ESET ENDPOINT SECURITY

Руководство пользователя

Microsoft® Windows® 8 / 7 / Vista / XP / 2000 / Home Server

Щелкните здесь, чтобы загрузить актуальную версию этого документа

ESET **ENDPOINT SECURITY**

Международная служба поддержки клиентов: www.eset.com/support

Версия 20. 2. 2013

Содержание

1. ESET Endpoint Security

ESET Endpoint Security представляет собой новый подход к созданию действительно комплексной системы безопасности компьютера. Новейшая версия модуля сканирования ThreatSense® в сочетании со специализированными модулями персонального файервола и защиты от спама обеспечивает скорость и точность, необходимые для безопасности компьютера. Таким образом, продукт представляет собой развитую систему непрерывного предупреждения атак и защиты компьютера от вредоносных программ.

ESET Endpoint Security — это комплексное решение для обеспечения безопасности, являющееся результатом долгих усилий, направленных на достижение оптимального сочетания максимальной степени защиты с минимальным влиянием на производительность компьютера. Современные технологии, основанные на применении искусственного интеллекта, способны превентивно противодействовать заражениям вирусами, шпионскими, троянскими, рекламными программами, червями, руткитами и другими атаками из Интернета без влияния на производительность компьютера и перерывов в работе.

Решение ESET Endpoint Security предназначено в первую очередь для использования на рабочих станциях в средах небольших и крупных предприятий. Его можно использовать с ESET Remote Administrator, что позволяет с легкостью управлять любым количеством клиентских рабочих станций, применять политики и правила, отслеживать обнаруживаемые угрозы и удаленно конфигурировать систему с любого подключенного к сети компьютера.

1.1 Системные требования

Для правильной работы ESET Endpoint Security система должна отвечать перечисленным ниже аппаратным и программным требованиям.

Microsoft® Windows® 2000, XP

Процессор 400 МГц, 32-разрядный (x86) или 64-разрядный (x64)
128 МБ оперативной памяти
320 МБ свободного места на диске
Монитор Super VGA (800 × 600)

Microsoft® Windows® 8, 7, Vista, Home Server

Процессор 1 ГГц, 32-разрядный (x86) или 64-разрядный (x64)
512 МБ оперативной памяти
320 МБ свободного места на диске
Монитор Super VGA (800 × 600)

1.2 Профилактика

При использовании компьютера, особенно во время работы в Интернете, необходимо помнить о том, что ни одна система защиты от вирусов не способна полностью устранить вероятность заражений и атак. Для того чтобы достигнуть наивысшей степени безопасности и комфорта, следуйте нескольким простым правилам и используйте систему защиты от вирусов надлежащим образом.

Регулярно обновляйте систему защиты от вирусов.

Согласно статистическим данным, полученным от системы своевременного обнаружения ESET Live Grid, тысячи новых уникальных заражений появляются ежедневно. Они пытаются обойти существующие меры безопасности и приносят доход их авторам за счет убытков других пользователей. Специалисты вирусной лаборатории ESET ежедневно анализируют угрозы, создают и предоставляют к загрузке новые обновления для непрерывного усовершенствования защиты пользователей от вирусов. Неправильно настроенная система обновлений снижает эффективность программы. Дополнительные сведения о настройке обновлений см. в главе Настройка обновлений.

Загружайте пакеты обновлений операционной системы и других программ.

Авторы вредоносных программ используют различные уязвимости в системе для увеличения эффективности распространения злонамеренного кода. По этой причине производители программного обеспечения внимательно следят за появлением отчетов о новых уязвимостях их программных продуктов и выпускают регулярные обновления, стараясь снизить вероятность появления новых угроз. Очень важно загружать эти обновления сразу после их выпуска. Примерами программных продуктов, регулярно нуждающихся в

обновлениях, являются операционные системы семейства Windows или широко распространенный веб-браузер Internet Explorer.

Архивируйте важные данные.

Авторы вредоносных программ обычно не заботятся о пользователях, а действия их продуктов зачастую ведут к полной неработоспособности операционной системы и намеренному повреждению важной информации. Необходимо регулярно создавать резервные копии важных конфиденциальных данных на внешних носителях, таких как DVD-диски или внешние жесткие диски. Профилактические меры такого рода позволяют быстро и просто восстановить данных в случае их повреждения.

Регулярно сканируйте компьютер на наличие вирусов.

Регулярное автоматическое сканирование компьютера с надлежащими параметрами помогает устранять заражения, которые могут быть пропущены модулем защиты в режиме реального времени вследствие устаревшей на тот момент базы данных сигнатур вирусов.

Следуйте основным правилам безопасности.

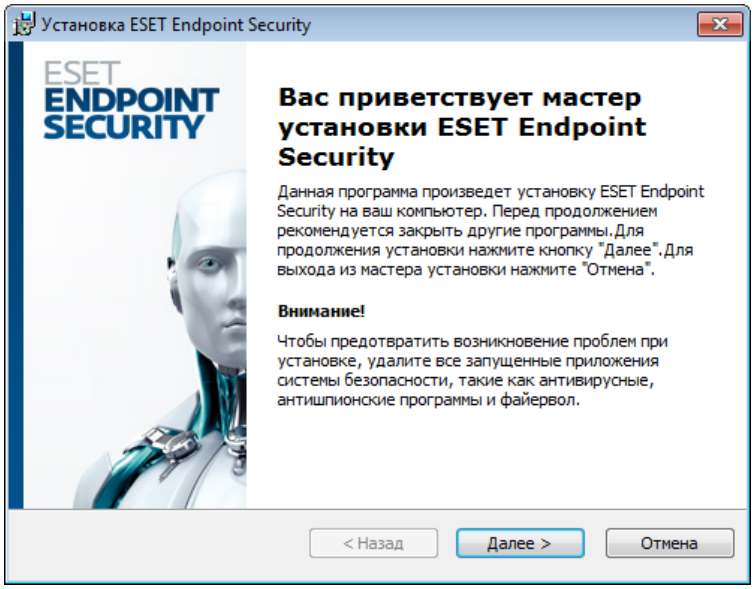
Это наиболее эффективное и полезное правило из всех — всегда будьте осторожны. На данный момент для работы многих заражений (их выполнения и распространения) необходимо вмешательство пользователя. Если соблюдать осторожность при открытии новых файлов, можно значительно сэкономить время и силы, которые в противном случае будут потрачены на устранение заражений. Некоторые полезные правила приведены ниже.

- Не посещайте подозрительные веб-сайты с множеством всплывающих окон и анимированной рекламой.
- Будьте осторожны при установке бесплатных программ, пакетов кодеков и т. п.. Используйте только безопасные программы и посещайте безопасные веб-сайты.
- Будьте осторожны, открывая вложения в сообщения электронной почты (особенно это касается сообщений, рассылаемых массово и отправленных неизвестными лицами).
- Не используйте учетную запись с правами администратора для повседневной работы на компьютере.

2. Установка

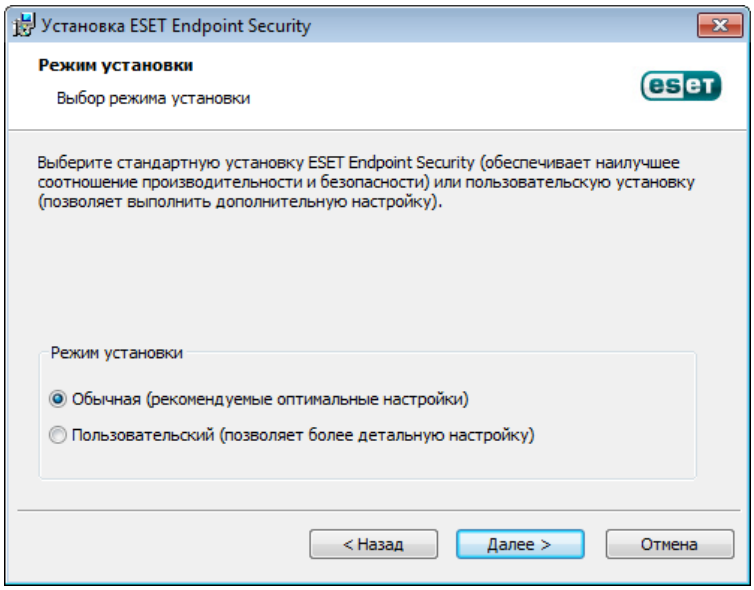
После запуска этого файла мастер установки поможет установить программу.

Внимание! Убедитесь в том, что на компьютере не установлены другие программы защиты от вирусов. Если на одном компьютере установлено два и более решения для защиты от вирусов, между ними может возникнуть конфликт. Рекомендуется удалить все прочие программы защиты от вирусов с компьютера. Список инструментов для удаления популярных антивирусных программ см. в нашей статье базы знаний (доступна на английском и на нескольких других языках).

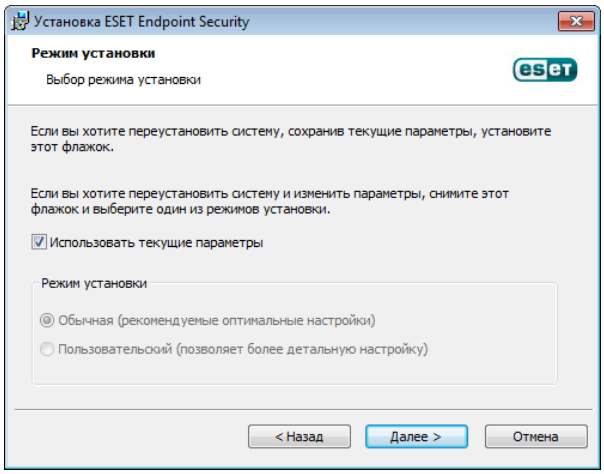


Сначала программа проверяет наличие более новой версии ESET Endpoint Security. При обнаружении более новой версии вы будете уведомлены об этом на первом этапе установки. Если выбрать возможность **Загрузить и установить новую версию**, новая версия будет загружена, после чего будет продолжена установка. На следующем этапе на экран будет выведено лицензионное соглашение с конечным пользователем. Прочтите его и нажмите кнопку **Принять**, чтобы подтвердить свое согласие с условиями лицензионного соглашения с конечным пользователем. После этого установка будет продолжена, причем существует два возможных сценария.

1. Если ESET Endpoint Security устанавливается на компьютер впервые, после принятия условий **лицензионного соглашения с конечным пользователем** на экран будет выведено показанное далее окно. Здесь можно выбрать режим установки (Обычная установка или Выборочная установка) и продолжить установку соответствующим образом.



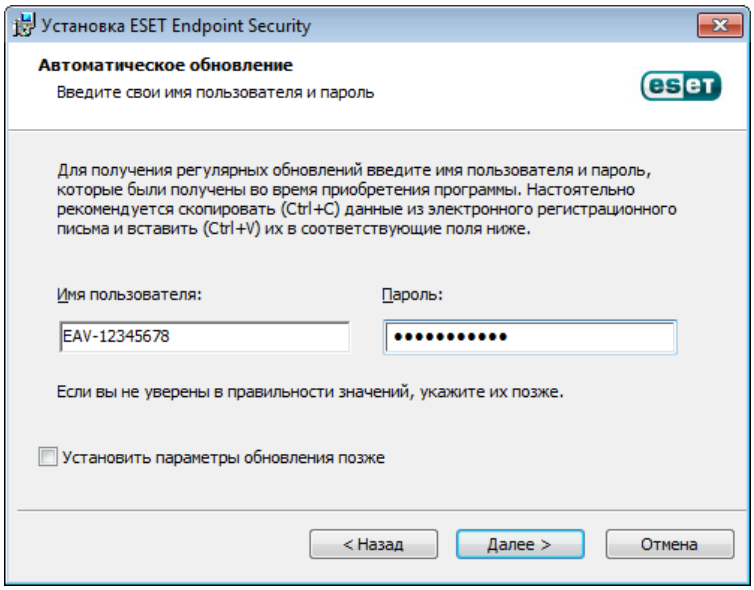
2. Если ESET Endpoint Security устанавливается поверх предыдущей версии данного программного обеспечения, в следующем окне вы можете выбрать, нужно ли сохранить существующие параметры для новой установки. Если же снять флажок **Использовать текущие параметры**, то вам будут доступны только два описанные выше варианта.



2.1 Обычная установка

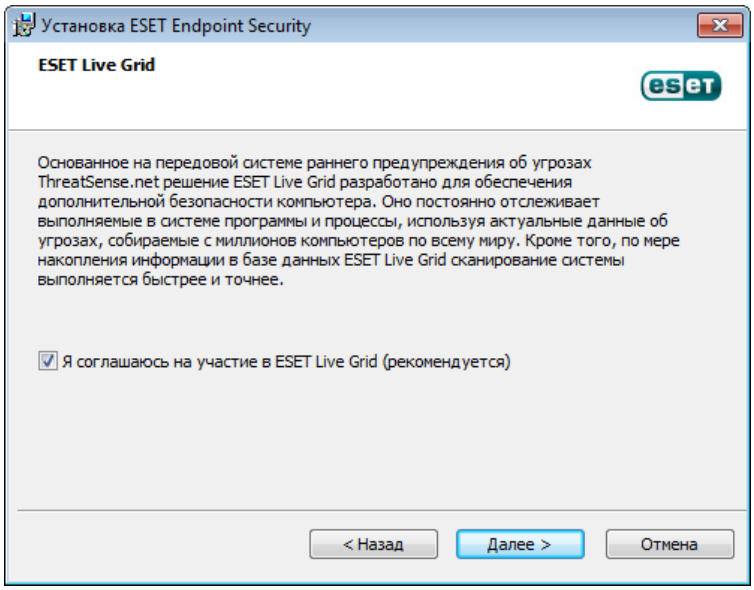
В режиме обычной установки предлагаются возможности для конфигурирования, достаточные для большинства пользователей. Эти параметры обеспечивают отличный уровень безопасности, простоту настройки и высокую производительность компьютера. Режим обычной установки — это вариант по умолчанию; при отсутствии особых требований не следует выбирать другой способ.

После выбора режима установки и нажатия кнопки **Далее** предлагается ввести имя пользователя и пароль для автоматического обновления программы. Это важно для обеспечения непрерывной защиты компьютера.



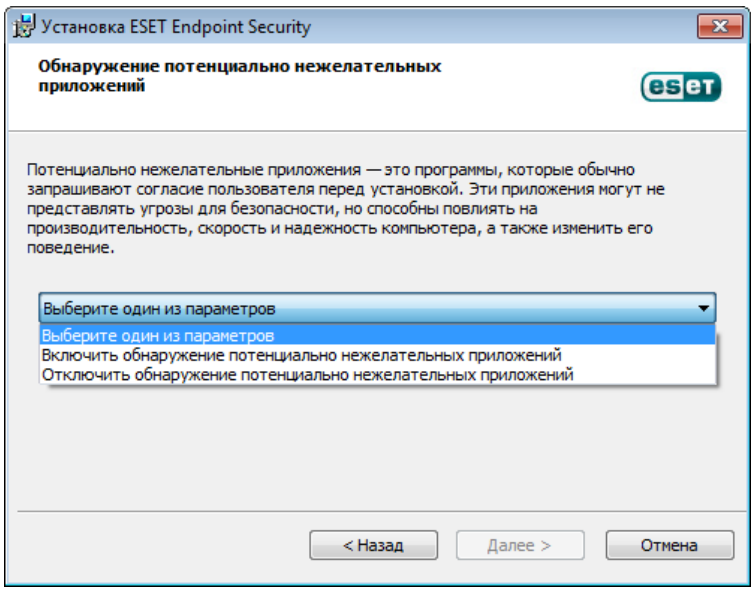
В соответствующих полях введите свои **имя пользователя** и **пароль**, то есть те самые данные аутентификации, которые были получены при приобретении или регистрации программы. Если у вас нет имени пользователя и пароля, установите флажок **Установить параметры обновления позже**. При этом учетные данные можно будет позднее ввести в самой программе.

На следующем этапе выполняется конфигурирование ESET Live Grid. Система ESET Live Grid предназначена для немедленного непрерывного информирования компании ESET о новых заражениях, что позволяет защищать пользователей. Эта система позволяет отправлять новые угрозы в вирусную лабораторию ESET, где они анализируются, обрабатываются и добавляются в базу данных сигнатур вирусов.

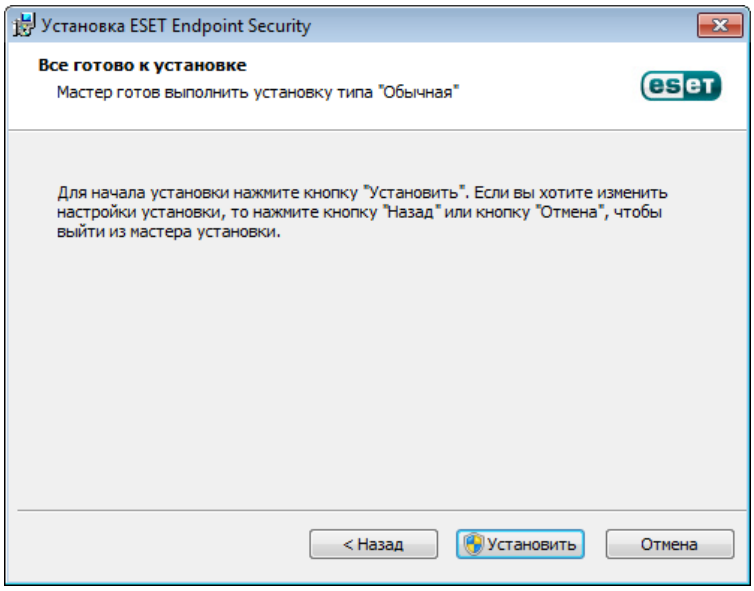


По умолчанию установлен флажок **Я соглашаюсь на участие в ESET Live Grid**, который активирует данную функцию.

Следующим действием при установке является конфигурирование обнаружения потенциально нежелательных приложений. Потенциально нежелательные приложения не обязательно являются вредоносными, но часто негативно влияют на работу операционной системы. Дополнительные сведения см. в главе Потенциально нежелательные приложения.



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



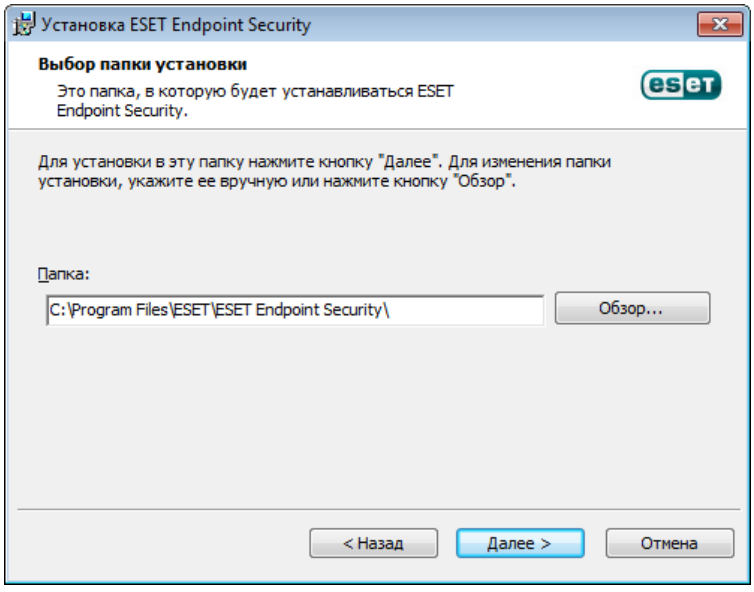
2.2 Выборочная установка

Режим выборочной установки предназначен для опытных пользователей, которые могут выполнить тонкую настройку программы и хотят изменить параметры расширенной настройки во время установки.

После выбора режима установки и нажатия кнопки **Далее** пользователю будет предложено выбрать папку для установки. По умолчанию программа устанавливается в указанную ниже папку.

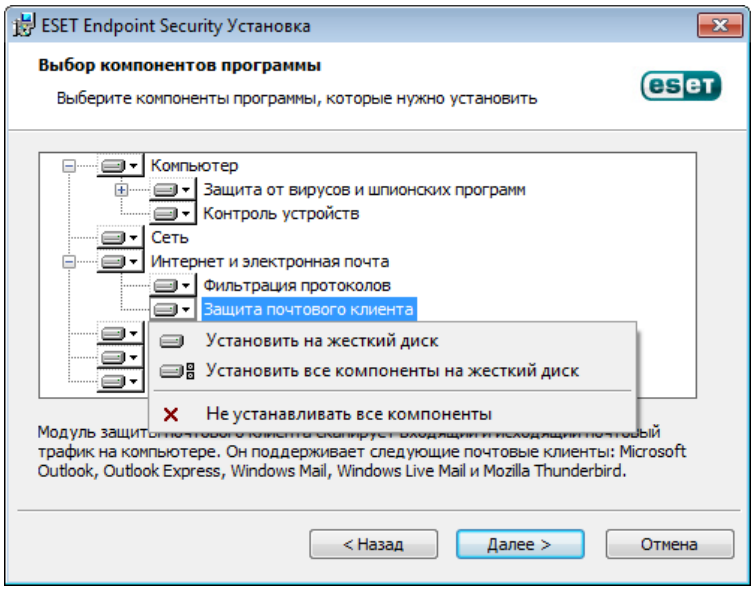
C:\Program Files\ESET\ESET Endpoint Security\

Нажмите кнопку **Обзор...**, чтобы изменить папку (не рекомендуется).

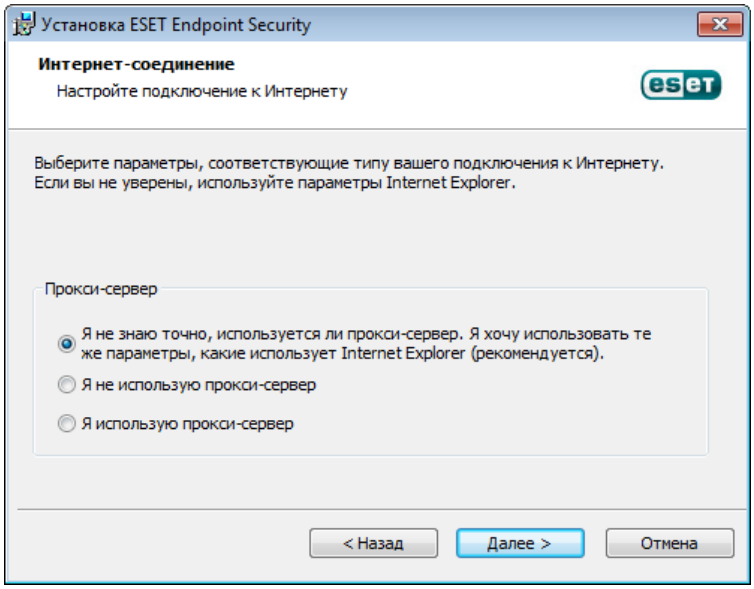


Затем заполните поля **Имя пользователя** и **Пароль**. Это действие аналогично соответствующему действию в режиме обычной установки (см. Обычная установка).

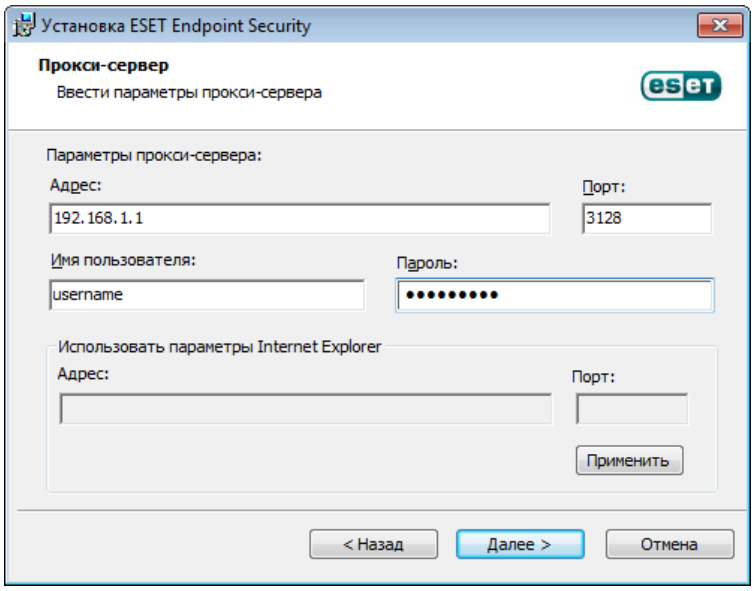
На следующем этапе нужно выбрать компоненты программы, которые требуется установить. Чтобы просмотреть варианты установки, разверните дерево компонентов и выберите функцию. По умолчанию выбран вариант **Установить на жесткий диск**. Если выбрать **Установить все компоненты на жесткий диск**, установлены будут все функции, относящиеся к выделенной ветви дерева. Чтобы отменить установку функции или компонента, выберите **Не устанавливать все компоненты**.



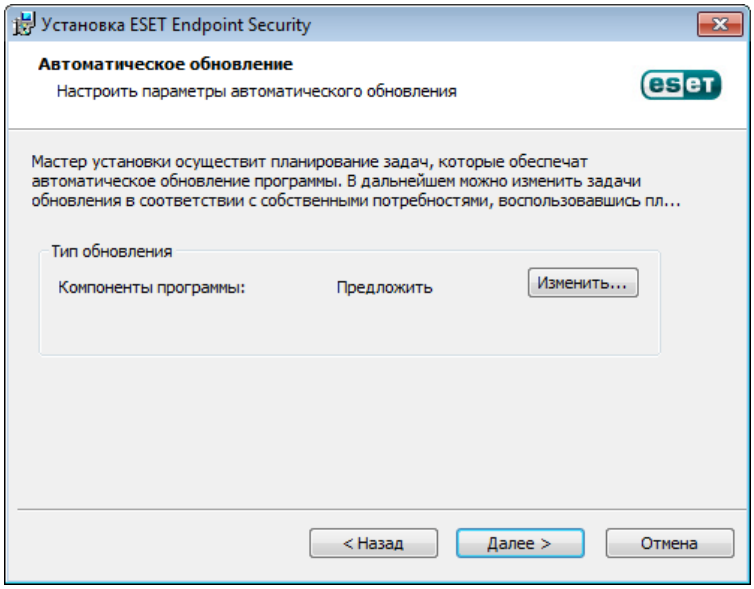
Нажмите кнопку **Далее**, чтобы перейти к настройке интернет-соединения. Если используется прокси-сервер, он должен быть корректно сконфигурирован для обеспечения обновления сигнатур вирусов. Если точно неизвестно, используется ли прокси-сервер для подключения к Интернету, выберите **Я не знаю точно, используется ли прокси-сервер. Я хочу использовать те же параметры, какие использует Internet Explorer (рекомендуется)** и нажмите кнопку **Далее**. Если прокси-сервер не используется, выберите вариант **Я не использую прокси-сервер**.



