ESET FILE SECURITY

для Microsoft Windows Server

Инструкция по установке и руководство пользователя

Microsoft® Windows® Server 2000 / 2003 / 2008 / 2008 R2

Щелкните здесь, чтобы загрузить актуальную версию этого документа

ESET **FILE SECURITY**

Программный продукт ESET File Security разработан компанией ESET, spol. s r.o..

Международная служба поддержки клиентов: www.eset.eu/support
Служба поддержки клиентов в Северной Америке: www.eset.com/support

Содержание

1. Введение

ESET File Security представляет собой интегрированное решение, специально предназначенное для работы в среде Microsoft Windows Server. Этот программный продукт обеспечивает эффективную надежную защиту от различных типов атак со стороны вредоносных программ. ESET File Security обеспечивает два типа защиты: защиту от вирусов и защиту от шпионских программ.

Основные функции ESET File Security

- Автоматические исключения : автоматическое обнаружение и исключение файлов на сервере, имеющих критическое значение для беспрепятственной работы.
- eShell (ESET Shell) — новый управляющий интерфейс командной строки, который позволяет опытным пользователям и администраторам использовать более расширенные возможности по управлению программными продуктами ESET.
- SelfDefense — технология, защищающая решения для обеспечения безопасности ESET от изменения и отключения.
- Эффективное устранение проблем благодаря встроенным расширенным средствам для решения различных проблем: ESET SysInspector для диагностики системы и ESET SysRescue для создания загрузочного компакт-диска аварийного восстановления.

ESET File Security поддерживает Microsoft Windows Server версий 2000, 2003 и 2008 в виде самостоятельной системы, а также Microsoft Windows Server в кластерной среде. Можно удаленно управлять ESET File Security в больших сетях с помощью ESET Remote Administrator.

1.1 Системные требования

Поддерживаемые операционные системы

- Microsoft Windows 2000 Server
- Microsoft Windows Server 2003 (x86 и x64)
- Microsoft Windows Server 2008 (x86 и x64)
- Microsoft Windows Server 2008 R2
- Microsoft Windows Small Business Server 2003 (x86)
- Microsoft Windows Small Business Server 2003 R2 (x86)
- Microsoft Windows Small Business Server 2008 (x64)
- Microsoft Windows Small Business Server 2011 (x64)

Требования к оборудованию зависят от используемой версии операционной системы. Рекомендуется ознакомиться с документацией на Microsoft Windows Server для получения дополнительных сведений о требованиях к оборудованию.

1.2 Типы защиты

Существует два типа защиты.

- Защита от вирусов
- Защита от шпионских программ

Защита от вирусов и шпионских программ — одна из основных функций программного продукта ESET File Security. Такая защита предотвращает вредоносные атаки на компьютер путем контроля файлов, электронной почты и подключений к Интернету. Если обнаруживается угроза, представляемая злонамеренным кодом, модуль защиты от вирусов может устранить ее, сначала заблокировав, а затем очистив, удалив или поместив на карантин.

1.3 Интерфейс пользователя

ESET File Security имеет графический интерфейс пользователя, задача которого заключается в том, чтобы быть настолько интуитивно понятным, насколько возможно. Графический интерфейс пользователя дает возможность быстро и просто использовать основные функции программы.

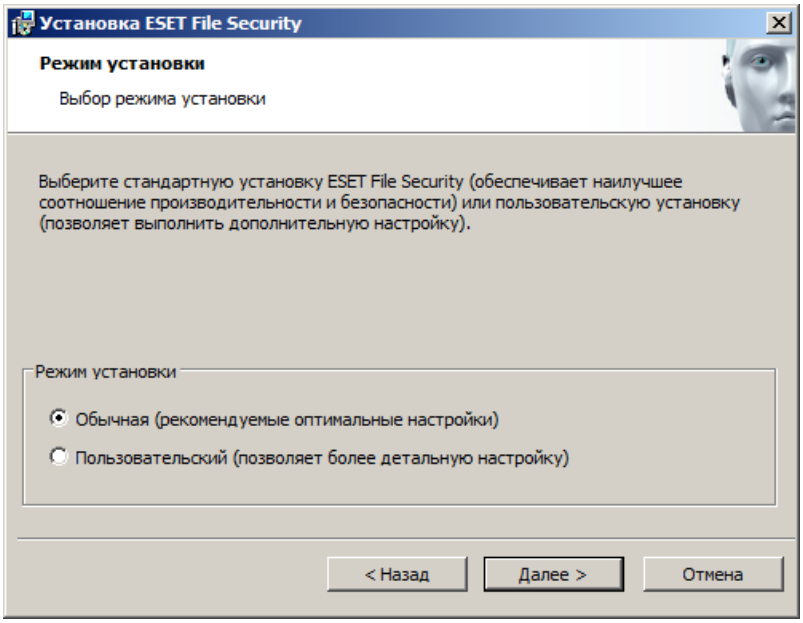
В дополнение к основному графическому интерфейсу пользователя существует также и **дерево расширенных параметров**, которое можно открыть с любой страницы программы, нажав клавишу F5.

После нажатия клавиши F5 открывается окно дерева расширенных параметров, в котором отображается перечень настраиваемых функций программы. В этом окне можно конфигурировать параметры в соответствии со своими потребностями. Древовидная структура разбита на два раздела: **Защита сервера** и **Защита компьютера**. В разделе **Защита сервера** перечисляются автоматические исключения, распространяющиеся именно на операционную систему и системные файлы сервера. В разделе **Защита компьютера** содержатся настраиваемые элементы для защиты самого сервера.

2. Установка

После приобретения ESET File Security установочный файл можно загрузить с веб-сайта ESET (www.eset.com) в виде пакета с расширением .msi. После запуска этого файла мастер установки поможет установить программу. Существует два типа установки, которые отличаются уровнями выбора параметров.

1. Обычная установка
2. Выборочная установка



ПРИМЕЧАНИЕ: Настоятельно рекомендуется устанавливать ESET File Security в только что установленной и сконфигурированной операционной системе, если это возможно. Однако при возникновении необходимости в установке программного продукта на существующей системе лучше всего удалить предыдущую версию ESET File Security, перезапустить сервер и установить новую версию ESET File Security после.

2.1 Обычная установка

Режим обычной установки позволяет быстро установить ESET File Security, выполнив в процессе установки лишь минимальные изменения конфигурации. Обычная установка — это режим установки по умолчанию; при отсутствии особых требований не рекомендуется выбирать другой режим. После установки ESET File Security на компьютере можно в любой момент изменить параметры и конфигурацию программы. В настоящем руководстве пользователя эти параметры и функциональность описываются подробно Параметры, активируемые в режиме обычной установки, обеспечивают отличный уровень безопасности в сочетании с удобством использования и высокой производительностью компьютера.

После выбора режима установки и нажатия кнопки «Далее» предлагается ввести имя пользователя и пароль. Этот этап играет важную роль в обеспечении постоянной защиты компьютера, так как имя пользователя и пароль делают возможным автоматическое обновление базы данных сигнатур вирусов.

Введите имя пользователя и пароль, полученные после покупки или регистрации программного продукта, в соответствующие поля. Если имени пользователя и пароля пока нет, их можно будет ввести непосредственно в программе позднее.

На следующем этапе конфигурируется система своевременного обнаружения ThreatSense.Net. Система своевременного обнаружения ThreatSense.Net предназначена для немедленного непрерывного информирования компании ESET о новых заражениях, что позволяет быстро реагировать и защищать пользователей. Эта система предусматривает отправку новых угроз в лабораторию ESET, где они анализируются, обрабатываются и добавляются в базу данных сигнатур вирусов. По умолчанию флажок **Включить систему своевременного обнаружения ThreatSense.Net** установлен. Для изменения расширенных параметров отправки подозрительных файлов нажмите **Дополнительные настройки...**.

Следующим этапом установки является конфигурирование **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.

Рекомендуется выбрать параметр **«Включить обнаружение потенциально нежелательного ПО»**, чтобы разрешить приложению ESET File Security выявлять угрозы такого типа. Если использовать эту функцию не следует, установите флажок **Выключить обнаружение потенциально нежелательного ПО**.

Последним этапом обычной установки является подтверждение установки. Для этого нажмите кнопку **Установить**.

2.2 Выборочная установка

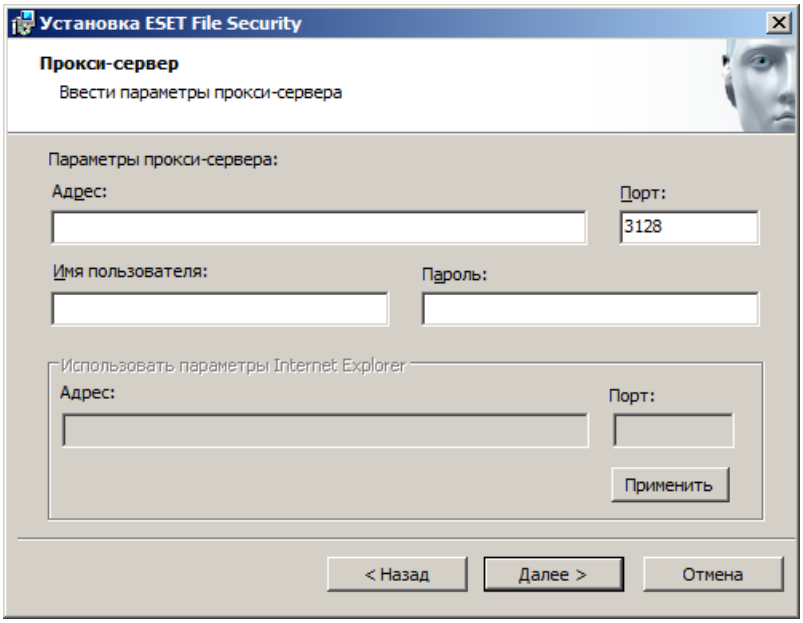
Выборочная установка предназначена для тех пользователей, которые хотят сконфигурировать программное обеспечение ESET File Security в ходе процесса установки.

После выбора режима установки и нажатия кнопки **Далее** пользователю будет предложено выбрать папку для установки. По умолчанию программа устанавливается в папку *C:\Program Files\ESET\ESET File Security*. Нажмите кнопку **Обзор...**, чтобы изменить папку (не рекомендуется).

Затем заполните поля **Имя пользователя** и **Пароль**. Это действие аналогично соответствующему действию в режиме обычной установки (см. Обычная установка).

После ввода имени пользователя и пароля нажмите кнопку **Далее**, чтобы перейти к окну **Настройте подключение к Интернету**.

Если используется прокси сервер, он должен быть корректно сконфигурирован для обеспечения нормальной работы обновления сигнатур вирусов. Если нужно сконфигурировать прокси-сервер автоматически, не меняйте параметр по умолчанию **Я не уверен, используется ли прокси-сервер. Я хочу использовать те же параметры, какие использует Internet Explorer (рекомендуется)** и нажмите кнопку **Далее**. Если прокси-сервер не используется, установите флажок **Я не использую прокси-сервер**.

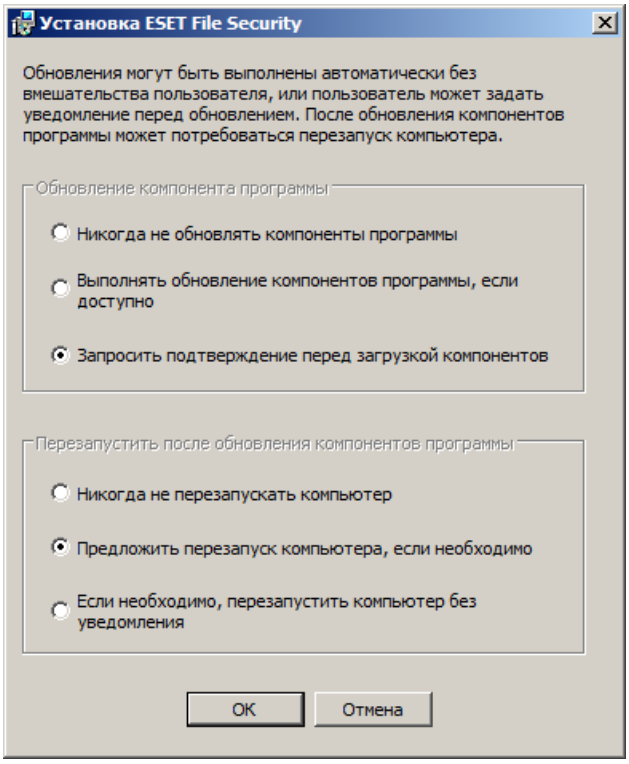


Если же вы предпочитаете ввести данные прокси-сервера самостоятельно, его параметры можно сконфигурировать вручную. Для конфигурирования параметров прокси-сервера выберите вариант **Я использую прокси-сервер** и нажмите кнопку **Далее**. Введите IP-адрес или URL-адрес прокси-сервера в поле **Адрес**. В поле **Порт** укажите порт, по которому этот прокси-сервер принимает запросы на соединение (по умолчанию 3128). Если прокси-сервер требует аутентификации, введите правильные **имя пользователя** и **пароль** для доступа к нему. Параметры прокси-сервера также по желанию могут быть скопированы из параметров Internet Explorer. После ввода сведений прокси-сервера нажмите кнопку **Применить** и подтвердите свой выбор.

Нажмите **Далее**, чтобы перейти к окну **Настроить параметры автоматического обновления**. На этом этапе можно задать, как в системе будет обрабатываться автоматическое обновление компонентов программы. Нажмите **Изменить...** для доступа к расширенным параметрам.

Если нет необходимости обновлять компоненты программы, выберите вариант **Никогда не обновлять компоненты программы**. Установите флажок **Запросить подтверждение перед загрузкой компонентов**,

чтобы перед загрузкой компонентов программы на экран выводилось окно подтверждения. Для автоматической загрузки обновлений компонентов программы выберите вариант **Выполнять обновление компонентов программы, если доступно**.



ПРИМЕЧАНИЕ: После обновления программных компонентов обычно нужно перезагрузить компьютер. Рекомендуется выбрать вариант **Никогда не перезапускать компьютер**. Полученные обновления компонентов будут активированы после следующего перезапуска сервера (вне зависимости от того, выполняется ли такой перезапуск по расписанию, вручную или как-либо иначе). Можно выбрать вариант **Предложить перезапуск компьютера, если необходимо**, если нужно, чтобы предлагалось перезапустить сервер после обновления компонентов. Если выбран этот параметр, то можно перезапустить сервер сразу же или отложить перезапуск и выполнить его позднее.

В следующем окне предлагается создать пароль для защиты параметров программы. Установите флажок **Защита параметров конфигурации паролем** и введите пароль в поля **Новый пароль** и **Подтвердить новый пароль**.

Следующие два этапа установки (**Система своевременного обнаружения ThreatSense.Net** и **Обнаружение потенциально нежелательных приложений**) совпадают с этапами режима обычной установки (см. раздел Обычная установка).

Нажмите **Установить** в окне **Все готово к установке**, чтобы завершить процесс установки.

2.3 Сервер терминалов

Если программное обеспечение ESET File Security установлено на сервере Windows Server, который выступает в качестве сервера терминалов, полезно будет отключить графический интерфейс пользователя ESET File Security, чтобы предотвратить запуск программы при каждом входе пользователя в систему. Конкретные инструкции по отключению приводятся в главе Отключение графического интерфейса пользователя на сервере терминалов.

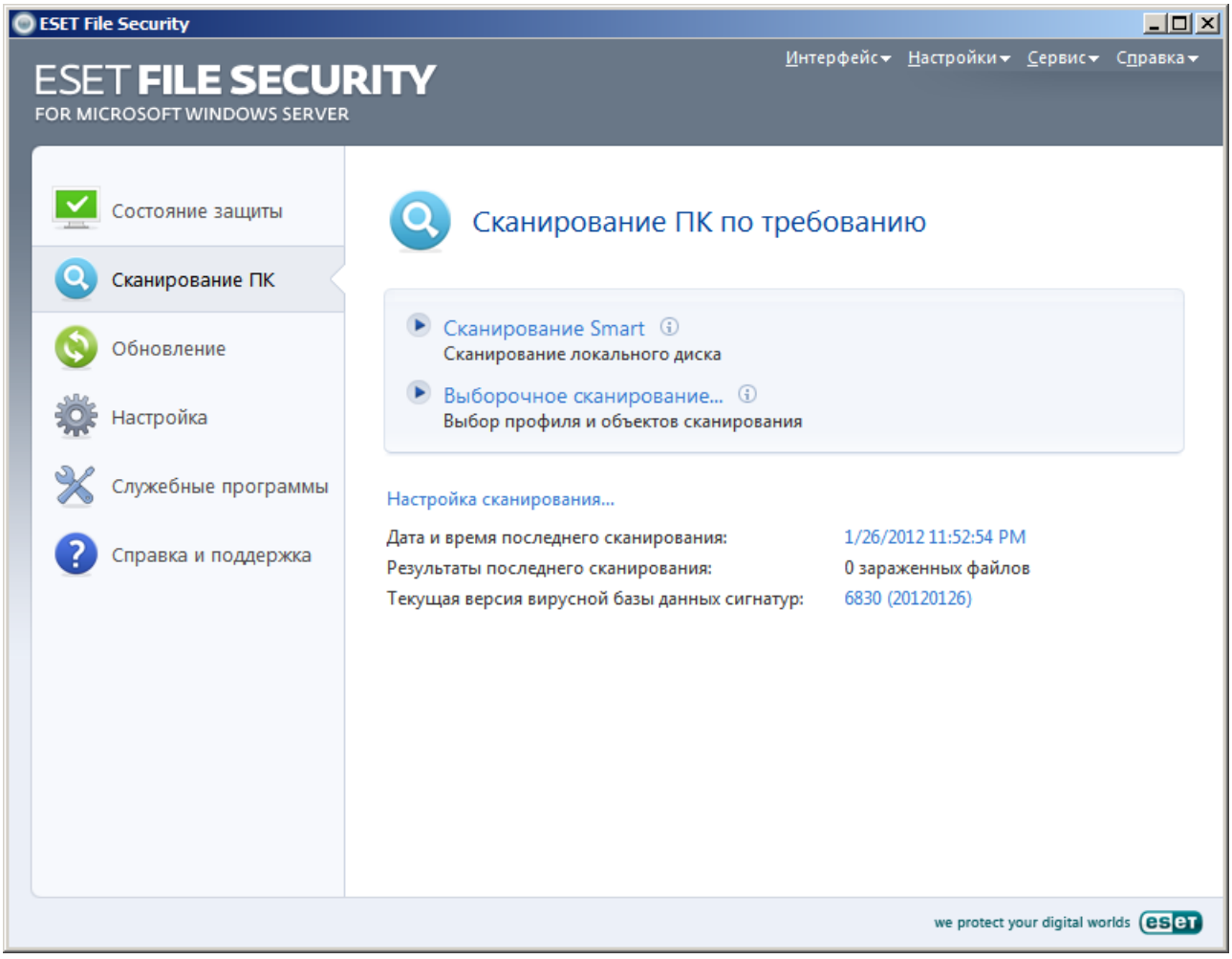
2.4 Обновление до новой версии

Более новые версии ESET File Security выпускаются для реализации улучшений или исправления проблем, которые не могут быть устранены автоматическим обновлением модулей программы. Обновление до новой версии можно выполнить одним из нескольких способов.

1. Автоматическое обновление путем обновления компонентов программы
   Поскольку обновления компонентов программы распространяются среди всех пользователей и могут повлиять на некоторые конфигурации компьютеров, они выпускаются только после длительного тестирования с целью обеспечения бесперебойного процесса обновления на всех возможных конфигурациях. Если нужно выполнить обновление до более новой версии сразу после ее выхода, нужно воспользоваться одним из описанных далее методов.
2. Обновление вручную путем загрузки и установки новой версии поверх предыдущей установленной
   В начале процесса установки можно принять решение о сохранении существующих параметров программы. Для этого нужно установить флажок **Использовать текущие параметры**.
3. Обновление вручную с автоматическим развертыванием в сетевой среде посредством ESET Remote Administrator.

2.5 Сканирование ПК по требованию

После установки приложения ESET File Security следует выполнить сканирование компьютера на наличие вредоносного кода. В главном окне программы выберите пункт **«Сканирование компьютера»**, а затем — **«Сканирование Smart»**. Дополнительную информацию о сканировании компьютера по требованию см. в разделе Сканирование ПК по требованию.



3. Руководство для начинающих

Этот раздел содержит обзор приложения ESET File Security и его основных параметров.

3.1 Введение в интерфейс пользователя

Главное окно ESET File Security 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 ESET File Security. Если активирован расширенный режим, отображаются подменю **Наблюдение** и **Статистика**.

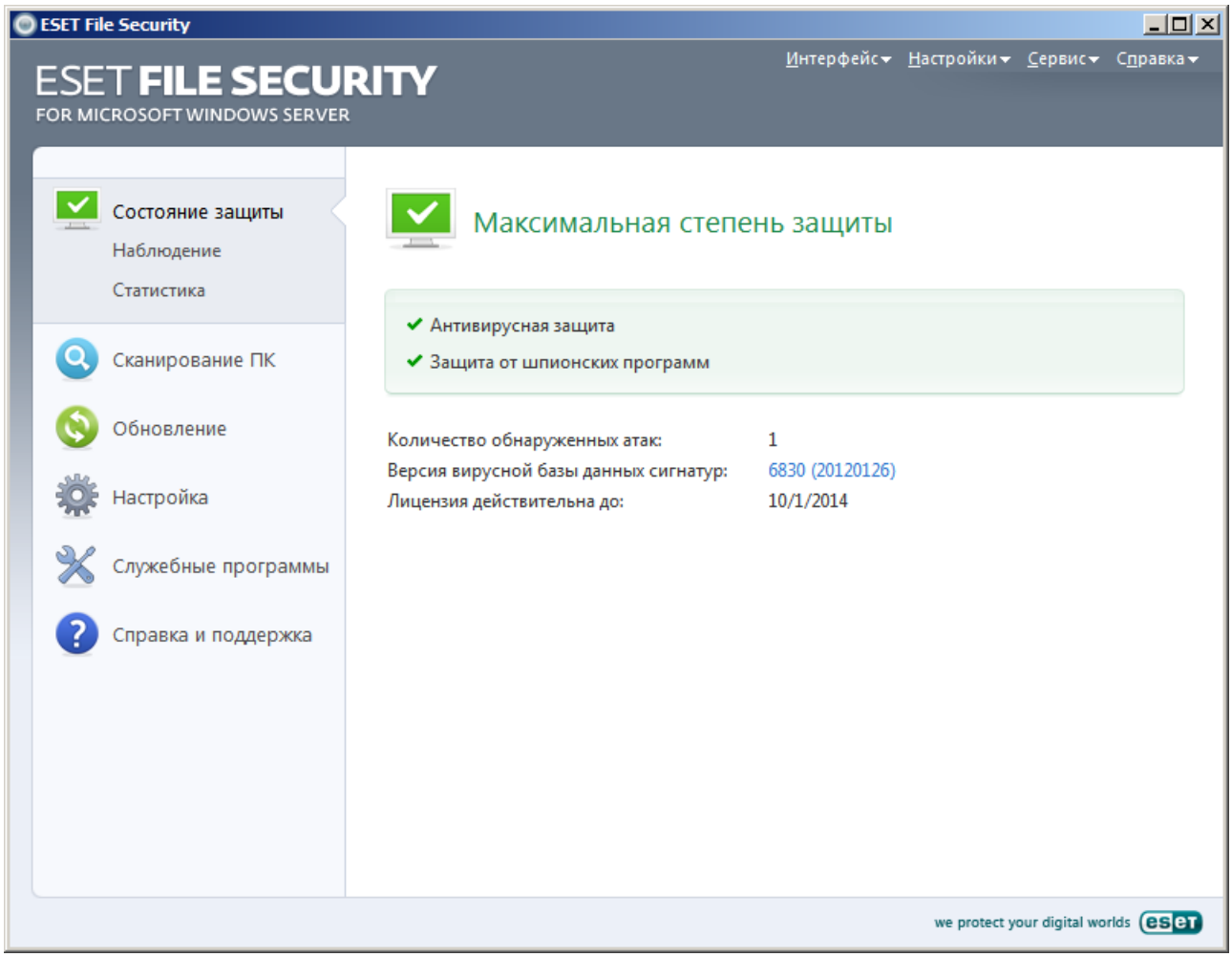
Сканирование ПК: этот пункт позволяет настроить и запустить сканирование компьютера по требованию.

Обновление: выводит на экран информацию об обновлениях базы данных сигнатур вирусов.

Настройка: этот параметр 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**, **планировщику** и **SysInspector**. Он отображается только в расширенном режиме.

Справка и поддержка: предоставляет доступ к файлам справки, базе знаний ESET, веб-сайту ESET и ссылкам, которые позволяют отправить запрос в службу поддержки клиентов.



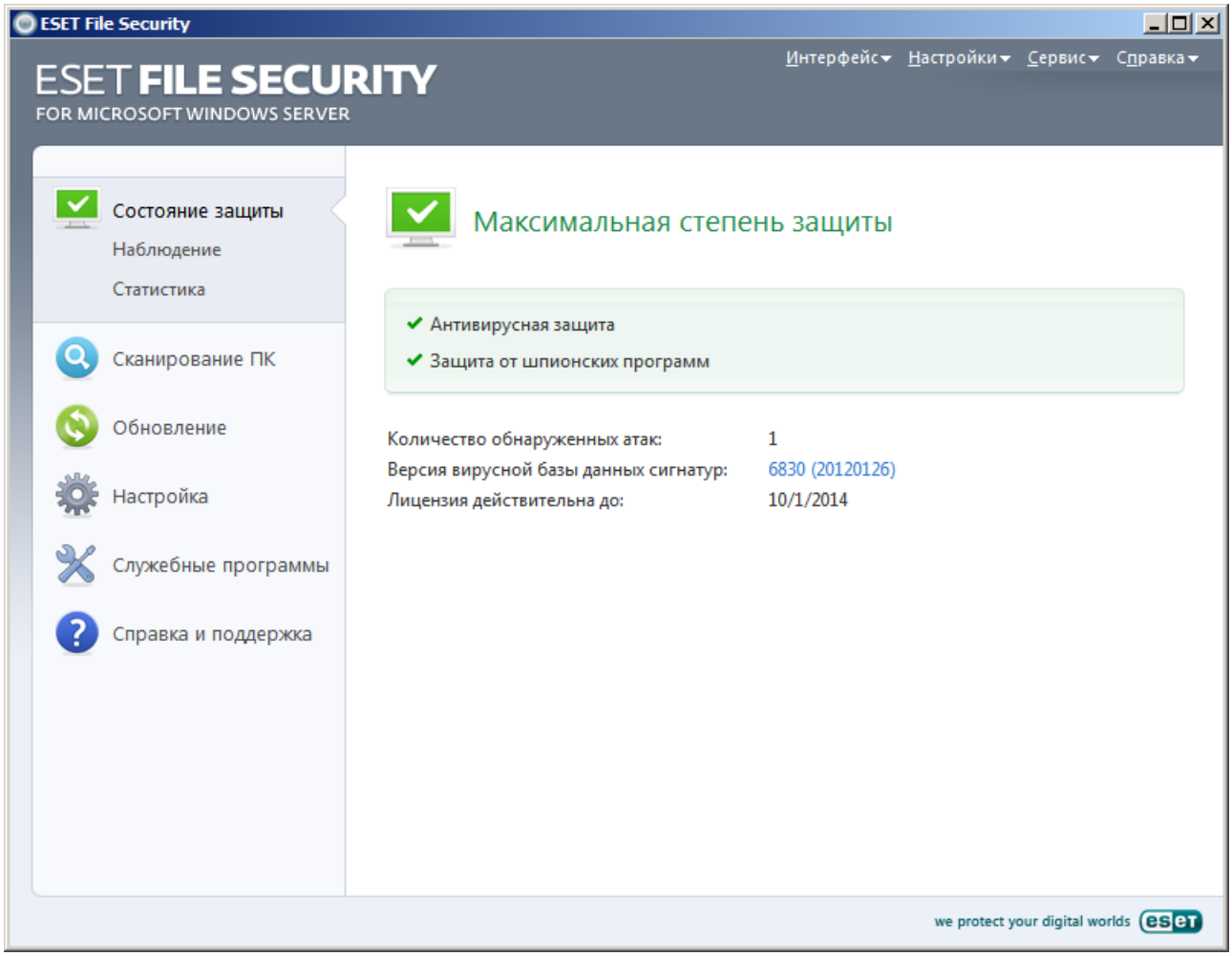
3.1.1 Проверка работоспособности системы

Чтобы просмотреть **состояние защиты**, выберите соответствующий пункт в главном меню. В главном окне появится сводная информация о работе ESET File Security и подменю с двумя пунктами: **Наблюдение** и **Статистика**. Для просмотра более подробных сведений о системе можно воспользоваться любым из этих пунктов.

Когда функциональность ESET File Security используется полностью, **состояние защиты** обозначается зеленым цветом. В противном случае используется оранжевый или желтый цвет, чтобы показать, что необходимо вмешательство пользователя.

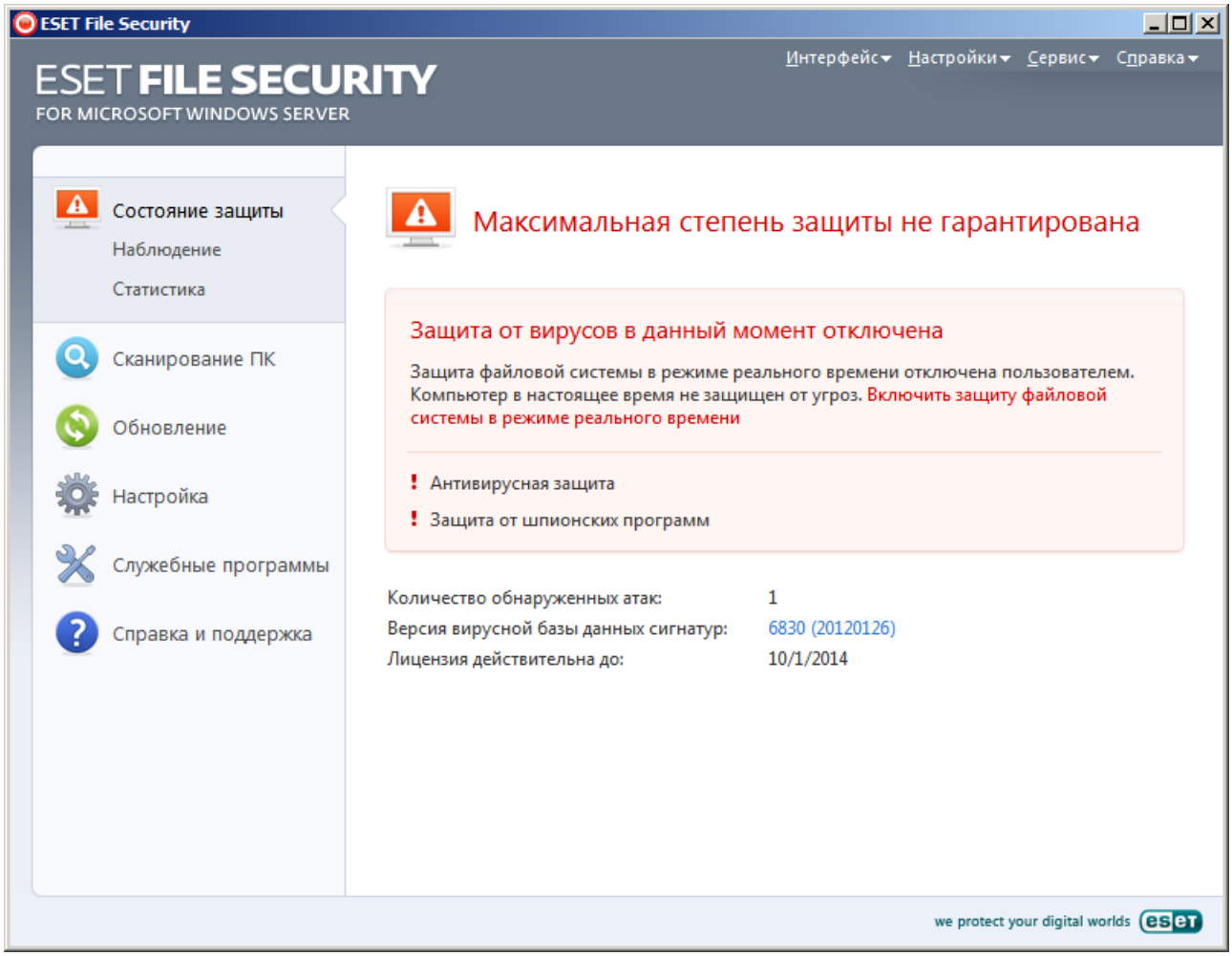
Пункт подменю **Наблюдение** позволяет просмотреть текущую активность файловой системы в виде графика, обновляемого в режиме реального времени (для обозначения времени используется горизонтальная ось). На вертикальной оси показывается объем считанных (синяя линия) и записанных (красная линия) данных.

Подменю **Статистика** позволяет увидеть количество зараженных, очищенных и незараженных объектов по модулям. Доступные модули можно выбирать с помощью раскрывающегося списка.



3.1.2 Действия, которые следует выполнить, если приложение не работает надлежащим образом

Если включенные модули работают правильно, они обозначаются зеленым флажком. При возникновении проблем появляется оранжевый значок уведомления или красный восклицательный знак, а в верхней части окна выводятся дополнительные сведения. Кроме того, предлагается решение проблемы. Чтобы изменить состояние отдельного модуля, выберите в главном меню пункт **«Настройка»** и выберите модуль.

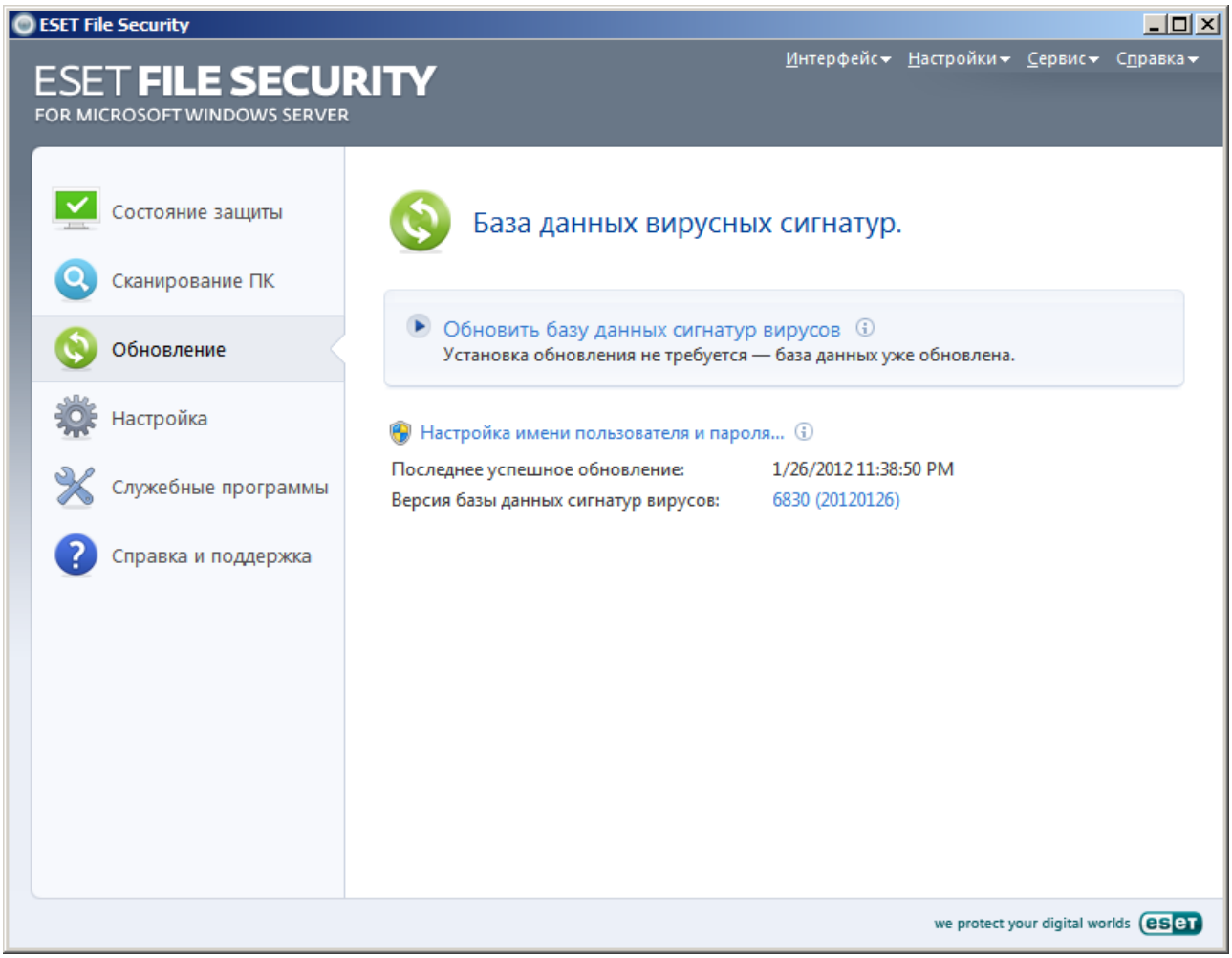


Если предложенные решения не позволяют устранить проблему, выберите пункт «Справка и поддержка» для доступа к файлам справки или поиска в базе знаний. Если же помощь все еще нужна, можно отправить запрос в службу поддержки клиентов ESET. Специалисты службы поддержки оперативно ответят на ваши вопросы и помогут найти решение проблемы.

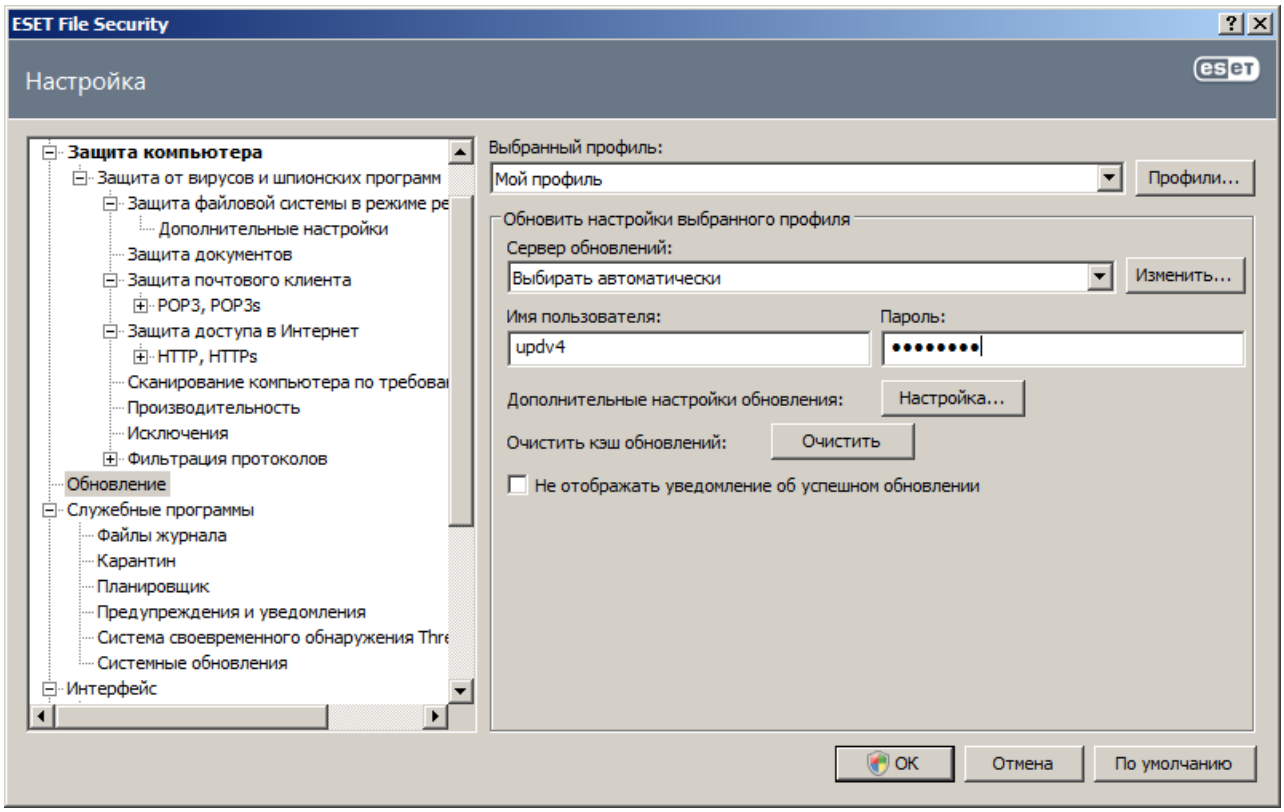
3.2 Настройка обновлений

Обновление базы данных сигнатур вирусов и компонентов программы является важнейшей частью обеспечения защиты компьютера от злонамеренного кода. Уделите внимание изучению конфигурирования и выполнения обновлений. В главном меню выберите пункт **Обновление** и нажмите **Обновить базу данных сигнатур вирусов** в основном окне, чтобы проверить наличие более новых обновлений базы данных. Пункт **Настройка имени пользователя и пароля...** позволяет вывести на экран диалоговое окно, в котором следует ввести имя пользователя и пароль (полученные при покупке).

Если имя пользователя и пароль вводились при установке ESET File Security, в этот момент не будет предложено ввести их.

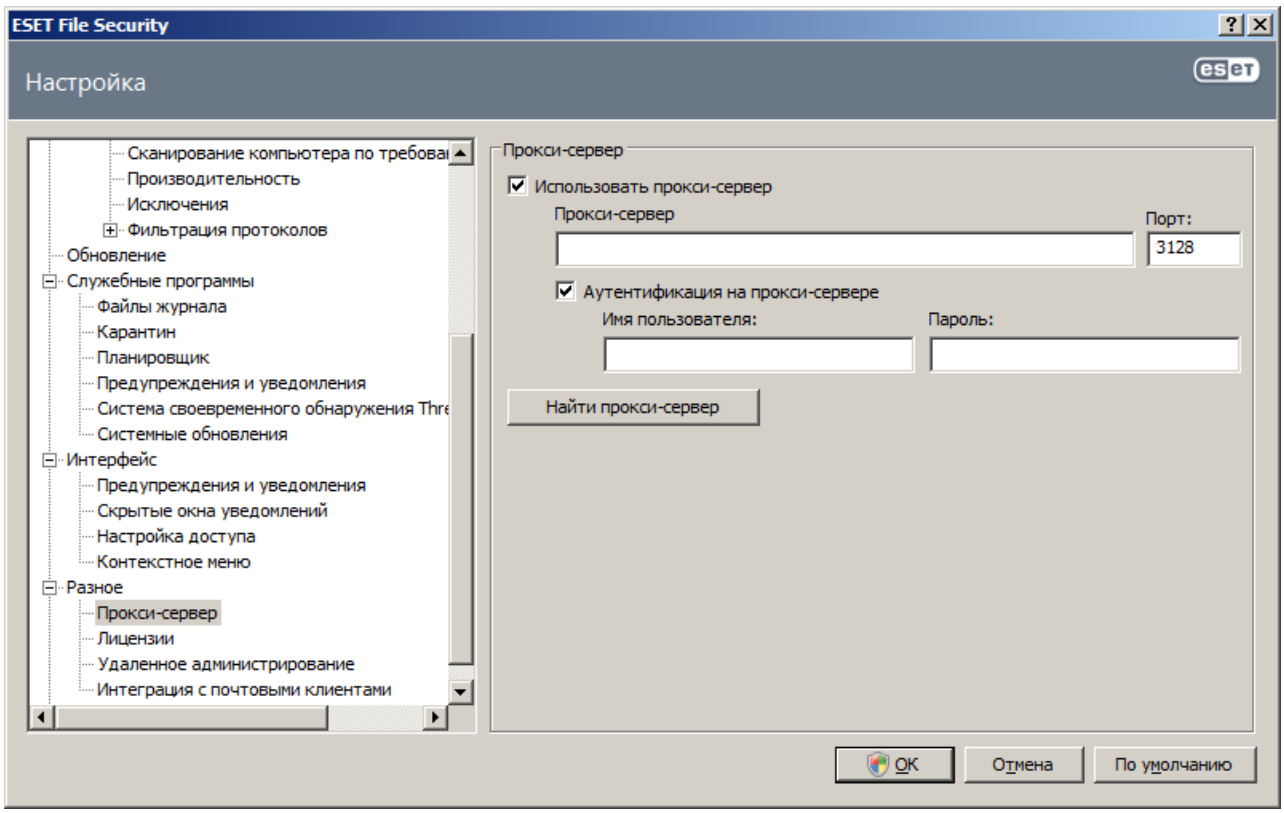


В окне «Дополнительные настройки» (нажмите **Настройка** в главном меню, а затем воспользуйтесь пунктом **Ввод всего дерева расширенных параметров...** или нажмите F5) содержатся дополнительные параметры обновления. Нажмите **Обновление** в дереве расширенных параметров. В раскрывающемся меню **Сервер обновлений:** должен быть выбран пункт **Выбирать автоматически**. Для конфигурирования расширенных параметров обновления, таких как режим обновления, доступ через прокси-сервер, подключения к локальной сети и создание копий сигнатур вирусов, нажмите кнопку **Настройка...**.



3.3 Настройка прокси-сервера

Если для управления подключениями к Интернету в системе, в которой используется ESET File Security, применяется прокси-сервер, это должно быть указано в разделе «Дополнительные настройки». Для доступа к окну настройки прокси-сервера нажмите кнопку F5, чтобы открыть окно расширенной настройки и выберите пункты **Разное** > **Прокси-сервер** в древовидной структуре. Установите флажок **Использовать прокси-сервер**, а затем заполните поля **Прокси-сервер** (IP-адрес) и **Порт**. При необходимости установите флажок **Аутентификация на прокси-сервере** и заполните поля **Имя пользователя** и **Пароль**.



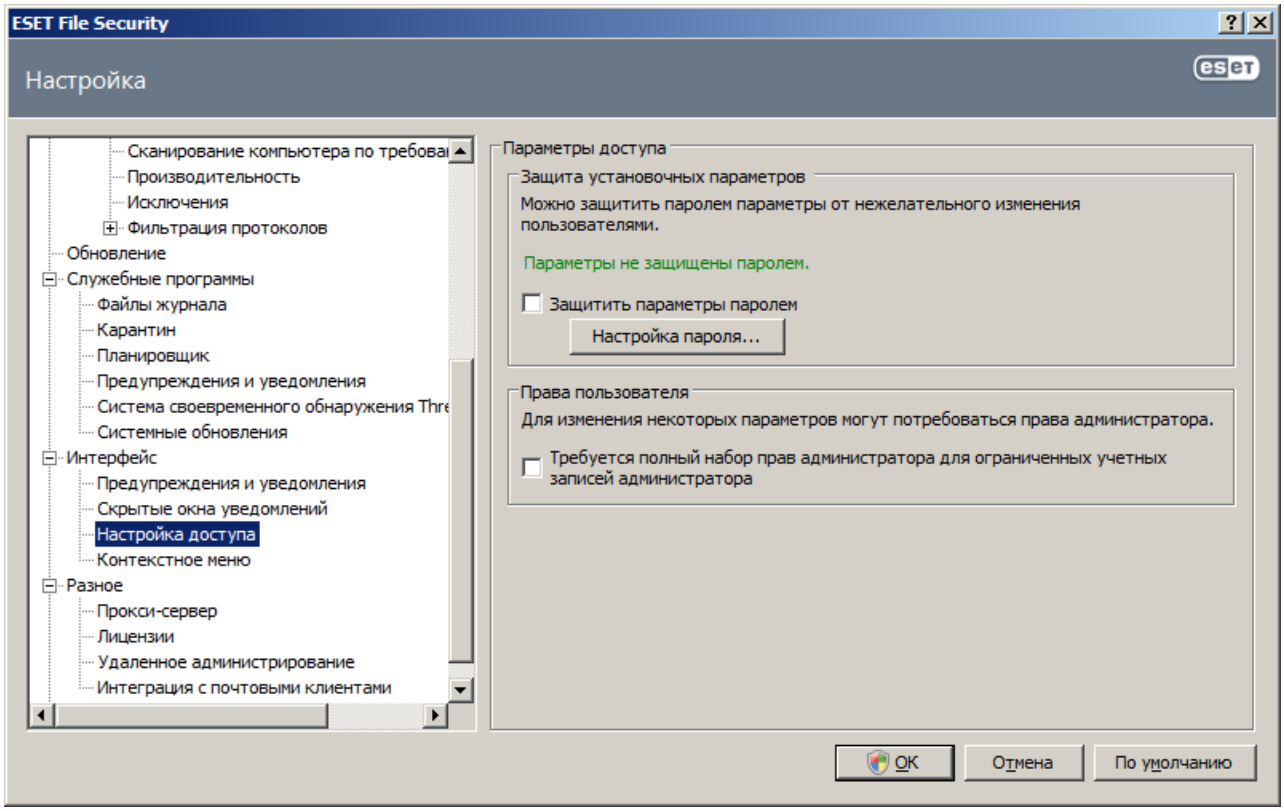
Если эта информация недоступна, можно попытаться автоматически обнаружить параметры прокси-сервера, нажав для этого кнопку **Найти прокси-сервер**.

ПРИМЕЧАНИЕ. Параметры прокси-сервера для различных профилей обновления могут различаться. В этом случае следует конфигурировать разные профили обновлений в разделе «Дополнительные настройки». Для этого следует нажать **Обновление** в дереве расширенных параметров.

3.4 Защита настроек

Параметры ESET File Security могут иметь большое значение с точки зрения политики безопасности организации. Несанкционированное изменение параметров способно нарушить стабильность работы системы и ослабить ее защиту. Для защиты параметров паролем в главном меню следует выбрать **Настройка** > **Ввод всего дерева расширенных параметров...** > **Интерфейс** > **Настройка доступа**, установить флажок **Параметры защищены паролем** и нажать кнопку **Настройка пароля...**.

Введите пароль в поля **Новый пароль** и **Подтвердить новый пароль** и нажмите кнопку **OK**. Этот пароль будет необходим в дальнейшем для внесения любых изменений в ESET File Security.



ПРИМЕЧАНИЕ: Нажмите эту ссылку, чтобы узнать, как данный параметр конфигурируется с помощью eShell.

4. Работа с ESET File Security

4.1 ESET File Security — защита сервера

ESET File Security обеспечивает защиту сервера за счет применения основных функций: защита от вирусов и шпионских программ, резидентная защита (защита в режиме реального времени), защита доступа в Интернет и защита почтового клиента. Дополнительные сведения о каждом из этих типов защиты доступны в разделе «ESET File Security, защита компьютера». Помимо этого, есть также функция, которая называется автоматические исключения. Эта функция выявляет критические файлы серверных приложений и серверной операционной системы и автоматически добавляет их в список Исключения. Это позволяет свести к минимуму риск возможных конфликтов и улучшить общую производительность сервера при работе программного обеспечения защиты от вирусов.

4.1.1 Автоматические исключения

Разработчики серверных приложений и операционных систем рекомендуют исключать наборы критических рабочих файлов и папок из антивирусного сканирования для большинства таких программных продуктов. Антивирусное сканирование может отрицательно повлиять на производительность сервера, привести к конфликтам и даже не дать некоторым приложениям работать на сервере. Исключения помогают свести к минимуму риск возможных конфликтов и улучшить общую производительность сервера при работе программного обеспечения защиты от вирусов.

ESET File Security выявляет критические файлы серверных приложений и серверных операционных система и автоматически добавляет их в список Исключения. После добавления в список серверный процесс или приложение может быть включено (по умолчанию) путем установки соответствующего флажка или же отключено его снятием. В результате ситуация будет развиваться следующим образом.

1) Если исключение для приложения или операционной системы остается активированным, все соответствующие критические файлы и папки будут добавлены в список файлов, исключенных из сканирования (**Дополнительные настройки** > **Защита компьютера** > **Защита от вирусов и шпионских программ** > **Исключения**). При каждом перезапуске сервера система автоматически проверяет исключения и восстанавливает все исключения, которые могли быть удалены из списка. Это рекомендуемая настройка, которая позволяет обеспечить постоянное применение рекомендованных автоматических исключений.

2) Если деактивировать исключение для приложения или операционной системы, соответствующие критические файлы и папки остаются в списке файлов, исключенных из сканирования (**Дополнительные настройки** > **Защита компьютера** > **Защита от вирусов и шпионских программ** > **Исключения**). Однако они не будут автоматически проверяться и восстанавливаться в списке **Исключения** при каждом перезапуске сервера (см. пункт 1 выше). Эту настройку рекомендуется применять только опытным пользователям, которым нужно удалить или изменить какие-либо из стандартных исключений. Если нужно удалить исключения из списка без перезапуска сервера, их следует удалить вручную (**Дополнительные настройки** > **Защита компьютера** > **Защита от вирусов и шпионских программ** > **Исключения)**.

Описанные выше настройки никак не влияют на любые пользовательские исключения, введенные вручную в разделе **Дополнительные настройки** > **Защита компьютера** > **Защита от вирусов и шпионских программ** > **Исключения**.

Автоматические исключения для серверных приложений и операционных систем выбираются на основе рекомендаций Microsoft. Для получения дополнительных сведений воспользуйтесь следующими ссылками.

http://support.microsoft.com/kb/822158
http://support.microsoft.com/kb/245822
http://support.microsoft.com/kb/823166
http://technet.microsoft.com/en-us/library/bb332342%28EXCHG.80%29.aspx
http://technet.microsoft.com/en-us/library/bb332342.aspx

4.2 ESET File Security - Защита компьютера

В ESET File Security есть все необходимые средства для обеспечения защиты сервера как компьютера. Этот программный продукт обеспечивает значительную защиту сервера, применяя следующие типы защиты: защита от вирусов и шпионских программ, резидентная защита (защита в режиме реального времени), защита доступа в Интернет и защита почтового клиента.

4.2.1 Защита от вирусов и шпионских программ

Защита от вирусов предотвращает вредоносные атаки на компьютер путем контроля файлов, электронной почты и связи через Интернет. Если обнаруживается содержащая злонамеренный код угроза, модуль защиты от вирусов может обезвредить ее, сначала заблокировав, а затем очистив, удалив или переместив на карантин.

4.2.1.1 Защита файловой системы в режиме реального времени

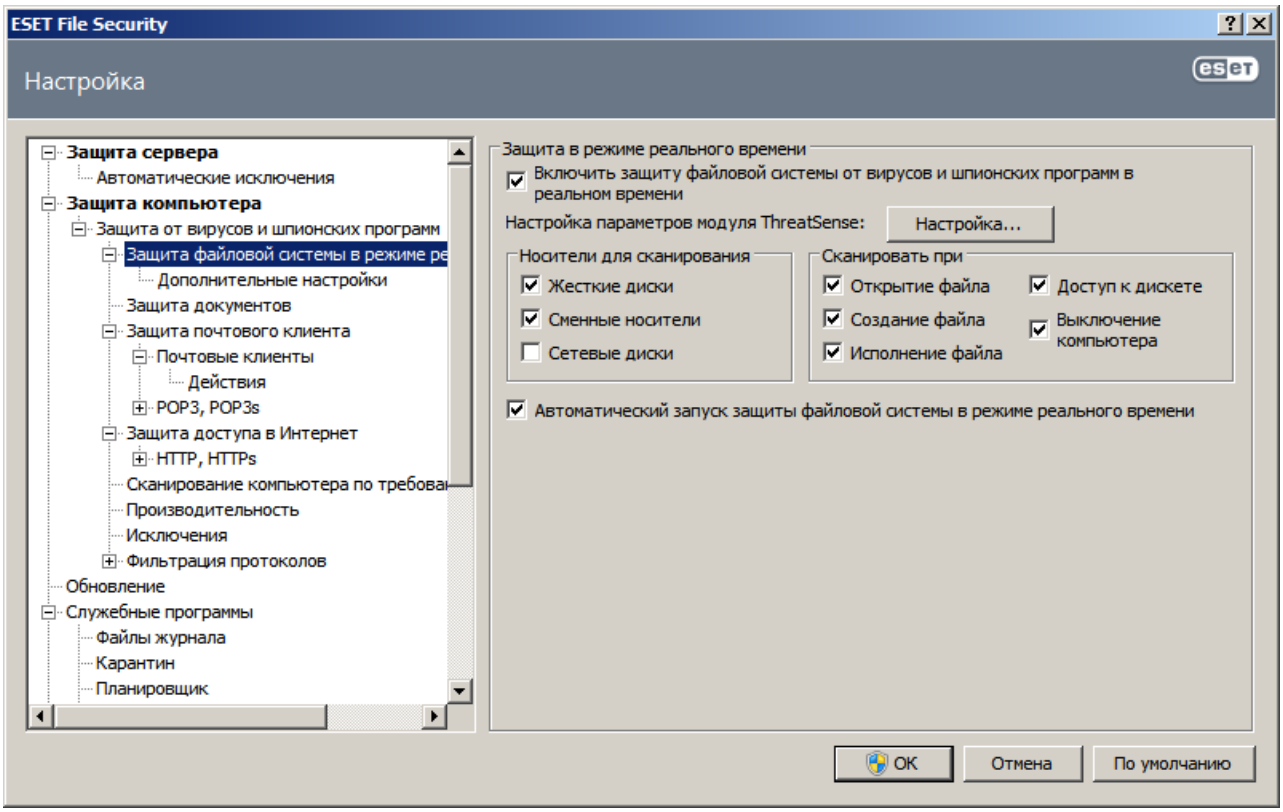
Защита файловой системы в режиме реального времени контролирует все события в системе, относящиеся к защите от вирусов. Все файлы сканируются на наличие злонамеренного кода в момент их открытия, создания или запуска. Защита файловой системы в режиме реального времени запускается при загрузке операционной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

4.2.1.1.1 Настройка управления

Защита файловой системы в режиме реального времени проверяет все типы носителей, причем контроль активируется различными событиями. За счет использования методов обнаружения ThreatSense (как описано в разделе Настройка параметров модуля ThreatSense) защита файловой системы в режиме реального времени может быть разной для вновь создаваемых и уже существующих файлов. Для вновь созданных файлов возможно применение более глубокого уровня контроля.

Для снижения влияния на производительность компьютера при использовании защиты в режиме реального времени файлы, которые уже сканировались, не сканируются повторно, пока не будут изменены. Файлы сканируются повторно сразу после каждого обновления базы данных сигнатур вирусов. Такое поведение конфигурируется с использованием оптимизации Smart. Если она отключена, все файлы сканируются каждый раз при доступе к ним. Для изменения этого параметра откройте окно «Дополнительные настройки» и нажмите **Защита от вирусов и шпионских программ** > **Защита файловой системы в режиме реального времени** в дереве расширенных параметров. Затем нажмите кнопку **Настройка...** рядом с пунктом **Настройка параметров модуля ThreatSense**, нажмите **Другое** и установите или снимите флажок **Включить оптимизацию Smart**.

По умолчанию защита в режиме реального времени запускается при загрузке системы и обеспечивает непрерывное сканирование. В особых случаях (например, в случае конфликта с другим модулем сканирования в режиме реального времени) защиту файловой системы в режиме реального времени можно отключить, сняв флажок **Автоматический запуск защиты файловой системы в режиме реального времени**.



4.2.1.1.1.1 Носители для сканирования

По умолчанию на наличие возможных угроз сканируются все типы носителей.

Жесткие диски: проверяются все жесткие диски, существующие в системе.

Съемные носители: дискеты, USB-устройства хранения и т. п.

Сетевые диски: сканируются все сопоставленные диски.

Рекомендуется оставить параметры по умолчанию, а изменять их только в особых случаях (например, если сканирование определенных носителей приводит к значительному замедлению обмена данными).

4.2.1.1.1.2 Сканировать при (сканирование по событию)

По умолчанию все файлы сканируются при открытии, создании или исполнении. Рекомендуется не изменять настройки по умолчанию, поскольку они обеспечивают максимальную защиту компьютера в режиме реального времени.

Параметр **Доступ к дискете** позволяет контролировать загрузочный сектор дискеты, когда открывается такой диск. Параметр **Выключение компьютера** обеспечивает проверку загрузочных секторов жесткого диска при выключении компьютера. Хотя загрузочные вирусы в настоящее время встречаются редко, рекомендуется оставить эти флажки установленными, так как по-прежнему существует вероятность заражения таким вирусом из альтернативного источника.

4.2.1.1.1.3 Расширенные параметры сканирования

Более подробную настройку можно выполнить в разделе **Защита компьютера** > **Защита от вирусов и шпионских программ** > **Защита в режиме реального времени** > **Дополнительные настройки**.

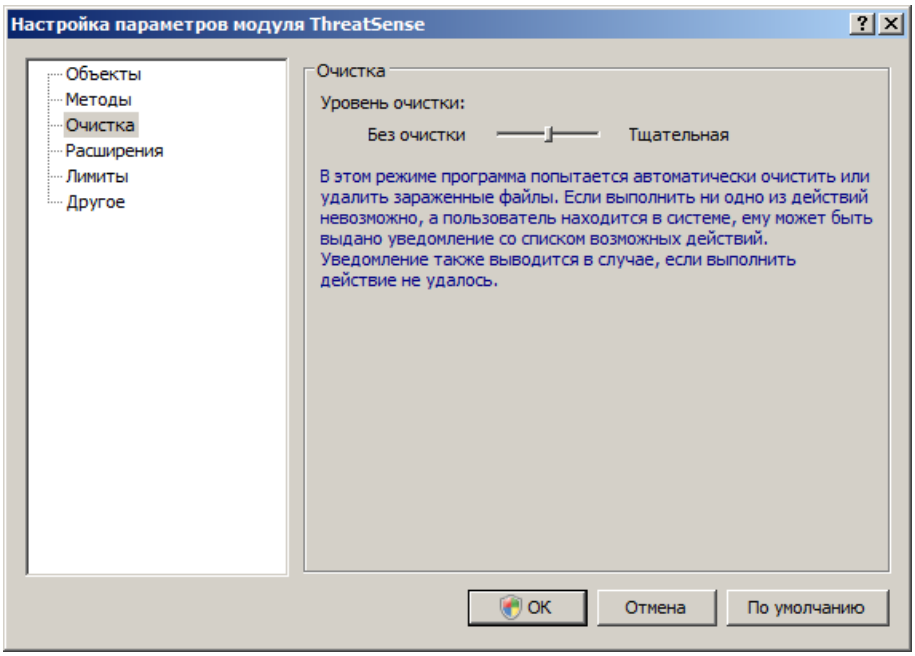
Дополнительные параметры модуля ThreatSense для новых и измененных файлов: вероятность заражения вновь созданных или измененных файлов выше по сравнению с существующими файлами. Именно поэтому программа проверяет эти файлы с дополнительными параметрами сканирования. Вместе с обычными методами сканирования, основанными на базе данных сигнатур вирусов, применяется расширенная эвристика, что значительно улучшает уровень обнаружения. В дополнение ко вновь созданным файлам выполняется также сканирование самораспаковывающихся файлов (.sfx) и упаковщиков (исполняемых файлов с внутренним сжатием). По умолчанию проверяются архивы с глубиной вложенности до 10 независимо от их фактического размера. Для изменения параметров сканирования архивов снимите флажок «Параметры сканирования архива по умолчанию».

