выберите команду **Изменить** рядом со списком существующих профилей.



Информацию о создании профиля, соответствующего конкретным требованиям, и описание каждого параметра сканирования см. в разделе Настройка параметров модуля 14.

Пример. Предположим, пользователю требуется создать собственный профиль сканирования, причем конфигурация сканирования Smart частично устраивает его, однако ему не требуется сканировать упаковщики и потенциально опасные приложения, а также нужно применить тщательную очистку. В диалоговом окне **Список профилей модуля сканирования по требованию** введите имя профиля и нажмите кнопку **Добавить**, а затем — **ОК**. После этого задайте нужные параметры, настроив **модуль** и указав **объекты сканирования**.



Настройка параметров модуля

Технология сканирования, используемая в System Center Endpoint Protection, является упреждающей, т. е. она защищает от новой угрозы уже в первые часы ее распространения. При этом используется сочетание нескольких методов (анализ кода, моделирование кода, обобщенные сигнатуры, сигнатуры вирусов), которые совместно в значительной степени повышают уровень безопасности компьютера. Модуль сканирования способен контролировать несколько потоков данных одновременно, за счет чего увеличивается эффективность обнаружения. Также эта технология эффективно предотвращает проникновение руткитов.

Параметры настройки технологии позволяют указать несколько параметров сканирования:
- типы и расширения файлов, подлежащих сканированию;
- сочетание различных методов обнаружения;
- уровни очистки и т. д.

Для того чтобы открыть окно настройки, выберите пункт **Настройка** > **Защита от вирусов и шпионских программ** > **Расширенная настройка параметров защиты от вирусов и шпионских программ** и нажмите кнопку **Настройка...** в разделах **Защита системы**, **Защита в режиме реального времени** и **Сканирование ПК**. Разные сценарии обеспечения безопасности требуют различных настроек, поэтому параметры модуля можно настроить отдельно для каждого из следующих модулей защиты:
- **Защита системы** > Автоматическая проверка файлов, исполняемых при запуске системы;
- **Защита в режиме реального времени** > Защита в режиме реального времени;
- **Сканирование ПК** > Сканирование ПК по требованию.

Параметры модуля оптимизированы для каждого из модулей, и их изменение может существенно повлиять на работу системы. Например, если настроить параметры таким образом, чтобы упаковщики проверялись всегда или модуль защиты в режиме реального времени использовал расширенную эвристику, это может замедлить работу системы. В связи с этим рекомендуется воздерживаться от изменения параметров по умолчанию для всех модулей, кроме модуля «Сканирование ПК».

Объекты

В разделе **Объекты** можно указать файлы, которые необходимо проверить на предмет заражения.

- **Файлы**: сканируются файлы всех часто используемых типов (программы, изображения, звуковые и видеофайлы, файлы баз данных и т. д.).
- **Символические ссылки**: сканируются файлы особого типа, содержащие текстовую строку, которая интерпретируется и используется операционной системой как путь к другому файлу или каталогу (только для модуля сканирования по требованию).
- **Почтовые файлы**: сканируются особые файлы, содержащие сообщения электронной почты (недоступно для модуля защиты в режиме реального времени).
- **Почтовые ящики**: сканируются почтовые ящики пользователя в системе (недоступно для защиты в режиме реального времени). Неправильное использование этого параметра может привести к конфликту с почтовым клиентом.
- **Архивы**: сканируются сжатые файлы в архивах .rar, .zip, .arj, .tar и т. д. (недоступно для защиты в режиме реального времени).
- **Самораспаковывающиеся архивы**: сканируются файлы, содержащиеся в самораспаковывающихся архивах (недоступно для защиты в режиме реального времени).
- **Упаковщики**: сканируются программы-упаковщики, которые в отличие от стандартных архивов распаковывают файлы динамически в системную память, и стандартные статические упаковщики (UPX, yoda, ASPack, FGS и т. д.).

Параметры

В разделе **Параметры** можно выбрать методы, которые будут использоваться при сканировании системы на предмет заражения. Доступны указанные ниже варианты.

- **Эвристический анализ**: при эвристическом анализе используется алгоритм, который анализируют активность программ на предмет вредоносных действий. Основным преимуществом обнаружения путем эвристического анализа является возможность обнаруживать новые вредоносные программы, сведения о которых еще не попали в список известных вирусов (базу данных сигнатур вирусов).
- **Расширенная эвристика**: этот метод основан на уникальном эвристическом алгоритме, оптимизированном для обнаружения компьютерных червей и троянских программ, написанных на языках программирования высокого уровня. Применение расширенной эвристики существенно улучшает возможности обнаружения вредоносных программ.
- **Потенциально нежелательные приложения**: такие приложения не обязательно являются вредоносными, но могут тем или иным образом снижать производительность системы. Такие приложения обычно запрашивают при установке согласие пользователя. После их установки работа системы изменяется. Наиболее заметны такие изменения, как появление нежелательных всплывающих окон, запуск скрытых процессов, увеличение степени использования системных ресурсов, изменение результатов поисковых запросов и обмен данными с удаленными серверами.
- **Потенциально опасные приложения**: в эту категорию входит коммерческое законное программное обеспечение, которым могут воспользоваться злоумышленники, если такие приложения были установлены без ведома пользователя. Это в том числе средства удаленного доступа. По умолчанию этот параметр отключен.

Очистка

Параметры очистки определяют способ очистки зараженных файлов модулем сканирования. Предусмотрено три описанных далее уровня очистки.

- **Без очистки**: зараженные файлы не очищаются автоматически. Программа выводит на экран предупреждение и предлагает пользователю выбрать нужное действие.
- **Стандартная очистка**: программа пытается автоматически очистить или удалить зараженный файл. Если невозможно автоматически выбрать правильное действие, пользователю предлагается сделать выбор. Выбор предоставляется и в том случае, если предопределенное действие не может быть выполнено.
- **Тщательная очистка**: программа очищает или удаляет все зараженные файлы (в том числе архивы). Единственное исключение — системные файлы. Если файлы невозможно очистить, на экран выводится предупреждение с предложением выбрать действие.