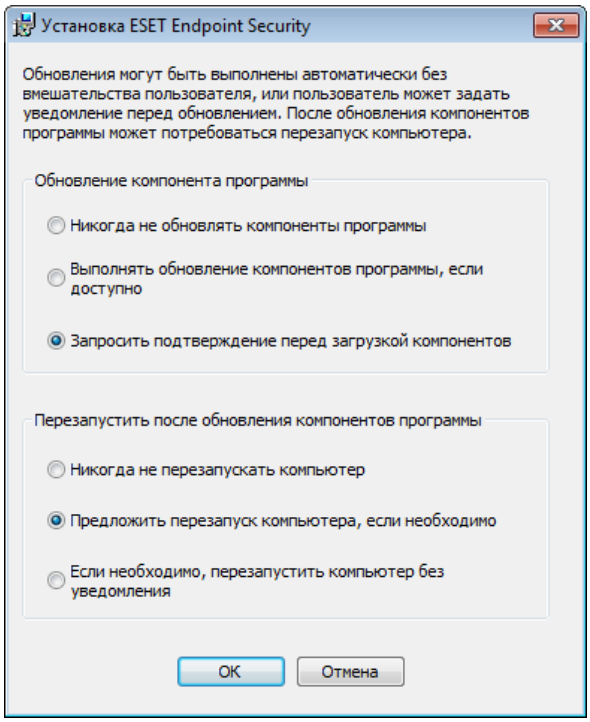
Для конфигурирования параметров прокси-сервера выберите вариант **Я использую прокси-сервер** и нажмите кнопку **Далее**. Введите IP-адрес или URL-адрес прокси-сервера в поле **Адрес**. В поле **Порт** укажите порт, по которому этот прокси-сервер принимает запросы на соединение (по умолчанию 3128). Если прокси-сервер требует аутентификации, введите правильные **имя пользователя** и **пароль**, которые необходимы для доступа к нему. Параметры прокси-сервера также по желанию могут быть скопированы из параметров Internet Explorer. Нажмите **Применить** и подтвердите выбор.



На этом этапе установки можно задать, как в системе будет обрабатываться автоматическое обновление программы. Нажмите **Изменить...** для доступа к расширенным параметрам.

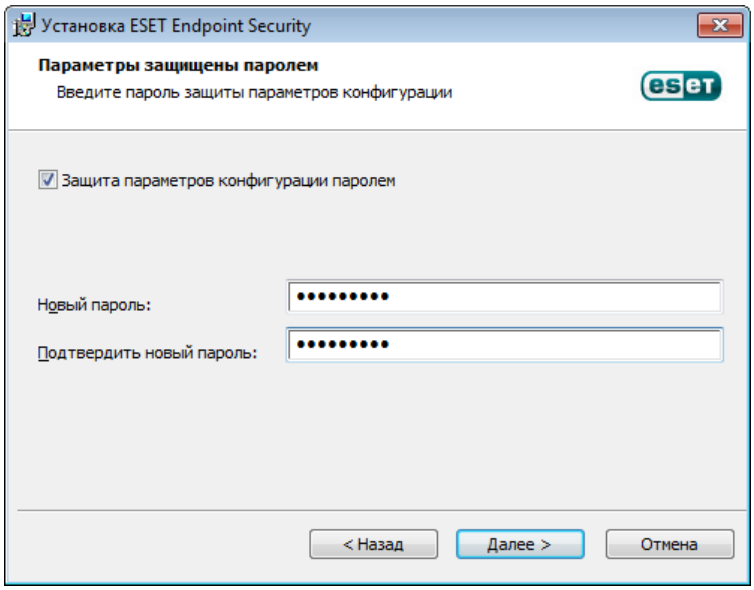


Если нет необходимости обновлять компоненты программы, выберите вариант **Никогда не обновлять компоненты программы**. Параметр **Запросить подтверждение перед загрузкой компонентов** включает вывод окна подтверждения перед каждой попыткой загрузить компоненты программы. Для автоматической загрузки обновлений компонентов программы выберите вариант **Выполнять обновление компонентов программы, если доступно**.



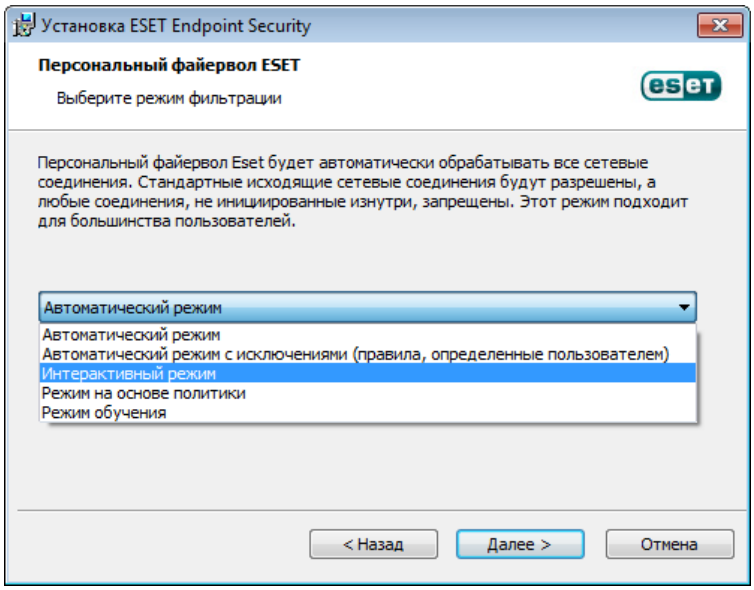
ПРИМЕЧАНИЕ. После обновления компонентов программы обычно нужно перезагрузить компьютер. Рекомендуется выбрать вариант **Если необходимо, перезапустить компьютер без уведомления**.

В следующем окне предлагается создать пароль для защиты параметров программы. Выберите вариант **Защита параметров конфигурации паролем** и введите пароль в поле **Новый пароль** и **Подтвердить новый пароль**. Он будет необходим для доступа к параметрам ESET Endpoint Security, а также для их изменения. Когда в обоих полях введены совпадающие пароли, нажмите кнопку **Далее**, чтобы продолжить.



Дальнейшие этапы **Автоматическое обновление**, **ESET Live Grid** и **Обнаружение потенциально нежелательных приложений** выполняются так же, как и при обычной установке (см. раздел Обычная установка).

Далее выберите режим фильтрации для персонального файервола ESET. В персональном файерволе ESET Endpoint Security существует пять режимов фильтрации. Поведение персонального файервола зависит от выбранного режима. Кроме того, от выбранного режима фильтрации зависит степень участия пользователя в процессе.



Нажмите **Установить** в окне **Все готово к установке**, чтобы завершить процесс установки. После завершения установки будет предложено активировать программный продукт. Для получения дополнительных сведений об активации программы см. раздел Обычная установка.

2.3 Ввод имени пользователя и пароля

Для того чтобы использовать программу наилучшим образом, необходимо регулярно обновлять ее. Это возможно только в том случае, если в окне **Настройка обновления** указаны правильные имя пользователя и пароль.

Если имя пользователя и пароль не указаны при установке, это возможно сделать сейчас. Нажмите сочетание клавиш **CTRL+U** и введите в окне «Информация о лицензии» данные о лицензии, полученные вместе с программой обеспечения безопасности ESET.

При вводе **имени пользователя** и **пароля** важно указывать их именно в том виде, в каком они получены.

- В имени пользователя и пароле учитывается регистр, в имени пользователя необходимо использовать дефис.
- Длина пароля равна десяти символам, причем все они написаны в нижнем регистре.
- В паролях не используется буква «L» (вместо нее нужно использовать цифру 1 (единица)).
- Прописная буква «O» на самом деле является нулем, тогда как строчная «o» — это и есть строчная «o».

Для обеспечения максимальной точности рекомендуется скопировать данные из регистрационного сообщения электронной почты и вставить их.

2.4 Обновление до новой версии

Более новые версии ESET Endpoint 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.

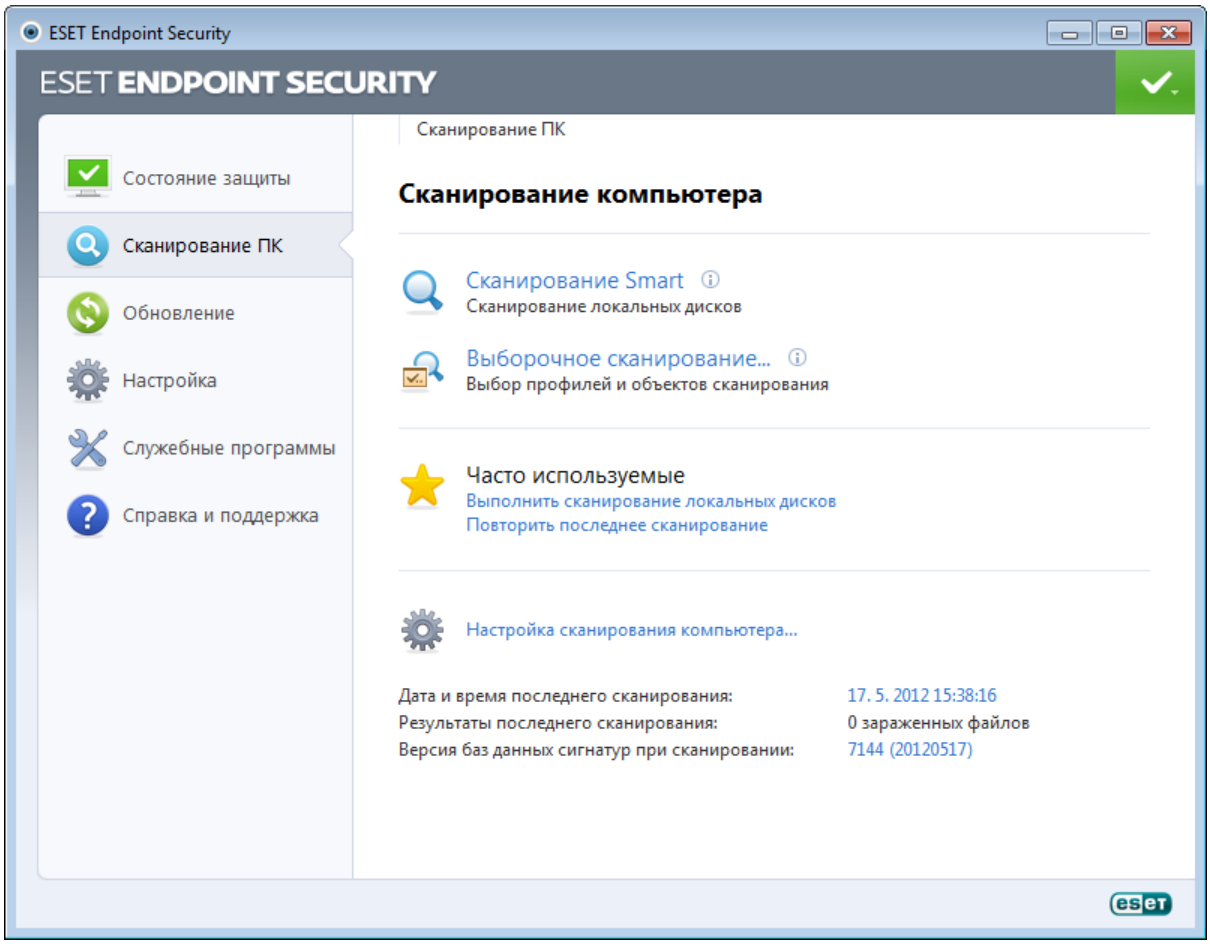
1. Автоматически путем обновления программы
   Поскольку обновления программы распространяются среди всех пользователей и могут повлиять на некоторые конфигурации компьютеров, они выпускаются только после длительного тестирования с целью обеспечения бесперебойной работы на всех возможных конфигурациях. Чтобы перейти на новую версию сразу после ее выпуска, воспользуйтесь одним из перечисленных ниже способов.

2. Вручную путем загрузки и установки новой версии поверх предыдущей.
   В начале процесса установки можно принять решение о сохранении существующих параметров программы. Для этого нужно установить флажок **Использовать текущие параметры**.

3. Вручную с автоматическим развертыванием в сетевой среде посредством ESET Remote Administrator

2.5 Сканирование компьютера

После установки ESET Endpoint Security следует выполнить сканирование компьютера для выявления злонамеренного кода. В главном окне программы выберите пункт **Сканирование компьютера**, а затем — **Сканирование Smart**. Для получения дополнительных сведений о сканировании компьютера см. раздел Сканирование компьютера.



3. Руководство для начинающих

В этом разделе приводятся общие сведения о программном обеспечении ESET Endpoint Security и его основных параметрах.

3.1 Общие сведения об интерфейсе пользователя

Главное окно ESET Endpoint 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 содержит сведения о состоянии защиты ESET Endpoint Security.

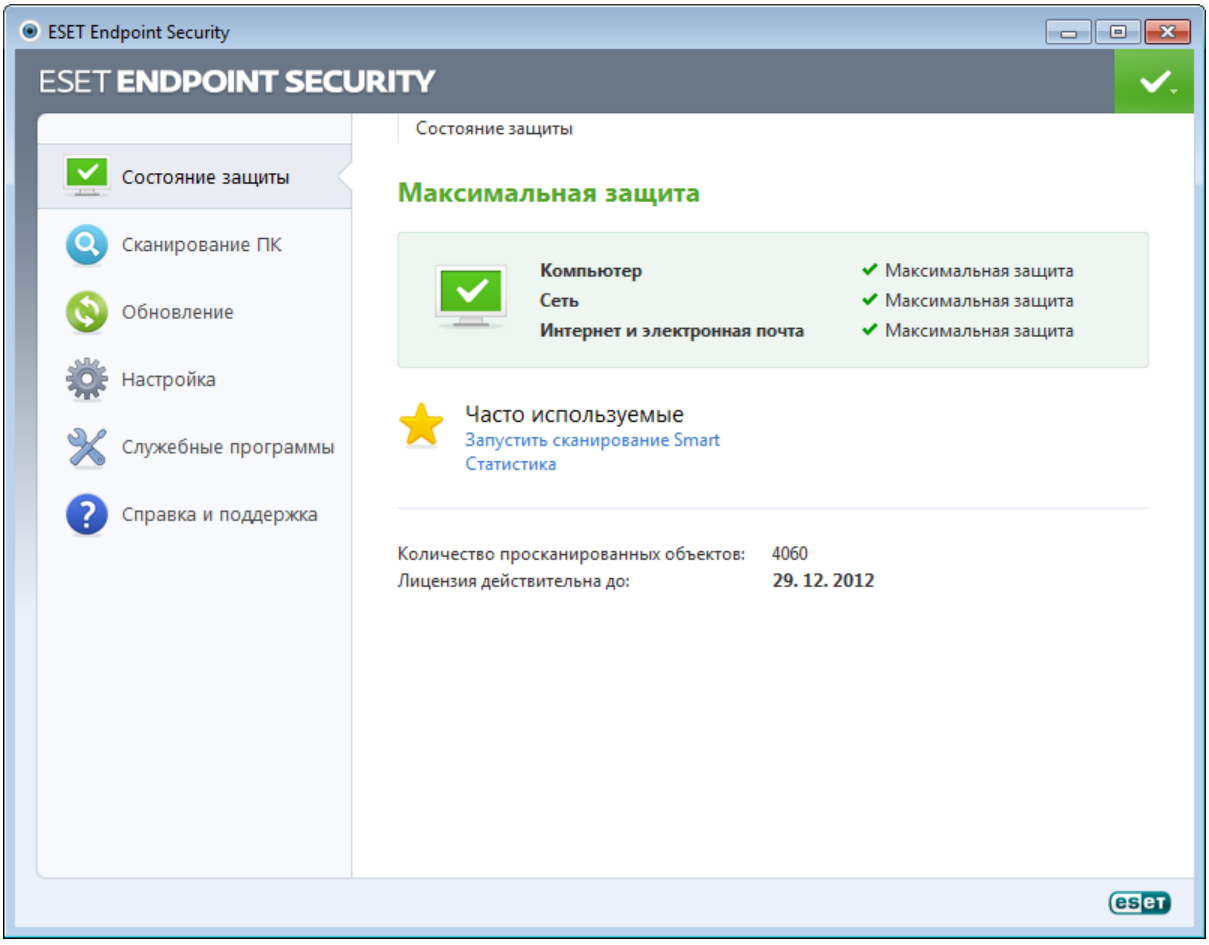
Сканирование компьютера: этот пункт позволяет сконфигурировать и запустить сканирование Smart или выборочное сканирование.

Обновление: выводит информацию об обновлениях базы данных сигнатур вирусов.

Настройка: этот пункт позволяет настроить уровень безопасности для компьютера, Интернета и электронной почты и сети .

Служебные программы: позволяет открыть файлы журнала, статистику защиты, программу мониторинга, запущенные процессы, сетевые подключения, планировщик, карантин, ESET SysInspector и ESET SysRescue.

Справка и поддержка: позволяет открыть файлы справки, базу знаний ESET, веб-сайт ESET, а также дает возможность воспользоваться ссылками, чтобы отправить запрос в службу поддержки клиентов.

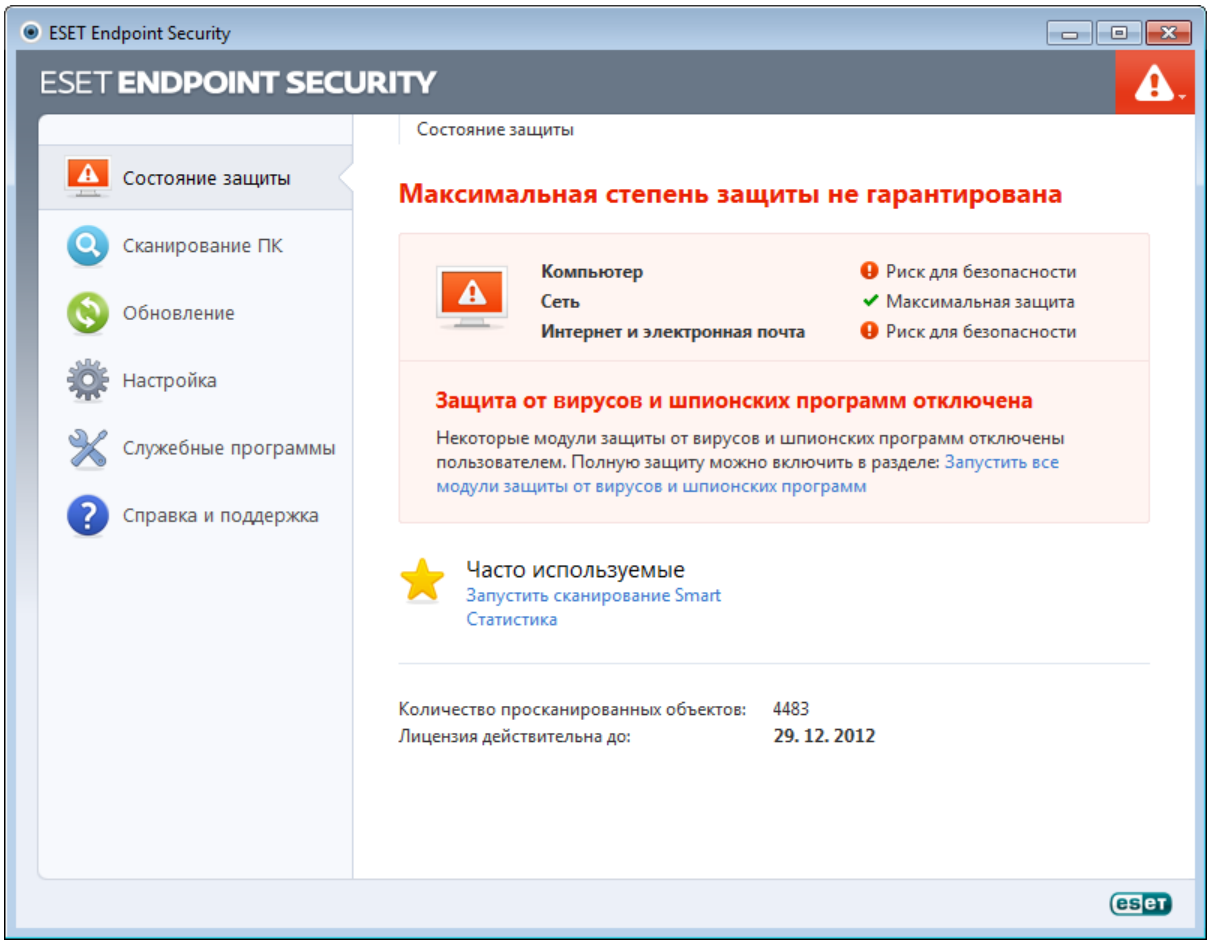


Окно **Состояние защиты** информирует пользователя об уровне безопасности и текущем уровне защиты компьютера. Зеленый значок **Максимальная защита** означает, что включена максимальная степень защиты.

В окне состояния также отображаются часто используемые функции ESET Endpoint Security. В этом же окне приводятся сведения о дате окончания срока действия лицензии на программу.

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

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



Красный значок показывает наличие критических проблем, из-за которых максимальная степень защиты компьютера не обеспечивается. Возможные причины:

- защита файловой системы в режиме реального времени отключена;
- персональный файервол отключен;
- устаревшая база данных сигнатур вирусов;
- программа не активирована;
- истек срок действия лицензии на программный продукт.

Оранжевый значок является признаком того, что отключена защита доступа в Интернет или защита почтового клиента, существуют проблемы с обновлением программы (устаревшая база данных сигнатур вирусов, невозможность выполнить обновление) или приближается дата окончания срока действия лицензии.

Защита от вирусов и шпионских программ отключена: эта проблема показывается красным значком и уведомлением о защите рядом с элементом **Компьютер**. Можно повторно включить защиту от вирусов и шпионских программ, щелкнув ссылку **Запустить все модули защиты от вирусов и шпионских программ**.

Защита доступа в Интернет отключена - Признаком этой проблемы является оранжевый значок с символом i и состояние **Уведомление о защите**. Вы можете повторно включить защиту доступа в Интернет щелкнув уведомление о защите, а затем **Включить защиту доступа в Интернет**.

Персональный файервол ESET отключен: эта проблема показывается красным значком и уведомлением о защите рядом с элементом **Сеть**. Для того чтобы повторно включить защиту сети, нажмите **Включить режим фильтрации**.

Срок действия вашей лицензии скоро закончится: признаком этой проблемы является появление восклицательного знака в значке состояния защиты. После окончания срока действия лицензии программа больше не сможет выполнять обновления, а значок состояния защиты станет красным.

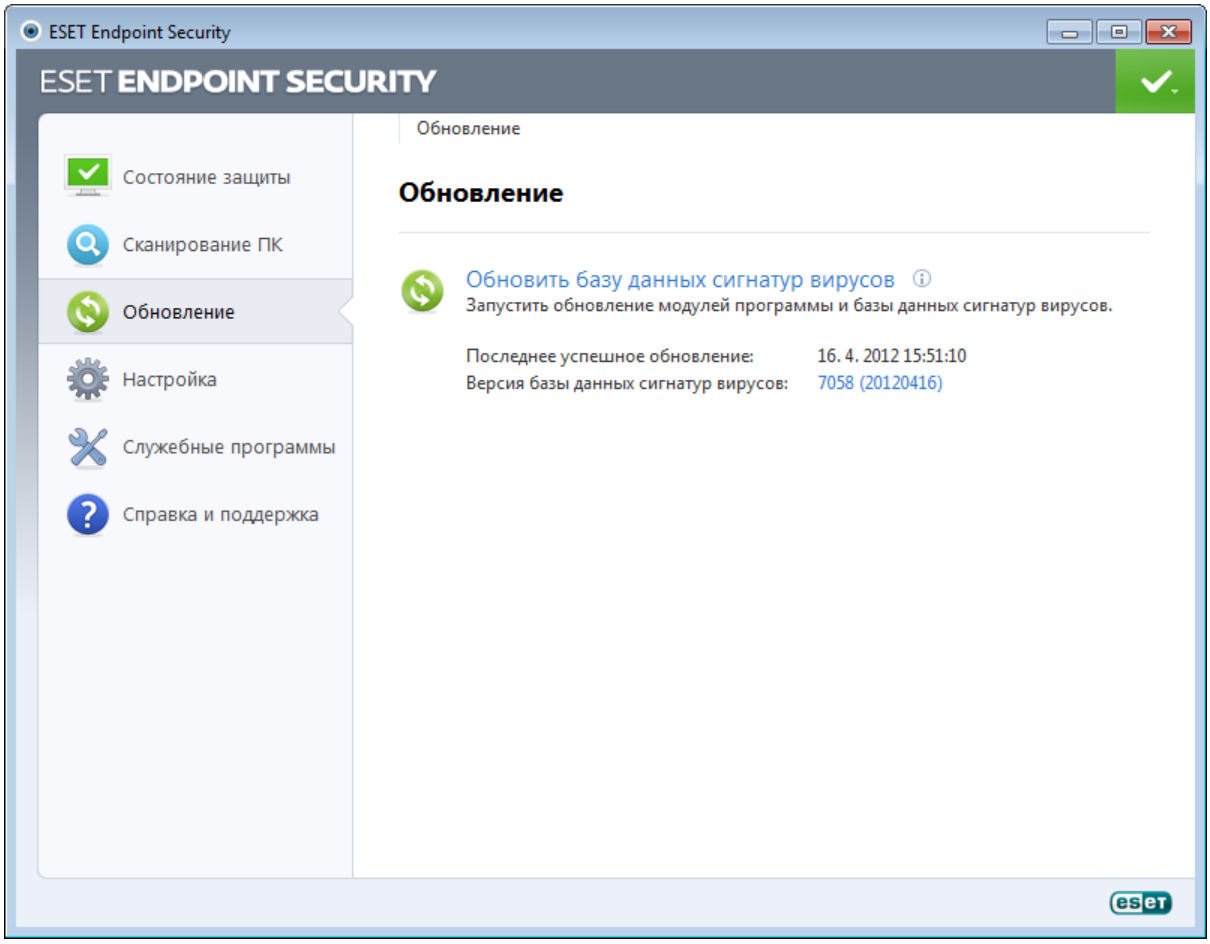
Срок действия лицензии истек: при возникновении этой проблемы значок состояния защиты становится красным. С этого момента программа больше не сможет выполнять обновления. Рекомендуется выполнить инструкции в окне предупреждения для продления лицензии.