Дополнительные параметры модуля ThreatSense.Net для исполняемых файлов: по умолчанию расширенная эвристика не применяется при исполнении файлов. Однако в некоторых случаев этот параметр может быть нужно включить (установив флажок **Расширенная эвристика запуска файлов**). Обратите внимание, что расширенная эвристика может замедлить выполнение некоторых программ из-за повышения системных требований.

4.2.1.1.2 Уровни очистки

Защита в режиме реального времени предусматривает три уровня очистки. Для выбора уровня очистки нажмите кнопку **Настройка...** в разделе **Защита файловой системы в режиме реального времени**, а затем выберите ветвь **Очистка**.

- При первом уровне, **Без очистки**, для каждого найденного заражения на экран выводится окно предупреждения с доступными для него действиями. Пользователь должен выбрать действие для каждого заражения отдельно. Этот уровень предназначен для более опытных пользователей, которые знают о действиях, которые следует предпринимать в случае заражения.
- При уровне по умолчанию автоматически выбирается и выполняется предварительно определенное действие (в зависимости от типа заражения). Обнаружение и удаление зараженных файлов сопровождается сообщением, выводимым в правом нижнем углу экрана. Автоматические действия не выполняются при обнаружении заражения в архиве (в котором также содержатся незараженные файлы), а также в случаях, когда для зараженных объектов нет предварительно заданного действия.
- Третий уровень, **Тщательная очистка**, является наиболее агрессивным: все зараженные объекты очищаются. Так как использование этого уровня может привести к потере нужных файлов, рекомендуется использовать его только в особых случаях.



4.2.1.1.3 Момент изменения конфигурации защиты в режиме реального времени

Защита в режиме реального времени является самой важной составляющей, необходимой для обеспечения безопасности компьютера. Поэтому необходимо быть внимательным при изменении ее параметров. Рекомендуется изменять параметры 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 ESET File Security все параметры оптимизированы для обеспечения максимального уровня безопасности системы для пользователей. Для восстановления параметров по умолчанию нажмите кнопку **По умолчанию**, расположенную в правом нижнем углу окна **Защита файловой системы в режиме реального времени** (**Дополнительные настройки** > **Защита от вирусов и шпионских программ** > **Защита файловой системы в режиме реального времени**).

4.2.1.1.4 Проверка защиты в режиме реального времени

Для проверки того, что защита в режиме реального времени действительно работает и обнаруживает вирусы, используйте проверочный файл eicar.com. Это специальный безвредный тестовый файл, который обнаруживается всеми программами защиты от вирусов. Файл создан компанией EICAR (Европейский институт антивирусных компьютерных исследований) для проверки функционирования программ защиты от вирусов. Файл eicar.com доступен для загрузки с веб-сайта http://www.eicar.org/download/eicar.com.

ПРИМЕЧАНИЕ. Перед осуществлением проверки защиты в режиме реального времени необходимо отключить файервол. Если файервол включен, он обнаружит данный файл и предотвратит его загрузку.

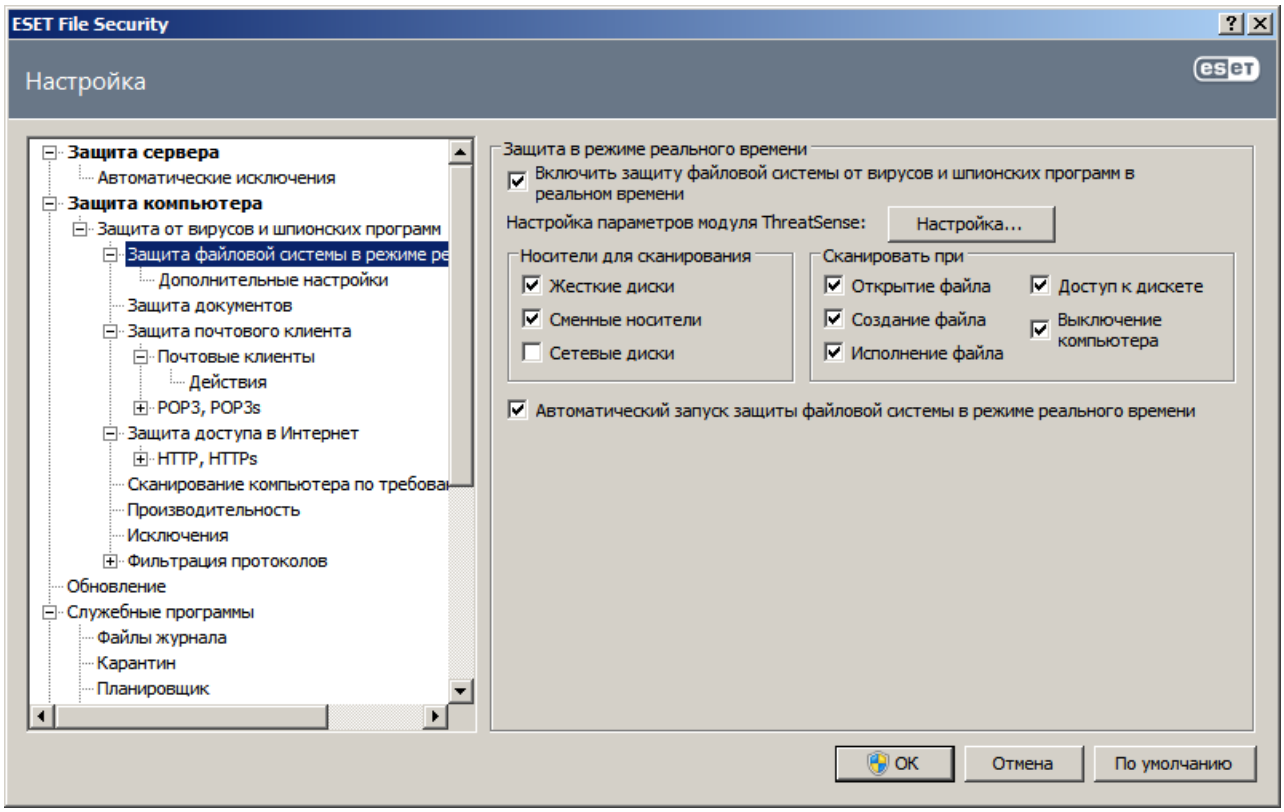
4.2.1.1.5 Решение проблем, возникающих при работе защиты файловой системы в режиме реального времени

В следующей главе рассказывается о проблемах, которые могут возникать при работе защиты в режиме реального времени, и о том, как их устранить.

Защита файловой системы в режиме реального времени отключена

Если защита в режиме реального времени непреднамеренно была отключена пользователем, ее нужно повторно активировать. Чтобы повторно активировать защиту файловой системы в режиме реального времени, в главном окне программы перейдите в раздел **Настройка** > **Защита от вирусов и шпионских программ** и щелкните ссылку **Включить защиту файловой системы в режиме реального времени**.

Если защита файловой системы в режиме реального времени не запускается при загрузке операционной системы, возможно, снят флажок **Автоматический запуск защиты файловой системы в режиме реального времени**. Чтобы установить этот флажок, перейдите в раздел «Дополнительные настройки» (F5) и нажмите **Защита файловой системы в режиме реального времени** в дереве расширенных параметров. Проверьте, что в разделе **Дополнительные настройки** в нижней части этого окна установлен флажок **Автоматический запуск защиты файловой системы в режиме реального времени**.



Защита в режиме реального времени не обнаруживает и не очищает заражения

Убедитесь в том, что на компьютере не установлены другие программы защиты от вирусов. При одновременной работе двух систем защиты в режиме реального времени могут возникнуть конфликты. Рекомендуется удалить все прочие программы защиты от вирусов с компьютера.

Защита в режиме реального времени на запускается

Если защита в режиме реального времени не запускается при загрузке операционной системы, но флажок

Автоматический запуск защиты файловой системы в режиме реального времени установлен, возможно, возник конфликт с другими программами. В этом случае обратитесь за консультацией к специалистам службы поддержки клиентов ESET.

4.2.1.2 Защита почтового клиента

Защита электронной почты обеспечивает контроль обмена данными по электронной почте через протокол POP3. При использовании подключаемого модуля для Microsoft Outlook ESET File Security позволяет контролировать весь обмен данными, осуществляемый почтовым клиентом (по протоколам POP3, MAPI, IMAP, HTTP).

При проверке входящих сообщений программа использует все современные методы сканирования, обеспечиваемые модулем сканирования ThreatSense. Это позволяет обнаруживать вредоносные программы даже до того, как данные о них попадают в базу данных сигнатур вирусов. Сканирование соединений по протоколу POP3 не зависит от используемого почтового клиента.

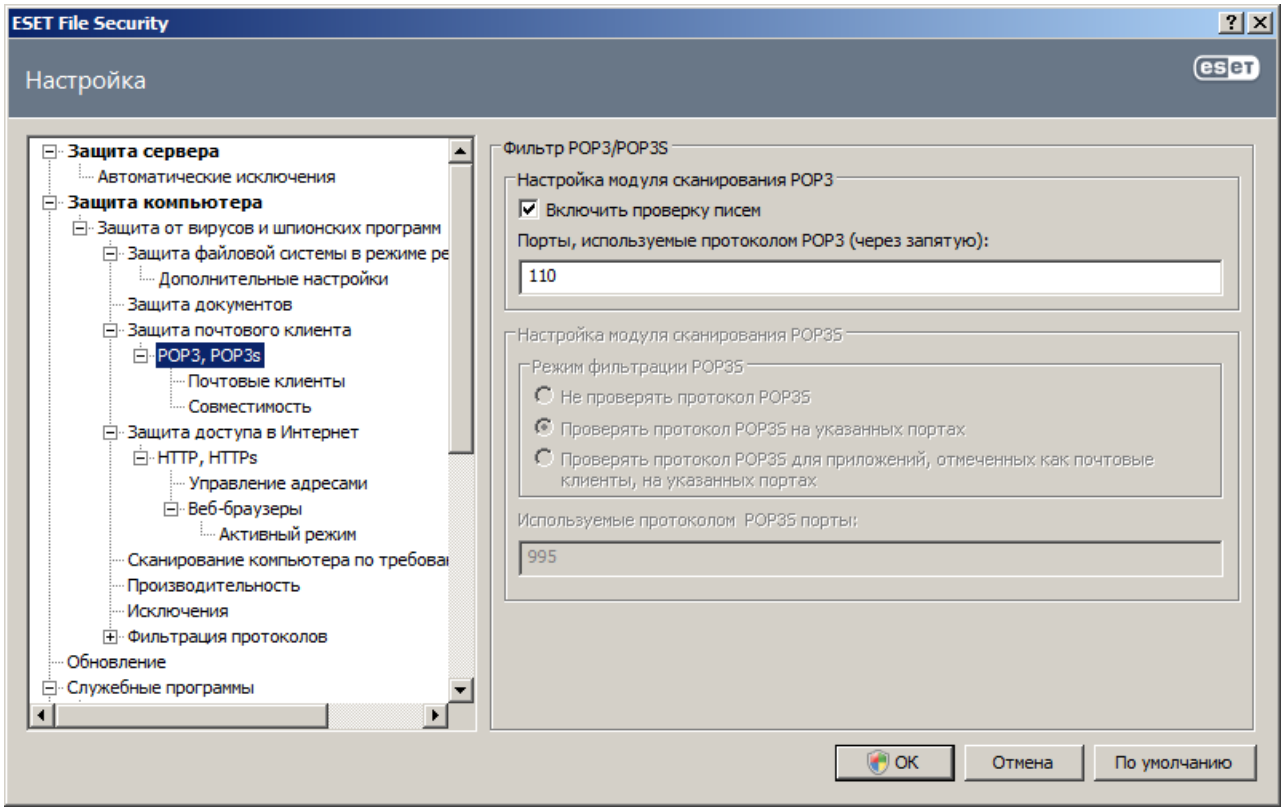
4.2.1.2.1 Проверка POP3

POP3 — самый распространенный протокол, используемый для получения электронной почты в почтовых клиентах. ESET File Security обеспечивает защиту этого протокола вне зависимости от используемого почтового клиента.

Модуль защиты, обеспечивающий эту функцию, автоматически инициируется при запуске операционной системы и остается активным в оперативной памяти. Для нормальной работы модуля убедитесь в том, что он включен. Проверка протокола POP3 осуществляется автоматически без необходимости в какой-либо дополнительной настройке конкретного почтового клиента. По умолчанию сканируются все соединения по порту 110, однако при необходимости могут быть добавлены и другие порты. Номера портов следует разделять запятыми.

Зашифрованное соединение не проверяется.

Для использования фильтрации протокола POP3/POP3S сначала нужно включить фильтрацию протоколов. Если параметры POP3/POP3S недоступны, перейдите в раздел **Защита компьютера** > **Защита от вирусов и шпионских программ** > **Фильтрация протоколов** из дерева расширенных параметров и установите флажок **Включить фильтрацию содержимого протоколов приложений**. Дополнительные сведения о фильтрации и конфигурации см. раздел Фильтрация протоколов.



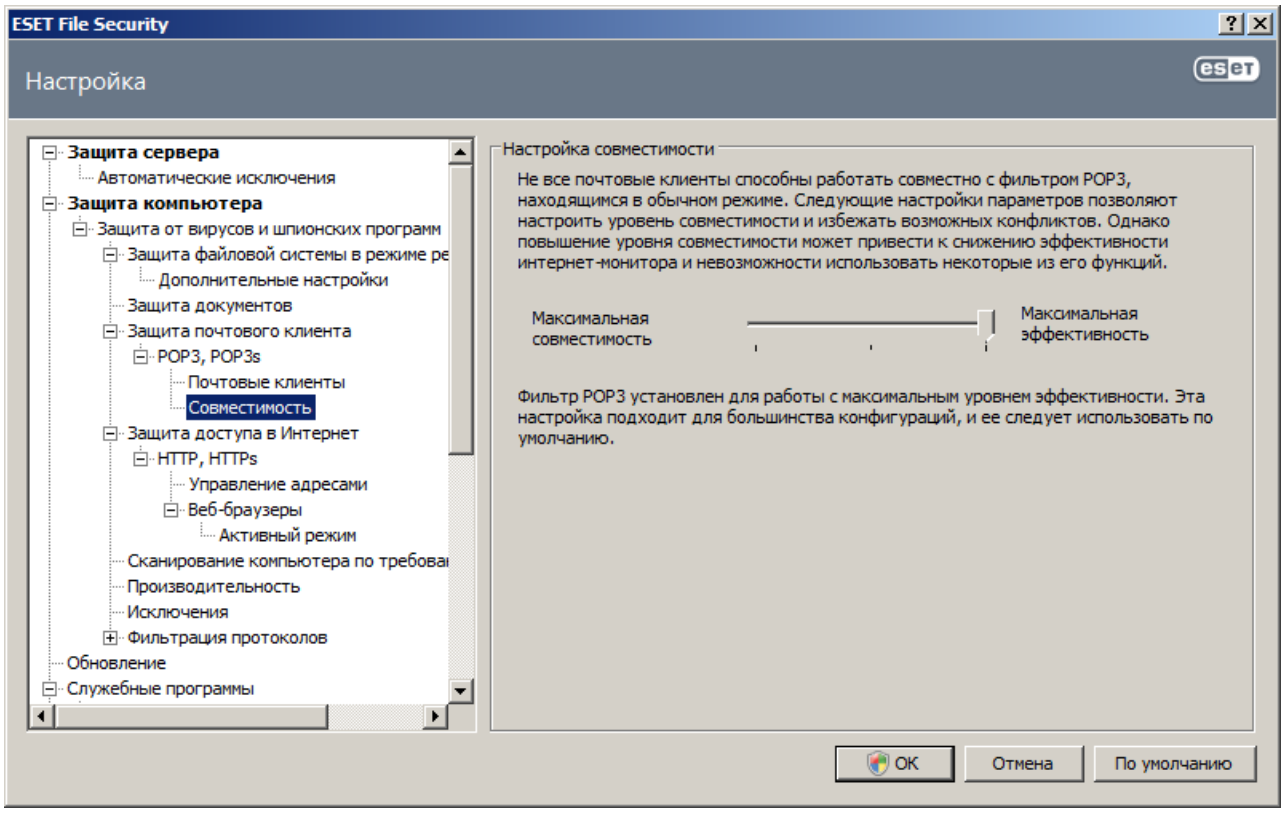
4.2.1.2.1.1 Совместимость

В некоторых программах для работы с электронной почтой могут возникать проблемы с фильтрацией POP3 (например, при медленном соединении с сервером в процессе получения сообщений могут возникать ошибки времени ожидания). В этом случае попробуйте изменить способ контроля трафика. Снижение уровня контроля может улучшить скорость процесса очистки. Для настройки уровня контроля при фильтрации POP3 из дерева расширенных параметров перейдите в раздел **Защита от вирусов и шпионских программ** > **Защита электронной почты** > **POP3, POP3s** > **Совместимость**.

Если используется вариант **Максимальная эффективность**, заражения удаляются из зараженных сообщений, а перед исходной темой сообщения вставляется информация о заражении (должен быть активирован вариант **Удалить** или **Очистить** или использоваться уровень очистки **Тщательная** или **По умолчанию**).

Режим **средней совместимости** изменяет способ получения сообщений. Сообщение постепенно отправляются в почтовый клиент. После передачи сообщения оно сканируется для выявления заражений. Однако при использовании такого уровня контроля возрастает риск заражения. Уровень очистки и применение уведомлений (текстовой информации, прикрепляемой к теме или телу сообщений) остаются теми же, что и для режима максимальной эффективности.

В режиме **максимальной совместимости** на экран выводится окно предупреждения, в котором пользователь информируется о получении зараженного сообщения. Никакая информация о зараженных файлах не добавляется в тему или тело доставленных сообщений, а заражения не удаляются автоматически (удалять их нужно в почтовом клиенте).

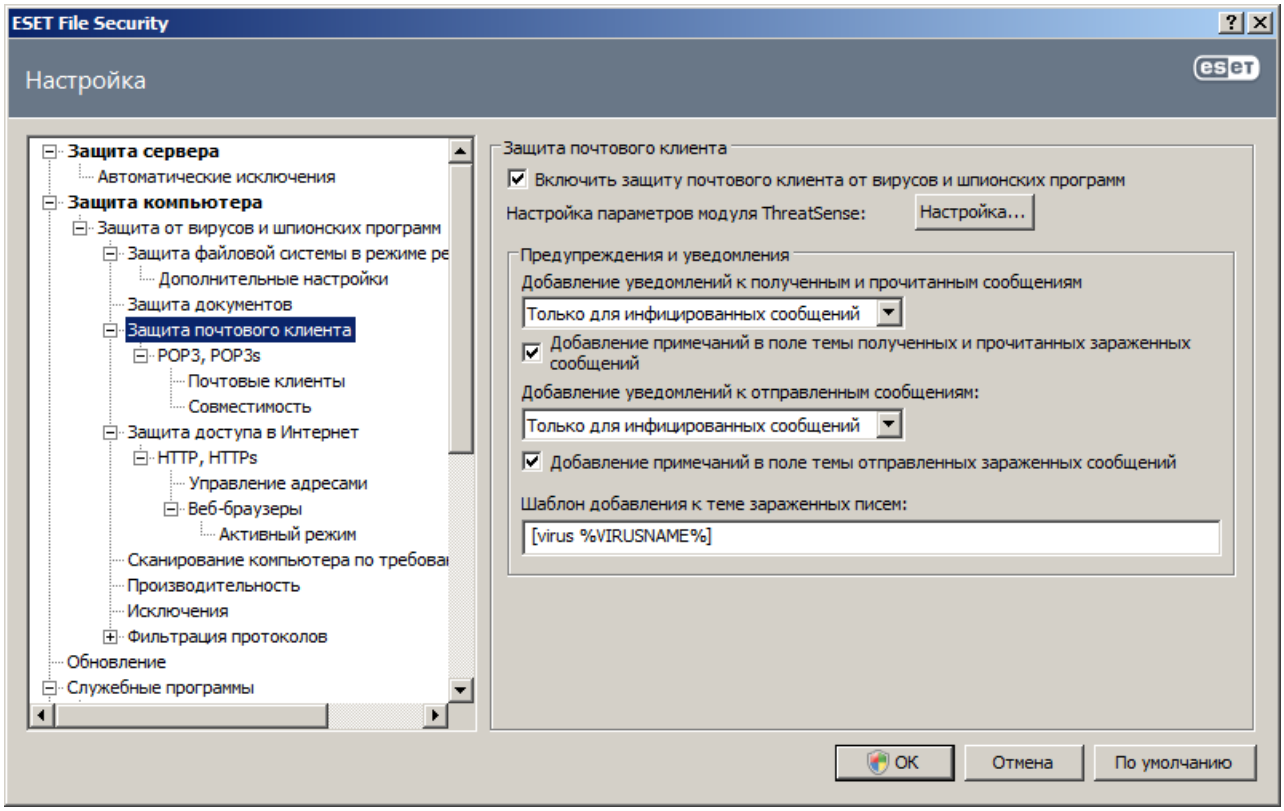


4.2.1.2.2 Интеграция с почтовыми клиентами

Интеграция ESET File Security с почтовыми клиентами увеличивает уровень активной защиты от вредоносного кода в сообщениях электронной почты. Если используемый почтовый клиент поддерживается, такую интеграцию можно настроить в ESET File Security. Если интеграция активирована, панель инструментов защиты от спама ESET File Security вставляется непосредственно в почтовый клиент, обеспечивая более эффективную защиту электронной почты. Параметры интеграции доступны в разделе **Настройка** > **Ввод всего дерева расширенных параметров...** > **Разное** > **Интеграция с почтовыми клиентами**. Интеграция с почтовыми клиентами позволяет активировать интеграцию с поддерживаемыми почтовыми клиентами. В настоящий момент поддерживаются следующие почтовые клиенты: Microsoft Outlook, Outlook Express, почта Windows, почта Windows Live и Mozilla Thunderbird.

Установите флажок **Отключить проверку при изменении содержимого папки "Входящие"**, если при работе с почтовым клиентом наблюдается замедление работы системы. Такая ситуация может возникнуть при загрузке электронной почты из Kerio Outlook Connector Store.

Защита электронной почты активируется в разделе **Настройка** > **Ввод всего дерева расширенных параметров...** > **Защита от вирусов и шпионских программ** > **Защита почтового клиента**, где нужно выбрать вариант **Включить защиту почтового клиента от вирусов и шпионских программ**.



4.2.1.2.2.1 Добавление уведомлений в тело сообщения электронной почты

Каждое сообщение электронной почты, просканированное ESET File Security, может быть помечено путем добавления уведомления в тему или тело сообщения. Эта функция повышает уровень доверия для получателя, а в случае обнаружения заражения предоставляет важную информацию об уровне угрозы для конкретного сообщения или отправителя.

Параметры для этой функции настраиваются в разделе **Дополнительные настройки** > **Защита от вирусов и шпионских программ** > **Защита почтового клиента**. Можно выбрать вариант **Добавление уведомлений к полученным и прочитанным сообщениям**, а также **Добавление уведомлений к отправленным сообщениям** . Также можно решить, следует ли добавлять уведомления ко всем просканированным сообщениям электронной почты, только к зараженным сообщениям или же не добавлять их вовсе.

ESET File Security также позволяет добавлять сообщения к исходной теме зараженного сообщения. Для активации добавления к теме установите и флажок **Добавление примечаний в поле темы полученных и прочитанных зараженных сообщений**, и флажок **Добавление примечаний в поле темы отправленных зараженных сообщений**.

Содержимое уведомлений можно изменять в поле **Шаблон добавления к теме зараженных писем**. Описанные выше изменения могут помочь автоматизировать процесс фильтрации зараженных сообщений, а также позволяют помещать сообщения с определенной темой (если эта функция поддерживается используемым почтовым клиентом) в отдельную папку.

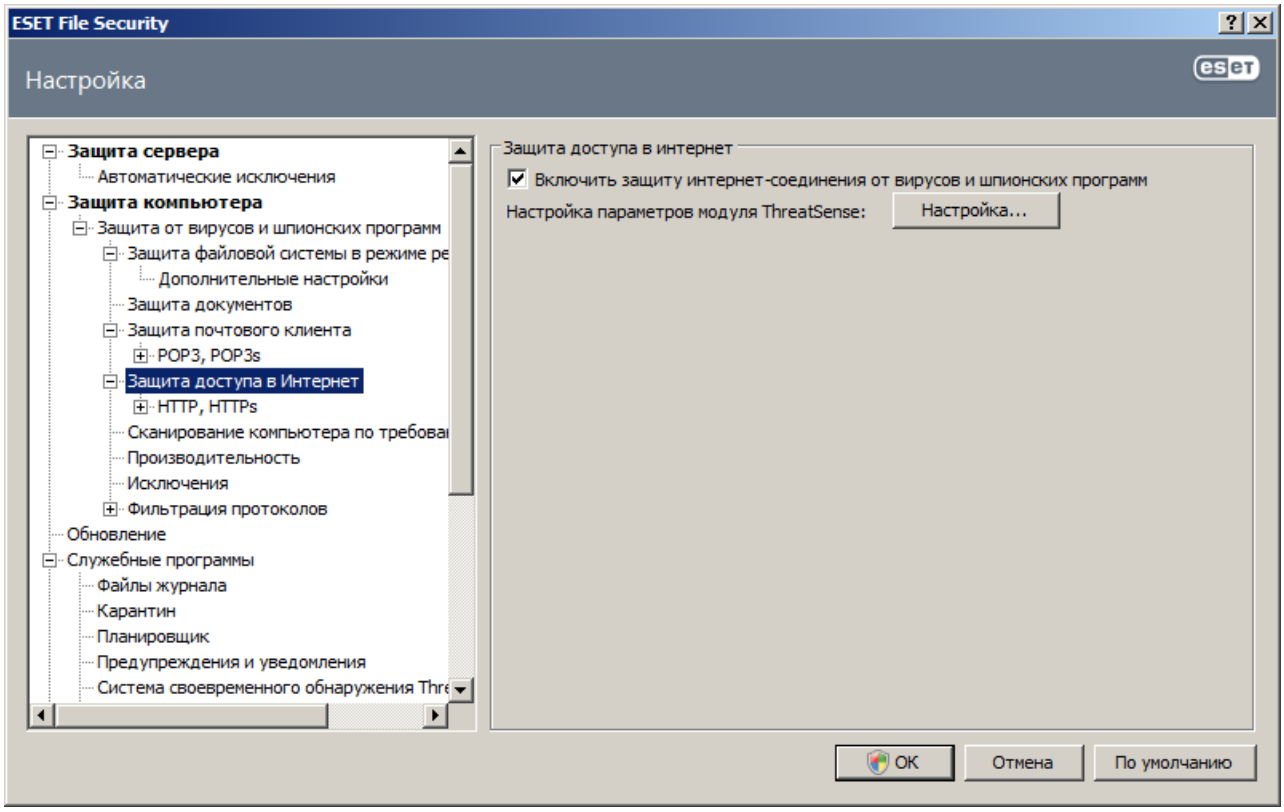
4.2.1.2.3 Удаление заражений

При получении зараженного сообщения электронной почты на экран выводится окно предупреждения. В этом окне содержатся имя отправителя, адрес его электронной почты и название заражения. В нижней части окна доступны варианты действий для обнаруженного объекта: **Очистить**, **Удалить** или **Пропустить**. Почти во всех случаях рекомендуется выбирать **Очистить** или **Удалить**. В некоторых ситуациях, если нужно получить зараженный файл, можно выбрать **Пропустить**.

Если включена **тщательная очистка**, на экран будет выведено информационное окно, в котором нельзя выбрать какое-либо действие.

4.2.1.3 Защита доступа в Интернет

Подключение к Интернету стало стандартной функцией персонального компьютера. К сожалению, Интернет также стал и основной средой распространения злонамеренного кода. Поэтому принципиально важно уделить особое внимание защите доступа в Интернет. Настоятельно рекомендуется установить флажок **Включить защиту интернет-соединения от вирусов и шпионских программ**. Этот параметр находится в разделе **Дополнительные настройки** (F5) > **Защита от вирусов и шпионских программ** > **Защита доступа в Интернет**.

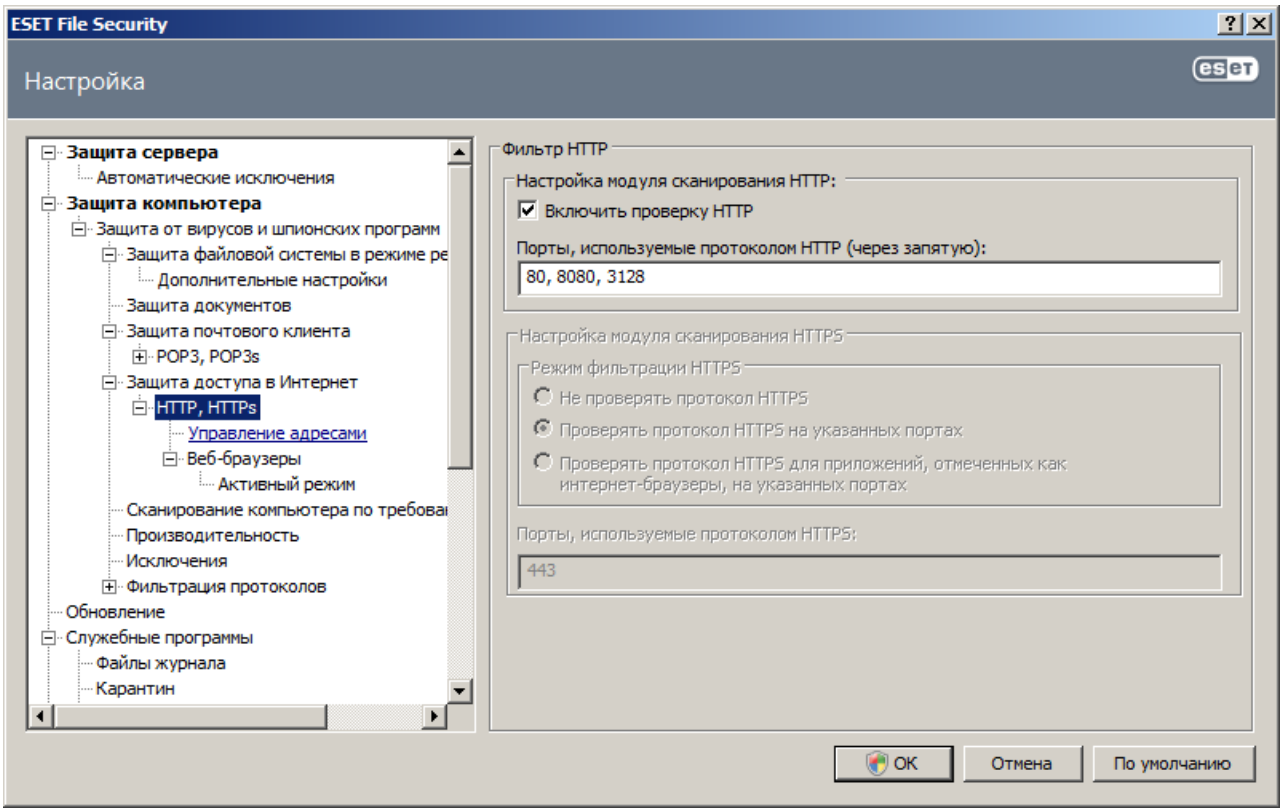


4.2.1.3.1 HTTP, HTTPs

Защита доступа в Интернет работает путем отслеживания соединений между веб-браузерами и удаленными серверами в соответствии с правилами протоколов HTTP и HTTPS. По умолчанию программа ESET File Security сконфигурирована на использование стандартов большинства веб-браузеров. Однако параметры модуля сканирования HTTP можно изменить в разделе **Дополнительные настройки** (F5) > **Защита от вирусов и шпионских программ** > **Защита доступа в Интернет** > **HTTP, HTTPS**. В главном окне фильтрации HTTP можно установить или снять флажок **Включить проверку HTTP**. Также можно указать номера портов, используемых для передачи данных по протоколу HTTP. По умолчанию предварительно заданы номера портов 80, 8080 и 3128. Проверка HTTPs может выполняться в следующих режимах.

Не проверять протокол HTTPS: зашифрованные соединения не будут проверяться.

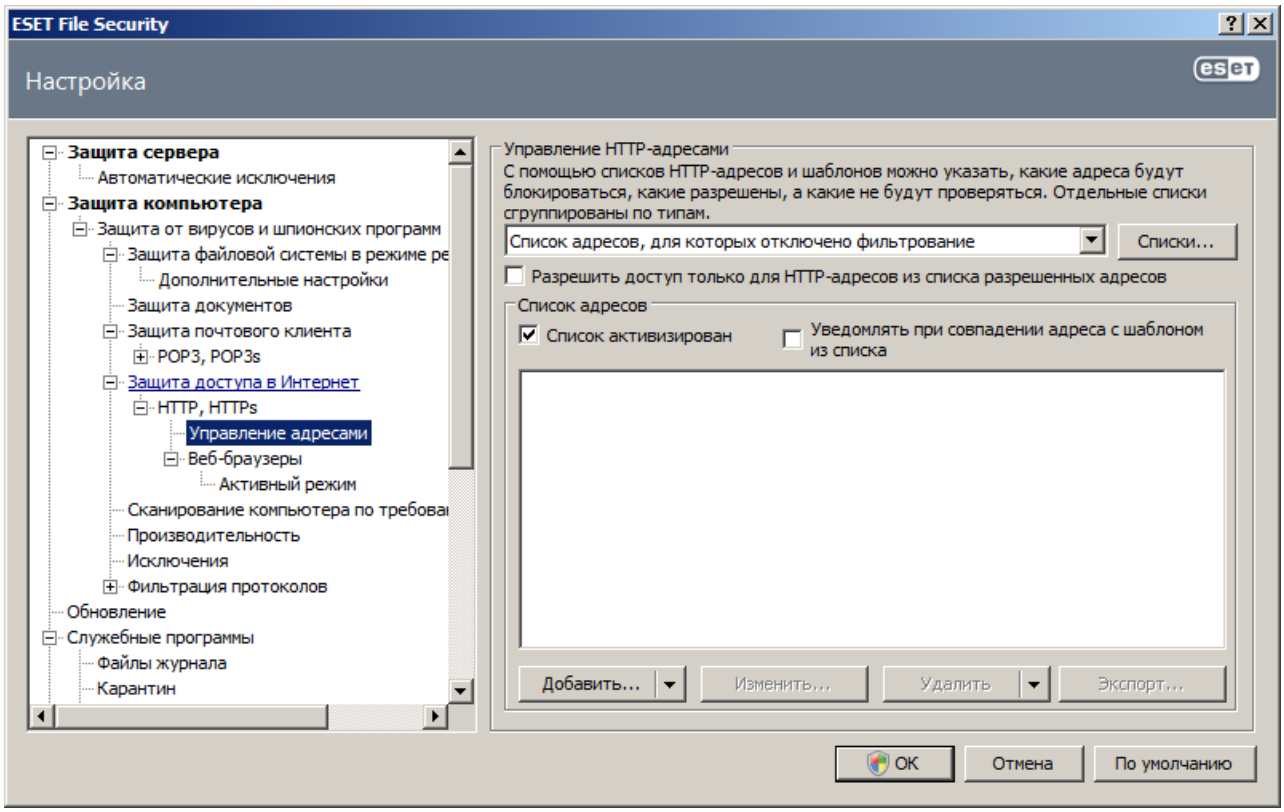
Проверять протокол HTTPs для выбранных портов: проверка протокола HTTPs выполняется только для портов, указанных в параметре **Порты, используемые протоколом HTTPS**.



4.2.1.3.1.1 Управление адресами

В этом разделе можно задавать HTTP-адреса, которые будут блокироваться, разрешаться или исключаться из проверки. Кнопки **Добавить...**, **Изменить...**, **Удалить** и **Экспорт...** позволяют управлять списками адресов. Веб-сайты из списка заблокированных адресов будут недоступны. Веб-сайты из списка исключенных адресов загружаются без сканирования на наличие вредоносного кода. Если выбрать вариант **Разрешить доступ только для HTTP-адресов из списка разрешенных адресов**, будут доступны только адреса из списка разрешенных, а остальные HTTP-адреса будут заблокированы.

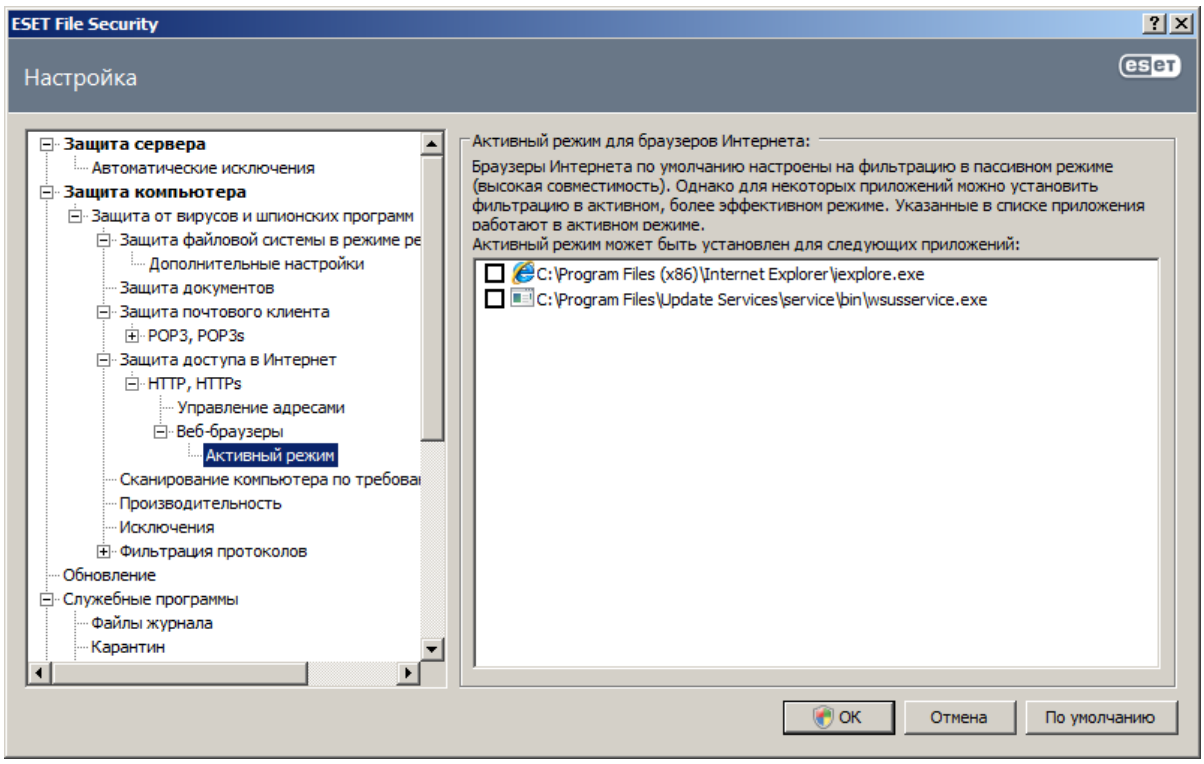
Во всех списках можно использовать символы шаблона «*» (звездочка) и «?» (вопросительный знак). Символ звездочки обозначает любую последовательность символов, а вопросительный знак — любой символ. Работать с содержимым списка исключенных адресов следует особенно аккуратно, так как он должен содержать только доверенные и безопасные адреса. Точно так же нужно убедиться в том, что символы шаблона в этом списке используются правильно. Чтобы активировать список, установите флажок **Список активизирован**. Для получения уведомлений при загрузке адреса из текущего списка установите флажок **Уведомлять при применении адреса из списка**.



4.2.1.3.1.2 Активный режим

Перечень приложений, помеченных в качестве веб-браузеров, можно просмотреть непосредственно в подменю **Веб-браузеры** ветви **HTTP, HTTPs**. В этом разделе также есть подменю **Активный режим**, которое определяет режим проверки для веб-браузеров.

Функция **Активный режим** удобна, так как позволяет проверять все передаваемые данные в целом. Если она отключена, соединения приложений отслеживаются частями в пакетном режиме. Это снижает эффективность процесса проверки данных, но при этом обеспечивает лучшую совместимость для перечисленных приложений. Если при использовании функции не возникает проблем, рекомендуется включить активный режим проверки, установив флажок рядом с нужным приложением.



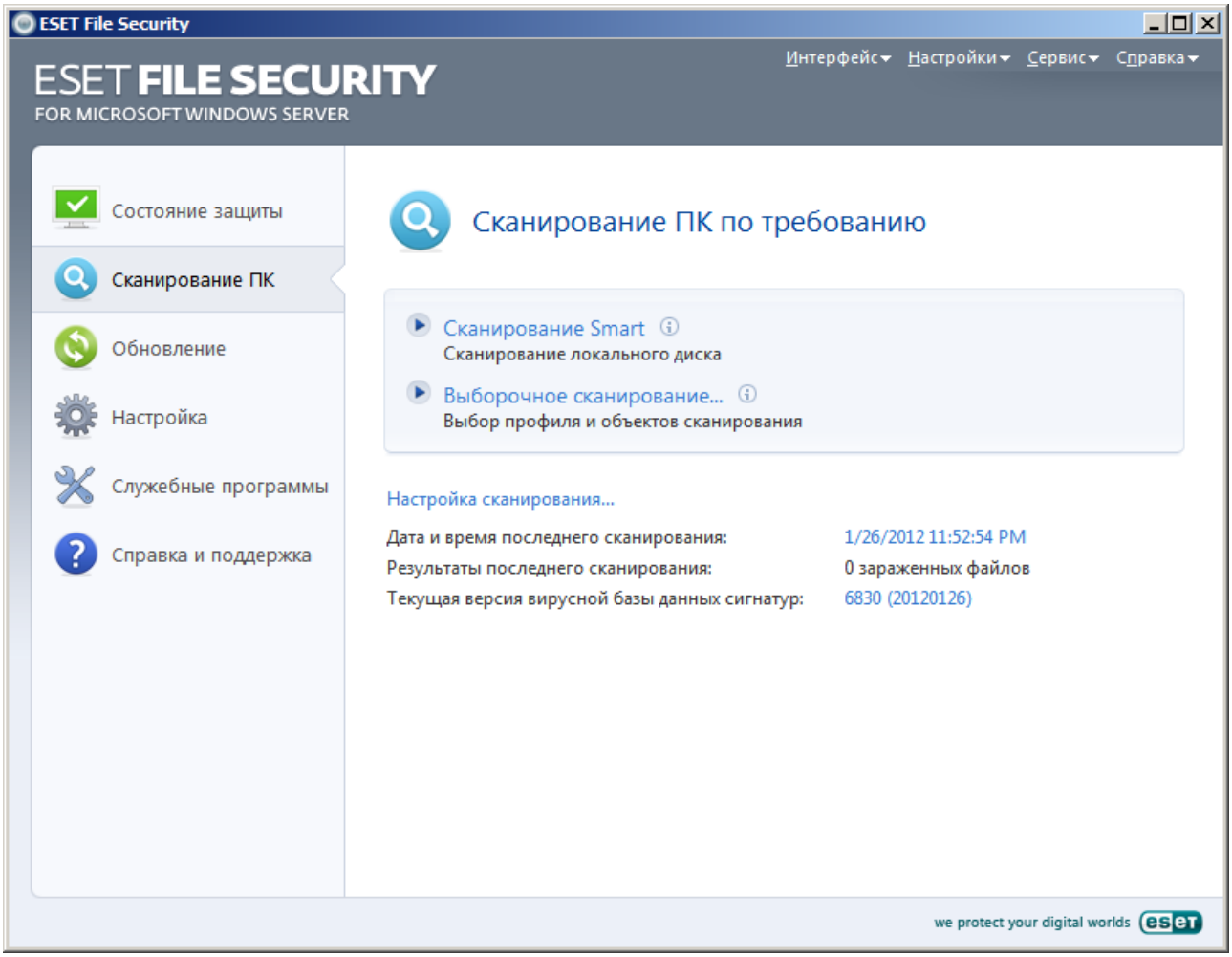
4.2.1.4 Сканирование ПК по требованию

При наличии подозрения, что компьютер заражен (необычное поведение и т. п.), следует выполнить сканирование компьютера по требованию для проверки наличия заражений. С точки зрения обеспечения безопасности принципиально важно выполнять сканирование компьютера регулярно, а не только при возникновении подозрений. Регулярное сканирование позволяет обнаружить заражения, пропущенные модулем сканирования в режиме реального времени при их записи на диск. Это может произойти, если модуль сканирования в режиме реального времени был отключен или использовалась устаревшая база данных сигнатур вирусов.

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

4.2.1.4.1 Тип сканирования

Существует два типа сканирования компьютера по требованию. **Сканирование Smart** позволяет быстро просканировать систему без настройки каких-либо параметров. **Выборочное сканирование...** дает возможность выбрать любой предопределенный профиль сканирования, а также указать конкретные объекты сканирования.



4.2.1.4.1.1 Сканирование Smart

Сканирование Smart позволяет быстро запустить сканирование компьютера и очистить зараженные файлы без вмешательства пользователя. Главным преимуществом этого метода является простота использования без подробной настройки сканирования. При сканировании Smart проверяются все файлы на локальных дисках и автоматически очищаются или удаляются обнаруженные заражения. В качестве уровня очистки автоматически выбран уровень по умолчанию. Дополнительную информацию о типах очистки см. в разделе Очистка.

4.2.1.4.1.2 Выборочное сканирование

Выборочное сканирование является оптимальным решением в том случае, когда нужно указать параметры сканирования, такие как объекты и методы сканирования. Преимуществом выборочного сканирования является возможность подробного конфигурирования параметров. Конфигурации можно сохранять в виде пользовательских профилей сканирования, которые удобно использовать, если регулярно выполняется сканирование с одними и теми же параметрами.

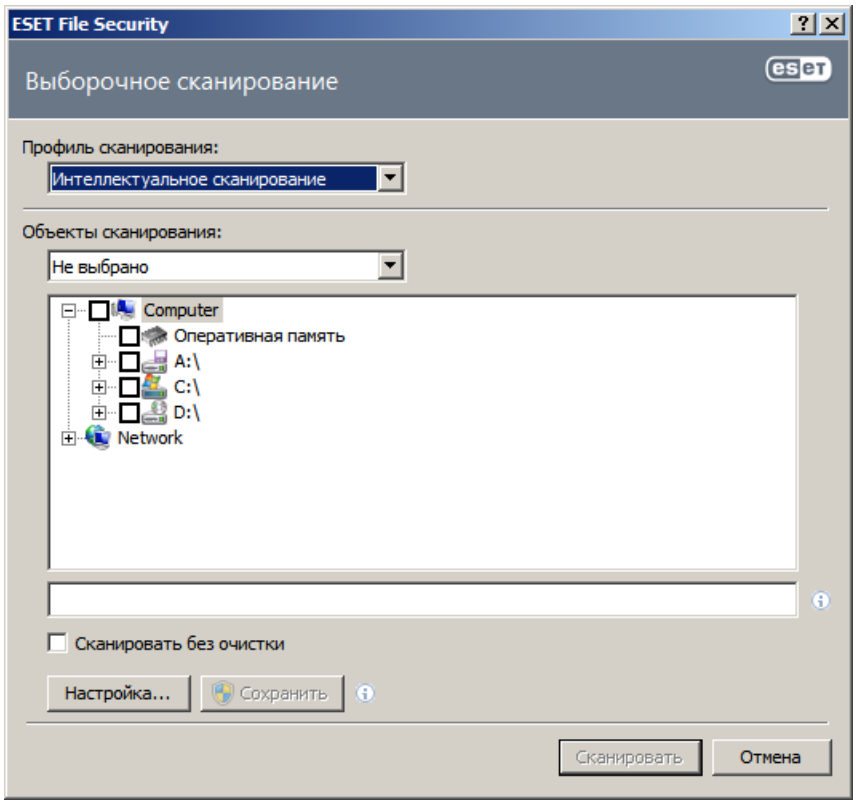
Для выбора объектов сканирования перейдите в раздел **Сканирование компьютера** > **Выборочное сканирование** и выберите один из вариантов из раскрывающегося меню **Объекты сканирования** или конкретные объекты сканирования в древовидной структуре. Объекты сканирования также можно задать более точно, указав пути к папкам и файлам, которые нужно сканировать. Если нужно только выполнить сканирование системы без дополнительных действий по очистке, установите флажок **Сканировать без очистки**. Кроме того, можно выбрать один из трех уровней очистки в разделе **Настройка...** > **Очистка**.

4.2.1.4.2 Объекты сканирования

В раскрывающемся меню объектов сканирования можно выбрать файлы, папки и устройства (диски), которые нужно сканировать на наличие вирусов.

По параметрам профиля : выбираются объекты, заданные в данном профиле сканирования.
Съемные носители : выбираются дискеты, USB-устройства хранения, компакт- и DVD-диски.
Жесткие диски : выбираются все жесткие диски, существующие в системе.
Сетевые диски : выбираются все подключенные сетевые диски.
Ничего не выбирать: отменяется выбор объектов.

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

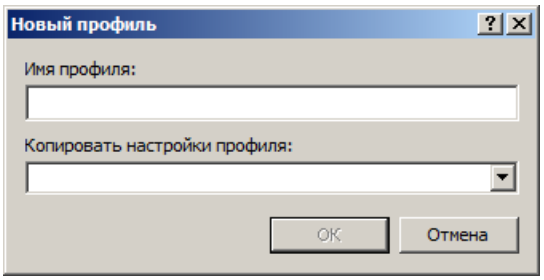


4.2.1.4.3 Профили сканирования

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

Для создания нового профиля откройте окно «Дополнительные настройки» (F5) и нажмите **Сканирование ПК по требованию** > **Профили...** В окне **Профили конфигурации** есть раскрывающееся меню, в котором перечисляются существующие профили сканирования, а также есть возможность создать новый. Для создания профиля сканирования в соответствии с конкретными потребностями см. раздел Настройка параметров модуля ThreatSense, где описывается каждый параметр, используемый для настройки сканирования.

ПРИМЕР. Предположим, пользователю требуется создать собственный профиль сканирования, причем конфигурация сканирования Smart частично устраивает его, но не нужно сканировать упаковщики или потенциально опасные приложения, но при этом нужно применить **тщательную очистку**. В окне **Профили конфигурации** нажмите кнопку **Добавить...**. Введите имя создаваемого профиля в поле **Имя профиля**, а затем выберите **Сканирование Smart** в раскрывающемся меню **Копировать настройки профиля**. Затем настройте остальные параметры в соответствии со своими потребностями.



4.2.1.4.4 Командная строка

Модуль защиты от вирусов программного обеспечения ESET File Security может быть запущен из командной строки вручную (с помощью команды «ecls») или в пакетном режиме (с помощью файла «bat»).

Следующие параметры и аргументы могут быть использованы при запуске сканирования по требованию из командной строки.

Общие параметры

- help	показать справку и выйти
- version	показать сведения о версии и выйти
- base-dir = ПАПКА	загрузить модули из ПАПКИ
- quar-dir = ПАПКА	ПАПКА карантина
- aind	показывать индикатор работы

Объекты

- files	сканировать файлы (по умолчанию)
- no-files	не сканировать файлы
- boots	сканировать загрузочные секторы (по умолчанию)
- no-boots	не сканировать загрузочные секторы
- arch	сканировать архивы (по умолчанию)
- no-arch	не сканировать архивы
- max-archive-level = УРОВЕНЬ	максимальный УРОВЕНЬ вложенности архивов
- scan-timeout = ИНТЕРВАЛ	сканировать архивы не дольше указанного ИНТЕРВАЛА в секундах. При достижении этого предельного значения сканирование архива останавливается, а сам процесс переходит к следующему файлу.
- max-arch-size=РАЗМЕР	сканировать только первый кусок файла РАЗМЕРОМ в байтах (по умолчанию 0 = не ограничено)
- mail	сканировать файлы электронной почты
- no-mail	не сканировать файлы электронной почты
- sfx	сканировать самораспаковывающиеся архивы
- no-sfx	не сканировать самораспаковывающиеся архивы
- rtp	сканировать упаковщики
- no-rtp	не сканировать упаковщики
- exclude = ПАПКА	исключить ПАПКУ из сканирования
- subdir	сканировать вложенные папки (по умолчанию)

- no-subdir	не сканировать вложенные папки
- max-subdir-level = УРОВЕНЬ	максимальный УРОВЕНЬ вложенности папок (по умолчанию 0 = не ограничено)
- symlink	следовать по символическим ссылкам (по умолчанию)
- no-symlink	пропускать символические ссылки
- ext-remove = РАСШИРЕНИЯ	
- ext-exclude = РАСШИРЕНИЯ	исключить из сканирования РАСШИРЕНИЯ, разделенные двоеточием

Методы

- adware	сканировать на наличие рекламных/шпионских/опасных программ
- no-adware	не сканировать на наличие рекламных/шпионских/опасных программ
- unsafe	сканировать на наличие потенциально опасных приложений
- no-unsafe	не сканировать на наличие потенциально опасных приложений
- unwanted	сканировать на наличие потенциально нежелательных приложений
- no-unwanted	не сканировать на наличие потенциально нежелательных приложений
- pattern	использовать сигнатуры
- no-pattern	не использовать сигнатуры
- heur	включить эвристический анализ
- no-heur	отключить эвристический анализ
- adv-heur	включить расширенную эвристику
- no-adv-heur	отключить расширенную эвристику

Очистка

- action = ДЕЙСТВИЕ	применить ДЕЙСТВИЕ к зараженным объектам. Возможные действия: «none» (ничего), «clean» (очистка), «prompt» (запрос)
- quarantine	копировать зараженные файлы в карантин (дополнительно к ДЕЙСТВИЮ)
- no-quarantine	не копировать зараженные файлы в карантин

Журналы

- log-file=ФАЙЛ	вывод журнала в ФАЙЛ
- log-rewrite	перезаписывать выходной файл (по умолчанию добавлять)
- log-all	регистрировать также незараженные файлы
- no-log-all	не регистрировать незараженные файлы (по умолчанию)

Возможные коды завершения сканирования

0	угроз не обнаружено
1	угроза обнаружена, но не очищена
10	остались зараженные файлы
101	ошибка архива
102	ошибка доступа
103	внутренняя ошибка

ПРИМЕЧАНИЕ: Значение кода завершения больше 100 означает, что файл не был просканирован и может быть заражен.

4.2.1.5 Производительность

В этом разделе можно задать количество модулей сканирования ThreatSense, которые следует использовать для сканирования на наличие вирусов. Большее количество модулей сканирования ThreatSense на многопроцессорных компьютерах может увеличить скорость сканирования. Приемлемы значения в диапазоне от 1 до 20.

ПРИМЕЧАНИЕ. Внесенные в этом разделе изменения будут применены только после перезапуска.

4.2.1.6 Фильтрация протоколов

Защита от вирусов протоколов приложений POP3 и HTTP обеспечивается модулем сканирования ThreatSense, в котором объединены все современные методы сканирования для выявления вредоносных программ. Контроль осуществляется автоматически вне зависимости от используемого веб-браузера и почтового клиента. Для фильтрации протоколов доступны перечисленные далее варианты (если установлен флажок **Включить фильтрацию содержимого протоколов приложений**).

Порты HTTP и POP3: сканирование ограничивается соединениями по известным портам, используемым протоколами HTTP и POP3.

Приложения, классифицированные как браузеры Интернета и почтовые клиенты: установите этот флажок, чтобы фильтровать только соединения для приложений, помеченных в качестве браузеров (**Защита доступа в Интернет** > **HTTP, HTTPS** > **Веб-браузеры**) или почтовых клиентов (**Защита почтового клиента** > **POP3, POP3s** > **Почтовые клиенты**).

Порты и приложения, классифицированные как браузеры Интернета или почтовые клиенты: и порты, и браузеры проверяются на наличие вредоносных программ.

ПРИМЕЧАНИЕ. Начиная с ОС Windows Vista с пакетом обновления 1 и Windows Server 2008, используется новый метод фильтрации соединений. Из-за этого раздел «Фильтрация протоколов» недоступен.

4.2.1.6.1 SSL

ESET File Security позволяет проверять инкапсулированные в SSL протоколы. Можно использовать различные режимы сканирования для защищенных SSL соединения, при которых используются доверенные сертификаты, неизвестные сертификаты или сертификаты, исключенные из проверки защищенных SSL соединений.

Всегда сканировать протокол SSL: выберите этот вариант, чтобы сканировать все защищенные SSL соединения за исключением защищенных сертификатами, исключенными из проверки. Если устанавливается новое соединение, использующее неизвестный заверенный сертификат, пользователь получит об этом соответствующее уведомление, а само соединение автоматически будет фильтроваться. При доступе к серверу с ненадежным сертификатом, который помечен пользователем в качестве доверенного (добавлен в список доверенных сертификатов), соединение с этим сервером разрешается, а содержимое канала связи фильтруется.

Запрашивать о новых сайтах (возможна настройка исключений): при выполнении входа на новый защищенный SSL сайт (с неизвестным сертификатом) на экран выводится диалоговое окно выбора. Этот режим позволяет создавать список сертификатов SSL, которые будут исключены из сканирования.

Не сканировать протокол SSL: если выбран этот параметр, программа не будет сканировать соединения по протоколу SSL.

Если сертификат невозможно проверить, используя хранилище доверенных корневых сертификатов сертифицирующих органов (**Фильтрация протоколов** > **SSL** > **Сертификаты**), выполняется одно из следующих действий.

Запрашивать действительность сертификата: пользователю предлагается выбрать действие.

Блокировать соединения, использующие сертификат: соединение с сайтом, использующим данный сертификат, разрывается.

Если сертификат недействителен или поврежден (**Фильтрация протоколов** > **SSL** > **Сертификаты**), выполняется одно из следующих действий.

Запрашивать действительность сертификата: пользователю предлагается выбрать действие.

Блокировать соединения, использующие сертификат: соединение с сайтом, использующим данный сертификат, разрывается.

4.2.1.6.1.1 Доверенные сертификаты

В дополнение к встроенному хранилищу доверенных корневых сертификатов сертифицирующих органов , где программой ESET File Security хранятся доверенные сертификаты, можно также создать собственный список доверенных сертификатов, доступный в разделе **Дополнительные настройки** (F5) > **Фильтрация протоколов** > **SSL** > **Сертификаты** > **Доверенные сертификаты**.

4.2.1.6.1.2 Исключенные сертификаты

В разделе «Исключенные сертификаты» перечислены сертификаты, которые считаются безопасными. Содержимое зашифрованных соединений, использующих сертификаты из данного списка, не будет проверяться на наличие угроз. Рекомендуется исключать только те веб-сертификаты, которые гарантированно являются безопасными, а соединение с их использованием не нуждается в проверке.

4.2.1.7 Настройка параметров модуля ThreatSense

ThreatSense — это технология, объединяющая ряд сложных методов обнаружения угроз. Эта технология 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 значительно повышают уровень безопасности компьютера. Модуль сканирования может контролировать несколько потоков данных одновременно, что делает эффективность и количество обнаруживаемых угроз максимальными. Технология ThreatSense также успешно уничтожает руткиты.

Для технологии ThreatSense можно настроить несколько параметров сканирования:

- типы и расширения файлов, подлежащих сканированию;
- сочетание различных методов обнаружения;
- уровни очистки и т. д.

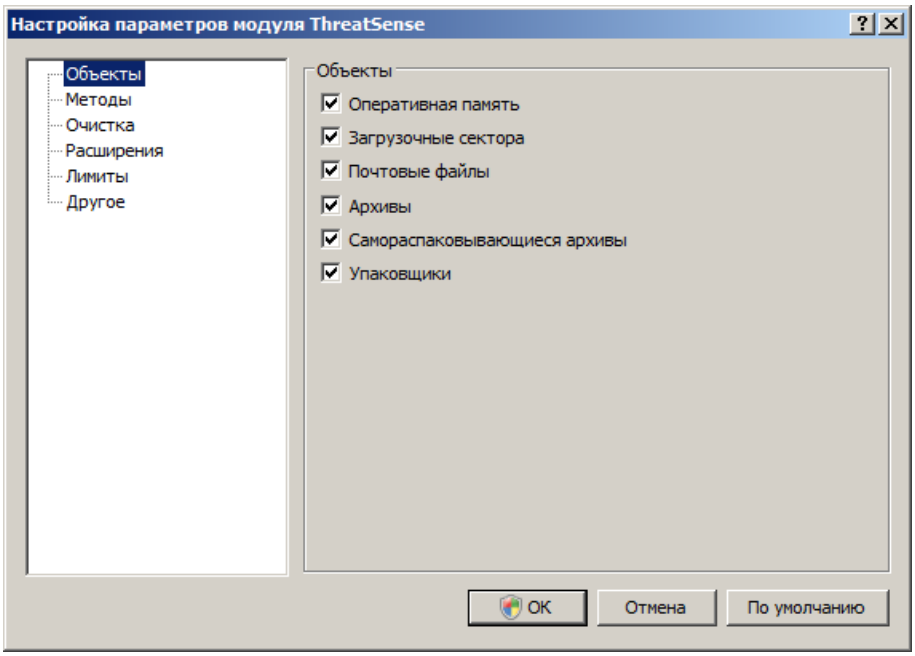
Для того чтобы открыть окно параметров, нажмите кнопку **Настройка...** в окне параметров любого модуля, использующего технологию ThreatSense (см. ниже). Разные сценарии обеспечения безопасности требуют различных настроек, поэтому технологию ThreatSense можно настроить отдельно для каждого из перечисленных далее модулей защиты.