Предупреждение. В стандартном режиме очистки, который используется по умолчанию, архив удаляется целиком только в том случае, если все файлы в нем заражены. Если в архиве есть нормальные файлы, он не удаляется. Если зараженный архив обнаруживается в режиме тщательной очистки, он удаляется целиком, даже если в нем есть незараженные файлы.

Расширения

Расширением называется часть имени файла, отделенная от основной части точкой. Расширение определяет тип файла или его содержимого. Этот раздел параметров модуля позволяет определить типы файлов, которые не нужно сканировать.

По умолчанию сканируются все файлы независимо от их расширения. Любое расширение можно добавить в список исключений из сканирования. С помощью кнопок **Добавить** и **Удалить** можно включать и запрещать сканирование для тех или иных расширений.

Иногда может быть необходимо исключить файлы из сканирования, если сканирование определенных типов файлов препятствует нормальной работе программы. Например, иногда целесообразно исключить из сканирования файлы с расширениями *.log*, *.cfg* и *.tmp*.

Ограничения

В разделе **Ограничения** можно указать максимальный размер объектов и количество уровней вложенности для сканирования архивов.

- **Максимальный размер:** определяет максимальный размер сканируемых объектов. После установки этого ограничения модуль защиты от вирусов будет проверять только объекты меньше указанного размера. Не рекомендуется изменять значение по умолчанию, так как обычно это не нужно. Этот параметр предназначен для опытных пользователей, которым необходимо исключить большие объекты из сканирования.
- **Максимальное время сканирования:** определяет максимальное время сканирования объекта. Если пользователь определил это значение, модуль защиты от вирусов прерывает сканирование текущего объекта по истечении указанного времени независимо от того, завершено ли оно.
- **Максимальный уровень вложенности:** определяет максимальную глубину сканирования архивов. Не рекомендуется изменять значение по умолчанию, равное 10; в обычных условиях для этого нет особой причины. Если сканирование преждевременно прерывается из-за превышения уровня вложенности, архив остается непроверенным.

- **Максимальный размер файла:** позволяет задать максимальный размер файлов в архиве (после извлечения), подлежащих сканированию. Если из-за этого ограничения сканирование прерывается до его завершения, архив остается непроверенным.

Другие

При включенном параметре «Оптимизация Smart» используются оптимальные настройки для обеспечения самого эффективного уровня сканирования с сохранением его высокой скорости. Разные модули защиты выполняют интеллектуальное сканирование, применяя различные методы для конкретных типов файлов. Оптимизация Smart не определена в продукте жестким образом. Коллектив разработчиков нашей компании постоянно вносит в нее изменения, которые можно интегрировать в System Center Endpoint Protection с помощью регулярных обновлений. Если оптимизация Smart отключена, при сканировании используются только пользовательские настройки ядра каждого модуля.

Сканировать альтернативные потоки данных: применимо только к модулю сканирования по требованию.
Альтернативные потоки данных (ветвление ресурсов или данных), используемые файловой системой, представляют собой связи между файлами и папками, которые не видны для обычных методов сканирования. Многие вредоносные программы выдают себя за альтернативные потоки данных, чтобы не быть обнаруженными.

Действия при обнаружении заражения

Заражение может произойти из разных источников: с веб-страниц, из общих папок, по электронной почте или со съемных носителей (USB-накопителей, внешних дисков, компакт- или DVD-дисков, дискет и т. п.).

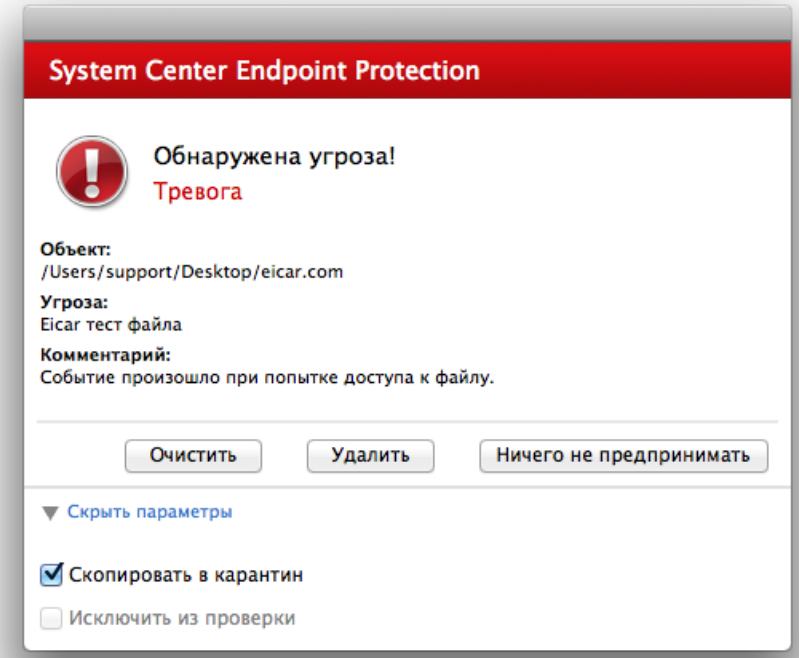
Если наблюдаются признаки заражения компьютера (например, он стал медленнее работать, часто «зависает» и т. п.), рекомендуется выполнить действия, описанные ниже.

1. Откройте System Center Endpoint Protection и выберите команду **Сканирование ПК**.
2. Выберите параметр **Сканирование Smart** (дополнительную информацию см. в разделе Сканирование Smart 12).
3. По завершении сканирования просмотрите в журнале количество проверенных, зараженных и очищенных файлов.

Если следует сканировать только определенную часть диска, выберите вариант **Выборочное сканирование** и укажите объекты, которые нужно сканировать на предмет наличия вирусов.