Если предложенные решения не позволяют устранить проблему, выберите пункт **Справка и поддержка** для доступа к файлам справки или поиска в базе знаний ESET.. Если же проблему устранить по-прежнему не удается, можно отправить запрос в службу поддержки клиентов ESET. Ее специалисты оперативно ответят на ваши вопросы и помогут найти решение.

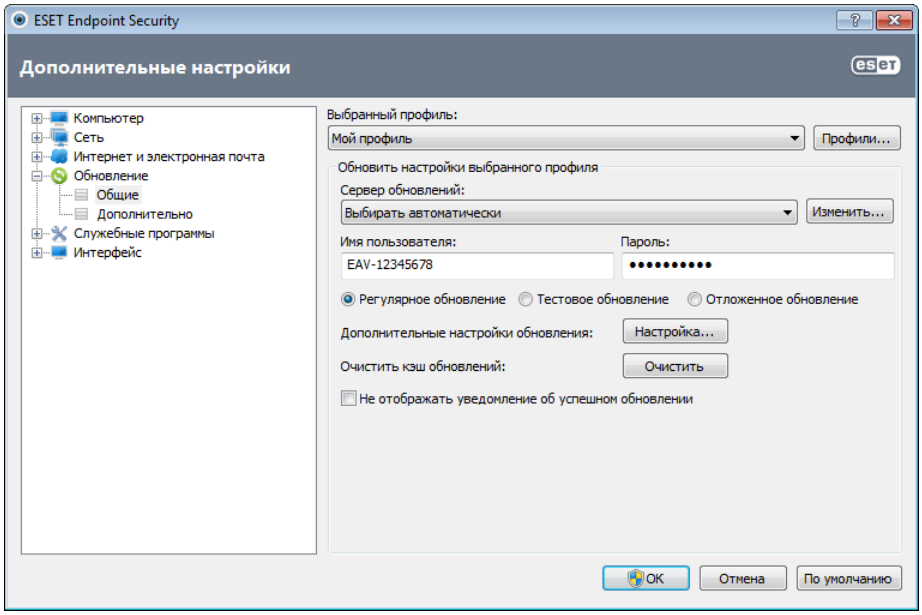
3.3 Настройка обновлений

Обновление базы данных сигнатур вирусов и компонентов программы является важнейшей частью обеспечения полной защиты компьютера от злонамеренного кода. Уделите особенное внимание изучению конфигурирования и работы этого процесса. В главном меню выберите пункт **Обновление**, после чего нажмите **Обновить базу данных сигнатур вирусов**, чтобы проверить наличие обновлений базы данных.

Если имя пользователя и пароль не указаны при установке ESET Endpoint Security, вам будет предложено сделать это на данном этапе.

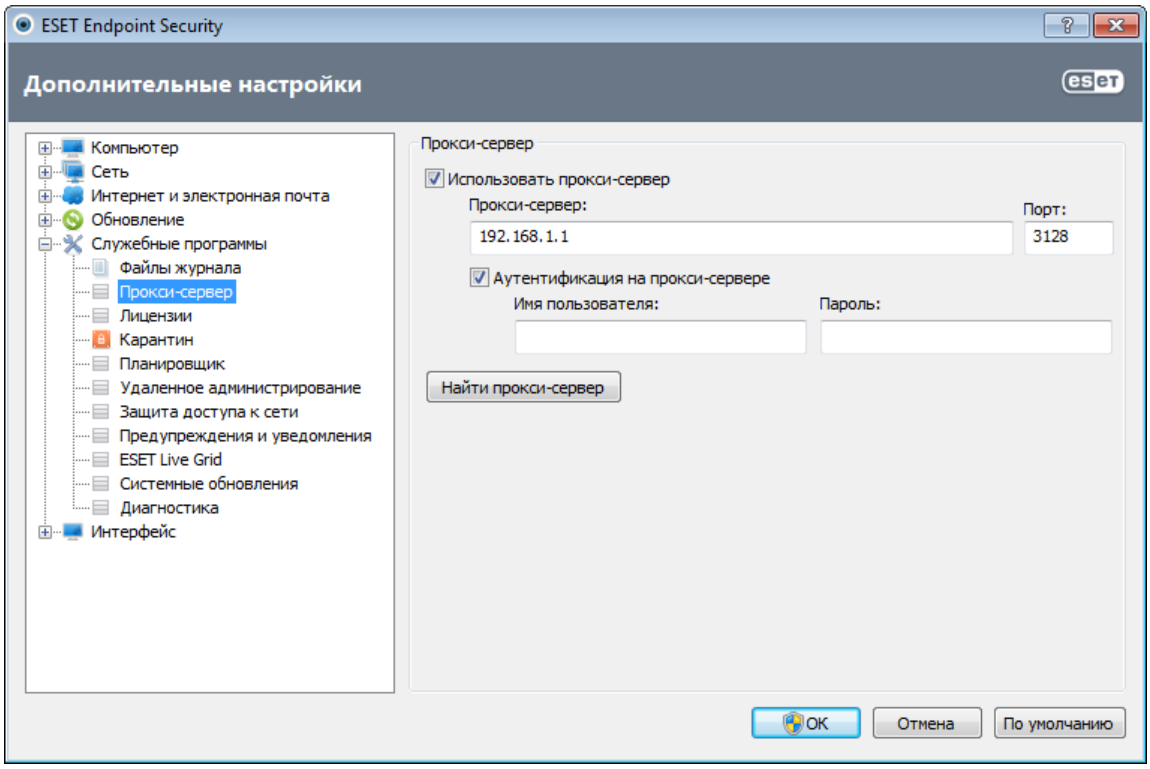


В окне «Дополнительные настройки» (выберите пункт **Настройка** в главном меню, после чего нажмите **Перейти к дополнительным настройкам** или F5 на клавиатуре) содержатся расширенные параметры обновления. Нажмите **Обновление** в дереве расширенных параметров в левой части окна. В раскрывающемся меню **Сервер обновлений** должен быть выбран пункт **Выбирать автоматически**. Для конфигурирования расширенных параметров обновлений, таких как режим обновления, доступ через прокси-сервер, подключения к локальной сети и создание копий сигнатур вирусов, нажмите кнопку **Настройка...**.



3.4 Настройка прокси-сервера

Если для управления подключениями к Интернету на компьютере, на котором используется ESET Endpoint Security, применяется прокси-сервер, это должно быть указано в разделе «Дополнительные настройки». Для доступа к окну настройки прокси-сервера нажмите клавишу F5, чтобы открыть окно «Дополнительные настройки», и выберите пункты **Служебные программы** > **Прокси-сервер** в дереве расширенных параметров. Выберите вариант **Использовать прокси-сервер**, а затем заполните поля **Прокси-сервер** (IP-адрес) и **Порт**. При необходимости установите флажок **Аутентификация на прокси-сервере**, а затем заполните поля **Имя пользователя** и **Пароль**.

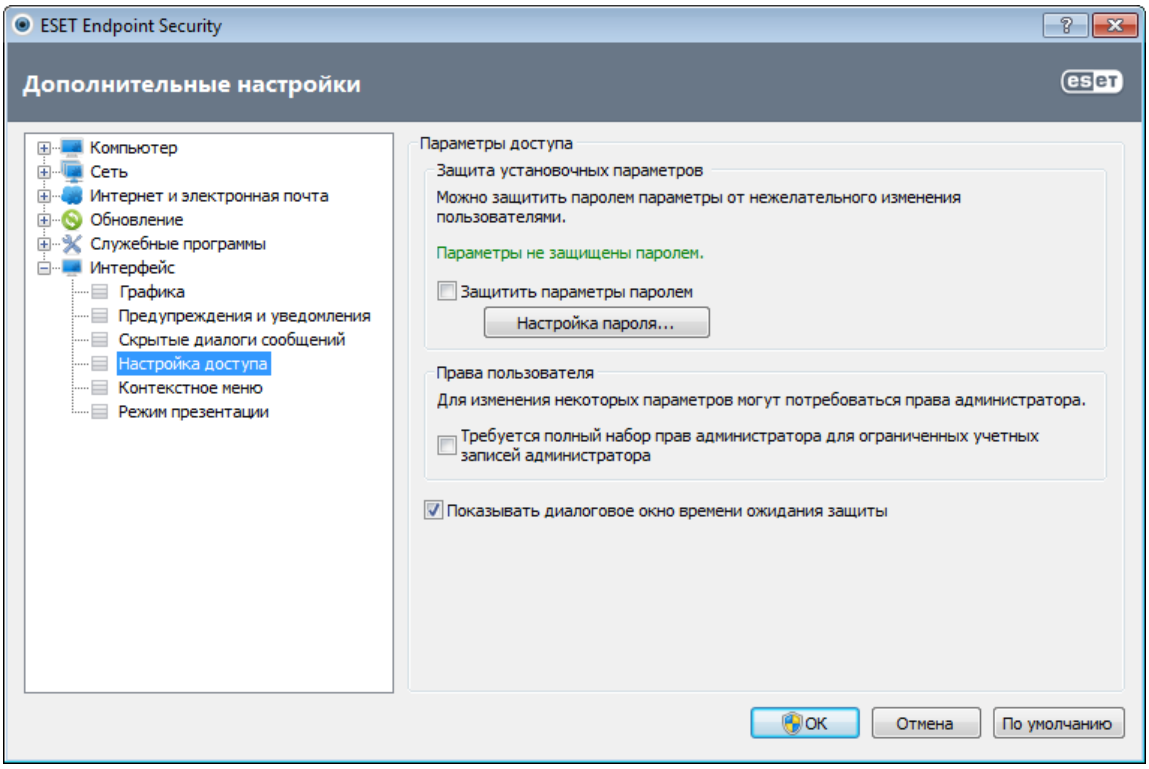


Если эта информация недоступна, можно попробовать автоматически обнаружить параметры прокси-сервера, нажав кнопку **Найти прокси-сервер**.

ПРИМЕЧАНИЕ. Параметры прокси-сервера для различных профилей обновления могут быть разными. В этом случае следует настроить разные профили обновления в разделе «Дополнительные настройки», выбрав для этого пункт **Обновление** в дереве расширенных параметров.

3.5 Защита настроек

Параметры ESET Endpoint Security могут иметь большое значение с точки зрения политики безопасности. Несанкционированное изменение параметров может нарушить стабильность работы системы и ослабить ее защиту. Для защиты установочных параметров паролем в главном меню выберите **Настройка** > **Перейти к дополнительным настройкам...** > **Интерфейс** > **Настройка доступа**, установите флажок **Параметры защищены паролем** и нажмите кнопку **Настройка пароля...**.

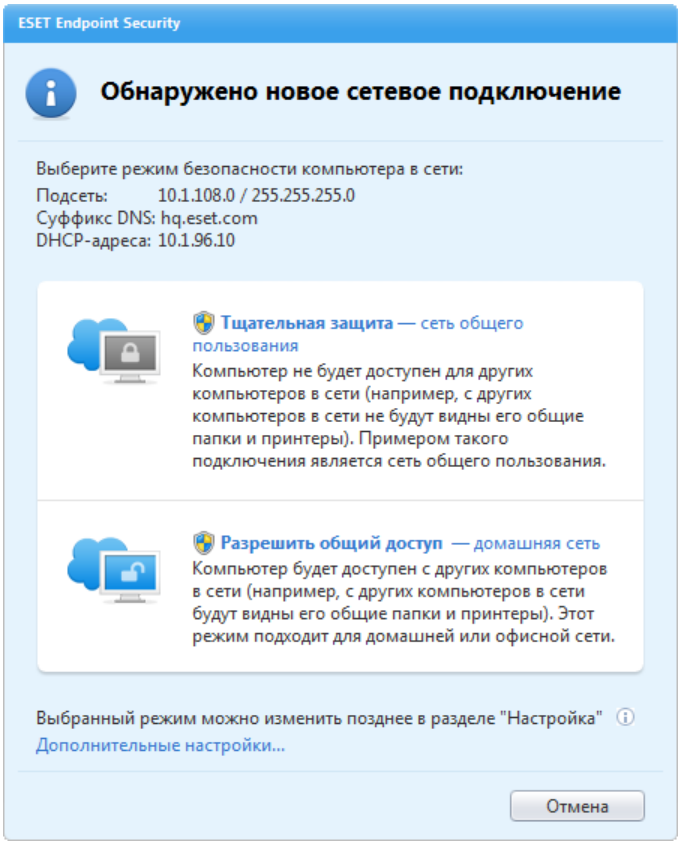


Введите пароль в поля **Новый пароль** и **Подтвердить новый пароль** и нажмите кнопку **ОК**. Этот пароль будет необходим для внесения любых изменений в настройки ESET Endpoint Security.

3.6 Настройка доверенной зоны

Необходимо сконфигурировать доверенную зону для защиты компьютера в сетевой среде. Настройка доверенной зоны для разрешения общего доступа дает возможность предоставить доступ другим пользователям к компьютеру. Нажмите **Настройка** > **Сеть** > **Изменить режим сетевой безопасности компьютера...**. На экран будет выведено окно, позволяющее выбрать нужный режим безопасности компьютера сети.

Обнаружение доверенной зоны происходит после установки ESET Endpoint Security и при каждом подключении компьютера к новой сети. Таким образом, обычно нет необходимости задавать доверенную зону. По умолчанию при обнаружении новой зоны на экран выводится диалоговое окно, позволяющее настроить уровень защиты для этой зоны.



Предупреждение. Неправильная настройка доверенной зоны может повлечь за собой снижение уровня безопасности компьютера.

ПРИМЕЧАНИЕ. По умолчанию рабочие станции из доверенной зоны получают доступ к файлам и принтерам, для которых открыт общий доступ, для них разрешены входящие соединения RPC, а также доступна служба удаленного рабочего стола.

4. Работа с ESET Endpoint Security

Параметры настройки ESET Endpoint Security дают пользователю возможность настраивать уровень защиты компьютера и сети.

Меню **Настройка** содержит перечисленные ниже параметры.

- **Компьютер**
- **Сеть**
- **Интернет и электронная почта**

Выберите защитный модуль, дополнительные параметры которого необходимо настроить.

В настройках защиты **Компьютер** можно включать и отключать следующие компоненты.

- **Защита файловой системы в режиме реального времени**: все файлы сканируются на наличие злонамеренного кода во время их открытия, создания или запуска.
- **Защита документов**: функция защиты документов сканирует документы Microsoft Office перед их открытием, а также проверяет файлы, автоматически загружаемые браузером Internet Explorer, такие как элементы Microsoft ActiveX.
- **Контроль устройств**: этот модуль позволяет сканировать, блокировать и изменять расширенные фильтры и разрешения, а также выбирать, как пользователь может получать доступ к конкретному устройству (компакт- или DVD-диску, USB-накопителю и т. д.) и работать с ним.
- **Система предотвращения вторжений на узел**: система предотвращения вторжений на узел отслеживает события в операционной системе и реагирует на них в соответствии с имеющимся набором правил.
- **Режим презентации**: включает или отключает режим презентации. На экран будет выведено предупреждающее сообщение (возможный риск для безопасности), а в оформлении главного окна будет применен оранжевый цвет после включения режима презентации.
- **Защита Anti-Stealth**: обнаружение опасных программ, таких как руткиты, которые способны скрывать свое присутствие от операционной системы. Это значит, что такие программы невозможно обнаружить с помощью обычных методов тестирования.

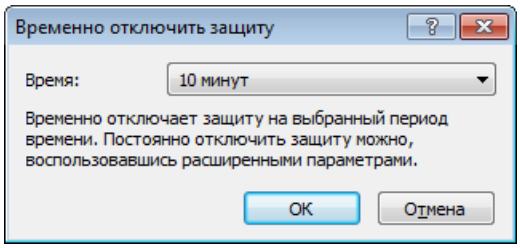
А разделе **Сеть** можно включать и отключать **Персональный файервол**.

В настройках защиты **Интернет и электронная почта** можно включать и отключать следующие компоненты.

- **Защита доступа в Интернет**: при включении этого параметра весь трафик по протоколам HTTP и HTTPS сканируется на наличие вредоносных программ.
- **Защита почтового клиента**: обеспечивает контроль обмена данными по протоколам POP3 и IMAP.
- **Защита от спама**: сканируются нежелательные сообщения, т. е. спам.
- **Контроль доступа в Интернет**: блокирование веб-страниц, которые могут содержать потенциально нежелательные материалы. Кроме того, работодатели или системные администраторы могут запрещать доступ к предварительно заданным категориям веб-сайтов (до 27).

ПРИМЕЧАНИЕ. Раздел «Защита документов» отображается на экране после активации параметра в разделе (**Перейти к дополнительным настройкам...** (F5) > **Компьютер** > **Защита от вирусов и шпионских программ** > **Защита документов** > **Интеграция с системой**).

Если нажать **Включено**, на экран будет выведено диалоговое окно **Временно отключить защиту**. Нажмите **ОК**, чтобы отключить выделенный компонент обеспечения безопасности. В раскрывающемся меню **Время** указывается период времени, на которое будет отключен выбранный компонент.



Для повторного включения защиты с помощью отключенного компонента безопасности нажмите **Отключено**.

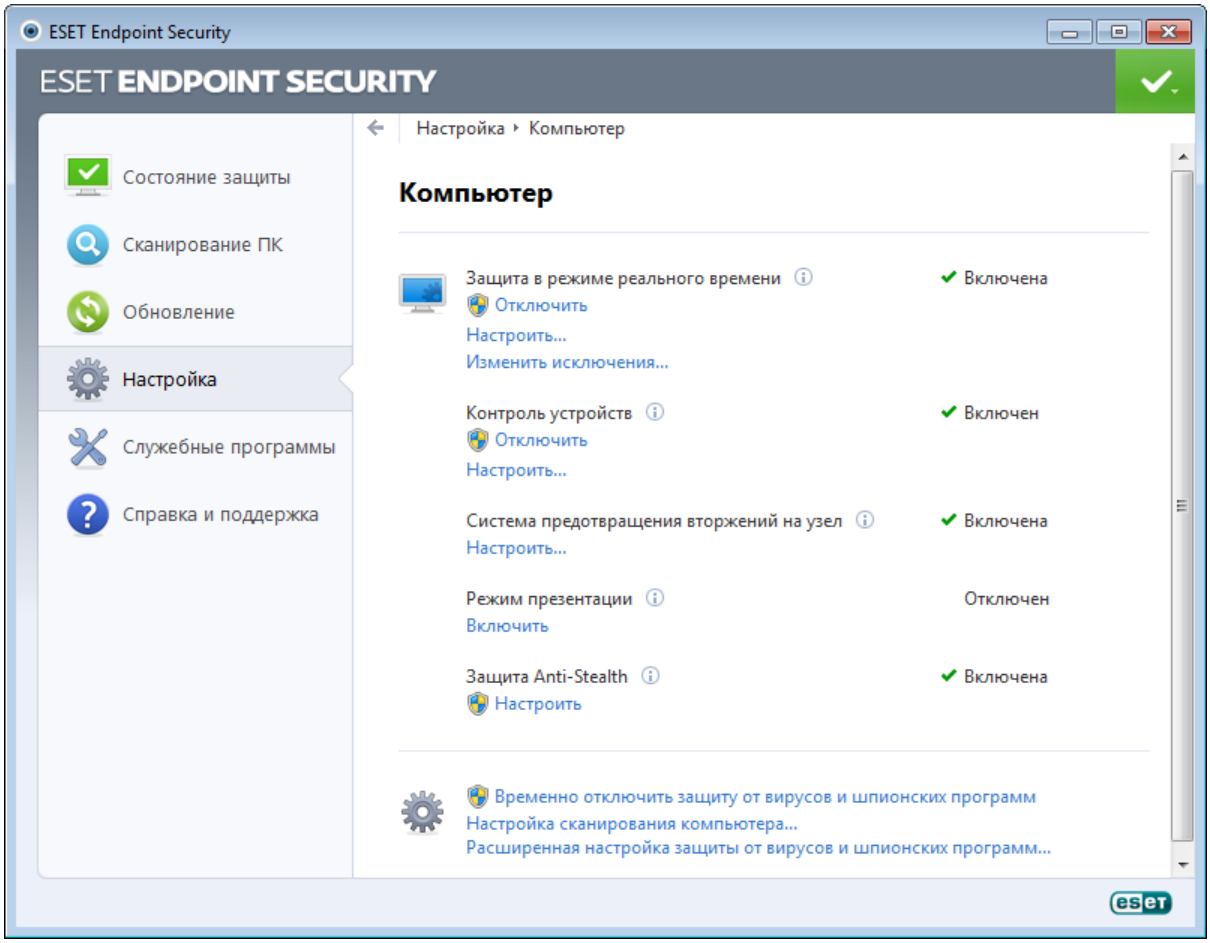
ПРИМЕЧАНИЕ. При отключении защиты таким методом все отключенные компоненты защиты будут повторно включены после перезагрузки компьютера.

В нижней части окна настройки есть дополнительные параметры. Чтобы загрузить параметры настройки из файла конфигурации в формате XML или сохранить текущие параметры настройки в файл конфигурации, воспользуйтесь функцией **Импорт и экспорт параметров...**.

4.1 Компьютер

Модуль **Компьютер** доступен на панели **Настройка**, которая появляется, если щелкнуть заголовок **Компьютер**. В этом окне представлена краткая информация обо всех модулях защиты. Чтобы временно отключить отдельный модуль, нажмите кнопку **Отключить** под названием нужного модуля. Обратите внимание, что при этом будет ослаблена защита вашего компьютера. Чтобы открыть подробные параметры для любого из модулей, нажмите кнопку **Настроить...**.

Нажмите **Изменить исключения...**, чтобы открыть окно настройки исключений, в котором можно исключить файлы и папки из сканирования.



Временно отключить защиту от вирусов и шпионских программ: отключение всех модулей защиты от вирусов и шпионских программ. На экран выводится диалоговое окно **Временно отключить защиту** с раскрывающимся меню **Время**. Раскрывающееся меню **Время** представляет период времени, на которое будет отключена защита. Нажмите кнопку **ОК** для подтверждения.

Настройка сканирования компьютера...: нажмите здесь, чтобы настроить параметры сканирования по требованию (сканирования, запускаемого вручную).

4.1.1 Защита от вирусов и шпионских программ

Защита от вирусов и шпионских программ предотвращает вредоносные атаки на компьютер путем контроля файлов, электронной почты и обмена данными 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.

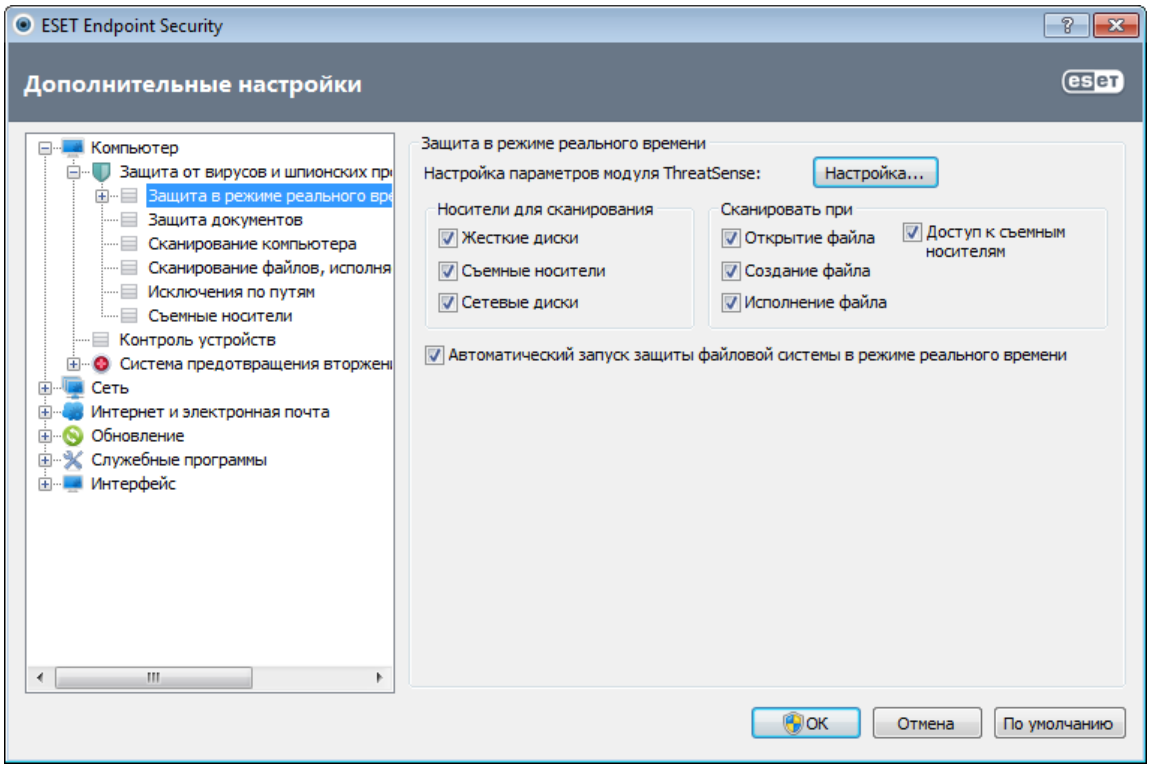
4.1.1.1 Защита файловой системы в режиме реального времени

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

Защита файловой системы в режиме реального времени проверяет все типы носителей и запускается различными событиями, такими как доступ к файлу. За счет использования методов обнаружения технологии ThreatSense (как описано в разделе Настройка параметров модуля ThreatSense) защита файловой системы в режиме реального времени может быть разной для 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 нажмите F5, чтобы открыть окно «Дополнительные настройки», и перейдите к разделу **Компьютер** > **Защита от вирусов и шпионских программ** > **Защита файловой системы в режиме реального времени** дерева расширенных параметров. Затем нажмите кнопку **Настройка...** рядом с пунктом **Настройка параметров модуля ThreatSense**, нажмите **Другое** и снимите или установите флажок **Включить оптимизацию Smart**.