- Защита файловой системы в режиме реального времени
- Проверка файлов, исполняемых при запуске системы
- Защита электронной почты
- Защита доступа в Интернет
- Сканирование ПК по требованию

Параметры ThreatSense хорошо оптимизированы для каждого из модулей, а их изменение ведет к существенным изменениям в поведении системы. Например, изменение параметров так, чтобы всегда сканировались упаковщики, или включение расширенной эвристики в модуле защиты файловой системы в режиме реального времени, может замедлить работу системы (обычно только новые файлы сканируются с применением этих методов). В связи с этим рекомендуется не изменять параметры ThreatSense по умолчанию ни для каких модулей, кроме модуля «Сканирование ПК по требованию».

4.2.1.7.1 Настройка объектов

В разделе **Объекты** можно указать компоненты и файлы, которые должны сканироваться на наличие заражений.



Оперативная память: выполняется сканирование на наличие угроз, которые атакуют оперативную память системы.

Загрузочные секторы: загрузочные секторы сканируются на наличие вирусов в основной загрузочной записи.

Файлы: сканируются файлы всех часто используемых типов (программы, изображения, звуковые и видеофайлы, файлы баз данных и т. д.).

Почтовые файлы: сканируются особые файлы, в которых хранятся сообщения электронной почты.

Архивы: сканируются сжатые файлы в архивах .rar, .zip, .arj, .tar и т. д.

Самораспаковывающиеся архивы: сканируются файлы, запакованные в самораспаковывающихся архивах, которые обычно имеют расширение .exe.

Упаковщики: сканируются упаковщики, которые в отличие от стандартных архивов распаковывают файлы динамически в системную память, и стандартные статические упаковщики (UPX, yoda, ASPack, FGS и т. д.).

4.2.1.7.2 Методы

В разделе **Параметры** можно выбрать методы, которые будут использоваться при сканировании системы на наличие заражений. Доступны следующие варианты:

Сигнатуры: сигнатуры представляют собой надежный и точный метод обнаружения и выявления заражений по имени с применением базы данных сигнатур вирусов.

Эвристика: при эвристическом анализе используются алгоритмы, которые анализируют вредоносную активность программ. 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).

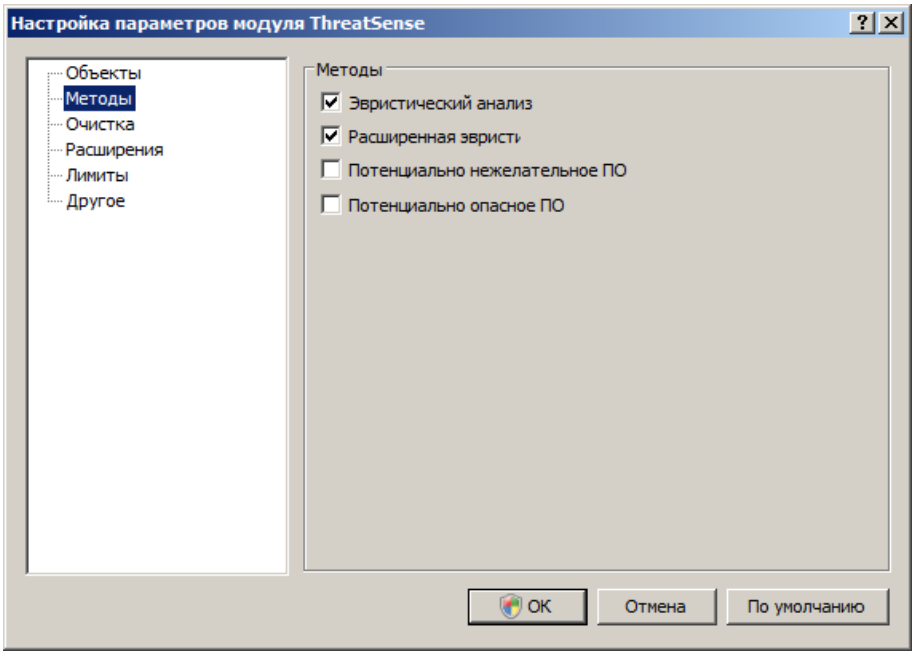
Расширенная эвристика: расширенная эвристика представляет собой уникальный эвристический алгоритм, разработанный компанией ESET и оптимизированный для обнаружения компьютерных червей и троянских программ, написанных на языках программирования высокого уровня. Расширенная эвристика значительно увеличивает возможности программы по обнаружению.

Рекламное/шпионское/опасное ПО: к этой категории относится программное обеспечение, которое собирает различную конфиденциальную информацию о пользователях без их согласия. Также к ней относится программное обеспечение, выводящее на экран рекламные материалы.

Потенциально нежелательное ПО: потенциально нежелательные приложения не обязательно являются вредоносными, но могут негативно влиять на производительность системы. Обычно для установки таких

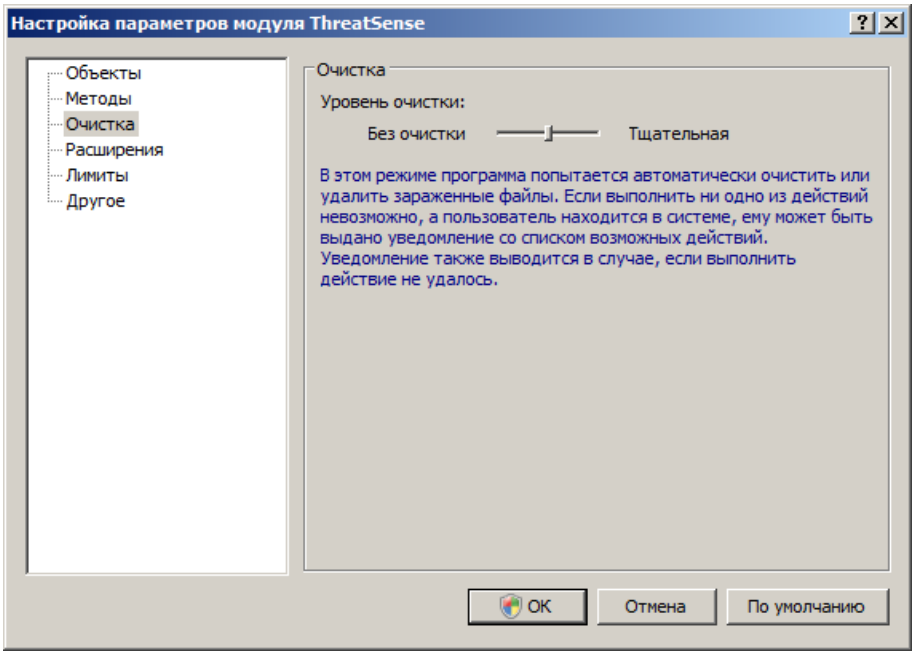
приложений запрашивается согласие пользователя. После их установки поведение системы изменяется (по сравнению с тем, как она вела себя до установки этих приложений). Наиболее существенные изменения связаны с возникновением нежелательных всплывающих окон, запуском и работой скрытых процессов, увеличением уровня использования системных ресурсов, изменениями результатов поиска и обменом данными с удаленными серверами.

Потенциально опасное ПО: к потенциально опасным приложениям относится нормальное коммерческое программное обеспечение. Это в том числе средства удаленного доступа. По умолчанию этот параметр отключен.



4.2.1.7.3 Очистка

Параметры процесса очистки определяют поведение модуля сканирования при очистке зараженных файлов. Предусмотрено три описанных далее уровня очистки.



Без очистки: зараженные файлы не очищаются автоматически. Программа выводит на экран предупреждение и предлагает пользователю выбрать нужное действие.

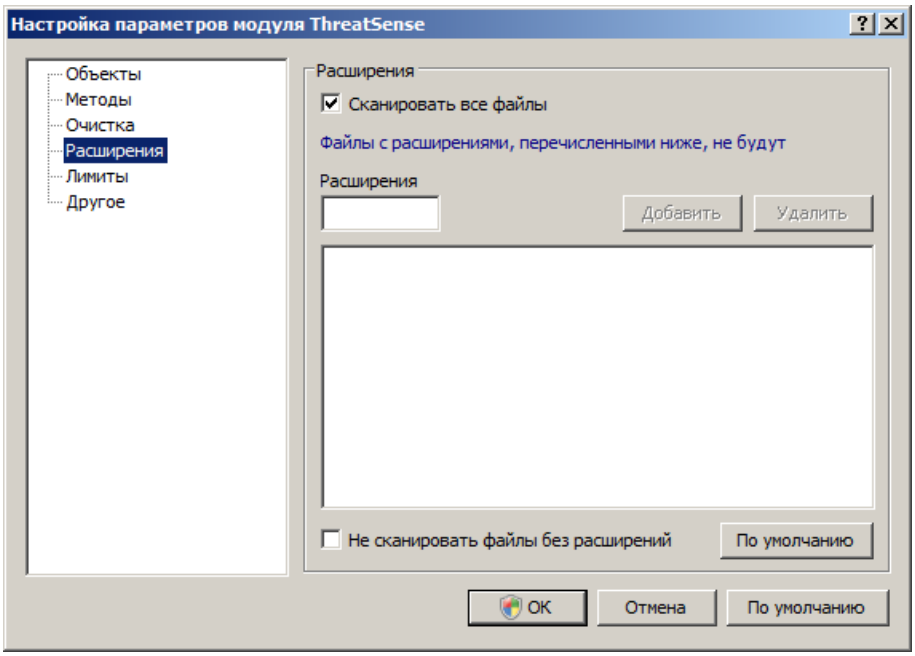
Стандартная очистка: программа пытается автоматически очистить или удалить зараженный файл. При невозможности выбрать необходимое действие автоматически программа предлагает сделать выбор пользователю. Выбор пользователю предоставляется и в том случае, если предварительно заданное действие не может быть выполнено.

Тщательная очистка: программа очищает или удаляет все зараженные файлы (в том числе архивы). Единственное исключение составляют системные файлы. Если файлы невозможно очистить, на экран выводится предупреждение с предложением выбрать действие.

Внимание: В используемом по умолчанию режиме 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.

4.2.1.7.4 Расширения

Расширением называется часть имени файла, отделенная от основной части точкой. Расширение определяет тип файла или его содержимого. Этот раздел параметров ThreatSense позволяет определить типы файлов, подлежащих сканированию.



По умолчанию сканируются все файлы независимо от их расширения. Любое расширение можно добавить в список файлов, исключенных из сканирования. Если снят флажок **Сканировать все файлы**, список меняется для отображения всех расширений файлов, которые сейчас подвергаются сканированию. С помощью кнопок **Добавить** и **Удалить** можно включать или запрещать сканирование для тех или иных расширений.

Для того чтобы включить сканирование файлов без расширений, установите флажок **Сканировать файлы без расширений**.

Иногда может быть необходимо исключить файлы из сканирования, если сканирование определенных типов файлов препятствует нормальной работе программы, которая использует эти расширения. Например, может быть полезно исключить расширения .edb, .eml и .tmp при использовании серверов Microsoft Exchange.

4.2.1.7.5 Ограничения

В разделе «Ограничения» можно указать максимальный размер объектов и уровни вложенности архивов для сканирования.

Максимальный размер объекта: определяет максимальный размер объектов, подлежащих сканированию. Данный модуль защиты от вирусов будет сканировать 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, в секундах: определяет максимальное время для сканирования объекта. Если пользователь укажет здесь собственное значение, модуль защиты от вирусов прекратит сканирование объекта по истечении указанного времени вне зависимости от того, было ли сканирование завершено.

Уровень вложенности архива: 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 в архиве: этот параметр позволяет указать максимальный размер файлов в архиве (после извлечения), подлежащих сканированию. Если этот параметр прерывает сканирование архива до завершения, то архив останется непроверенным.

4.2.1.7.6 Другое

Сканировать альтернативные потоки данных (ADS): альтернативные потоки данных используются файловой системой NTFS для связей файлов и папок, которые не видны для обычных методов сканирования. Многие заражения маскируются под альтернативные потоки данных, пытаясь избежать обнаружения.

Запустить фоновое сканирование с низким приоритетом: каждый процесс сканирования потребляет некоторое количество системных ресурсов. Если пользователь работает с ресурсоемкими программами, можно активировать фоновое сканирование с низким приоритетом и высвободить тем самым ресурсы для других приложений.

Регистрировать все объекты: если этот флажок установлен, в файле журнала будет содержаться информация обо всех просканированных файлах, в том числе незараженных.

Включить оптимизацию Smart: установите этот флажок, чтобы уже просканированные файлы не сканировались повторно, пока не будут изменены. Файлы сканируются повторно сразу после каждого обновления базы данных сигнатур вирусов.

Сохранить отметку о времени последнего доступа: установите этот флажок, чтобы сохранять исходную отметку о времени доступа к сканируемым файлам, не обновляя ее (например, для использования с системами резервного копирования данных).

Прокрутить журнал: этот параметр позволяет включать и отключать прокрутку журнала. Если флажок установлен, в окне можно прокручивать отображаемую информацию вверх.

Показывать уведомление о завершении сканирования в отдельном окне: открывает отдельное окно с информацией о результатах сканирования.

4.2.1.8 Действия при обнаружении заражения

Заражения могут попасть на компьютер из различных источников: веб-сайты, общие папки, электронная почта или съемные носители (USB-устройства, внешние диски, компакт-диски, DVD-диски и т. д.).

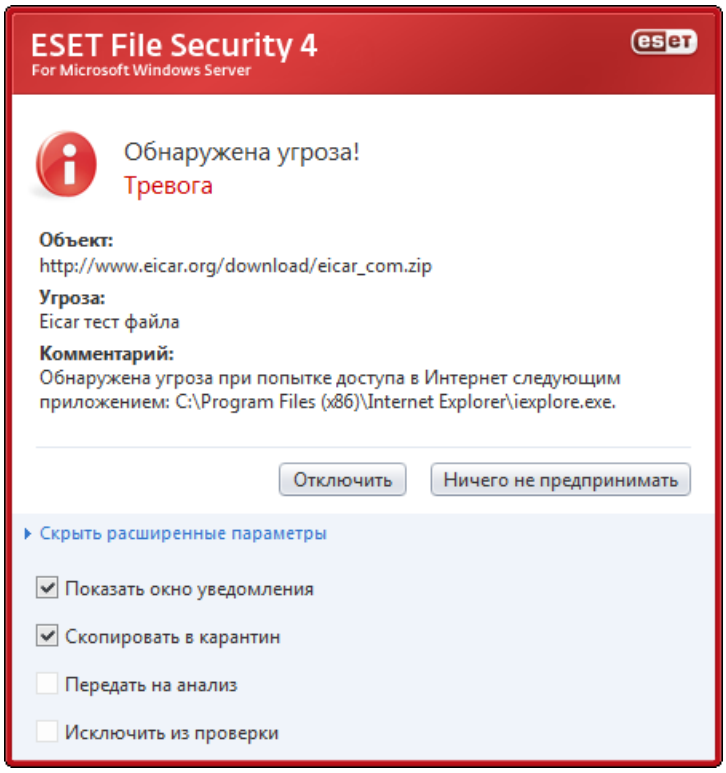
Если на компьютере возникли признаки заражения вредоносной программой (например, он стал медленнее работать, часто зависает и т. п.), рекомендуется выполнить следующие действия.

- Откройте ESET File Security и нажмите «Сканирование компьютера».
- Нажмите **Сканирование Smart** (Дополнительные сведения см. в разделе Сканирование Smart)
- После окончания сканирования проверьте количество просканированных, зараженных и очищенных файлов в журнале.

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

Ниже описан общий случай работы ESET File Security с заражениями. Предположим, что заражение обнаружено модулем защиты файловой системы в режиме реального времени при уровне очистки по умолчанию. Модуль попытается очистить или удалить файл. Если действие по умолчанию для модуля защиты в режиме реального времени не определено, его предлагается выбрать пользователю в специальном окне предупреждения. Обычно доступны действия **Очистить**, **Удалить** и **Пропустить**. Не рекомендуется выбирать вариант **Пропустить**, так как в этом случае зараженные файлы останутся на компьютере. Исключением может быть ситуация, когда имеется полная уверенность в том, что файл безвреден и был обнаружен по ошибке.

Очистка и удаление: примените очистку, если полезный файл был атакован вирусом, который добавил вредоносный код к полезному. В этом случае сначала программа пытается очистить зараженный файл, чтобы восстановить его первоначальное состояние. Если файл содержит только вредоносный код, его следует удалить.



Если зараженный файл заблокирован или используется каким-либо системным процессом, обычно он удаляется только после освобождения. Как правило, это происходит после перезапуска системы.

Удаление файлов из архивов: в режиме очистки по умолчанию архив удаляется целиком только в том случае, если он содержит только зараженные файлы. Иначе говоря, архивы, в которых есть незараженные файлы, не удаляются. Однако следует проявлять осторожность при сканировании в режиме тщательной очистки, так как в этом режиме архив удаляется, если содержит хотя бы один зараженный файл, независимо от состояния других файлов в архиве.

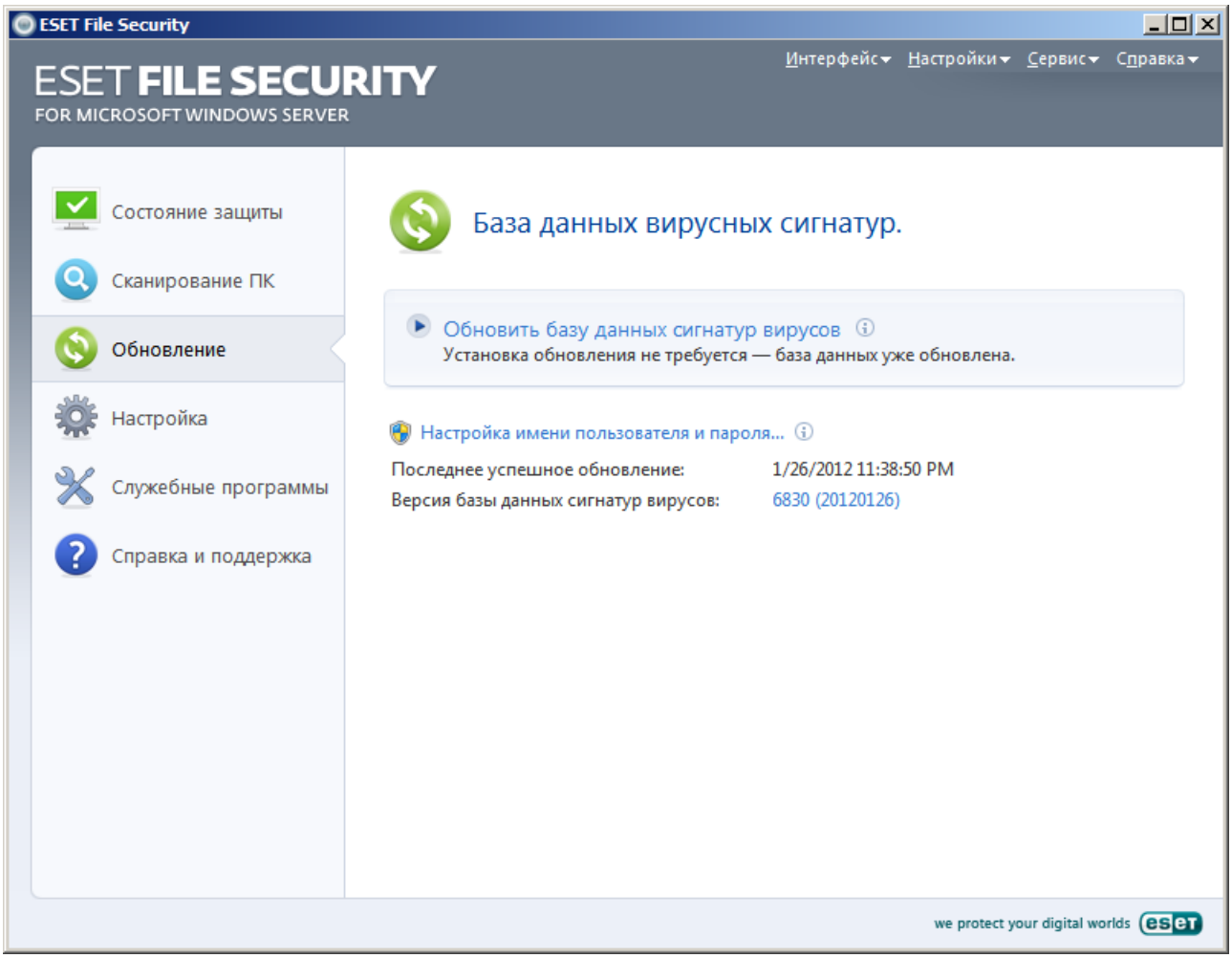
4.3 Обновление программы

Регулярное обновление ESET File Security — основное условие обеспечения максимально высокого уровня безопасности. Модуль обновления поддерживает актуальность программы двумя способами: путем обновления базы данных сигнатур вирусов и путем обновления компонентов системы.

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. Также в основном окне указывается версия базы данных сигнатур вирусов. Этот числовой индикатор представляет собой активную ссылку на страницу веб-сайта ESET, где перечисляются все сигнатуры, добавленные при данном обновлении.

Кроме того, есть функция для запуска процесса обновления принудительно (**Обновить базу данных сигнатур вирусов**), а также основные параметры обновления, такие как имя пользователя и пароль для доступа к серверам обновлений ESET.

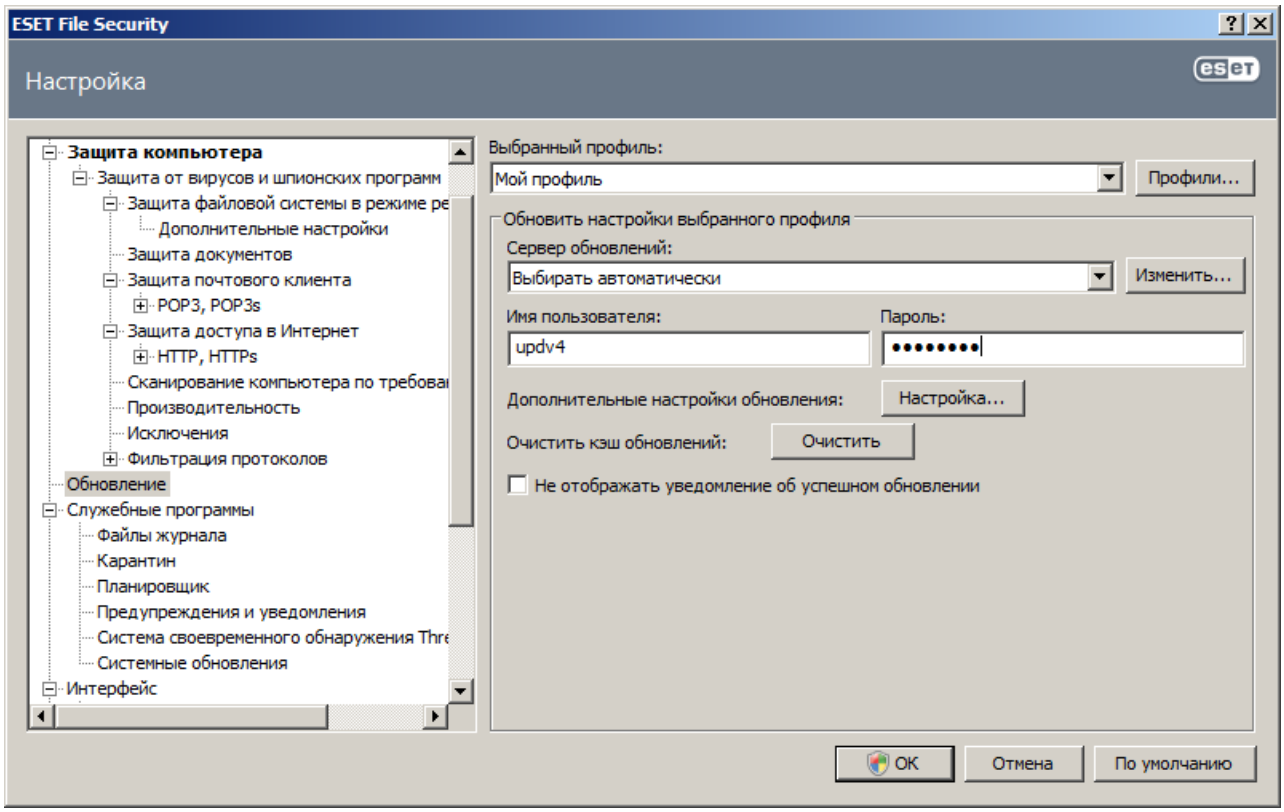
Нажмите ссылку **Активация программы**, чтобы открыть форму регистрации, в которой вы сможете активировать свой программный продукт обеспечения безопасности ESET, после чего получите по электронной почте сообщение с данными аутентификации (имя пользователя и пароль).



ПРИМЕЧАНИЕ: Имя пользователя и пароль предоставляются компанией ESET после приобретения программы ESET File Security.

4.3.1 Настройка обновлений

В разделе параметров обновления указывается информация об источниках обновлений, такая как серверы обновлений и данные аутентификации для них. По умолчанию в раскрывающемся меню **Сервер обновлений** выбран параметр **Выбирать автоматически**, обеспечивающий автоматическую загрузку файлов обновлений с сервера ESET с минимальным расходом трафика. Параметры обновлений доступны в дереве расширенных параметров (клавиша F5) раздела **Обновление**.

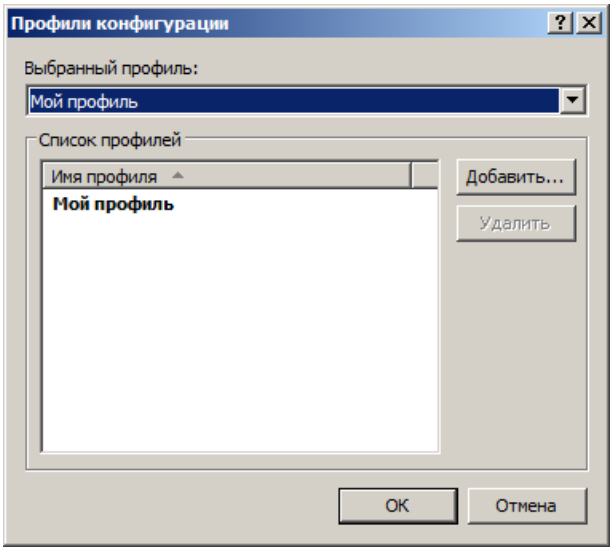


Список доступных серверов обновлений можно просмотреть с помощью раскрывающегося меню **Сервер обновлений**. Для добавления нового сервера обновлений нажмите кнопку **Изменить...** в разделе **Обновить настройки выбранного профиля**, а затем кнопку **Добавить**. Для аутентификации на серверах обновлений используются **имя пользователя** и **пароль**, созданные и отправленные вам после покупки.

4.3.1.1 Профили обновления

Профили обновления можно создавать для различных конфигураций и задач обновления. Создание профилей обновления особенно полезно для пользователей мобильных устройств, которые могут создать вспомогательный профиль в случае, когда свойства подключения к Интернету регулярно меняются.

В раскрывающемся меню **Выбранный профиль** отображается текущий профиль. По умолчанию это **Мой профиль**. Для создания нового профиля нажмите кнопку **Профили...**, затем **Добавить...** и введите нужное **Имя профиля**. При создании нового профиля можно скопировать параметры из уже существующего профиля, выбрав его в раскрывающемся меню **Копировать настройки профиля**.



В окне настройки профиля можно выбрать сервер обновлений из списка доступных серверов или добавить новый. Список существующих серверов обновлений можно просмотреть с помощью раскрывающегося меню **Сервер обновлений**. Для добавления нового сервера обновлений нажмите кнопку **Изменить...** в разделе **Обновить настройки выбранного профиля**, а затем кнопку **Добавить**.

4.3.1.2 Дополнительные настройки обновления

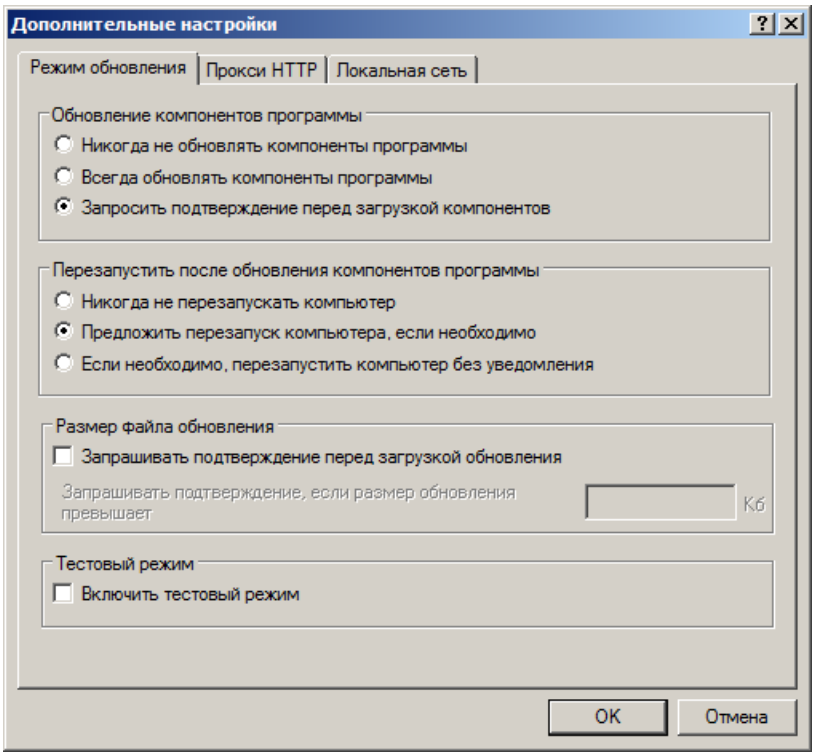
Для просмотра расширенных параметров обновления нажмите кнопку **Настройка...**. Расширенные параметры обновления позволяют настроить **режим обновления**, **прокси HTTP**, **локальную сеть** и **зеркало**.

4.3.1.2.1 Режим обновления

Вкладка **«Режим обновления»** содержит параметры обновления программы.

В разделе **Обновление компонентов программы** доступно три описанных далее варианта.

- **Никогда не обновлять компоненты программы**: появляющиеся обновления компонентов программы не будут загружаться.
- **Выполнять обновление компонентов программы, если доступно**: появляющиеся обновления компонентов программы будут устанавливаться автоматически.
- **Запросить подтверждение перед загрузкой компонентов**: Вариант по умолчанию. Пользователю будет предлагаться подтвердить обновление компонентов программы или отказаться от него, когда такое обновление становится доступно.



После обновления компонентов программы может быть необходимо перезапустить компьютер, чтобы все модули работали полностью корректно. В разделе **Перезапустить после обновления компонентов программы** можно выбрать один из следующих вариантов.

- **Никогда не перезапускать компьютер**
- **Предложить перезапуск компьютера, если необходимо**
- **Если необходимо, перезапустить компьютер без уведомления**

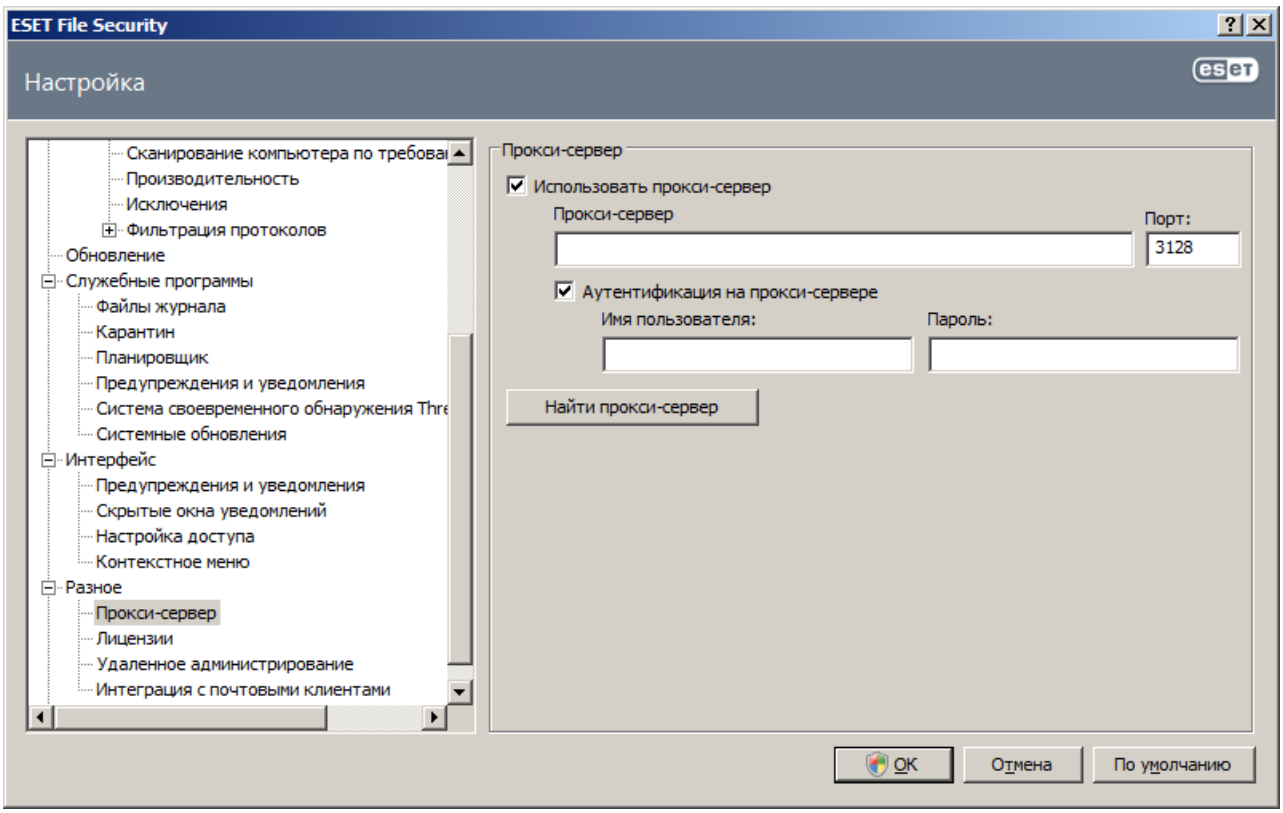
По умолчанию выбран вариант **Предложить перезапуск компьютера, если необходимо**. Наиболее подходящий вариант зависит от конкретной рабочей станции, на которой будут применяться параметры. Необходимо помнить о том, что существует разница между рабочими станциями и серверами. Например, автоматический перезапуск сервера после обновления программы может привести к серьезным проблемам.

4.3.1.2.2 Прокси-сервер

В ESET File Security настройку прокси-сервера можно выполнить в двух разных разделах дерева расширенных параметров.

Во-первых, параметры прокси-сервера можно сконфигурировать в разделе **Разное** > **Прокси-сервер**. Настройка прокси-сервера на этом уровне позволяет задать его параметры для программы ESET File Security в целом. Они используются всеми модулями программы, которым требуется подключение к Интернету.

Для настройки параметров прокси-сервера на этом уровне установите флажок **Использовать прокси-сервер**, а затем введите адрес прокси-сервера в поле **Прокси-сервер** и номер **порта** в соответствующее поле.



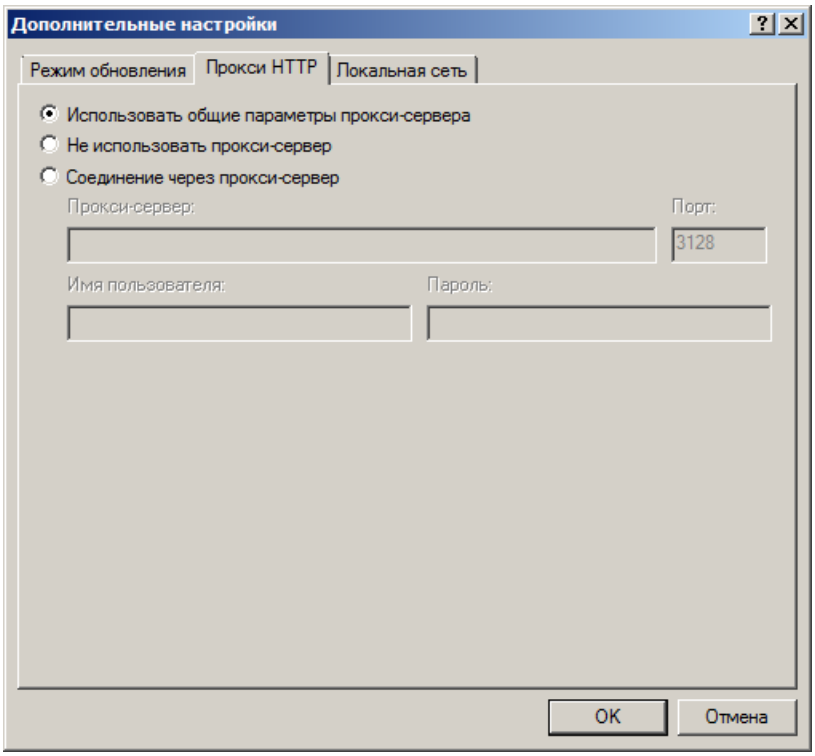
Если требуется аутентификация на прокси-сервере, установите флажок **«Прокси-сервер требует аутентификации»**, а затем укажите **имя пользователя** и **пароль** в соответствующих полях. Нажмите кнопку **Найти прокси-сервер**, чтобы автоматически определить параметры прокси-сервера и вставить их. Будут скопированы параметры, указанные в Internet Explorer.

ПРИМЕЧАНИЕ: Эта функция не позволяет получить данные аутентификации (имя пользователя и пароль), их пользователь должен указать самостоятельно.

Также параметры прокси-сервера можно настроить в разделе «Дополнительные настройки обновления». В этом случае параметры применяются к конкретному профилю обновления. Параметры прокси-сервера для конкретного профиля обновления можно открыть, перейдя на вкладку **Прокси HTTP** в разделе **Дополнительные настройки обновления**. Здесь можно выбрать один из трех вариантов.

- **Использовать общие параметры прокси-сервера**
- **Не использовать прокси-сервер**
- **«Соединение через прокси-сервер»** (указываются параметры подключения).

Если выбрать вариант **Использовать общие параметры прокси-сервера**, будут использоваться параметры прокси-сервера, уже заданные в разделе **Разное** > **Прокси-сервер** дерева расширенных параметров (как описано в начале данной статьи).



Выберите вариант **Не использовать прокси-сервер**, чтобы указать, что не будет использоваться прокси-сервер для обновления ESET File Security.

Вариант **Соединение через прокси-сервер** следует выбрать, если для обновления ESET File Security нужно использовать прокси-сервер, причем он отличается от указанного в общие параметрах (**Разное** > **Прокси-сервер**). В этом случае нужно указать параметры: адрес (поле **Прокси-сервер**), **порт** для соединения, а также при необходимости **имя пользователя** и **пароль**.

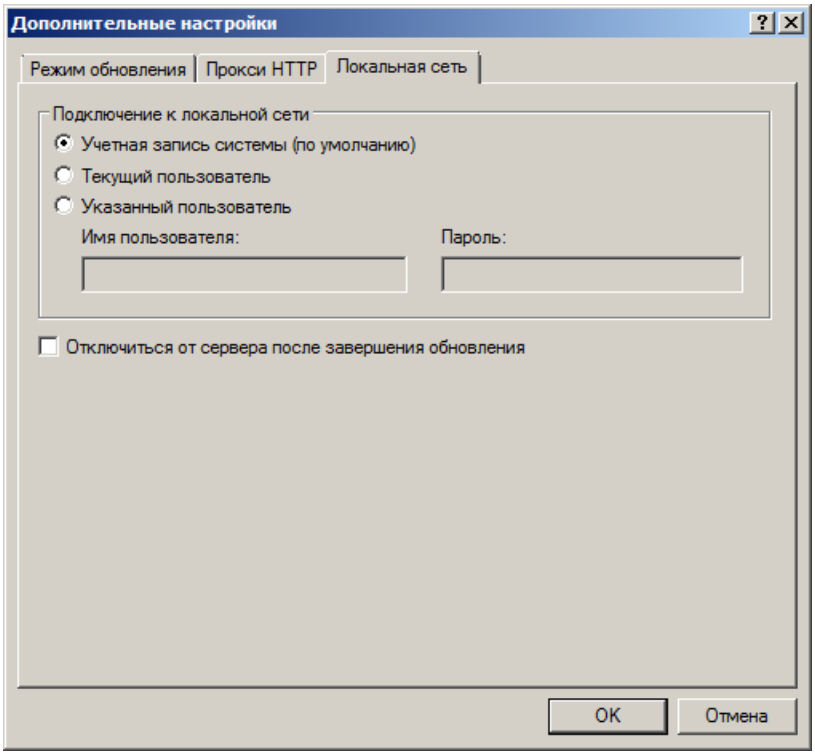
Также этот вариант следует выбрать, если общие параметры прокси-сервера заданы не были, но при этом ESET File Security будет подключаться к прокси-серверу для получения обновлений.

По умолчанию выбран вариант **Использовать общие параметры прокси-сервера**.

4.3.1.2.3 Подключение к локальной сети

При обновлении с локального сервера под управлением операционной системы на базе NT по умолчанию требуется аутентификация всех сетевых подключений. Чаще всего у локальной учетной записи системы недостаточно прав для доступа к папке зеркала (папке, в которой хранятся копии файлов обновления). В этом случае введите имя пользователя и пароль в разделе параметров обновления или укажите существующую учетную запись, под которой программа сможет получить доступ к серверу обновлений (зеркалу).

Для конфигурирования такой учетной записи перейдите на вкладку **Локальная сеть**. В разделе **Подключение к локальной сети** можно выбрать один из следующих вариантов: **Учетная запись системы (по умолчанию)**, **Текущий пользователь** и **Указанный пользователь**.



Выберите **Учетная запись системы (по умолчанию)**, чтобы использовать для аутентификации учетную запись системы. Если данные аутентификации в главном разделе параметров обновлений не указаны, как правило, процесса аутентификации не происходит.

Для того чтобы программа использовала для аутентификации учетную запись, под которой в данный момент выполнен вход в систему, выберите вариант **Текущий пользователь**. Недостаток этого варианта заключается в том, что программа не может подключиться к серверу обновлений, если в данный момент ни один пользователь не выполнил вход в систему.

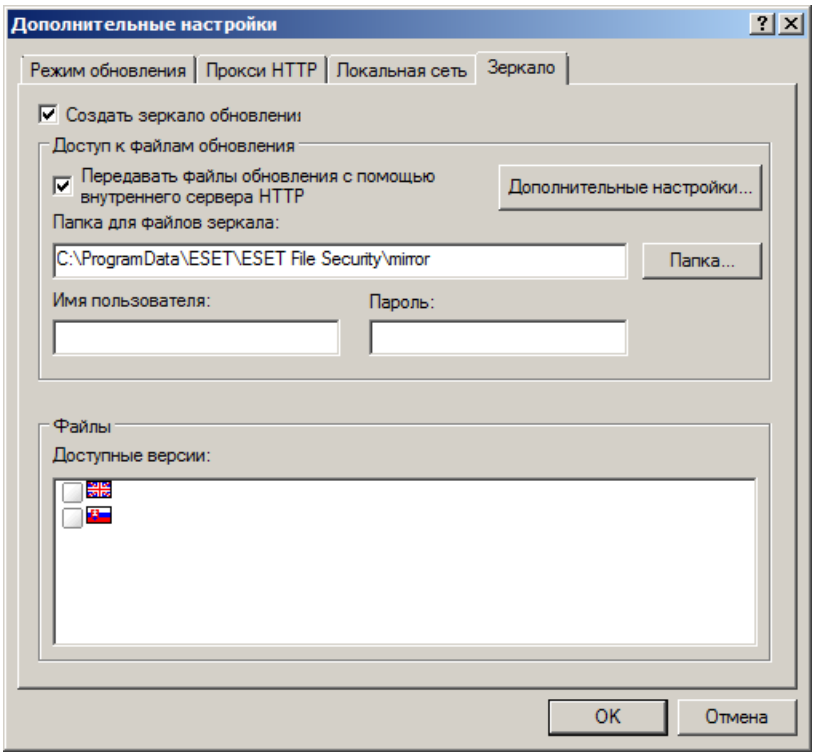
Выберите **«Указанный пользователь»**, если нужно указать учетную запись пользователя для аутентификации.

Внимание: Если выбран вариант **Текущий пользователь** или **Указанный пользователь**, может произойти ошибка при изменении учетной записи программы. В главном разделе параметров обновления рекомендуется указывать данные аутентификации в локальной сети. В этом разделе параметров обновлений данные аутентификации нужно указать в следующем формате: имя_домена\пользователь (а для рабочей группы рабочая_группа\имя) и пароль. При обновлении по протоколу HTTP с локального сервера аутентификация не требуется.

4.3.1.2.4 Создание копий обновлений, зеркало

ESET File Security позволяет создавать копии файлов обновлений, которые могут использоваться для обновления других рабочих станций в сети. Обновление клиентских рабочих станций с зеркала оптимизирует трафик в сети и сокращает объем потребляемого интернет-трафика.

Параметры конфигурации локального сервера зеркала можно найти (после добавления действительного лицензионного ключа в менеджере лицензий, который расположен в разделе «Дополнительные настройки» ESET File Security), воспользовавшись разделом **Дополнительные настройки обновления**. Для доступа к этому разделу нажмите клавишу F5 и выберите **Обновление** в дереве расширенных параметров, после чего нажмите кнопку **Настройка...** рядом с пунктом **Дополнительные настройки обновления** и перейдите на вкладку **Зеркало**.



На первом этапе настройки зеркала нужно выбрать вариант «Создать зеркало обновления». После этого становятся доступны другие параметры настройки зеркала, такие как способ доступа к файлам обновлений и путь к файлам зеркала.

Методы активации зеркала подробно описываются в разделе Обновление с зеркала. Пока что достаточно заметить, что существует два основных метода доступа к зеркалу: папка с файлами обновлений может существовать как общая сетевая папка или как HTTP-сервер.

Папка, предназначенная для хранения файлов обновлений, указывается в разделе **Папка для дублируемых файлов**. Нажмите **Папка...**, чтобы найти нужную папку на локальном компьютере или в общей сетевой папке. Если для указанной папки нужна авторизация, данные аутентификации должны быть указаны в полях **Имя пользователя** и **Пароль**. Имя пользователя и пароль следует вводить в формате *Домен/ Пользователь* или *Рабочая_группа/Пользователь*. Не забудьте ввести соответствующие пароли.

При настройке зеркала пользователь также может указать языковые версии, для которых нужно загружать копии обновлений. Настройка языковых версий доступна в разделе **Файлы** — **Доступные версии**.

4.3.1.2.4.1 Обновление с зеркала

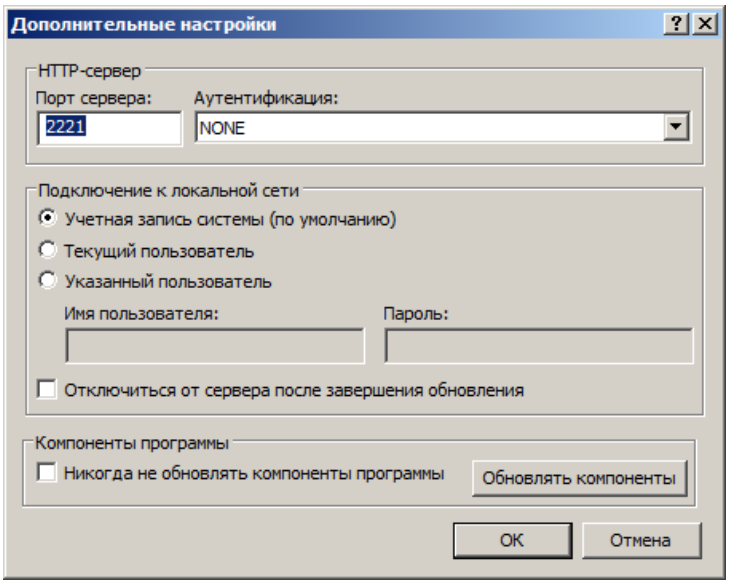
Существует два основных метода настройки зеркала: папка с файлами обновлений может существовать как общая сетевая папка или как HTTP-сервер.

Доступ к файлам зеркала с помощью внутреннего сервера HTTP

Это вариант по умолчанию, выбранный в предварительно заданной конфигурации программы. Для обеспечения доступа к зеркалу с помощью HTTP-сервера перейдите в раздел **Дополнительные настройки обновления** (вкладка **Зеркало**) и выберите вариант **Создать зеркало обновления**.

В разделе **Дополнительные настройки** вкладки **Зеркало** можно указать **Порт сервера**, на котором HTTP-сервер будет принимать запросы, а также тип **аутентификации**, используемой HTTP-сервером. По умолчанию порт сервера имеет значение **2221**. В параметре **Аутентификация** определяется метод аутентификации, используемый для доступа к файлам обновлений. Доступны следующие варианты: **Ничего**, **Основное** и **NTLM**. Для того чтобы использовать кодирование base64 и упрощенную аутентификацию по имени пользователя и паролю, выберите **Основное**. Вариант **NTLM** обеспечивает шифрование за счет метода безопасного шифрования. Для аутентификации используется учетная запись пользователя, созданная на рабочей станции, которая предоставляет общий доступ к файлам обновлений. Значение по умолчанию — **Ничего**. Этот вариант дает доступ к файлам обновлений без аутентификации.

Внимание: Если планируется организовать доступ к файлам обновлений с помощью HTTP-сервера, папка зеркала должна находиться на том же компьютере, что и экземпляр ESET File Security, который ее создает.



После завершения настройки зеркала следует воспользоваться рабочими станциями и добавить новый сервер обновлений в формате **http://IP-адрес_вашего_сервера:2221**. Для этого выполните следующие действия.

- Откройте раздел ESET File Security **Дополнительные настройки** и нажмите **Обновление** .
- Нажмите **Изменить...** справа от раскрывающегося меню **Сервер обновлений** и добавьте новый сервер в формате http://IP_адрес_вашего_сервера:2221.
- Выберите вновь добавленный сервер из списка серверов обновлений.

Доступ к зеркалу через общий системный ресурс

Сначала необходимо создать общую папку на локальном или сетевом устройстве. При создании папки для зеркала необходимо предоставить права на запись пользователю, который будет размещать в ней файлы обновлений, и права на чтение всем пользователям, которые будут получать обновления ESET File Security из папки зеркала.

Далее следует сконфигурировать доступ к зеркалу в разделе **Дополнительные настройки обновления** (вкладка **Зеркало**), сняв флажок **Передавать файлы обновления с помощью внутреннего сервера HTTP**. Этот вариант включен по умолчанию после установки программы.

Если общая папка расположена на другом компьютере в сети, необходимо указать данные аутентификации для доступа к этому компьютеру. Для ввода данных аутентификации откройте раздел «Дополнительные настройки» ESET File Security (F5) и выберите ветвь **Обновление**. Нажмите кнопку **Настройка...** и перейдите на вкладку **Локальная сеть**. Этот параметр аналогичен используемому для обновления и описан в разделе Подключение к локальной сети.

После окончания настройки зеркала укажите на рабочих станциях адрес нового сервера обновлений в формате \\UNC-ИМЯ_КОМПЬЮТЕРА\ПУТЬ. Это действие можно выполнить следующим образом.

- Откройте раздел «Дополнительные настройки» ESET File Security и нажмите **Обновление**.
- Нажмите **Изменить...** рядом с пунктом «Сервер обновлений» и добавьте новый сервер в формате *\\UNC-ИМЯ_КОМПЬЮТЕРА\ПУТЬ*.
- Выберите вновь добавленный сервер из списка серверов обновлений.

ПРИМЕЧАНИЕ: Для корректной работы путь к папке зеркала в этом случае должен быть указан в формате UNC. Обновления с сопоставленных сетевых дисков могут не работать.

4.3.1.2.4.2 Устранение проблем при обновлении с зеркала

В большинстве случаев проблемы при обновлении с сервера зеркала возникают в связи с одной или несколькими из следующих причин: неверное указание параметров папки зеркала, неверные данные аутентификации для папки зеркала, неверные параметры на рабочих станциях, которые пытаются загружать файлы обновлений с зеркала, а также различные сочетания этих причин. Ниже приведен краткий обзор наиболее часто возникающих проблем при обновлении с зеркала.

Ошибка при подключении ESET File Security к серверу зеркала: обычно происходит при указании неправильных данных сервера обновлений (сетевого пути к папке зеркала), с которого рабочие станции загружают обновления. Для проверки папки нажмите кнопку **Пуск** Windows, выберите **Выполнить**, вставьте имя папки и нажмите кнопку **ОК**. На экран должно быть выведено содержимое папки.

ESET File Security **запрашивает имя пользователя и пароль**: вероятная причина заключается в том, что введены неверные данные аутентификации (имя пользователя и пароль) в разделе обновлений. Имя пользователя и пароль используются для доступа к серверу обновлений, с которого выполняется обновление программы. Убедитесь, что данные аутентификации указаны верно и в правильном формате. Например, *Домен/Имя_пользователя* или *Рабочая_группа/ имя_пользователя* в сочетании с соответствующим паролем. Если сервер зеркала доступен всем участникам сети, это не означает, что у любого пользователя есть к нему доступ. Параметр «Все участники» означает то, что папка доступна всем пользователям домена, а не то, что предоставляется доступ без авторизации. В результате, если папка доступна всем участникам, все же необходимо указать доменное имя пользователя и пароль в настройках обновления.

Ошибка при подключении ESET File Security к серверу зеркала: обмен данными по указанному порту подключения к HTTP-версии зеркала блокируется.

4.3.2 Создание задач обновления

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

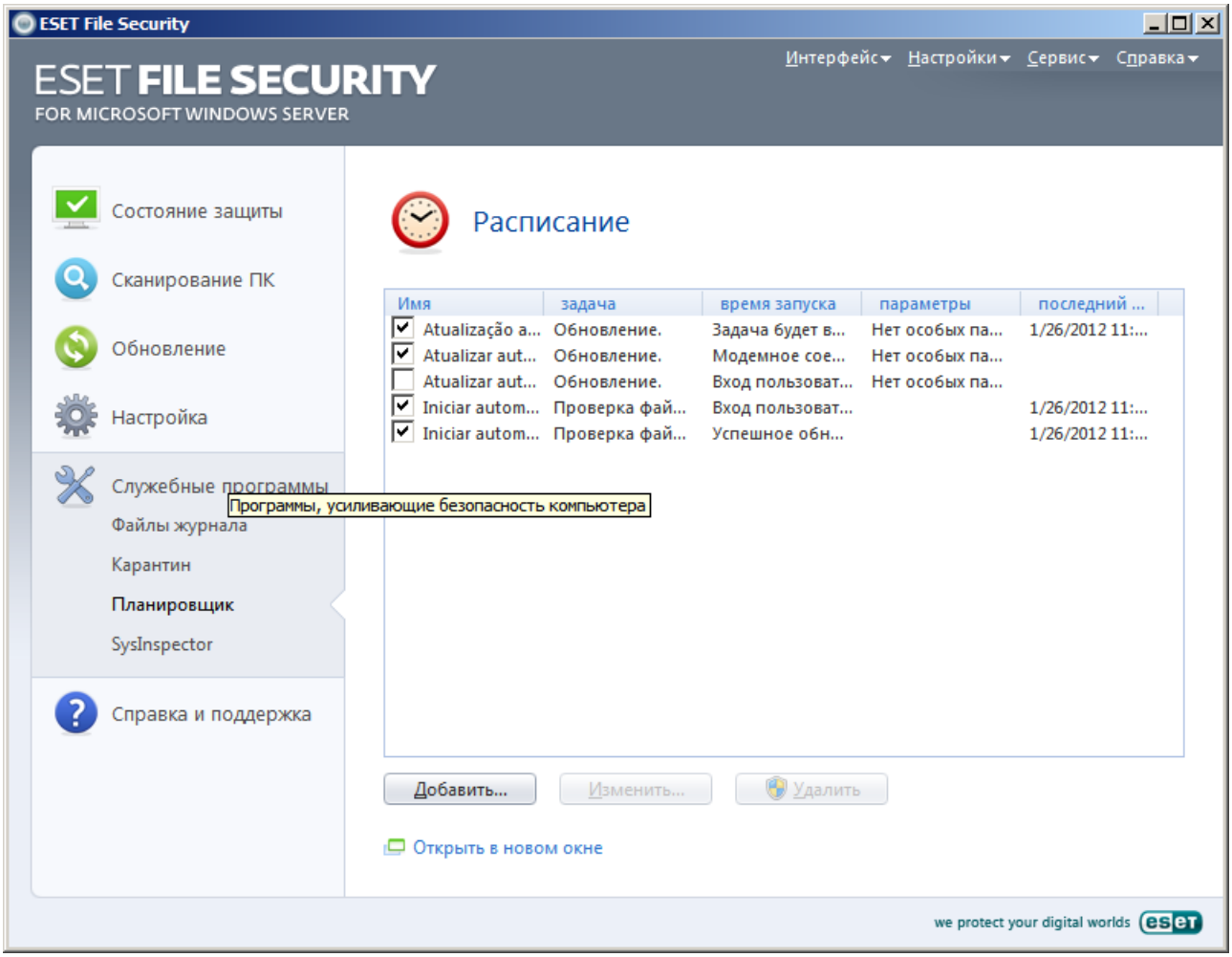
Обновления также можно выполнять как запланированную задачу. Для конфигурирования запланированной задачи перейдите в раздел **Служебные программы** > **Планировщик**. По умолчанию в ESET File Security активированы указанные ниже задачи.

- **Регулярное автоматическое обновление**
- **Автоматическое обновление после установки коммутируемого соединения**
- **Автоматическое обновление после входа пользователя в систему**

Каждую задачу обновления можно изменить в соответствии с конкретными требованиями. В дополнение к существующим по умолчанию задачам обновления можно создать другие задачи с пользовательскими настройками. Дополнительную информацию о создании и настройке задач обновления см. в разделе Планировщик.

4.4 Планировщик

Планировщик доступен, если в ESET File Security активирован расширенный режим. Перейти к **планировщику** можно через главное меню ESET File Security, воспользовавшись пунктом **Служебные программы**. В планировщике содержится полный список всех запланированных задач и их свойства, такие как заданные дата, время и используемый профиль сканирования.



По умолчанию в **планировщике** отображаются следующие запланированные задачи.

- **Регулярное автоматическое обновление**
- **Автоматическое обновление после установки коммутируемого соединения**
- **Автоматическое обновление после входа пользователя в систему**
- **Автоматическая проверка файлов при запуске (после входа пользователя в систему)**
- **Автоматическая проверка файлов при запуске (после обновления базы данных сигнатур вирусов)**

Для изменения параметров существующей запланированной задачи (как существующей по умолчанию, так и пользовательской) щелкните нужную задачу правой кнопкой мыши и выберите в контекстном меню пункт **Изменить...** или выделите задачу, которую необходимо изменить, и нажмите кнопку **Изменить...**.

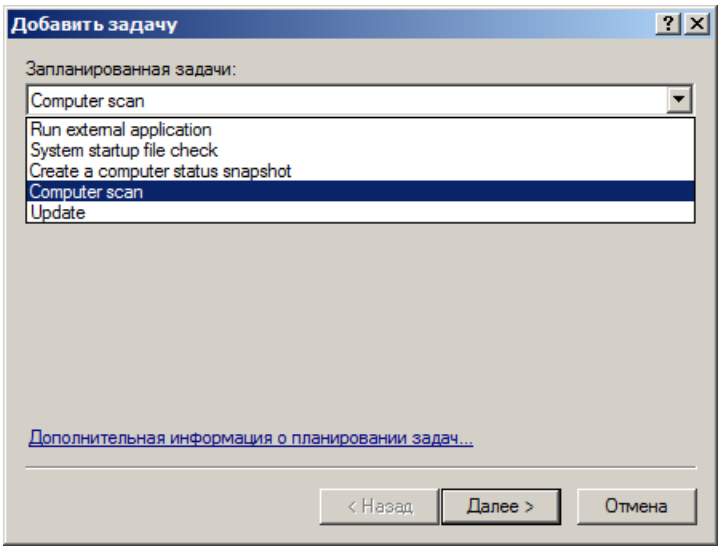
4.4.1 Цель планирования задач

Планировщик управляет запланированными задачами и запускает их с предварительно заданными параметрами и свойствами. Параметры содержат информацию, такую как дата и время исполнения, а также профили обновления, которые следует использовать при выполнении задачи.

4.4.2 Создание новых задач

Для создания задачи в планировщике нажмите кнопку **Добавить...** или щелкните правой кнопкой мыши и выберите в контекстном меню команду **Добавить...**. Доступно пять типов задач.

- **Запуск внешнего приложения**
- **Проверка файлов, исполняемых при запуске системы**
- **Создать снимок состояния компьютера**
- **Сканирование ПК по требованию**
- **Обновление**



Поскольку **обновление** — одна из самых часто используемых запланированных задач, ниже описано добавление задачи обновления.

В раскрывающемся меню **Запланированная задача** выберите пункт **Обновление**. Нажмите кнопку **Далее** и введите название задачи в поле **Название задачи**. Выберите частоту выполнения задачи. Доступны следующие варианты: **Однократно**, **Многократно**, **Ежедневно**, **Еженедельно** и **При определенных условиях**. В зависимости от указанной частоты запуска будут запрошены различные параметры обновления. Затем укажите, какое действие следует предпринимать, если задача не может быть выполнена в установленное время. Доступны следующие три варианта.