Ниже описано, что происходит, когда система System Center Endpoint Protection выявляет заражение. Предположим, что заражение обнаружено модулем защиты файловой системы в режиме реального времени при уровне очистки по умолчанию. Сначала модуль пытается очистить или удалить файл. Если действие по умолчанию для модуля защиты в режиме реального времени не определено, его предлагается выбрать пользователю. Обычно можно выбрать действие **Очистить**, **Удалить** или **Ничего не предпринимать**. Действие **Ничего не предпринимать** выбирать не рекомендуется, так как в этом случае зараженный файл останется на компьютере. Исключением может быть ситуация, когда имеется полная уверенность в том, что файл безвреден и попал под подозрение по ошибке.

«Очистка и удаление»: используйте очистку, если файл был атакован вирусом, добавившим в него вредоносный код. В этом случае в первую очередь следует попытаться очистить файл, чтобы восстановить его первоначальное состояние. Если файл содержит только вредоносный код, его следует удалить.



Удаление файлов из архивов. В режиме очистки по умолчанию архив удаляется целиком, если он содержит только зараженные файлы. Иначе говоря, архивы, в которых есть незараженные файлы, не удаляются. Однако сканирование в режиме **Тщательная очистка** следует применять с осторожностью: в этом режиме архив удаляется, если содержит хотя бы один зараженный файл, независимо от состояния других файлов в архиве.

Обновление программы

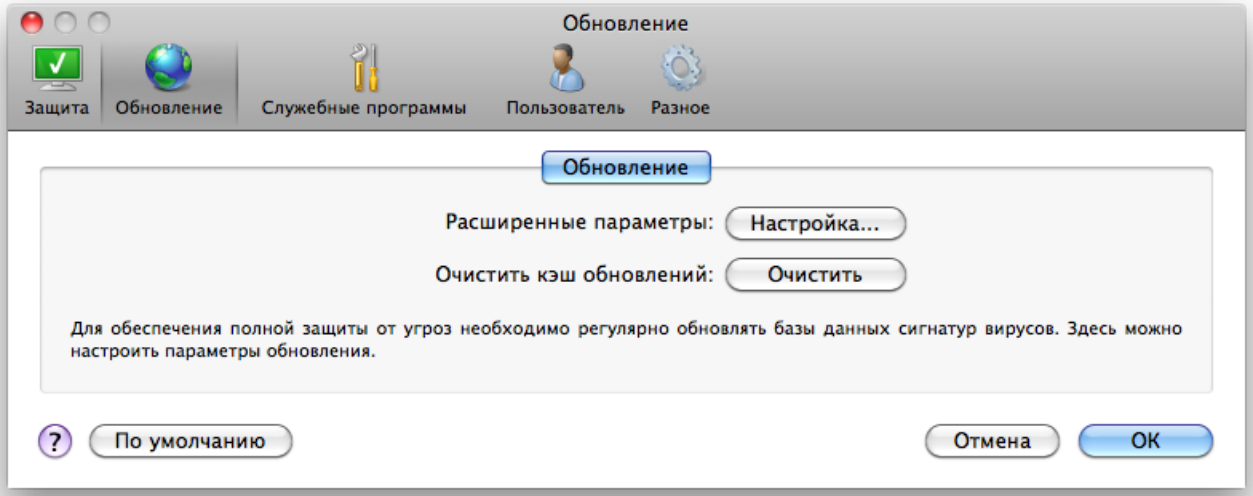
Для обеспечения максимального уровня безопасности необходимо регулярно обновлять System Center Endpoint Protection. Модуль обновления поддерживает актуальное состояние программы, загружая самую последнюю версию базы данных сигнатур вирусов.

Выбрав пункт **Обновление** в главном меню, можно получить информацию о текущем состоянии обновления, в том числе дату и время последнего успешно выполненного обновления, а также сведения о необходимости обновления. Чтобы вручную запустить процесс обновления, нажмите **Обновить базу данных сигнатур вирусов**.

Обычно после корректного завершения загрузки в окне обновления выводится сообщение *Обновление не обязательно: установленная база данных сигнатур вирусов актуальна*.

В окне обновления также выводятся сведения о версии базы данных сигнатур вирусов. Этот числовой индикатор представляет собой активную ссылку на список всех сигнатур, добавленных в базу данных в текущем обновлении.

Настройка обновления



Для того чтобы включить тестовый режим (для загрузки тестовых обновлений), нажмите кнопку **Настройка** рядом с пунктом **Расширенные параметры** и установите флажок **Включить тестовые обновления**. Для отключения отображения уведомлений на панели задач после каждого успешно выполненного обновления установите флажок **Не отображать уведомление об успешном обновлении**.

Чтобы удалить временные данные обновлений, нажмите кнопку **Очистить** рядом с пунктом **Очистить кэш обновлений**. Используйте эту функцию при возникновении проблем в ходе обновления.

Создание задач обновления

Обновление можно запустить вручную с помощью функции **Обновить базу данных сигнатур вирусов** в основном окне, которое выводится на экран после выбора пункта **Обновление** в главном меню.

Обновления также можно выполнять как запланированную задачу. Для конфигурирования запланированной задачи перейдите в раздел **Служебные программы** > **Планировщик**. По умолчанию в System Center Endpoint Protection активированы указанные ниже задачи.

- **Регулярное автоматическое обновление**
- **Автоматическое обновление после входа пользователя в систему**

Каждую из задач обновления можно изменить в соответствии с конкретными требованиями. Кроме задач по умолчанию можно создать другие задачи обновления с пользовательскими настройками. Дополнительные сведения о создании и настройке задач обновления см. в разделе Планировщик 19.