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



4.1.1.1.1 Носители для сканирования

По умолчанию на наличие возможных угроз сканируются все типы носителей.

Локальные диски: контролируются все жесткие диски, существующие в системе.

Съемные носители: дискеты, компакт-/DVD-диски, 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).

4.1.1.1.2 Сканировать при (сканирование при определенных условиях)

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.

Открытие файла: включение и отключение сканирования открываемых файлов.

Создание файла: включает и отключает сканирование созданных или измененных файлов.

Исполнение файла: включение и отключение сканирования исполняемых файлов.

Доступ к съемным носителям: включение и отключение сканирования при доступе к конкретному съемному носителю, на котором могут храниться данные.

4.1.1.1.3 Расширенные параметры сканирования

Более подробные параметры настройки можно найти в разделе **Компьютер** > **Защита от вирусов и шпионских программ** > **Защита файловой системы 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 аналогичным показателем для существующих файлов. Именно поэтому программа проверяет эти файлы с дополнительными параметрами сканирования. Вместе с обычными методами сканирования, основанными на сигнатурах, применяется расширенная эвристика, что значительно улучшает уровень обнаружения, поскольку эвристический анализ делает возможным обнаружение новых угроз еще до выпуска обновлений базы данных сигнатур вирусов. 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 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 функции расширенной эвристики могут замедлить выполнение некоторых программ из-за повышения требований к системе. Если активирован параметр **Расширенная эвристика запуска файлов с внешних устройств** , то при необходимости исключить определенные съемные носители (например, USB-устройства) или порты из сканирования с применением расширенной эвристики запуска файлов, нажмите **Исключения...**, чтобы открыть окно исключения съемных носителей. Здесь можно настроить параметры, установив или сняв флажки, которые представляют каждый из портов.

4.1.1.1.4 Уровни очистки

Защита в режиме реального времени предусматривает три уровня очистки (для доступа к ним нажмите кнопку **Настройка...** в разделе **Защита файловой системы в режиме реального времени** и воспользуйтесь ветвью **Очистка**).

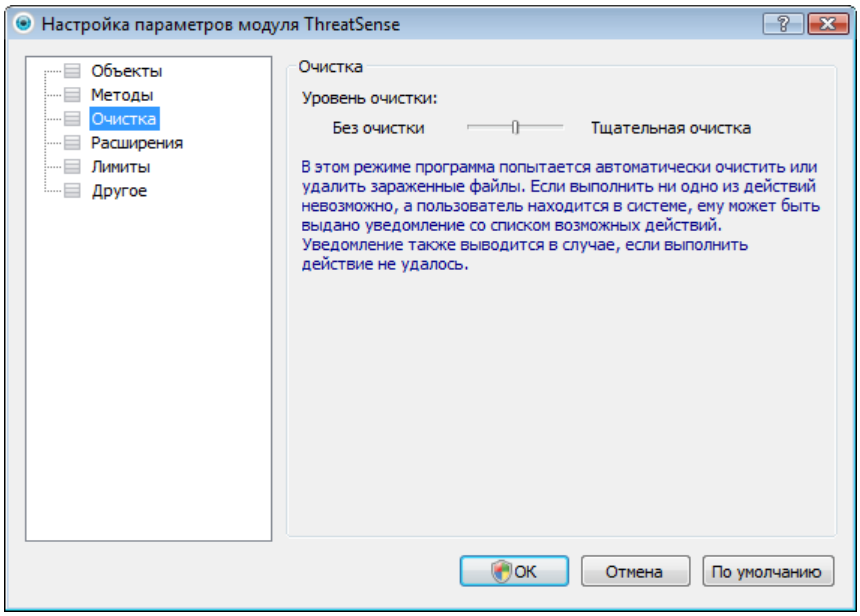
Без очистки: зараженные файлы не будут очищаться автоматически. Программа выводит на экран окно предупреждения и предлагает пользователю выбрать действие. Этот уровень предназначен для более опытных пользователей, которые знают о действиях, которые следует предпринимать в случае заражения.

Стандартная очистка: программа пытается автоматически очистить или удалить зараженный файл на основе предварительно определенного действия (в зависимости от типа заражения). Обнаружение и удаление зараженных файлов сопровождается информационным сообщением, располагающимся в правом нижнем углу

экрана. Если невозможно выбрать правильное действие автоматически, программа предложит пользователю выбрать действие. То же самое произойдет в том случае, если предварительно определенное действие невозможно выполнить.

Тщательная очистка: программа очищает или удаляет все зараженные файлы. Исключение составляют только системные файлы. Если очистка невозможна, на экран выводится окно предупреждения, в котором пользователю предлагается выполнить определенное действие.

Предупреждение. Если в архиве содержатся зараженные файлы, существует два варианта обработки архива. В стандартном режиме (при стандартной очистке) целиком удаляется архив, все файлы в котором заражены. В режиме **Тщательная очистка** удаляется архив, в котором заражен хотя бы один файл, независимо от состояния остальных файлов.



4.1.1.1.5 Момент изменения конфигурации защиты в режиме реального времени

Защита в режиме реального времени является наиболее существенным элементом всей системы обеспечения безопасности. 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 Endpoint Security все параметры оптимизированы для максимальной защиты системы. Для восстановления параметров по умолчанию нажмите кнопку **По умолчанию**, расположенную в правом нижнем углу окна **Защита файловой системы в режиме реального времени** (**Дополнительные настройки** > **Компьютер** > **Защита от вирусов и шпионских программ** > **Защита файловой системы в режиме реального времени**).

4.1.1.1.6 Проверка модуля защиты в режиме реального времени

Для того чтобы проверить функционирование защиты файловой системы в режиме реального времени, используйте проверочный файл eicar.com. Этот файл содержит безвредный код, который, однако, 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 необходимо отключить файервол. Если файервол включен, он обнаружит данный файл и предотвратит его загрузку.

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

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

Защита файловой системы в режиме реального времени отключена

Если защита файловой системы в режиме реального времени непреднамеренно была отключена пользователем, ее нужно включить. Для повторной активации защиты в режиме реального времени перейдите в раздел **Настройка** и в главном окне программы нажмите **Защита файловой системы в режиме реального времени**.

Если защита файловой системы в режиме реального времени не запускается при загрузке операционной системы, обычно это связано с тем, что отключен параметр **Автоматический запуск защиты файловой системы в режиме реального времени**. Чтобы установить этот флажок, перейдите в раздел «Дополнительные настройки» (F5) и нажмите **Компьютер** > **Защита от вирусов и шпионских программ** > **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 от вирусов могут возникнуть конфликты. Рекомендуется удалить все прочие программы защиты от вирусов с компьютера.

Защита файловой системы в режиме реального времени на запускается

Если защита не запускается при загрузке системы, но функция **Автоматический запуск защиты файловой системы в режиме реального времени** включена, возможно, возник конфликт с другими приложениями. В этом случае обратитесь за консультацией в службу поддержки клиентов ESET.

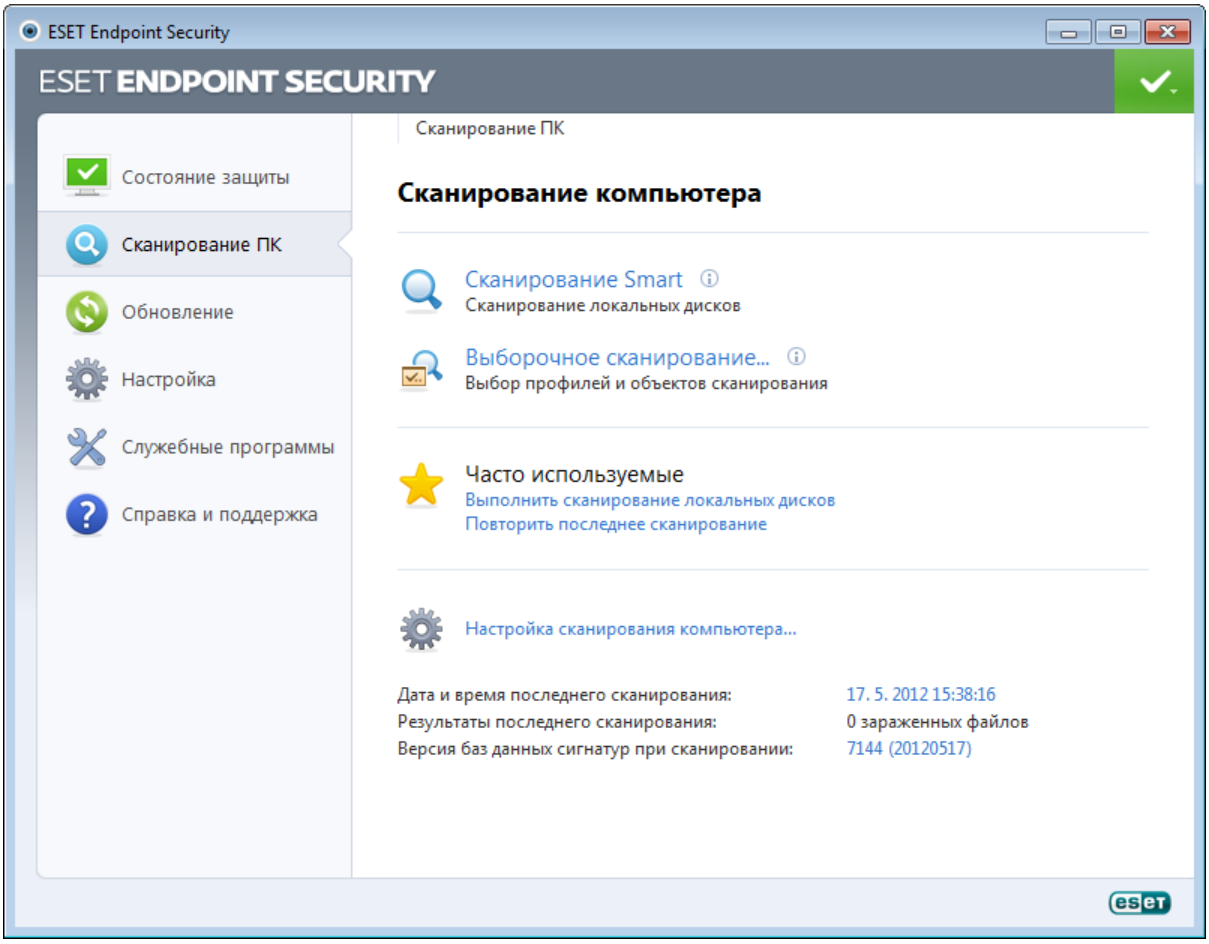
4.1.1.2 Защита документов

Функция защиты документов сканирует документы Microsoft Office перед их открытием, а также проверяет файлы, автоматически загружаемые браузером Internet Explorer, такие как элементы Microsoft ActiveX. Параметр **Интеграция с системой** активирует систему защиты. Для изменения этого параметра нажмите F5, чтобы открыть окно «Дополнительные настройки», и перейдите к разделу **Компьютер** > **Защита от вирусов и шпионских программ** > **Защита документов** дерева расширенных параметров. При активации этого параметра защита документов становится доступна из главного окна ESET Endpoint Security в разделе **Настройка** > **Компьютер**.

Эта функция активируется приложениями, в которых используется Microsoft Antivirus API (например, Microsoft Office 2000 и более поздних версий или Microsoft Internet Explorer 5.0 и более поздних версий).

4.1.1.3 Сканирование компьютера

Модуль сканирования компьютера по требованию является важной частью решения, обеспечивающего защиту от вирусов. Он используется для сканирования файлов и папок на компьютере. С точки зрения обеспечения безопасности принципиально важно выполнять сканирование компьютера регулярно, а не только при возникновении подозрений. Рекомендуется регулярно выполнять полное сканирование компьютера для обнаружения вирусов, которые не были найдены защитой файловой системы в режиме реального времени при записи на диск. Это может произойти, если в тот момент защита файловой системы в режиме реального времени была отключена, база данных вирусов была устаревшей или же файл не был распознан как вирус при сохранении на диск.



Доступно два типа **сканирования ПК**. **Сканирование Smart** позволяет быстро просканировать систему без настройки каких-либо параметров. Тип **Выборочное сканирование** позволяет выбрать предопределенный профиль сканирования и указать объекты, которые нужно проверить.

См. главу Ход сканирования для получения дополнительных сведений о процессе сканирования.

Рекомендуется запускать сканирование компьютера не реже одного раза в месяц. Можно сконфигурировать сканирование в качестве запланированной задачи в разделе **Служебные программы** > **Планировщик**.

4.1.1.3.1 Тип сканирования

4.1.1.3.1.1 Сканирование Smart

Сканирование Smart позволяет быстро запустить сканирование компьютера и очистить зараженные файлы без вмешательства пользователя. Преимущество сканирования Smart заключается в том, что оно удобно в выполнении и не требует тщательного конфигурирования 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.

4.1.1.3.1.2 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 применять, 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, 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**.

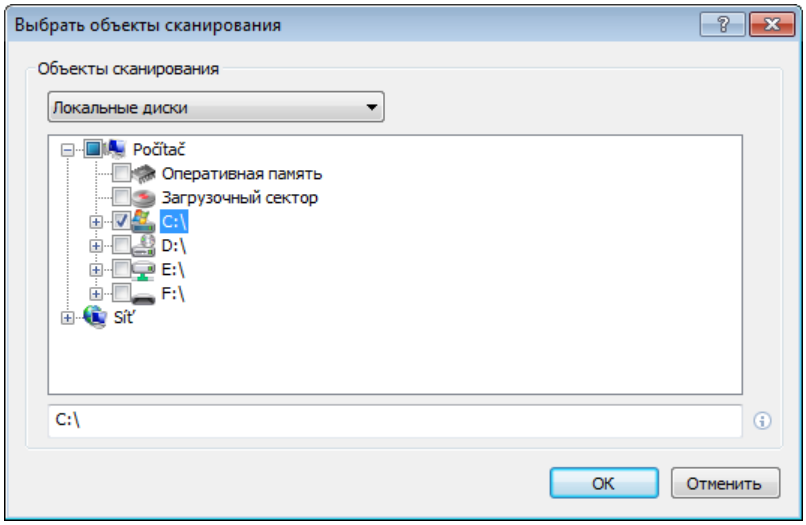
Пользователям, не имеющим достаточного опыта работы с антивирусными программами, не рекомендуется выполнять выборочное сканирование.

4.1.1.3.2 Объекты сканирования

Окно «Объекты сканирования» позволяет определить, какие объекты (оперативная память, жесткие диски, секторы, файлы и папки) будут сканироваться для выявления заражений. В раскрывающемся меню **Объекты сканирования** можно выбрать предварительно определенные объекты сканирования.

- **По параметрам профиля**: выбираются объекты, указанные в выделенном профиле сканирования.
- **Съемные носители**: выбираются дискеты, USB-устройства хранения, компакт- и DVD-диски.
- **Локальные диски**: выбираются все жесткие диски, существующие в системе.
- **Сетевые диски**: выбираются все подключенные сетевые диски.
- **Не выбрано**: отменяется выбор объектов.

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



Для быстрого перехода к какому-либо объекту сканирования или добавления его непосредственно укажите нужный объект в пустом поле под списком папок. Это возможно только в том случае, если в древовидной структуре не выбраны никакие объекты, а в меню **Объекты сканирования** выбран пункт **Не выбрано**.

4.1.1.3.3 Профили сканирования

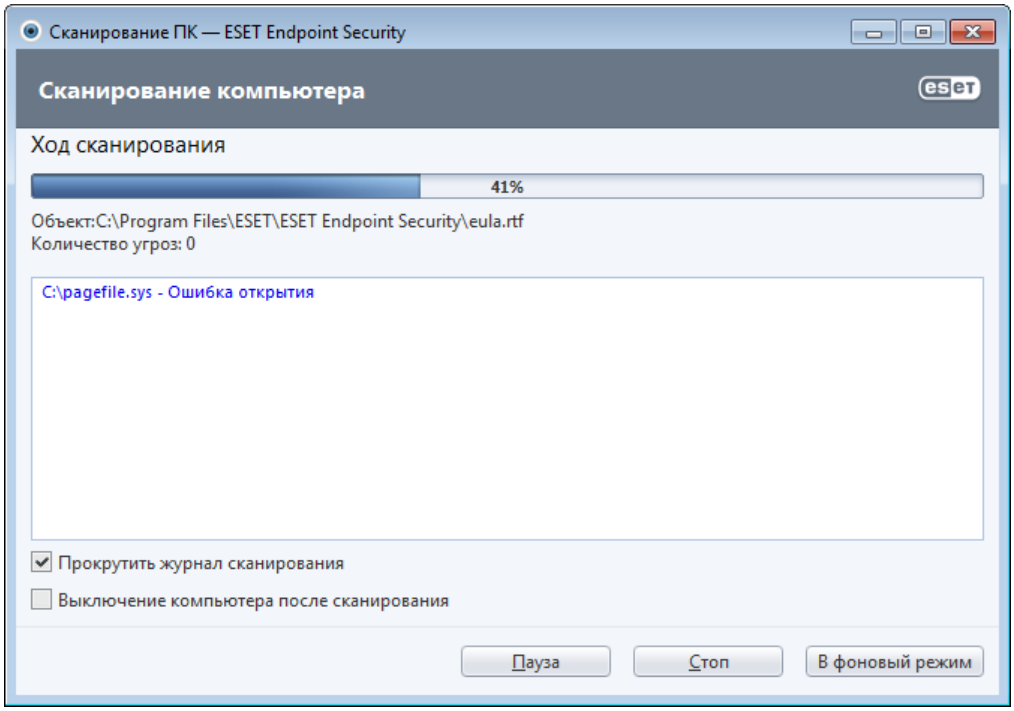
Предпочтительные параметры сканирования можно сохранить для использования в дальнейшем. Рекомендуется создать отдельный профиль для каждого регулярно используемого сканирования (с различными объектами, методами сканирования и прочими параметрами).

Для создания профиля откройте окно «Дополнительные настройки» (F5) и нажмите **Компьютер** > **Защита от вирусов и шпионских программ** > **Сканирование компьютера** > **Профили...**. В окне **Профили конфигурации** есть раскрывающееся меню **Выбранный профиль**, в котором перечисляются существующие профили сканирования и 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.

4.1.1.3.4 Ход сканирования

В окне хода сканирования отображается текущее состояние сканирования и информация о количестве файлов, в которых обнаружен злонамеренный код.



ПРИМЕЧАНИЕ. Нормально, что некоторые файлы, такие как защищенные паролем файлы или файлы, используемые исключительно операционной системой (обычно pagefile.sys и некоторые файлы журналов), не могут сканироваться.

Ход сканирования: индикатор выполнения показывает процентное отношение уже просканированных объектов к оставшимся. Значение получается на основе общего количества объектов, включенных в сканирование.

Объект: имя объекта, который сканируется в настоящий момент, и его расположение.

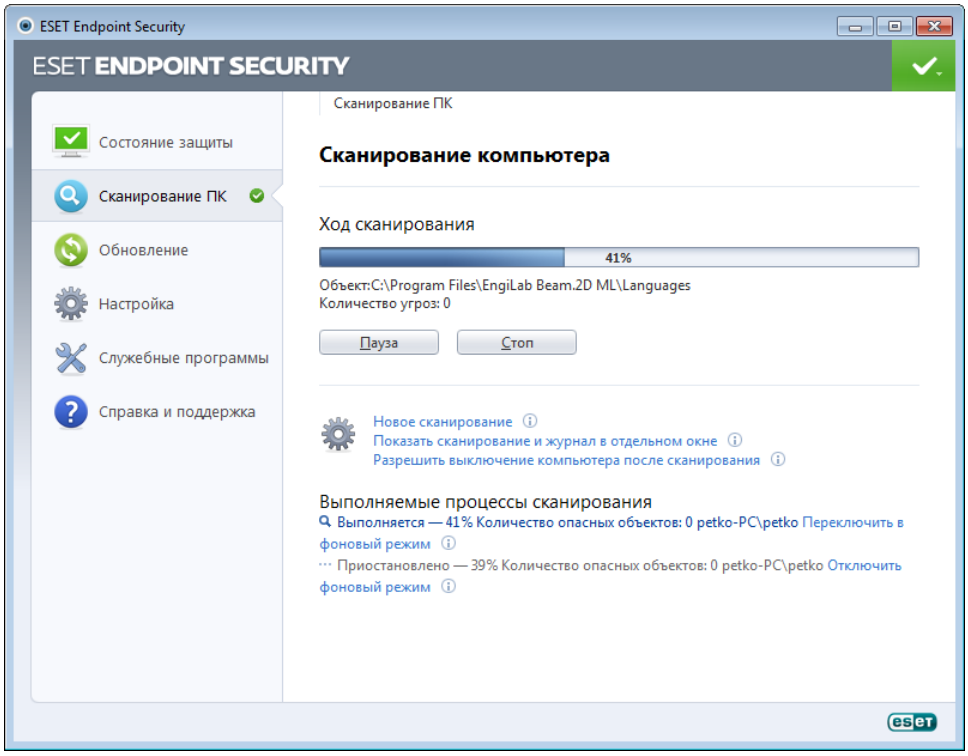
Количество угроз: общее количество угроз, обнаруженных при сканировании.

Пауза: приостановка сканирования.

Продолжить: эта возможность становится доступна после приостановки выполнения сканирования. Нажмите **Продолжить**, чтобы возобновить сканирование.

Остановить: прекращение сканирования.

В фоновый режим: можно выполнить еще одно параллельное сканирование. В таком случае уже выполняемое сканирование будет свернуто и выполняться в фоновом режиме.



Нажмите **Отключить фоновый режим** чтобы отключить фоновый режим и вернуться к процессу сканирования.

Прокрутить журнал сканирования: если этот параметр активирован, журнал сканирования будет прокручиваться автоматически при добавлении новых записей, чтобы были видны самые свежие элементы.

Разрешить выключение компьютера после сканирования: включает запланированное завершение работы по завершении сканирования компьютера по требованию. На экран будет выведено диалоговое окно подтверждения завершения работы. Оно будет активно в течение 60 секунд, когда можно будет отменить выключение компьютера. Нажмите **Отмена**, если нужно отменить завершение работы.

4.1.1.4 Сканирование файлов, исполняемых при запуске системы

При загрузке компьютера и обновлении базы данных сигнатур вирусов автоматически проверяются файлы, исполняемые при запуске системы. Это сканирование зависит от конфигурации и задач планировщика.

Сканирование файлов, исполняемых при запуске системы, входит в задачу планировщика **Проверка файлов, исполняемых при запуске системы**. Чтобы изменить параметры сканирования, перейдите в раздел **Служебные программы** > **Планировщик**, выберите параметр **Автоматическая проверка файлов при запуске системы** и нажмите кнопку **Изменить...**. На последнем этапе отобразится диалоговое окно Автоматическая проверка файлов при запуске системы (дополнительные сведения см. в следующем разделе).

Более подробные инструкции по созданию задач в планировщике и управлению ими см. в разделе Создание новой задачи.

4.1.1.4.1 Автоматическая проверка файлов при запуске системы

Раскрывающееся меню **Уровень сканирования**: задает глубину сканирования для файлов, загружаемых при запуске системы. Ниже перечислены значения этого параметра, определяющие количество сканируемых файлов (по возрастанию).

- **Только наиболее часто используемые файлы** (наименьшее количество сканируемых файлов)
- **Часто используемые файлы**
- **Обычно используемые файлы**
- **Редко используемые файлы**
- **Все зарегистрированные типы файлов** (наибольшее количество сканируемых файлов)

Также существуют две особые группы **уровней сканирования**.

- **Файлы, запускающиеся перед входом пользователя**: содержит файлы из таких папок, которые позволяют выполнение файлов без входа пользователя в систему (в том числе большинство элементов, исполняемых при запуске системы: службы, объекты модуля поддержки браузера, уведомления Winlogon, задания в планировщике Windows, известные библиотеки DLL и т. д.).
- **Файлы, запускающиеся после входа пользователя**: содержит файлы из таких папок, которые позволяют выполнение файлов только после входа пользователя в систему (в том числе элементы, запускаемые под конкретными учетными записями: обычно файлы из папки HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows\CurrentVersion\Run).

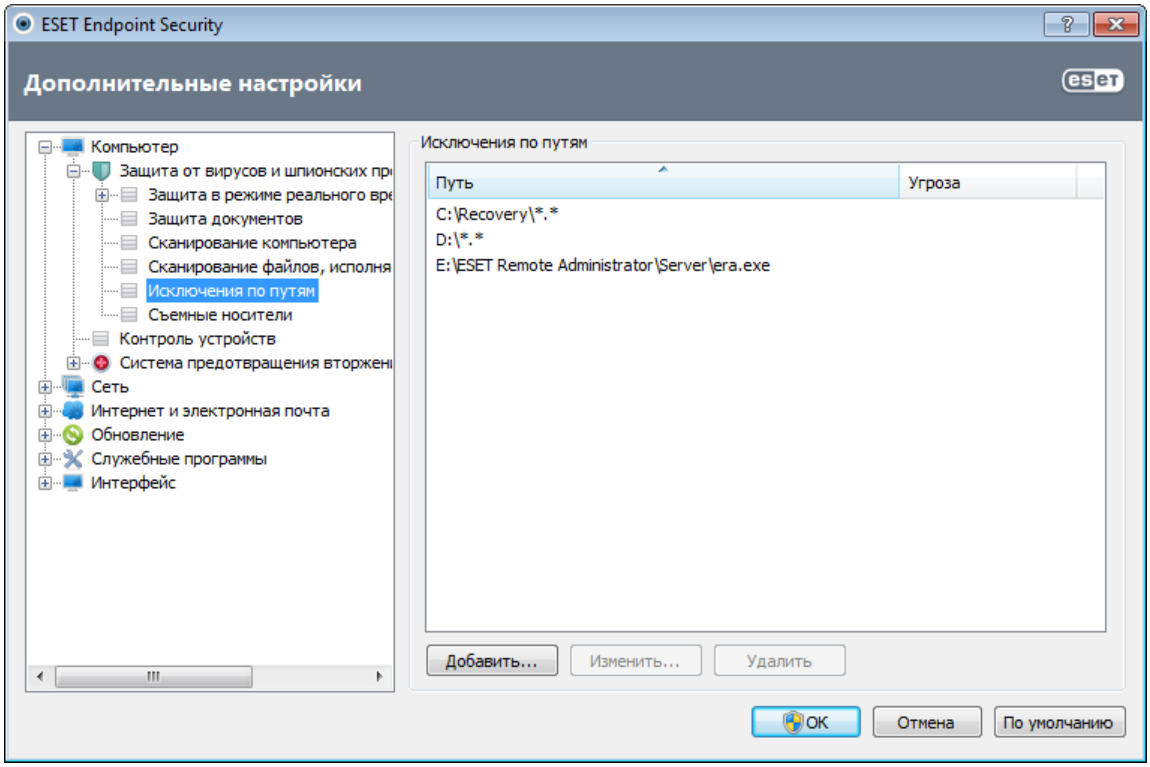
Списки подлежащих сканированию файлов являются фиксированными для каждой группы.