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

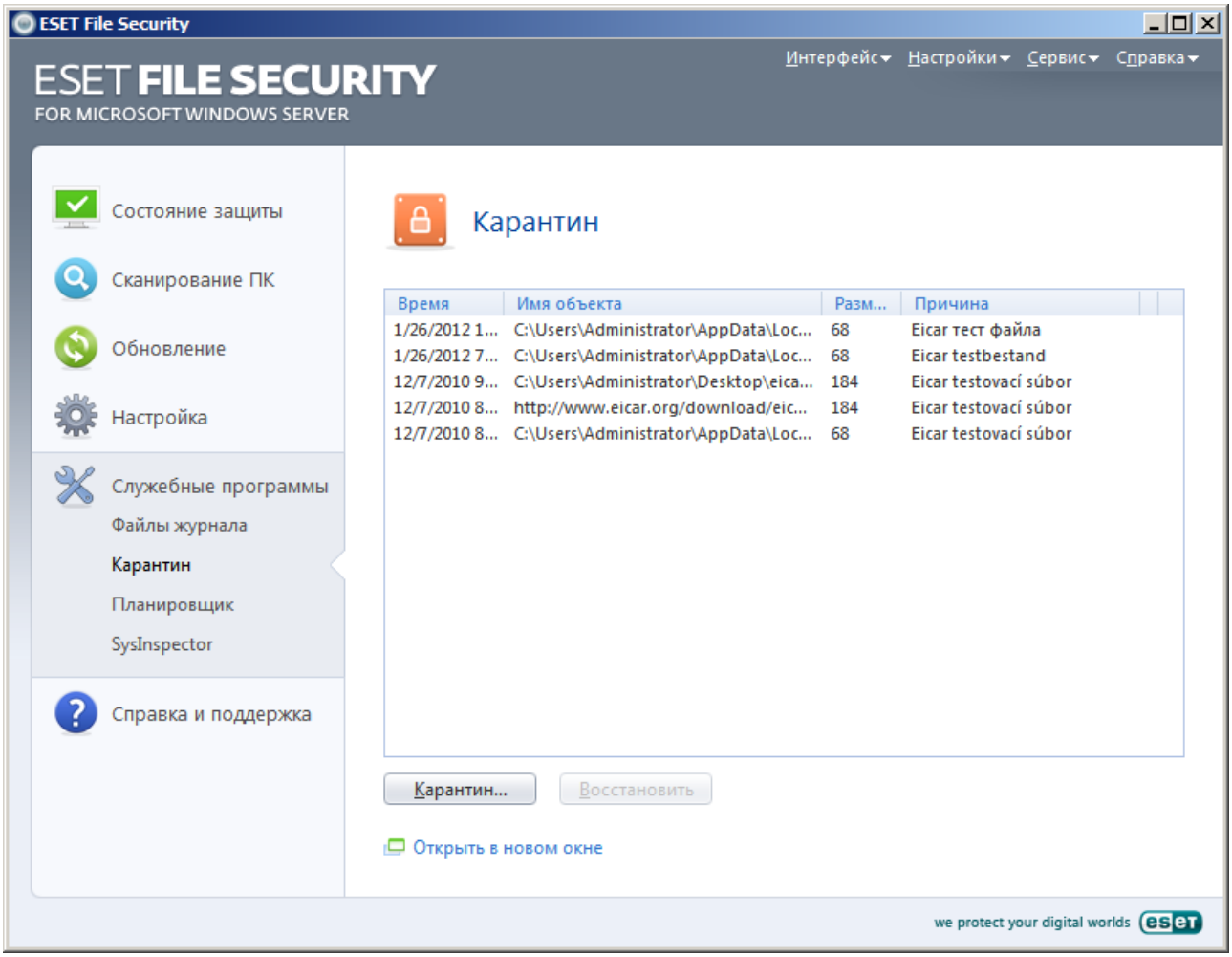
На следующем этапе отображается сводная информация о текущей запланированной задаче. Пункт **Запустить задачу с указанными параметрами** автоматически выбран. Нажмите кнопку **Готово**.

На экран будет выведено диалоговое окно, в котором можно выбрать профили, используемые для запланированной задачи. Можно выбрать основной профиль и вспомогательный, который будет использоваться, если задачу невозможно выполнить с применением основного профиля. Подтвердите настройки, нажав кнопку **OK** в окне **Профили обновления**. Новая задача появится в списке существующих запланированных.

4.5 Карантин

Главная задача карантина заключается в безопасном хранении 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 ESET File Security к зараженным.

Поместить на карантин можно любой файл. Рекомендуется помещать на карантин файлы с подозрительной активностью, которые, тем не менее, не обнаруживаются модулем сканирования защиты от вирусов. Файлы на карантине можно отправить на анализ в лабораторию ESET.



Информацию о файлах, помещенных на карантин, можно просмотреть в виде таблицы, содержащей дату и время помещения файла на карантин, путь к его исходному расположению, его размер в байтах, причину помещения файла на карантин (например, мнение пользователя об объекте) и количество обнаруженных угроз (например, если архив содержит несколько вирусов).

4.5.1 Помещение файлов на карантин

Программа ESET File Security автоматически помещает удаленные файлы на карантин (если этот параметр не был отменен пользователем в окне предупреждения). При желании любой подозрительный файл можно поместить на карантин вручную с помощью кнопки **Карантин...**. При этом исходная копия файла не удаляется. Для этого также можно воспользоваться контекстным меню, нажав правой кнопкой мыши в окне **Карантин** и выбрав пункт **Добавить...**.

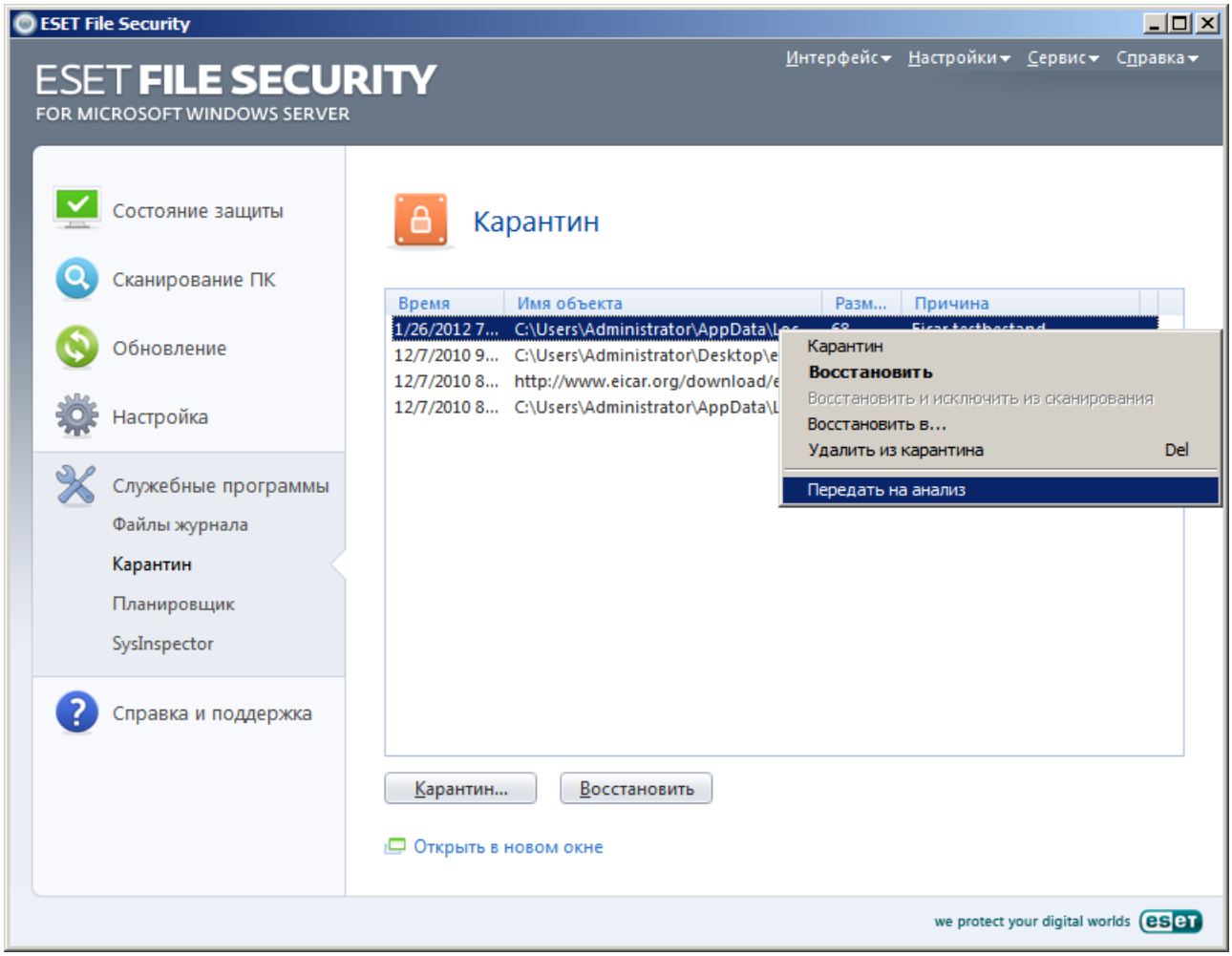
4.5.2 Восстановление из карантина

Файлы, находящиеся на карантине, можно восстановить в исходном месте. Для этого используется функция **Восстановить**. Команда **Восстановить** доступна в контекстном меню, которое открывается правым щелчком мыши по нужному файлу в окне «Карантин». Контекстное меню содержит также функцию **Восстановить в**, которая позволяет восстановить файл в месте, отличном от исходного.

ПРИМЕЧАНИЕ. Если программа поместила незараженный файл на карантин по ошибке, исключите этот файл из процесса сканирования после восстановления и отправьте его в службу поддержки клиентов ESET.

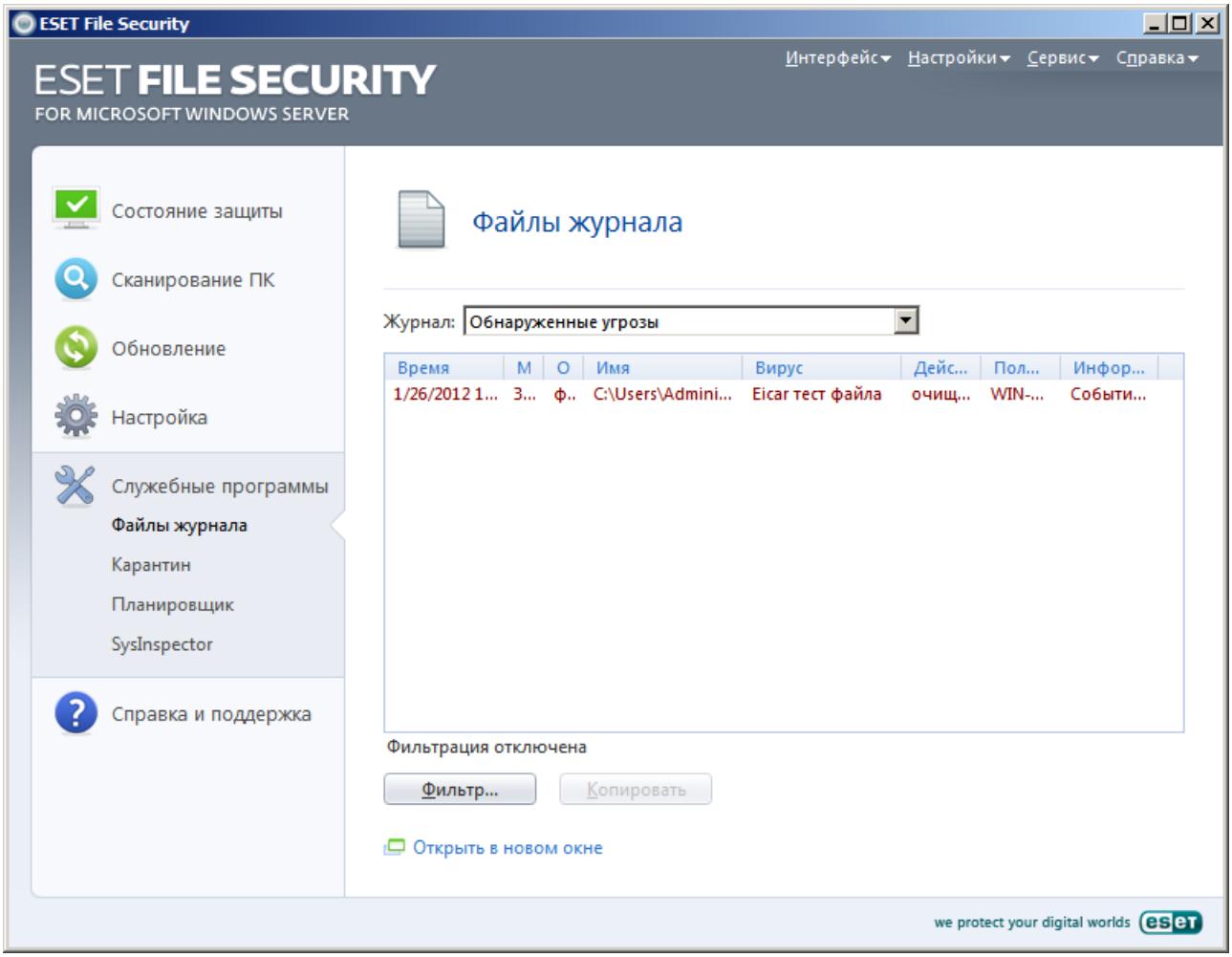
4.5.3 Отправка файла из карантина

Если на карантин помещен подозрительный файл, не обнаруженный программой, или файл неверно квалифицирован как зараженный (например, путем эвристического анализа кода) и помещен на карантин, отправьте его в лабораторию ESET. Чтобы отправить файл из карантина, щелкните его правой кнопкой мыши и выберите в контекстном меню пункт **Передать на анализ**.



4.6 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 неполадок. Оно выполняется в фоновом режиме без вмешательства пользователя. Данные сохраняются в соответствии с текущими параметрами степени детализации журнала. Просматривать текстовые сообщения и журналы можно непосредственно в среде ESET File Security.



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

- **Обнаруженные угрозы**: позволяет просмотреть все данные о событиях, имеющих отношение к обнаружению заражений.
- **События**: этот журнал упрощает устранение проблем. В нем регистрируются все важные действия, выполняемые программой ESET File Security.
- **Сканирование ПК по требованию**: в этом окне отображаются результаты всех выполненных операций сканирования. Чтобы получить подробную информацию о той или иной операции сканирования 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**. Для выбора нескольких записей можно использовать клавиши CTRL и SHIFT.

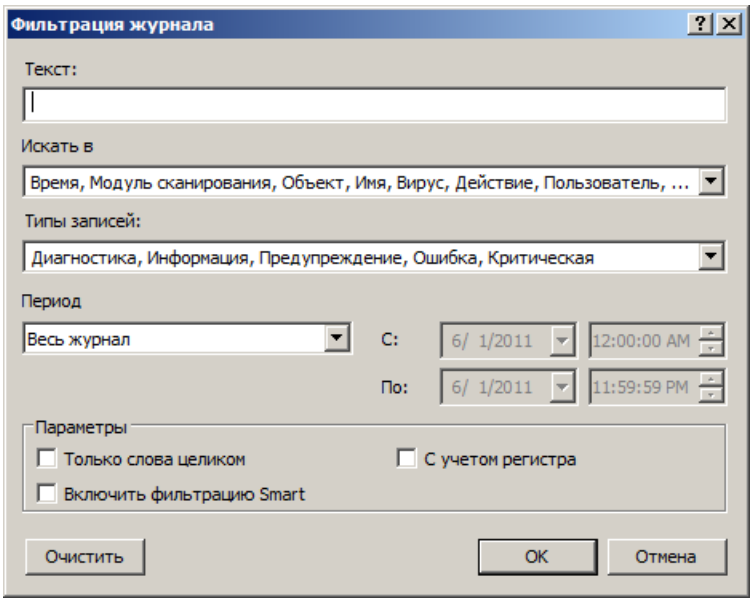
4.6.1 Фильтрация журнала

Фильтрация журнала — удобная функция, помогающая находить записи в файлах журнала, особенно когда записей много и сложно найти нужную информацию.

При использовании фильтрации можно ввести строку **поиска** для фильтра, указать, в каких **столбцах выполнять поиск**, выбрать **типы записей** и задать **период времени**, чтобы сократить количество записей. Если указать определенные параметры фильтрации, только отвечающие таким условиям записи отображаются в окне **Файлы журнала**, что обеспечивает удобный быстрый просмотр.

Для того чтобы открыть окно **Фильтрация журнала**, один раз нажмите кнопку **Фильтр...** в разделе **Служебные программы** > **Файлы журнала** или воспользуйтесь сочетанием клавиш Ctrl + Shift + F.

ПРИМЕЧАНИЕ: Для поиска конкретной записи можно использовать вместо фильтрации журнала функцию Найти в журнале или же применять обе функции совместно.



Если указать определенные параметры фильтрации, только отвечающие таким условиям записи отображаются в окне «Файлы журнала». Это позволяет отфильтровать записи (сократить их количество), благодаря чему найти нужное будет проще. Чем более конкретные параметры фильтра используются, тем меньше результатов вы получите.

Что:: введите строку (слово целиком или частично). Будут показаны только записи, в которых содержится эта строка. Остальные записи не будут видимы, что позволяет удобнее работать с журналом.

Искать в столбцах:: выберите, какие столбцы будут учитываться при фильтрации. Для использования в фильтрации можно отметить один столбец или сразу несколько. По умолчанию отмечаются все столбцы:

- **Время**
- **Модуль**
- **Событие**
- **Пользователь**

Типы записей:: позволяет выбрать, записи какого типа следует показывать. Можно выбрать один конкретный тип записей, несколько типов одновременно или же показывать все типы записей (по умолчанию):

- **Диагностика**
- **Информация**
- **Внимание**
- **Ошибка**
- **Критические**

Период времени:: этот параметр позволяет фильтровать записи по времени. Можно выбрать одно из следующих значений.

- **Весь журнал** (по умолчанию): фильтрация по периоду времени не выполняется, отображается журнал целиком.
- **Последний день**
- **Последняя неделя**
- **Последний месяц**
- **Период**: если выбрать это значение, то можно указать конкретный период времени (дата и время), чтобы на экран выводились только те записи, регистрация которых относится к указанному периоду.

В дополнение к указанным выше параметрам фильтрации можно также использовать ряд **параметров**.

Только слова целиком: будут показаны только записи, соответствующие строке, введенной в текстовом поле **Что**, как целому слову.

С учетом регистра: будут показаны только записи, соответствующие строке, введенной в текстовом поле **Что**, с учетом регистра.

Включить фильтрацию Smart: этот параметр позволяет ESET File Security выполнять фильтрацию с применением своих собственных методов.

По окончании настройки параметров фильтрации нажмите кнопку **OK**, чтобы применить созданный фильтр. В окне **Файлы журнала** будут показаны только записи, соответствующие критериям фильтра.

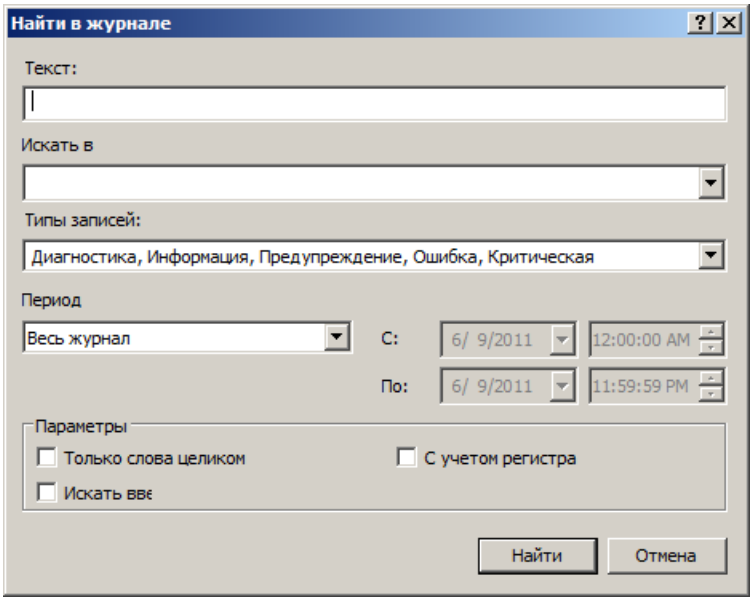
4.6.2 Найти в журнале

В дополнение к фильтрации журнала можно использовать в файлах журнала функцию поиска. Но использовать ее можно и независимо от фильтрации журнала. Эта функция полезна, когда в журналах нужно найти определенные записи. Как и фильтрация журнала, данная функция поиска помогает найти нужную информацию, особенно если количество записей слишком велико.

При использовании функции поиска в журнале можно ввести строку **поиска**, указать, в каких **столбцах выполнять поиск**, выбрать **типы записей** и задать **период времени**, чтобы искать только записи, относящиеся к этому периоду. Если указать определенные параметры поиска, только отвечающие таким условиям записи отображаются в окне «Файлы журнала».

Для выполнения поиска в журналах откройте окно **Найти в журнале**, нажав клавиши Ctrl + f.

ПРИМЕЧАНИЕ: Функцию «Найти в журнале» можно использовать в сочетании с фильтрацией журнала. Сначала можно сократить количество записей, воспользовавшись фильтрацией журнала, а затем приступить к поиску только в уже отфильтрованных записях.



Что:: введите строку (слово целиком или частично). Будут найдены только записи, в которых содержится эта строка. Остальные записи будут опущены.

Искать в столбцах:: выберите, какие столбцы будут учитываться при поиске. Для использования в поиске можно отметить один столбец или сразу несколько. По умолчанию отмечаются все столбцы:

- **Время**
- **Модуль**
- **Событие**
- **Пользователь**

Типы записей:: позволяет выбрать, записи какого типа следует искать. Можно выбрать один конкретный тип записей, несколько типов одновременно или же искать все типы записей (по умолчанию):

- **Диагностика**
- **Информация**
- **Внимание**
- **Ошибка**
- **Критические**

Период времени:: этот параметр позволяет находить только записи, относящиеся к определенному периоду времени. Можно выбрать одно из следующих значений.

- **Весь журнал** (по умолчанию): поиск по периоду времени не выполняется, поиск ведется в журнале целиком.
- **Последний день**
- **Последняя неделя**
- **Последний месяц**
- **Период**: если выбрать это значение, то можно указать конкретный период времени (дата и время), чтобы выполнялся поиск только тех записей, регистрация которых относится к указанному периоду.

В дополнение к указанным выше параметрам поиска можно также использовать ряд **параметров**.

Только слова целиком: будут найдены только записи, соответствующие строке, введенной в текстовом поле **Что**, как целому слову.

С учетом регистра: будут найдены только записи, соответствующие строке, введенной в текстовом поле **Что**, с учетом регистра.

Искать вверх: поиск выполняется с текущего места вверх.

После конфигурирования параметров поиска нажмите кнопку **Найти**, чтобы приступить к поиску. Поиск прекращается, когда находится первая соответствующая его критериям запись. Снова нажмите кнопку **Найти**, чтобы продолжить поиск. Поиск в файлах журнала ведется сверху вниз, начиная с текущего положения (выделенной записи).

4.6.3 Обслуживание журнала

Настройку ведения журнала ESET File Security можно открыть из главного окна программы. Нажмите **Настройка** > **Ввод всего дерева расширенных параметров...** > **Служебные программы** > **Файлы журнала**. Для файлов журнала можно задать параметры, указанные ниже.

- **Удалять записи автоматически**: записи журнала, созданные больше указанного количества дней назад, автоматически удаляются.
- **Оптимизировать файлы журналов автоматически**: включается автоматическая дефрагментация файлов журнала при превышении указанного значения неиспользуемых данных в процентах.
- **Минимальная степень детализации журнала**: задается степень детализации ведения журнала. Возможны следующие варианты.

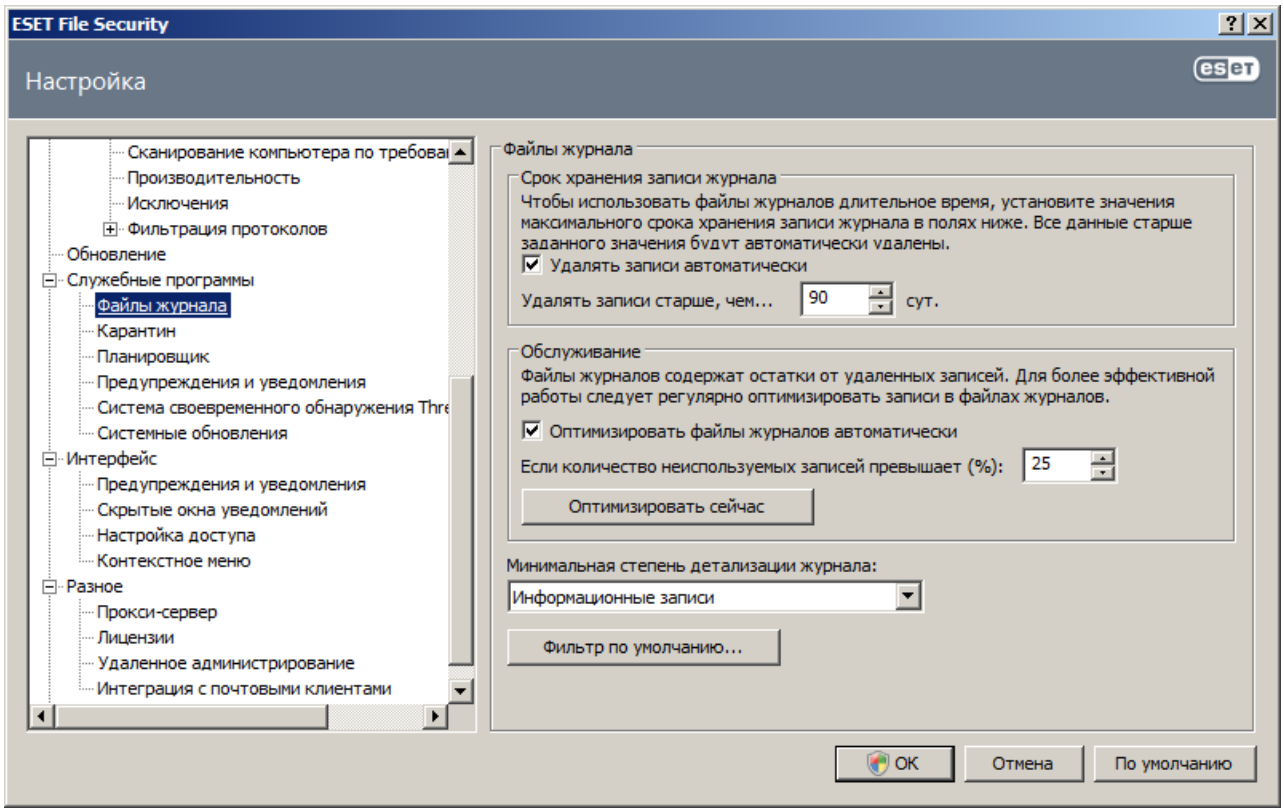
- **Диагностические записи**: записывается информация, необходимая для тонкой настройки программы, а также все перечисленные выше записи.

- **Информационные записи**: записываются информационные сообщения, в том числе сообщения об успешном выполнении обновления, а также все перечисленные выше записи.

- **Предупреждения**: записывается информация обо всех критических ошибках и предупреждениях.

- **Ошибки**: записываются только сообщения типа «Ошибка загрузки файла», а также критические ошибки.

- **Критические предупреждения**: регистрируются только критические ошибки (ошибки запуска защиты от вирусов и т. п.).



4.7 ESET SysInspector

4.7.1 Введение в ESET SysInspector

ESET SysInspector — это приложение, которое тщательно проверяет компьютер и отображает собранные данные в понятном виде. Представляемые данные, такие как информация об установленных драйверах и приложениях, сетевых подключениях и важных записях реестра, позволяют определить причину подозрительного поведения системы, которое может быть вызвано несовместимостью программного или аппаратного обеспечения или заражением вредоносными программами.

Существует два способа воспользоваться приложением ESET SysInspector. Во-первых, можно открыть интегрированную в ESET File Security версию, а, во-вторых, загрузить самостоятельную версию (SysInspector.exe) бесплатно с веб-сайта ESET. Для того чтобы открыть ESET SysInspector, нажмите **Служебные программы** > **ESET SysInspector**. Обе версии аналогичны по своим функциям и имеют одинаковые элементы управления программой. Единственное отличие заключается в том, как осуществляется управление результатами. И загружаемая, и интегрированная версии позволяют экспортировать снимки системы в файл в формате XML и сохранять его на диске. Однако интегрированная версия также дает возможность сохранять снимки системы непосредственно в разделе **Служебные программы** > **ESET SysInspector** (для получения дополнительных сведений см. раздел ESET SysInspector как часть ESET File Security).

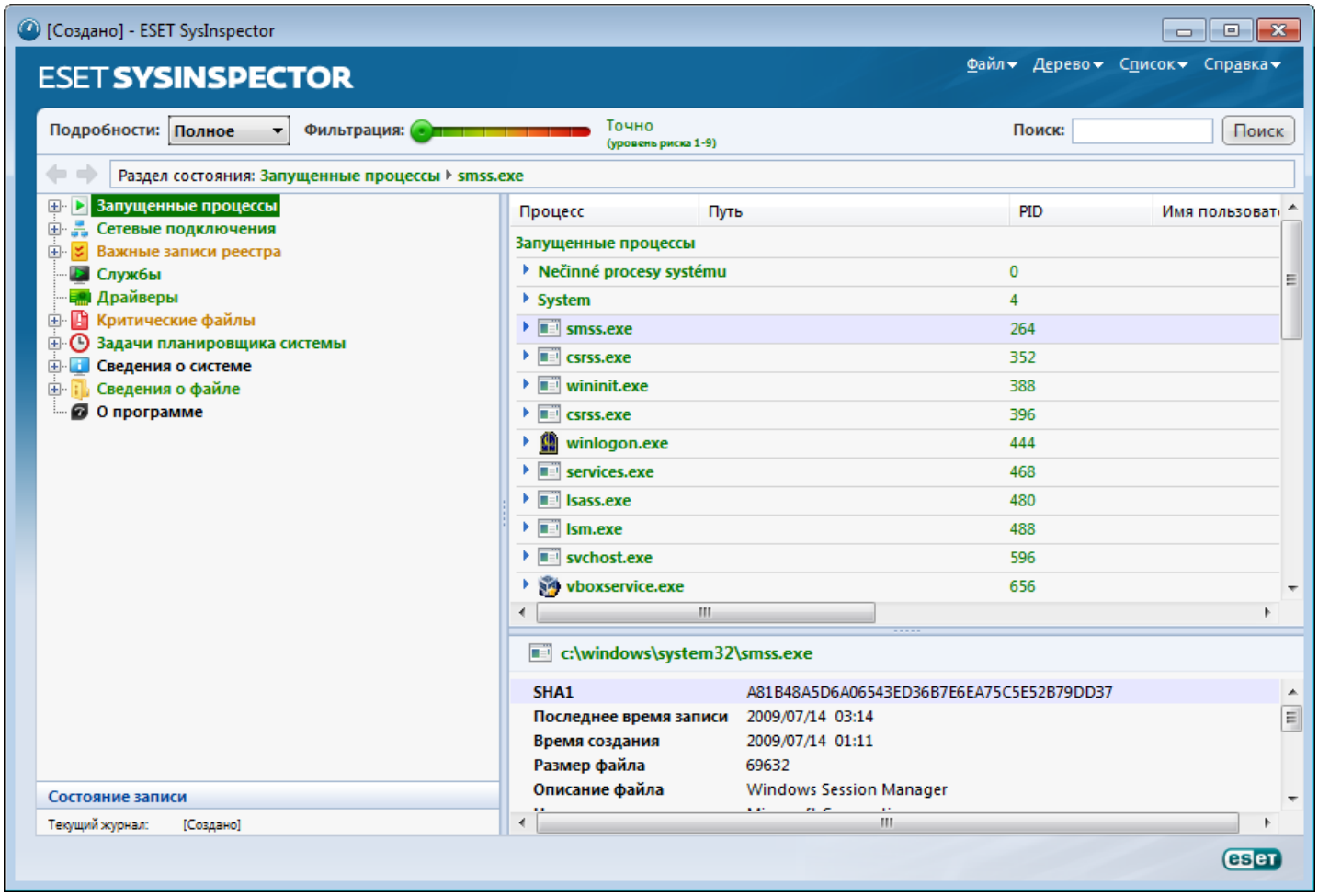
Дайте ESET SysInspector некоторое время на сканирование компьютера. Этот процесс может занять от 10 секунд до нескольких минут в зависимости от конфигурации оборудования, операционной системы и количества установленных на компьютере приложений.

4.7.1.1 Запуск ESET SysInspector

Чтобы запустить ESET SysInspector, достаточно выполнить файл *SysInspector.exe*, загруженный с веб-сайта ESET. Если у вас уже установлен один из продуктов ESET для обеспечения безопасности, ESET SysInspector можно запустить непосредственно из меню «Пуск» (**Программы** > **ESET** > **ESET File Security**). Подождите, пока программа проверяет систему: это может занять несколько минут в зависимости от оборудования и собираемых данных.

4.7.2 Интерфейс пользователя и работа в приложении

Для ясности главное окно разделено на четыре раздела: вверху находятся элементы управления программой, слева — окно навигации, справа по центру — окно описания, а справа внизу — окно подробных сведений. В разделе «Состояние журнала» указаны основные параметры журнала (используемый фильтр, тип фильтра, является ли журнал результатом сравнения и т. д.).



4.7.2.1 Элементы управления программой

В этом разделе описаны все элементы управления программой, доступные в ESET SysInspector.

Файл

Если нажать **Файл**, то можно сохранить данные о текущем состоянии системы для их последующего изучения или открыть ранее сохраненный журнал. Если планируется опубликовать журнал, для его создания рекомендуется использовать пункт меню **Подходит для отправки**. В этом случае из журнала исключается конфиденциальная информация (имя текущего пользователя, имя компьютера, имя домена, права текущего пользователя, переменные среды и т. п.).

ПРИМЕЧАНИЕ. Чтобы просмотреть сохраненные ранее отчеты ESET SysInspector, достаточно просто перетащить их в главное окно программы.

Дерево

Позволяет развернуть или свернуть все узлы, а также экспортировать выделенные разделы в сценарий службы.

Список

Содержит функции, облегчающие навигацию по программе, а также прочие функции, такие как поиск информации в Интернете.

Справка

Содержит сведения о приложении и его функциях.

Подробности

Этот параметр влияет на информацию, выводимую в главном окне, чтобы проще работать с ней. В основном режиме пользователю доступна информация, необходимая для поиска решений стандартных проблем, возникающих в системе. В режиме «Среднее» программа отображает реже используемые сведения. В режиме «Полное» ESET SysInspector выводит на экран всю информацию, необходимую для решения самых нестандартных проблем.

Фильтрация элементов

Фильтрация элементов очень удобна для поиска подозрительных файлов или записей реестра, существующие в системе. С помощью ползунка можно фильтровать элементы по их уровню риска. Если ползунок установлен в крайнее левое положение (уровень риска 1), отображаются все элементы. При перемещении ползунка вправо программа будет отфильтровывать все элементы с уровнем риска, меньшим текущего уровня, и выводить на экран только те элементы, уровень подозрительности которых выше данного уровня. Если ползунок находится в крайнем правом положении, программа отображает только определенно вредоносные элементы.

Все элементы, имеющие уровень риска от 6 до 9, могут представлять угрозу для безопасности. Если вы не используете какие-либо решения по обеспечению безопасности ESET, после нахождения любых таких элементов с помощью ESET SysInspector рекомендуется просканировать компьютер, воспользовавшись ESET Online Scanner. ESET Online Scanner является бесплатной службой.

ПРИМЕЧАНИЕ. Уровень риска элемента легко определяется путем сравнения цвета элемента с цветом на ползунке уровней рисков.

Поиск

Поиск можно использовать для быстрого нахождения определенного элемента по его названию или части названия. Результаты поиска отображаются в окне описания.

Возврат

С помощью стрелок назад и вперед можно переходить в окне описания к ранее отображенной информации. Вместо кнопок перехода назад и вперед можно использовать клавишу Backspace и пробел.

Раздел состояния

Отображает текущий узел в окне навигации.

Внимание! Элементы, выделенные красным цветом, являются неизвестными, поэтому программа помечает их как потенциально опасные. Если элемент выделен красным, это не означает, что соответствующий файл можно удалить. Перед удалением убедитесь, что файлы действительно опасны или не являются необходимыми.

4.7.2.2 Навигация в ESET SysInspector

ESET SysInspector распределяет информацию разных типов по нескольким основным разделам, называемым узлами. Для того чтобы получить дополнительные сведения о каком-либо узле (если таковые есть), разверните его для просмотра вложенных узлов. Для того чтобы открыть или свернуть узел, дважды щелкните название узла или нажмите значок ⊞ или ⊟ рядом с его названием. При перемещении по древовидной структуре узлов в окне навигации о каждом из них доступны различные сведения, отображаемые в окне описания. При переходе к конкретному элементу в окне описания дополнительные сведения об этом элементе можно просмотреть в окне подробных сведений.

Ниже описаны главные узлы в окне навигации и относящиеся к ним сведения в окнах описания и подробной информации.

Запущенные процессы

Этот узел содержит сведения о приложениях и процессах, выполняемых в момент создания журнала. В окне описания могут находиться дополнительные сведения о каждом из процессов, например названия динамических библиотек, используемых процессом, и их местонахождение в системе, название поставщика приложения, уровень риска файла и т. п.

В окне подробной информации содержатся дополнительные сведения об элементах, выбранных в окне описания, такие как размер файла или его хэш.

ПРИМЕЧАНИЕ. Любая операционная система состоит из нескольких важных компонентов ядра, которые

постоянно выполняются и обеспечивают работу базовых принципиально важных функций других пользовательских приложений. В определенных случаях путь к файлам таких процессов отображается в ESET SysInspector с символами «\??\» в начале. Эти символы обеспечивают оптимизацию до запуска таких процессов и с точки зрения системы являются безопасными.

Сетевые подключения

В окне описания перечислены процессы и приложения, которые обмениваются данными через сеть по протоколу, выбранному в окне навигации (TCP или UDP), а также удаленные адреса, с которыми эти приложения устанавливают соединения. Также можно проверить IP-адреса DNS-серверов.

В окне подробной информации содержатся дополнительные сведения об элементах, выбранных в окне описания, такие как размер файла или его хэш.

Важные записи реестра

Содержит список определенных записей реестра, которые часто бывают связаны с различными проблемами в системе, такие как записи, задающие автоматически загружаемые программы, объекты модуля поддержки обозревателя и т. п.

В окне описания также могут быть перечислены файлы, связанные с некоторыми из этих записей. В окне подробных сведений может быть представлена дополнительная информация.

Службы

В окне описания перечислены файлы, зарегистрированные в качестве служб Windows. В окне подробных сведений можно увидеть способ запуска службы, а также просмотреть определенную информацию о файле.

Драйверы

Список драйверов, установленных в системе.

Критические файлы

В окне описания отображается содержимое критически важных файлов операционной системы Microsoft Windows.

Информация о системе

Содержит подробные сведения об оборудовании и программном обеспечении, а также информацию о заданных переменных среды и правах пользователя.

Сведения о файле

Список важных системных файлов и файлов в папке Program Files. В окнах описания и подробных сведений может отображаться дополнительная информация о них.

О программе

Информация о приложении ESET SysInspector.

4.7.2.3 Сравнение

С помощью функции сравнения пользователь может сравнить два существующих журнала. Результатом выполнения этой команды является набор элементов, не совпадающих в этих журналах. Это позволяет отслеживать изменения в системе, что удобно, например, для обнаружения деятельности злонамеренного кода.

После запуска приложение создает новый журнал, который открывается в новом окне. Для того чтобы сохранить журнал в файл, в меню **Файл** выберите пункт **Сохранить журнал**. Сохраненные файлы журналов можно впоследствии открывать и просматривать. Чтобы открыть существующий журнал, в меню **Файл** выберите пункт **Открыть журнал**. В главном окне программы ESET SysInspector в каждый момент времени отображается только один журнал.

Преимущество сравнения двух журналов заключается в том, что можно одновременно просматривать активный в данный момент журнал и сохраненный в файл журнал. Для сравнения журналов в меню **Файл** выберите пункт **Сравнить журналы** и выполните команду **Выбрать файл**. Выбранный журнал будет сравниваться с активным журналом в главном окне программы. В сравнительном журнале отображаются только различия между этими двумя журналами.

ПРИМЕЧАНИЕ. При сравнении двух файлов журналов в меню **Файл** выберите пункт **Сохранить журнал** и сохраните журнал как файл в формате ZIP. В результате будут сохранены оба файла. Если такой файл впоследствии открыть, содержащиеся в нем журналы сравниваются автоматически.

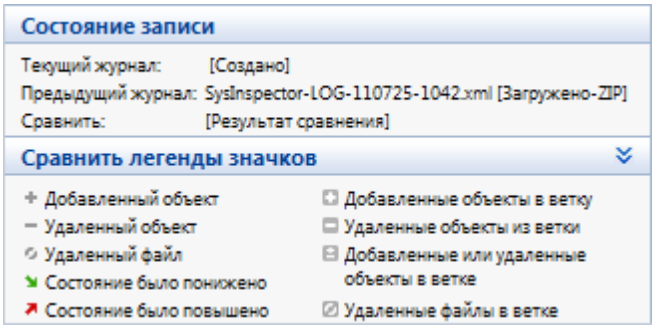
Напротив отображенных элементов ESET SysInspector выводит символы, обозначающие различия между сравниваемыми журналами.

Элементы, помеченные символом «-», присутствуют только в активном журнале, но отсутствуют в открытом журнале, с которым он сравнивается. Элементы, отмеченные знаком +, есть только в открытом журнале и отсутствуют в активном.

Описание всех символов, которые могут отображаться напротив элементов

- + новое значение, отсутствует в предыдущем журнале
- раздел древовидной структуры содержит новые значения
- – удаленное значение, присутствует только в предыдущем журнале
- раздел древовидной структуры содержит удаленные значения
- значение или файл были изменены
- раздел древовидной структуры содержит измененные значения или файлы
- уровень риска снизился, то есть был выше в предыдущем журнале
- уровень риска повысился или был ниже в предыдущей версии журнала

В специальном разделе в левом нижнем углу окна отображается описание всех символов, а также названия сравниваемых журналов.



Любой сравнительный журнал можно сохранить в файл и открыть его позже.

Пример

Создайте и сохраните журнал, содержащий исходную информацию о системе, в файл с названием «предыдущий.xml». После внесения изменений в систему откройте ESET SysInspector и дайте приложению возможность создать новый журнал. Сохраните его в файл с названием *текущий.xml*.

Чтобы отследить различия между этими двумя журналами, в меню **Файл** выберите пункт **Сравнить журналы**. Программа создаст сравнительный журнал, содержащий различиями между сравниваемыми.

Тот же результат можно получить с помощью следующих параметров командной строки:

SysIsnpector.exe текущий.xml предыдущий.xml

4.7.3 Параметры командной строки

В ESET SysInspector можно формировать отчеты из командной строки. Для этого используются перечисленные ниже параметры.

/gen	создание журнала непосредственно из командной строки без запуска графического интерфейса пользователя
/privacy	создание журнала без включения в него конфиденциальной информации
/zip	сохранение журнала непосредственно на диск в сжатом файле
/silent	скрытие индикатора выполнения при создании журнала
/help, /?	отображение сведений о параметрах командной строки

Примеры

Чтобы открыть определенный журнал непосредственно в браузере, воспользуйтесь следующей командой: *SysInspector.exe "c:\клиентский_журнал.xml"*
Чтобы создать журнал в текущей папке, воспользуйтесь следующей командой: *SysInspector.exe /gen*
Чтобы создать журнал в определенной папке, воспользуйтесь следующей командой: *SysInspector.exe /gen="c:\папка\"*
Чтобы создать журнал в определенной папке и в определенном файле, воспользуйтесь следующей командой: *SysInspector.exe /gen="c:\папка\новый_журнал.xml"*
Чтобы создать журнал, из которого исключена конфиденциальная информация, непосредственно в сжатом файле, воспользуйтесь следующей командой: *SysInspector.exe /gen="c:\новый_журнал.zip" /privacy /zip*
Чтобы сравнить два журнала, воспользуйтесь следующей командой: *SysInspector.exe "текущий.xml" "исходный.xml"*

ПРИМЕЧАНИЕ. Если название файла или папки содержит пробел, это название необходимо заключить в кавычки.

4.7.4 Сценарий службы

Сценарий службы — это инструмент, который помогает пользователям ESET SysInspector легко удалять нежелательные объекты с компьютера.

Сценарий службы позволяет целиком или частично экспортировать журнал ESET SysInspector. После экспорта пользователь может пометить нежелательные объекты для удаления. Затем можно запустить сценарий с отредактированным журналом для удаления помеченных объектов.

Сценарий службы для пользователей, имеющих опыт в диагностике компьютерных систем. Неквалифицированное внесение изменений может привести к повреждению операционной системы.

Пример

При наличии подозрения о заражении компьютера вирусом, который не обнаруживается программой защиты от вирусов, можно выполнить описанные далее указания.

- Запустите ESET SysInspector и создайте новый снимок системы.
- Выделите первый элемент в разделе слева (в древовидной структуре), нажмите клавишу CTRL, а затем выберите последний элемент, чтобы пометить все элементы.
- Щелкните правой кнопкой мыши выделенные объекты и выберите пункт контекстного меню **Экспортировать выбранные разделы в сценарий службы** .
- Выделенные объекты будут экспортированы в новый журнал.
- Далее следует наиболее важный этап всей процедуры. Откройте созданный журнал и измените атрибут «-» на «+» для всех объектов, которые нужно удалить. Убедитесь, что не помечены никакие важные файлы или объекты операционной системы.
- Откройте ESET SysInspector, воспользуйтесь пунктом меню **Файл** > **Запустить сценарий службы** и введите путь к сценарию.
- Нажмите кнопку **ОК**, чтобы запустить сценарий.

4.7.4.1 Создание сценариев службы

Для того чтобы создать сценарий, щелкните правой кнопкой мыши любой объект в древовидном меню (в левой панели) главного окна ESET SysInspector. В контекстном меню выберите команду **Экспортировать все разделы в сценарий службы** или **Экспортировать выбранные разделы в сценарий службы**.

ПРИМЕЧАНИЕ. Сценарий службы нельзя экспортировать во время сравнения двух журналов.

4.7.4.2 Структура сценария службы

Первая строка заголовка сценария содержит данные о версии модуля (ev), версии графического интерфейса пользователя (gv) и версии журнала (lv). Эти данные позволяют отслеживать изменения в файле в формате XML, используемом для создания сценария. Они предотвращают появление несоответствий на этапе выполнения. Эту часть сценария изменять не следует.

Остальное содержимое файла разбито на разделы, элементы которых можно редактировать. Те из них, которые должны быть обработаны сценарием, следует пометить. Для этого символ «-» перед элементом нужно заменить на символ «+». Разделы отделяются друг от друга пустой строкой. Каждый раздел имеет собственный номер и название.

01) Running processes (Запущенные процессы)

В этом разделе содержится список процессов, запущенных в системе. Каждый процесс идентифицируется по UNC-пути, а также по хэш-коду CRC16, заключенному в символы звездочки (*).

Пример.

```
01) Running processes:
- \SystemRoot\System32\smss.exe *4725*
- C:\Windows\system32\svchost.exe *FD08*
+ C:\Windows\system32\module32.exe *CF8A*
[...]
```

В данном примере выделен (помечен символом «+») процесс module32.exe. При выполнении сценария этот процесс будет завершен.

02) Loaded modules (Загруженные модули)

В этом разделе перечислены используемые в данный момент системные модули.

Пример.

```
02) Loaded modules:
- c:\windows\system32\svchost.exe
- c:\windows\system32\kernel32.dll
+ c:\windows\system32\khbekhb.dll
- c:\windows\system32\advapi32.dll
[...]
```

В данном примере модуль khbekhb.dll помечен символом «+». При выполнении сценария процессы, использующие данный модуль, распознаются и завершаются.

03) TCP connections (Подключения по TCP)

Этот раздел содержит данные о существующих подключениях по TCP.

Пример.

```
03) TCP connections:
- Active connection: 127.0.0.1:30606 -> 127.0.0.1:55320, owner: ekrn.exe
- Active connection: 127.0.0.1:50007 -> 127.0.0.1:50006,
- Active connection: 127.0.0.1:55320 -> 127.0.0.1:30606, owner: OUTLOOK.EXE
- Listening on *, port 135 (epmap), owner: svchost.exe
+ Listening on *, port 2401, owner: fservice.exe Listening on *, port 445 (microsoft-ds), owner:
System
[...]
```

При запуске сценария обнаруживается владелец сокета помеченных подключений по TCP, после чего сокет останавливается, высвобождая системные ресурсы.

04) UDP endpoints (Конечные точки UDP)

Этот раздел содержит информацию о существующих конечных точках UDP.

Пример.

```
04) UDP endpoints:
- 0.0.0.0, port 123 (ntp)
+ 0.0.0.0, port 3702
- 0.0.0.0, port 4500 (ipsec-msft)
- 0.0.0.0, port 500 (isakmp)
[...]
```

При выполнении сценария определяется владелец сокета помеченных конечных точек UDP, после чего сокет останавливается.

05) DNS server entries (Записи DNS-сервера)

Этот раздел содержит информацию о текущей конфигурации DNS-сервера.

Пример.

```
05) DNS server entries:
+ 204.74.105.85
- 172.16.152.2
[...]
```

При выполнении сценария помеченные записи DNS-сервера удаляются.

06) Important registry entries (Важные записи реестра)

Этот раздел содержит информацию о важных записях реестра.

Пример.

```
06) Important registry entries:
* Category: Standard Autostart (3 items)
 HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Run
- HotKeysCmds = C:\Windows\system32\hkcmd.exe
- IgfxTray = C:\Windows\system32\igfxtray.exe
 HKCU\SOFTWARE\Microsoft\Windows\CurrentVersion\Run
- Google Update = "C:\Users\antoniak\AppData\Local\Google\Update\GoogleUpdate.exe" /c
* Category: Internet Explorer (7 items)
 HKLM\Software\Microsoft\Internet Explorer\Main
+ Default_Page_URL = http://thatcrack.com/
[...]
```

При выполнении сценария помеченные записи будут удалены, сведены к 0-разрядным значениям или же будут восстановлены их значения по умолчанию. Действия, применяемые к конкретным записям, зависят от категории и значения записи реестра.

07) Services (Службы)

Этот раздел содержит список служб, зарегистрированных в системе.

Пример.

```
07) Services:
- Name: Andrea ADI Filters Service, exe path: c:\windows\system32\aeadisrv.exe, state: Running,
startup: Automatic
- Name: Application Experience Service, exe path: c:\windows\system32\aelupsvc.dll, state: Running,
startup: Automatic
- Name: Application Layer Gateway Service, exe path: c:\windows\system32\alg.exe, state: Stopped,
startup: Manual
[...]
```

При выполнении сценария помеченные службы, а также все зависящие от них службы будут остановлены и удалены.

08) Drivers (Драйверы)

В этом разделе перечислены установленные драйверы.

Пример.

```
08) Drivers:
- Name: Microsoft ACPI Driver, exe path: c:\windows\system32\drivers\acpi.sys, state: Running,
startup: Boot
- Name: ADI UAA Function Driver for High Definition Audio Service, exe path: c:\windows\system32
\drivers\adihdaud.sys, state: Running, startup: Manual
[...]
```

При выполнении сценария регистрация выбранных драйверов отменяется, а драйверы удаляются.

09) Critical files (Критические файлы)

Этот раздел содержит информацию о файлах, являющихся критическими для операционной системы.

Пример.

```
09) Critical files:
* File: win.ini
- [fonts]
- [extensions]
- [files]
- MAPI=1
[...]
* File: system.ini
- [386Enh]
- woafont=dosapp.fon
- EGA80WOA.FON=EGA80WOA.FON
[...]
* File: hosts
- 127.0.0.1 localhost
- ::1 localhost
[...]
```

Либо выбранные элементы будут удалены, либо будут восстановлены их исходные значения.

4.7.4.3 Выполнение сценариев службы

Пометьте все нужные объекты, сохраните и закройте сценарий. Запустите измененный сценарий непосредственно из главного окна ESET SysInspector с помощью команды **Запустить сценарий службы** в меню «Файл». При открытии сценария на экран будет выведено следующее сообщение: **«Выполнить сценарий службы "%Scriptname%"?»** После подтверждения может появиться еще одно предупреждение, сообщающее о попытке запуска неподписанного сценария. Для того чтобы запустить сценарий, нажмите кнопку **Запуск**.

В диалоговом окне будет подтверждено успешное выполнение сценария.

Если сценарий удалось обработать только частично, на экран будет выведено диалоговое окно с таким сообщением: **«Сценарий службы частично выполнен. Просмотреть отчет об ошибках?»** Для того чтобы просмотреть полный отчет об ошибках, в котором перечислены операции, нажмите кнопку **Да**.

Если сценарий не был распознан, на экран будет выведено диалоговое окно с таким сообщением: **«Выбранный сценарий службы не подписан. Выполнение неподписанных и неизвестных сценариев может привести к повреждению данных на компьютере. Выполнить сценарий и все действия?»** Это может быть связано с несоответствиями в сценарии (поврежден заголовок, повреждено название раздела, пропущена пустая разделительная строка и т. д.). В этом случае откройте файл сценария и исправьте ошибки или создайте новый сценарий службы.

4.7.5 Сочетания клавиш

Ниже представлен список сочетаний клавиш, которые можно использовать при работе с ESET SysInspector.

Файл

Ctrl + O	открытие существующего журнала
Ctrl + S	сохранение созданных журналов

Создать

Ctrl + G	стандартная проверка состояния системы
Ctrl + H	выполнение проверки системы, при которой также может регистрироваться конфиденциальная информация

Фильтрация элементов

1, O	безопасные элементы, отображаются элементы с уровнем риска от 1 до 9
2	безопасные элементы, отображаются элементы с уровнем риска от 2 до 9
3	безопасные элементы, отображаются элементы с уровнем риска от 3 до 9
4, U	неизвестные элементы, отображаются элементы с уровнем риска от 4 до 9
5	неизвестные элементы, отображаются элементы с уровнем риска от 5 до 9
6	неизвестные элементы, отображаются элементы с уровнем риска от 6 до 9
7, B	опасные элементы, отображаются элементы с уровнем риска от 7 до 9
8	опасные элементы, отображаются элементы с уровнем риска от 8 до 9
9	опасные элементы, отображаются элементы с уровнем риска 9
-	понижение уровня риска
+	повышение уровня риска
Ctrl + 9	выбор режима фильтрации, равный или более высокий уровень
Ctrl + O	выбор режима фильтрации, только равный уровень

Представление

Ctrl + 5	просмотр по производителям, все производители
Ctrl + 6	просмотр по производителям, только Microsoft
Ctrl + 7	просмотр по производителям, все другие производители
Ctrl + 3	отображение полных сведений
Ctrl + 2	отображение сведений средней степени подробности
Ctrl + 1	основной вид
BackSpace	переход на один шаг назад
Пробел	переход на один шаг вперед
Ctrl + W	разворачивание дерева
Ctrl + Q	сворачивание дерева

Прочие элементы управления

Ctrl + T	переход к исходному местоположению элемента после его выделения в результатах поиска
Ctrl + P	отображение основных сведений об элементе
Ctrl + A	отображение всех сведений об элементе
Ctrl + C	копирование дерева текущего элемента
Ctrl + X	копирование элементов
Ctrl + B	поиск сведений о выбранных файлах в Интернете
Ctrl + L	открытие папки, в которой находится выделенный файл
Ctrl + R	открытие соответствующей записи в редакторе реестра
Ctrl + Z	копирование пути к файлу (если элемент связан с файлом)
Ctrl + F	переход в поле поиска
Ctrl + D	закрытие результатов поиска
Ctrl + E	запуск сценария службы

Сравнение

Ctrl + Alt + O	открытие исходного или сравниваемого с ним журнала
Ctrl + Alt + R	отмена сравнения
Ctrl + Alt + 1	отображение всех элементов
Ctrl + Alt + 2	отображение только добавленных элементов, в журнале отображаются только элементы из текущего журнала
Ctrl + Alt + 3	отображение только удаленных элементов, в журнале отображаются только элементы из предыдущего журнала
Ctrl + Alt + 4	отображение только замененных элементов (в том числе файлов)
Ctrl + Alt + 5	отображение только различий между журналами
Ctrl + Alt + C	отображение сравнения
Ctrl + Alt + N	отображение текущего журнала
Ctrl + Alt + P	открытие предыдущего журнала

Разное

F1	просмотр справки
Alt + F4	закрытие программы
Alt + Shift + F4	закрытие программы без вывода запроса
Ctrl + I	статистика журнала

4.7.6 Часто задаваемые вопросы

Требуются ли для запуска ESET SysInspector права администратора?

Хотя для запуска ESET SysInspector права администратора не требуются, некоторые из собираемых этим приложением данных доступны только для учетной записи администратора. Запуск под учетной записью обычного пользователя или пользователя с ограниченным доступом приведет к сбору меньшего объема данных о системе.

Создает ли ESET SysInspector файл журнала?

ESET SysInspector может создать файл журнала с конфигурацией системы. Для сохранения такого журнала выберите в главном меню команду **Файл** > **Сохранить журнал**. Журналы сохраняются в формате XML. По умолчанию файлы сохраняются в папке *%USERPROFILE%\Мои документы* в файл с именем «SysInpsector-%COMPUTERNAME%-ГГММДД-ЧЧММ.XML». Перед сохранением файла журнала можно изменить его местоположение и название.

Как просмотреть файл журнала ESET SysInspector?

Для просмотра журнала, созданного в ESET SysInspector, запустите программу и выберите в главном меню команду **Файл** > **Открыть журнал**. Файлы журнала также можно перетаскивать в окно приложения ESET SysInspector. Если вы часто просматриваете файлы журнала ESET SysInspector, рекомендуется создать на рабочем столе ярлык для файла SYSINSPECTOR.EXE. После этого просматриваемые файлы можно просто перетаскивать на этот ярлык. Из соображений безопасности в ОС Windows Vista/7 может быть не разрешено перетаскивать элементы между окнами, имеющими разные параметры безопасности.

Доступна ли спецификация для формата файлов журнала? Существует ли пакет SDK?

В настоящее время ни спецификация файла журнала, ни пакет SDK недоступны, поскольку программа все еще находится на стадии разработки. Возможно, мы выпустим их после выхода конечной версии программы в зависимости от отзывов пользователей и наличия интереса.

Как ESET SysInspector оценивает риск определенного объекта?

В большинстве случаев ESET SysInspector присваивает объектам (файлам, процессам, разделам реестра и т. п.) уровни риска, используя наборы эвристических правил, которые изучают характеристики каждого объекта и затем оценивают вероятность их вредоносного действия. На основе такого эвристического анализа объектам присваивается уровень риска от 1 — безопасно (зеленый) до 9 — опасно (красный). В панели навигации слева разделы окрашиваются в разные цвета в зависимости от самого высокого уровня риска содержащихся в них объектов.

Означает ли уровень риска «6 — неизвестно (красный)», что объект является опасным?

Анализ ESET SysInspector не гарантирует, что какой-либо объект является вредоносным. Такая оценка должна выполняться специалистом по безопасности. Приложение ESET SysInspector разработано для того, чтобы специалист по безопасности имел возможность быстро оценить, какие объекты системы следует изучить и проверить их необычное поведение.

Зачем ESET SysInspector в ходе работы подключается к Интернету?

Как и многие приложения, приложение ESET SysInspector подписано цифровой подписью («сертификатом»), которая гарантирует, что издателем данного программного обеспечения является компания ESET и что само программное обеспечение не было изменено. Для проверки сертификата операционная система связывается с центром сертификации, чтобы подтвердить подлинность издателя программного обеспечения. Это нормальное поведение всех программ с цифровыми подписями в ОС Microsoft Windows.

Что такое технология Anti-Stealth?

Технология Anti-Stealth обеспечивает эффективное обнаружение руткитов.

Если система подвергается атаке злонамеренного кода, который ведет себя как руткит, пользователь подвергается риску повреждения или воровства данных. Без специального инструмента для борьбы с руткитами обнаружить их практически невозможно.

Почему иногда в файлах, помеченных как «Подписано MS», в записи «Название компании» стоит название другой компании?

При попытке идентифицировать цифровую подпись исполняемого файла ESET SysInspector сначала проверяет

наличие в файле встроенной цифровой подписи. В этом случае найденная в файле цифровая подпись будет использовать для проверки. Если же в файле отсутствует цифровая подпись, ESI начинает поиск соответствующего CAT-файла (в каталоге безопасности *%systemroot%\system32\catroot*), в котором содержатся сведения об обрабатываемом исполняемом файле. Если соответствующий CAT-файл найден, его цифровая подпись будет применена в процессе проверки исполняемого файла.

Поэтому иногда в некоторых файлах с пометкой «Подписано MS» имеется другая запись о названии компании.

Пример.

В ОС Windows 2000 есть приложение HyperTerminal, которое находится в папке *C:\Program Files\Windows NT*. Исполняемый файл приложения не имеет цифровой подписи, однако программа ESET SysInspector помечает его в качестве подписанного корпорацией Microsoft. Причиной этому служит ссылка в файле *C:\WINNT\system32\CatRoot\{F750E6C3-38EE-11D1-85E5-00C04FC295EE}\sp4.cat*, которая указывает на файл *C:\Program Files\Windows NT\hypertrm.exe* (основной исполняемый файл приложения HyperTerminal), а файл *sp4.cat* имеет цифровую подпись Microsoft.

4.7.7 ESET SysInspector как часть ESET File Security

Для того чтобы открыть ESET SysInspector в ESET File Security, в меню **Служебные программы** выберите пункт **ESET SysInspector**. В окне ESET SysInspector используется система управления, аналогичная той, которая применяется в окнах журналов сканирования компьютера и запланированных задач. Для выполнения всех операций со снимками системы (создание, просмотр, сравнение, удаление и экспорт) достаточно одного или двух щелчков мыши.

Окно ESET SysInspector содержит основные сведения о созданных снимках состояния, такие как время создания, краткий комментарий, имя создавшего снимок пользователя и состояние снимка.