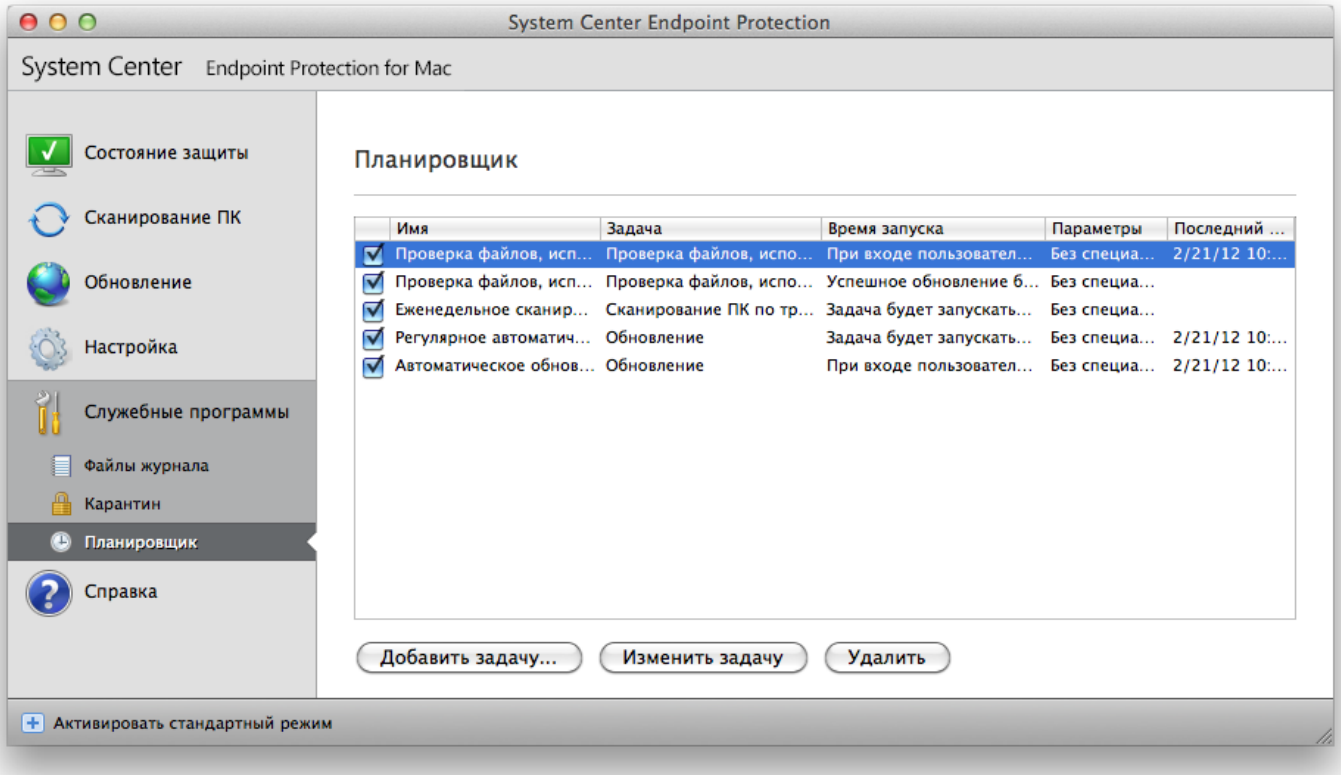
Обновление до новой сборки

Для обеспечения максимальной защиты важно использовать новейшую сборку System Center Endpoint Protection. Для того чтобы проверить наличие новой версии, выберите пункт **Обновление** в главном меню в левой части окна. Если доступна новая сборка, в нижней части окна будет выведено сообщение *Дост упна новая версия эт ой программы!*. Нажмите **Подробнее...**, чтобы вывести на экран новое окно с информацией о номере версии доступной сборки и перечнем изменений.

Нажмите кнопку **Загрузить**, чтобы загрузить новейшую сборку. Нажмите кнопку **Закрыть**, чтобы закрыть это окно и загрузить обновление позднее.

Планировщик

Планировщик доступен, если в System Center Endpoint Protection активирован расширенный режим. Перейти к планировщику можно через главное меню System Center Endpoint Protection, воспользовавшись пунктом **Служебные программы**. **Планировщик** содержит полный список всех запланированных задач и их параметры запуска (дату, время и используемый профиль сканирования).



По умолчанию в планировщике отображаются следующие запланированные задачи:

- Регулярное автоматическое обновление
- Автоматическое обновление после входа пользователя в систему
- Проверка файлов при входе пользователя
- Проверка файлов после обновления базы данных сигнатур вирусов
- Обслуживание журнала (после установки флажка **Показывать системные задачи** при настройке планировщика)
- Еженедельное сканирование

Чтобы изменить конфигурацию имеющейся запланированной задачи (как задачи по умолчанию, так и пользовательской), щелкните ее, удерживая нажатой клавишу CTRL, и выберите в контекстном меню команду **Изменить...** или выделите задачу и нажмите кнопку **Изменить задачу**.

Цель планирования задач

Планировщик управляет запланированными задачами и запускает их по расписанию с предопределенными параметрами. Параметры и свойства задач содержат такую информацию, как дата и время выполнения задачи, а также используемые при этом профили.

Создание новых задач

Для того чтобы создать задачу в планировщике, нажмите кнопку **Добавить задачу...** или щелкните в пустом поле, удерживая клавишу CTRL, и выберите в контекстном меню команду **Добавить...**. Доступны пять типов запланированных задач. Они указаны ниже.

- **Запустить приложение**
- **Обновление**
- **Обслуживание журнала**
- **Сканирование ПК по требованию**
- **Проверка файлов, исполняемых при запуске системы**

Поскольку обновление — одна из самых часто используемых запланированных задач, ниже приведены сведения о том, как добавить новую задачу обновления.

В раскрывающемся меню **Запланированная задача** выберите пункт **Обновление**. Введите имя задачи в поле **Название задачи**. Укажите частоту выполнения задачи в раскрывающемся меню **Выполнить задачу**. Доступны указанные ниже варианты. **Определяется пользователем**, **Однократно**, **Регулярно**, **Ежедневно**, **Еженедельно** и **При наступлении события**. В зависимости от указанной частоты запуска будут запрошены различные параметры обновления.