Приоритет сканирования: уровень приоритета, используемый при запуске сканирования.

- **Средний**: средняя нагрузка на систему.
- **Ниже среднего**: низкая нагрузка на систему.
- **Низкий**: минимальная нагрузка на систему.
- **При бездействии**: задача будет выполняться только при бездействии системы.

4.1.1.5 Исключения по путям

Исключения позволяют исключить файлы и папки из сканирования. Не рекомендуется изменять представленные здесь параметры, чтобы обеспечить проверку всех объектов на наличие угроз. Однако в некоторых случаях может быть необходимо исключить какой-либо объект. Например, большие записи баз данных, которые могли бы замедлить работу компьютера при сканировании, или программное обеспечение, конфликтующее с процессом сканирования.



Путь — путь к исключаемым файлам и папкам.

Угроза: если рядом с исключаемым файлом указано имя угрозы, файл не сканируется только на наличие этой угрозы, а не вообще. Поэтому если файл окажется заражен другой вредоносной программой, модуль защиты от вирусов ее обнаружит. Этот тип исключений можно использовать только для определенных видов заражений. Создать такое исключение можно либо в окне предупреждения об угрозе, в котором сообщается о заражении (нажмите **Показать параметры**, а затем выберите **Исключить из обнаружения**), либо в разделе **Настройка** > **Карантин**, используя пункт контекстного меню **Восстановить и исключить из обнаружения** находящегося на карантине файла.

Добавить: команда, исключающая объекты из сканирования.

Изменить...: команда, изменяющая выделенные записи.

Удалить: команда, удаляющая выделенные записи.

Для исключения объекта из сканирования выполните следующие действия.

1. Нажмите **Добавить...**.
2. Введите путь к объекту или выделите его в древовидной структуре.

Для указания групп файлов можно использовать символы шаблона. Вопросительный знак (?) обозначает один любой символ, а звездочка (*) — любое количество символов.

Примеры

- Если нужно исключить все файлы в папке, следует ввести путь к папке и использовать маску «*.*».
- Для того чтобы исключить весь диск, в том числе все файлы и подпапки на нем, используйте маску «D:*».
- Если нужно исключить только файлы с расширением .doc, используйте маску «*.doc».
- Если имя исполняемого файла содержит определенное количество символов (и символы могут меняться), причем известна только первая буква имени (скажем, «D»), следует использовать следующий формат: «D????.exe». Вопросительные знаки замещают отсутствующие (неизвестные) символы.

4.1.1.6 Настройка параметров модуля ThreatSense

ThreatSense — это технология, состоящие из множества 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:

- расширения и типы файлов, подлежащих сканированию;
- сочетание методов обнаружения угроз;
- 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
- Защита документов
- Защита почтового клиента
- Защита доступа в Интернет,
- Сканирование компьютера

Параметры ThreatSense хорошо оптимизированы для каждого из модулей, а их изменение значительно влияет на поведение системы. Например, изменение параметров сканирования упаковщиков в режиме реального времени 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). Рекомендуется не изменять параметры ThreatSense по умолчанию ни для каких модулей, кроме модуля «Сканирование компьютера».

4.1.1.6.1 Объекты

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.

Почтовые файлы: программа поддерживает расширения DBX (Outlook Express) и EML.

Архивы: программа поддерживает расширения ARJ, BZ2, CAB, CHM, DBX, GZIP, ISO/BIN/NRG, LHA, MIME, NSIS, RAR, SIS, TAR, TNEF, UUE, WISE, ZIP, ACE и многие другие.

Самораспаковывающиеся архивы: самораспаковывающиеся архивы (файлы с расширением SFX) — это

архивы, которым для распаковки не нужны специальные программы.

Упаковщики: в отличие от стандартных типов архивов упаковщики, будучи выполненными, распаковываются в память. Благодаря эмуляции кода модуль сканирования поддерживает не только стандартные статические упаковщики (UPX, yoda, ASPack, FGS и т. д.), но и множество других типов упаковщиков.

4.1.1.6.2 Параметры

В разделе **Параметры** можно выбрать методы, которые будут использоваться при сканировании компьютера на наличие заражений. Доступны указанные ниже варианты.

Эвристика — это алгоритм, анализирующий злонамеренную активность программ. Главным достоинством этого метода является способность идентифицировать вредоносные программы, сведения о которых отсутствуют в существующей базе данных сигнатур вирусов. Недостатком же является вероятность (очень небольшая) ложных тревог.

Расширенная эвристика/DNA/Сигнатуры Smart: метод расширенной эвристики базируется на уникальном эвристическом алгоритме, разработанном компанией ESET, оптимизированном для обнаружения компьютерных червей и троянских программ и написанном на языках программирования высокого уровня. Благодаря расширенной эвристике значительно увеличиваются способности программы по обнаружению. С помощью сигнатур осуществляется точное обнаружение и идентификация вирусов. Система автоматического обновления обеспечивает наличие новых сигнатур через несколько часов после обнаружения угрозы. Недостатком же сигнатур является то, что они позволяют обнаруживать только известные вирусы (или их незначительно модифицированные версии).

Потенциально нежелательные приложения не всегда являются вредоносными, однако могут негативно повлиять 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 (всплывающие окна, реклама).
- Активируются и выполняются скрытые процессы.
- Повышается уровень потребления системных ресурсов.
- Появляются изменения в результатах поиска.
- Приложение обменивается данными с удаленными серверами.

Потенциально опасное ПО: к потенциально опасным приложениям относится нормальное коммерческое программное обеспечение. В эту категорию входят такие программы, как средства удаленного доступа, приложения для взлома паролей и клавиатурные шпионы (программы, регистрирующие каждое нажатие клавиши на клавиатуре пользователем). Этот параметр по умолчанию деактивирован.

ESET Live Grid: благодаря разработанной ESET технологии репутации информация о просканированных файлах сравнивается с данными системы ESET Live Grid, работающей на основе облака, чтобы улучшить показатели обнаружения и скорость сканирования.

4.1.1.6.3 Очистка

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

Без очистки: зараженные файлы не будут очищаться автоматически. Программа выводит на экран окно предупреждения и предлагает пользователю выбрать действие. Этот уровень предназначен для более опытных пользователей, которые знают о действиях, которые следует предпринимать в случае заражения.

Стандартная очистка: программа пытается автоматически очистить или удалить зараженный файл на основе предварительно определенного действия (в зависимости от типа заражения). Обнаружение и удаление зараженных файлов сопровождается информационным сообщением, располагающимся в правом нижнем углу экрана. Если невозможно выбрать правильное действие автоматически, программа предложит пользователю выбрать действие. То же самое произойдет в том случае, если предварительно определенное действие невозможно выполнить.

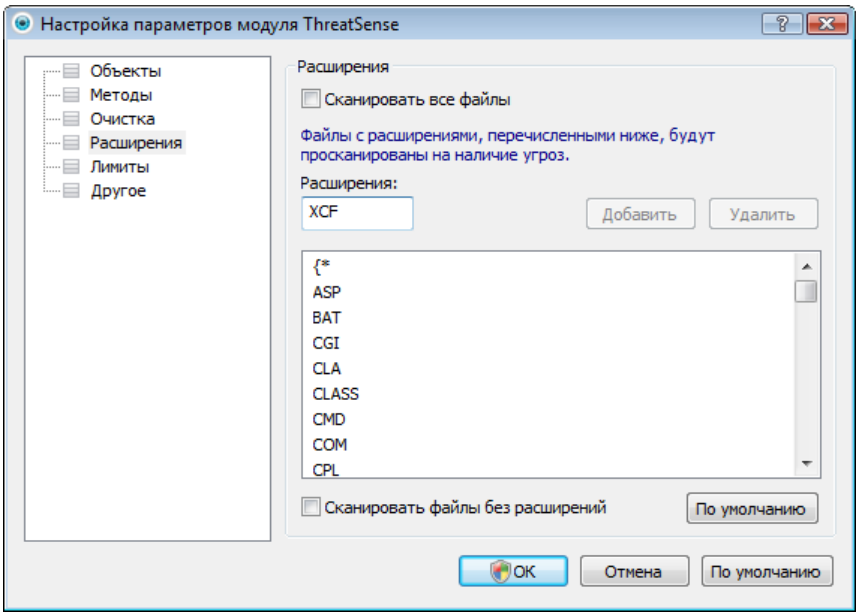
Тщательная очистка: программа очищает или удаляет все зараженные файлы. Исключение составляют только системные файлы. Если очистка невозможна, на экран выводится окно предупреждения, в котором пользователю предлагается выполнить определенное действие.

Предупреждение. Если в архиве содержатся зараженные файлы, существует два варианта обработки архива. В стандартном режиме (при стандартной очистке) целиком удаляется архив, все файлы в котором заражены. В

режиме **Тщательная очистка** удаляется архив, в котором заражен хотя бы один файл, независимо от состояния остальных файлов.

4.1.1.6.4 Расширение

Расширением называется часть имени файла, отделенная от основной части точкой. Оно 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.

Для того чтобы включить сканирование файлов без расширений, установите флажок **Сканировать файлы без расширений**. Параметр **Не сканировать файлы без расширений** становится доступен, когда установлен флажок **Сканировать все файлы**.

Иногда может быть необходимо исключить файлы, 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.

С помощью кнопок **Добавить** и **Удалить** можно изменять содержимое списка, разрешая или запрещая сканирование для определенных расширений. При вводе **расширения** активируется кнопка **Добавить**, с помощью которой можно добавить новое расширение в список. Чтобы удалить расширение из списка, выберите его и нажмите кнопку **Удалить**.

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.

Для того чтобы сканировать только список расширений по умолчанию, нажмите кнопку **По умолчанию** и выберите ответ **Да** в окне с запросом подтверждения.

4.1.1.6.5 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. Этот параметр рекомендуется менять только опытным пользователям, у которых есть веские основания для исключения из сканирования больших объектов. Значение по умолчанию — не ограничено.

Максимальное время сканирования, в секундах: определяет максимальное значение времени 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. Значение по умолчанию — не ограничено.

Уровень вложенности архива: определяет максимальную глубину проверки архивов. Значение по умолчанию — 10.

Максимальный размер файла в архиве: этот параметр позволяет задать максимальный размер файлов в архиве (при их извлечении), которые должны сканироваться. Значение по умолчанию — не ограничено.

Если сканирование преждевременно прерывается по одной из этих причин, флажок архива остается снятым.

Примечание. Не рекомендуется изменять значения по умолчанию, так как обычно для этого нет особой причины.

4.1.1.6.6 Другое

В разделе **Другое** можно конфигурировать следующие параметры.

Регистрировать все объекты: если этот флажок установлен, в файле журнала будет содержаться информация обо всех просканированных файлах, в том числе незараженных. Например, если в архиве найден вирус, в журнале также будут перечислены незараженные файлы из архива.

Включить оптимизацию Smart: при включенной оптимизации Smart используются оптимальные параметры для обеспечения самого эффективного уровня сканирования с сохранением его максимально высокой скорости. Разные модули защиты выполняют интеллектуальное сканирование, применяя отдельные методы для различных типов файлов. Если оптимизация Smart отключена, при сканировании используются только пользовательские настройки ядра ThreatSense каждого модуля.

При настройке модуля ThreatSense также доступны представленные ниже параметры.

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.

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

4.1.1.7 Действия при обнаружении заражения

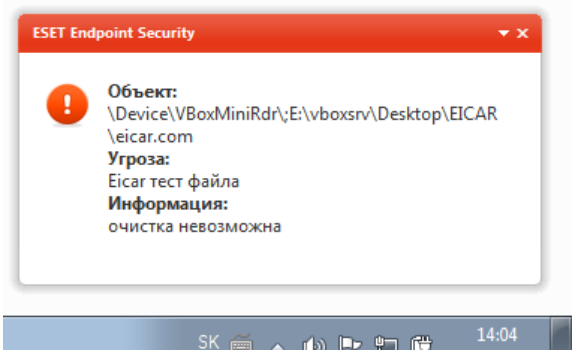
Заражения могут попасть на компьютер из различных источников, таких как веб-сайты, общие папки, электронная почта или съемные носители (USB-устройства, внешние диски, компакт- или DVD-диски, дискеты и т. д.).

Стандартное поведение

Обычно ESET Endpoint Security обнаруживает заражения с помощью перечисленных ниже модулей.

- Защита файловой системы в режиме реального времени
- Защита доступа в Интернет,
- Защита почтового клиента
- Сканирование компьютера по требованию

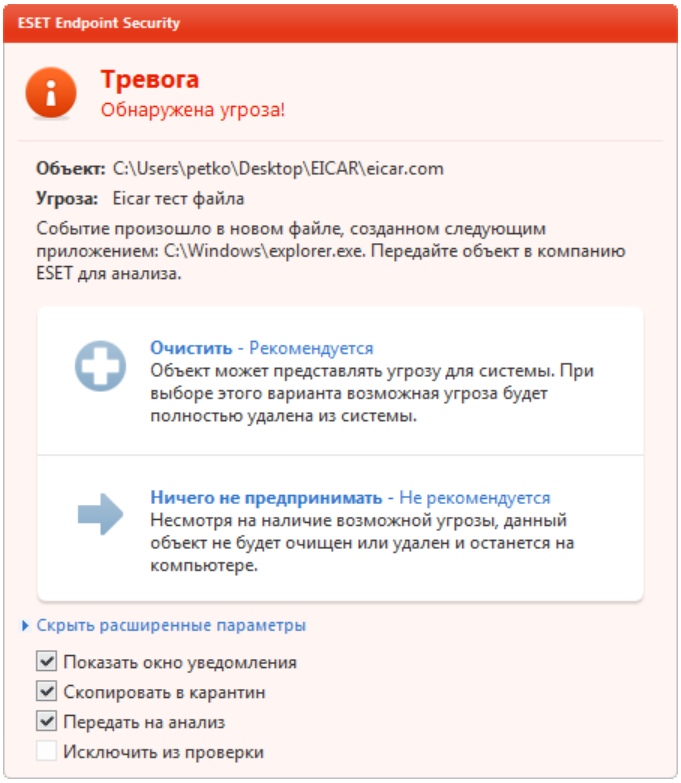
Каждый модуль использует уровень очистки по умолчанию и пытается очистить файл, поместить его в карантин или разорвать соединение. Окно уведомлений отображается в соответствующей области в правом нижнем углу экрана. Дополнительные сведения об уровнях очистки и поведении см. в разделе Очистка.



Очистка и удаление

Если действие по умолчанию для модуля защиты файловой системы в режиме реального времени не определено, его предлагается выбрать пользователю в специальном окне предупреждения. Обычно можно выбрать действие **Очистить**, **Удалить** или **Ничего не предпринимать**. Не рекомендуется выбирать действие **Ничего не предпринимать**, поскольку при этом зараженные файлы не будут очищены. Исключение допустимо только в том случае, если вы полностью уверены, что файл безвреден и был обнаружен по ошибке.

Примените очистку, если полезный файл был атакован вирусом, который добавил к нему вредоносный код. 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 при этом архив удаляется, если содержит хотя бы один зараженный файл, независимо от состояния других файлов в архиве.

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

- Откройте ESET Endpoint Security и выберите команду «Сканирование компьютера».
- Выберите вариант **Сканирование Smart** (дополнительную информацию см. в разделе Сканирование Smart).
- После окончания сканирования проверьте количество просканированных, зараженных и очищенных файлов в журнале.

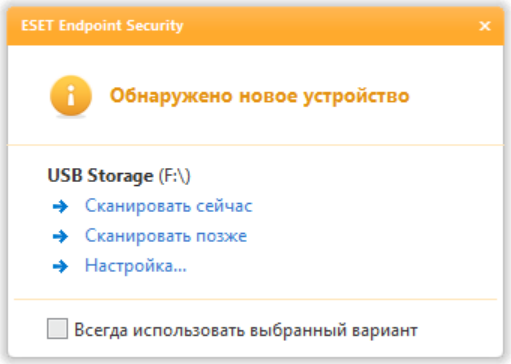
Если следует сканировать только определенную часть диска, выберите вариант **Выборочное сканирование** и укажите объекты, которые нужно сканировать на предмет наличия вирусов.

4.1.2 Съемные носители

ESET Endpoint Security обеспечивает автоматическое сканирование съемных носителей (компакт- и DVD-дисков, USB-устройств и т. п.). Данный модуль позволяет сканировать подключенный носитель. Это может быть удобно, если администратор компьютера хочет предотвратить подключение пользователями съемных носителей с нежелательным содержимым.

Действие, предпринимаемое после подключения внешних устройств выбор действия, которое будет по умолчанию выполняться после подключения к компьютеру съемного носителя (компакт- или DVD-диска, USB-устройства). Если выбран вариант **Показать параметры сканирования**, на экран будет выведено уведомление, в котором можно будет выбрать нужное действие.

- **Сканировать сейчас**: будет выполнено сканирование по требованию подключенного съемного носителя.
- **Сканировать позже**: не будет выполнено никаких действий, а окно **Обнаружено новое устройство** будет закрыто.
- **Настройка...**: переход в раздел настройки работы со съемными носителями.



Кроме того, в ESET Endpoint Security есть модуль контроля устройств, позволяющий задавать правила, которые ограничивают использование внешних устройств на указанном компьютере. Дополнительные сведения об этом модуле см. в разделе Контроль устройств.

4.1.3 Контроль устройств

ESET Endpoint Security обеспечивает автоматическое управление устройствами (компакт- и DVD-дисками, USB-устройствами и т. п.). Данный модуль позволяет сканировать, блокировать и изменять расширенные фильтры и разрешения, а также выбирать, как пользователь может получать доступ к конкретному устройству и работать с ним. Это может быть удобно, если администратор компьютера хочет предотвратить использование устройств с нежелательным содержимым.

Поддерживаемые внешние устройства

- Компакт-диски/DVD-диски/диски Blu-ray
- USB-хранилище
- Устройство FireWire
- Устройство обработки изображений
- USB-принтер
- Bluetooth-устройство
- Устройство чтения карт
- Модем
- LPT/COM-порт

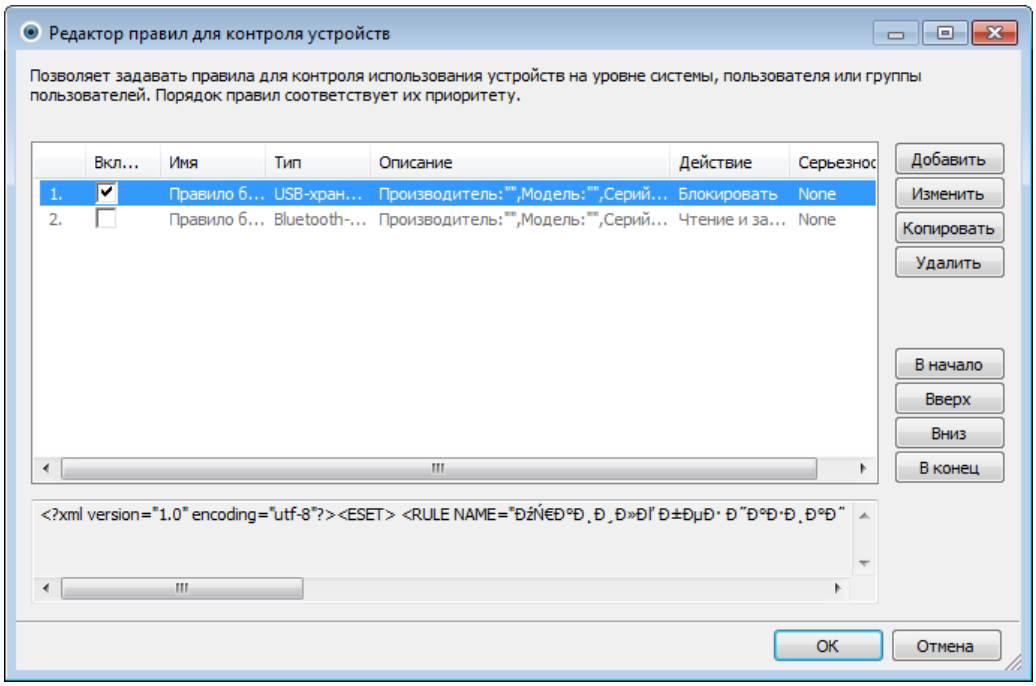
Параметры контроля устройств можно изменить в разделе **Дополнительные настройки** (F5) > **Контроль устройств**.

Если установить флажок **Интеграция с системой**, то будет активирована функция контроля устройств в системе ESET Endpoint Security. Чтобы это изменение подействовало, необходимо перезагрузить компьютер. После включения контроля устройств активируется кнопка **Конфигурировать правила...**, которая позволяет открывать окно Редактор правил для контроля устройств.

Если подключенное внешнее устройство будет соответствовать существующему правилу, предусматривающему действие **Блокировать**, то в нижнем правом углу будет отображаться окно уведомления, а к устройству не будет предоставляться доступ.

4.1.3.1 Правила контроля устройств

В окне **Редактор правил для контроля устройств** отображаются существующие правила. С его помощью можно контролировать внешние устройства, которые пользователи подключают к компьютеру.



Вы можете разрешить или заблокировать определенные устройства для конкретных пользователей или их групп, а также в соответствии с дополнительными параметрами, которые задаются в конфигурации правил. В списке правил представлен ряд их описаний, например названия и типы внешних устройств, действия, выполняемые после их подключения к компьютеру, а также вносимая в журнал серьезность.

Для управления правилом используйте кнопки **Создать** или **Изменить**. Чтобы создать правило с использованием заранее заданных параметров из другого правила, нажмите кнопку **Копировать**. XML-строки, которые отображаются, если щелкнуть правило, можно скопировать в буфер обмена. Кроме того, они могут помочь системным администраторам экспортировать или импортировать эти данные, а также использовать их, например, в ESET Remote Administrator.

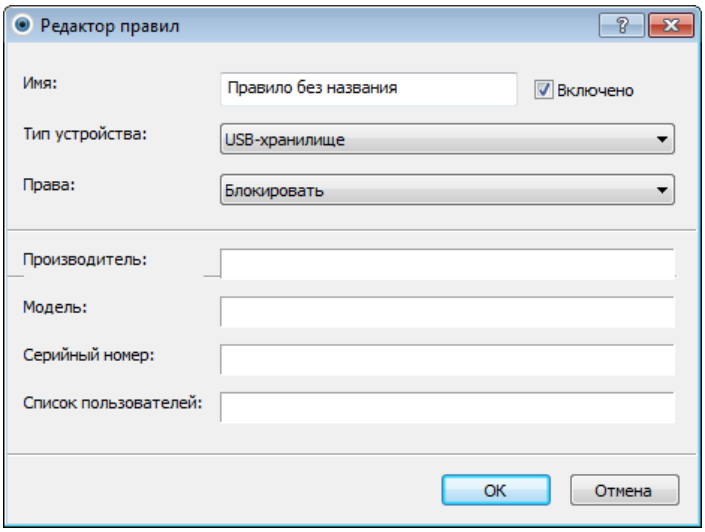
Чтобы выделить несколько правил, щелкните их, удерживая нажатой клавишу CTRL. Затем их можно будет одновременно удалить либо переместить к началу или концу списка. Флажок **Включено** позволяет включить или отключить правило. Это может быть полезно, если вы не хотите полностью удалять правило, чтобы воспользоваться им позднее.

Управление основано на правилах, которые отсортированы по приоритету: правила с более высоким приоритетом находятся в начале.

Чтобы открыть контекстное меню правила, щелкните его правой кнопкой мыши. В нем для правила можно настроить степень детализации (серьезность) записей в журнале. Записи журнала можно просмотреть в главном окне ESET Endpoint Security в разделе **Служебные программы** > **Файлы журнала**.

4.1.3.2 Добавление правил контроля устройств

Правило контроля устройств определяет действие, выполняемое при подключении к компьютеру устройств, которые соответствуют заданным критериям.



Чтобы упростить идентификацию правила, введите его описание в поле **Имя**. Чтобы включить или отключить правило, установите или снимите флажок **Включено**. Это может быть полезно в том случае, если вы не хотите полностью удалять правило.

Тип устройства

В раскрывающемся меню выберите тип внешнего устройства (USB/Bluetooth/FireWire и т. д.). Типы устройств наследуются от операционной системы. Их можно просмотреть с помощью диспетчера устройств, в котором отображается все подключенное к компьютеру оборудование. Тип **Оптический привод** в этом раскрывающемся меню соответствует оптическим накопителям данных (например, компакт- или DVD-дискам). К накопителям относятся внешние диски и традиционные устройства чтения карт памяти, подключенные по протоколу USB или FireWire. Примерами устройств обработки изображений служат сканеры и камеры. Устройства чтения смарт-карт позволяют читать карты со встроенными микросхемами, такие как SIM-карты или идентификационные карточки.

Права

Доступ к устройствам, не предназначенным для хранения данных, можно только разрешить или заблокировать. Напротив, правила для устройств хранения данных позволяют выбрать одно из указанных ниже прав.