Для **сравнения**, **добавления** и **удаления** снимков используются соответствующие кнопки, расположенные в окне ESET SysInspector под списком снимков. Эти функции также можно вызвать из контекстного меню. Для просмотра выбранного снимка системы используется команда контекстного меню **Просмотреть**. Чтобы экспортировать выделенный снимок в файл, щелкните его правой кнопкой и выберите в контекстном меню пункт **Экспорт...**.

Далее приведено подробное описание доступных функций.

- **Сравнить** : позволяет сравнить два существующих журнала. Эта функция удобна, если нужно найти различия между текущим и более старым журналом. Для сравнения необходимо выбрать два снимка состояния.
- **Добавить** : создание новой записи. Перед созданием записи нужно ввести краткий комментарий к ней. Ход создания формируемого в данный момент снимка отображается в столбце **Состояние** . Все уже созданные снимки помечены надписью **Создано** .
- **Удаление** : удаление записей из списка.
- **Экспорт...**: сохранение выделенной записи в файл в формате XML (также есть возможность создания заархивированной версии).

4.8 ESET SysRescue

ESET SysRescue — это утилита для создания загрузочного диска, содержащего ESET File Security. Главным преимуществом ESET SysRescue является то, что программа ESET File Security работает независимо от операционной системы компьютера, имея при этом доступ к жесткому диску и всей файловой системе. Это позволяет удалять такие заражения, которые в обычной ситуации (например, при запущенной операционной системе и т. п.) удалить невозможно.

4.8.1 Минимальные требования

ESET SysRescue работает в среде предустановки Microsoft Windows версии 2.x, созданной на основе Windows Vista. Среда предустановки Windows является частью бесплатного пакета автоматической установки Windows (Windows AIK), поэтому перед созданием компакт-диска ESET SysRescue необходимо установить Windows AIK (http://go.eset.eu/AIK). Поскольку поддержка среды предустановки Windows ограничивается ее 32-разрядной версией, необходимо использовать 32-разрядный установочный пакет ESET File Security при создании ESET SysRescue в 64-разрядных операционных системах. Средство ESET SysRescue поддерживает пакет Windows AIK версии 1.1 и более поздних. Средство ESET SysRescue доступно в составе ESET File Security версии 4.0 и более поздних.

Поддерживаемые операционные системы

- Windows 7
- Windows Vista
- Windows Vista с пакетом обновления 1
- Windows Vista с пакетом обновления 2
- Windows Server 2008
- Windows Server 2003 с пакетом обновления 1 с KB926044
- Windows Server 2003 с пакетом обновления 2
- Windows XP с пакетом обновления 2 с KB926044
- Windows XP с пакетом обновления 3

4.8.2 Создание компакт-диска аварийного восстановления

Чтобы запустить мастер ESET SysRescue, выберите в меню **Пуск** > **Программы** > **ESET** > **ESET File Security** > **ESET SysRescue**.

На первом этапе мастер определяет наличие в системе установленного пакета Windows AIK и подходящего для создания загрузочного носителя устройства записи. Если пакет *Windows AIK* не установлен на компьютере, установлен некорректно или поврежден, мастер предложит установить этот пакет или ввести путь к папке с Windows AIK (http://go.eset.eu/AIK).

На следующем этапе предлагается выбрать носитель для размещения на нем файлов ESET SysRescue.

4.8.3 Выбор объекта

Помимо компакт-диска, DVD-диска и USB-устройства, ESET SysRescue также можно сохранить в файл образа диска ISO. Впоследствии этот файл с образом ISO можно записать на компакт- или DVD-диск или использовать его другим способом (например, в виртуальной среде VMware или VirtualBox).

Если в качестве целевого носителя было выбрано USB-устройство, загрузка с него может не работать на некоторых компьютерах. Некоторые версии BIOS могут сообщать о наличии проблем при обмене данными между BIOS и диспетчером загрузки (например, в Windows Vista), в результате чего загрузка завершается следующим сообщением об ошибке:

```
file : \boot\bcd
status : 0xc000000e
info : an error occurred while attemping to read the boot configuration data (ошибка при попытке чтения конф
```

При появлении этого сообщения рекомендуется выбрать в качестве носителя компакт-диск вместо USB-устройства.

4.8.4 Параметры

Прежде чем приступать к созданию ESET SysRescue, мастер установки выведет на экран параметры компиляции на последнем этапе мастера ESET SysRescue. Их можно изменить, нажав кнопку **Изменить...**. Доступны следующие параметры.

- Папки
- Противовирусная программа ESET
- Дополнительно
- Интернет-протокол
- Загрузочное USB-устройство (когда в качестве объекта выбрано USB-устройство)
- Запись (когда в качестве объекта выбран дисковод компакт- или DVD-дисков)

Если не указан установочный пакет MSI или на компьютере не установлено никакое решение обеспечения безопасности ESET, кнопка **Создать** будет неактивна. Чтобы выбрать установочный пакет, нажмите кнопку **Изменить** и перейдите на вкладку **Противовирусная программа ESET**. Если не ввести имя пользователя и пароль (**Изменить** > **Противовирусная программа ESET**), кнопка **Создать** также будет неактивна.

4.8.4.1 Папки

Папка временного хранения — это рабочий каталог для файлов, необходимый для компиляции ESET SysRescue.

Папка ISO — это папка, в которую сохраняется полученный файл ISO после завершения компиляции.

В списке на этой вкладке перечислены все локальные и сопоставленные сетевые диски с указанием доступного на них места. Если какие-то из показанных папок располагаются на диске, где свободного места недостаточно, рекомендуется выбрать другой диск, на котором места больше. В противном случае недостаток свободного места приведет к досрочному завершению компиляции.

Внешние приложения: позволяет указать дополнительные программы, которые будут выполняться или устанавливаться после загрузки с носителя ESET SysRescue.

Включить внешние приложения: позволяет добавить внешние программы в компиляцию ESET SysRescue.

Выбранная папка: папка, где расположены программы, которые следует добавить на диск ESET SysRescue.

4.8.4.2 Противовирусная программа ESET

При создании компакт-диска ESET SysRescue можно выбрать один из двух источников файлов ESET для компилятора.

Папка ESS/EAV — файлы, уже содержащиеся в папке, в которую установлен программный продукт ESET.

Файл MSI — файлы, которые содержатся в установочном файле MSI.

Далее можно обновить местоположение nup-файлов. Обычно следует выбирать вариант по умолчанию **ESS/папка EAV/MSI-файл**. В некоторых случаях можно выбрать собственную **папку обновлений**, например, чтобы использовать более старую или новую версию базы данных сигнатур вирусов.

В качестве источника имени пользователя и пароля можно использовать один из двух следующих вариантов.

Установленная программа ESS/EAV: имя пользователя и пароль копируются из установленной программы ESET File Security.

От пользователя: имя пользователя и пароль вводятся в соответствующие текстовые поля, расположенные ниже.

ПРИМЕЧАНИЕ. Программа ESET File Security на компакт-диске ESET SysRescue обновляется либо через Интернет, либо из решения ESET Security, установленного на компьютере, на котором запускается компакт-диск ESET SysRescue.

4.8.4.3 Дополнительные параметры

На вкладке **Дополнительно** можно оптимизировать параметры компакт-диска ESET SysRescue в соответствии с объемом оперативной памяти компьютера. Чтобы записать содержимое компакт-диска в оперативную память (ОЗУ), выберите вариант **576 МБ и больше**. Если выбрать пункт **менее 576 МБ**, при работе среды предустановки Windows будет постоянно происходить обращение к компакт-диску восстановления.

В разделе **Внешние драйверы** можно вставить драйверы для конкретного оборудования (обычно для сетевого адаптера). Хотя среда предустановки Windows основана на ОС Windows Vista с пакетом обновления 1, которая поддерживает самое разнообразное оборудование, иногда оборудование все же не распознается. В этом случае нужно будет добавить драйвер вручную. Добавить драйвер в компиляцию ESET SysRescue можно двумя способами: вручную (кнопка **Добавить**) и автоматически (кнопка **Авто поиск**). При добавлении драйвера вручную необходимо указать путь к соответствующему INF-файлу (в той же папке должен находиться и SYS-файл). В случае автоматического добавления драйвер находится в операционной системе данного компьютера автоматически. Режим автоматического добавления рекомендуется использовать только в том случае, если средство ESET SysRescue установлено на компьютере с такой же сетевой картой, как и на компьютере, на котором был создан диск ESET SysRescue. При создании диска ESET SysRescue драйвер добавляется в компиляцию, поэтому пользователю впоследствии не приходится его искать.

4.8.4.4 Интернет-протокол

В этом разделе можно конфигурировать базовую информацию сети и настраивать предварительно заданные подключения после выполнения ESET SysRescue.

Выберите **Автоматический частный IP-адрес**, чтобы получать IP-адрес автоматически с сервера DHCP.

Либо же это сетевое подключение может использовать заданный вручную IP-адрес (также называемый статическим IP-адресом). Выберите вариант **Особый**, чтобы конфигурировать соответственные параметры IP. Если выбрать этот вариант, нужно указать **IP-адрес** и (для локальных сетей и высокоскоростных подключений к Интернету) **маску подсети**. Введите адреса основного и дополнительного серверов DNS в поля **Предпочтительный сервер DNS** и **Дополнительный сервер DNS**.

4.8.4.5 Загрузочное USB-устройство

Если в качестве целевого носителя было выбрано USB-устройство, на вкладке **Загрузочное USB-устройство** можно указать один из доступных USB-носителей (если доступно несколько USB-устройств).

Выберите нужное **устройство**, на которое будет установлено приложение ESET SysRescue.

Внимание: Выбранное USB-устройство будет отформатировано при создании ESET SysRescue. Все данные на этом устройстве будут удалены.

Если выбрать вариант **Быстрое форматирование**, то при форматировании будут удалены все файлы из раздела, но диск не будет сканироваться на наличие поврежденных секторов. Используйте этот вариант, если USB-устройство уже форматировалось ранее и вы уверены, что оно не повреждено.

4.8.4.6 Запись

Если в качестве целевого носителя выбран компакт- или DVD-диск, на вкладке **Запись** можно задать дополнительные параметры записи.

Удалить файл ISO: установите этот флажок, чтобы удалить временные файлы ISO после создания компакт-диска ESET SysRescue.

Удаление разрешено: этот параметр позволяет сделать выбор между быстрой и полной очисткой диска.

Записывающее устройство: выберите дисковод, который будет использоваться для записи.

Предупреждение. Этот параметр установлен по умолчанию. При использовании перезаписываемого компакт- или DVD-диска все данные на нем будут стерты.

В разделе «Носитель» указаны сведения о диске в дисководе.

Скорость записи: выберите нужную скорость из раскрывающегося меню. При выборе скорости необходимо учитывать возможности записывающего устройства и тип компакт- или DVD-диска.

4.8.5 Работа с ESET SysRescue

Для эффективного использования аварийного восстановления с компакт- и DVD-дисков или USB-устройств необходимо загрузить компьютер с загрузочного носителя, на котором установлено средство ESET SysRescue. Порядок загрузки настраивается в BIOS. Также на этапе загрузки компьютера можно использовать меню загрузки; обычно оно вызывается с помощью клавиш F9–F12 в зависимости от версии материнской платы и BIOS.

После загрузки с загрузочного устройства будет запущена программа ESET File Security. Поскольку средство ESET SysRescue используется лишь в особых случаях, некоторые модули защиты и функции программы, имеющиеся в стандартной версии ESET File Security, не нужны, а потому их список сужен до функций **сканирования компьютера**, **обновления** и некоторых разделов **настройки**. Возможность обновлять базу данных сигнатур вирусов является самой важной функцией ESET SysRescue, рекомендуется обновить программу, прежде чем приступать к сканированию компьютера.

4.8.5.1 Использование ESET SysRescue

Предположим, что компьютеры в сети были заражены вирусом, который вносит изменения в исполняемые файлы (.exe). ESET File Security может очистить все зараженные файлы кроме *explorer.exe*, который невозможно очистить даже в безопасном режиме.

Это связано с тем, что *explorer.exe*, будучи одним из важнейших процессов Windows, запускается также и в безопасном режиме. ESET File Security не сможет выполнить никаких действий с файлом, из-за чего он останется зараженным.

В такой ситуации можно использовать ESET SysRescue для решения этой проблемы. Средству ESET SysRescue не нужны никакие компоненты операционной системы компьютера, а потому оно может обработать (очистить, удалить) любой файл на диске.

4.9 Интерфейс пользователя

Параметры интерфейса пользователя в ESET File Security позволяют настроить рабочую среду в соответствии с конкретными требованиями. Эти параметры доступны в ветви **Интерфейс** дерева расширенных параметров ESET File Security.

В разделе **Элементы интерфейса** параметр **Расширенный режим** дает пользователям возможность включать и отключать расширенный режим. В расширенном режиме отображаются более подробные параметры и дополнительные элементы управления для ESET File Security.

Флажок **Графический интерфейс** следует снять, если отображение графических элементов снижает производительность компьютера или вызывает другие проблемы. Графический интерфейс также может быть необходимо отключить пользователям с ослабленным зрением, поскольку он может конфликтовать со специальными приложениями, используемыми для работы с отображаемым на экране текстом.

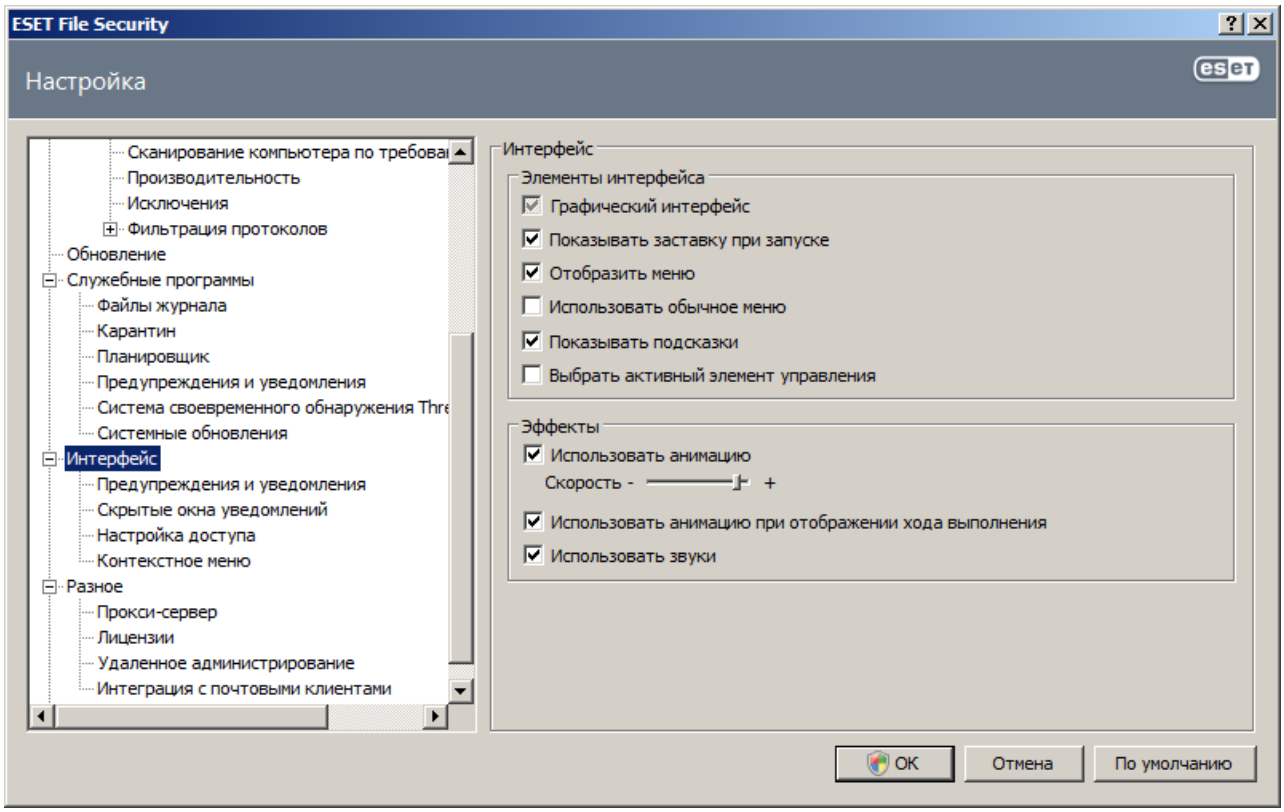
Если нужно отключить заставку ESET File Security, снимите флажок **Показывать заставку при запуске**.

В верхней части главного окна программы ESET File Security находится обычное меню, которое можно активировать или отключить с помощью флажка **Использовать обычное меню**.

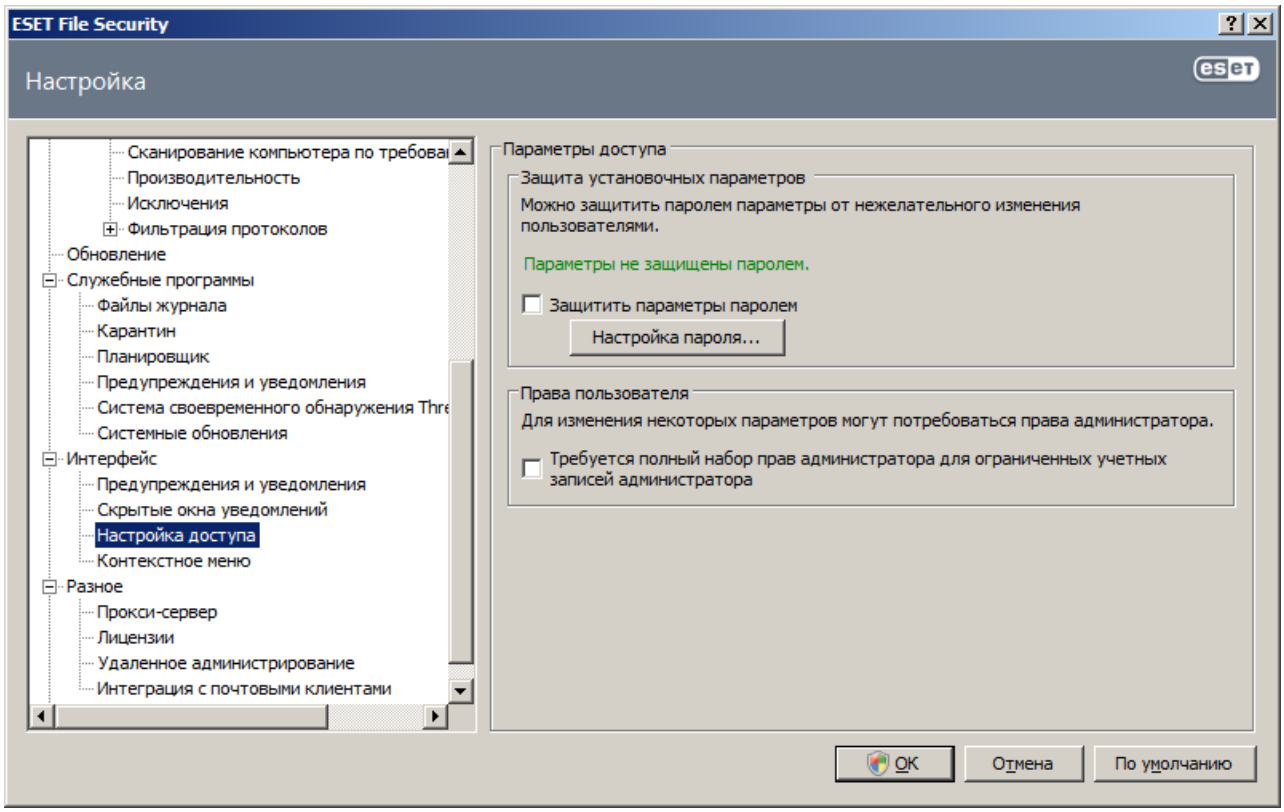
Если установлен флажок **Показывать подсказки**, при наведении курсора на какой-либо элемент на экран будет выводиться его краткое описание. При установленном флажке **Выбрать активный элемент управления** система будет выделять любой элемент, в данный момент находящийся в активной области курсора мыши. Выделенный элемент активируется нажатием кнопки мыши.

Для уменьшения или увеличения скорости анимированных эффектов установите флажок **Использовать анимацию** и переместите ползунок **Скорость** влево или вправо.

Для того чтобы использовать анимированные значки для отображения хода выполнения различных операций, установите флажок **Использовать анимацию при отображении хода выполнения**. Если программа должна воспроизводить звуковое предупреждение при возникновении важного события, установите флажок **Использовать звуки**.



Функции **интерфейса пользователя** также позволяют защищать параметры ESET File Security паролем. Этот параметр расположен в подменю **Защита настроек** раздела **Интерфейс**. Для обеспечения максимальной безопасности компьютера принципиально важно правильно сконфигурировать программу. Несанкционированное изменение может привести к потере важных данных. Для установки пароля для защиты параметров нажмите **Настройка пароля...**.



4.9.1 Предупреждения и уведомления

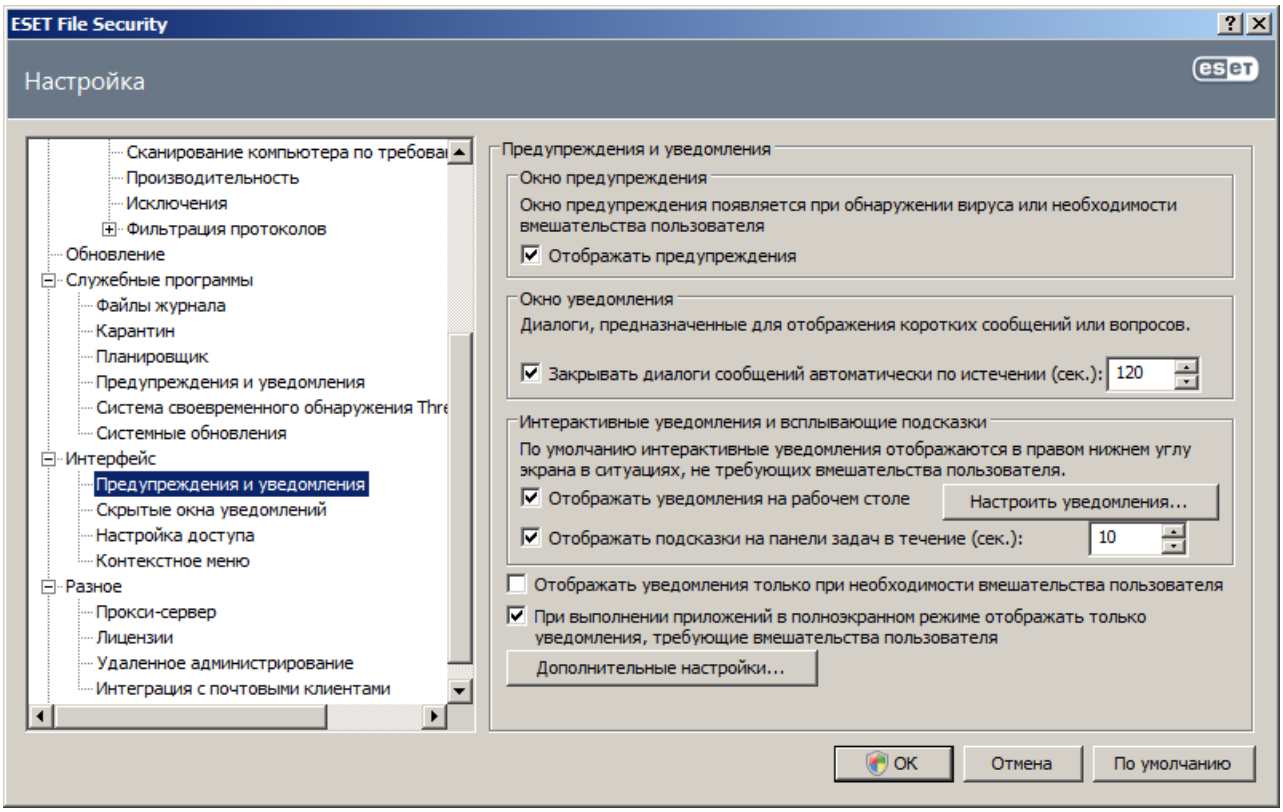
Раздел **Настройка предупреждений и уведомлений** (является подчиненным по отношению к разделу **Интерфейс**) позволяет сконфигурировать обработку системных уведомлений и предупреждений об угрозах в ESET File Security.

Первый пункт — **«Окно предупреждения»**. Если этот флажок снят, окна предупреждения не будут выводиться на экран. Такой подход следует использовать только в небольшом количестве особых ситуаций. В большинстве случаев рекомендуется оставить для этого параметра значение по умолчанию (включен).

Для того чтобы всплывающие окна закрывались автоматически по истечении определенного периода времени, установите флажок **Закрывать диалоги сообщений автоматически по истечении (сек.)**. Если окно предупреждения не будет закрыто пользователем, оно закрывается автоматически через указанный промежуток времени.

Уведомления на рабочем столе и всплывающие подсказки предназначены только для информирования и не требуют участия пользователя. Они отображаются в области уведомлений в правом нижнем углу экрана. Для того чтобы активировать отображение уведомлений на рабочем столе, установите флажок **Отображать уведомления на рабочем столе**. Более подробные параметры — время отображения и прозрачность окна — доступны с помощью кнопки **Настроить уведомления...**.

Для предварительного просмотра уведомлений нажмите кнопку **Просмотр**. Параметр **«Отображать подсказки на панели задач в течение (сек.)»** предназначен для настройки времени отображения всплывающих подсказок.



Нажмите **Дополнительные настройки...**, чтобы ввести расширенные параметры **предупреждений и уведомлений**, среди которых есть также и вариант **Отображать уведомления только при необходимости вмешательства пользователя**. Этот параметр позволяет включать и выключать отображение предупреждений и уведомлений, которые не требуют вмешательства со стороны пользователя. Установите флажок **При выполнении приложений в полноэкранном режиме отображать только уведомления, требующие вмешательства пользователя**, чтобы запретить все неинтерактивные уведомления. В раскрывающемся меню **Минимальная детализация отображаемых событий** можно выбрать начальный уровень серьезности предупреждений и уведомлений, которые следует отображать.

Последний параметр этого раздела позволяет сконфигурировать, кто именно должен получать уведомления в многопользовательской среде. Поле **В многопользовательских системах отображать уведомления для пользователя** позволяет решить, кто именно будет получать важные уведомления от ESET File Security. Обычно это системный или сетевой администратор. Этот параметр особенно полезен для серверов терминалов при условии, что все системные уведомления отправляются администратору.

4.9.2 Отключение графического интерфейса пользователя на сервере терминалов

В этой главе описывается процесс отключения графического интерфейса пользователя программы ESET File Security при выполнении на сервере терминалов Windows для сеансов работы пользователя.

Обычно графический интерфейс пользователя ESET File Security запускается при каждом входе удаленного пользователя на сервер и создании сеанса терминала. Обычно это нежелательно на серверах терминалов. Если нужно отключить графический интерфейс пользователя для сеансов терминала, выполните следующие действия.

1. Запустите *regedit.exe*
2. Найдите запись *HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run*
3. Щелкните правой кнопкой мыши значение *egui* и выберите пункт контекстного меню *Изменить…*
4. Добавьте параметр `/terminal` в конец существующей строки

Ниже приведен пример данных значения *egui* :

```
"C:\Program Files\ESET\ESET File Security\egui.exe" /hide /waitservice /terminal
```

Если нужно отменить этот параметр и включить автоматический запуск графического интерфейса пользователя ESET File Security, удалите параметр `/terminal` . Для перехода к значению реестра *egui* повторите действия 1–3

4.10 eShell

eShell (сокращение от «ESET Shell») — это интерфейс командной строки для ESET File Security. Это альтернатива графическому интерфейсу пользователя. В eShell есть все функции и возможности, обычно предоставляемые графическим интерфейсом пользователя. eShell позволяет конфигурировать и администрировать программу без каких-либо ограничений, не используя графический интерфейс пользователя. С помощью eShell можно делать практически все то же самое, что обычно делается с помощью графического интерфейса пользователя.

В дополнение ко всем функциям, которые доступны в графическом интерфейсе пользователя, этот интерфейс также предлагает возможности автоматизации за счет выполнения сценариев, которые позволяют конфигурировать, изменять конфигурацию и выполнять какие-либо действия. eShell также может быть полезен тем пользователям, которые предпочитают командную строку графическому интерфейсу.

В этом разделе описывается навигация в eShell и использование этого интерфейса, а также перечисляются все команды с описанием их предназначения и функций.

eShell может запускаться в двух режимах.

- Интерактивный режим полезен, когда нужно именно работать с eShell (а не просто выполнить одну команду), например при изменении конфигурации, просмотре журналов и т. п. Также интерактивный режим можно применять, если пользователю еще не знакомы все команды. Интерактивный режим облегчит навигацию по контексту. В нем также отображаются доступные команды, которые можно использовать в рамках определенного контекста.
- Режим единичной команды/пакетный режим: этот режим можно использовать, если нужно только выполнить какую-либо команду, не входя в интерактивный режим eShell. Это можно сделать с помощью командной строки Windows, введя `eshell` с соответствующими параметрами. Пример.

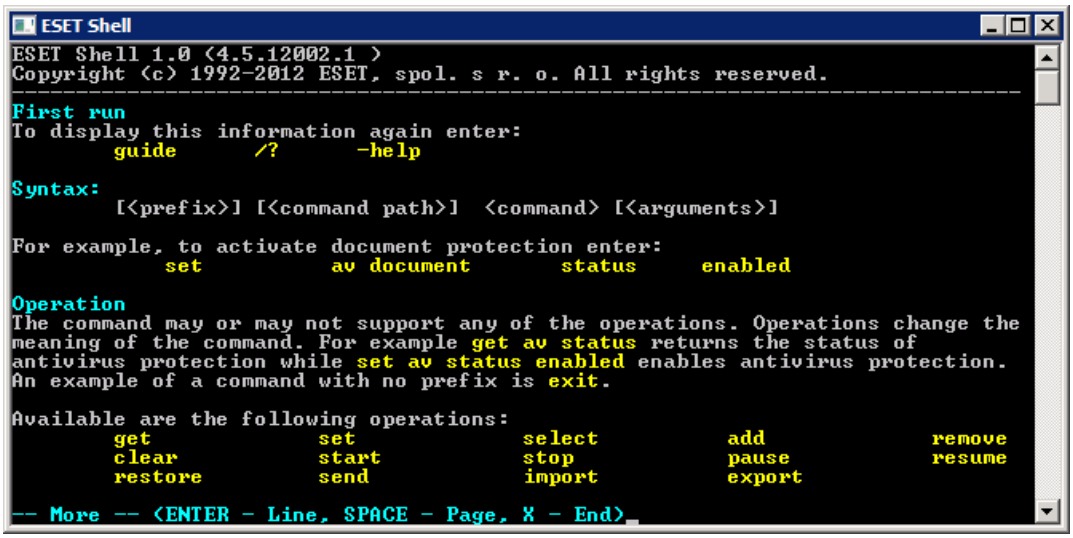
```
eshell set av document status enabled
```

ПРИМЕЧАНИЕ: Для выполнения команд eShell из командной строки Windows или запуска пакетных файлов сначала нужно включить эту функциональность (команда `set general access batch` должна быть выполнена в интерактивном режиме). Для получения дополнительных сведений о команде «set batch» воспользуйтесь этой ссылкой.

Для входа в интерактивный режим eShell можно использовать один из описанных далее двух способов.

- Через меню «Пуск» Windows: **Пуск** > **Все программы** > **ESET** > **ESET File Security** > **ESET shell**.
- Через командную строку Windows, введя `eshell` и нажав клавишу Enter.

При первом запуске eShell в интерактивном режиме на экран будет выведено окно первого запуска.



В нем приводятся основные примеры использования eShell с синтаксисом, префиксами, путями команд, сокращенными формами, псевдонимами и т. д. По сути, это краткое руководство по eShell.

ПРИМЕЧАНИЕ: При необходимости в дальнейшем вывести на экран окно первого запуска введите команду `guide .`

ПРИМЕЧАНИЕ: В командах не учитывается регистр, можно использовать как прописные, так и строчные буквы, но это не повлияет на выполнение команд.

4.10.1 Использование

Синтаксис
Он показывает, как составляется команда, т. е. как размещать префикс, контекст, аргументы, параметры и т. д. Это общий синтаксис, используемый в пределах всего интерфейса eShell.

[<префикс>] [<путь команды>] <команда> [<аргументы>]

Пример (команда активирует защиту документов)
`SET AV DOCUMENT STATUS ENABLED`

`SET` — префикс.
`AV DOCUMENT` — путь к конкретной команде, контекст, к которому данная команда относится.
`STATUS` — собственно команда.
`ENABLED` — аргумент для команды.

Если ввести `HELP` или `?` вместе с командой, на экран будет выведен синтаксис для данной команды. Пример. `CLEANLEVEL HELP` отобразит синтаксис для команды `CLEANLEVEL .`

СИНТАКСИС
```
[get] | restore cleanlevel
set cleanlevel none | normal | strict
```

Видно, что конструкция `[get]` заключена в скобки. Это показывает, что префикс `get` используется по умолчанию для команды `cleanlevel .` Это означает, что при выполнении команды `cleanlevel` без указания какого-либо префикса будет использоваться префикс по умолчанию (в данном случае `get cleanlevel`). Использование команд без префиксов позволяет сэкономить время на ввод данных. Обычно `get` является префиксом по умолчанию для большинства команд, но нужно точно знать префикс по умолчанию для конкретной команды и быть уверенным в том, что он соответствует тому, что нужно выполнить.

ПРИМЕЧАНИЕ: В командах не учитывается регистр, можно использовать как прописные, так и строчные буквы, но это не повлияет на выполнение команд.

Префикс/операция
Это операция. Например, `GET` предоставляет сведения о том, как сконфигурирована определенная функциональность ESET File Security, или показывает состояние (например, `GET AV STATUS` покажет текущее состояние защиты). В то же время `SET` конфигурирует функциональность или меняет ее состояние (`SET AV STATUS ENABLED` активирует защиту).

Ниже перечислены известные префиксы, которые можно использовать в eShell, но команда может поддерживать или не поддерживать любые из них.

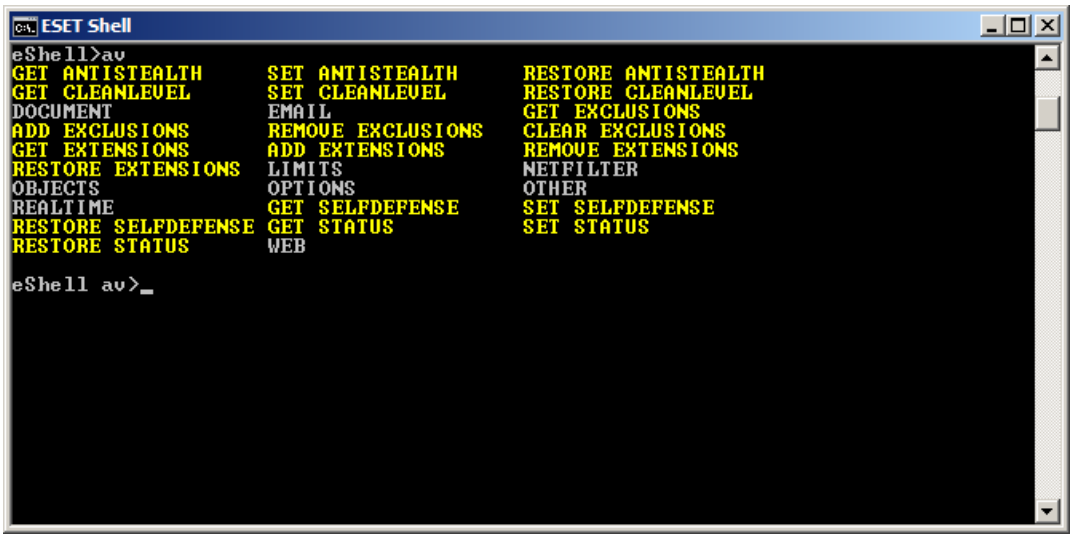
`GET` : возвращается текущий параметр/состояние.
`SET` : задается значение или состояние.
`SELECT` : выбирается элемент.
`ADD` : добавляется элемент.
`REMOVE` : удаляется элемент.
`CLEAR` : удаляются все элементы или файлы.
`START` : запускается действие.
`STOP` : останавливается действие.
`PAUSE` : приостанавливается действие.
`RESUME` : возобновляется действие.
`RESTORE` : восстанавливаются параметры/объект/файл по умолчанию.
`SEND` : отправляется объект или файл.
`IMPORT` : выполняется импорт из файла.
`EXPORT` : выполняется экспорт в файл.

Такие префиксы, как `GET` и `SET` , используются со многими командами, но некоторые команды, такие как `EXIT`, не используют префикса.

Путь команды/контекст
Команды размещаются в контекстах, которые образуют древовидную структуру. Верхний уровень древовидной структуры является корневым. При запуске eShell открывается именно корневой уровень.

```
eShell>
```

Можно либо выполнять команды непосредственно здесь или вводить имя контекста, чтобы перемещаться по древовидной структуре. Например, при вводе контекста `TOOLS` на экран будут выведены все команды и подчиненные контексты, доступные в данном контексте.



Желтым цветом обозначены команды, которые можно выполнять, а серым — подчиненные контексты, в которые можно войти. В подчиненном контексте содержатся дальнейшие команды.

Если нужно вернуться на более высокий уровень, следует использовать `..` (две точки). Например, предположим, что мы находимся здесь.

```
eShell av options>
```

введите `..` для того чтобы перейти на один уровень вверх, к

```
eShell av>
```

Или же при необходимости возврата на корневой уровень из `eShell av options>` (отделен от корневого уровня двумя уровнями) просто введите `.. ..` (две точки, пробел, еще две точки). Это позволит перейти на два уровня вверх, то есть к корневому контексту в данном случае. Эту возможность можно использовать вне зависимости от того, насколько глубоко в древовидной структуре контекстов вы находитесь. Используйте нужное количество сочетаний символов `..` для перехода на необходимый уровень.

Путь указывается относительно текущего контекста. Если команда содержится в текущем контексте, путь вводить не нужно. Например, для выполнения `GET AV STATUS` введите

`GET AV STATUS` при нахождении в корневом контексте (командная строка показывает `eShell>`)
`GET STATUS` при нахождении в контексте `AV` (командная строка показывает `eShell av>`)
`.. GET STATUS` при нахождении в контексте `AV OPTIONS` (командная строка показывает `eShell av options>`)

Аргумент
Это действие, которое выполняется для конкретной команды. Например, команда `CLEANLEVEL` может использоваться с такими аргументами.

`none` : без очистки.
`normal` : стандартная очистка.
`strict` : тщательная очистка.

Другим примером являются аргументы `ENABLED` или `DISABLED` , которые используются для включения и отключения определенной функции или функциональности.

Сокращенная форма/краткие команды
eShell позволяет сокращать контексты, команды и аргументы (при условии, что аргумент является параметром или альтернативным вариантом). Невозможно сократить префикс или аргумент, который является конкретным значением, таким как число, имя или путь.

Примеры краткой формы

```
set status enabled  => set stat en
add av exclusions C:\path\file.ext => add av exc C:\path\file.ext
```

Если две команды или два контекста начинаются с одних и тех же букв, например `ABOUT` и `AV`, и вводится `A` в качестве сокращенной команды, eShell не сможет решить, какую из этих двух команд нужно выполнить. Поэтому на экран будет выведено сообщение об ошибке и список команд, начинающихся с «A», из которого можно выбрать необходимое.

```
eShell>a
The following command is not unique: a

The following commands are available in this context:
 ABOUT: показывает информацию о программе.
 AV: изменяет контекст на av.
```

Затем при добавлении еще одной или нескольких букв (например, `AB` вместо просто `A`) eShell выполнит `ABOUT` , так как теперь эта команда является уникальной.

ПРИМЕЧАНИЕ: Если нужно наверняка знать, что команда будет выполнена именно так, как нужно, рекомендуется не сокращать команды, аргументы и т. д. и использовать полную форму. В этом случае все будет выполнено именно так, как нужно, и удастся избежать нежелательных ошибок. Это особенно верно для пакетных файлов/сценариев.

Псевдонимы
Псевдоним — это альтернативное название, которое может использоваться для выполнения команды (при условии, что этой команде присвоен псевдоним). Есть несколько псевдонимов по умолчанию, которые перечислены далее.

`(глобально) help` - ?
`(глобально) close` — exit
`(глобально) quit` — exit
`(глобально) bye` — exit
`warnlog` — tools log events
`virlog` — tools log detections

Под «(глобально)» понимается, что такую команду можно использовать в любом месте вне зависимости от текущего контекста. Одной команде может быть назначено несколько псевдонимов. Например, у команды `EXIT` есть псевдонимы `CLOSE`, `QUIT` и `BYE`. Если нужно выйти из eShell, можно использовать собственно команду `EXIT` или любой из нее псевдонимов. Псевдоним `VIRLOG` по сути является псевдонимом команды `DETECTIONS` в контексте `TOOLS LOG` . Таким образом команда DETECTIONS доступна непосредственно в корневом контексте `ROOT` , что позволяет проще использовать ее (не нужно вводить `TOOLS` и затем `LOG` , и выполнять ее непосредственно в `ROOT`).

eShell дает пользователям возможность задавать собственные псевдонимы. Воспользуйтесь этой ссылкой,

чтобы узнать, как создать псевдоним.

Защищенные команды
Некоторые команды являются защищенными и могут быть выполнены только после ввода пароля. Дополнительные сведения о защищенных паролем командах доступны по этой ссылке.

Guide
При выполнении команды `GUIDE` на экран будет выведено окно первого запуска, в котором объясняется использование eShell. Эта команда доступна в контексте `ROOT` (`eShell>`).

Help
Когда команда `HELP` используется самостоятельно, на экран выводится список всех доступных команд с префиксами, а также всех подчиненных контекстов, существующих в текущем контексте. Также будет предоставлено краткое описание каждой команды и подчиненного контекста. При использовании `HELP` в качестве аргумента с какой-либо командой (например, `CLEANLEVEL HELP`) на экран будут выведены подробные сведения об этой команде. На экран будут выведены СИНТАКСИС, ОПЕРАЦИИ, АРГУМЕНТЫ И ПСЕВДОНИМЫ для этой команды с кратким описанием каждого элемента.

История команд
eShell хранит историю выполненных ранее команд. Это распространяется только на текущий интерактивный сеанс eShell. После выхода из eShell история команд будет удалена. С помощью стрелок вверх и вниз на клавиатуре можно перемещаться по истории. После нахождения нужной команды ее можно выполнить повторно или внести в нее изменения, не вводя всю команду целиком заново.

CLS/очистка экрана
Команда `CLS` позволяет очистить экран. Она работает точно так же, как в командной строке Windows и других аналогичных интерфейсах командной строки.

EXIT / CLOSE / QUIT / BYE
Для того чтобы закрыть eShell или выйти из этого интерфейса, можно воспользоваться любой из этих команд (`EXIT`, `CLOSE`, `QUIT` или `BYE`).

4.10.2 Команды

В этом разделе перечисляются все доступные команды eShell с описаниями.

ПРИМЕЧАНИЕ: В командах не учитывается регистр, можно использовать как прописные, так и строчные буквы, но это не повлияет на выполнение команд.

Команды, присутствующие в контексте **ROOT**

ABOUT

На экран выводятся сведения о программе. Отображается название установленного программного продукта, номер версии, установленные компоненты (в том числе номер версии каждого компонента) и основная информация о сервере и операционной системе, на которых выполняется ESET File Security.

ПУТЬ В КОНТЕКСТЕ

```
root
```

BATCH

Запускается пакетный режим eShell. Это очень полезно при выполнении пакетных файлов и сценариев, рекомендуется использовать этот вариант с пакетными файлами. Поместите `START BATCH` как первую команду в пакетном файле или сценарии, чтобы включить пакетный режим. При включении этой функции не предлагается использовать интерактивный ввод (например, вводить пароль), а отсутствующие аргументы заменяются на аргументы по умолчанию. Это гарантирует, что пакетный файл не остановится до окончания выполнения из-за того, что eShell ожидает каких-либо действий от пользователя. Таким образом, пакетный файл должен выполняться без остановок (если нет ошибок или неверных команд в пакетном файле).

ПУТЬ В КОНТЕКСТЕ

```
root
```

СИНТАКСИС

```
[start] batch
```

ОПЕРАЦИИ

`start` : запускается eShell в пакетном режиме.

ПУТЬ В КОНТЕКСТЕ

`root`

ПРИМЕРЫ

`start batch` : запускается пакетный режим eShell.

CONNECT

Выполняется подключение к ядру ESET.

ПУТЬ В КОНТЕКСТЕ

`root`

GUIDE

На экран выводится окно первого запуска.

ПУТЬ В КОНТЕКСТЕ

`root`

PASSWORD

Обычно для выполнения защищенных паролем команд предлагается ввести пароль. Это делается из соображений безопасности. Это применяется к таким командам, которые отключают защиту от вирусов или могут повлиять на функциональность ESET File Security. Пользователю предлагается ввести пароль при каждом выполнении такой команды. Однако можно задать этот пароль, чтобы не вводить его каждый раз. Он будет сохранен в eShell и будет использоваться автоматически при выполнении защищенной паролем команды. Это значит, что не придется вводить пароль каждый раз.

ПРИМЕЧАНИЕ: Заданный пароль работает только в текущем интерактивном сеансе eShell. После выхода из eShell заданный пароль будет удален. При повторном запуске eShell пароль нужно задать снова.

Такой заданный пароль также очень удобен при выполнении пакетных файлов или сценариев. Ниже приведен пример такого пакетного файла.

```
eshell start batch "&" set password plain <вашпароль> "&" set status disabled
```

Такая объединенная команда запускает пакетный режим, задает пароль, который будет использоваться, и отключает защиту.

ПУТЬ В КОНТЕКСТЕ

`root`

СИНТАКСИС

`[get] | restore password`

`set password [plain <пароль>]`

ОПЕРАЦИИ

`get` : показать пароль.

`set` : задать или очистить пароль.

`restore` : очистить пароль.

АРГУМЕНТЫ

`plain` : переход ко вводу пароля как параметра.

`password` : пароль.

ПРИМЕРЫ

`set password plain <вашпароль>` : задается пароль, который будет использоваться для защищенных паролем команд.

`restore password` : очищается пароль.

ПРИМЕРЫ

`get password` : эта команда позволяет увидеть, сконфигурирован ли пароль (на экран при этом выводятся только символы «звездочка» (*), сам пароль не отображается). Если символов «звездочка» нет, это значит, что пароль не установлен.

`set password plain <вашпароль>` : эта команда позволяет задать пароль.

`restore password` : эта команда очищает заданный пароль.

STATUS

Отображается информация о текущем состоянии защиты ESET File Security (аналогично графическому интерфейсу пользователя).

ПУТЬ В КОНТЕКСТЕ

`root`

СИНТАКСИС

```
[get] | restore status

set status disabled | enabled
```

ОПЕРАЦИИ

`get` : показать состояние защиты от вирусов.

`set` : отключить или включить защиту от вирусов.

`restore` : восстановить параметры по умолчанию.

АРГУМЕНТЫ

`disabled` : отключить защиту от вирусов.

`enabled` : включить защиту от вирусов.

ПРИМЕРЫ

`get status` : отображается текущее состояние защиты.

`set status disabled` : отключается защита.

`restore status` : для защиты восстанавливаются параметры по умолчанию (включена).

VIRLOG

Это псевдоним команды DETECTIONS. Эта команда полезна, когда нужно просмотреть информацию об обнаруженных заражениях. Воспользуйтесь этой ссылкой, чтобы ознакомиться с подробными сведениями об этой команде и ее использовании.

WARNLOG

Это псевдоним команды EVENTS. Эта команда полезна, когда нужно просмотреть информацию о различных событиях.

Воспользуйтесь этой ссылкой, чтобы ознакомиться с подробными сведениями об этой команде и ее использовании.

4.10.2.1 Контекст «AV»

ANTISTEALTH

Включить технологию Anti-Stealth.

СИНТАКСИС

```
[get] | restore antistealth

set antistealth disabled | enabled
```

ОПЕРАЦИИ

`get` : возвращается текущий параметр/состояние.

`set` : задается значение или состояние.

`restore` : восстанавливаются параметры/объект/файл по умолчанию.

АРГУМЕНТЫ

`disabled` : отключается функция или параметр.

`enabled` : включается функция или активируется параметр.

CLEANLEVEL

Уровень очистки.

СИНТАКСИС

```
[get] | restore cleanlevel

set cleanlevel none | normal | strict
```

ОПЕРАЦИИ

`get` : возвращается текущий параметр/состояние.

`set` : задается значение или состояние.

`restore` : восстанавливаются параметры/объект/файл по умолчанию.

АРГУМЕНТЫ

`none` : без очистки.

`normal` : стандартная очистка.

`strict` : тщательная очистка.

EXCLUSIONS

Исключения.

СИНТАКСИС

```
[get] | clear exclusions

add | remove exclusions <исключение>
```

ОПЕРАЦИИ

`get` : возвращается текущий параметр/состояние.

`add` : добавляется элемент.

`remove` : удаляется элемент.

АРГУМЕНТЫ

`exclusion` : исключенный файл/папка/маска.

EXTENSIONS

Сканируемые/исключенные расширения.

СИНТАКСИС

```
[get] | restore extensions

add | remove extensions <расширение> | /all | /extless
```

ОПЕРАЦИИ

`get` : возвращается текущий параметр/состояние.

`add` : добавляется элемент.

`remove` : удаляется элемент.

`restore` : восстанавливаются параметры/объект/файл по умолчанию.

АРГУМЕНТЫ

`extension` : расширение.

`all` : все файлы.

`extless` : файлы без расширений.

RESTART

Перезапуск ядра ESET.

СИНТАКСИС

```
restart
```

SELFDEFENSE

Самозащита.

СИНТАКСИС

```
[get] | restore selfdefense

set selfdefense disabled | enabled
```

ОПЕРАЦИИ

`get` : возвращается текущий параметр/состояние.

`set` : задается значение или состояние.

`restore` : восстанавливаются параметры/объект/файл по умолчанию.

АРГУМЕНТЫ

`disabled` : отключается функция или параметр.

`enabled` : включается функция или активируется параметр.

STATUS

Состояние защиты от вирусов.

СИНТАКСИС

```
[get] | restore status

set status disabled | enabled
```

ОПЕРАЦИИ

`get` : показать состояние защиты от вирусов.

`set` : отключить или включить защиту от вирусов.

`restore` : восстанавливаются параметры/объект/файл по умолчанию.

АРГУМЕНТЫ

`disabled` : отключить защиту от вирусов.

`enabled` : включить защиту от вирусов.

4.10.2.2 Контекст «AV DOCUMENT»

CLEANLEVEL

Уровень очистки.

СИНТАКСИС

```
[get] | restore cleanlevel
set cleanlevel none | normal | strict
```

ОПЕРАЦИИ

`get` : возвращается текущий параметр/состояние.

`set` : задается значение или состояние.

`restore` : восстанавливаются параметры/объект/файл по умолчанию.

АРГУМЕНТЫ

`none` : без очистки.

`normal` : стандартная очистка.

`strict` : тщательная очистка.

EXTENSIONS

Сканируемые/исключенные расширения.

СИНТАКСИС

```
[get] | restore extensions
add | remove extensions <расширение> | /all | /extless
```

ОПЕРАЦИИ

`get` : возвращается текущий параметр/состояние.

`add` : добавляется элемент.

`remove` : удаляется элемент.

`restore` : восстанавливаются параметры/объект/файл по умолчанию.

АРГУМЕНТЫ

`extension` : расширение.

`all` : все файлы.

`extless` : файлы без расширений.

INTEGRATION

Интеграция защиты документов в систему.

СИНТАКСИС

```
[get] | restore integration
set integration disabled | enabled
```

ОПЕРАЦИИ

`get` : возвращается текущий параметр/состояние.

`set` : задается значение или состояние.

`restore` : восстанавливаются параметры/объект/файл по умолчанию.

АРГУМЕНТЫ

`disabled` : отключается функция или параметр.

`enabled` : включается функция или активируется параметр.

STATUS

Текущее состояние защиты документов.

СИНТАКСИС

```
[get] | restore status

set status disabled | enabled
```

ОПЕРАЦИИ

`get` : возвращается текущий параметр/состояние.

`set` : задается значение или состояние.

`restore` : восстанавливаются параметры/объект/файл по умолчанию.

АРГУМЕНТЫ

`disabled` : отключается функция или параметр.

`enabled` : включается функция или активируется параметр.

4.10.2.3 Контекст «AV DOCUMENT LIMITS ARCHIVE»

УРОВЕНЬ

Уровень вложенности архивов.

СИНТАКСИС

```
[get] | restore level

set level <число>
```

ОПЕРАЦИИ

`get` : возвращается текущий параметр/состояние.

`set` : задается значение или состояние.

`restore` : восстанавливаются параметры/объект/файл по умолчанию.

АРГУМЕНТЫ

`число` : уровень от 1 до 20 или 0 для выбора параметров по умолчанию.

SIZE

Максимальный размер файла в архиве в килобайтах.

СИНТАКСИС

```
[get] | restore size

set size <число>
```

ОПЕРАЦИИ

`get` : возвращается текущий параметр/состояние.

`set` : задается значение или состояние.

`restore` : восстанавливаются параметры/объект/файл по умолчанию.

АРГУМЕНТЫ

`число` : размер в Кб или 0 для выбора параметров по умолчанию.

4.10.2.4 Контекст «AV DOCUMENT LIMITS OBJECTS»

SIZE

Максимальный размер архива (Кб).

СИНТАКСИС

```
[get] | restore size

set size <число>
```

ОПЕРАЦИИ

`get` : возвращается текущий параметр/состояние.

`set` : задается значение или состояние.

`restore` : восстанавливаются параметры/объект/файл по умолчанию.

АРГУМЕНТЫ

`число` : размер в Кб или 0 для выбора параметров по умолчанию.

TIMEOUT

Максимальное время сканирования архивов в секундах.

СИНТАКСИС

```
[get] | restore timeout

set timeout <число>
```

ОПЕРАЦИИ

`get` : возвращается текущий параметр/состояние.

`set` : задается значение или состояние.

`restore` : восстанавливаются параметры/объект/файл по умолчанию.

АРГУМЕНТЫ

`число` : время в секундах или 0 для выбора параметров по умолчанию.

4.10.2.5 Контекст «AV DOCUMENT OBJECTS»

ARCHIVE

Сканировать архивы.

СИНТАКСИС

```
[get] | restore archive

set archive disabled | enabled
```

ОПЕРАЦИИ

`get` : возвращается текущий параметр/состояние.

`set` : задается значение или состояние.

`restore` : восстанавливаются параметры/объект/файл по умолчанию.

АРГУМЕНТЫ

`disabled` : отключается функция или параметр.

`enabled` : включается функция или активируется параметр.

BOOT

Сканировать загрузочные секторы.

СИНТАКСИС

```
[get] | restore boot

set boot disabled | enabled
```

ОПЕРАЦИИ

`get` : возвращается текущий параметр/состояние.

`set` : задается значение или состояние.

`restore` : восстанавливаются параметры/объект/файл по умолчанию.

АРГУМЕНТЫ

`disabled` : отключается функция или параметр.

`enabled` : включается функция или активируется параметр.

EMAIL

Сканировать файлы электронной почты.

СИНТАКСИС

```
[get] | restore email

set email disabled | enabled
```

ОПЕРАЦИИ

`get` : возвращается текущий параметр/состояние.

`set` : задается значение или состояние.

`restore` : восстанавливаются параметры/объект/файл по умолчанию.

АРГУМЕНТЫ

`disabled` : отключается функция или параметр.

`enabled` : включается функция или активируется параметр.

FILE

Сканировать файлы.

СИНТАКСИС

```
[get] | restore file

set file disabled | enabled
```

ОПЕРАЦИИ

`get` : возвращается текущий параметр/состояние.

`set` : задается значение или состояние.

`restore` : восстанавливаются параметры/объект/файл по умолчанию.

АРГУМЕНТЫ

`disabled` : отключается функция или параметр.

`enabled` : включается функция или активируется параметр.

MEMORY

Сканировать память.

СИНТАКСИС

```
[get] | restore memory

set memory disabled | enabled
```

ОПЕРАЦИИ

`get` : возвращается текущий параметр/состояние.

`set` : задается значение или состояние.

`restore` : восстанавливаются параметры/объект/файл по умолчанию.

АРГУМЕНТЫ

`disabled` : отключается функция или параметр.

`enabled` : включается функция или активируется параметр.

RUNTIME

Сканировать упаковщики.

СИНТАКСИС

```
[get] | restore runtime
set runtime disabled | enabled
```

ОПЕРАЦИИ

`get` : возвращается текущий параметр/состояние.

`set` : задается значение или состояние.

`restore` : восстанавливаются параметры/объект/файл по умолчанию.

АРГУМЕНТЫ

`disabled` : отключается функция или параметр.

`enabled` : включается функция или активируется параметр.

SFX

Сканировать самораспаковывающиеся архивы.

СИНТАКСИС

```
[get] | restore sfx
set sfx disabled | enabled
```

ОПЕРАЦИИ

`get` : возвращается текущий параметр/состояние.

`set` : задается значение или состояние.

`restore` : восстанавливаются параметры/объект/файл по умолчанию.

АРГУМЕНТЫ

`disabled` : отключается функция или параметр.

`enabled` : включается функция или активируется параметр.

4.10.2.6 Контекст «AV DOCUMENT OPTIONS»

ADVHEURISTICS

Использовать расширенную эвристику.

СИНТАКСИС

```
[get] | restore advheuristics
set advheuristics disabled | enabled
```

ОПЕРАЦИИ

`get` : возвращается текущий параметр/состояние.

`set` : задается значение или состояние.

`restore` : восстанавливаются параметры/объект/файл по умолчанию.

АРГУМЕНТЫ

`disabled` : отключается функция или параметр.

`enabled` : включается функция или активируется параметр.

ADWARE

Обнаружение рекламных/шпионских/опасных программ.

СИНТАКСИС

```
[get] | restore adware

set adware disabled | enabled
```

ОПЕРАЦИИ

`get` : возвращается текущий параметр/состояние.

`set` : задается значение или состояние.

`restore` : восстанавливаются параметры/объект/файл по умолчанию.

АРГУМЕНТЫ

`disabled` : отключается функция или параметр.

`enabled` : включается функция или активируется параметр.

HEURISTICS

Использовать эвристический анализ.

СИНТАКСИС

```
[get] | restore heuristics

set heuristics disabled | enabled
```

ОПЕРАЦИИ

`get` : возвращается текущий параметр/состояние.

`set` : задается значение или состояние.

`restore` : восстанавливаются параметры/объект/файл по умолчанию.

АРГУМЕНТЫ

`disabled` : отключается функция или параметр.

`enabled` : включается функция или активируется параметр.

SIGNATURES

Использовать сигнатуры.

СИНТАКСИС

```
[get] | restore signatures

set signatures disabled | enabled
```

ОПЕРАЦИИ

`get` : возвращается текущий параметр/состояние.

`set` : задается значение или состояние.

`restore` : восстанавливаются параметры/объект/файл по умолчанию.

АРГУМЕНТЫ

`disabled` : отключается функция или параметр.

`enabled` : включается функция или активируется параметр.

UNSAFE

Обнаружение потенциально опасных приложений.

СИНТАКСИС

```
[get] | restore unsafe

set unsafe disabled | enabled
```

ОПЕРАЦИИ

`get` : возвращается текущий параметр/состояние.

`set` : задается значение или состояние.

`restore` : восстанавливаются параметры/объект/файл по умолчанию.

АРГУМЕНТЫ

`disabled` : отключается функция или параметр.

`enabled` : включается функция или активируется параметр.

UNWANTED

Обнаружение потенциально нежелательных приложений.

СИНТАКСИС

```
[get] | restore unwanted

set unwanted disabled | enabled
```

ОПЕРАЦИИ

`get` : возвращается текущий параметр/состояние.

`set` : задается значение или состояние.

`restore` : восстанавливаются параметры/объект/файл по умолчанию.

АРГУМЕНТЫ

`disabled` : отключается функция или параметр.

`enabled` : включается функция или активируется параметр.

4.10.2.7 Контекст «AV DOCUMENT OTHER»

LOGALL

Регистрировать все объекты.

СИНТАКСИС

```
[get] | restore logall

set logall disabled | enabled
```

ОПЕРАЦИИ

`get` : возвращается текущий параметр/состояние.

`set` : задается значение или состояние.

`restore` : восстанавливаются параметры/объект/файл по умолчанию.

АРГУМЕНТЫ

`disabled` : отключается функция или параметр.

`enabled` : включается функция или активируется параметр.

OPTIMIZE

Оптимизация Smart.

СИНТАКСИС

```
[get] | restore optimize
set optimize disabled | enabled
```

ОПЕРАЦИИ

`get` : возвращается текущий параметр/состояние.

`set` : задается значение или состояние.

`restore` : восстанавливаются параметры/объект/файл по умолчанию.

АРГУМЕНТЫ

`disabled` : отключается функция или параметр.

`enabled` : включается функция или активируется параметр.

4.10.2.8 Контекст «AV EMAIL»

ACTION

Действие для зараженных сообщений.

СИНТАКСИС

```
[get] | restore action
set action none | delete | movedeleted | moveto
```

ОПЕРАЦИИ

`get` : возвращается текущий параметр/состояние.

`set` : задается значение или состояние.

`restore` : восстанавливаются параметры/объект/файл по умолчанию.

АРГУМЕНТЫ

`none` : ничего не предпринимать.

`delete` : удалить сообщение.

`movedeleted` : переместить в папку «Удаленные».

`moveto` : переместить в папку.

CLIENTS

Почтовые клиенты.

СИНТАКСИС

```
[get] clients
add | remove clients <путь>
```

ОПЕРАЦИИ

`get` : возвращается текущий параметр/состояние.

`add` : добавляется элемент.

`remove` : удаляется элемент.

АРГУМЕНТЫ

`путь` : путь приложения.

ПРИМЕЧАНИЕ: При фильтрации только по приложениям нужно указать, какие из них используются в качестве

почтовых клиентов. Если приложение не помечено как почтовый клиент, электронная почта может не сканироваться.

QUARANTINE

Папка зараженных сообщений.

СИНТАКСИС

```
[get] | restore quarantine

set quarantine <строка>
```

ОПЕРАЦИИ

`get` : возвращается текущий параметр/состояние.