Если выбран вариант **Определяется пользователем**, будет предложено указать дату и время в формате cron (дополнительные сведения см. в разделе Создание пользовательской задачи 20).

Затем укажите, какое действие следует предпринимать, если задача не может быть выполнена в установленное время. Доступны следующие три варианта.

- **Ждать до следующего запланированного момента**
- **Выполнить задачу как можно скорее**
- **Выполнить задачу немедленно, если время, прошедшее с последнего запуска, превысило указанный интервал** (интервал можно указать с помощью параметра **Минимальный интервал между задачами**)

После этого появится окно со сводной информацией о текущей запланированной задаче. Нажмите кнопку **Готово**.

Новая задача появится в списке запланированных.

По умолчанию система включает запланированные задачи, которые обеспечивают правильную работу приложения. Изменить эти задачи нельзя, и по умолчанию они скрыты. Для того чтобы сделать эти задачи видимыми, выберите по очереди пункты **Настройка** > **Ввести настройки приложения...** > **Служебные программы** > **Планировщик** и установите флажок **Показывать системные задачи**.

Создание пользовательской задачи

Дату и время **пользовательской** задачи необходимо указывать в формате cron с расширенным значением года (строка из шести полей, разделенных пробелами):

```
минута (0-59) час (0-23) число месяца (1-31) месяц(1-12) год (1970-2099) день недели (0-7, воскресенье — 0 ил
```

Пример.

```
30 6 22 3 2012 4
```

Специальные символы, которые поддерживаются в выражениях cron, указаны ниже.

- Звездочка (`*`) — выражение соответствует всем значениям поля, например звездочка в третьем поле (число месяца) означает любое число
- Дефис (`-`) — задает диапазон, например `3-9`
- Запятая (`,`) — разделяет элементы списка, например `1,3,7,8`
- Косая черта (`/`) — задает шаг диапазона, например `3-28/5` в третьем поле (число месяца) означает третье число любого месяца, а также другие числа с шагом пять дней.

Названия дней (понедельник — воскресенье) и месяцев (январь — декабрь) не поддерживаются.

ПРИМЕЧАНИЕ. Если заданы число месяца и день недели, команда выполняется только в случае совпадения значений по обоим полям.

Карантин

Карантин предназначен в первую очередь для безопасного хранения зараженных файлов. Файлы следует помещать на карантин, если они не могут быть очищены или безопасно удалены, если удалять их не рекомендуется или если они ошибочно отнесены программой System Center Endpoint Protection к зараженным.

Поместить на карантин можно любой файл. Рекомендуется помещать на карантин файлы с подозрительной активностью, которые, тем не менее, не определяются модулем сканирования как зараженные.

Информацию о файлах, помещенных на карантин, можно просмотреть в виде таблицы, содержащей дату и время помещения зараженного файла на карантин, путь к его исходному расположению, его размер в байтах, причину помещения файла на карантин (например, мнение пользователя) и количество обнаруженных угроз (например, если архив содержит несколько заражений). Папка карантина с помещенными в нее файлами (*/Library/Application Support/Microsoft/scep/cache/quarantine*) остается на компьютере даже после удаления System Center Endpoint Protection. Файлы на карантине хранятся в безопасном зашифрованном виде. Их можно восстановить после повторной установки приложения System Center Endpoint Protection.

Помещение файлов на карантин

Программа System Center Endpoint Protection автоматически помещает удаленные файлы на карантин (если эта функция не была отключена пользователем в окне предупреждения). При желании любой подозрительный файл можно поместить на карантин вручную с помощью кнопки **Карантин...**. Для этого также можно использовать контекстное меню. Нажмите клавишу CTRL, щелкните мышью в пустом поле, выберите **Карантин**, выделите файл, который нужно поместить на карантин, и нажмите кнопку **Открыть**.

Восстановление из карантина

Файлы, находящиеся на карантине, можно восстановить в исходном месте. Для этого используется кнопка **Восстановить**. Функция восстановления также доступна в контекстном меню. Для ее использования нужно нажать клавишу CTRL, нажать нужный файл в окне **Карантин**, а затем выбрать пункт **Восстановить**. Контекстное меню содержит также функцию **Восстановить в...**, которая позволяет восстановить файл в месте, отличном от исходного.

Файлы журнала

Файлы журнала содержат информацию о важных программных событиях и предоставляют сводные сведения об обнаруженных угрозах. Ведение журнала является важнейшим элементом анализа, обнаружения угроз и устранения проблем. Оно выполняется в фоновом режиме без вмешательства пользователя. Данные сохраняются в соответствии с текущими параметрами степени детализации журнала. Просматривать текстовые сообщения и файлы журнала, а также архивировать их можно непосредственно в среде System Center Endpoint Protection.

Получить доступ к файлам журнала можно из главного окна System Center Endpoint Protection с помощью команды **Служебные программы** > **Файлы журнала**. Выберите нужный тип журнала в раскрывающемся меню **Журнал** в верхней части окна. Доступны следующие журналы:

1. **Обнаруженные угрозы**: позволяет просмотреть все данные о событиях, имеющих отношение к обнаружению заражений.
2. **События**: этот журнал упрощает устранение проблем. В нем регистрируются все важные действия, выполняемые System Center Endpoint Protection.
3. **Сканирование ПК**: в этом окне отображаются результаты всех выполненных операций сканирования. Чтобы получить подробную информацию о той или иной операции сканирования ПК по требованию, дважды щелкните соответствующую запись.

Для того чтобы скопировать в буфер обмена информацию из любого раздела журнала, выделите необходимую запись и нажмите кнопку **Копировать**.

Обслуживание журнала

Конфигурация журнала System Center Endpoint Protection доступна из главного окна программы. Нажмите **Настройка** > **Ввести настройки приложения...** > **Служебные программы** > **Файлы журнала**. Для файлов журнала можно задать параметры, указанные ниже.

- **Автоматически удалять устаревшие записи журнала**: записи в журнале старше указанного времени (в днях) будут автоматически удаляться.
- **Оптимизировать файлы журналов автоматически**: включает автоматическую дефрагментацию файлов журналов при достижении указанной процентной доли неиспользуемых записей.