- **Блокировать**: доступ к устройству будет заблокирован.
- **Только чтение**: будет разрешено только чтение данных с устройства.
- **Чтение и запись**: будет разрешен полный доступ к устройству.

Обратите внимание на то, что не для всех типов устройств доступен полный список прав (действий). Если на устройстве есть место для хранения данных, все три действия будут доступны. Если устройства не предназначены для хранения данных, доступны только два действия (например, право **Только чтение** неприменимо к Bluetooth-устройствам: доступ к ним можно только разрешить или заблокировать).

Прочие параметры, с помощью которых можно точно настраивать и изменять правила для конкретных устройств. Все параметры не зависят от регистра.

- **Производитель**: фильтрация по имени или идентификатору поставщика.
- **Модель**: наименование устройства.
- **Серийный номер**: у внешних устройств обычно есть серийные номера. Когда речь идет о компакт- или DVD-диске, то это серийный номер конкретного носителя, а не дисковода компакт-дисков.

Примечание. Если не указать три описанные выше дескриптора, то правило будет игнорировать их при проверке устройств.

Совет. Чтобы узнать параметры устройства, создайте разрешающее правило, соответствующее его типу, подключите устройство к компьютеру, а затем просмотрите сведения в журнале контроля устройств.

Правила можно назначать только для некоторых пользователей или их групп, добавленных в **список**

пользователей.

- **Добавить**: открывается диалоговое окно **Тип объекта: пользователи и группы**, в котором можно выбрать нужных пользователей.
- **Удалить**: выбранный пользователь удаляется из фильтра.

4.1.4 Система предотвращения вторжений на узел

Система предотвращения вторжений на узел защищает от вредоносных программ и другой нежелательной активности, которые пытаются отрицательно повлиять на безопасность компьютера. В системе предотвращения вторжений на узел используется расширенный анализ поведения в сочетании с возможностями сетевой фильтрации по обнаружению, благодаря чему отслеживаются запущенные процессы, файлы и разделы реестра. Система предотвращения вторжений на узел стоит отдельно от защиты файловой системы в режиме реального времени и не является файерволом; она отслеживает только процессы, запущенные в операционной системе.

Система предотвращения вторжений на узел доступна в разделе **Дополнительные настройки** (F5), открыть который можно через меню **Компьютер** > **Система предотвращения вторжений на узел**. Состояние системы предотвращения вторжений на узел (включена или отключена) отображается в главном окне ESET Endpoint Security, в области **Настройка**, в правой части раздела **Компьютер**.

Параметры системы предотвращения вторжений на узел находятся в разделе **Дополнительные настройки** (F5). Для доступа к системе предотвращения вторжений на узел в дереве расширенных параметров, последовательно выберите элементы **Компьютер** > **Система предотвращения вторжений на узел**. Состояние системы предотвращения вторжений на узел (включена или отключена) отображается в главном окне ESET Endpoint Security, на панели **Настройка**, в правой части раздела «Компьютер».

Предупреждение. Изменения в параметры системы предотвращения вторжений на узел должны вносить только опытные пользователи.

В ESET Endpoint Security есть встроенная технология самозащиты, которая не позволяет вредоносным программам повредить или отключить защиту от вирусов и шпионских программ, благодаря чему пользователь в любой момент времени может быть уверен в защите компьютера. Изменения параметров **Включить систему предотвращения вторжений на узел** и **Включить Self-defense** вступают в силу после перезапуска операционной системы Windows. Для отключения **системы предотвращения вторжений на узел** в целом также нужно будет перезагрузить компьютер.

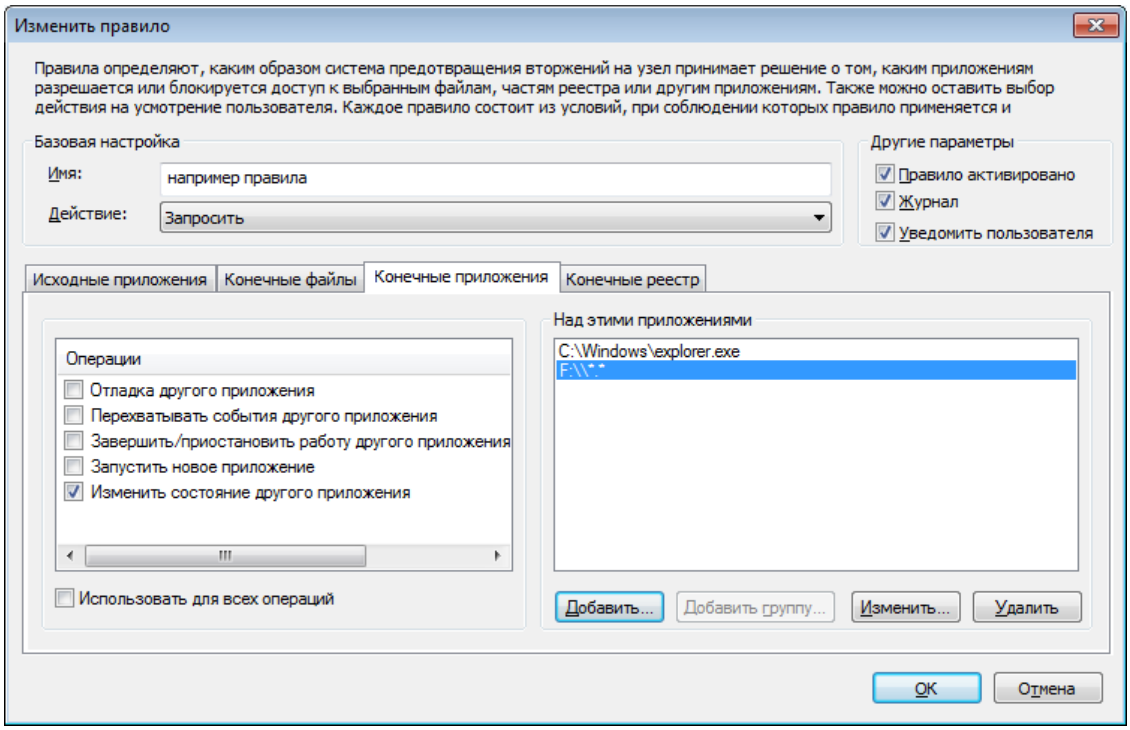
Фильтрацию можно осуществлять в одном из описанных далее четырех режимов.

- **Автоматический режим с правилами**: операции включены за исключением предварительно заданных правил, которые защищают компьютер.
- **Интерактивный режим**: пользователю будет предлагаться подтверждать операции.
- **Режим на основе политики**: операции блокируются.
- **Режим обучения**: операции включены, причем после каждой операции создается правило. Правила, создаваемые в таком режиме, можно просмотреть в разделе **Редактор правил**, но их приоритет ниже, чем у правил, создаваемых вручную или в автоматическом режиме. После выбора варианта **Режим обучения** становится доступна функция **Уведомлять об окончании режима обучения через X дней**. После окончания указанного периода времени режим обучения вновь отключается. Максимальная продолжительность периода времени составляет 14 дней. По окончании такого периода времени на экран будет выведено всплывающее окно, в котором можно изменить правила и выбрать другой режим фильтрации.

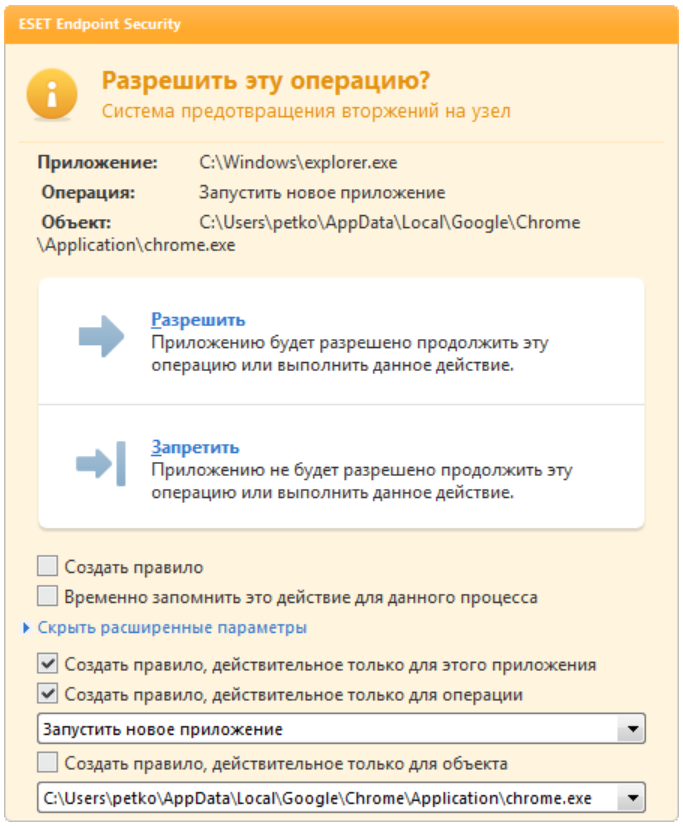
Система предотвращения вторжений на узел отслеживает события в операционной системе и реагирует на них соответствующим образом на основе правил, которые аналогичны правилам персонального файервола. Выберите **Конфигурировать правила...**, чтобы открыть окно управления правилами системы предотвращения вторжений на узел. Здесь можно выбирать, создавать, изменять или удалять правила.

В следующем примере будет показано, как ограничить нежелательное поведение приложений.

1. Присвойте правилу имя и выберите **Блокировать** в раскрывающемся меню **Действие**.
2. Откройте вкладку **Конечные приложения**. Оставьте вкладку **Исходные приложения** пустой, чтобы новое правило применялось ко всем приложениям, которые пытаются выполнить любую операцию, выбранную в списке **Операции**, с приложениями, присутствующими в списке **Над этими приложениями**.
3. Выберите **Изменить состояние другого приложения** (все операции описаны в справке к продукту; нажмите клавишу F1 в представленном ниже окне).
4. Добавьте одно или несколько приложений, которые следует защищать.
5. Установите флажок **Уведомить пользователя**, чтобы пользователь уведомлялся о применении правила.
6. Для сохранения нового правила нажмите кнопку **OK**.



Если в качестве действия по умолчанию выбрано **Запросить**, на экран каждый раз выводится диалоговое окно. Это дает пользователю возможность **запретить** или **разрешить** операцию. Если пользователь не выбирает действие в течение в течение определенного времени, выбирается новое действие на основе правил.



В этом диалоговом окне можно создавать правила на основе любого нового действия, обнаруженного

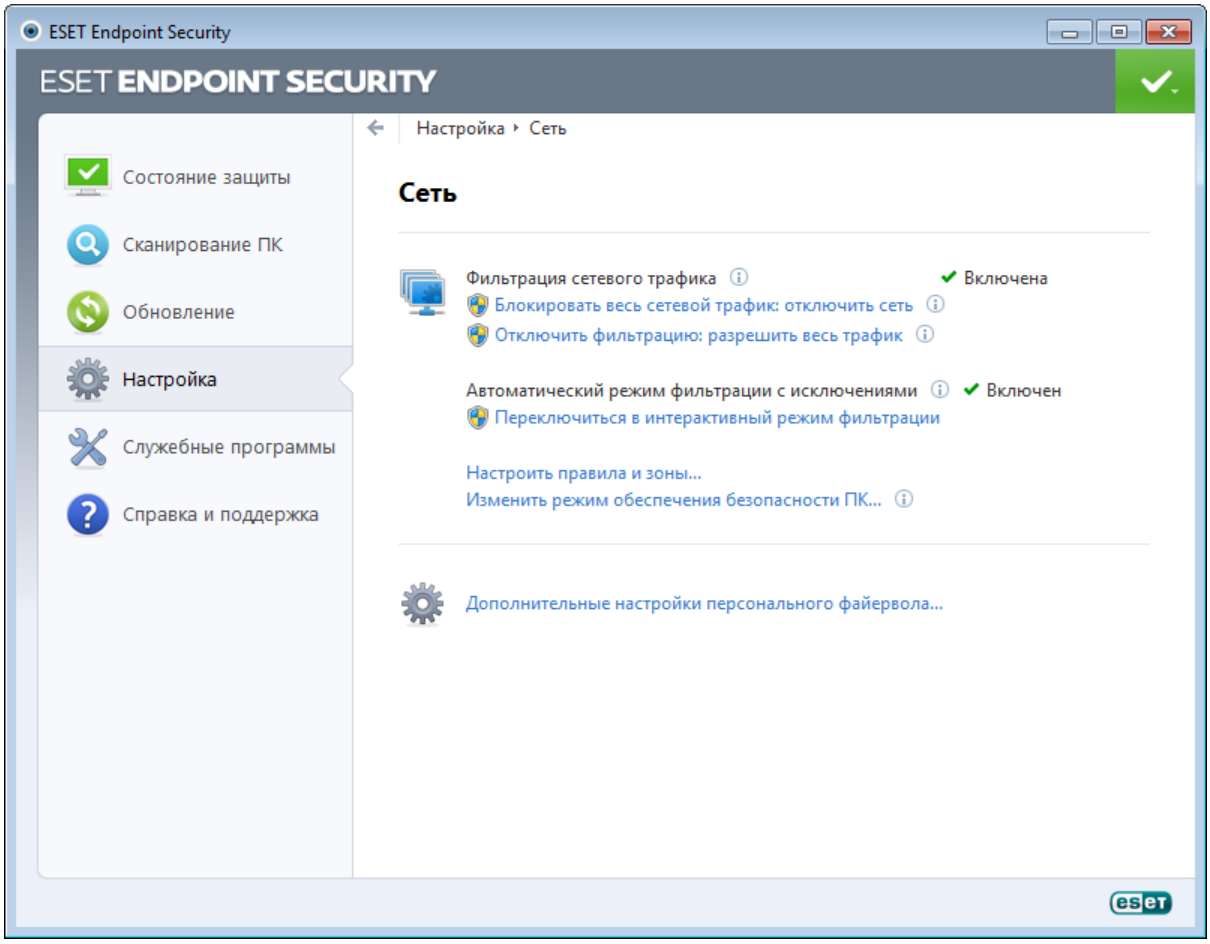
системой предотвращения вторжений на узел, а затем определять условия, в соответствии с которыми данное действие будет разрешено или запрещено. Конкретные параметры можно отобразить, нажав **Показать параметры**. Правила, создаваемые таким способом, считаются равнозначными созданным вручную правилам, поэтому правило, созданное в диалоговом окне, может быть менее подробным, чем правило, которое вызвало появление такого диалогового окна. Это значит, что после создания такого правила эта же операция может вызвать появление такого же окна.

Параметр **Временно запомнить это действие для данного процесса** приводит к использованию действия (**Разрешить**/**Запретить**) до тех пор, пока не будут изменены правила или режим фильтрации, обновлен модуль системы предотвращения вторжений на узел или не перезапущена система. После применения какого-либо из этих трех действий временные правила будут удалены.

4.2 Сеть

Персональный файервол управляет всем сетевым трафиком компьютера в обоих направлениях. Процесс основан на запрете или разрешении отдельных сетевых соединений в соответствии с определенными правилами. Персональный файервол обеспечивает противодействие сетевым атакам со стороны удаленных компьютеров и разрешает блокирование некоторых служб. Кроме того, он обеспечивает защиту от вирусов при обмене данными по протоколам HTTP, POP3 и IMAP. Функционально модуль является очень важным элементом в системе компьютерной безопасности.

Конфигурация персонального файервола доступна в области **Настройка**, которая появляется при нажатии заголовка **Сеть**. Здесь можно изменять режим фильтрации, правила и дополнительные параметры. В этом окне также предоставляется доступ к дополнительным параметрам программы.



Заблокировать весь сетевой трафик можно только с помощью функции **Блокировать весь трафик: отключить сеть**. Все прочие входящие и исходящие соединения будут блокироваться персональным файерволом. Используйте эту функцию только в особых случаях, когда возникает опасная критическая ситуация, требующая немедленного отключения от сети.

Запретить фильтрацию: разрешить весь трафик является противоположностью блокирования всего трафика. В этом режиме персональный файервол отключает все функции фильтрации и разрешает все входящие и исходящие соединения. Такой режим аналогичен полному отсутствию файервола. Если для фильтрации сетевого трафика выбрано состояние **Блокировка**, параметр **Переключить в режим**

фильтрации включает файервол.

Когда активирован режим автоматической фильтрации, доступны перечисленные ниже параметры.

- **Режим автоматической фильтрации**: чтобы сменить режим фильтрации, выберите команду **Переключить в режим интерактивной фильтрации**.
- **Настройка зоны...**: отображает настройки доверенной зоны.

Когда активирован режим интерактивной фильтрации, доступны перечисленные ниже параметры.

- **Режим интерактивной фильтрации**: чтобы сменить режим фильтрации, выберите команду **Переключить в режим автоматической фильтрации** или **Переключить в режим автоматической фильтрации с исключениями** в зависимости от текущего режима фильтрации.
- **Настроить правила и зоны...**: открытие окна **Настройка зон и правил**, в котором можно задать, каким образом файервол будет обрабатывать сетевые подключения.

Изменить режим сетевой безопасности компьютера...: этот параметр позволяет выбрать между максимальной и разрешенной защитой.

Дополнительные настройки персонального файервола...: позволяет получить доступ к дополнительным параметрам персонального файервола.

4.2.1 Режимы фильтрации

В персональном файерволе ESET Endpoint Security существует пять режимов фильтрации. Режимы фильтрации доступны в разделе **Дополнительные настройки** (F5), открыть который можно через меню **Сеть** > **Персональный файервол**. Поведение персонального файервола зависит от выбранного режима. Кроме того, от выбранного режима фильтрации зависит степень участия пользователя в процессе.

Фильтрацию можно осуществлять в одном из описанных далее пяти режимов.

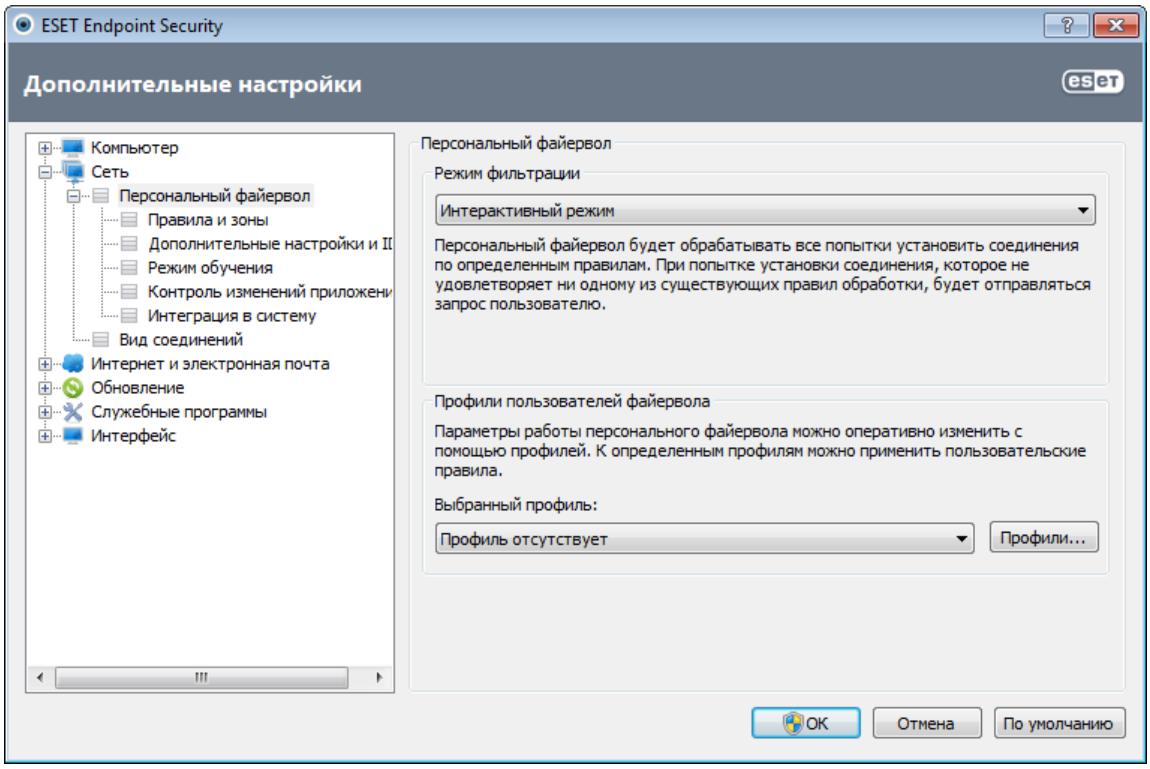
Автоматический режим — режим по умолчанию. Этот режим подходит для пользователей, которые предпочитают простоту и удобство в использовании персонального файервола без необходимости создания правил. Автоматический режим разрешает весь исходящий трафик для компьютера пользователя и блокирует все новые соединения извне.

Автоматический режим с исключениями (правила, определенные пользователем): в дополнение к автоматическому режиму пользователю разрешено также добавлять собственные правила.

Интерактивный режим: позволяет создать собственную конфигурацию персонального файервола. Если обнаружено соединение, на которое не распространяется ни одно из существующих правил, на экран выводится диалоговое окно с уведомлением о неизвестном подключении. В этом окне можно запретить или разрешить соединение, а также на основе этого решения создать правило для применения в будущем. Если принимается решение о создании нового правила, в соответствии с этим правилом все будущие соединения этого типа будут разрешены или запрещены.

Режим на основе политики: блокирует все соединения, не удовлетворяющие ни одному из ранее определенных разрешающих правил. Этот режим предназначен для опытных пользователей, которые точно знают, какие соединения им необходимы. Все прочие неуказанные соединения будут блокироваться персональным файерволом.

Режим обучения: автоматическое создание и сохранение правил; этот режим удобен для первоначальной настройки персонального файервола. Участие пользователя не требуется, потому что ESET Endpoint Security сохраняет правила согласно предварительно настроенным параметрам. Режим обучения является небезопасным, поэтому рекомендуется использовать его только до момента создания правил для всех необходимых соединений.

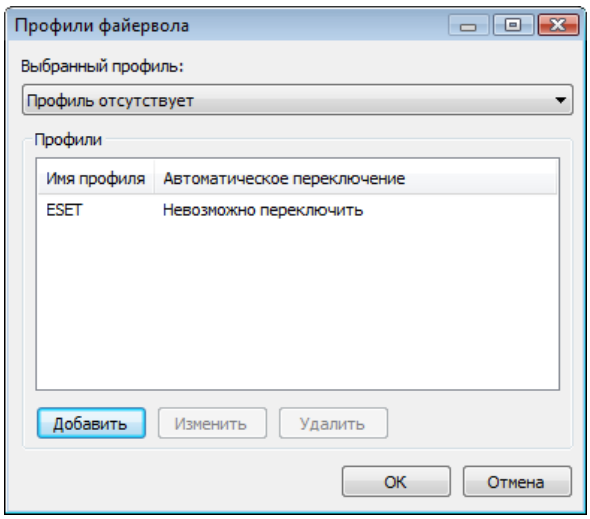


Профили позволяют контролировать поведение персонального файервола ESET Endpoint Security.

4.2.2 Профили файервола

Профили позволяют контролировать поведение персонального файервола ESET Endpoint Security. При создании или изменении правила персонального файервола его можно назначить отдельному профилю или применить ко всем профилям. При выборе определенного профиля действуют только глобальные правила (правила без указания профиля) и правила, назначенные этому профилю. Для удобного изменения поведения персонального файервола можно создать несколько профилей с различными назначенными правилами.

Нажмите кнопку **Профили...** (см. рисунок в разделе Режимы фильтрации), чтобы открыть окно **Профили файервола**, в котором можно **добавлять**, **изменять** и **удалять** профили. Имейте в виду, что **изменить** или **удалить** профиль, указанный в раскрывающемся меню **Выбранный профиль**, нельзя. При добавлении или изменении профиля можно задать условия, при которых он запустится.

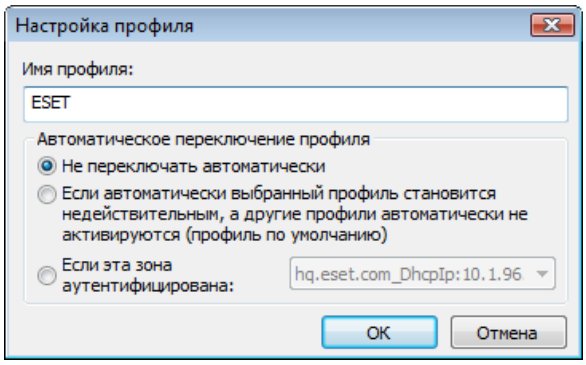


При создании профиля можно выбрать события, которые будут запускать его. Доступны указанные ниже варианты.

- **Не переключать автоматически**: автоматический запуск отключен (профиль должен быть активирован вручную).
- **Если автоматически выбранный профиль становится недействительным, а другие профили автоматически не активируются (профиль по умолчанию)**: когда автоматически выбранный профиль становится недействительным (например, компьютер подключен к недоверенной сети, см. раздел

Аутентификация сети), а другой профиль не активируется (компьютер не подключен к другой доверенной сети), персональный файервол переключится на этот профиль. Этот параметр можно установить только для одного профиля.