`set` : задается значение или состояние.

`restore` : восстанавливаются параметры/объект/файл по умолчанию.

АРГУМЕНТЫ

`строка` : имя папки.

STATUS

Состояние защиты почтового клиента.

СИНТАКСИС

```
[get] | restore status

set status disabled | enabled
```

ОПЕРАЦИИ

`get` : возвращается текущий параметр/состояние.

`set` : задается значение или состояние.

`restore` : восстанавливаются параметры/объект/файл по умолчанию.

АРГУМЕНТЫ

`disabled` : отключается функция или параметр.

`enabled` : включается функция или активируется параметр.

4.10.2.9 Контекст «AV EMAIL GENERAL»

CLEANLEVEL

Уровень очистки.

СИНТАКСИС

```
[get] | restore cleanlevel

set cleanlevel none | normal | strict
```

ОПЕРАЦИИ

`get` : возвращается текущий параметр/состояние.

`set` : задается значение или состояние.

`restore` : восстанавливаются параметры/объект/файл по умолчанию.

АРГУМЕНТЫ

`none` : без очистки.

`normal` : стандартная очистка.

`strict` : тщательная очистка.

EXTENSIONS

Сканируемые/исключенные расширения.

СИНТАКСИС

```
[get] | restore extensions
add | remove extensions <расширение> | /all | /extless
```

ОПЕРАЦИИ

`get` : возвращается текущий параметр/состояние.

`add` : добавляется элемент.

`remove` : удаляется элемент.

`restore` : восстанавливаются параметры/объект/файл по умолчанию.

АРГУМЕНТЫ

`extension` : расширение.

`all` : все файлы.

`extless` : файлы без расширений.

4.10.2.10 Контекст «AV EMAIL GENERAL LIMITS ARCHIVE»

LEVEL

Уровень вложенности архивов.

СИНТАКСИС

```
[get] | restore level
set level <число>
```

ОПЕРАЦИИ

`get` : возвращается текущий параметр/состояние.

`set` : задается значение или состояние.

`restore` : восстанавливаются параметры/объект/файл по умолчанию.

АРГУМЕНТЫ

`число` : уровень от 1 до 20 или 0 для выбора параметров по умолчанию.

SIZE

Максимальный размер файла в архиве в килобайтах.

СИНТАКСИС

```
[get] | restore size
set size <число>
```

ОПЕРАЦИИ

`get` : возвращается текущий параметр/состояние.

`set` : задается значение или состояние.

`restore` : восстанавливаются параметры/объект/файл по умолчанию.

АРГУМЕНТЫ

`число` : размер в Кб или 0 для выбора параметров по умолчанию.

4.10.2.11 Контекст «AV EMAIL GENERAL LIMITS OBJECTS»

SIZE

Максимальный размер архива (Кб).

СИНТАКСИС

```
[get] | restore size

set size <число>
```

ОПЕРАЦИИ

`get` : возвращается текущий параметр/состояние.

`set` : задается значение или состояние.

`restore` : восстанавливаются параметры/объект/файл по умолчанию.

АРГУМЕНТЫ

`число` : размер в Кб или 0 для выбора параметров по умолчанию.

TIMEOUT

Максимальное время сканирования архивов в секундах.

СИНТАКСИС

```
[get] | restore timeout

set timeout <число>
```

ОПЕРАЦИИ

`get` : возвращается текущий параметр/состояние.

`set` : задается значение или состояние.

`restore` : восстанавливаются параметры/объект/файл по умолчанию.

АРГУМЕНТЫ

`число` : время в секундах или 0 для выбора параметров по умолчанию.

4.10.2.12 Контекст «AV EMAIL GENERAL OBJECTS»

ARCHIVE

Сканировать архивы.

СИНТАКСИС

```
[get] | restore archive

set archive disabled | enabled
```

ОПЕРАЦИИ

`get` : возвращается текущий параметр/состояние.

`set` : задается значение или состояние.

`restore` : восстанавливаются параметры/объект/файл по умолчанию.

АРГУМЕНТЫ

`disabled` : отключается функция или параметр.

`enabled` : включается функция или активируется параметр.

BOOT

Сканировать загрузочные секторы.

СИНТАКСИС

```
[get] | restore boot

set boot disabled | enabled
```

ОПЕРАЦИИ

`get` : возвращается текущий параметр/состояние.

`set` : задается значение или состояние.

`restore` : восстанавливаются параметры/объект/файл по умолчанию.

АРГУМЕНТЫ

`disabled` : отключается функция или параметр.

`enabled` : включается функция или активируется параметр.

EMAIL

Сканировать файлы электронной почты.

СИНТАКСИС

```
[get] | restore email

set email disabled | enabled
```

ОПЕРАЦИИ

`get` : возвращается текущий параметр/состояние.

`set` : задается значение или состояние.

`restore` : восстанавливаются параметры/объект/файл по умолчанию.

АРГУМЕНТЫ

`disabled` : отключается функция или параметр.

`enabled` : включается функция или активируется параметр.

FILE

Сканировать файлы.

СИНТАКСИС

```
[get] | restore file

set file disabled | enabled
```

ОПЕРАЦИИ

`get` : возвращается текущий параметр/состояние.

`set` : задается значение или состояние.

`restore` : восстанавливаются параметры/объект/файл по умолчанию.

АРГУМЕНТЫ

`disabled` : отключается функция или параметр.

`enabled` : включается функция или активируется параметр.

MEMORY

Сканировать память.

СИНТАКСИС

```
[get] | restore memory

set memory disabled | enabled
```

ОПЕРАЦИИ

`get` : возвращается текущий параметр/состояние.

`set` : задается значение или состояние.

`restore` : восстанавливаются параметры/объект/файл по умолчанию.

АРГУМЕНТЫ

`disabled` : отключается функция или параметр.

`enabled` : включается функция или активируется параметр.

RUNTIME

Сканировать упаковщики.

СИНТАКСИС

```
[get] | restore runtime
set runtime disabled | enabled
```

ОПЕРАЦИИ

`get` : возвращается текущий параметр/состояние.

`set` : задается значение или состояние.

`restore` : восстанавливаются параметры/объект/файл по умолчанию.

АРГУМЕНТЫ

`disabled` : отключается функция или параметр.

`enabled` : включается функция или активируется параметр.

SFX

Сканировать самораспаковывающиеся архивы.

СИНТАКСИС

```
[get] | restore sfx
set sfx disabled | enabled
```

ОПЕРАЦИИ

`get` : возвращается текущий параметр/состояние.

`set` : задается значение или состояние.

`restore` : восстанавливаются параметры/объект/файл по умолчанию.

АРГУМЕНТЫ

`disabled` : отключается функция или параметр.

`enabled` : включается функция или активируется параметр.

4.10.2.13 Контекст «AV EMAIL GENERAL OPTIONS»

ADVHEURISTICS

Использовать расширенную эвристику.

СИНТАКСИС

```
[get] | restore advheuristics
set advheuristics disabled | enabled
```

ОПЕРАЦИИ

`get` : возвращается текущий параметр/состояние.

`set` : задается значение или состояние.

`restore` : восстанавливаются параметры/объект/файл по умолчанию.

АРГУМЕНТЫ

`disabled` : отключается функция или параметр.

`enabled` : включается функция или активируется параметр.

ADWARE

Обнаружение рекламных/шпионских/опасных программ.

СИНТАКСИС

```
[get] | restore adware

set adware disabled | enabled
```

ОПЕРАЦИИ

`get` : возвращается текущий параметр/состояние.

`set` : задается значение или состояние.

`restore` : восстанавливаются параметры/объект/файл по умолчанию.

АРГУМЕНТЫ

`disabled` : отключается функция или параметр.

`enabled` : включается функция или активируется параметр.

HEURISTICS

Использовать эвристический анализ.

СИНТАКСИС

```
[get] | restore heuristics

set heuristics disabled | enabled
```

ОПЕРАЦИИ

`get` : возвращается текущий параметр/состояние.

`set` : задается значение или состояние.

`restore` : восстанавливаются параметры/объект/файл по умолчанию.

АРГУМЕНТЫ

`disabled` : отключается функция или параметр.

`enabled` : включается функция или активируется параметр.

SIGNATURES

Использовать сигнатуры.

СИНТАКСИС

```
[get] | restore signatures

set signatures disabled | enabled
```

ОПЕРАЦИИ

`get` : возвращается текущий параметр/состояние.

`set` : задается значение или состояние.

`restore` : восстанавливаются параметры/объект/файл по умолчанию.

АРГУМЕНТЫ

`disabled` : отключается функция или параметр.

`enabled` : включается функция или активируется параметр.

UNSAFE

Обнаружение потенциально опасных приложений.

СИНТАКСИС

```
[get] | restore unsafe

set unsafe disabled | enabled
```

ОПЕРАЦИИ

`get` : возвращается текущий параметр/состояние.

`set` : задается значение или состояние.

`restore` : восстанавливаются параметры/объект/файл по умолчанию.

АРГУМЕНТЫ

`disabled` : отключается функция или параметр.

`enabled` : включается функция или активируется параметр.

UNWANTED

Обнаружение потенциально нежелательных приложений.

СИНТАКСИС

```
[get] | restore unwanted

set unwanted disabled | enabled
```

ОПЕРАЦИИ

`get` : возвращается текущий параметр/состояние.

`set` : задается значение или состояние.

`restore` : восстанавливаются параметры/объект/файл по умолчанию.

АРГУМЕНТЫ

`disabled` : отключается функция или параметр.

`enabled` : включается функция или активируется параметр.

4.10.2.14 Контекст «AV EMAIL GENERAL OTHER»

LOGALL

Регистрировать все объекты.

СИНТАКСИС

```
[get] | restore logall

set logall disabled | enabled
```

ОПЕРАЦИИ

`get` : возвращается текущий параметр/состояние.

`set` : задается значение или состояние.

`restore` : восстанавливаются параметры/объект/файл по умолчанию.

АРГУМЕНТЫ

`disabled` : отключается функция или параметр.

`enabled` : включается функция или активируется параметр.

OPTIMIZE

Оптимизация Smart.

СИНТАКСИС

```
[get] | restore optimize
set optimize disabled | enabled
```

ОПЕРАЦИИ

`get` : возвращается текущий параметр/состояние.

`set` : задается значение или состояние.

`restore` : восстанавливаются параметры/объект/файл по умолчанию.

АРГУМЕНТЫ

`disabled` : отключается функция или параметр.

`enabled` : включается функция или активируется параметр.

4.10.2.15 Контекст «AV EMAIL MESSAGE CONVERT»

PLAIN

Преобразовывать тело сообщения электронной почты в простой текст.

СИНТАКСИС

```
[get] | restore plain
set plain disabled | enabled
```

ОПЕРАЦИИ

`get` : возвращается текущий параметр/состояние.

`set` : задается значение или состояние.

`restore` : восстанавливаются параметры/объект/файл по умолчанию.

АРГУМЕНТЫ

`disabled` : отключается функция или параметр.

`enabled` : включается функция или активируется параметр.

4.10.2.16 Контекст «AV EMAIL MODIFY»

TEMPLATE

Шаблон для добавления к теме зараженных сообщений.

СИНТАКСИС

```
[get] | restore template
set template [<строка>]
```

ОПЕРАЦИИ

`get` : возвращается текущий параметр/состояние.

`set` : задается значение или состояние.

`restore` : восстанавливаются параметры/объект/файл по умолчанию.

АРГУМЕНТЫ

`строка` : текст.

4.10.2.17 Контекст «AV EMAIL MODIFY RECEIVED»

BODY

Добавление уведомлений к полученным и прочитанным сообщениям.

СИНТАКСИС

```
[get] | restore body
set body never | infected | all
```

ОПЕРАЦИИ

`get` : возвращается текущий параметр/состояние.

`set` : задается значение или состояние.

`restore` : восстанавливаются параметры/объект/файл по умолчанию.

АРГУМЕНТЫ

`never` : не добавлять.

`infected` : только в зараженные сообщения.

`all` : во все сообщения.

SUBJECT

Добавление примечания в поле темы полученных и отправленных зараженных сообщений.

СИНТАКСИС

```
[get] | restore subject
set subject disabled | enabled
```

ОПЕРАЦИИ

`get` : возвращается текущий параметр/состояние.

`set` : задается значение или состояние.

`restore` : восстанавливаются параметры/объект/файл по умолчанию.

АРГУМЕНТЫ

`disabled` : отключается функция или параметр.

`enabled` : включается функция или активируется параметр.

4.10.2.18 Контекст «AV EMAIL MODIFY SENT»

BODY

Добавление уведомлений к полученным и прочитанным сообщениям.

СИНТАКСИС

```
[get] | restore body
set body never | infected | all
```

ОПЕРАЦИИ

`get` : возвращается текущий параметр/состояние.

`set` : задается значение или состояние.

`restore` : восстанавливаются параметры/объект/файл по умолчанию.

АРГУМЕНТЫ

`never` : не добавлять.

`infected` : только в зараженные сообщения.

`all` : во все сообщения.

SUBJECT

Добавление примечания в поле темы полученных и отправленных зараженных сообщений.

СИНТАКСИС

```
[get] | restore subject

set subject disabled | enabled
```

ОПЕРАЦИИ

`get` : возвращается текущий параметр/состояние.

`set` : задается значение или состояние.

`restore` : восстанавливаются параметры/объект/файл по умолчанию.

АРГУМЕНТЫ

`disabled` : отключается функция или параметр.

`enabled` : включается функция или активируется параметр.

4.10.2.19 Контекст «AV EMAIL OEXPRESS/WINMAIL»

INTEGRATION

Интегрировать в Outlook Express и почту Windows.

СИНТАКСИС

```
[get] | restore integration

set integration disabled | enabled
```

ОПЕРАЦИИ

`get` : возвращается текущий параметр/состояние.

`set` : задается значение или состояние.

`restore` : восстанавливаются параметры/объект/файл по умолчанию.

АРГУМЕНТЫ

`disabled` : отключается функция или параметр.

`enabled` : включается функция или активируется параметр.

4.10.2.20 Контекст «AV EMAIL OUTLOOK»

FORCEADDIN

Использовать надстройку COM в предыдущих версиях Microsoft Outlook.

СИНТАКСИС

```
[get] | restore forceaddin

set forceaddin 2010newer | 2007newer | allversions
```

ОПЕРАЦИИ

`get` : возвращается текущий параметр/состояние.

`set` : задается значение или состояние.

`restore` : восстанавливаются параметры/объект/файл по умолчанию.

АРГУМЕНТЫ

`2010newer` : Miscrosoft Outlook 2010 и более поздних версий.

`2007newer` : Miscrosoft Outlook 2007 и более поздних версий.

`allversions` : все версии Microsoft Outlook.

INTEGRATION

Интегрировать в Microsoft Outlook.

СИНТАКСИС

```
[get] | restore integration
set integration disabled | enabled
```

ОПЕРАЦИИ

`get` : возвращается текущий параметр/состояние.

`set` : задается значение или состояние.

`restore` : восстанавливаются параметры/объект/файл по умолчанию.

АРГУМЕНТЫ

`disabled` : отключается функция или параметр.

`enabled` : включается функция или активируется параметр.

SYNCFIX

Включить разрешение конфликтов синхронизации в Microsoft Outlook.

СИНТАКСИС

```
[get] | restore syncfix
set syncfix <число>
```

ОПЕРАЦИИ

`get` : возвращается текущий параметр/состояние.

`set` : задается значение или состояние.

`restore` : восстанавливаются параметры/объект/файл по умолчанию.

`0` — отключено, `3` — полностью включено, другие возможные значения.

4.10.2.21 Контекст «AV EMAIL OUTLOOK RESCAN»

ONCHANGE

Отключить проверку при изменении содержимого папки «Входящие».

СИНТАКСИС

```
[get] | restore onchange
set onchange disabled | enabled
```

ОПЕРАЦИИ

`get` : возвращается текущий параметр/состояние.

`set` : задается значение или состояние.

`restore` : восстанавливаются параметры/объект/файл по умолчанию.

АРГУМЕНТЫ

`disabled` : отключается функция или параметр.

`enabled` : включается функция или активируется параметр.

4.10.2.22 Контекст «AV EMAIL PROTOCOL POP3»

COMPATIBILITY

Настройка совместимости.

СИНТАКСИС

```
[get] | restore compatibility

set compatibility compatible | both | effective
```

ОПЕРАЦИИ

`get` : возвращается текущий параметр/состояние.

`set` : задается значение или состояние.

`restore` : восстанавливаются параметры/объект/файл по умолчанию.

АРГУМЕНТЫ

`compatible` : максимальный уровень совместимости.

`both` : средний уровень совместимости.

`effective` : максимальная эффективность.

ПРИМЕЧАНИЕ: Не все почтовые клиенты способны корректно работать совместно с фильтрацией POP3 в обычном режиме. Следующие параметры позволяют настроить уровень совместимости, чтобы избежать возможных конфликтов. Однако повышение уровня совместимости может привести к снижению эффективности интернет-монитора и невозможности использовать некоторые из его функций.

PORTS

Порты, используемые протоколом POP3.

СИНТАКСИС

```
[get] | restore ports

set ports [<строка>]
```

ОПЕРАЦИИ

`get` : возвращается текущий параметр/состояние.

`set` : задается значение или состояние.

`restore` : восстанавливаются параметры/объект/файл по умолчанию.

АРГУМЕНТЫ

`строка` : номера портов через запятую.

USE

Проверять POP3.

СИНТАКСИС

```
[get] | restore use

set use disabled | enabled
```

ОПЕРАЦИИ

`get` : возвращается текущий параметр/состояние.

`set` : задается значение или состояние.

`restore` : восстанавливаются параметры/объект/файл по умолчанию.

АРГУМЕНТЫ

`disabled` : отключается функция или параметр.

`enabled` : включается функция или активируется параметр.

4.10.2.23 Контекст «AV EMAIL PROTOCOL POP3S»

COMPATIBILITY

Настройка совместимости.

СИНТАКСИС

```
[get] | restore compatibility

set compatibility compatible | both | effective
```

ОПЕРАЦИИ

`get` : возвращается текущий параметр/состояние.

`set` : задается значение или состояние.

`restore` : восстанавливаются параметры/объект/файл по умолчанию.

АРГУМЕНТЫ

`compatible` : максимальный уровень совместимости.

`both` : средний уровень совместимости.

`effective` : максимальная эффективность.

ПРИМЕЧАНИЕ: Не все почтовые клиенты способны корректно работать совместно с фильтрацией POP3S в обычном режиме. Следующие параметры позволяют настроить уровень совместимости, чтобы избежать возможных конфликтов. Однако повышение уровня совместимости может привести к снижению эффективности интернет-монитора и невозможности использовать некоторые из его функций.

РЕЖИМ

Режим фильтрации POP3S.

СИНТАКСИС

```
[get] | restore mode

set mode none | ports | clients
```

ОПЕРАЦИИ

`get` : возвращается текущий параметр/состояние.

`set` : задается значение или состояние.

`restore` : восстанавливаются параметры/объект/файл по умолчанию.

АРГУМЕНТЫ

`none` : не проверять протокол POP3S.

`ports` : проверять протокол POP3S на указанных портах.

`clients` : проверять протокол POP3S для приложений, отмеченных как почтовые клиенты, на указанных портах.

PORTS

Порты, используемые протоколом POP3S.

СИНТАКСИС

```
[get] | restore ports

set ports [<строка>]
```

ОПЕРАЦИИ

`get` : возвращается текущий параметр/состояние.

`set` : задается значение или состояние.

`restore` : восстанавливаются параметры/объект/файл по умолчанию.

АРГУМЕНТЫ

`строка` : номера портов через запятую.

4.10.2.24 Контекст «AV EMAIL RESCAN»

ONUPDATE

Повторить сканирование после обновления.

СИНТАКСИС

```
[get] | restore onupdate
set onupdate disabled | enabled
```

ОПЕРАЦИИ

`get` : возвращается текущий параметр/состояние.

`set` : задается значение или состояние.

`restore` : восстанавливаются параметры/объект/файл по умолчанию.

АРГУМЕНТЫ

`disabled` : отключается функция или параметр.

`enabled` : включается функция или активируется параметр.

4.10.2.25 Контекст «AV EMAIL SCAN»

OTHERMODULES

Включить результаты сканирования другими модулями.

СИНТАКСИС

```
[get] | restore othermodules
set othermodules disabled | enabled
```

ОПЕРАЦИИ

`get` : возвращается текущий параметр/состояние.

`set` : задается значение или состояние.

`restore` : восстанавливаются параметры/объект/файл по умолчанию.

АРГУМЕНТЫ

`disabled` : отключается функция или параметр.

`enabled` : включается функция или активируется параметр.

PLAIN

Сканировать тело сообщений в формате обычного текста.

СИНТАКСИС

```
[get] | restore plain
set plain disabled | enabled
```

ОПЕРАЦИИ

`get` : возвращается текущий параметр/состояние.

`set` : задается значение или состояние.

`restore` : восстанавливаются параметры/объект/файл по умолчанию.

АРГУМЕНТЫ

`disabled` : отключается функция или параметр.

`enabled` : включается функция или активируется параметр.

READ

Сканировать прочитанные сообщения.

СИНТАКСИС

```
[get] | restore read

set read disabled | enabled
```

ОПЕРАЦИИ

`get` : возвращается текущий параметр/состояние.

`set` : задается значение или состояние.

`restore` : восстанавливаются параметры/объект/файл по умолчанию.

АРГУМЕНТЫ

`disabled` : отключается функция или параметр.

`enabled` : включается функция или активируется параметр.

RECEIVED

Сканировать полученные сообщения.

СИНТАКСИС

```
[get] | restore received

set received disabled | enabled
```

ОПЕРАЦИИ

`get` : возвращается текущий параметр/состояние.

`set` : задается значение или состояние.

`restore` : восстанавливаются параметры/объект/файл по умолчанию.

АРГУМЕНТЫ

`disabled` : отключается функция или параметр.

`enabled` : включается функция или активируется параметр.

RTF

Сканировать тело сообщений в формате RTF.

СИНТАКСИС

```
[get] | restore rtf

set rtf disabled | enabled
```

ОПЕРАЦИИ

`get` : возвращается текущий параметр/состояние.

`set` : задается значение или состояние.

`restore` : восстанавливаются параметры/объект/файл по умолчанию.

АРГУМЕНТЫ

`disabled` : отключается функция или параметр.

`enabled` : включается функция или активируется параметр.

SENT

Сканировать отправленные сообщения.

СИНТАКСИС

```
[get] | restore sent
set sent disabled | enabled
```

ОПЕРАЦИИ

`get` : возвращается текущий параметр/состояние.

`set` : задается значение или состояние.

`restore` : восстанавливаются параметры/объект/файл по умолчанию.

АРГУМЕНТЫ

`disabled` : отключается функция или параметр.

`enabled` : включается функция или активируется параметр.

4.10.2.26 Контекст «AV EMAIL THUNDERBIRD»

INTEGRATION

Интегрировать в Mozilla Thunderbird.

СИНТАКСИС

```
[get] | restore integration
set integration disabled | enabled
```

ОПЕРАЦИИ

`get` : возвращается текущий параметр/состояние.

`set` : задается значение или состояние.

`restore` : восстанавливаются параметры/объект/файл по умолчанию.

АРГУМЕНТЫ

`disabled` : отключается функция или параметр.

`enabled` : включается функция или активируется параметр.

4.10.2.27 Контекст «AV EMAIL WINLIVE»

INTEGRATION

Интегрировать в Windows Live Mail.

СИНТАКСИС

```
[get] | restore integration
set integration disabled | enabled
```

ОПЕРАЦИИ

`get` : возвращается текущий параметр/состояние.

`set` : задается значение или состояние.

`restore` : восстанавливаются параметры/объект/файл по умолчанию.

АРГУМЕНТЫ

`disabled` : отключается функция или параметр.

`enabled` : включается функция или активируется параметр.

4.10.2.28 Контекст «AV LIMITS ARCHIVE»

LEVEL

Уровень вложенности архивов.

СИНТАКСИС

```
[get] | restore level
```

```
set level <число>
```

ОПЕРАЦИИ

`get` : возвращается текущий параметр/состояние.

`set` : задается значение или состояние.

`restore` : восстанавливаются параметры/объект/файл по умолчанию.

АРГУМЕНТЫ

`число` : уровень от 1 до 20 или 0 для выбора параметров по умолчанию.

SIZE

Максимальный размер файла в архиве в килобайтах.

СИНТАКСИС

```
[get] | restore size
```

```
set size <число>
```

ОПЕРАЦИИ

`get` : возвращается текущий параметр/состояние.

`set` : задается значение или состояние.

`restore` : восстанавливаются параметры/объект/файл по умолчанию.

АРГУМЕНТЫ

`число` : размер в Кб или 0 для выбора параметров по умолчанию.

4.10.2.29 Контекст «AV LIMITS OBJECTS»

SIZE

Максимальный размер архива (Кб).

СИНТАКСИС

```
[get] | restore size
```

```
set size <число>
```

ОПЕРАЦИИ

`get` : возвращается текущий параметр/состояние.

`set` : задается значение или состояние.

`restore` : восстанавливаются параметры/объект/файл по умолчанию.

АРГУМЕНТЫ

`число` : размер в Кб или 0 для выбора параметров по умолчанию.

TIMEOUT

Максимальное время сканирования архивов в секундах.

СИНТАКСИС

```
[get] | restore timeout

set timeout <число>
```

ОПЕРАЦИИ

`get` : возвращается текущий параметр/состояние.

`set` : задается значение или состояние.

`restore` : восстанавливаются параметры/объект/файл по умолчанию.

АРГУМЕНТЫ

`число` : время в секундах или 0 для выбора параметров по умолчанию.

4.10.2.30 Контекст «AV NETFILTER»

AUTOSTART

Автоматически запускать фильтрацию содержимого приложений, использующих протоколы HTTP и POP3.

СИНТАКСИС

```
[get] | restore autostart

set autostart disabled | enabled
```

ОПЕРАЦИИ

`get` : возвращается текущий параметр/состояние.

`set` : задается значение или состояние.

`restore` : восстанавливаются параметры/объект/файл по умолчанию.

АРГУМЕНТЫ

`disabled` : отключается функция или параметр.

`enabled` : включается функция или активируется параметр.

EXCLUDED

Приложения, для которых отключена фильтрация протоколов.

СИНТАКСИС

```
[get] excluded

add | remove excluded <путь>
```

ОПЕРАЦИИ

`get` : возвращается текущий параметр/состояние.

`add` : добавляется элемент.

`remove` : удаляется элемент.

АРГУМЕНТЫ

`путь` : путь приложения.

РЕЖИМ

Перенаправить трафик на фильтрацию.

СИНТАКСИС

```
[get] | restore mode

set mode ports | application | both
```

ОПЕРАЦИИ

`get` : возвращается текущий параметр/состояние.

`set` : задается значение или состояние.

`restore` : восстанавливаются параметры/объект/файл по умолчанию.

АРГУМЕНТЫ

`ports` : порты HTTP и POP3.

`приложение` : приложения, помеченные как веб-браузеры или почтовые клиенты.

`both` : порты и приложения, помеченные как веб-браузеры или почтовые клиенты.

STATUS

Включить фильтрацию содержимого приложений, использующих протоколы HTTP и POP3.

СИНТАКСИС

```
[get] | restore status

set status disabled | enabled
```

ОПЕРАЦИИ

`get` : возвращается текущий параметр/состояние.

`set` : задается значение или состояние.

`restore` : восстанавливаются параметры/объект/файл по умолчанию.

АРГУМЕНТЫ

`disabled` : отключается функция или параметр.

`enabled` : включается функция или активируется параметр.

4.10.2.31 Контекст «AV NETFILTER PROTOCOL SSL»

BLOCKSSL2

Блокировать шифрованное соединение с использованием устаревшего протокола SSL версии 2.

СИНТАКСИС

```
[get] | restore blockssl2

set blockssl2 disabled | enabled
```

ОПЕРАЦИИ

`get` : возвращается текущий параметр/состояние.

`set` : задается значение или состояние.

`restore` : восстанавливаются параметры/объект/файл по умолчанию.

АРГУМЕНТЫ

`disabled` : отключается функция или параметр.

`enabled` : включается функция или активируется параметр.

EXCEPTIONS

Применять созданные исключения на основе сертификатов.

СИНТАКСИС

```
[get] | restore exceptions

set exceptions disabled | enabled
```

ОПЕРАЦИИ

`get` : возвращается текущий параметр/состояние.

`set` : задается значение или состояние.

`restore` : восстанавливаются параметры/объект/файл по умолчанию.

АРГУМЕНТЫ

`disabled` : отключается функция или параметр.

`enabled` : включается функция или активируется параметр.

РЕЖИМ

Режим фильтрации SSL.

СИНТАКСИС

```
[get] | restore mode

set mode allways | ask | none
```

ОПЕРАЦИИ

`get` : возвращается текущий параметр/состояние.

`set` : задается значение или состояние.

`restore` : восстанавливаются параметры/объект/файл по умолчанию.

АРГУМЕНТЫ

`allways` : всегда проверять SSL.

`ask` : запрашивать о новых сайтах (возможна настройка исключений).

`none` : не проверять протокол SSL.

4.10.2.32 Контекст «AV NETFILTER PROTOCOL SSL CERTIFICATE»

ADDTOBROWSERS

Добавить корневой сертификат к известным браузерам.

СИНТАКСИС

```
[get] | restore addtobrowsers

set addtobrowsers disabled | enabled
```

ОПЕРАЦИИ

`get` : возвращается текущий параметр/состояние.

`set` : задается значение или состояние.

`restore` : восстанавливаются параметры/объект/файл по умолчанию.

АРГУМЕНТЫ

`disabled` : отключается функция или параметр.

`enabled` : включается функция или активируется параметр.

ПРИМЕЧАНИЕ: Чтобы обеспечить надлежащую проверку трафика, шифруемого по протоколу SSL, в хранилище TRCA будет добавлен корневой сертификат ESET, spol. s r.o.

EXCLUDED

Список сертификатов, исключенных из фильтрации содержимого.

СИНТАКСИС

```
[get] excluded

 remove excluded <имя>
```

ОПЕРАЦИИ

`get` : возвращается текущий параметр/состояние.

`remove` : удаляется элемент.

АРГУМЕНТЫ

`имя` : имя сертификата.

NOTTRUSTED

Не доверенный, если сертификат недействителен или поврежден.

СИНТАКСИС

```
[get] | restore nottrusted

set nottrusted ask | block
```

ОПЕРАЦИИ

`get` : возвращается текущий параметр/состояние.

`set` : задается значение или состояние.

`restore` : восстанавливаются параметры/объект/файл по умолчанию.

АРГУМЕНТЫ

`ask` : запрашивать действительность сертификата.

`block` : блокировать соединения, использующие сертификат.

TRUSTED

Список доверенных сертификатов.

СИНТАКСИС

```
[get] trusted

remove trusted <имя>
```

ОПЕРАЦИИ

`get` : возвращается текущий параметр/состояние.

`remove` : удаляется элемент.

АРГУМЕНТЫ

`имя` : имя сертификата.

UNKNOWNROOT

Неизвестный корневой, если проверить сертификат с помощью хранилища TRCA не удается.

СИНТАКСИС

```
[get] | restore unknownroot

set unknownroot ask | block
```

ОПЕРАЦИИ

`get` : возвращается текущий параметр/состояние.

`set` : задается значение или состояние.

`restore` : восстанавливаются параметры/объект/файл по умолчанию.

АРГУМЕНТЫ

`ask` : запрашивать действительность сертификата.

`block` : блокировать соединения, использующие сертификат.

4.10.2.33 Контекст «AV OBJECTS»

ARCHIVE

Сканировать архивы.

СИНТАКСИС

```
[get] | restore archive

set archive disabled | enabled
```

ОПЕРАЦИИ

`get` : возвращается текущий параметр/состояние.

`set` : задается значение или состояние.

`restore` : восстанавливаются параметры/объект/файл по умолчанию.

АРГУМЕНТЫ

`disabled` : отключается функция или параметр.

`enabled` : включается функция или активируется параметр.

BOOT

Сканировать загрузочные секторы.

СИНТАКСИС

```
[get] | restore boot

set boot disabled | enabled
```

ОПЕРАЦИИ

`get` : возвращается текущий параметр/состояние.

`set` : задается значение или состояние.

`restore` : восстанавливаются параметры/объект/файл по умолчанию.

АРГУМЕНТЫ

`disabled` : отключается функция или параметр.

`enabled` : включается функция или активируется параметр.

EMAIL

Сканировать файлы электронной почты.

СИНТАКСИС

```
[get] | restore email

set email disabled | enabled
```

ОПЕРАЦИИ

`get` : возвращается текущий параметр/состояние.

`set` : задается значение или состояние.

`restore` : восстанавливаются параметры/объект/файл по умолчанию.

АРГУМЕНТЫ

`disabled` : отключается функция или параметр.

`enabled` : включается функция или активируется параметр.

FILE

Сканировать файлы.

СИНТАКСИС

```
[get] | restore file
set file disabled | enabled
```

ОПЕРАЦИИ

`get` : возвращается текущий параметр/состояние.

`set` : задается значение или состояние.

`restore` : восстанавливаются параметры/объект/файл по умолчанию.

АРГУМЕНТЫ

`disabled` : отключается функция или параметр.

`enabled` : включается функция или активируется параметр.

MEMORY

Сканировать память.

СИНТАКСИС

```
[get] | restore memory
set memory disabled | enabled
```

ОПЕРАЦИИ

`get` : возвращается текущий параметр/состояние.

`set` : задается значение или состояние.

`restore` : восстанавливаются параметры/объект/файл по умолчанию.

АРГУМЕНТЫ

`disabled` : отключается функция или параметр.

`enabled` : включается функция или активируется параметр.

RUNTIME

Сканировать упаковщики.

СИНТАКСИС

```
[get] | restore runtime
set runtime disabled | enabled
```

ОПЕРАЦИИ

`get` : возвращается текущий параметр/состояние.

`set` : задается значение или состояние.

`restore` : восстанавливаются параметры/объект/файл по умолчанию.

АРГУМЕНТЫ

`disabled` : отключается функция или параметр.

`enabled` : включается функция или активируется параметр.

SFX

Сканировать самораспаковывающиеся архивы.

СИНТАКСИС

```
[get] | restore sfx
set sfx disabled | enabled
```

ОПЕРАЦИИ

`get` : возвращается текущий параметр/состояние.

`set` : задается значение или состояние.

`restore` : восстанавливаются параметры/объект/файл по умолчанию.

АРГУМЕНТЫ

`disabled` : отключается функция или параметр.

`enabled` : включается функция или активируется параметр.

4.10.2.34 Контекст «AV OPTIONS»

ADVHEURISTICS

Использовать расширенную эвристику.

СИНТАКСИС

```
[get] | restore advheuristics

set advheuristics disabled | enabled
```

ОПЕРАЦИИ

`get` : возвращается текущий параметр/состояние.

`set` : задается значение или состояние.

`restore` : восстанавливаются параметры/объект/файл по умолчанию.

АРГУМЕНТЫ

`disabled` : отключается функция или параметр.

`enabled` : включается функция или активируется параметр.

ADWARE

Обнаружение рекламных/шпионских/опасных программ.

СИНТАКСИС

```
[get] | restore adware

set adware disabled | enabled
```

ОПЕРАЦИИ

`get` : возвращается текущий параметр/состояние.

`set` : задается значение или состояние.

`restore` : восстанавливаются параметры/объект/файл по умолчанию.

АРГУМЕНТЫ

`disabled` : отключается функция или параметр.

`enabled` : включается функция или активируется параметр.

HEURISTICS

Использовать эвристический анализ.

СИНТАКСИС

```
[get] | restore heuristics

set heuristics disabled | enabled
```

ОПЕРАЦИИ

`get` : возвращается текущий параметр/состояние.

`set` : задается значение или состояние.

`restore` : восстанавливаются параметры/объект/файл по умолчанию.

АРГУМЕНТЫ

`disabled` : отключается функция или параметр.

`enabled` : включается функция или активируется параметр.

SIGNATURES

Использовать сигнатуры.

СИНТАКСИС

```
[get] | restore signatures

set signatures disabled | enabled
```

ОПЕРАЦИИ

`get` : возвращается текущий параметр/состояние.

`set` : задается значение или состояние.

`restore` : восстанавливаются параметры/объект/файл по умолчанию.

АРГУМЕНТЫ

`disabled` : отключается функция или параметр.

`enabled` : включается функция или активируется параметр.

UNSAFE

Обнаружение потенциально опасных приложений.

СИНТАКСИС

```
[get] | restore unsafe

set unsafe disabled | enabled
```

ОПЕРАЦИИ

`get` : возвращается текущий параметр/состояние.

`set` : задается значение или состояние.

`restore` : восстанавливаются параметры/объект/файл по умолчанию.

АРГУМЕНТЫ

`disabled` : отключается функция или параметр.

`enabled` : включается функция или активируется параметр.

UNWANTED

Обнаружение потенциально нежелательных приложений.

СИНТАКСИС

```
[get] | restore unwanted

set unwanted disabled | enabled
```

ОПЕРАЦИИ

`get` : возвращается текущий параметр/состояние.

`set` : задается значение или состояние.

`restore` : восстанавливаются параметры/объект/файл по умолчанию.

АРГУМЕНТЫ

`disabled` : отключается функция или параметр.

`enabled` : включается функция или активируется параметр.

4.10.2.35 Контекст «AV OTHER»

LOGALL

Регистрировать все объекты.

СИНТАКСИС

```
[get] | restore logall

set logall disabled | enabled
```

ОПЕРАЦИИ

`get` : возвращается текущий параметр/состояние.

`set` : задается значение или состояние.

`restore` : восстанавливаются параметры/объект/файл по умолчанию.

АРГУМЕНТЫ

`disabled` : отключается функция или параметр.

`enabled` : включается функция или активируется параметр.

OPTIMIZE

Оптимизация Smart.

СИНТАКСИС

```
[get] | restore optimize

set optimize disabled | enabled
```

ОПЕРАЦИИ

`get` : возвращается текущий параметр/состояние.

`set` : задается значение или состояние.

`restore` : восстанавливаются параметры/объект/файл по умолчанию.

АРГУМЕНТЫ

`disabled` : отключается функция или параметр.

`enabled` : включается функция или активируется параметр.

4.10.2.36 Контекст «AV REALTIME»

AUTOSTART

Запускать защиту в режиме реального времени автоматически.

СИНТАКСИС

```
[get] | restore autostart

set autostart disabled | enabled
```

ОПЕРАЦИИ

`get` : возвращается текущий параметр/состояние.

`set` : задается значение или состояние.

`restore` : восстанавливаются параметры/объект/файл по умолчанию.

АРГУМЕНТЫ

`disabled` : отключается функция или параметр.

`enabled` : включается функция или активируется параметр.

CLEANLEVEL

Уровень очистки.

СИНТАКСИС

```
[get] | restore cleanlevel

set cleanlevel none | normal | strict
```

ОПЕРАЦИИ

`get` : возвращается текущий параметр/состояние.

`set` : задается значение или состояние.

`restore` : восстанавливаются параметры/объект/файл по умолчанию.

АРГУМЕНТЫ

`none` : без очистки.

`normal` : стандартная очистка.

`strict` : тщательная очистка.

EXTENSIONS

Сканируемые/исключенные расширения.

СИНТАКСИС

```
[get] | restore extensions

add | remove extensions <расширение> | /all | /extless
```

ОПЕРАЦИИ

`get` : возвращается текущий параметр/состояние.

`add` : добавляется элемент.

`remove` : удаляется элемент.

`restore` : восстанавливаются параметры/объект/файл по умолчанию.

АРГУМЕНТЫ

`extension` : расширение.

`all` : все файлы.

`extless` : файлы без расширений.

STATUS

Состояние защита компьютера в режиме реального времени.

СИНТАКСИС

```
[get] | restore status

set status disabled | enabled
```

ОПЕРАЦИИ

`get` : возвращается текущий параметр/состояние.

`set` : задается значение или состояние.

`restore` : восстанавливаются параметры/объект/файл по умолчанию.

АРГУМЕНТЫ

`disabled` : отключается функция или параметр.

`enabled` : включается функция или активируется параметр.

4.10.2.37 Контекст «AV REALTIME DISK»

FLOPPY

Сканировать съемные носители.

СИНТАКСИС

```
[get] | restore floppy
set floppy disabled | enabled
```

ОПЕРАЦИИ

`get` : возвращается текущий параметр/состояние.

`set` : задается значение или состояние.

`restore` : восстанавливаются параметры/объект/файл по умолчанию.

АРГУМЕНТЫ

`disabled` : отключается функция или параметр.

`enabled` : включается функция или активируется параметр.

LOCAL

Сканировать локальные диски.

СИНТАКСИС

```
[get] | restore local
set local disabled | enabled
```

ОПЕРАЦИИ

`get` : возвращается текущий параметр/состояние.

`set` : задается значение или состояние.

`restore` : восстанавливаются параметры/объект/файл по умолчанию.

АРГУМЕНТЫ

`disabled` : отключается функция или параметр.

`enabled` : включается функция или активируется параметр.

NETWORK

Сканировать сетевые диски.

СИНТАКСИС

```
[get] | restore network
set network disabled | enabled
```

ОПЕРАЦИИ

`get` : возвращается текущий параметр/состояние.

`set` : задается значение или состояние.

`restore` : восстанавливаются параметры/объект/файл по умолчанию.

АРГУМЕНТЫ

`disabled` : отключается функция или параметр.

`enabled` : включается функция или активируется параметр.

4.10.2.38 Контекст «AV REALTIME EVENT»

CREATE

Сканировать файлы при создании.

СИНТАКСИС

```
[get] | restore create

set create disabled | enabled
```

ОПЕРАЦИИ

`get` : возвращается текущий параметр/состояние.

`set` : задается значение или состояние.

`restore` : восстанавливаются параметры/объект/файл по умолчанию.

АРГУМЕНТЫ

`disabled` : отключается функция или параметр.

`enabled` : включается функция или активируется параметр.

EXECUTE

Сканировать файлы при запуске.

СИНТАКСИС

```
[get] | restore execute

set execute disabled | enabled
```

ОПЕРАЦИИ

`get` : возвращается текущий параметр/состояние.

`set` : задается значение или состояние.

`restore` : восстанавливаются параметры/объект/файл по умолчанию.

АРГУМЕНТЫ

`disabled` : отключается функция или параметр.

`enabled` : включается функция или активируется параметр.

FLOPPYACCESS

Сканировать при доступе к гибкому диску.

СИНТАКСИС

```
[get] | restore floppyaccess

set floppyaccess disabled | enabled
```

ОПЕРАЦИИ

`get` : возвращается текущий параметр/состояние.

`set` : задается значение или состояние.

`restore` : восстанавливаются параметры/объект/файл по умолчанию.

АРГУМЕНТЫ

`disabled` : отключается функция или параметр.

`enabled` : включается функция или активируется параметр.

OPEN

Сканировать файлы при открытии.

СИНТАКСИС

```
[get] | restore open

set open disabled | enabled
```

ОПЕРАЦИИ

`get` : возвращается текущий параметр/состояние.

`set` : задается значение или состояние.

`restore` : восстанавливаются параметры/объект/файл по умолчанию.

АРГУМЕНТЫ

`disabled` : отключается функция или параметр.

`enabled` : включается функция или активируется параметр.

SHUTDOWN

Сканировать при выключении компьютера.

СИНТАКСИС

```
[get] | restore shutdown

set shutdown disabled | enabled
```

ОПЕРАЦИИ

`get` : возвращается текущий параметр/состояние.

`set` : задается значение или состояние.

`restore` : восстанавливаются параметры/объект/файл по умолчанию.

АРГУМЕНТЫ

`disabled` : отключается функция или параметр.

`enabled` : включается функция или активируется параметр.

4.10.2.39 Контекст «AV REALTIME EXECUTABLE»

ADVHEURISTICS

Включить расширенную эвристику запуска файлов.

СИНТАКСИС

```
[get] | restore advheuristics

set advheuristics disabled | enabled
```

ОПЕРАЦИИ

`get` : возвращается текущий параметр/состояние.

`set` : задается значение или состояние.

`restore` : восстанавливаются параметры/объект/файл по умолчанию.

АРГУМЕНТЫ

`disabled` : отключается функция или параметр.

`enabled` : включается функция или активируется параметр.

4.10.2.40 Контекст «AV REALTIME EXECUTABLE FROMREMOVABLE»

ADVHEURISTICS

Включить расширенную эвристику запуска файлов со съемных носителей.

СИНТАКСИС

```
[get] | restore advheuristics

set advheuristics disabled | enabled
```

ОПЕРАЦИИ

`get` : возвращается текущий параметр/состояние.

`set` : задается значение или состояние.

`restore` : восстанавливаются параметры/объект/файл по умолчанию.

АРГУМЕНТЫ

`disabled` : отключается функция или параметр.

`enabled` : включается функция или активируется параметр.

EXCLUSION

Исключения для дисков USB.

СИНТАКСИС

```
[get] | restore exclusion

select exclusion none | <диск> | all
```

ОПЕРАЦИИ

`get` : возвращается текущий параметр/состояние.

`select` : выбирается элемент.

`restore` : восстанавливаются параметры/объект/файл по умолчанию.

АРГУМЕНТЫ

`none` : отменяется выбор всех дисков.

`диск` : буквенное обозначение диска, который нужно выбрать или выбор которого нужно отменить.

`all` : выбираются все диски.

ПРИМЕЧАНИЕ: Используйте этот параметр, чтобы разрешить исключения из сканирования с использованием расширенной эвристики при запуске файлов. К выбранным устройствам будут применены параметры расширенной эвристики для жестких дисков.

4.10.2.41 Контекст «AV REALTIME LIMITS ARCHIVE»

LEVEL

Уровень вложенности архивов.

СИНТАКСИС

```
[get] | restore level

set level <число>
```

ОПЕРАЦИИ

`get` : возвращается текущий параметр/состояние.

`set` : задается значение или состояние.

`restore` : восстанавливаются параметры/объект/файл по умолчанию.

АРГУМЕНТЫ

`число` : уровень от 1 до 20 или 0 для выбора параметров по умолчанию.

SIZE

Максимальный размер файла в архиве в килобайтах.

СИНТАКСИС

```
[get] | restore size
```

```
set size <число>
```

ОПЕРАЦИИ

`get` : возвращается текущий параметр/состояние.

`set` : задается значение или состояние.

`restore` : восстанавливаются параметры/объект/файл по умолчанию.

АРГУМЕНТЫ

`число` : размер в Кб или 0 для выбора параметров по умолчанию.

4.10.2.42 Контекст «AV REALTIME LIMITS OBJECTS»

SIZE

Максимальный размер архива (Кб).

СИНТАКСИС

```
[get] | restore size
```

```
set size <число>
```

ОПЕРАЦИИ

`get` : возвращается текущий параметр/состояние.

`set` : задается значение или состояние.

`restore` : восстанавливаются параметры/объект/файл по умолчанию.

АРГУМЕНТЫ

`число` : размер в Кб или 0 для выбора параметров по умолчанию.

TIMEOUT

Максимальное время сканирования архивов в секундах.

СИНТАКСИС

```
[get] | restore timeout
```

```
set timeout <число>
```

ОПЕРАЦИИ

`get` : возвращается текущий параметр/состояние.

`set` : задается значение или состояние.

`restore` : восстанавливаются параметры/объект/файл по умолчанию.

АРГУМЕНТЫ

`число` : время в секундах или 0 для выбора параметров по умолчанию.

4.10.2.43 Контекст «AV REALTIME OBJECTS»

ARCHIVE

Сканировать архивы.

СИНТАКСИС

```
[get] | restore archive

set archive disabled | enabled
```

ОПЕРАЦИИ

`get` : возвращается текущий параметр/состояние.

`set` : задается значение или состояние.

`restore` : восстанавливаются параметры/объект/файл по умолчанию.

АРГУМЕНТЫ

`disabled` : отключается функция или параметр.

`enabled` : включается функция или активируется параметр.

BOOT

Сканировать загрузочные секторы.

СИНТАКСИС

```
[get] | restore boot

set boot disabled | enabled
```

ОПЕРАЦИИ

`get` : возвращается текущий параметр/состояние.

`set` : задается значение или состояние.

`restore` : восстанавливаются параметры/объект/файл по умолчанию.

АРГУМЕНТЫ

`disabled` : отключается функция или параметр.

`enabled` : включается функция или активируется параметр.

EMAIL

Сканировать файлы электронной почты.

СИНТАКСИС

```
[get] | restore email

set email disabled | enabled
```

ОПЕРАЦИИ

`get` : возвращается текущий параметр/состояние.

`set` : задается значение или состояние.

`restore` : восстанавливаются параметры/объект/файл по умолчанию.

АРГУМЕНТЫ

`disabled` : отключается функция или параметр.

`enabled` : включается функция или активируется параметр.

FILE

Сканировать файлы.

СИНТАКСИС

```
[get] | restore file
set file disabled | enabled
```

ОПЕРАЦИИ

`get` : возвращается текущий параметр/состояние.

`set` : задается значение или состояние.

`restore` : восстанавливаются параметры/объект/файл по умолчанию.

АРГУМЕНТЫ

`disabled` : отключается функция или параметр.

`enabled` : включается функция или активируется параметр.

MEMORY

Сканировать память.

СИНТАКСИС

```
[get] | restore memory
set memory disabled | enabled
```

ОПЕРАЦИИ

`get` : возвращается текущий параметр/состояние.

`set` : задается значение или состояние.

`restore` : восстанавливаются параметры/объект/файл по умолчанию.

АРГУМЕНТЫ

`disabled` : отключается функция или параметр.

`enabled` : включается функция или активируется параметр.

RUNTIME

Сканировать упаковщики.

СИНТАКСИС

```
[get] | restore runtime
set runtime disabled | enabled
```

ОПЕРАЦИИ

`get` : возвращается текущий параметр/состояние.

`set` : задается значение или состояние.

`restore` : восстанавливаются параметры/объект/файл по умолчанию.

АРГУМЕНТЫ

`disabled` : отключается функция или параметр.

`enabled` : включается функция или активируется параметр.

SFX

Сканировать самораспаковывающиеся архивы.

СИНТАКСИС

```
[get] | restore sfx
set sfx disabled | enabled
```

ОПЕРАЦИИ

`get` : возвращается текущий параметр/состояние.

`set` : задается значение или состояние.

`restore` : восстанавливаются параметры/объект/файл по умолчанию.

АРГУМЕНТЫ

`disabled` : отключается функция или параметр.

`enabled` : включается функция или активируется параметр.

4.10.2.44 Контекст «AV REALTIME ONWRITE»

ADVHEURISTICS

Включить расширенную эвристику для новых и измененных файлов.

СИНТАКСИС

```
[get] | restore advheuristics

set advheuristics disabled | enabled
```

ОПЕРАЦИИ

`get` : возвращается текущий параметр/состояние.

`set` : задается значение или состояние.

`restore` : восстанавливаются параметры/объект/файл по умолчанию.

АРГУМЕНТЫ

`disabled` : отключается функция или параметр.

`enabled` : включается функция или активируется параметр.

RUNTIME

Сканировать новые и измененные архивы.

СИНТАКСИС

```
[get] | restore runtime

set runtime disabled | enabled
```

ОПЕРАЦИИ

`get` : возвращается текущий параметр/состояние.

`set` : задается значение или состояние.

`restore` : восстанавливаются параметры/объект/файл по умолчанию.

АРГУМЕНТЫ

`disabled` : отключается функция или параметр.

`enabled` : включается функция или активируется параметр.

SFX

Сканировать новые и измененные самораспаковывающиеся архивы.

СИНТАКСИС

```
[get] | restore sfx

set sfx disabled | enabled
```

ОПЕРАЦИИ

`get` : возвращается текущий параметр/состояние.

`set` : задается значение или состояние.

`restore` : восстанавливаются параметры/объект/файл по умолчанию.

АРГУМЕНТЫ

`disabled` : отключается функция или параметр.

`enabled` : включается функция или активируется параметр.

4.10.2.45 Контекст «AV REALTIME ONWRITE ARCHIVE»

LEVEL

Глубина вложенности архивов.

СИНТАКСИС

```
[get] | restore level
set level <число>
```

ОПЕРАЦИИ

`get` : возвращается текущий параметр/состояние.

`set` : задается значение или состояние.

`restore` : восстанавливаются параметры/объект/файл по умолчанию.

АРГУМЕНТЫ

`число` : уровень (от 0 до 20).

SIZE

Максимальный размер сканируемого архивного файла в килобайтах.

СИНТАКСИС

```
[get] | restore size
set size <число>
```

ОПЕРАЦИИ

`get` : возвращается текущий параметр/состояние.

`set` : задается значение или состояние.

`restore` : восстанавливаются параметры/объект/файл по умолчанию.

АРГУМЕНТЫ

`число` : размер (Кб).

4.10.2.46 Контекст «AV REALTIME OPTIONS»

ADVHEURISTICS

Использовать расширенную эвристику.

СИНТАКСИС

```
[get] | restore advheuristics
set advheuristics disabled | enabled
```

ОПЕРАЦИИ

`get` : возвращается текущий параметр/состояние.

`set` : задается значение или состояние.

`restore` : восстанавливаются параметры/объект/файл по умолчанию.

АРГУМЕНТЫ

`disabled` : отключается функция или параметр.

`enabled` : включается функция или активируется параметр.

ADWARE

Обнаружение рекламных/шпионских/опасных программ.

СИНТАКСИС

```
[get] | restore adware

set adware disabled | enabled
```

ОПЕРАЦИИ

`get` : возвращается текущий параметр/состояние.

`set` : задается значение или состояние.

`restore` : восстанавливаются параметры/объект/файл по умолчанию.

АРГУМЕНТЫ

`disabled` : отключается функция или параметр.

`enabled` : включается функция или активируется параметр.

HEURISTICS

Использовать эвристический анализ.

СИНТАКСИС

```
[get] | restore heuristics

set heuristics disabled | enabled
```

ОПЕРАЦИИ

`get` : возвращается текущий параметр/состояние.

`set` : задается значение или состояние.

`restore` : восстанавливаются параметры/объект/файл по умолчанию.

АРГУМЕНТЫ

`disabled` : отключается функция или параметр.

`enabled` : включается функция или активируется параметр.

SIGNATURES

Использовать сигнатуры.

СИНТАКСИС

```
[get] | restore signatures

set signatures disabled | enabled
```

ОПЕРАЦИИ

`get` : возвращается текущий параметр/состояние.

`set` : задается значение или состояние.

`restore` : восстанавливаются параметры/объект/файл по умолчанию.

АРГУМЕНТЫ

`disabled` : отключается функция или параметр.

`enabled` : включается функция или активируется параметр.

UNSAFE

Обнаружение потенциально опасных приложений.

СИНТАКСИС

```
[get] | restore unsafe
set unsafe disabled | enabled
```

ОПЕРАЦИИ

`get` : возвращается текущий параметр/состояние.

`set` : задается значение или состояние.

`restore` : восстанавливаются параметры/объект/файл по умолчанию.

АРГУМЕНТЫ

`disabled` : отключается функция или параметр.

`enabled` : включается функция или активируется параметр.

UNWANTED

Обнаружение потенциально нежелательных приложений.

СИНТАКСИС

```
[get] | restore unwanted
set unwanted disabled | enabled
```

ОПЕРАЦИИ

`get` : возвращается текущий параметр/состояние.

`set` : задается значение или состояние.

`restore` : восстанавливаются параметры/объект/файл по умолчанию.

АРГУМЕНТЫ

`disabled` : отключается функция или параметр.

`enabled` : включается функция или активируется параметр.

4.10.2.47 Контекст «AV REALTIME OTHER»

LOGALL

Регистрировать все объекты.

СИНТАКСИС

```
[get] | restore logall
set logall disabled | enabled
```

ОПЕРАЦИИ

`get` : возвращается текущий параметр/состояние.

`set` : задается значение или состояние.

`restore` : восстанавливаются параметры/объект/файл по умолчанию.

АРГУМЕНТЫ

`disabled` : отключается функция или параметр.

`enabled` : включается функция или активируется параметр.

OPTIMIZE

Оптимизация Smart.

СИНТАКСИС

```
[get] | restore optimize
set optimize disabled | enabled
```

ОПЕРАЦИИ

`get` : возвращается текущий параметр/состояние.

`set` : задается значение или состояние.

`restore` : восстанавливаются параметры/объект/файл по умолчанию.

АРГУМЕНТЫ

`disabled` : отключается функция или параметр.

`enabled` : включается функция или активируется параметр.

4.10.2.48 Контекст «AV REALTIME REMOVABLE»

BLOCK

Блокировать съемные носители.

СИНТАКСИС

```
[get] | restore block
set block disabled | enabled
```

ОПЕРАЦИИ

`get` : возвращается текущий параметр/состояние.

`set` : задается значение или состояние.

`restore` : восстанавливаются параметры/объект/файл по умолчанию.

АРГУМЕНТЫ

`disabled` : отключается функция или параметр.

`enabled` : включается функция или активируется параметр.

EXCLUSION

Разрешенные съемные носители.

СИНТАКСИС

```
[get] | restore exclusion
select exclusion none | <диск> | all
```

ОПЕРАЦИИ

`get` : возвращается текущий параметр/состояние.

`select` : выбирается элемент.

`restore` : восстанавливаются параметры/объект/файл по умолчанию.

АРГУМЕНТЫ

`none` : отменяется выбор всех дисков.

`диск` : буквенное обозначение диска, который нужно выбрать или выбор которого нужно отменить.

`all` : выбираются все диски.

ПРИМЕЧАНИЕ: Используйте этот параметр, чтобы разрешить доступ к съемным носителям (компакт-дискам, гибким дискам, дискам USB). Если пометить носитель, ограничения на доступ к этому конкретному носителю будут отменены.

4.10.2.49 Контекст «AV WEB»

BROWSERS

Веб-браузеры.

СИНТАКСИС

```
[get] browsers
```

```
add | remove browsers <путь>
```

ОПЕРАЦИИ

`get` : возвращается текущий параметр/состояние.

`add` : добавляется элемент.

`remove` : удаляется элемент.

АРГУМЕНТЫ

`путь` : путь приложения.

ПРИМЕЧАНИЕ: Для усиления безопасности рекомендуется пометить все приложения, используемые в качестве веб-браузеров, установив соответствующий флажок. Если какое-либо приложение не помечено как веб-браузер, сканирование передаваемых приложением данных не гарантируется.

CLEANLEVEL

Уровень очистки.

СИНТАКСИС

```
[get] | restore cleanlevel
```

```
set cleanlevel none | normal | strict
```

ОПЕРАЦИИ

`get` : возвращается текущий параметр/состояние.

`set` : задается значение или состояние.

`restore` : восстанавливаются параметры/объект/файл по умолчанию.

АРГУМЕНТЫ

`none` : без очистки.

`normal` : стандартная очистка.

`strict` : тщательная очистка.

EXTENSIONS

Сканируемые/исключенные расширения.

СИНТАКСИС

```
[get] | restore extensions
```

```
add | remove extensions <расширение> | /all | /extless
```

ОПЕРАЦИИ

`get` : возвращается текущий параметр/состояние.

`add` : добавляется элемент.

`remove` : удаляется элемент.

`restore` : восстанавливаются параметры/объект/файл по умолчанию.

АРГУМЕНТЫ

`extension` : расширение.

`all` : все файлы.

`extless` : файлы без расширений.

STATUS

Защита доступа в Интернет.

СИНТАКСИС

```
[get] | restore status

set status disabled | enabled
```

ОПЕРАЦИИ

`get` : возвращается текущий параметр/состояние.

`set` : задается значение или состояние.

`restore` : восстанавливаются параметры/объект/файл по умолчанию.

АРГУМЕНТЫ

`disabled` : отключается функция или параметр.

`enabled` : включается функция или активируется параметр.

4.10.2.50 Контекст «AV WEB ADDRESSMGMT»

ADDRESS

Управление адресами в выбранном списке.

СИНТАКСИС

```
[get] | clear address

add | remove address <адрес>

import | export address <путь>
```

ОПЕРАЦИИ

`get` : возвращается текущий параметр/состояние.

`add` : добавляется элемент.

`remove` : удаляется элемент.

`import` : выполняется импорт из файла.

`export` : выполняется экспорт в файл.

`clear` : удаляются все элементы или файлы.

АРГУМЕНТЫ

`адрес` : адрес.

`путь` : путь к файлу.

LIST

Управление списками адресов.

СИНТАКСИС

```
[get] | restore list

set list <имя_списка> disabled | enabled

select | remove list <имя_списка>

add list allowed <имя_списка> | blocked <имя_списка> | excluded <имя_списка>
```

ОПЕРАЦИИ

`get` : возвращается текущий параметр/состояние.

`set` : задается значение или состояние.

`select` : выбирается для изменения.

`add` : добавляется элемент.

`remove` : удаляется элемент.

АРГУМЕНТЫ

`имя_списка` : имя списка.

`disabled` : не использовать список.

`enabled` : использовать список.

`allowed` : список разрешенных адресов.

`blocked` : список заблокированных адресов.

`excluded` : список адресов, исключенных из фильтрации.

ПРИМЕЧАНИЕ: Для изменения выбранного списка (помечен символом «x») используйте команду `av web addressmgmt address .`

NOTIFY

Уведомлять при совпадении адреса с шаблоном из списка.

СИНТАКСИС

```
[get] | restore notify

set notify disabled | enabled
```

ОПЕРАЦИИ

`get` : возвращается текущий параметр/состояние.

`set` : задается значение или состояние.

`restore` : восстанавливаются параметры/объект/файл по умолчанию.

АРГУМЕНТЫ

`disabled` : отключается функция или параметр.

`enabled` : включается функция или активируется параметр.

WHITELISTED

Разрешить доступ только для HTTP-адресов из списка разрешенных адресов.

СИНТАКСИС

```
[get] | restore whitelisted

set whitelisted disabled | enabled
```

ОПЕРАЦИИ

`get` : возвращается текущий параметр/состояние.

`set` : задается значение или состояние.

`restore` : восстанавливаются параметры/объект/файл по умолчанию.

АРГУМЕНТЫ

`disabled` : отключается функция или параметр.

`enabled` : включается функция или активируется параметр.

4.10.2.51 Контекст «AV WEB LIMITS ARCHIVE»

LEVEL

Уровень вложенности архивов.