Всю важную информацию, отображаемую в окнах программы, сообщениях об угрозах и событиях, можно сохранять в понятных для человека текстовых форматах, например в формате обычного текста или CSV (данные с разделителями-запятыми). Если необходимо сделать эти файлы доступными для обработки в сторонних приложениях, установите флажок **Включить запись журналов в текстовые файлы**.

Чтобы указать целевую папку для сохранения файлов журнала, нажмите кнопку **Настройка...** рядом с элементом **Расширенная настройка**.

В зависимости от настроек в разделе **Текстовые файлы журнала: изменение** можно сохранять журналы с записью следующих данных.

- Угрозы, обнаруженные с помощью модулей сканирования при запуске системы, защиты в режиме реального времени и сканирования компьютера, сохраняются в файле с именем threatslog.txt.
- Такие события, как *Неверное имя пользоват еля и пароль*, *Не удает ся обновит ь базу данных сигнат ур вирусов* и т. д., записываются в файл eventslog.txt.
- Результаты всех выполненных сканирований сохраняются в формате scanlog.HOMEP.txt.

Чтобы настроить фильтры для **записей журнала сканирования компьютера по умолчанию**, нажмите кнопку **Изменить...** рядом с этим параметром и выберите нужные типы журналов. Дополнительные сведения об этих типах журнала приведены в этой главе 22.

Фильтрация журнала

В журналах хранится информация о важных системных событиях. Функция фильтрации журнала позволяет отобразить записи о событиях определенного типа.

Ниже указаны типы журналов, используемые чаще всего.

- **Критические предупреждения**: в эти журналы записываются критические системные ошибки (например, сбой запуска защиты от вирусов).
- **Ошибки**: в эти журналы записываются сообщения об ошибках типа *«Не удалось загрузит ь файл»* и критические ошибки.
- **Предупреждения**: в эти журналы записываются сообщения с предупреждениями.
- **Информационные записи**: в эти журналы записываются информационные сообщения, в том числе сообщения о выполненных обновлениях, предупреждения и т. д.
- **Диагностические записи**: в эти журналы записываются данные, необходимые для точной настройки программы, а также все описанные выше записи.

Интерфейс пользователя

Параметры интерфейса пользователя в System Center Endpoint Protection позволяют настроить рабочую среду в соответствии с конкретными требованиями. Эти параметры конфигурации доступны в разделе **Настройка** > **Ввести настройки приложения...** > **Пользователь** > **Интерфейс**.

В этом разделе можно переключиться в расширенный режим, в котором отображаются более детальные настройки и дополнительные элементы управления System Center Endpoint Protection.

Для того чтобы включить заставку, которая отображается при запуске, установите флажок **Показывать заставку при запуске**.

В разделе **Использовать обычное меню** можно установить флажки **В стандартном режиме** и **В расширенном режиме**, чтобы включить использование стандартного меню в главном окне программы в соответствующем режиме.

Для того чтобы включить подсказки, установите флажок **Показывать подсказки**. Параметр **Показывать скрытые файлы** позволяет просматривать и выбирать скрытые файлы при настройке **объектов сканирования**.

Предупреждения и уведомления

Раздел **Предупреждения и уведомления** позволяет настроить обработку системных уведомлений и предупреждений об угрозах в System Center Endpoint Protection.

Если снять флажок **Отображать предупреждения**, предупреждения выводиться не будут, поэтому делать это без особых причин не рекомендуется. В большинстве случаев рекомендуется оставить для этого параметра значение по умолчанию (флажок установлен).

Флажок **Отображать уведомления на рабочем столе** включает показ предупреждений, не требующих вмешательства пользователя, на рабочем столе (по умолчанию в правом верхнем углу экрана). Можно задать длительность отображения уведомления, указав значение параметра **Закрывать окна уведомлений автоматически через** в **секундах**.

Расширенные параметры предупреждений и уведомлений

Отображать уведомления только в случае необходимости вмешательства пользователя
Этот параметр позволяет включить или отключить вывод сообщений, требующих вмешательства пользователя.

Отображать уведомления только в случае необходимости вмешательства пользователя при выполнении приложений в полноэкранном режиме
Этот параметр полезен при проведении презентаций и выполнении других задач, при которых задействован весь экран целиком.

Разрешения

Параметры System Center Endpoint Protection могут иметь большое значение для политики безопасности организации. Несанкционированное изменение может нарушить стабильность работы компьютера и ослабить его защиту. Поэтому можно выбрать пользователей, которым разрешено изменять конфигурацию программы.

Для того чтобы указать пользователей с правами, воспользуйтесь пунктом меню **Настройка** > **Ввести настройки приложения...** > **Пользователь** > **Разрешения**.

Для обеспечения максимальной безопасности компьютера принципиально важно правильно сконфигурировать программу. Несанкционированное изменение может привести к потере важных данных. Для составления списка пользователей с правами выберите их в списке **Пользователи** в левой части окна и нажмите кнопку **Добавить**. Для того чтобы удалить пользователя, выберите его имя в списке пользователей с правами в правой части окна и нажмите кнопку **Удалить**.

ПРИМЕЧАНИЕ. Если список пользователей с правами пуст, изменять настройки приложения могут все пользователи системы.