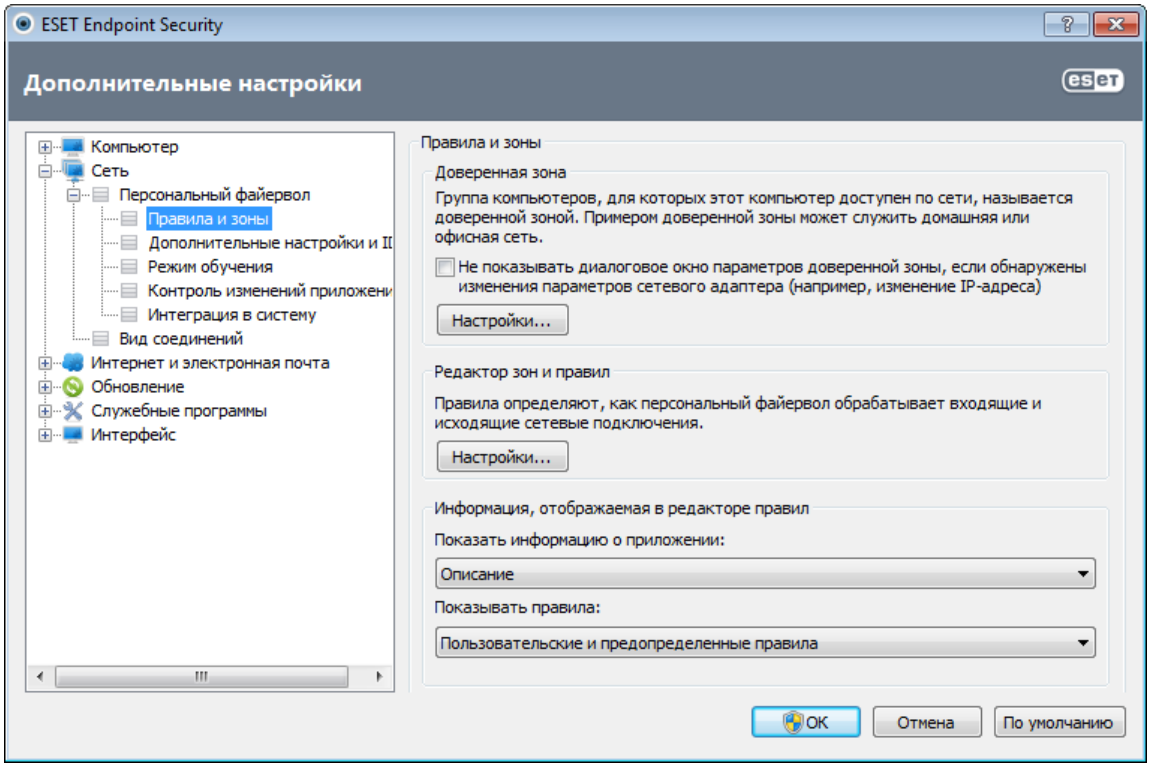
- **Если эта зона аутентифицирована**: этот профиль запустится, когда определенная зона будет аутентифицирована (см. раздел Аутентификация сети).



При переключении профилей персонального файервола в правом нижнем углу рядом с системными часами появляется соответствующее уведомление.

4.2.3 Настройка и использование правил

Правило содержит набор параметров и условий, которые позволяют целенаправленно проверять сетевые соединения и выполнять необходимые действия в соответствии с этими условиями. При использовании персонального файервола пользователь может задать действия, которые необходимо совершить при попытке соединения. Для того чтобы настроить правило фильтрации, перейдите в окно **Дополнительные настройки** (F5) > **Сеть** > **Персональный файервол** > **Правила и зоны**.



Нажмите кнопку **Настройка...** в разделе **Доверенная зона**, чтобы вывести на экран диалоговое окно настройки доверенной зоны. Параметр **Не показывать диалоговое окно параметров доверенной зоны, если обнаружены изменения параметров сетевого адаптера** дает пользователю возможность отключить вывод окна параметров доверенной зоны при обнаружении новой подсети. При этом используются параметры текущей доверенной зоны.

ПРИМЕЧАНИЕ. Если персональный файервол настроен на работу в **автоматическом режиме**, некоторые параметры недоступны.

Нажмите кнопку Настройка... в разделе **Редактор зон и правил**, чтобы вывести на экран окно **Настройка зон и правил**, где представлены общие сведения о правилах или зонах (в зависимости от выбранной вкладки).

Окно разделено на две области. Верхняя область содержит правила в краткой форме. Нижняя область содержит подробную информацию о правиле, выбранном в верхней области. В нижней части окна расположены кнопки **Создать**, **Изменить** и **Удалить (Del)**, которые позволяют конфигурировать правила.

Подключения можно разделить на входящие и исходящие. Входящие подключения инициируются удаленным компьютером, который пытается подключиться к локальной системе. При исходящим соединении, наоборот, локальный компьютер пытается подключиться к удаленному.

При возникновении неизвестного соединения пользователь должен разрешить или запретить его. Нежелательные, небезопасные или неизвестные соединения несут угрозу безопасности для компьютера. При установлении такого соединения рекомендуется обратить особое внимание на удаленный компьютер и приложение, которые пытаются установить это соединение с компьютером. Многие типы заражений пытаются получить и отправить личные данные или загрузить другие злонамеренные приложения на компьютер. Персональный файервол дает пользователю возможность обнаружить и разорвать такие подключения.

Показать информацию о приложении: позволяет определить, какие из приложений будут отображаться в списке правил. Доступны указанные ниже варианты.

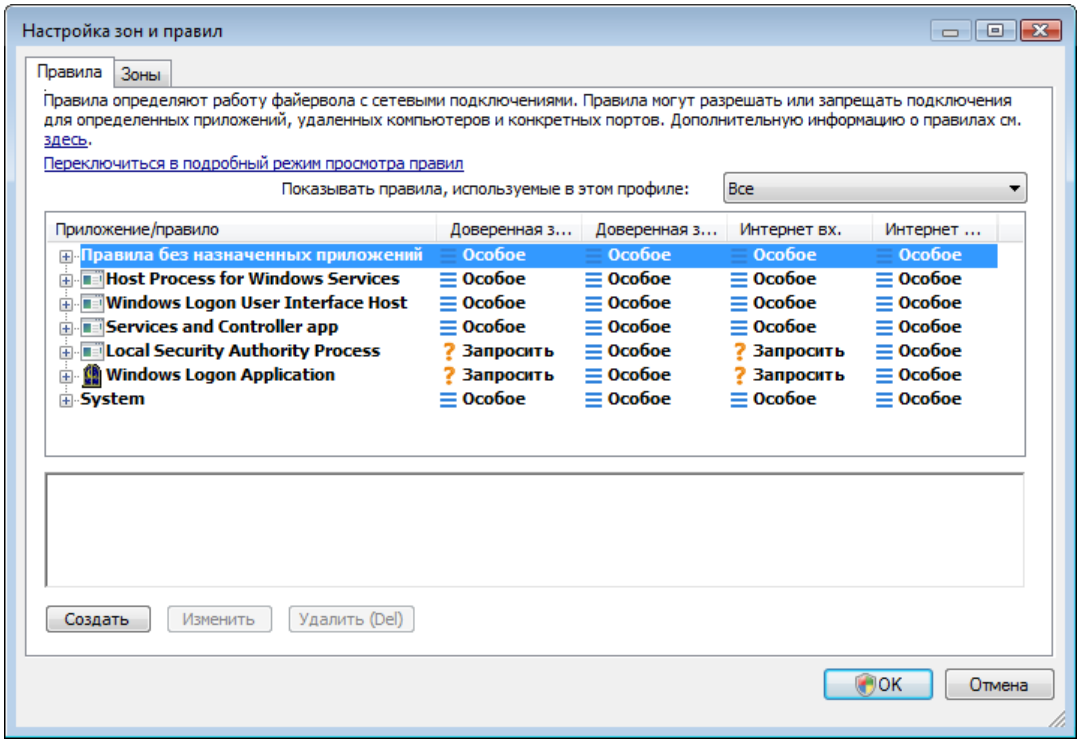
- **Полный путь**: полный путь к исполняемому файлу приложения.
- **Описание**: описание приложения.
- **Имя** — имя исполняемого файла приложения.

Выберите тип правил, которые будут отображаться в списке **Показывать правила**.

- **Только пользовательские правила**: на экран выводятся только правила, созданные пользователем.
- **Пользовательские и предопределенные правила**: отображение всех определенных пользователем правил и правил, заданных по умолчанию.
- **Все правила (включая системные)**: на экран выводятся все правила.

4.2.3.1 Настройка правил

В разделе настройки правил можно просмотреть правила, которые применяются к трафику, генерируемому различными приложениями в пределах доверенных зон и сети Интернет. По умолчанию правила добавляются автоматически в соответствии с реакцией пользователя на новое подключение. Для получения дополнительных сведений о приложении щелкните по его названию. Данные отобразятся в нижней части окна.



В начале каждой строки, соответствующей правилу, расположена кнопка, позволяющая свернуть или развернуть (+/-) информационное поле. Для получения дополнительной информации о правиле щелкните название приложения в столбце **Приложение/правило**. Данные отобразятся в нижней части окна. Для изменения режима представления служит контекстное меню. Оно также используется для добавления,

изменения и удаления правил.

Доверенная зона вх./исх.: действия, которые относятся к входящим или исходящим подключениям в пределах доверенной зоны.

Интернет вх./исх.: действия, связанные с входящими или исходящими подключениями к Интернету.

Для каждого типа (направления) соединения можно использовать следующие действия.

- **Разрешить**: разрешить соединения.
- **Запросить**: пользователю будет предложено разрешить или запретить соединение при каждой новой попытке установить его.
- **Запретить**: запретить соединения.
- **Особое**: невозможно классифицировать другими действиями. Например, если IP-адрес или порт разрешены в персональном файерволе, невозможно точно классифицировать, разрешены ли входящие или исходящие соединения соответствующего приложения.

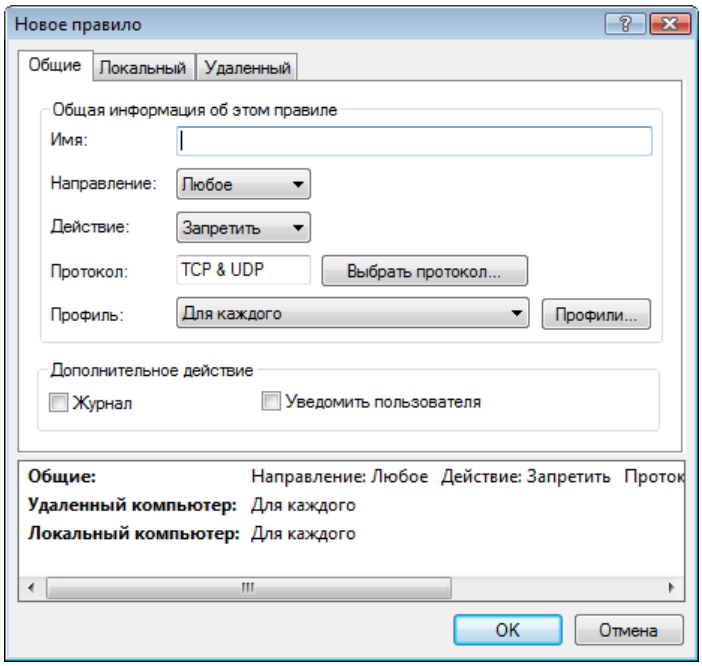
При установке нового приложения, которое обращается к сети, или при изменении параметров существующего подключения (адрес удаленного компьютера, номер порта и т. п.) нужно создавать новое правило. Для изменения существующего правила перейдите на вкладку **Правила** и нажмите кнопку **Изменить**.

4.2.3.2 Изменение правил

Изменение требуется при каждом изменении отслеживаемых параметров. В такой ситуации правило не может удовлетворять условиям, а указанное действие не может быть применено. При изменении параметров соединение может быть отклонено, что вызовет проблемы в работе с приложением. Примером может быть изменение сетевого адреса или номера порта удаленного компьютера.

Верхняя часть диалогового окна содержит три вкладки.

- **Общие**: укажите название правила, направление подключения, действие, протокол и профиль, к которому будет применено правило.
- **Локальный**: на экран выводится информация о локальном компьютере, участвующем в подключении, с указанием номера локального порта или диапазона портов и названия приложения, которое установило подключение.
- **Удаленный**: на этой вкладке приводится информация об удаленном порте (диапазоне портов). Также здесь можно указать список удаленных IP-адресов или зон для конкретного правила.



Протокол: протокол передачи данных, используемый для правила. Нажмите **Выбрать протокол...**, чтобы открыть окно Выбор протокола.

По умолчанию все правила активируются **для каждого** профиля. Также вы можете выбрать собственный профиль файервола, нажав кнопку **Профили...**.

Если нажать **Журнал**, действия, связанные с этим правилом, будут регистрироваться в журнале. **Уведомить пользователя**: вывод сообщения в случае применения правила.

Информационная область отображает общие сведения о правиле в нижней части всех трех вкладок. Та же информация выводится на экран и если нажать правило в главном окне (**Служебные программы** > **Сетевые подключения**; щелкните правило правой кнопкой мыши и воспользуйтесь функцией **Показать подробности** (см. главу Сетевые подключения)).

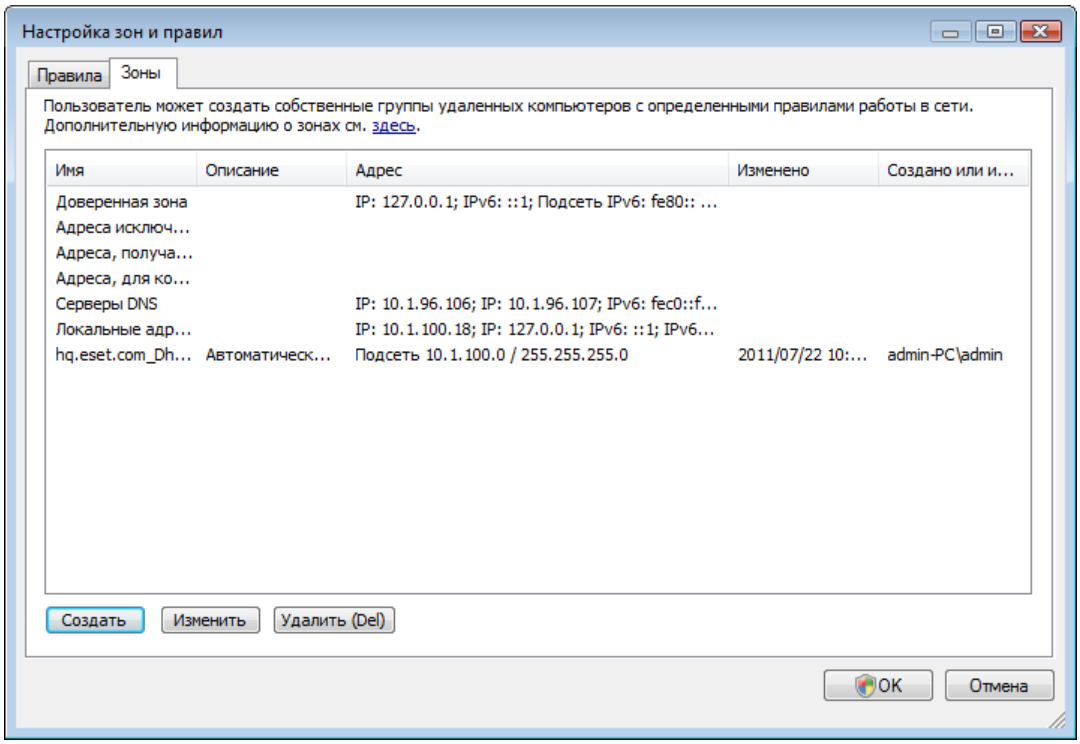
При создании нового правила нужно ввести его название в поле **Имя**. В раскрывающемся меню **Направление** выберите направление, к которому применяется правило. В раскрывающемся меню **Действие** укажите действие, которое должно выполняться в том случае, если подключение соответствует правилу.

Хорошим примером является создание правила доступа в Интернет для веб-браузера. В этом случае необходимо выполнить следующие настройки:

- На вкладке **Общие** включите исходящие подключения по протоколам TCP и UDP.
- Добавьте процесс, представляющий приложение браузера (для браузера Internet Explorer — iexplore.exe), на вкладке **Локальный**.
- На вкладке **Удаленный** включите порт 80, только если следует разрешить стандартные действия, связанные с посещением веб-страниц.

4.2.4 Настройка зон

В окне **Настройка зоны** можно задать имя зоны, ее описание, список сетевых адресов и параметры аутентификации (см. раздел Аутентификация зон: конфигурация клиента).



Зона представляет собой логически объединенную группу сетевых адресов. Каждому адресу в группе присваивается аналогичное правило, которое определено для всей группы в целом. Примером такой группы является **доверенная зона**. Доверенная зона представляет собой группу сетевых адресов, которым пользователь полностью доверяет и соединения с которыми не блокируются персональным файерволом ни в коем случае.

Такие зоны могут быть созданы на вкладке **Зоны** окна **Настройка зон и правил**. Для этого нажмите кнопку **Изменить**. Введите **имя** и **описание** зоны, а затем добавьте удаленный IP-адрес, нажав кнопку **Добавить адрес IPv4/IPv6**.

4.2.4.1 Аутентификация сети

Для мобильных компьютеров рекомендуется проверять надежность сети, к которой выполняется подключение. Доверенная зона определяется локальным IP-адресом сетевого адаптера. Портативные компьютеры часто входят в сети с IP-адресами, похожими на адрес доверенной сети. Если параметр доверенной зоны **Тщательная защита** не выбран, персональный файервол продолжит работать в режиме **Разрешить общий доступ**.

Для того чтобы избежать подобной ситуации, рекомендуется использовать аутентификацию зон.

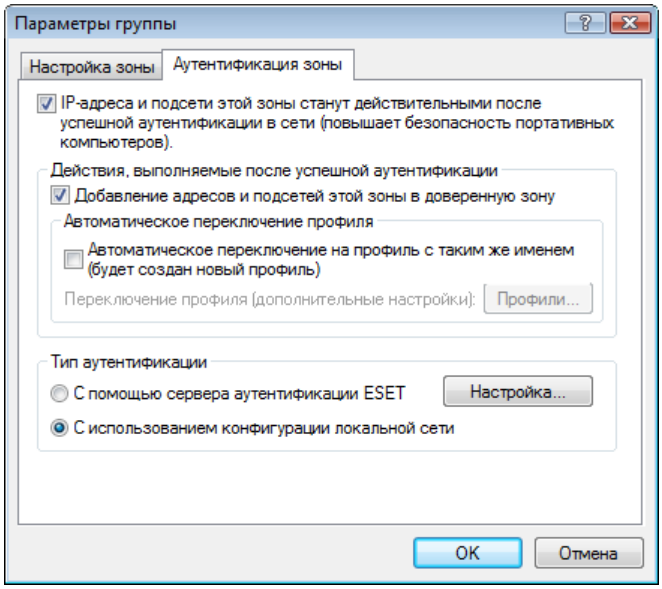
4.2.4.1.1 Аутентификация зон: конфигурация клиента

В окне **Настройка зон и правил** перейдите на вкладку **Зоны** и создайте зону, используя имя зоны, аутентифицированной сервером. Для того чтобы добавить маску подсети, содержащую сервер аутентификации, нажмите кнопку **Добавить адрес IPv4** и выберите параметр **Подсеть**.

Перейдите на вкладку **Аутентификация зоны**. Каждую зону можно настроить на аутентификацию на сервере. Зона (ее IP-адрес и подсеть) будут действительны после успешной аутентификации, т. е. такие действия, как изменение профиля файервола и добавление адреса или подсети зоны в доверенную зону, будут выполняться только после успешной аутентификации.

Установите флажок **IP-адреса и подсети этой зоны станут действительными после...**, чтобы зона становилась недействительной, если аутентификация не пройдена. Для того чтобы выбрать профиль персонального файервола, который будет активироваться после аутентификации, нажмите кнопку **Профили...**.

Если выбран параметр **Добавление адресов и подсетей этой зоны в доверенную зону**, после успешной аутентификации адреса и подсети зоны будут добавлены в доверенную зону (рекомендуется). Если аутентификация не выполнена, адреса не будут добавлены в доверенную зону. Если активирован параметр **Автоматическое переключение на профиль с таким же именем (будет создан новый профиль)**, после выполнения аутентификации будет создан новый профиль. Нажмите кнопку **Профили...**, чтобы открыть окно Профили файервола.



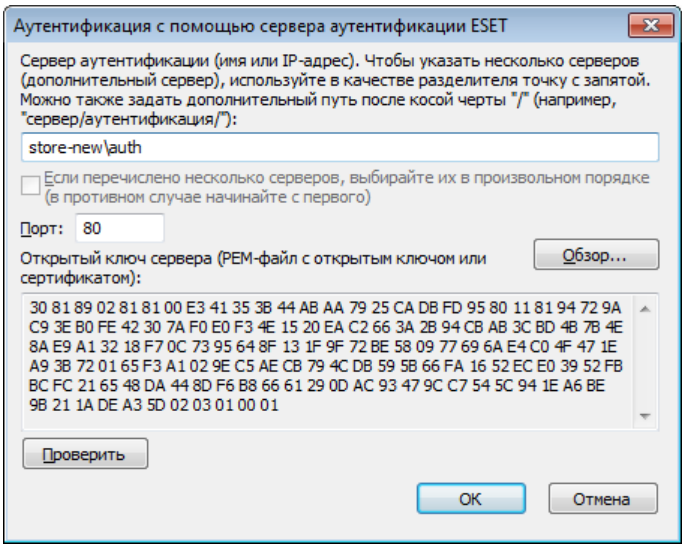
Существует два типа аутентификации.

1) С помощью сервера аутентификации ESET

В рамках аутентификации зоны выполняется поиск в сети определенного сервера, а для аутентификации сервера используется асимметричное шифрование (RSA). Процесс аутентификации повторяется для каждой сети, к которой подключается компьютер. Нажмите **Настройка...** и укажите имя сервера, его прослушивающий порт и открытый ключ, соответствующий закрытому ключу сервера (см. раздел Аутентификация зон: конфигурация сервера). Имя сервера можно ввести в форме IP-адреса либо имени DNS или NetBios. После имени сервера можно указать путь к файлу на сервере (например, имя_сервера_/каталог1/каталог2/аутентификация). На случай недоступности первого сервера можно указать дополнительные серверы через точку с запятой.

Открытым ключом может быть файл одного из указанных ниже типов.

- Зашифрованный открытый ключ в формате PEM (.pem)
  Этот ключ можно создать с помощью приложения ESET Authentication Server (см. раздел Аутентификация зон: конфигурация сервера).
- Зашифрованный открытый ключ
- Сертификат открытого ключа (.crt)



Для того чтобы проверить настройки, нажмите кнопку **Проверить**. Если аутентификация прошла успешно, на экран будет выведено сообщение Аутентификация сервера выполнена успешно. Если аутентификация не настроена должным образом, на экран будет выведено одно из указанных ниже сообщений.

Сбой аутентификации сервера. Максимальное время аутентификации истекло.
Сервер аутентификации недоступен. Проверьте имя сервера и IP-адрес либо параметры персонального файервола клиента, а также параметры сервера.

Произошла ошибка при обмене данными с сервером.
Сервер аутентификации не работает. Запустите службу сервера аутентификации (см. раздел Аутентификация зон: конфигурация сервера).

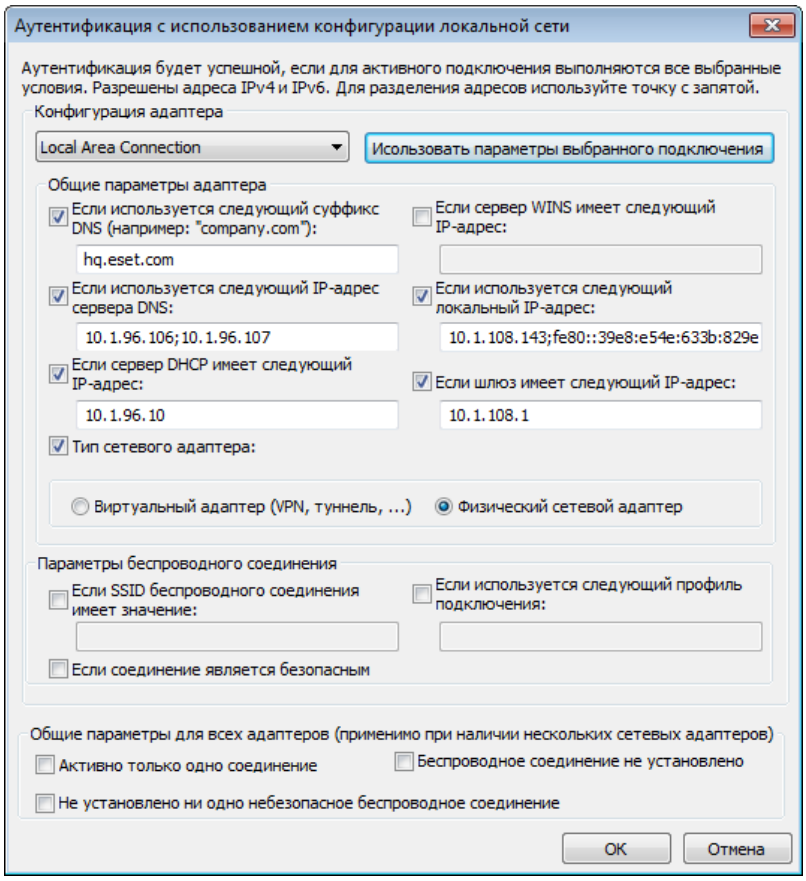
Имя зоны аутентификации не соответствует имени зоны сервера.
Настроенное имя зоны не соответствует зоне сервера аутентификации. Проверьте обе зоны и задайте для них одинаковые имена.

Сбой аутентификации сервера. Адрес сервера не найден в списке адресов указанной зоны.
IP-адрес компьютера, на котором запущен сервер аутентификации, находится вне заданного диапазона IP-адресов в текущей конфигурации зоны.

Сбой аутентификации сервера. Возможно, введен недействительный открытый ключ.
Убедитесь в том, что указанный открытый ключ соответствует закрытому ключу сервера. Кроме того, проверьте, не поврежден ли файл открытого ключа.

2) С использованием конфигурации локальной сети

Аутентификация выполняется на основе параметров адаптера локальной сети. Зона считается аутентифицированной, если действительны все параметры, выбранные для активного подключения.