СИНТАКСИС

```
[get] | restore level

set level <число>
```

ОПЕРАЦИИ

`get` : возвращается текущий параметр/состояние.

`set` : задается значение или состояние.

`restore` : восстанавливаются параметры/объект/файл по умолчанию.

АРГУМЕНТЫ

`число` : уровень от 1 до 20 или 0 для выбора параметров по умолчанию.

SIZE

Максимальный размер файла в архиве в килобайтах.

СИНТАКСИС

```
[get] | restore size

set size <число>
```

ОПЕРАЦИИ

`get` : возвращается текущий параметр/состояние.

`set` : задается значение или состояние.

`restore` : восстанавливаются параметры/объект/файл по умолчанию.

АРГУМЕНТЫ

`число` : размер в Кб или 0 для выбора параметров по умолчанию.

4.10.2.52 Контекст «AV WEB LIMITS OBJECTS»

SIZE

Максимальный размер архива (Кб).

СИНТАКСИС

```
[get] | restore size

set size <число>
```

ОПЕРАЦИИ

`get` : возвращается текущий параметр/состояние.

`set` : задается значение или состояние.

`restore` : восстанавливаются параметры/объект/файл по умолчанию.

АРГУМЕНТЫ

`число` : размер в Кб или 0 для выбора параметров по умолчанию.

TIMEOUT

Максимальное время сканирования архивов в секундах.

СИНТАКСИС

```
[get] | restore timeout

set timeout <число>
```

ОПЕРАЦИИ

`get` : возвращается текущий параметр/состояние.

`set` : задается значение или состояние.

`restore` : восстанавливаются параметры/объект/файл по умолчанию.

АРГУМЕНТЫ

`число` : время в секундах или 0 для выбора параметров по умолчанию.

4.10.2.53 Контекст «AV WEB OBJECTS»

ARCHIVE

Сканировать архивы.

СИНТАКСИС

```
[get] | restore archive

set archive disabled | enabled
```

ОПЕРАЦИИ

`get` : возвращается текущий параметр/состояние.

`set` : задается значение или состояние.

`restore` : восстанавливаются параметры/объект/файл по умолчанию.

АРГУМЕНТЫ

`disabled` : отключается функция или параметр.

`enabled` : включается функция или активируется параметр.

BOOT

Сканировать загрузочные секторы.

СИНТАКСИС

```
[get] | restore boot

set boot disabled | enabled
```

ОПЕРАЦИИ

`get` : возвращается текущий параметр/состояние.

`set` : задается значение или состояние.

`restore` : восстанавливаются параметры/объект/файл по умолчанию.

АРГУМЕНТЫ

`disabled` : отключается функция или параметр.

`enabled` : включается функция или активируется параметр.

EMAIL

Сканировать файлы электронной почты.

СИНТАКСИС

```
[get] | restore email

set email disabled | enabled
```

ОПЕРАЦИИ

`get` : возвращается текущий параметр/состояние.

`set` : задается значение или состояние.

`restore` : восстанавливаются параметры/объект/файл по умолчанию.

АРГУМЕНТЫ

`disabled` : отключается функция или параметр.

`enabled` : включается функция или активируется параметр.

FILE

Сканировать файлы.

СИНТАКСИС

```
[get] | restore file

set file disabled | enabled
```

ОПЕРАЦИИ

`get` : возвращается текущий параметр/состояние.

`set` : задается значение или состояние.

`restore` : восстанавливаются параметры/объект/файл по умолчанию.

АРГУМЕНТЫ

`disabled` : отключается функция или параметр.

`enabled` : включается функция или активируется параметр.

MEMORY

Сканировать память.

СИНТАКСИС

```
[get] | restore memory

set memory disabled | enabled
```

ОПЕРАЦИИ

`get` : возвращается текущий параметр/состояние.

`set` : задается значение или состояние.

`restore` : восстанавливаются параметры/объект/файл по умолчанию.

АРГУМЕНТЫ

`disabled` : отключается функция или параметр.

`enabled` : включается функция или активируется параметр.

RUNTIME

Сканировать упаковщики.

СИНТАКСИС

```
[get] | restore runtime

set runtime disabled | enabled
```

ОПЕРАЦИИ

`get` : возвращается текущий параметр/состояние.

`set` : задается значение или состояние.

`restore` : восстанавливаются параметры/объект/файл по умолчанию.

АРГУМЕНТЫ

`disabled` : отключается функция или параметр.

`enabled` : включается функция или активируется параметр.

SFX

Сканировать самораспаковывающиеся архивы.

СИНТАКСИС

```
[get] | restore sfx
set sfx disabled | enabled
```

ОПЕРАЦИИ

`get` : возвращается текущий параметр/состояние.

`set` : задается значение или состояние.

`restore` : восстанавливаются параметры/объект/файл по умолчанию.

АРГУМЕНТЫ

`disabled` : отключается функция или параметр.

`enabled` : включается функция или активируется параметр.

4.10.2.54 Контекст «AV WEB OPTIONS»

ADVHEURISTICS

Использовать расширенную эвристику.

СИНТАКСИС

```
[get] | restore advheuristics
set advheuristics disabled | enabled
```

ОПЕРАЦИИ

`get` : возвращается текущий параметр/состояние.

`set` : задается значение или состояние.

`restore` : восстанавливаются параметры/объект/файл по умолчанию.

АРГУМЕНТЫ

`disabled` : отключается функция или параметр.

`enabled` : включается функция или активируется параметр.

ADWARE

Обнаружение рекламных/шпионских/опасных программ.

СИНТАКСИС

```
[get] | restore adware
set adware disabled | enabled
```

ОПЕРАЦИИ

`get` : возвращается текущий параметр/состояние.

`set` : задается значение или состояние.

`restore` : восстанавливаются параметры/объект/файл по умолчанию.

АРГУМЕНТЫ

`disabled` : отключается функция или параметр.

`enabled` : включается функция или активируется параметр.

HEURISTICS

Использовать эвристический анализ.

СИНТАКСИС

```
[get] | restore heuristics

set heuristics disabled | enabled
```

ОПЕРАЦИИ

`get` : возвращается текущий параметр/состояние.

`set` : задается значение или состояние.

`restore` : восстанавливаются параметры/объект/файл по умолчанию.

АРГУМЕНТЫ

`disabled` : отключается функция или параметр.

`enabled` : включается функция или активируется параметр.

SIGNATURES

Использовать сигнатуры.

СИНТАКСИС

```
[get] | restore signatures

set signatures disabled | enabled
```

ОПЕРАЦИИ

`get` : возвращается текущий параметр/состояние.

`set` : задается значение или состояние.

`restore` : восстанавливаются параметры/объект/файл по умолчанию.

АРГУМЕНТЫ

`disabled` : отключается функция или параметр.

`enabled` : включается функция или активируется параметр.

UNSAFE

Обнаружение потенциально опасных приложений.

СИНТАКСИС

```
[get] | restore unsafe

set unsafe disabled | enabled
```

ОПЕРАЦИИ

`get` : возвращается текущий параметр/состояние.

`set` : задается значение или состояние.

`restore` : восстанавливаются параметры/объект/файл по умолчанию.

АРГУМЕНТЫ

`disabled` : отключается функция или параметр.

`enabled` : включается функция или активируется параметр.

UNWANTED

Обнаружение потенциально нежелательных приложений.

СИНТАКСИС

```
[get] | restore unwanted
set unwanted disabled | enabled
```

ОПЕРАЦИИ

`get` : возвращается текущий параметр/состояние.

`set` : задается значение или состояние.

`restore` : восстанавливаются параметры/объект/файл по умолчанию.

АРГУМЕНТЫ

`disabled` : отключается функция или параметр.

`enabled` : включается функция или активируется параметр.

4.10.2.55 Контекст «AV WEB OPTIONS BROWSERS»

ACTIVEMODE

Активный режим для веб-браузеров.

СИНТАКСИС

```
[get] activemode
add | remove activemode <путь>
```

ОПЕРАЦИИ

`get` : возвращается текущий параметр/состояние.

`add` : добавляется элемент.

`remove` : удаляется элемент.

АРГУМЕНТЫ

`путь` : путь приложения.

ПРИМЕЧАНИЕ: Программы, добавленные в этот список, автоматически добавляются в список веб-браузеров.

4.10.2.56 Контекст «AV WEB OTHER»

LOGALL

Регистрировать все объекты.

СИНТАКСИС

```
[get] | restore logall
set logall disabled | enabled
```

ОПЕРАЦИИ

`get` : возвращается текущий параметр/состояние.

`set` : задается значение или состояние.

`restore` : восстанавливаются параметры/объект/файл по умолчанию.

АРГУМЕНТЫ

`disabled` : отключается функция или параметр.

`enabled` : включается функция или активируется параметр.

OPTIMIZE

Оптимизация Smart.

СИНТАКСИС

```
[get] | restore optimize
set optimize disabled | enabled
```

ОПЕРАЦИИ

`get` : возвращается текущий параметр/состояние.

`set` : задается значение или состояние.

`restore` : восстанавливаются параметры/объект/файл по умолчанию.

АРГУМЕНТЫ

`disabled` : отключается функция или параметр.

`enabled` : включается функция или активируется параметр.

4.10.2.57 Контекст «AV WEB PROTOCOL HTTP»

PORTS

Порты, используемые протоколом HTTP.

СИНТАКСИС

```
[get] | restore ports
set ports [<строка>]
```

ОПЕРАЦИИ

`get` : возвращается текущий параметр/состояние.

`set` : задается значение или состояние.

`restore` : восстанавливаются параметры/объект/файл по умолчанию.

АРГУМЕНТЫ

`строка` : номера портов через двоеточие.

USE

Сканировать HTTP.

СИНТАКСИС

```
[get] | restore use
set use disabled | enabled
```

ОПЕРАЦИИ

`get` : возвращается текущий параметр/состояние.

`set` : задается значение или состояние.

`restore` : восстанавливаются параметры/объект/файл по умолчанию.

АРГУМЕНТЫ

`disabled` : отключается функция или параметр.

`enabled` : включается функция или активируется параметр.

4.10.2.58 Контекст «AV WEB PROTOCOL HTTPS»

РЕЖИМ

Режим фильтрации HTTPS.

СИНТАКСИС

```
[get] | restore mode
set mode none | ports | browsers
```

ОПЕРАЦИИ

`get` : возвращается текущий параметр/состояние.

`set` : задается значение или состояние.

`restore` : восстанавливаются параметры/объект/файл по умолчанию.

АРГУМЕНТЫ

`none` : не проверять протоколы.

`ports` : проверять протокол HTTPS на указанных портах.

`browsers` : проверять протокол HTTPS для приложений, помеченных как браузеры, на указанных портах.

PORTS

Порты, используемые протоколом HTTPS.

СИНТАКСИС

```
[get] | restore ports
set ports [<строка>]
```

ОПЕРАЦИИ

`get` : возвращается текущий параметр/состояние.

`set` : задается значение или состояние.

`restore` : восстанавливаются параметры/объект/файл по умолчанию.

АРГУМЕНТЫ

`строка` : номера портов через запятую.

4.10.2.59 Контекст «GENERAL»

CONFIG

Импорт и экспорт параметров.

СИНТАКСИС

```
import | export config <путь>
```

ОПЕРАЦИИ

`import` : выполняется импорт из файла.

`export` : выполняется экспорт в файл.

АРГУМЕНТЫ

`путь` : путь к файлу.

LICENSE

Управление лицензиями.

СИНТАКСИС

```
[get] license
import license <путь>
export license <ИД> <путь>
remove license <ИД>
```

ОПЕРАЦИИ

`get` : возвращается текущий параметр/состояние.

`remove` : удаляется элемент.

`import` : выполняется импорт из файла.

`export` : выполняется экспорт в файл.

АРГУМЕНТЫ

`путь` : путь к файлу лицензии.

`ИД` : идентификатор лицензии.

4.10.2.60 Контекст «GENERAL ACCESS»

ADMIN

Защита параметров правами администратора.

СИНТАКСИС

```
[get] | restore admin
set admin disabled | enabled
```

ОПЕРАЦИИ

`get` : возвращается текущий параметр/состояние.

`set` : задается значение или состояние.

`restore` : восстанавливаются параметры/объект/файл по умолчанию.

АРГУМЕНТЫ

`disabled` : отключается функция или параметр.

`enabled` : включается функция или активируется параметр.

BATCH

Выполнять команды, введенные как аргументы, когда работает eShell.

СИНТАКСИС

```
[get] | restore batch
set batch disabled | <время> | allways
```

ОПЕРАЦИИ

`get` : возвращается текущий параметр/состояние.

`set` : задается значение или состояние.

`restore` : восстанавливаются параметры/объект/файл по умолчанию.

АРГУМЕНТЫ

`disabled` : отключено.

`время` : временной интервал в минутах (от 1 до 1440 минут).

`allways` : всегда.

PASSWORD

Этот пароль используется для защищенных паролем команд. Обычно для выполнения защищенных паролем команд предлагается ввести пароль. Это делается из соображений безопасности. Это применяется к таким командам, которые отключают защиту от вирусов или могут повлиять на функциональность ESET File Security. Пользователю предлагается ввести пароль при каждом выполнении такой команды. Либо же можно задать этот пароль для текущего сеанса eShell, после чего не будет предлагаться ввести пароль. Для получения дополнительных сведений воспользуйтесь этой ссылкой.

Для интерактивного ввода пароля (рекомендуется) следует оставить параметры пустыми. Для сброса пароля введите пустой пароль.

ПУТЬ В КОНТЕКСТЕ

```
general access
```

СИНТАКСИС

```
[get] | restore | set password
```

ОПЕРАЦИИ

`get` : показать пароль.

`set` : установить пароль.

`restore` : сбросить пароль.

ПРИМЕРЫ

`get password` : эта команда позволяет увидеть, сконфигурирован ли пароль (на экран при этом выводятся только символы «звездочка» (*), сам пароль не отображается). Если символов «звездочка» нет, это значит, что пароль не установлен.

`set password` : с помощью этой команды можно задать пароль, просто введя его (если пароль не вводится, защита параметров не используется).

`restore password` : эта команда очищает существующий пароль (защита параметров не будет использоваться).

АНАЛОГ В ГРАФИЧЕСКОМ ИНТЕРФЕЙСЕ ПОЛЬЗОВАТЕЛЯ

Нажмите эту ссылку, чтобы узнать, как данный параметр конфигурируется с помощью графического интерфейса пользователя.

4.10.2.61 Контекст «GENERAL ESHELL»

ALIAS

Управление псевдонимами.

СИНТАКСИС

```
[get] | clear | restore alias
```

```
add alias [.] <псевдоним>=<команда>
```

```
remove alias <псевдоним>
```

```
import | export alias <путь>
```

ОПЕРАЦИИ

`get` : возвращается текущий параметр/состояние.

`add` : добавляется элемент.

`remove` : удаляется элемент.

`import` : выполняется импорт из файла.

`export` : выполняется экспорт в файл.

`restore` : восстанавливаются параметры/объект/файл по умолчанию.

АРГУМЕНТЫ

`.` : создается глобальный псевдоним.

`псевдоним` : новый псевдоним.

`команда` : связанная команда (действительность команды не проверяется).

`псевдоним` : псевдоним, который нужно удалить.

`путь` : путь к файлу.

LISTER

Использовать средство составления списков.

СИНТАКСИС

```
[get] | restore lister
set lister disabled | enabled
```

ОПЕРАЦИИ

`get` : возвращается текущий параметр/состояние.

`set` : задается значение или состояние.

`restore` : восстанавливаются параметры/объект/файл по умолчанию.

АРГУМЕНТЫ

`disabled` : отключается функция или параметр.

`enabled` : включается функция или активируется параметр.

4.10.2.62 Контекст «GENERAL ESHELL COLOR»

ALIAS

Цвет псевдонима.

СИНТАКСИС

```
[get] | restore alias
set alias [black | navy | grass | ltblue | brown | purple | olive | ltgray | gray | blue | green | cyan | re
| magenta | yellow | white]
```

ОПЕРАЦИИ

`get` : возвращается текущий параметр/состояние.

`set` : задается значение или состояние.

`restore` : восстанавливаются параметры/объект/файл по умолчанию.

АРГУМЕНТЫ

`black` : черный.

`navy` : темно-синий.

`grass` : ярко-зеленый.

`ltblue` : светло-синий.

`brown` : коричневый.

`purple` : лиловый.

`olive` : оливковый.

`ltgray` : светло-серый.

`gray` : серый.

`blue` : синий.

`green` : зеленый.

`cyan` : голубой.

`red` : красный.

`magenta` : пурпурный.

`yellow` : желтый.

`white` : белый.

COMMAND

Цвет команд.

СИНТАКСИС

```
[get] | restore command
```

```
set command [black | navy | grass | ltblue | brown | purple | olive | ltgray | gray | blue | green | cyan | red | magenta | yellow | white]
```

ОПЕРАЦИИ

`get` : возвращается текущий параметр/состояние.

`set` : задается значение или состояние.

`restore` : восстанавливаются параметры/объект/файл по умолчанию.

АРГУМЕНТЫ

`black` : черный.

`navy` : темно-синий.

`grass` : ярко-зеленый.

`ltblue` : светло-синий.

`brown` : коричневый.

`purple` : лиловый.

`olive` : оливковый.

`ltgray` : светло-серый.

`gray` : серый.

`blue` : синий.

`green` : зеленый.

`cyan` : голубой.

`red` : красный.

`magenta` : пурпурный.

`yellow` : желтый.

`white` : белый.

CONTEXT

Цвет контекста.

СИНТАКСИС

```
[get] | restore context
```

```
set context [black | navy | grass | ltblue | brown | purple | olive | ltgray | gray | blue | green | cyan | red | magenta | yellow | white]
```

ОПЕРАЦИИ

`get` : возвращается текущий параметр/состояние.

`set` : задается значение или состояние.

`restore` : восстанавливаются параметры/объект/файл по умолчанию.

АРГУМЕНТЫ

`black` : черный.

`navy` : темно-синий.

`grass` : ярко-зеленый.

`ltblue` : светло-синий.

`brown` : коричневый.

`purple` : лиловый.

`olive` : оливковый.

`ltgray` : светло-серый.

`gray` : серый.

`blue` : синий.

`green` : зеленый.

`cyan` : голубой.

`red` : красный.

`magenta` : пурпурный.

`yellow` : желтый.

`white` : белый.

DEFAULT

Основной цвет.

СИНТАКСИС

```
[get] | restore default
```

```
set default [black | navy | grass | ltblue | brown | purple | olive | ltgray | gray | blue | green | cyan | red | magenta | yellow | white]
```

ОПЕРАЦИИ

`get` : возвращается текущий параметр/состояние.

`set` : задается значение или состояние.

`restore` : восстанавливаются параметры/объект/файл по умолчанию.

АРГУМЕНТЫ

`black` : черный.

`navy` : темно-синий.

`grass` : ярко-зеленый.

`ltblue` : светло-синий.

`brown` : коричневый.

`purple` : лиловый.

`olive` : оливковый.

`ltgray` : светло-серый.

`gray` : серый.

`blue` : синий.

`green` : зеленый.

`cyan` : голубой.

`red` : красный.

`magenta` : пурпурный.

`yellow` : желтый.

`white` : белый.

DISABLED

Цвет при отсутствии данных.

СИНТАКСИС

```
[get] | restore disabled
```

```
set disabled [black | navy | grass | ltblue | brown | purple | olive | ltgray | gray | blue | green |
cyan | red | magenta | yellow | white]
```

ОПЕРАЦИИ

`get` : возвращается текущий параметр/состояние.

`set` : задается значение или состояние.

`restore` : восстанавливаются параметры/объект/файл по умолчанию.

АРГУМЕНТЫ

`black` : черный.

`navy` : темно-синий.

`grass` : ярко-зеленый.

`ltblue` : светло-синий.

`brown` : коричневый.

`purple` : лиловый.

`olive` : оливковый.

`ltgray` : светло-серый.

`gray` : серый.

`blue` : синий.

`green` : зеленый.

`cyan` : голубой.

`red` : красный.

`magenta` : пурпурный.

`yellow` : желтый.

`white` : белый.

ERROR

Цвет сообщений об ошибках.

СИНТАКСИС

```
[get] | restore error
```

```
set error [black | navy | grass | ltblue | brown | purple | olive | ltgray | gray | blue | green |
cyan | red | magenta | yellow | white]
```

ОПЕРАЦИИ

`get` : возвращается текущий параметр/состояние.

`set` : задается значение или состояние.

`restore` : восстанавливаются параметры/объект/файл по умолчанию.

АРГУМЕНТЫ

`black` : черный.

`navy` : темно-синий.

`grass` : ярко-зеленый.

`ltblue` : светло-синий.

`brown` : коричневый.

`purple` : лиловый.

`olive` : оливковый.

`ltgray` : светло-серый.

`gray` : серый.

`blue` : синий.

`green` : зеленый.

`cyan` : голубой.

`red` : красный.

`magenta` : пурпурный.

`yellow` : желтый.

`white` : белый.

INTERACTIVE

Цвет интерактивных операций.

СИНТАКСИС

```
[get] | restore interactive
```

```
set interactive [black | navy | grass | ltblue | brown | purple | olive | ltgray | gray | blue |
green | cyan | red | magenta | yellow | white]
```

ОПЕРАЦИИ

`get` : возвращается текущий параметр/состояние.

`set` : задается значение или состояние.

`restore` : восстанавливаются параметры/объект/файл по умолчанию.

АРГУМЕНТЫ

`black` : черный.

`navy` : темно-синий.

`grass` : ярко-зеленый.

`ltblue` : светло-синий.

`brown` : коричневый.

`purple` : лиловый.

`olive` : оливковый.

`ltgray` : светло-серый.

`gray` : серый.

`blue` : синий.

`green` : зеленый.

`cyan` : голубой.

`red` : красный.

`magenta` : пурпурный.

`yellow` : желтый.

`white` : белый.

LIST1

Цвет списка 1.

СИНТАКСИС

```
[get] | restore list1
```

```
set list1 [black | navy | grass | ltblue | brown | purple | olive | ltgray | gray | blue | green |
cyan | red | magenta | yellow | white]
```

ОПЕРАЦИИ

`get` : возвращается текущий параметр/состояние.

`set` : задается значение или состояние.

`restore` : восстанавливаются параметры/объект/файл по умолчанию.

АРГУМЕНТЫ

`black` : черный.

`navy` : темно-синий.

`grass` : ярко-зеленый.

`ltblue` : светло-синий.

`brown` : коричневый.

`purple` : лиловый.

`olive` : оливковый.

`ltgray` : светло-серый.

`gray` : серый.

`blue` : синий.

`green` : зеленый.

`cyan` : голубой.

`red` : красный.

`magenta` : пурпурный.

`yellow` : желтый.

`white` : белый.

LIST2

Цвет списка 2.

СИНТАКСИС

```
[get] | restore list2
```

```
set list2 [black | navy | grass | ltblue | brown | purple | olive | ltgray | gray | blue | green |
cyan | red | magenta | yellow | white]
```

ОПЕРАЦИИ

`get` : возвращается текущий параметр/состояние.

`set` : задается значение или состояние.

`restore` : восстанавливаются параметры/объект/файл по умолчанию.

АРГУМЕНТЫ

`black` : черный.

`navy` : темно-синий.

`grass` : ярко-зеленый.

`ltblue` : светло-синий.

`brown` : коричневый.

`purple` : лиловый.

`olive` : оливковый.

`ltgray` : светло-серый.

`gray` : серый.

`blue` : синий.

`green` : зеленый.

`cyan` : голубой.

`red` : красный.

`magenta` : пурпурный.

`yellow` : желтый.

`white` : белый.

SUCCESS

Цвет состояния ОК.

СИНТАКСИС

```
[get] | restore success
```

```
set success [black | navy | grass | ltblue | brown | purple | olive | ltgray | gray | blue | green |
cyan | red | magenta | yellow | white]
```

ОПЕРАЦИИ

`get` : возвращается текущий параметр/состояние.

`set` : задается значение или состояние.

`restore` : восстанавливаются параметры/объект/файл по умолчанию.

АРГУМЕНТЫ

`black` : черный.

`navy` : темно-синий.

`grass` : ярко-зеленый.

`ltblue` : светло-синий.

`brown` : коричневый.

`purple` : лиловый.

`olive` : оливковый.

`ltgray` : светло-серый.

`gray` : серый.

`blue` : синий.

`green` : зеленый.

`cyan` : голубой.

`red` : красный.

`magenta` : пурпурный.

`yellow` : желтый.

`white` : белый.

WARNING

Цвет предупреждающих сообщений.

СИНТАКСИС

```
[get] | restore warning
```

```
set warning [black | navy | grass | ltblue | brown | purple | olive | ltgray | gray | blue | green | cyan | red | magenta | yellow | white]
```

ОПЕРАЦИИ

`get` : возвращается текущий параметр/состояние.

`set` : задается значение или состояние.

`restore` : восстанавливаются параметры/объект/файл по умолчанию.

АРГУМЕНТЫ

`black` : черный.

`navy` : темно-синий.

`grass` : ярко-зеленый.

`ltblue` : светло-синий.

`brown` : коричневый.

`purple` : лиловый.

`olive` : оливковый.

`ltgray` : светло-серый.

`gray` : серый.

`blue` : синий.

`green` : зеленый.

`cyan` : голубой.

`red` : красный.

`magenta` : пурпурный.

`yellow` : желтый.

`white` : белый.

4.10.2.63 Контекст «GENERAL ESHELL OUTPUT»

UTF8

Результат в кодировке UTF8.

СИНТАКСИС

```
[get] | restore utf8

set utf8 disabled | enabled
```

ОПЕРАЦИИ

`get` : возвращается текущий параметр/состояние.

`set` : задается значение или состояние.

`restore` : восстанавливаются параметры/объект/файл по умолчанию.

АРГУМЕНТЫ

`disabled` : отключается функция или параметр.

`enabled` : включается функция или активируется параметр.

ПРИМЕЧАНИЕ: Для корректного вывода на экран в командной строке должен использоваться шрифт TrueType, такой как Lucida Console.

4.10.2.64 Контекст «GENERAL ESHELL STARTUP»

LOADCOMMANDS

Загружать все команды при запуске.

СИНТАКСИС

```
[get] | restore loadcommands

set loadcommands disabled | enabled
```

ОПЕРАЦИИ

`get` : возвращается текущий параметр/состояние.

`set` : задается значение или состояние.

`restore` : восстанавливаются параметры/объект/файл по умолчанию.

АРГУМЕНТЫ

`disabled` : отключается функция или параметр.

`enabled` : включается функция или активируется параметр.

STATUS

Отображать состояние защиты при запуске.

СИНТАКСИС

```
[get] | restore status

set status disabled | enabled
```

ОПЕРАЦИИ

`get` : возвращается текущий параметр/состояние.

`set` : задается значение или состояние.

`restore` : восстанавливаются параметры/объект/файл по умолчанию.

АРГУМЕНТЫ

`disabled` : отключается функция или параметр.

`enabled` : включается функция или активируется параметр.

4.10.2.65 Контекст «GENERAL ESHELL VIEW»

CMDHELP

Выводить на экран справку при сбое выполнения команд.

СИНТАКСИС

```
[get] | restore cmdhelp
set cmdhelp disabled | enabled
```

ОПЕРАЦИИ

`get` : возвращается текущий параметр/состояние.

`set` : задается значение или состояние.

`restore` : восстанавливаются параметры/объект/файл по умолчанию.

АРГУМЕНТЫ

`disabled` : отключается функция или параметр.

`enabled` : включается функция или активируется параметр.

COLORS

Использовать цвета.

СИНТАКСИС

```
[get] | restore colors
set colors disabled | enabled
```

ОПЕРАЦИИ

`get` : возвращается текущий параметр/состояние.

`set` : задается значение или состояние.

`restore` : восстанавливаются параметры/объект/файл по умолчанию.

АРГУМЕНТЫ

`disabled` : отключается функция или параметр.

`enabled` : включается функция или активируется параметр.

FITWIDTH

Обрезать текст по ширине.

СИНТАКСИС

```
[get] | restore fitwidth
set fitwidth disabled | enabled
```

ОПЕРАЦИИ

`get` : возвращается текущий параметр/состояние.

`set` : задается значение или состояние.

`restore` : восстанавливаются параметры/объект/файл по умолчанию.

АРГУМЕНТЫ

`disabled` : отключается функция или параметр.

`enabled` : включается функция или активируется параметр.

GLOBAL

Показать глобальные команды.

СИНТАКСИС

```
[get] | restore global

set global disabled | enabled
```

ОПЕРАЦИИ

`get` : возвращается текущий параметр/состояние.

`set` : задается значение или состояние.

`restore` : восстанавливаются параметры/объект/файл по умолчанию.

АРГУМЕНТЫ

`disabled` : отключается функция или параметр.

`enabled` : включается функция или активируется параметр.

HIDDEN

Показать скрытые команды.

СИНТАКСИС

```
[get] | restore hidden

set hidden disabled | enabled
```

ОПЕРАЦИИ

`get` : возвращается текущий параметр/состояние.

`set` : задается значение или состояние.

`restore` : восстанавливаются параметры/объект/файл по умолчанию.

АРГУМЕНТЫ

`disabled` : отключается функция или параметр.

`enabled` : включается функция или активируется параметр.

OPERATIONS

Показать операции в списке команд.

СИНТАКСИС

```
[get] | restore operations

set operations disabled | enabled
```

ОПЕРАЦИИ

`get` : возвращается текущий параметр/состояние.

`set` : задается значение или состояние.

`restore` : восстанавливаются параметры/объект/файл по умолчанию.

АРГУМЕНТЫ

`disabled` : отключается функция или параметр.

`enabled` : включается функция или активируется параметр.

SHORTLIST

Показать краткий список команд при изменении контекста.

СИНТАКСИС

```
[get] | restore shortlist
```

```
set shortlist disabled | enabled
```

ОПЕРАЦИИ

`get` : возвращается текущий параметр/состояние.

`set` : задается значение или состояние.

`restore` : восстанавливаются параметры/объект/файл по умолчанию.

АРГУМЕНТЫ

`disabled` : отключается функция или параметр.

`enabled` : включается функция или активируется параметр.

SYNTAXHINT

Показывать подсказки по синтаксису команд.

СИНТАКСИС

```
[get] | restore syntaxhint
```

```
set syntaxhint disabled | enabled
```

ОПЕРАЦИИ

`get` : возвращается текущий параметр/состояние.

`set` : задается значение или состояние.

`restore` : восстанавливаются параметры/объект/файл по умолчанию.

АРГУМЕНТЫ

`disabled` : отключается функция или параметр.

`enabled` : включается функция или активируется параметр.

VALUESONLY

Отображать только значения без описания.

СИНТАКСИС

```
[get] | restore valuesonly
```

```
set valuesonly disabled | enabled
```

ОПЕРАЦИИ

`get` : возвращается текущий параметр/состояние.

`set` : задается значение или состояние.

`restore` : восстанавливаются параметры/объект/файл по умолчанию.

АРГУМЕНТЫ

`disabled` : отключается функция или параметр.

`enabled` : включается функция или активируется параметр.

4.10.2.66 Контекст «GENERAL PERFORMANCE»

SCANNERS

Количество выполняемых процессов сканирования.

СИНТАКСИС

```
[get] | restore scanners
set scanners <число>
```

ОПЕРАЦИИ

`get` : возвращается текущий параметр/состояние.

`set` : задается значение или состояние.

`restore` : восстанавливаются параметры/объект/файл по умолчанию.

АРГУМЕНТЫ

`число` : количество (1–20).

4.10.2.67 Контекст «GENERAL PROXY»

ADDRESS

Адрес прокси-сервера.

СИНТАКСИС

```
[get] | restore address
set address [<строка>]
```

ОПЕРАЦИИ

`get` : возвращается текущий параметр/состояние.

`set` : задается значение или состояние.

`restore` : восстанавливаются параметры/объект/файл по умолчанию.

АРГУМЕНТЫ

`строка` : адрес.

DETECT

Обнаружение конфигурации прокси-сервера.

СИНТАКСИС

```
detect
```

LOGIN

Имя для входа в систему.

СИНТАКСИС

```
[get] | restore login
set login [<строка>]
```

ОПЕРАЦИИ

`get` : возвращается текущий параметр/состояние.

`set` : задается значение или состояние.

`restore` : восстанавливаются параметры/объект/файл по умолчанию.

АРГУМЕНТЫ

`строка` : имя.

PASSWORD

Пароль для доступа к прокси-серверу.

СИНТАКСИС

```
[get] | restore password

set password [plain <пароль>]
```

ОПЕРАЦИИ

`get` : возвращается текущий параметр/состояние.

`set` : задается значение или состояние.

`restore` : восстанавливаются параметры/объект/файл по умолчанию.

АРГУМЕНТЫ

`plain` : переход ко вводу пароля как параметра.

`password` : пароль.

PORT

Порт

СИНТАКСИС

```
[get] | restore port

set port <число>
```

ОПЕРАЦИИ

`get` : возвращается текущий параметр/состояние.

`set` : задается значение или состояние.

`restore` : восстанавливаются параметры/объект/файл по умолчанию.

АРГУМЕНТЫ

`число` : номер порта.

USE

Использовать прокси-сервер.

СИНТАКСИС

```
[get] | restore use

set use disabled | enabled
```

ОПЕРАЦИИ

`get` : возвращается текущий параметр/состояние.

`set` : задается значение или состояние.

`restore` : восстанавливаются параметры/объект/файл по умолчанию.

АРГУМЕНТЫ

`disabled` : отключается функция или параметр.

`enabled` : включается функция или активируется параметр.

4.10.2.68 Контекст «GENERAL QUARANTINE RESCAN»

UPDATE

Повторно сканировать файлы в папке карантина после обновлений.

СИНТАКСИС

```
[get] | restore update

set update disabled | enabled
```

ОПЕРАЦИИ

`get` : возвращается текущий параметр/состояние.

`set` : задается значение или состояние.

restore: восстанавливаются параметры/объект/файл по умолчанию.

АРГУМЕНТЫ

`disabled` : отключается функция или параметр.

`enabled` : включается функция или активируется параметр.

4.10.2.69 Контекст «GENERAL REMOTE»

INTERVAL

Интервал подключения (в минутах).

СИНТАКСИС

```
[get] | restore interval

set interval <число>
```

ОПЕРАЦИИ

`get` : возвращается текущий параметр/состояние.

`set` : задается значение или состояние.

`restore` : восстанавливаются параметры/объект/файл по умолчанию.

АРГУМЕНТЫ

`число` : время в минутах (1–1440).

USE

Подключение к ERA Server.

СИНТАКСИС

```
[get] | restore use

set use disabled | enabled
```

ОПЕРАЦИИ

`get` : возвращается текущий параметр/состояние.

`set` : задается значение или состояние.

`restore` : восстанавливаются параметры/объект/файл по умолчанию.

АРГУМЕНТЫ

`disabled` : отключается функция или параметр.

`enabled` : включается функция или активируется параметр.

4.10.2.70 Контекст «GENERAL REMOTE SERVER PRIMARY»

ADDRESS

Адрес ERA Server.

СИНТАКСИС

```
[get] | restore address

set address [<строка>]
```

ОПЕРАЦИИ

`get` : возвращается текущий параметр/состояние.

`set` : задается значение или состояние.

`restore` : восстанавливаются параметры/объект/файл по умолчанию.

АРГУМЕНТЫ

`строка` : адрес.

ENCRYPT

Блокировать незашифрованные подключения.

СИНТАКСИС

```
[get] | restore encrypt

set encrypt disabled | enabled
```

ОПЕРАЦИИ

`get` : возвращается текущий параметр/состояние.

`set` : задается значение или состояние.

`restore` : восстанавливаются параметры/объект/файл по умолчанию.

АРГУМЕНТЫ

`disabled` : отключается функция или параметр.

`enabled` : включается функция или активируется параметр.

PASSWORD

Пароль для доступа к ERA Server.

СИНТАКСИС

```
[get] | restore password

set password [plain <пароль>]
```

ОПЕРАЦИИ

`get` : возвращается текущий параметр/состояние.

`set` : задается значение или состояние.

`restore` : восстанавливаются параметры/объект/файл по умолчанию.

АРГУМЕНТЫ

`plain` : переход ко вводу пароля как параметра.

`password` : пароль.

PORT

Порт ERA Server.

СИНТАКСИС

[get] | restore port

set port <число>

ОПЕРАЦИИ

get : возвращается текущий параметр/состояние.

set : задается значение или состояние.

restore : восстанавливаются параметры/объект/файл по умолчанию.

АРГУМЕНТЫ

число : номер порта.

4.10.2.71 Контекст «GENERAL REMOTE SERVER SECONDARY»

ADDRESS

Адрес ERA Server.

СИНТАКСИС

[get] | restore address

set address [<строка>]

ОПЕРАЦИИ

get : возвращается текущий параметр/состояние.

set : задается значение или состояние.

restore : восстанавливаются параметры/объект/файл по умолчанию.

АРГУМЕНТЫ

строка : адрес.

ENCRYPT

Блокировать незашифрованные подключения.

СИНТАКСИС

[get] | restore encrypt

set encrypt disabled | enabled

ОПЕРАЦИИ

get : возвращается текущий параметр/состояние.

set : задается значение или состояние.

restore : восстанавливаются параметры/объект/файл по умолчанию.

АРГУМЕНТЫ

disabled : отключается функция или параметр.

enabled : включается функция или активируется параметр.

PASSWORD

Пароль для доступа к ERA Server.

СИНТАКСИС

[get] | restore password

set password [plain <пароль>]

ОПЕРАЦИИ

get : возвращается текущий параметр/состояние.

`set` : задается значение или состояние.

`restore` : восстанавливаются параметры/объект/файл по умолчанию.

АРГУМЕНТЫ

`plain` : переход ко вводу пароля как параметра.

`password` : пароль.

PORT

Порт ERA Server.

СИНТАКСИС

```
[get] | restore port

set port <число>
```

ОПЕРАЦИИ

`get` : возвращается текущий параметр/состояние.

`set` : задается значение или состояние.

`restore` : восстанавливаются параметры/объект/файл по умолчанию.

АРГУМЕНТЫ

`число` : номер порта.

4.10.2.72 Контекст «GENERAL TS.NET»

EXCLUSION

Исключить из отправки.

СИНТАКСИС

```
[get] | restore exclusion

add | remove exclusion <исключение>
```

ОПЕРАЦИИ

`get` : возвращается текущий параметр/состояние.

`add` : добавляется элемент.

`remove` : удаляется элемент.

`restore` : восстанавливаются параметры/объект/файл по умолчанию.

АРГУМЕНТЫ

`exclusion` : расширение.

FROM

Адрес электронной почты для связи.

СИНТАКСИС

```
[get] | restore from

set from [<строка>]
```

ОПЕРАЦИИ

`get` : возвращается текущий параметр/состояние.

`set` : задается значение или состояние.

`restore` : восстанавливаются параметры/объект/файл по умолчанию.

АРГУМЕНТЫ

`строка` : адрес электронной почты.

LOGING

Создание журналов.

СИНТАКСИС

[get] | restore loging

set loging disabled | enabled

ОПЕРАЦИИ

get: возвращается текущий параметр/состояние.

set: задается значение или состояние.

restore: восстанавливаются параметры/объект/файл по умолчанию.

АРГУМЕНТЫ

disabled: отключается функция или параметр.

enabled: включается функция или активируется параметр.

SENDING

Отправка подозрительных файлов.

СИНТАКСИС

```
[get] | restore sending
set sending none | ask | auto
```

ОПЕРАЦИИ

`get` : возвращается текущий параметр/состояние.

`set` : задается значение или состояние.

`restore` : восстанавливаются параметры/объект/файл по умолчанию.

АРГУМЕНТЫ

`none` : не отправлять.

`ask` : запрашивать подтверждение перед отправкой на анализ.

`auto` : отправлять на анализ без подтверждения.

VIA

Средство отправки.

СИНТАКСИС

```
[get] | restore via
set via auto | ra | direct
```

ОПЕРАЦИИ

`get` : возвращается текущий параметр/состояние.

`set` : задается значение или состояние.

`restore` : восстанавливаются параметры/объект/файл по умолчанию.

АРГУМЕНТЫ

`auto` : средствами удаленного администрирования или непосредственно в ESET.

`ra` : средствами удаленного администрирования.

`direct` : непосредственно в ESET.

WHEN

Момент отправки подозрительных файлов.

СИНТАКСИС

```
[get] | restore when

set when asap | update
```

ОПЕРАЦИИ

`get` : возвращается текущий параметр/состояние.

`set` : задается значение или состояние.

`restore` : восстанавливаются параметры/объект/файл по умолчанию.

АРГУМЕНТЫ

`asap` : как можно скорее.

`update` : в процессе обновления.

4.10.2.73 Контекст «GENERAL TS.NET STATISTICS»

SENDING

Отправка статистической информации.

СИНТАКСИС

```
[get] | restore sending

set sending disabled | enabled
```

ОПЕРАЦИИ

`get` : возвращается текущий параметр/состояние.

`set` : задается значение или состояние.

`restore` : восстанавливаются параметры/объект/файл по умолчанию.

АРГУМЕНТЫ

`disabled` : отключается функция или параметр.

`enabled` : включается функция или активируется параметр.

WHEN

Передача анонимной статистической информации.

СИНТАКСИС

```
[get] | restore when

set when asap | update
```

ОПЕРАЦИИ

`get` : возвращается текущий параметр/состояние.

`set` : задается значение или состояние.

`restore` : восстанавливаются параметры/объект/файл по умолчанию.

АРГУМЕНТЫ

`asap` : как можно скорее.

`update` : в процессе обновления.

4.10.2.74 Контекст «SCANNER»

CLEANLEVEL

Уровень очистки.

СИНТАКСИС

```
[get] | restore cleanlevel
set cleanlevel none | normal | strict
```

ОПЕРАЦИИ

`get` : возвращается текущий параметр/состояние.

`set` : задается значение или состояние.

`restore` : восстанавливаются параметры/объект/файл по умолчанию.

АРГУМЕНТЫ

`none` : без очистки.

`normal` : стандартная очистка.

`strict` : тщательная очистка.

EXTENSIONS

Сканируемые/исключенные расширения.

СИНТАКСИС

```
[get] | restore extensions
add | remove extensions <расширение> | /all | /extless
```

ОПЕРАЦИИ

`get` : возвращается текущий параметр/состояние.

`add` : добавляется элемент.

`remove` : удаляется элемент.

`restore` : восстанавливаются параметры/объект/файл по умолчанию.

АРГУМЕНТЫ

`extension` : расширение.

`all` : все файлы.

`extless` : файлы без расширений.

ПРОФИЛЬ

Управление профилями сканирования компьютера.

СИНТАКСИС

```
[get] profile
select | remove profile <имя>
add profile new: <имя> [copyfrom: <имя>]
```

ОПЕРАЦИИ

`get` : возвращается текущий параметр/состояние.

`select` : выбирается элемент.

`add` : добавляется элемент.

`remove` : удаляется элемент.

АРГУМЕНТЫ

`имя` : имя профиля.

`new` : новый профиль.

`copyfrom` : копировать настройки профиля.

ПРИМЕЧАНИЕ: Другие команды контекста ссылаются на активный профиль (помеченный символом «x»). Для выбора активного профиля воспользуйтесь командой `select scanner profile <имя профиля>`.

SCAN

Сканирование компьютера.

СИНТАКСИС

```
[get] | clear scan

start scan [readonly]

pause | resume | stop scan <ИД> | all
```

ОПЕРАЦИИ

`get` : показываются выполняемые и завершенные процессы сканирования.

`start` : запускается сканирование компьютера для выбранного профиля.

`stop` : останавливается сканирование.

`resume` : продолжается приостановленное сканирование.

`pause` : приостанавливается сканирование.

`clear` : удаляются завершенные процессы сканирования из списка.

АРГУМЕНТЫ

`readonly` : сканировать без очистки.

`ИД` : идентификатор сканирования для выполнения команды.

`all` : выполнить команду для всех процессов сканирования.

TARGET

Объекты сканирования для активного профиля.

СИНТАКСИС

```
[get] target

add | remove target <путь>
```

ОПЕРАЦИИ

`get` : возвращается текущий параметр/состояние.

`add` : добавляется элемент.

`remove` : удаляется элемент.

АРГУМЕНТЫ

`путь` : путь/объект сканирования.

ПРИМЕЧАНИЕ: Для сканирования загрузочных секторов введите `X: \${Boot}` где «X» — это имя сканируемого диска.

4.10.2.75 Контекст «SCANNER LIMITS ARCHIVE»

LEVEL

Уровень вложенности архивов.

СИНТАКСИС

```
[get] | restore level

set level <число>
```

ОПЕРАЦИИ

`get` : возвращается текущий параметр/состояние.

`set` : задается значение или состояние.

`restore` : восстанавливаются параметры/объект/файл по умолчанию.

АРГУМЕНТЫ

`число` : уровень от 1 до 20 или 0 для выбора параметров по умолчанию.

SIZE

Максимальный размер файла в архиве в килобайтах.

СИНТАКСИС

```
[get] | restore size

set size <число>
```

ОПЕРАЦИИ

`get` : возвращается текущий параметр/состояние.

`set` : задается значение или состояние.

`restore` : восстанавливаются параметры/объект/файл по умолчанию.

АРГУМЕНТЫ

`число` : размер в Кб или 0 для выбора параметров по умолчанию.

4.10.2.76 Контекст «SCANNER LIMITS OBJECTS»

SIZE

Максимальный размер архива (Кб).

СИНТАКСИС

```
[get] | restore size

set size <число>
```

ОПЕРАЦИИ

`get` : возвращается текущий параметр/состояние.

`set` : задается значение или состояние.

`restore` : восстанавливаются параметры/объект/файл по умолчанию.

АРГУМЕНТЫ

`число` : размер в Кб или 0 для выбора параметров по умолчанию.

TIMEOUT

Максимальное время сканирования архивов в секундах.

СИНТАКСИС

```
[get] | restore timeout

set timeout <число>
```

ОПЕРАЦИИ

`get` : возвращается текущий параметр/состояние.

`set` : задается значение или состояние.

`restore` : восстанавливаются параметры/объект/файл по умолчанию.

АРГУМЕНТЫ

`число` : время в секундах или 0 для выбора параметров по умолчанию.

4.10.2.77 Контекст «SCANNER OBJECTS»

ARCHIVE

Сканировать архивы.

СИНТАКСИС

```
[get] | restore archive

set archive disabled | enabled
```

ОПЕРАЦИИ

`get` : возвращается текущий параметр/состояние.

`set` : задается значение или состояние.

`restore` : восстанавливаются параметры/объект/файл по умолчанию.

АРГУМЕНТЫ

`disabled` : отключается функция или параметр.

`enabled` : включается функция или активируется параметр.

BOOT

Сканировать загрузочные секторы.

СИНТАКСИС

```
[get] | restore boot

set boot disabled | enabled
```

ОПЕРАЦИИ

`get` : возвращается текущий параметр/состояние.

`set` : задается значение или состояние.

`restore` : восстанавливаются параметры/объект/файл по умолчанию.

АРГУМЕНТЫ

`disabled` : отключается функция или параметр.

`enabled` : включается функция или активируется параметр.

EMAIL

Сканировать файлы электронной почты.

СИНТАКСИС

```
[get] | restore email

set email disabled | enabled
```

ОПЕРАЦИИ

`get` : возвращается текущий параметр/состояние.

`set` : задается значение или состояние.

`restore` : восстанавливаются параметры/объект/файл по умолчанию.

АРГУМЕНТЫ

`disabled` : отключается функция или параметр.

`enabled` : включается функция или активируется параметр.

FILE

Сканировать файлы.

СИНТАКСИС

```
[get] | restore file

set file disabled | enabled
```

ОПЕРАЦИИ

`get` : возвращается текущий параметр/состояние.

`set` : задается значение или состояние.

`restore` : восстанавливаются параметры/объект/файл по умолчанию.

АРГУМЕНТЫ

`disabled` : отключается функция или параметр.

`enabled` : включается функция или активируется параметр.

MEMORY

Сканировать память.

СИНТАКСИС

```
[get] | restore memory

set memory disabled | enabled
```

ОПЕРАЦИИ

`get` : возвращается текущий параметр/состояние.

`set` : задается значение или состояние.

`restore` : восстанавливаются параметры/объект/файл по умолчанию.

АРГУМЕНТЫ

`disabled` : отключается функция или параметр.

`enabled` : включается функция или активируется параметр.

RUNTIME

Сканировать упаковщики.

СИНТАКСИС

```
[get] | restore runtime

set runtime disabled | enabled
```

ОПЕРАЦИИ

`get` : возвращается текущий параметр/состояние.

`set` : задается значение или состояние.

`restore` : восстанавливаются параметры/объект/файл по умолчанию.

АРГУМЕНТЫ

`disabled` : отключается функция или параметр.

`enabled` : включается функция или активируется параметр.

SFX

Сканировать самораспаковывающиеся архивы.

СИНТАКСИС

```
[get] | restore sfx
set sfx disabled | enabled
```

ОПЕРАЦИИ

`get` : возвращается текущий параметр/состояние.

`set` : задается значение или состояние.

`restore` : восстанавливаются параметры/объект/файл по умолчанию.

АРГУМЕНТЫ

`disabled` : отключается функция или параметр.

`enabled` : включается функция или активируется параметр.

4.10.2.78 Контекст «SCANNER OPTIONS»

ADVHEURISTICS

Использовать расширенную эвристику.

СИНТАКСИС

```
[get] | restore advheuristics
set advheuristics disabled | enabled
```

ОПЕРАЦИИ

`get` : возвращается текущий параметр/состояние.

`set` : задается значение или состояние.

`restore` : восстанавливаются параметры/объект/файл по умолчанию.

АРГУМЕНТЫ

`disabled` : отключается функция или параметр.

`enabled` : включается функция или активируется параметр.

ADWARE

Обнаружение рекламных/шпионских/опасных программ.

СИНТАКСИС

```
[get] | restore adware
set adware disabled | enabled
```

ОПЕРАЦИИ

`get` : возвращается текущий параметр/состояние.

`set` : задается значение или состояние.

`restore` : восстанавливаются параметры/объект/файл по умолчанию.

АРГУМЕНТЫ

`disabled` : отключается функция или параметр.

`enabled` : включается функция или активируется параметр.

HEURISTICS

Использовать эвристический анализ.

СИНТАКСИС

```
[get] | restore heuristics

set heuristics disabled | enabled
```

ОПЕРАЦИИ

`get` : возвращается текущий параметр/состояние.

`set` : задается значение или состояние.

`restore` : восстанавливаются параметры/объект/файл по умолчанию.

АРГУМЕНТЫ

`disabled` : отключается функция или параметр.

`enabled` : включается функция или активируется параметр.

SIGNATURES

Использовать сигнатуры.

СИНТАКСИС

```
[get] | restore signatures

set signatures disabled | enabled
```

ОПЕРАЦИИ

`get` : возвращается текущий параметр/состояние.

`set` : задается значение или состояние.

`restore` : восстанавливаются параметры/объект/файл по умолчанию.

АРГУМЕНТЫ

`disabled` : отключается функция или параметр.

`enabled` : включается функция или активируется параметр.

UNSAFE

Обнаружение потенциально опасных приложений.

СИНТАКСИС

```
[get] | restore unsafe

set unsafe disabled | enabled
```

ОПЕРАЦИИ

`get` : возвращается текущий параметр/состояние.

`set` : задается значение или состояние.

`restore` : восстанавливаются параметры/объект/файл по умолчанию.

АРГУМЕНТЫ

`disabled` : отключается функция или параметр.

`enabled` : включается функция или активируется параметр.

UNWANTED

Обнаружение потенциально нежелательных приложений.

СИНТАКСИС

```
[get] | restore unwanted

set unwanted disabled | enabled
```

ОПЕРАЦИИ

`get` : возвращается текущий параметр/состояние.

`set` : задается значение или состояние.

`restore` : восстанавливаются параметры/объект/файл по умолчанию.

АРГУМЕНТЫ

`disabled` : отключается функция или параметр.

`enabled` : включается функция или активируется параметр.

4.10.2.79 Контекст «SCANNER OTHER»

ADS

Сканировать альтернативные потоки данных (ADS).

СИНТАКСИС

```
[get] | restore ads

set ads disabled | enabled
```

ОПЕРАЦИИ

`get` : возвращается текущий параметр/состояние.

`set` : задается значение или состояние.

`restore` : восстанавливаются параметры/объект/файл по умолчанию.

АРГУМЕНТЫ

`disabled` : отключается функция или параметр.

`enabled` : включается функция или активируется параметр.

LOGALL

Регистрировать все объекты.

СИНТАКСИС

```
[get] | restore logall

set logall disabled | enabled
```

ОПЕРАЦИИ

`get` : возвращается текущий параметр/состояние.

`set` : задается значение или состояние.

`restore` : восстанавливаются параметры/объект/файл по умолчанию.

АРГУМЕНТЫ

`disabled` : отключается функция или параметр.

`enabled` : включается функция или активируется параметр.

LOWPRIORITY

Запустить фоновое сканирование с низким приоритетом.

СИНТАКСИС

```
[get] | restore lowpriority
```

```
set lowpriority disabled | enabled
```

ОПЕРАЦИИ

`get` : возвращается текущий параметр/состояние.

`set` : задается значение или состояние.

`restore` : восстанавливаются параметры/объект/файл по умолчанию.

АРГУМЕНТЫ

`disabled` : отключается функция или параметр.

`enabled` : включается функция или активируется параметр.

OPTIMIZE

Оптимизация Smart.

СИНТАКСИС

```
[get] | restore optimize
```

```
set optimize disabled | enabled
```

ОПЕРАЦИИ

`get` : возвращается текущий параметр/состояние.

`set` : задается значение или состояние.

`restore` : восстанавливаются параметры/объект/файл по умолчанию.

АРГУМЕНТЫ

`disabled` : отключается функция или параметр.

`enabled` : включается функция или активируется параметр.

PRESERVETIME

Сохранить отметку о времени последнего доступа.

СИНТАКСИС

```
[get] | restore preservetime
```

```
set preservetime disabled | enabled
```

ОПЕРАЦИИ

`get` : возвращается текущий параметр/состояние.

`set` : задается значение или состояние.

`restore` : восстанавливаются параметры/объект/файл по умолчанию.

АРГУМЕНТЫ

`disabled` : отключается функция или параметр.

`enabled` : включается функция или активируется параметр.

SCROLL

Прокрутить журнал сканирования.

СИНТАКСИС

```
[get] | restore scroll
```

```
set scroll disabled | enabled
```

ОПЕРАЦИИ

`get` : возвращается текущий параметр/состояние.

`set` : задается значение или состояние.

`restore` : восстанавливаются параметры/объект/файл по умолчанию.

АРГУМЕНТЫ

`disabled` : отключается функция или параметр.

`enabled` : включается функция или активируется параметр.

4.10.2.80 Контекст «SERVER»

AUTOEXCLUSIONS

Управление автоматическими исключениями.

СИНТАКСИС

```
[get] | restore autoexclusions
```

```
select autoexclusions <сервер>
```

ОПЕРАЦИИ

`get` : возвращается текущий параметр/состояние.

`select` : выбирается элемент.

`restore` : восстанавливаются параметры/объект/файл по умолчанию.

АРГУМЕНТЫ

`server` : имя сервера.

4.10.2.81 Контекст «TOOLS»

QUARANTINE

Карантин.

СИНТАКСИС

```
[get] quarantine
```

```
add quarantine <путь>
```

```
send | remove | restore quarantine <ИД>
```

ОПЕРАЦИИ

`get` : возвращается текущий параметр/состояние.

`add` : добавляется элемент.

`remove` : удаляется элемент.

`restore` : восстанавливаются параметры/объект/файл по умолчанию.

`send` : отправляется элемент или файл.

АРГУМЕНТЫ

`путь` : путь к файлу.

`ИД` : идентификатор файла на карантине.

STATISTICS

Статистика.

СИНТАКСИС

```
[get] | clear statistics
```

ОПЕРАЦИИ

`get` : показать статистику.

`clear` : сброс статистики.

SYSINSPECTOR

SysInspector.

СИНТАКСИС

```
[get] sysinspector

add | remove sysinspector <имя>

export sysinspector <имя> to:<путь>
```

ОПЕРАЦИИ

`get` : возвращается текущий параметр/состояние.

`add` : добавляется элемент.

`remove` : удаляется элемент.

`export` : выполняется экспорт в файл.

АРГУМЕНТЫ

`имя` : комментарий.

`путь` : имя файла (.zip или .xml).

4.10.2.82 Контекст «TOOLS ACTIVITY»

FILESYSTEM

Файловая система.

СИНТАКСИС

```
[get] filesystem [<количество>] [seconds | minutes | hours [<год>-<месяц>]]
```

NETWORK

Сетевая активность.

СИНТАКСИС

```
[get] network [<количество>] [seconds | minutes | hours [<год>-<месяц>]]
```

АРГУМЕНТЫ

`количество` : количество записей для отображения.

`seconds` : выборка за 1 секунду.

`minutes` : выборка за 1 минуту.

`hours` : выборка за 1 час.

`год` : показать записи за год.

`месяц` : показать записи за месяц.

4.10.2.83 Контекст «TOOLS LOG»

DETECTIONS

Эта команда полезна, когда нужно просмотреть информацию об обнаруженных заражениях.

ПУТЬ В КОНТЕКСТЕ

`root`

СИНТАКСИС

`[get] detections [count <число>] [from <год>-<месяц>-<день> <часы>:<минуты>:<секунды>] [to <год>-<месяц>-<де`

`clear detections`

ОПЕРАЦИИ

`get` : возвращается текущий параметр/состояние.

`clear` : удаляются все элементы или файлы.

АРГУМЕНТЫ

`количество` : показывается выбранное количество записей.

`число` : количество записей.

`from` : показываются записи, начиная с указанного времени.

`год` : год.

`месяц` : месяц.

`день` : день.

`часы` : часы.

`минуты` : минуты.

`секунды` : секунды.

`to` : показываются записи до выбранного времени.

ПСЕВДОНИМЫ

`virlog`

ПРИМЕРЫ

`get detections from 2011-04-14 01:30:00` : на экран выводятся заражения, обнаруженные после 01:30:00 14 апреля 2011 года (при задании даты также нужно указывать время, чтобы эта команда работала корректно).

`clear detections` : очищается журнал полностью.

EVENTS

Эта команда полезна, когда нужно просмотреть информацию о различных событиях.

СИНТАКСИС

`[get] events [count <число>] [from <год>-<месяц>-<день> <часы>:<минуты>:<секунды>] [to <год>-<месяц>-<день> <часы>:<минуты>:<секунды>]`

`clear events`

ОПЕРАЦИИ

`get` : возвращается текущий параметр/состояние.

`clear` : удаляются все элементы или файлы.

АРГУМЕНТЫ

`количество` : показывается выбранное количество записей.

`число` : количество записей.

`from` : показываются записи, начиная с указанного времени.

`год` : год.

`месяц` : месяц.

`день` : день.

`часы` : часы.

`минуты` : минуты.

`секунды` : секунды.

`to` : показываются записи до выбранного времени.

ПСЕВДОНИМЫ

`warnlog`

ПРИМЕРЫ

`get events from 2011-04-14 01:30:00` : на экран выводятся все события, произошедшие после 01:30:00 14 апреля 2011 года (при задании даты также нужно указывать время, чтобы эта команда работала корректно).

`clear events` : очищается журнал полностью.

FILTER

Минимальная детализация отображаемых событий.

СИНТАКСИС

```
[get] | restore filter
```

```
set filter [[none] [critical] [errors] [warnings] [informative] [diagnostic] [all]] [smart]
```

ОПЕРАЦИИ

`get` : возвращается текущий параметр/состояние.

`set` : задается значение или состояние.

`restore` : восстанавливаются параметры/объект/файл по умолчанию.

АРГУМЕНТЫ

`none` : никакие записи.

`critical` : критические ошибки.

`errors` : ошибки.

`warnings` : предупреждения.

`informative` : информационные записи.

`diagnostic` : диагностические записи.

`all` : все записи.

`smart` : фильтрация Smart.

SCANNERS

Журнал «Сканирование компьютера» или список журналов.

СИНТАКСИС

```
[get] scanners [id <ид>] [count <число>] [from <год>-<месяц>-<день> <часы>:<минуты>:<секунды>] [to <год>-<месяц>-<день> <часы>:<минуты>:<секунды>]
```

```
clear scanners
```

ОПЕРАЦИИ

`get` : возвращается текущий параметр/состояние.

`clear` : удаляются все элементы или файлы.

АРГУМЕНТЫ

`ид` : показываются сведения о сканировании компьютера с этим идентификатором.

`ид` : идентификатор сканирования.

`количество` : показывается только выбранное количество записей.

`число` : количество записей.

`from` : показываются только записи с выбранного времени.

`год` : год.

`месяц` : месяц.

`день` : день.

`часы` : часы.

`минуты` : минуты.

`секунды` : секунды.

`to` : показываются только записи с выбранного времени.

VERBOSITY

Минимальная степень детализации журнала.

СИНТАКСИС

```
[get] | restore verbosity
set verbosity critical | errors | warnings | informative | diagnostic
```

ОПЕРАЦИИ

`get` : возвращается текущий параметр/состояние.

`set` : задается значение или состояние.

`restore` : восстанавливаются параметры/объект/файл по умолчанию.

АРГУМЕНТЫ

`critical` : критические ошибки.

`errors` : ошибки.

`warnings` : предупреждения.

`informative` : информационные записи.

`diagnostic` : диагностические записи.

4.10.2.84 Контекст «TOOLS LOG CLEANING»

TIMEOUT

Срок хранения записи журнала (в днях).

СИНТАКСИС

```
[get] | restore timeout
set timeout <число>
```

ОПЕРАЦИИ

`get` : возвращается текущий параметр/состояние.

`set` : задается значение или состояние.

`restore` : восстанавливаются параметры/объект/файл по умолчанию.

АРГУМЕНТЫ

`число` : количество дней (1–365).

USE

Автоматическое удаление журналов.

СИНТАКСИС

```
[get] | restore use

set use disabled | enabled
```

ОПЕРАЦИИ

`get` : возвращается текущий параметр/состояние.

`set` : задается значение или состояние.

`restore` : восстанавливаются параметры/объект/файл по умолчанию.