Контекстное меню

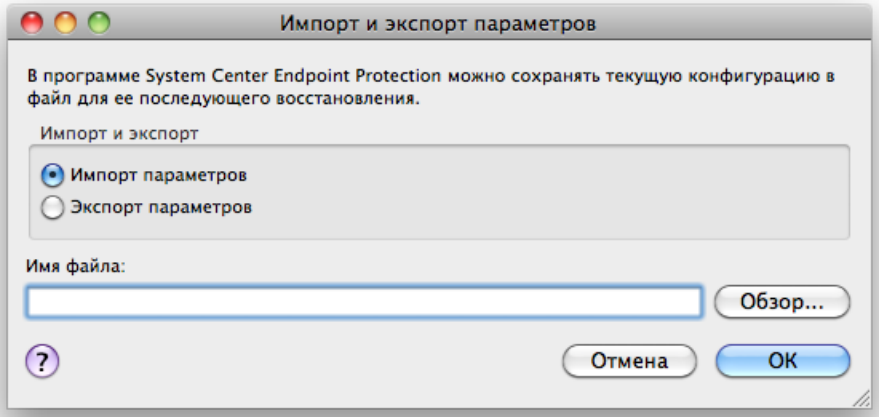
Интеграцию элементов в контекстное меню можно включить в разделе **Настройка** > **Ввести настройки приложения...** > **Пользователь** > **Контекстное меню**, установив флажок **Встроить в контекстное меню**.

Для опытных пользователей

Импорт и экспорт параметров

Импорт или экспорт конфигурации System Center Endpoint Protection можно выполнить в расширенном режиме в разделе **Настройка**.

Для хранения конфигурации при импорте и экспорте используются файлы архивов. Импорт и экспорт удобны, если нужно создать резервную копию текущей конфигурации System Center Endpoint Protection для дальнейшего использования. Экспорт параметров также полезен, если необходимо использовать выбранную конфигурацию System Center Endpoint Protection на нескольких системах, поскольку файл конфигурации можно легко импортировать для переноса нужных настроек.



Импорт параметров

Импортировать конфигурацию несложно. В главном меню выберите пункт **Настройка** > **Импорт и экспорт параметров...**, а затем — пункт **Импорт параметров**. Введите имя файла конфигурации или нажмите кнопку **Обзор...**, чтобы выбрать файл, который необходимо импортировать.

Экспорт параметров

Процедура экспорта конфигурации похожа на ее импорт. В главном меню выберите пункт **Настройка** > **Импорт и экспорт параметров...**. Выберите пункт **Экспорт параметров** и введите имя файла конфигурации. С помощью проводника выберите место на компьютере для сохранения файла конфигурации.

Настройка прокси-сервера

Параметры прокси-сервера можно настроить в разделе **Разное** > **Прокси-сервер**. Настройка прокси-сервера на этом уровне позволяет задать его параметры для всех функций программы System Center Endpoint Protection. Они используются всеми модулями программы, которым требуется подключение к Интернету.

Чтобы задать параметры прокси-сервера на этом уровне, установите флажок **Использовать прокси-сервер**, а затем введите IP- или URL-адрес прокси-сервера в поле **Прокси-сервер**. В соответствующем поле укажите порт, по которому прокси-сервер принимает запросы на соединение (по умолчанию 3128). Если требуется аутентификация на прокси-сервере, установите флажок **Прокси-сервер требует аутентификации**, а затем укажите **имя пользователя** и **пароль** в соответствующих полях.

Блокирование съемных носителей

Съемные носители (например, компакт-диски или USB-накопители) могут содержать вредоносный код и подвергать компьютер опасности. Чтобы заблокировать их, установите флажок **Включить блокирование съемных носителей**. Чтобы разрешить доступ к носителям определенных типов, снимите флажки для тех типов носителей, которые необходимо разрешить.

Установите флажок **Другие**, если необходимо применить эти настройки к другим типам носителей, кроме компакт- и DVD-дисков, FireWire и USB. В частности, эта настройка применяется в случае любых внешних устройств, подключаемых к компьютеру через интерфейс Thunderbolt.

Глоссарий

Типы заражений

Под заражением понимается вредоносная программа, которая пытается проникнуть на компьютер пользователя и (или) причинить ему вред.

Вирусы

Компьютерный вирус — это такой вид заражения, который повреждает существующие файлы на компьютере. Название было выбрано из-за сходства с биологическими вирусами, так как они используют похожие методы для распространения с компьютера на компьютер.

Компьютерные вирусы атакуют в основном исполняемые файлы, сценарии и документы. Для размножения вирус присоединяет свое «тело» к концу заражаемого файла. Краткое описание цикла размножения: после запуска зараженного файла вирус активируется (перед активацией самого приложения) и выполняет свою задачу. Только после этого запускается само приложение. Вирус не может заразить компьютер, пока пользователь (по ошибке или намеренно) собственноручно не запустит файл с вредоносной программой.

Компьютерные вирусы могут быть разными по целям и степени опасности. Некоторые из вирусов особо опасны, так как могут удалять файлы с жесткого диска. С другой стороны, некоторые вирусы не причиняют никакого вреда. Они просто раздражают пользователя и демонстрируют возможности своих авторов.

Важно отметить, что количество вирусов постоянно снижается по сравнению с троянскими и шпионскими программами, так как они не представляют для авторов экономической выгоды. Кроме того, термин «вирус» часто неправильно используют для описания всех возможных типов заражений. Однако постепенно он выходит из употребления, и на смену ему приходит более точный термин «вредоносная программа».

Если компьютер заражен вирусом, необходимо восстановить исходное состояние зараженных файлов, т. е. очистить их с помощью программы защиты от вирусов.

Примеры вирусов: *OneHalf*, *Tenga* и *Yankee Doodle*.

Черви

Компьютерные черви — это содержащие злонамеренный код программы, которые атакуют главные компьютеры и распространяются через сеть. Основное различие между вирусами и червями заключается в том, что черви могут реплицироваться и распространяться самостоятельно, так как они не зависят от зараженных файлов или загрузочных секторов. Черви распространяются, используя адресную книгу пользователя или уязвимости в системе безопасности сетевых приложений.

Черви намного более жизнеспособны, чем компьютерные вирусы. Благодаря Интернету они могут распространиться по всему земному шару за считаные часы после запуска в сеть. В некоторых случаях счет идет даже на минуты. Эта способность быстро самостоятельно реплицироваться делает черви более опасными, чем другие типы вредоносных программ.

Работающий в системе червь может доставить много неудобств пользователю: он может удалять файлы, снижать производительность системы или даже отключать другие программы. По сути компьютерный червь может служить в качестве «транспортного средства» для других типов заражений.

Если компьютер заражен червем, рекомендуется удалить зараженные файлы, поскольку они с большой вероятностью содержат злонамеренный код.

Примеры широко известных червей: *Lovsan/Blaster*, *Stration/Warezov*, *Bagle* и *Netsky*.

Троянские программы

Исторически троянскими программами называют особую группу заражений, которые выдают себя за полезные, чтобы пользователи запускали их. Сегодня троянские программы не нуждаются в подобной маскировке. Единственная их цель — как можно проще проникнуть в систему и запустить вредоносный код. Сегодня троянская программа — очень общий термин, используемый для обозначения любого заражения, которое невозможно отнести к какому-либо конкретному классу.

Так как эта категория весьма широка, ее часто разбивают на несколько подкатегорий.

- Загрузчик — вредоносная программа, которая загружает другие заражения из Интернета.
- Dropper — тип троянских программ, разработанных для заражения компьютеров другими вредоносными программами.
- Backdoor — приложение, которое обменивается данными со злоумышленниками, позволяя им получить доступ к системе и контроль над ней.

- Клавиатурный шпион — такие программы записывают все, что пользователь набирает на клавиатуре, и отправляют эту информацию злоумышленникам.
- Программа дозвона — программы, которые пытаются набирать номера телефонов, звонки на которые оплачивает вызывающий абонент. При этом пользователю практически невозможно заметить, что создается новое подключение. Программы дозвона могут причинить вред только пользователям модемов. К счастью, модемы уже распространены не столь широко, как раньше.
- Как правило, троянские программы распространяются в виде исполняемых файлов. Если на компьютере будет обнаружен файл, относящийся к категории троянских программ, рекомендуется удалить его, так как он скорее всего содержит вредоносный код.

Примеры широко известных троянских программ: *NetBus, Trojandownloader.Small.ZL, Slapper.*

Рекламные программы

Рекламными программами называют программное обеспечение, распространение которого обеспечивается за счет рекламы. Программы, демонстрирующие пользователю рекламу, попадают в эту категорию. Рекламные приложения часто автоматически открывают всплывающие окна с рекламой в веб-браузере или изменяют домашнюю страницу. Рекламные программы часто распространяются в комплекте с бесплатными. Это позволяет их создателям покрывать расходы на разработку полезных программ.

Сами по себе рекламные программы не опасны, но они доставляют неудобства пользователям. Опасность состоит в том, что в рекламных программах могут быть реализованы дополнительные функции слежения, как в шпионских программах.

Если пользователь решает использовать бесплатный программный продукт, ему следует уделить особое внимание установке. Чаще всего программа установки предупреждает об установке дополнительной рекламной программы. Часто пользователь имеет возможность отказаться от ее установки и установить только сам программный продукт без рекламной программы.

Некоторые программы нельзя установить без рекламных модулей, в противном случае их функциональность ограничивается. Это приводит к тому, что рекламная программа часто получает доступ к системе на «законных» основаниях, так как пользователь дал согласие на ее установку. В этом случает лучше заранее обезопасить себя, чем потом жалеть. В случае обнаружения файла, классифицированного как рекламная программа, рекомендуется удалить его, так как скорее всего он содержит злонамеренный код.

Шпионские программы

К этой категории относятся все приложения, которые отправляют конфиденциальные данные злоумышленникам без ведома и согласия их владельца. Шпионские программы используют функции слежения для отправки различной статистической информации, такой как список посещенных веб-сайтов, адреса электронной почты из адресных книг пользователя или набираемый на клавиатуре текст.

Авторы шпионских программ утверждают, что эти методы служат для изучения требований и интересов пользователей и позволяют создавать рекламные материалы, более полно соответствующие интересам целевой аудитории. Проблема в том, что нет четкой границы между полезными и вредоносными приложениями, и никто не гарантирует, что собираемая информация не будет использована во вред. Данные, полученные шпионскими программами, могут содержать защитные коды, PIN-коды, номера счетов и т. д. Шпионские программы часто поставляются в комплекте с бесплатными версиями программ самими их авторами с целью получения доходов или стимулирования продаж программного обеспечения. Часто пользователей информируют о наличии шпионских программ во время установки основной программы, чтобы поощрить их к приобретению платной версии.

Примерами хорошо известного бесплатного программного обеспечения, вместе с которым поставляется шпионское, могут служить клиенты пиринговых (P2P) сетей. Программы Spyfalcon и Spy Sheriff (и многие другие) относятся к особой подкатегории шпионских программ. Утверждается, что они предназначены для защиты от шпионских программ, но на самом деле сами являются таковыми.

В случае обнаружения файла, классифицированного как шпионская программа, рекомендуется удалить его, так как скорее всего он содержит вредоносный код.

Потенциально опасные приложения

Существует множество нормальных программ, предназначенных для упрощения администрирования подключенных к сети компьютеров. Однако злоумышленники могут использовать их для причинения вреда. System Center Endpoint Protection позволяет выявлять такие угрозы.

В качестве «потенциально опасных приложений» выступает нормальное коммерческое программное обеспечение. В эту категорию входят такие программы, как средства удаленного доступа, приложения для взлома паролей и клавиатурные шпионы (программы, записывающие нажатия клавиш на клавиатуре).

Если такая программа обнаружена на компьютере, но вы не устанавливали ее, обратитесь к администратору сети за консультацией или удалите ее.

Потенциально нежелательные приложения

Потенциально нежелательные приложения не обязательно являются вредоносными, но могут отрицательно влиять на производительность компьютера. Такие приложения обычно запрашивают при установке согласие пользователя. После их установки работа системы изменяется. Наиболее заметны следующие изменения.

- Открываются новые окна, которые не появлялись ранее.
- Активируются и выполняются скрытые процессы.
- Повышается уровень потребления системных ресурсов.
- Появляются изменения в результатах поиска.
- Приложение подключается к удаленным серверам.