АРГУМЕНТЫ

`disabled` : отключается функция или параметр.

`enabled` : включается функция или активируется параметр.

4.10.2.85 Контекст «TOOLS LOG OPTIMIZE»

LEVEL

Оптимизация по превышению количества неиспользуемых записей (в процентах).

СИНТАКСИС

```
[get] | restore level

set level <число>
```

ОПЕРАЦИИ

`get` : возвращается текущий параметр/состояние.

`set` : задается значение или состояние.

`restore` : восстанавливаются параметры/объект/файл по умолчанию.

АРГУМЕНТЫ

`число` : доля неиспользуемых записей в процентах (1–100).

USE

Автоматическая оптимизация журналов.

СИНТАКСИС

```
[get] | restore use

set use disabled | enabled
```

ОПЕРАЦИИ

`get` : возвращается текущий параметр/состояние.

`set` : задается значение или состояние.

`restore` : восстанавливаются параметры/объект/файл по умолчанию.

АРГУМЕНТЫ

`disabled` : отключается функция или параметр.

`enabled` : включается функция или активируется параметр.

4.10.2.86 Контекст «TOOLS NOTIFICATION»

VERBOSITY

Минимальная степень детализации уведомлений.

СИНТАКСИС

```
[get] | restore verbosity
set verbosity critical | errors | warnings | informative | diagnostic
```

ОПЕРАЦИИ

`get` : возвращается текущий параметр/состояние.

`set` : задается значение или состояние.

`restore` : восстанавливаются параметры/объект/файл по умолчанию.

АРГУМЕНТЫ

`critical` : критические ошибки.

`errors` : ошибки.

`warnings` : предупреждения.

`informative` : информационные записи.

`diagnostic` : диагностические записи.

4.10.2.87 Контекст «TOOLS NOTIFICATION EMAIL»

FROM

Адрес электронной почты отправителя.

СИНТАКСИС

```
[get] | restore from
set from [<строка>]
```

ОПЕРАЦИИ

`get` : возвращается текущий параметр/состояние.

`set` : задается значение или состояние.

`restore` : восстанавливаются параметры/объект/файл по умолчанию.

АРГУМЕНТЫ

`строка` : адрес электронной почты.

LOGIN

Имя для входа в систему.

СИНТАКСИС

```
[get] | restore login
set login [<строка>]
```

ОПЕРАЦИИ

`get` : возвращается текущий параметр/состояние.

`set` : задается значение или состояние.

`restore` : восстанавливаются параметры/объект/файл по умолчанию.

АРГУМЕНТЫ

`строка` : имя.

PASSWORD

Пароль.

СИНТАКСИС

```
[get] | restore password
set password [plain <пароль>]
```

ОПЕРАЦИИ

`get` : возвращается текущий параметр/состояние.

`set` : задается значение или состояние.

`restore` : восстанавливаются параметры/объект/файл по умолчанию.

АРГУМЕНТЫ

`plain` : переход ко вводу пароля как параметра.

`password` : пароль.

SERVER

Адрес SMTP-сервера.

СИНТАКСИС

```
[get] | restore server
set server [<строка>]
```

ОПЕРАЦИИ

`get` : возвращается текущий параметр/состояние.

`set` : задается значение или состояние.

`restore` : восстанавливаются параметры/объект/файл по умолчанию.

АРГУМЕНТЫ

`строка` : адрес.

TO

Адрес электронной почты получателей.

СИНТАКСИС

```
[get] | restore to
set to [<строка>]
```

ОПЕРАЦИИ

`get` : возвращается текущий параметр/состояние.

`set` : задается значение или состояние.

`restore` : восстанавливаются параметры/объект/файл по умолчанию.

АРГУМЕНТЫ

`строка` : адрес электронной почты.

USE

Отправка событий по электронной почте.

СИНТАКСИС

```
[get] | restore use
```

```
set use disabled | enabled
```

ОПЕРАЦИИ

`get` : возвращается текущий параметр/состояние.

`set` : задается значение или состояние.

`restore` : восстанавливаются параметры/объект/файл по умолчанию.

АРГУМЕНТЫ

`disabled` : отключается функция или параметр.

`enabled` : включается функция или активируется параметр.

4.10.2.88 Контекст «TOOLS NOTIFICATION MESSAGE»

ENCODING

Кодировка предупреждающего сообщения.

СИНТАКСИС

```
[get] | restore encoding
```

```
set encoding nolocal | localcharset | localencoding | ISO-2022-JP
```

ОПЕРАЦИИ

`get` : возвращается текущий параметр/состояние.

`set` : задается значение или состояние.

`restore` : восстанавливаются параметры/объект/файл по умолчанию.

АРГУМЕНТЫ

`nolocal` : не использовать символы национального алфавита.

`localcharset` : использовать символы национального алфавита.

`localencoding` : использовать символы и кодировку национального алфавита.

`ISO` : использовать кодировку ISO-2022-JP (только для японской версии).

4.10.2.89 Контекст «TOOLS NOTIFICATION MESSAGE FORMAT»

DETECTION

Формат предупреждений об угрозах.

СИНТАКСИС

```
[get] | restore detection
```

```
set detection [<строка>]
```

ОПЕРАЦИИ

`get` : возвращается текущий параметр/состояние.

`set` : задается значение или состояние.

`restore` : восстанавливаются параметры/объект/файл по умолчанию.

АРГУМЕНТЫ

`строка` : формат сообщений.

Параметры формата сообщений.

`%TimeStamp%` — дата и время события.

`%Scanner%` — модуль, обнаруживший событие.

`%ComputerName%` — имя компьютера.

`%ProgramName%` — программа, вызвавшая событие.

`%ErrorDescription%` — описание ошибки.

Для выбора формата сообщения нужно заменить ключевые слова (заключенные между символами процента «%») на соответствующие значения.

ПРИМЕЧАНИЕ: У сообщений о вирусах и предупреждениях ESET File Security есть формат по умолчанию. Не рекомендуется менять этот формат. Можно изменить формат, если используется автоматическая система обработки электронной почты.

EVENT

Формат событий.

СИНТАКСИС

```
[get] | restore event

set event [<строка>]
```

ОПЕРАЦИИ

`get` : возвращается текущий параметр/состояние.

`set` : задается значение или состояние.

`restore` : восстанавливаются параметры/объект/файл по умолчанию.

АРГУМЕНТЫ

`строка` : формат сообщений.

Параметры формата сообщений.

`%TimeStamp%` — дата и время события.

`%Scanner%` — модуль, обнаруживший событие.

`%ComputerName%` — имя компьютера.

`%ProgramName%` — программа, вызвавшая событие.

`%InfectedObject%` — зараженный объект (файл, сообщение электронной почты и т. д.).

`%VirusName%` — имя вируса.

Для выбора формата сообщения нужно заменить ключевые слова (заключенные между символами процента «%») на соответствующие значения.

ПРИМЕЧАНИЕ: У сообщений о вирусах и предупреждениях ESET File Security есть формат по умолчанию. Не рекомендуется менять этот формат. Можно изменить формат, если используется автоматическая система обработки электронной почты.

4.10.2.90 Контекст «TOOLS NOTIFICATION WINPOPUP»

ADDRESS

Отправлять уведомления компьютерам с именами.

СИНТАКСИС

```
[get] | restore address

set address [<строка>]
```

ОПЕРАЦИИ

`get` : возвращается текущий параметр/состояние.

`set` : задается значение или состояние.

`restore` : восстанавливаются параметры/объект/файл по умолчанию.

АРГУМЕНТЫ

`строка` : имена компьютеров через запятую.

TIMEOUT

Интервал отправки на компьютеры в локальной сети.

СИНТАКСИС

```
[get] | restore timeout
set timeout <число>
```

ОПЕРАЦИИ

`get` : возвращается текущий параметр/состояние.

`set` : задается значение или состояние.

`restore` : восстанавливаются параметры/объект/файл по умолчанию.

АРГУМЕНТЫ

`число` : интервал в секундах (1–3600).

USE

Отправлять события на компьютеры в локальной сети.

СИНТАКСИС

```
[get] | restore use
set use disabled | enabled
```

ОПЕРАЦИИ

`get` : возвращается текущий параметр/состояние.

`set` : задается значение или состояние.

`restore` : восстанавливаются параметры/объект/файл по умолчанию.

АРГУМЕНТЫ

`disabled` : отключается функция или параметр.

`enabled` : включается функция или активируется параметр.

4.10.2.91 Контекст «TOOLS SCHEDULER»

ACTION

Действие запланированной задачи.

СИНТАКСИС

```
[get] action
set action external | logmaintenance | startupcheck | status | scan | update
```

ОПЕРАЦИИ

`get` : возвращается текущий параметр/состояние.

`set` : задается значение или состояние.

АРГУМЕНТЫ

`external` : запуск внешнего приложения.

`logmaintenance` : обслуживание журнала.

`startupcheck` : сканирование файлов, исполняемых при запуске системы.

`состояние` : создание снимка состояния компьютера.

`scan` : сканирование компьютера.

`update` : обновление.

TASK

Запланированные задачи.

СИНТАКСИС

```
[get] | select task [<ИД>]
set task <ИД> disabled | enabled
add task <имя_задачи>
remove | start task <ИД>
```

ОПЕРАЦИИ

`get` : возвращается текущий параметр/состояние.

`set` : задается значение или состояние.

`select` : выбирается элемент.

`add` : добавляется элемент.

`remove` : удаляется элемент.

`start` : запускается задача.

АРГУМЕНТЫ

`ИД` : идентификатор задачи.

`disabled` : отключается функция или параметр.

`enabled` : включается функция или активируется параметр.

`имя_задачи` : название задачи.

TRIGGER

Выполнение задачи.

СИНТАКСИС

```
[get] trigger
set trigger once | repeat | daily | weekly | event
```

ОПЕРАЦИИ

`get` : возвращается текущий параметр/состояние.

`set` : задается значение или состояние.

АРГУМЕНТЫ

`once` : однократно.

`repeat` : многократно.

`daily` : ежедневно.

`weekly` : еженедельно.

`event` : при определенных условиях.

4.10.2.92 Контекст «TOOLS SCHEDULER EVENT»

INTERVAL

Выполнить задачу один раз в пределах указанного промежутка времени (в часах).

СИНТАКСИС

```
[get] interval
```

```
set interval <часы>
```

ОПЕРАЦИИ

`get` : возвращается текущий параметр/состояние.

`set` : задается значение или состояние.

АРГУМЕНТЫ

`часы` : время в часах (1–720).

TYPE

Задача, запускаемая по событию.

СИНТАКСИС

```
[get] type
```

```
set type startup | startuponcedaily | dialup | engineupdate | appupdate | logon | detection
```

ОПЕРАЦИИ

`get` : возвращается текущий параметр/состояние.

`set` : задается значение или состояние.

АРГУМЕНТЫ

`startup` : при запуске компьютера.

`startuponcedaily` : каждые сутки при первом запуске компьютера.

`dialup` : коммутируемое подключение к Интернету/VPN.

`engineupdate` : обновление сигнатур вирусов.

`appupdate` : обновление компонента программы.

`logon` : вход пользователя в систему.

`detection` : обнаружение угроз.

4.10.2.93 Контекст «TOOLS SCHEDULER FAILSAFE»

EXECUTE

Действие, выполняемое в случае, если задача не была запущена в назначенное время.

СИНТАКСИС

```
[get] execute
```

```
set execute asap | iftimeout | no
```

ОПЕРАЦИИ

`get` : возвращается текущий параметр/состояние.

`set` : задается значение или состояние.

АРГУМЕНТЫ

`asap` : выполнить задачу как можно скорее.

`iftimeout` : выполнить задачу немедленно, если время после последнего запуска выходит за указанный интервал.

`no` : не выполнять с задержкой.

ПРИМЕЧАНИЕ: Чтобы задать ограничение, введите `SET TOOLS SCHEDULER EDIT FAILSAFE TIMEOUT <ЧАСЫ>`.

TIMEOUT

Интервал задачи (в часах).

СИНТАКСИС

```
[get] timeout
```

```
set timeout <часы>
```

ОПЕРАЦИИ

`get` : возвращается текущий параметр/состояние.

`set` : задается значение или состояние.

АРГУМЕНТЫ

`часы` : время в часах (1–720).

4.10.2.94 Контекст «TOOLS SCHEDULER PARAMETERS CHECK»

LEVEL

Уровень сканирования.

СИНТАКСИС

```
[get] level
```

```
set level [before_logon | after_logon | most_frequent | frequent | common | rare | all]
```

ОПЕРАЦИИ

`get` : возвращается текущий параметр/состояние.

`set` : задается значение или состояние.

АРГУМЕНТЫ

`before_logon` : файлы, запускающиеся перед входом пользователя.

`after_logon` : файлы, запускающиеся после входа пользователя.

`most_frequent` : только наиболее часто используемые файлы.

`frequent` : часто используемые файлы.

`common` : обычно используемые файлы.

`rare` : редко используемые файлы.

`all` : зарегистрированные файлы.

PRIORITY

Приоритет сканирования.

СИНТАКСИС

```
[get] priority
```

```
set priority [normal | low | lowest | idle]
```

ОПЕРАЦИИ

`get` : возвращается текущий параметр/состояние.

`set` : задается значение или состояние.

АРГУМЕНТЫ

`normal` : нормальный.

`low` : более низкий.

`lowest` : самый низкий.

`idle` : при бездействии.

4.10.2.95 Контекст «TOOLS SCHEDULER PARAMETERS EXTERNAL»

ARGUMENTS

Аргументы.

СИНТАКСИС

```
[get] arguments
```

```
set arguments <аргументы>
```

ОПЕРАЦИИ

`get` : возвращается текущий параметр/состояние.

`set` : задается значение или состояние.

АРГУМЕНТЫ

`аргументы` : аргументы.

DIRECTORY

Рабочая папка.

СИНТАКСИС

```
[get] directory
```

```
set directory <путь>
```

ОПЕРАЦИИ

`get` : возвращается текущий параметр/состояние.

`set` : задается значение или состояние.

АРГУМЕНТЫ

`путь` : путь.

EXECUTABLE

Исполняемый файл.

СИНТАКСИС

```
[get] executable
```

```
set executable <путь>
```

ОПЕРАЦИИ

`get` : возвращается текущий параметр/состояние.

`set` : задается значение или состояние.

АРГУМЕНТЫ

`путь` : путь.

4.10.2.96 Контекст «TOOLS SCHEDULER PARAMETERS SCAN»

PROFILE

Профиль сканирования.

СИНТАКСИС

```
[get] profile
set profile <профиль>
```

ОПЕРАЦИИ

`get` : возвращается текущий параметр/состояние.

`set` : задается значение или состояние.

АРГУМЕНТЫ

`профиль` : имя профиля.

READONLY

Сканировать без очистки.

СИНТАКСИС

```
[get] readonly
set readonly disabled | enabled
```

ОПЕРАЦИИ

`get` : возвращается текущий параметр/состояние.

`set` : задается значение или состояние.

АРГУМЕНТЫ

`disabled` : отключается функция или параметр.

`enabled` : включается функция или активируется параметр.

TARGET

Объекты сканирования.

СИНТАКСИС

```
[get] | clear target
add | remove target <путь>
```

ОПЕРАЦИИ

`get` : возвращается текущий параметр/состояние.

`add` : добавляется элемент.

`remove` : удаляется элемент.

`clear` : удаляются все элементы или файлы.

АРГУМЕНТЫ

`путь` : путь сканирования/объект.

4.10.2.97 Контекст «TOOLS SCHEDULER PARAMETERS UPDATE»

PRIMARY

Профиль обновления.

СИНТАКСИС

```
[get] primary
```

```
set primary [<профиль>]
```

ОПЕРАЦИИ

`get` : возвращается текущий параметр/состояние.

`set` : задается значение или состояние.

АРГУМЕНТЫ

`профиль` : имя профиля.

SECONDARY

Альтернативный профиль обновления.

СИНТАКСИС

```
[get] secondary
```

```
set secondary [<профиль>]
```

ОПЕРАЦИИ

`get` : возвращается текущий параметр/состояние.

`set` : задается значение или состояние.

АРГУМЕНТЫ

`профиль` : имя профиля.

4.10.2.98 Контекст «TOOLS SCHEDULER REPEAT»

INTERVAL

Интервал задачи (в минутах).

СИНТАКСИС

```
[get] interval
```

```
set interval <минуты>
```

ОПЕРАЦИИ

`get` : возвращается текущий параметр/состояние.

`set` : задается значение или состояние.

АРГУМЕНТЫ

`minutes` : время в минутах (1–720 часов).

4.10.2.99 Контекст «TOOLS SCHEDULER STARTUP»

DATE

Задача будет выполняться в выбранную дату.

СИНТАКСИС

```
[get] date
```

```
set date <год>-<месяц>-<день>
```

ОПЕРАЦИИ

`get` : возвращается текущий параметр/состояние.

`set` : задается значение или состояние.

АРГУМЕНТЫ

`год` : год.

`месяц` : месяц.

`день` : день.

DAYS

Запускать задачу в выбранные дни.

СИНТАКСИС

```
[get] days
```

```
set days [none] [monday] [tuesday] [wednesday] [thurdsday] [friday] [saturday] [sunday] [all]
```

ОПЕРАЦИИ

`get` : возвращается текущий параметр/состояние.

`set` : задается значение или состояние.

АРГУМЕНТЫ

`none` : день не указан.

`monday` : понедельник.

`tuesday` : вторник.

`wednesday` : среда.

`thurdsday` : четверг.

`friday` : пятница.

`saturday` : суббота.

`sunday` : воскресенье.

`all` : каждый день.

TIME

Задача будет выполняться в выбранное время.

СИНТАКСИС

```
[get] time
```

```
set time <часы>:<минуты>:<секунды>
```

ОПЕРАЦИИ

`get` : возвращается текущий параметр/состояние.

`set` : задается значение или состояние.

АРГУМЕНТЫ

`часы` : часы.

`минуты` : минуты.

`секунды` : секунды.

4.10.2.100 Контекст «UPDATE»

CACHE

Очистить кэш обновлений.

СИНТАКСИС

```
clear cache
```

COMPONENTS

Обновить компоненты программы.

СИНТАКСИС

```
[get] | restore components
```

```
set components never | allways | ask
```

ОПЕРАЦИИ

`get` : возвращается текущий параметр/состояние.

`set` : задается значение или состояние.

`restore` : восстанавливаются параметры/объект/файл по умолчанию.

АРГУМЕНТЫ

`never` : не обновлять.

`allways` : всегда обновлять.

`ask` : запросить подтверждение перед загрузкой компонентов программы.

LOGIN

Имя пользователя для входа в систему.

СИНТАКСИС

```
[get] | restore login
```

```
set login [<строка>]
```

ОПЕРАЦИИ

`get` : возвращается текущий параметр/состояние.

`set` : задается значение или состояние.

`restore` : восстанавливаются параметры/объект/файл по умолчанию.

АРГУМЕНТЫ

`строка` : имя.

ПРИМЕЧАНИЕ: Введите имя пользователя и пароль, полученные после покупки или активации. Настоятельно рекомендуется скопировать (Ctrl + C) данные из регистрационного сообщения электронной почты и вставить (Ctrl + V) их в соответствующие поля.

PASSWORD

Пароль.

СИНТАКСИС

```
[get] | restore password
```

`set password [plain <пароль>]`

ОПЕРАЦИИ

`get` : показать пароль.

`set` : задать или удалить пароль.

`restore` : восстанавливаются параметры/объект/файл по умолчанию.

АРГУМЕНТЫ

`plain` : переход ко вводу пароля как параметра.

`password` : пароль.

ПРИМЕЧАНИЕ: Введите имя пользователя и пароль, полученные после покупки или активации. Настоятельно рекомендуется скопировать (Ctrl + C) данные из регистрационного сообщения электронной почты и вставить (Ctrl + V) их в соответствующие поля.

PRERELEASE

включить тестовые обновления.

СИНТАКСИС

`[get] | restore prerelease`

`set prerelease disabled | enabled`

ОПЕРАЦИИ

`get` : возвращается текущий параметр/состояние.

`set` : задается значение или состояние.

`restore` : восстанавливаются параметры/объект/файл по умолчанию.

АРГУМЕНТЫ

`disabled` : отключается функция или параметр.

`enabled` : включается функция или активируется параметр.

PROFILE

Управление профилями обновления.

СИНТАКСИС

`[get] profile`

`select | remove profile <имя>`

`add profile new: <имя> [copyfrom: <имя>]`

ОПЕРАЦИИ

`get` : возвращается текущий параметр/состояние.

`select` : выбирается элемент.

`add` : добавляется элемент.

`remove` : удаляется элемент.

АРГУМЕНТЫ

`имя` : имя профиля.

`new` : новый профиль.

`copyfrom` : копировать настройки профиля.

ПРИМЕЧАНИЕ: Другие команды контекста ссылаются на активный профиль (помеченный символом «x»). Для выбора активного профиля воспользуйтесь командой `select update profile <имя профиля>`.

SERVER

Серверы обновлений.

СИНТАКСИС

```
[get] | restore server
select | add | remove server <сервер>
```

ОПЕРАЦИИ

`get` : возвращается текущий параметр/состояние.

`select` : выбирается элемент.

`add` : добавляется элемент.

`remove` : удаляется элемент.

`restore` : восстанавливаются параметры/объект/файл по умолчанию.

АРГУМЕНТЫ

`server` : адрес сервера.

STATUS

Показать состояние обновлений.

СИНТАКСИС

```
[get] status
```

UPDATE

Обновление.

СИНТАКСИС

```
start | stop update
```

ОПЕРАЦИИ

`start` : запустить обновление.

`stop` : отменить обновление.

4.10.2.101 Контекст «UPDATE CONNECTION»

DISCONNECT

Отключиться от сервера после завершения обновления.

СИНТАКСИС

```
[get] | restore disconnect
set disconnect disabled | enabled
```

ОПЕРАЦИИ

`get` : возвращается текущий параметр/состояние.

`set` : задается значение или состояние.

`restore` : восстанавливаются параметры/объект/файл по умолчанию.

АРГУМЕНТЫ

`disabled` : отключается функция или параметр.

`enabled` : включается функция или активируется параметр.

LOGIN

Имя пользователя.

СИНТАКСИС

```
[get] | restore login

set login [<строка>]
```

ОПЕРАЦИИ

`get` : возвращается текущий параметр/состояние.

`set` : задается значение или состояние.

`restore` : восстанавливаются параметры/объект/файл по умолчанию.

АРГУМЕНТЫ

`строка` : имя.

PASSWORD

Пароль.

СИНТАКСИС

```
[get] | restore password

set password [plain <пароль>]
```

ОПЕРАЦИИ

`get` : показать пароль.

`set` : задать или удалить пароль.

`restore` : восстанавливаются параметры/объект/файл по умолчанию.

АРГУМЕНТЫ

`plain` : переход ко вводу пароля как параметра.

`password` : пароль.

RUNAS

Подключение к локальной сети.

СИНТАКСИС

```
[get] | restore runas

set runas system | current | specified
```

ОПЕРАЦИИ

`get` : возвращается текущий параметр/состояние.

`set` : задается значение или состояние.

`restore` : восстанавливаются параметры/объект/файл по умолчанию.

АРГУМЕНТЫ

`system` : учетная запись системы (по умолчанию).

`current` : текущий пользователь.

`specified` : указанный пользователь.

4.10.2.102 Контекст «UPDATE MIRROR»

ПАПКА

Папка для дублируемых файлов.

СИНТАКСИС

```
[get] | restore folder

set folder [<строка>]
```

ОПЕРАЦИИ

`get` : возвращается текущий параметр/состояние.

`set` : задается значение или состояние.

`restore` : восстанавливаются параметры/объект/файл по умолчанию.

АРГУМЕНТЫ

`строка` : путь к папке.

LOGIN

Имя пользователя.

СИНТАКСИС

```
[get] | restore login

set login [<строка>]
```

ОПЕРАЦИИ

`get` : возвращается текущий параметр/состояние.

`set` : задается значение или состояние.

`restore` : восстанавливаются параметры/объект/файл по умолчанию.

АРГУМЕНТЫ

`строка` : имя.

PASSWORD

Пароль.

СИНТАКСИС

```
[get] | restore password

set password [plain <пароль>]
```

ОПЕРАЦИИ

`get` : показать пароль.

`set` : задать или удалить пароль.

`restore` : восстанавливаются параметры/объект/файл по умолчанию.

АРГУМЕНТЫ

`plain` : переход ко вводу пароля как параметра.

`password` : пароль.

USE

Создать зеркало обновлений.

СИНТАКСИС

```
[get] | restore use
```

```
set use disabled | enabled
```

ОПЕРАЦИИ

`get` : возвращается текущий параметр/состояние.

`set` : задается значение или состояние.

`restore` : восстанавливаются параметры/объект/файл по умолчанию.

АРГУМЕНТЫ

`disabled` : отключается функция или параметр.

`enabled` : включается функция или активируется параметр.

VERSIONS

Управление версиями обновлений.

СИНТАКСИС

```
[get] | restore versions
```

```
select versions <версия>
```

ОПЕРАЦИИ

`get` : показать доступные версии.

`select` : выбрать версию обновления или отменить выбор.

`restore` : восстанавливаются параметры/объект/файл по умолчанию.

АРГУМЕНТЫ

`version` : имя версии.

4.10.2.103 Контекст «UPDATE MIRROR SERVER»

AUTHORIZATION

Использовать аутентификацию.

СИНТАКСИС

```
[get] | restore authorization
```

```
set authorization none | basic | ntlm
```

ОПЕРАЦИИ

`get` : возвращается текущий параметр/состояние.

`set` : задается значение или состояние.

`restore` : восстанавливаются параметры/объект/файл по умолчанию.

АРГУМЕНТЫ

`none` : нет.

`basic` : обычная.

`ntlm` : NTLM.

DISCONNECT

Отключиться от сервера после завершения обновления.

СИНТАКСИС

```
[get] | restore disconnect
```

```
set disconnect disabled | enabled
```

ОПЕРАЦИИ

`get` : возвращается текущий параметр/состояние.

`set` : задается значение или состояние.

`restore` : восстанавливаются параметры/объект/файл по умолчанию.

АРГУМЕНТЫ

`disabled` : отключается функция или параметр.

`enabled` : включается функция или активируется параметр.

LOGIN

Имя пользователя.

СИНТАКСИС

```
[get] | restore login
set login [<строка>]
```

ОПЕРАЦИИ

`get` : возвращается текущий параметр/состояние.

`set` : задается значение или состояние.

`restore` : восстанавливаются параметры/объект/файл по умолчанию.

АРГУМЕНТЫ

`строка` : имя.

PASSWORD

Пароль.

СИНТАКСИС

```
[get] | restore password
set password [plain <пароль>]
```

ОПЕРАЦИИ

`get` : показать пароль.

`set` : задать или удалить пароль.

`restore` : восстанавливаются параметры/объект/файл по умолчанию.

АРГУМЕНТЫ

`plain` : переход ко вводу пароля как параметра.

`password` : пароль.

PORT

Порт.

СИНТАКСИС

```
[get] | restore port
set port <число>
```

ОПЕРАЦИИ

`get` : возвращается текущий параметр/состояние.

`set` : задается значение или состояние.

`restore` : восстанавливаются параметры/объект/файл по умолчанию.

АРГУМЕНТЫ

`число` : номер порта.

RUNAS

Подключение к локальной сети.

СИНТАКСИС

```
[get] | restore runas
set runas system | current | specified
```

ОПЕРАЦИИ

`get` : возвращается текущий параметр/состояние.

`set` : задается значение или состояние.

`restore` : восстанавливаются параметры/объект/файл по умолчанию.

АРГУМЕНТЫ

`system` : учетная запись системы (по умолчанию).

`current` : текущий пользователь.

`specified` : указанный пользователь.

SELECTEDPCU

Выбранное обновление компонентов программы для зеркала.

СИНТАКСИС

```
[get] | restore selectedpcu
set selectedpcu [<строка>]
```

ОПЕРАЦИИ

`get` : возвращается текущий параметр/состояние.

`set` : задается значение или состояние.

`restore` : восстанавливаются параметры/объект/файл по умолчанию.

USE

Передавать файлы обновления через внутренний сервер HTTP.

СИНТАКСИС

```
[get] | restore use
set use disabled | enabled
```

ОПЕРАЦИИ

`get` : возвращается текущий параметр/состояние.

`set` : задается значение или состояние.

`restore` : восстанавливаются параметры/объект/файл по умолчанию.

АРГУМЕНТЫ

`disabled` : отключается функция или параметр.

`enabled` : включается функция или активируется параметр.

4.10.2.104 Контекст «UPDATE NOTIFICATION»

DOWNLOAD

Запрашивать подтверждение перед загрузкой обновления.

СИНТАКСИС

```
[get] | restore download

set download disabled | enabled
```

ОПЕРАЦИИ

`get` : возвращается текущий параметр/состояние.

`set` : задается значение или состояние.

`restore` : восстанавливаются параметры/объект/файл по умолчанию.

АРГУМЕНТЫ

`disabled` : отключается функция или параметр.

`enabled` : включается функция или активируется параметр.

HIDE

Не отображать уведомление об успешном обновлении.

СИНТАКСИС

```
[get] | restore hide

set hide disabled | enabled
```

ОПЕРАЦИИ

`get` : возвращается текущий параметр/состояние.

`set` : задается значение или состояние.

`restore` : восстанавливаются параметры/объект/файл по умолчанию.

АРГУМЕНТЫ

`disabled` : отключается функция или параметр.

`enabled` : включается функция или активируется параметр.

SIZE

Запрашивать подтверждение, если размер обновления превышает значение в килобайтах.

СИНТАКСИС

```
[get] | restore size

set size <число>
```

ОПЕРАЦИИ

`get` : возвращается текущий параметр/состояние.

`set` : задается значение или состояние.

`restore` : восстанавливаются параметры/объект/файл по умолчанию.

АРГУМЕНТЫ

`число` : размер файла (Кб).

ПРИМЕЧАНИЕ: Для того чтобы отключить уведомления об обновлениях, введите `0` .

4.10.2.105 Контекст «UPDATE PROXY»

LOGIN

Имя пользователя.

СИНТАКСИС

```
[get] | restore login
set login [<строка>]
```

ОПЕРАЦИИ

`get` : возвращается текущий параметр/состояние.

`set` : задается значение или состояние.

`restore` : восстанавливаются параметры/объект/файл по умолчанию.

АРГУМЕНТЫ

`строка` : имя.

РЕЖИМ

Настройка прокси HTTP.

СИНТАКСИС

```
[get] | restore mode
set mode global | noproxy | userdefined
```

ОПЕРАЦИИ

`get` : возвращается текущий параметр/состояние.

`set` : задается значение или состояние.

`restore` : восстанавливаются параметры/объект/файл по умолчанию.

АРГУМЕНТЫ

`global` : использовать общие параметры прокси-сервера.

`noproxy` : не использовать прокси-сервер.

`userdefined` : соединение через прокси-сервер.

PASSWORD

Пароль.

СИНТАКСИС

```
[get] | restore password
set password [plain <пароль>]
```

ОПЕРАЦИИ

`get` : показать пароль.

`set` : задать или удалить пароль.

`restore` : восстанавливаются параметры/объект/файл по умолчанию.

АРГУМЕНТЫ

`plain` : переход ко вводу пароля как параметра.

`password` : пароль.

PORT

Порт прокси-сервера.

СИНТАКСИС

```
[get] | restore port
set port <число>
```

ОПЕРАЦИИ

`get` : возвращается текущий параметр/состояние.

`set` : задается значение или состояние.

`restore` : восстанавливаются параметры/объект/файл по умолчанию.

АРГУМЕНТЫ

`число` : номер порта.

SERVER

Прокси-сервер.

СИНТАКСИС

```
[get] | restore server
set server [<строка>]
```

ОПЕРАЦИИ

`get` : возвращается текущий параметр/состояние.

`set` : задается значение или состояние.

`restore` : восстанавливаются параметры/объект/файл по умолчанию.

АРГУМЕНТЫ

`строка` : адрес сервера.

4.10.2.106 Контекст «UPDATE SYSTEM»

NOTIFY

Уведомлять об отсутствующих обновлениях, начиная с уровня.

СИНТАКСИС

```
[get] | restore notify
set notify no | optional | recommended | important | critical
```

ОПЕРАЦИИ

`get` : возвращается текущий параметр/состояние.

`set` : задается значение или состояние.

`restore` : восстанавливаются параметры/объект/файл по умолчанию.

АРГУМЕНТЫ

`no` : нет.

`optional` : необязательное.

`recommended` : рекомендуемое.

`important` : важное.

`critical` : критическое.

RESTART

Перезапустить компьютер после обновления компонентов программы.

СИНТАКСИС

`[get] | restore restart`

`set restart never | ask | auto`

ОПЕРАЦИИ

`get` : возвращается текущий параметр/состояние.

`set` : задается значение или состояние.

`restore` : восстанавливаются параметры/объект/файл по умолчанию.

АРГУМЕНТЫ

`never` : не перезапускать.

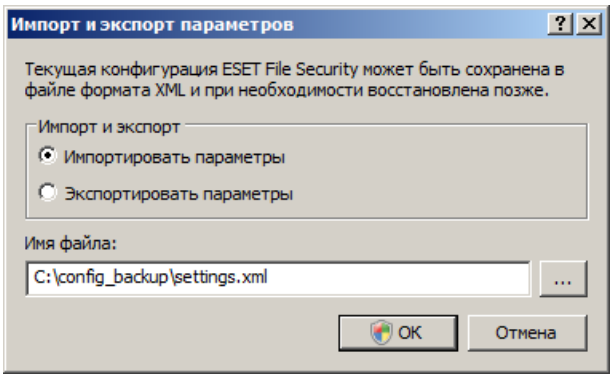
`ask` : запрашивать подтверждение перед перезапуском.

`auto` : перезапускать автоматически.

4.11 Импорт и экспорт параметров

Импорт и экспорт конфигураций ESET File Security выполняется в разделе **Настройка**. Для этого используется ссылка **Импорт и экспорт параметров**.

И для импорта, и для экспорта используются файлы в формате XML. Импорт и экспорт удобны, если нужно создать резервную копию текущей конфигурации ESET File Security для дальнейшего использования. Экспорт параметров также полезен, если необходимо использовать выбранную конфигурацию ESET File Security на нескольких компьютерах. Для этого файл XML можно легко импортировать для переноса нужных параметров.



4.12 ThreatSense.Net

Система своевременного обнаружения ThreatSense.Net оперативно непрерывно уведомляет компанию ESET о новых заражениях. Действующая в обоих направлениях система своевременного обнаружения ThreatSense.Net имеет единственное предназначение — сделать защиту компьютера пользователя еще более надежной. Лучшим способом обеспечить обнаружение новых угроз сразу после их появления является сбор информации от как можно большего числа пользователей. Существует два варианта работы.

1. Пользователь отключает систему своевременного обнаружения ThreatSense.Net. Функциональность программного обеспечения при этом не ограничивается, и пользователь все равно получает наилучшую защиту.

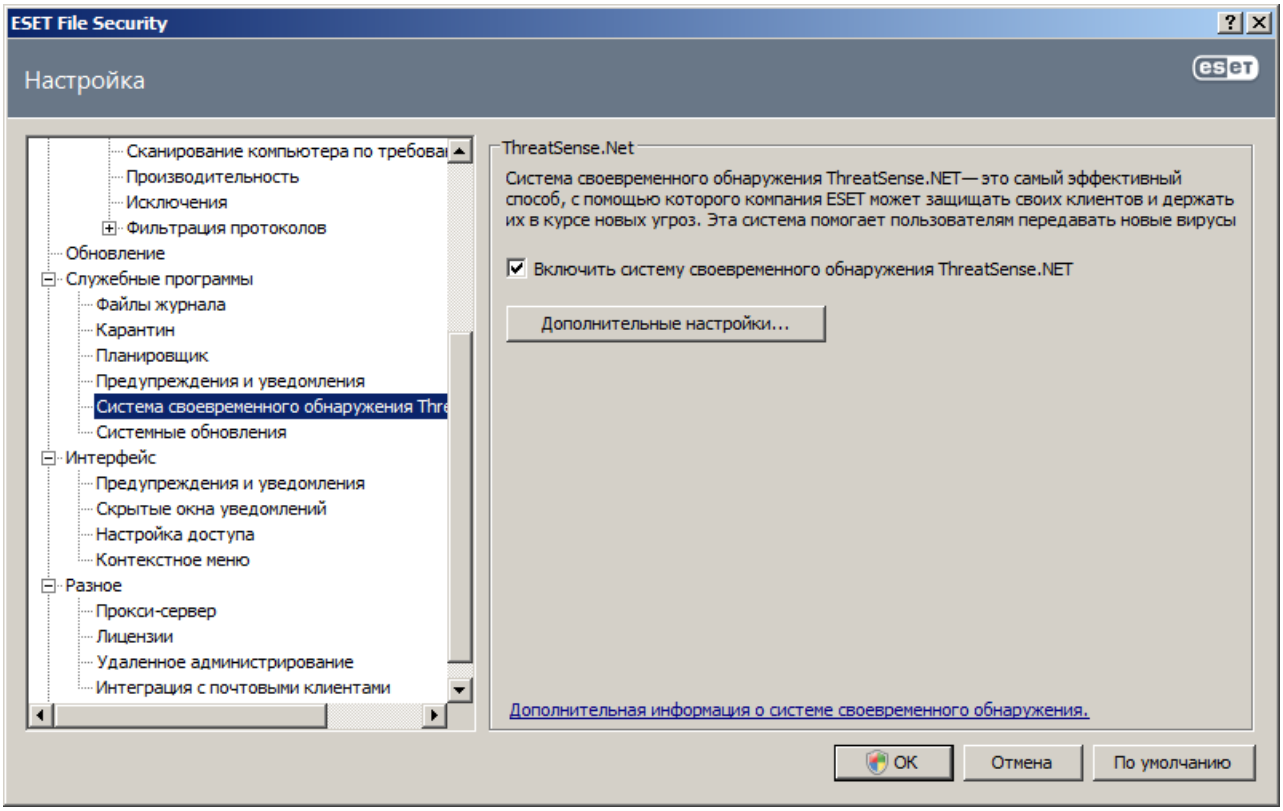
2. Можно разрешить системе своевременного обнаружения ThreatSense.Net отправлять анонимную информацию о новых угрозах и файлах, содержащих неизвестный пока опасный код. Файл может быть отправлен в ESET для тщательного анализа. Изучение этих угроз поможет компании ESET обновить средства обнаружения угроз.

Система своевременного обнаружения ThreatSense.Net собирает о компьютерах пользователей информацию, которая связана с новыми обнаруженными угрозами. Это может быть образец кода или копия файла, в котором возникла угроза, путь к такому файлу, его имя, дата и время, имя процесса, в рамках которого угроза появилась на компьютере, и сведения об операционной системе.

Поскольку в отправляемую в лабораторию ESET информацию могут иногда попадать сведения о пользователе и его компьютере (например, имя пользователя в пути к файлу), компания ESET заверяет, что такая информация будет использоваться исключительно для немедленного реагирования на новые угрозы.

По умолчанию программа ESET File Security запрашивает разрешение на отправку подозрительных файлов в лабораторию ESET для тщательного анализа. Всегда исключаются файлы с определенными расширениями, такими как .doc и .xls. Также можно добавить другие расширения, если политика вашей организации предписывает исключение из отправки.

Параметры системы своевременного обнаружения ThreatSense.Net доступны через дерево расширенных параметров в разделе **Служебные программы** > **ThreatSense.Net**. Установите флажок **Включить систему быстрого оповещения ThreatSense**, чтобы активировать ее, и нажмите кнопку **Дополнительные настройки**.

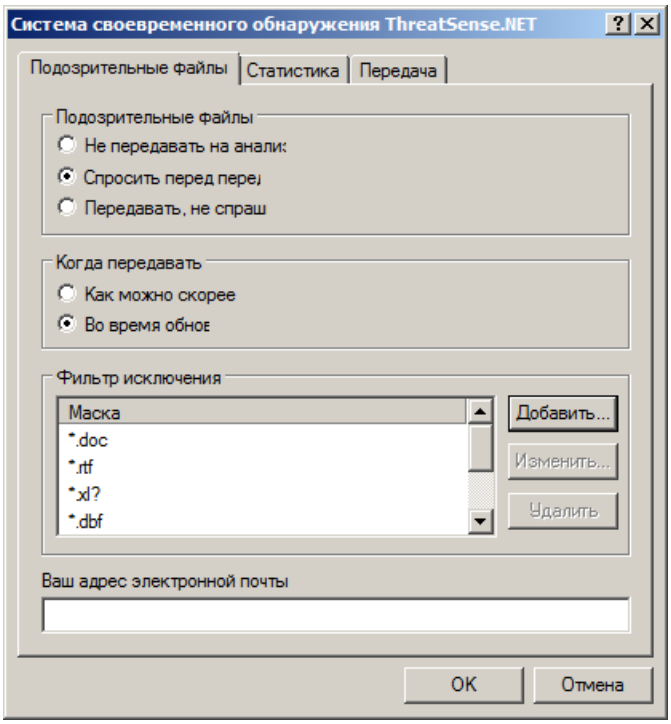


4.12.1 Подозрительные файлы

На вкладке **Подозрительные файлы** можно сконфигурировать способ отправки угроз в лабораторию ESET на анализ.

При обнаружении подозрительного файла его можно отправить в лабораторию ESET на анализ. Если это вредоносное приложение, информация о нем будет включена в следующее обновление сигнатур вирусов.

Можно настроить автоматическую отправку файлов или же выбрать вариант **Спросить перед передачей**, если хотите знать, какие файлы будут отправлены на анализ, и подтверждать данное действие.



Если вы не хотите отправлять файлы на анализ, установите флажок **Не передавать на анализ**. Отказ от отправки файлов на анализ не влияет на отправку статистической информации, для конфигурирования которой существуют собственные параметры (см. раздел Статистика).

Когда передавать: по умолчанию для отправки подозрительных файлов в лабораторию ESET выбран вариант **Как можно скорее**. Этот вариант рекомендуется использовать, если существует постоянное подключение к Интернету, а подозрительные файлы могут доставляться без задержек. Установите флажок **Во время обновления**, чтобы подозрительные файлы загружались в ThreatSense.Net при следующем обновлении.

Фильтр исключения: этот вариант позволяет исключить из отправки определенные файлы или папки. Например, может быть полезно исключить файлы, в которых может присутствовать конфиденциальная информация, такие как документы и электронные таблицы. Файлы наиболее распространенных типов (.doc и т. п.) исключаются по умолчанию. При желании можно дополнять список исключенных файлов.

Адрес электронной почты (необязательно): можно отправить адрес электронной почты вместе с подозрительными файлами, чтобы специалисты ESET могли обратиться к вам, если для анализа потребуется дополнительная информация. Имейте в виду, что компания ESET не отправляет ответы пользователям без необходимости.

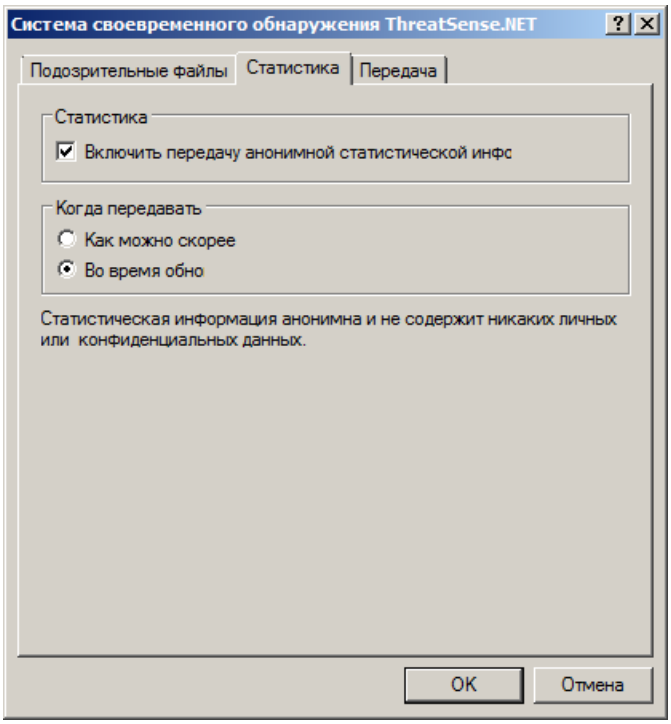
4.12.2 Статистика

Система своевременного обнаружения ThreatSense.Net собирает анонимную информацию о компьютерах пользователей, связанную со вновь обнаруженными угрозами. Это может быть имя заражения, дата и время обнаружения, версия программного продукта обеспечения безопасности ESET, версия операционной системы и информация о расположении. Обычно статистика отправляется на серверы ESET один или два раза в день.

Пример отправляемого пакета со статистикой представлен ниже.

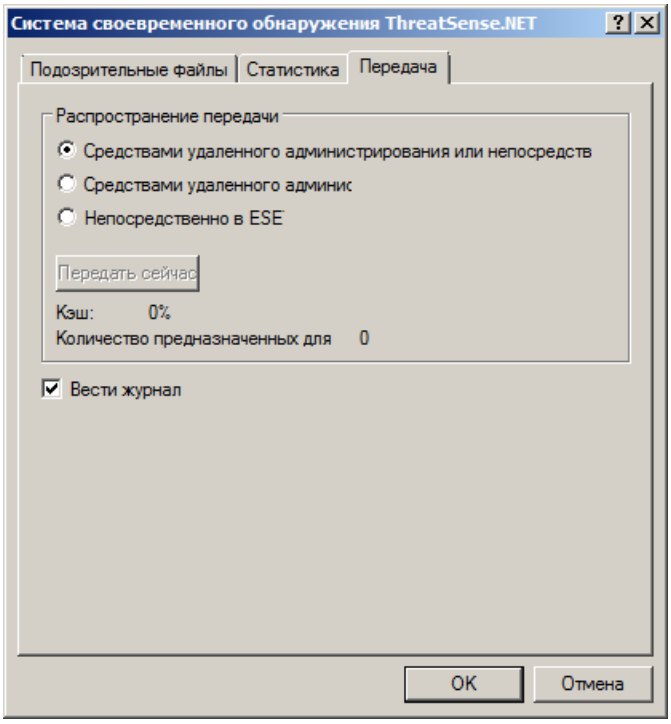
```
# utc_time=2005-04-14 07:21:28
# country="Slovakia"
# language="ENGLISH"
# osver=5.1.2600 NT
# engine=5417
# components=2.50.2
# moduleid=0x4e4f4d41
# filesize=28368
# filename=C:\Documents and Settings\Administrator\Local Settings\Temporary Internet Files\Content.IE5\C14J8
```

Когда отправлять: можно указать, когда будет отправляться статистическая информация. Если выбрать вариант **Как можно скорее**, статистическая информация будет отправляться сразу после сбора. Этот вариант уместен при наличии постоянного подключения к Интернету. Если выбран вариант **Во время обновления**, статистическая информация будет отправляться одним пакетом при следующем обновлении.



4.12.3 Отправка

Можно выбрать, как именно файлы и статистическая информация будут отправляться в компанию ESET. Выберите вариант **Средствами удаленного администрирования или непосредственно в ESET** для отправки файлов и статистической информации любым доступным способом. Выберите вариант **Средствами удаленного администрирования**, чтобы отправлять файлы и статистику на сервер удаленного администрирования, который уже обеспечивает их отправку в лабораторию ESET. При выборе варианта **Непосредственно в ESET** подозрительные файлы и статистика отправляются программой в лабораторию ESET напрямую.



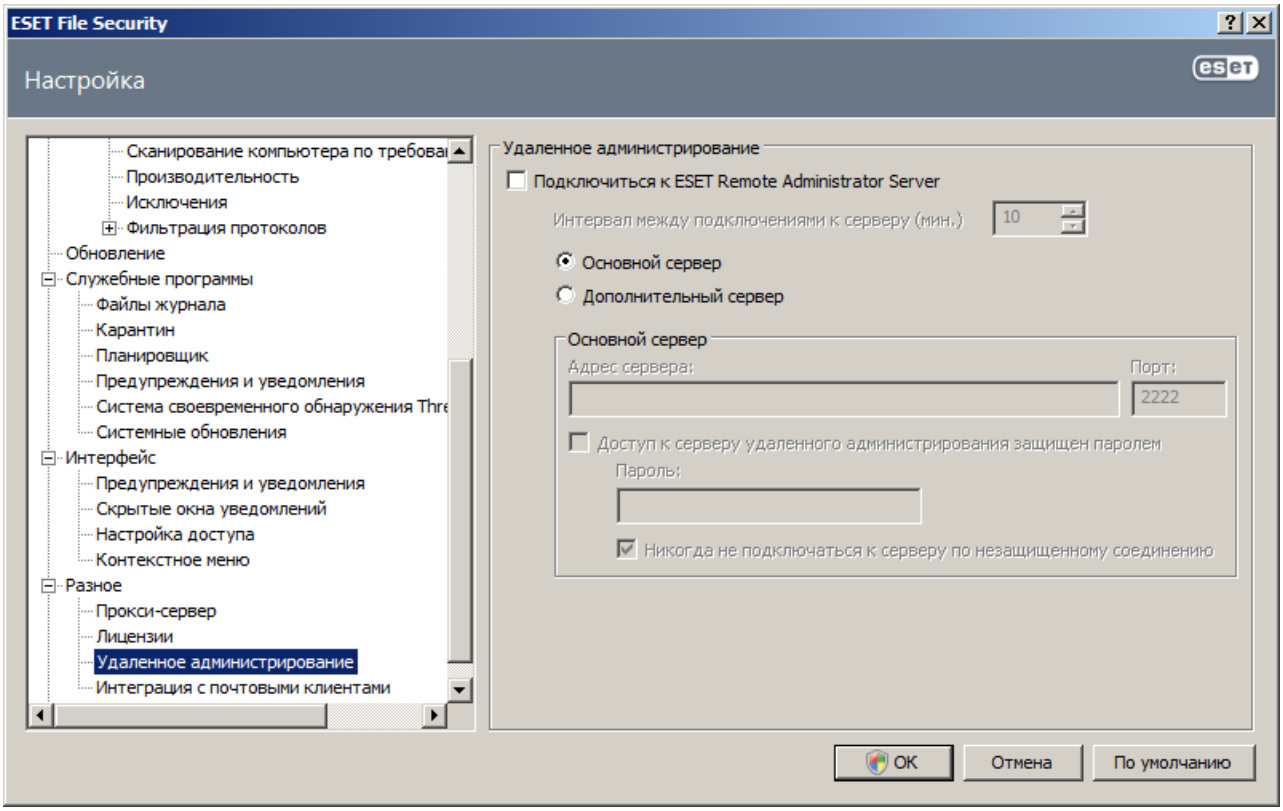
Если есть ожидающие отправки файлы, будет доступна кнопка **Передать сейчас**. Нажмите эту кнопку, чтобы немедленно отправить файлы и статистическую информацию.

Установите флажок **Вкл ведение журнала**, чтобы создать журнал для регистрации фактов отправки файлов и статистической информации.

4.13 Удаленное администрирование

ESET Remote Administrator (ERA) — это полезное средство, используемое для управления политикой безопасности и получения общих сведений о безопасности сети. Это особенно полезно в больших сетях. Средство ERA не только повышает уровень безопасности, но и облегчает администрирование ESET File Security на клиентских рабочих станциях.

Параметры удаленного администрирования доступны из главного окна программы ESET File Security. Нажмите **Настройка** > **Ввод всего дерева расширенных параметров...** > **Разное** > **Удаленное администрирование**.



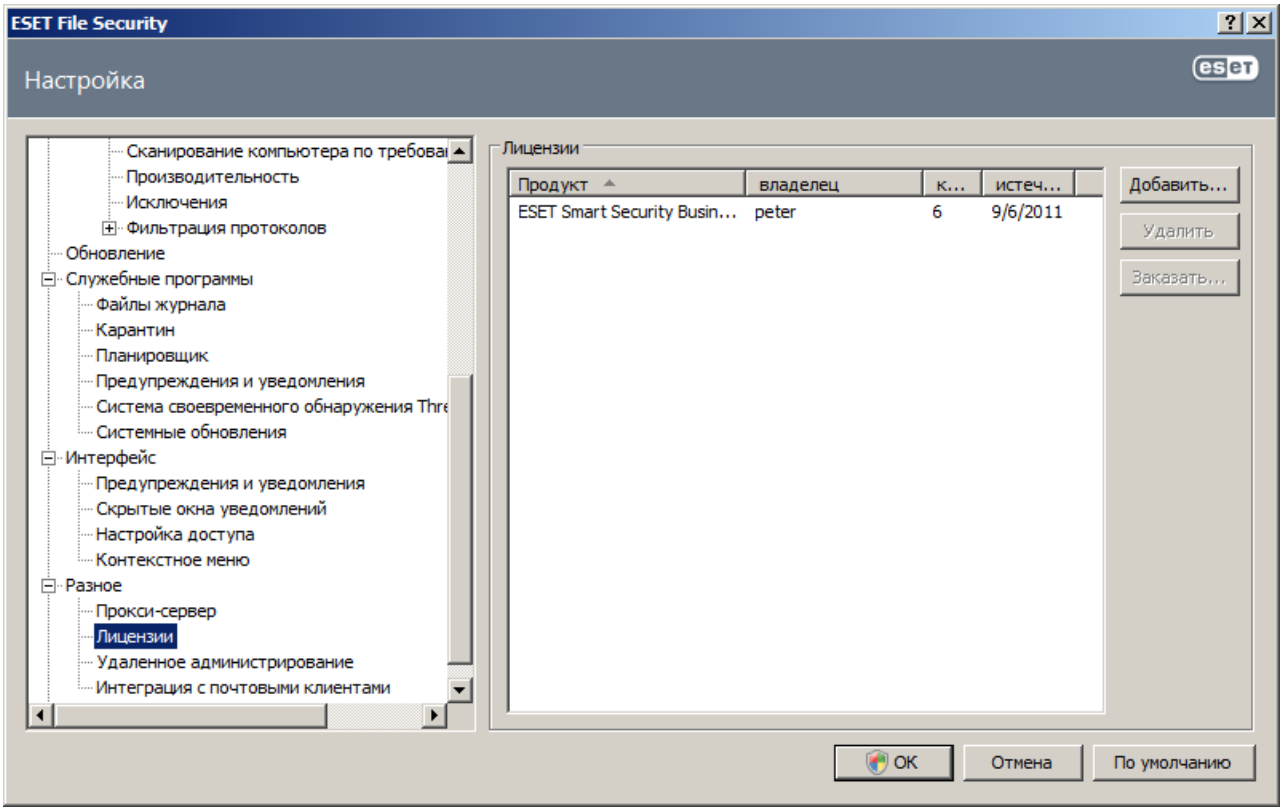
Активируйте удаленное администрирование, установив флажок **«Подключиться к серверу Remote Administrator Server»**. После этого станут доступны остальные описанные далее параметры.

- **Интервал между подключениями к серверу (мин.)** : этим параметром задается частота подключения ESET File Security к серверу ERA Server. Если установлено значение 0, данные отправляются каждые 5 секунд.
- **Адрес сервера:**: сетевой адрес сервера, на котором установлен сервер ERA Server.
- **Порт:** в этом поле указан предварительно заданный порт сервера, используемый для соединения. Рекомендуется не изменять порт по умолчанию (2222).
- **Для доступа к серверу Remote Administrator требуется аутентификация**: позволяет ввести пароль для подключения к серверу ERA Server, если он необходим.

Нажмите кнопку **OK**, чтобы подтвердить внесение изменений, и примените параметры. ESET File Security будет использовать эти параметры для подключения к серверу ERA Server.

4.14 Лицензии

В ветви **Лицензии** можно управлять лицензионными ключами для ESET File Security и других программных продуктов ESET, таких как ESET Mail Security и прочие. После покупки лицензионные ключи доставляются вместе с именем пользователя и паролем. Для добавления или удаления лицензионного ключа нажмите соответствующую кнопку в окне менеджера лицензий. Менеджер лицензий можно открыть через дерево расширенных параметров в разделе **Разное** > **Лицензии**.



Лицензионный ключ представляет собой текстовый файл, содержащий информацию о приобретенном продукте: владелец лицензии, количество лицензий и дата окончания срока действия.

В окне менеджера лицензий можно загрузить и просмотреть содержимое лицензионного ключа, нажав кнопку **Добавить...**, после чего на экран будет выведена соответствующая информация. Для того чтобы удалить файлы лицензии из списка, нажмите **Удалить**.

Если срок действия лицензионного ключа истек и вы хотите продлить лицензию, нажмите кнопку **Заказать...**, после чего вы перейдете в наш интернет-магазин.

5. Глоссарий

5.1 Типы заражений

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

5.1.1 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 и документы. Для размножения вирус присоединяет свое «тело» к концу заражаемого файла. Компьютерный вирус функционирует следующим способом: после запуска зараженного файла вирус активируется (это происходит перед активацией самого приложения) и выполняет возложенные на него задачи. Только после этого запускается само приложение. Вирус не может заразить компьютер, пока пользователь (по ошибке или намеренно) собственноручно не запустит вредоносную программу.

Компьютерные вирусы могут быть разными по целям и степени опасности. Некоторые из вирусов особо опасны, так как могут целенаправленно 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 для защиты от вирусов.

Примеры вирусов: OneHalf, Tenga и Yankee Doodle.

5.1.2 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.

Поэтому черви намного более подвижны, чем компьютерные вирусы. Благодаря широкой популярности Интернета они могут распространяться по всему земному шару за считаные часы или даже минуты после запуска. Эта способность быстро самостоятельно реплицироваться делает черви более опасными, чем другие типы вредоносных программ.

Действующий в системе червь может доставить множество 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.

5.1.3 Троянские программы

Исторически троянскими программами называли такой класс заражений, которые пытаются маскироваться под полезные программы, тем самым заставляя пользователя запускать их. Однако важно отметить, что на сегодняшний день это определение устарело, и троянские программы больше не нуждаются в подобного рода маскировке. Единственной их целью является как можно более простое проникновение в систему и выполнение своих вредоносных задач. 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, способная загружать другие заражения из Интернета.
- **Dropper** — тип троянской программы, которая предназначена 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** — программа, которая регистрирует все, что пользователь набирает на клавиатуре, и отправляет эту информацию злоумышленникам.
- **Программа дозвона** — программа, которая предназначена для набора номеров телефонов, вызовы на которые оплачивает вызывающий абонент. При этом пользователь практически не может заметить, что создано новое подключение. Программы дозвона могут нанести вред только пользователям модемов, которые уже не распространены столь широко, как раньше.

Троянская программа обычно представляет собой исполняемый файл с расширением exe. Если на компьютере обнаружен файл, классифицированный как троянская программа, рекомендуется удалить его, так как он с большой вероятностью содержит злонамеренный код.

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

5.1.4 Руткиты

Руткитом называется вредоносная программа, которая предоставляет злоумышленникам полный доступ к компьютеру, не проявляя при этом своего присутствия в системе. После получения доступа к системе (обычно путем использования ее уязвимостей) руткиты используют функции операционной системы, чтобы избежать обнаружения программным обеспечением защиты от вирусов: используются механизмы маскировки процессов, файлов и данных реестра Windows и т. п. По этой причине их активность практически невозможно обнаружить, используя стандартные методы тестирования.

Существует два уровня обнаружения, направленных на борьбу с руткитами.

1) Обнаружение при попытке проникновения в систему. Их еще нет в системе, то есть они не активны. Многие системы защиты от вирусов способны устранить руткиты на этом уровне (при условии, что они действительно обнаруживают такие файлы как зараженные).
2) Обнаружение при попытке скрыться во время обычной проверки. В распоряжении пользователей ESET File Security есть преимущества технологии Anti-Stealth, которая позволяет обнаружить и устранить активные руткиты.

5.1.5 Рекламные программы

Под рекламной программой понимается программное обеспечение, поддерживаемое рекламой. Программы, демонстрирующие пользователю рекламные материалы, относятся к этой категории. Частыми признаками работы рекламных программ являются появление всплывающих окон с рекламой в веб-браузере или изменение домашней страницы. Рекламные программы часто распространяются в комплекте с бесплатными программами. Это позволяет их создателям покрывать расходы на разработку полезных (как правило) программ.

Сами по себе рекламные программы не опасны, но они раздражают пользователей. Опасность заключается в том, что в рекламных программах могут быть реализованы дополнительные функции слежения, подобно шпионским программам.

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 либо их функциональность будет ограничена. 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 случае лучше перестраховаться. В случае обнаружения на компьютере файла, классифицированного как рекламная программа, рекомендуется удалить его, так как скорее всего он содержит злонамеренный код.

5.1.6 Шпионские программы

К этой категории относятся все приложения, которые отправляют личную информацию без ведома и согласия 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 потребностей и интересов пользователей и позволяют демонстрировать рекламные материалы, более соответствующие интересам целевой аудитории. Проблема заключается в том, что нет четкой границы между полезными и вредоносными приложениями, и никто не гарантирует, что получаемая 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 известных бесплатных программных продуктов, вместе с которыми поставляются шпионские программы, могут служить клиентские приложения 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 они сами являются таковыми.

В случае обнаружения на компьютере файла, классифицированного как шпионская программа, рекомендуется удалить его, так как с высокой вероятностью он содержит злонамеренный код.

5.1.7 Потенциально опасное ПО

Существует множество нормальных программ, предназначенных для упрощения администрирования подключенных к сети компьютеров. Однако злоумышленники могут использовать их для причинения вреда. Программное обеспечение ESET File Security позволяет обнаруживать 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, регистрирующие нажатия клавиш на клавиатуре).

Если потенциально опасное приложение обнаружено и работает на компьютере (но пользователь не устанавливал его), следует обратиться к администратору сети или удалить приложение.

5.1.8 Потенциально нежелательное ПО

Потенциально нежелательные приложения не обязательно являются вредоносными, но могут отрицательно влиять на производительность компьютера. Обычно для установки таких приложений запрашивается согласие пользователя. После их установки поведение системы изменяется (по сравнению с тем, как она вела себя до установки этих приложений). Наиболее заметные изменения перечислены далее.

- Открываются новые окна, которые не появлялись ранее.
- Активируются и выполняются скрытые процессы.
- Повышается уровень потребления системных ресурсов.
- Появляются изменения в результатах поиска.
- Приложение обменивается данными с удаленными серверами.