4.2.4.1.2 Аутентификация зон: конфигурация сервера

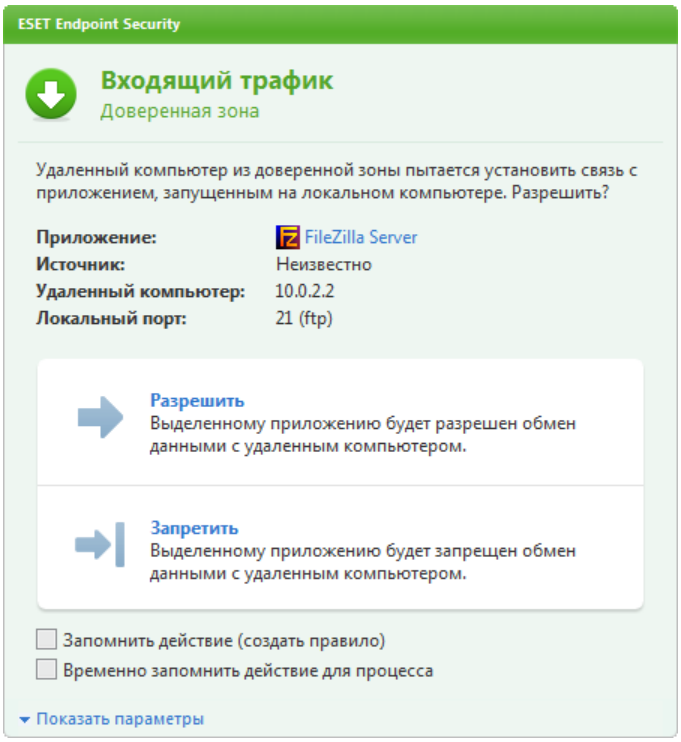
Аутентификацию сети можно выполнить с помощью любого подключенного к ней компьютера или сервера. Для этого на компьютер или сервер, который всегда доступен для аутентификации, когда клиент пытается подключиться к сети, нужно установить приложение ESET Authentication Server. Файл установки приложения ESET Authentication Server можно загрузить с веб-сайта ESET.

После установки ESET Authentication Server на экран будет выведено диалоговое окно. (Приложение можно запустить, нажав кнопку **Пуск** и выбрав последовательно пункты **Программы** > **ESET** > **ESET Authentication Server**).

Для того чтобы настроить сервер аутентификации, введите имя зоны аутентификации, прослушивающий порт сервера (по умолчанию 80) и место, в котором будут храниться открытый и закрытый ключи. Далее создайте открытый и закрытый ключи, которые будут использоваться при аутентификации. Закрытый ключ должен использоваться на сервере, а открытый — импортироваться на сторону клиента, что можно сделать в разделе аутентификации зоны при настройке зоны в файерволе.

4.2.5 Установка соединения: обнаружение

Персональный файервол обнаруживает каждое из вновь созданных сетевых соединений. Активный режим персонального файервола определяет, какие действия должны выполняться для нового правила. Если активирован **Автоматический режим** или **Режим на основе политики**, персональный файервол выполнит предварительно заданные действия без какого-либо вмешательства пользователя. В интерактивном режиме выводится информационное окно с уведомлением об установлении соединения. Оно содержит информацию о новом соединении. Пользователь может разрешить или запретить (заблокировать) соединение. Если соединения одного типа возникают регулярно, и их приходится разрешать вручную, рекомендуется создать для них правило. Для этого выберите функцию **Запомнить действие (создать правило)** и сохраните новое правило для персонального файервола. Если персональный файервол обнаружит такое соединение в будущем, он применит это правило.



Будьте внимательны при создании новых правил и разрешайте только те соединения, которые действительно безопасны. Если разрешить все соединения, персональный файервол не сможет обеспечивать защиту. Ниже перечислены наиболее важные параметры соединений.

- **Удаленный компьютер**: разрешить соединения только с доверенными и известными адресами.
- **Локальное приложение**: не рекомендуется разрешать соединения с неизвестными приложениями и процессами.
- **Номер порта**: соединения на стандартных портах (например, порт номер 80 для просмотра веб-страниц) в обычных условиях должны быть разрешены.

Компьютерные вирусы для размножения часто используют соединения с Интернетом или скрытые соединения, через которые происходит заражение других компьютеров. Если правила настроены надлежащим образом, персональный файервол является эффективным средством противодействия разнообразным злонамеренным атакам.

4.2.6 Ведение журнала

Персональный файервол ESET Endpoint Security сохраняет данные обо всех важных событиях в файле журнала, который можно открыть с помощью главного меню. Выберите **Служебные программы** > **Файлы журнала**, а затем **Журнал персонального файервола Eset** в раскрывающемся меню **Журнал**.

Файлы журнала представляют собой незаменимый инструмент для обнаружения ошибок и выявления вторжений на компьютер. Журналы персонального файервола ESET содержат следующую информацию.

- Дата и время события
- Имя события
- Источник
- Сетевой адрес объекта
- Сетевой протокол передачи данных
- Примененное правило или имя червя (если обнаружено)
- Задействованное приложение
- Пользователь

Тщательный анализ информации значительно облегчает процесс оптимизации безопасности компьютера. Многие факторы являются признаками потенциальных угроз и позволяют пользователю свести их влияние к минимуму: слишком частые соединения от неизвестных компьютеров, множественные попытки установить соединение, сетевая активность неизвестных приложений или с использованием неизвестных номеров портов.

4.2.7 Интеграция в систему

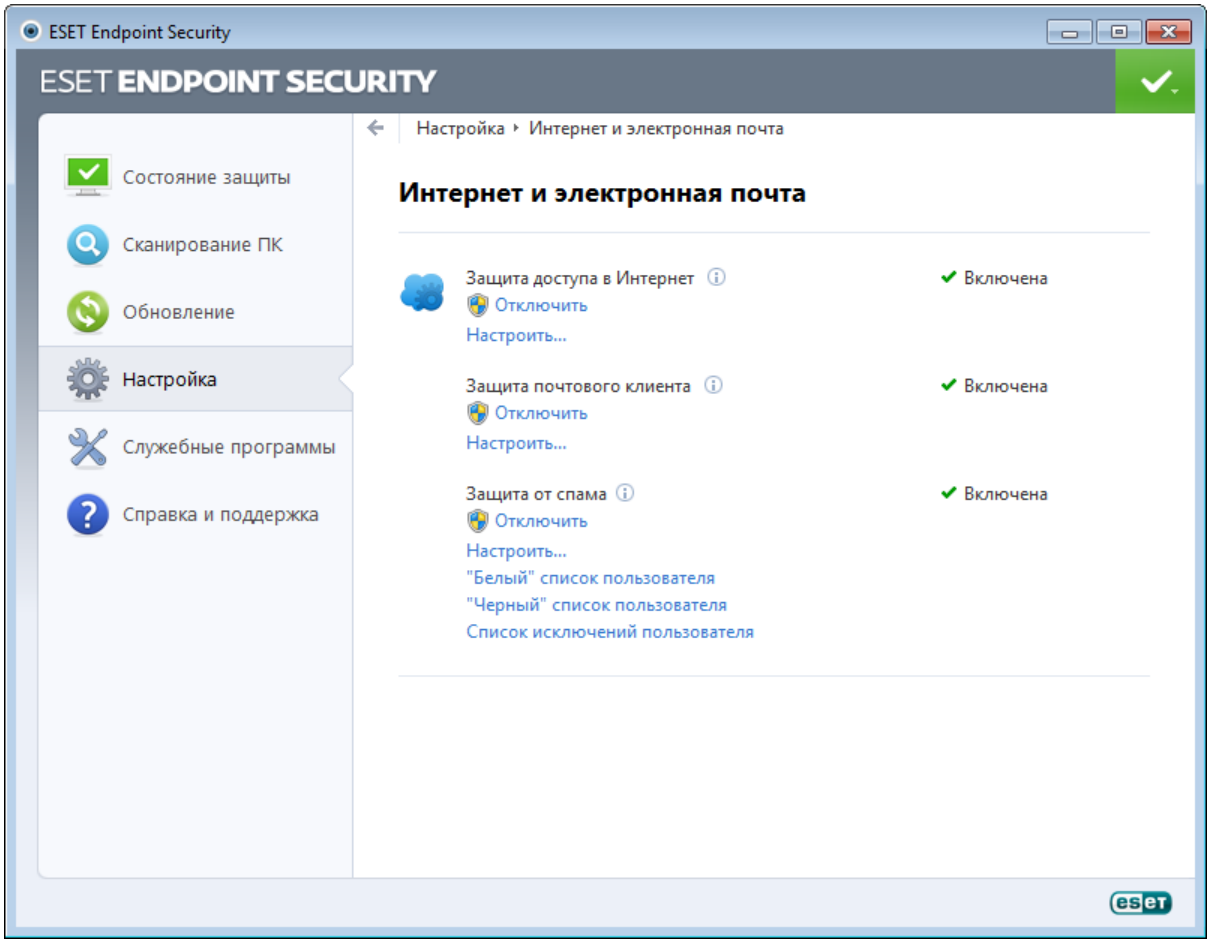
Персональный файервол ESET Endpoint Security может работать на нескольких уровнях, которые описаны далее.

- **Все функции активны**: персональный файервол полностью интегрирован, а все его компоненты активны (вариант по умолчанию). Если компьютер подключен к сетям большого размера или к Интернету, рекомендуется оставить этот параметр активированным. Это самый безопасный вариант, который обеспечивает полную защиту компьютера.
- **Персональный файервол неактивен**: персональный файервол интегрирован в систему, через него выполняются сетевые подключения, но проверка на наличие угроз не осуществляется.
- **Сканировать только протоколы уровня приложений**: активны только те компоненты персонального файервола, которые обеспечивают сканирование протоколов приложений (HTTP, POP3, IMAP и их защищенные версии). Если протоколы приложений не сканируются, защита осуществляется на уровне защиты файловой системы в режиме реального времени и сканирования компьютера по требованию.
- **Персональный файервол полностью отключен**: установите этот флажок, чтобы полностью удалить регистрацию персонального файервола в системе. Никакое сканирование не выполняется. Это может быть удобно при тестировании: если приложение блокируется, можно проверить, заблокировано ли оно файерволом. Это наименее безопасный вариант, поэтому рекомендуется очень осторожно полностью отключать файервол.

Отложить обновление модуля персонального файервола до перезагрузки компьютера: обновление будет только загружаться, тогда как установка будет выполнена только в ходе перезагрузки компьютера.

4.3 Интернет и электронная почта

Конфигурация Интернета и электронной почты доступна в области **Настройка**, которая появляется при нажатии заголовка **Интернет и электронная почта**. В этом окне предоставляется доступ к дополнительным параметрам программы.



Подключение к Интернету стало стандартной функцией персонального компьютера. К сожалению, Интернет также стал и основной средой распространения злонамеренного кода. По этой причине принципиально важно уделить особое внимание **защите доступа в Интернет**.

Защита почтового клиента обеспечивает контроль обмена данными по протоколам POP3 и IMAP. При использовании подключаемого модуля для почтового клиента ESET Endpoint Security позволяет контролировать весь обмен данными, осуществляемый почтовым клиентом (по протоколам POP3, MAPI, IMAP, HTTP).

Функция **защиты от спама** отфильтровывает нежелательные сообщения, поступающие по электронной почте.

Отключить: отключение защиты Интернета и электронной почты/защиты от спама для почтовых клиентов.

Настроить...: переход к расширенным параметрам защиты Интернета и электронной почты/защиты от спама .

«Белый» список пользователя: открывает диалоговое окно, в котором можно добавить, изменить и удалить адреса электронной почты, считающиеся безопасными. Сообщения электронной почты, адрес отправителя которых присутствует в «белом» списке, не будут сканироваться на предмет наличия спама.

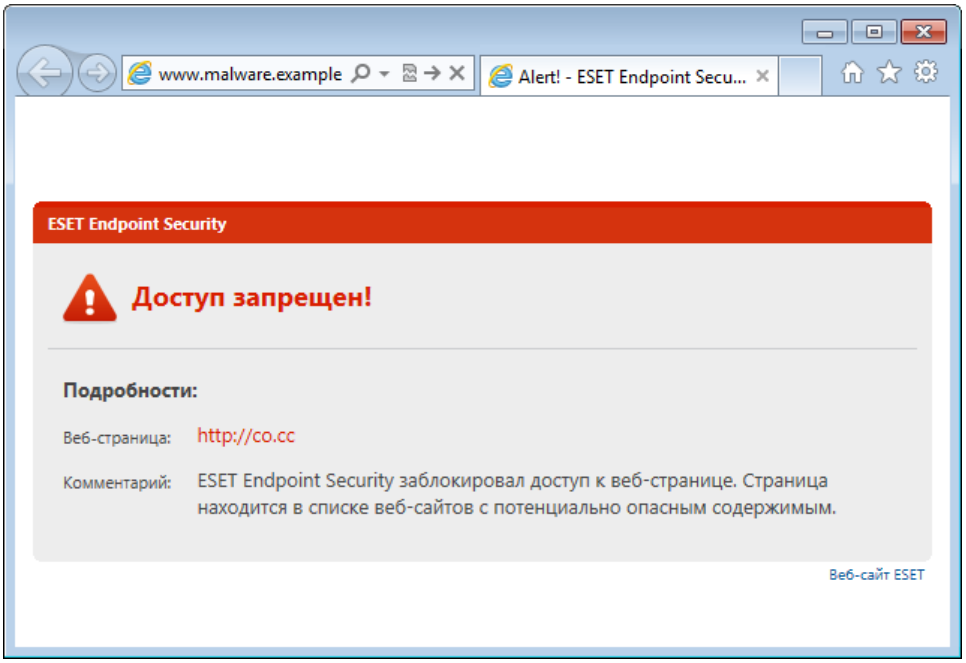
«Черный» список пользователя: открывает диалоговое окно, в котором можно добавить, изменить и удалить адреса электронной почты, считающиеся небезопасными. Сообщения электронной почты, адрес отправителя которых присутствует в «черном» списке, будут считаться спамом.

Список исключений пользователя: открывает диалоговое окно, в котором можно добавить, изменить и удалить адреса электронной почты, которые могут быть подделаны и использованы для отправки спама. Сообщения электронной почты, адрес отправителя которых присутствует в списке исключений, всегда будут сканироваться на предмет наличия спама. По умолчанию в списке исключений присутствуют адреса электронной почты из существующих учетных записей почтовых клиентов.

4.3.1 Защита доступа в Интернет

Подключение к Интернету стало стандартной функцией персонального компьютера. К сожалению, Интернет также стал и основной средой распространения злонамеренного кода. Защита доступа в Интернет работает путем отслеживания соединений между веб-браузерами и удаленными серверами в соответствии с правилами протоколов HTTP и HTTPS.

Термин «фишинг» обозначает преступную деятельность, в рамках которой используются методы социальной инженерии (манипулирование пользователем, направленное на получение конфиденциальной информации). Дополнительные сведения о ней см. в глоссарии. ESET Endpoint Security обеспечивает защиту от фишинга: веб-страницы, которые заведомо содержат подобные материалы, всегда блокируются.



Мы настоятельно рекомендуем включить защиту доступа в Интернет . Это можно сделать в главном окне ESET Endpoint Security, перейдя в раздел **Настройка** > **Интернет и электронная почта** > **Защита доступа в Интернет**.

4.3.1.1 HTTP, HTTPs

По умолчанию программа ESET Endpoint Security сконфигурирована на использование стандартов большинства веб-браузеров. Однако параметры модуля сканирования HTTP можно изменить в разделе **Дополнительные настройки** (F5) > **Интернет и электронная почта** > **Защита доступа в Интернет** > **HTTP, HTTPS**. В главном окне **Фильтр 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 (HTTP), 8080 и 3128 (прокси-сервер).

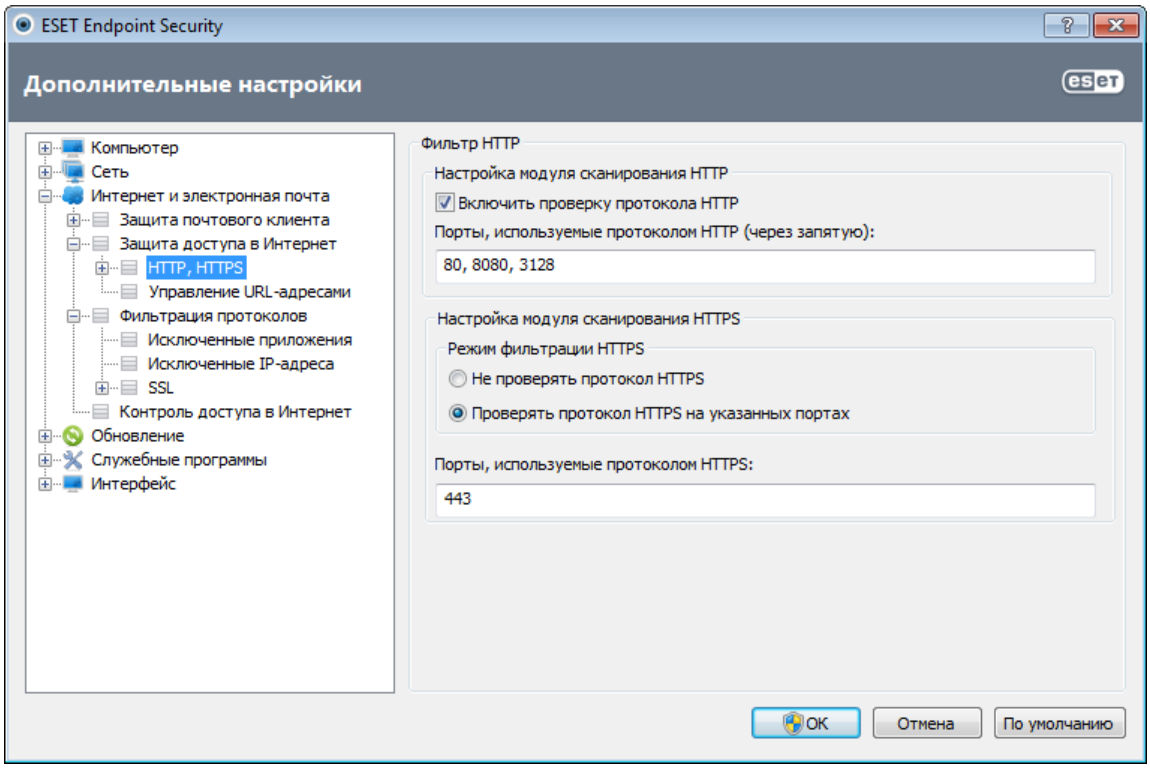
ESET Endpoint Security также поддерживает проверку протокола HTTPS. В этом типе соединения для передачи информации между сервером и клиентом используется зашифрованный канал. ESET Endpoint Security проверяет соединения, использующие методы шифрования SSL и TLS. Проверка HTTPS может выполняться в следующих режимах.

Не проверять протокол HTTPS: зашифрованные соединения не будут проверяться.

Проверять протокол HTTPS на указанных портах: соединения по протоколу HTTPS проверяются только на портах, указанных в параметре **Порты, используемые протоколом HTTPS**.

Проверять протокол HTTPS на указанных портах: проверяются только приложения, указанные в разделе Веб-браузеры и использующие порты, перечисленные в параметре **Порты, используемые протоколом HTTPS**. По умолчанию задан порт 443.

Зашифрованные соединения не будут сканироваться. Чтобы включить сканирование зашифрованных соединений и просмотреть настройки модуля сканирования, нажмите Проверка протокола SSL в разделе «Дополнительные настройки» (**Интернет и электронная почта** > **Фильтрация протоколов** > **SSL**) и установите флажок **Всегда сканировать протокол SSL**.



4.3.1.1.1 Активный режим для веб-браузеров

В ESET Endpoint Security также есть подменю **Активный режим**, которое определяет режим проверки для веб-браузеров.

Активный режим полезен, поскольку проверяет данные, которые передаются обращающимися к Интернету приложениями, в целом вне зависимости от того, помечены такие приложения как веб-браузеры или нет (дополнительные сведения см. в разделе Клиенты Интернета и электронной почты). Если он отключен, осуществляемый приложениями обмен данными контролируется 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. Активный режим работает описанным ниже образом. Когда находящееся под наблюдением приложение загружает данные, то

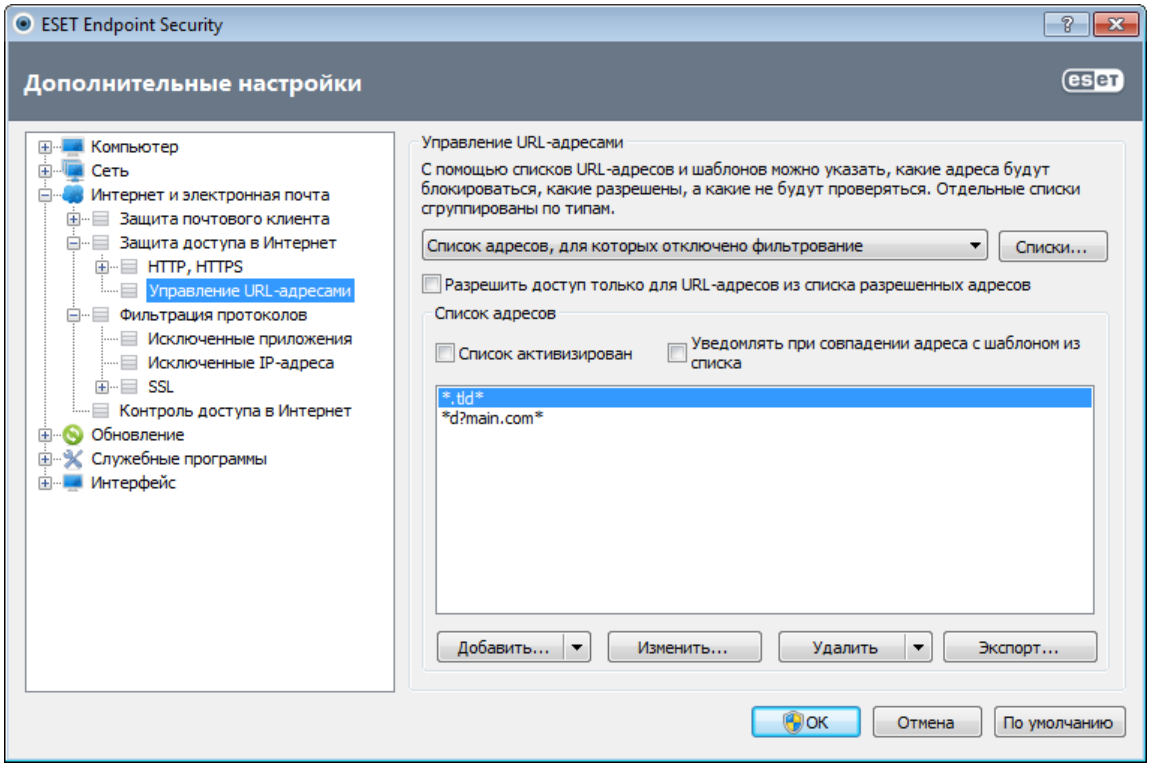
они сначала сохраняются во временном файле, созданном ESET Endpoint Security. В это время данные недоступны такому приложению. После окончания загрузки данные проверяются на наличие злонамеренного кода. Если не обнаружено заражение, данные отправляются в исходное приложение. Этот процесс обеспечивает полный контроль над соединениями, осуществляемыми находящимся под наблюдением приложением. В пассивном режиме данные сразу передаются запросившему их приложению, чтобы избежать задержек.

4.3.1.2 Управление URL-адресами

В разделе управления URL-адресами 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 будут недоступны. Веб-сайты из списка исключенных адресов загружаются без проверки на вредоносный код. Если выбрать вариант **Разрешить доступ только для URL-адресов из списка разрешенных адресов**, будут доступны только адреса из списка разрешенных, а остальные HTTP-адреса будут заблокированы.

Если добавить URL-адрес в **Список адресов, для которых отключено фильтрование**, этот адрес будет исключен из сканирования. Также можно разрешать или блокировать определенные адреса, добавляя их соответственно в **Список разрешенных адресов** или в **Список заблокированных адресов**. После нажатия кнопки **Списки...** на экран будет выведено окно **Списки HTTP-адресов и шаблонов**, где можно **Добавить** или **Удалить** списки адресов. Для добавление URL-адресов HTTPS в список должен быть активирован параметр **Всегда сканировать** протокол SSL.

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 совпадении адреса с шаблоном из списка**.



Добавить.../Из файла: позволяет добавить адрес в список вручную (**Добавить**) или из файла в текстовом формате (**Из файла**). Вариант **Из файла** также позволяет добавить несколько URL-адресов/масок из текстового файла.

Изменить...: позволяет вручную изменять адреса, например, добавляя символы маски («*» и «?»).

Удалить/Удалить все: нажмите кнопку **Удалить**, чтобы удалить из списка выделенный адрес. Для удаления всех адресов нажмите кнопку **Удалить все**.

Экспорт...: адреса из текущего списка сохраняются в простой текстовый файл.

4.3.2 Защита почтового клиента

Защита электронной почты обеспечивает контроль безопасности обмена данными по протоколам POP3 и IMAP. При использовании подключаемого модуля для Microsoft Outlook и других почтовых клиентов ESET Endpoint 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 протоколам POP3 и IMAP не зависит от используемого почтового клиента.

Параметры для этой функции настраиваются в разделе **Дополнительные настройки** > **Интернет и электронная почта** > **Защита почтового клиента**.

Настройка параметров модуля ThreatSense: расширенная настройка модуля сканирования для защиты от вирусов, которая позволяет конфигурировать объекты сканирования, методы обнаружения и т. д. Нажмите кнопку **Настройка...**, чтобы вывести на экран окно подробной настройки модуля сканирования.

После проверки к сообщению электронной почты может быть прикреплено уведомление с результатами сканирования. Можно выбрать вариант **Добавление уведомлений к полученным и прочитанным сообщениям**, а также **Добавление уведомлений к отправленным сообщениям**. На такие добавленные уведомления нельзя полагаться полностью, поскольку они могут затеряться в сложных сообщениях в формате HTML или быть сфабрикованы некоторыми вирусами. Уведомления могут быть добавлены к входящим и прочитанным сообщениям или к исходящим сообщениям (или и к тем, и к другим). Доступны следующие варианты.

- **Никогда**: уведомления не будут добавляться вообще.
- **Только для инфицированных сообщений**: будут отмечены только сообщения, содержащие злонамеренные программы (по умолчанию).
- **Во все просканированные сообщения электронной почты**: программа будет добавлять уведомления ко всем просканированным сообщениям электронной почты.

Добавление примечаний в поле темы полученных и прочитанных зараженных сообщений: установите этот флажок, если защитой электронной почты должны добавляться предупреждения о вирусах в тему зараженных сообщений. Эта функция позволяет осуществлять простую фильтрацию зараженных сообщений по теме (если поддерживается почтовым клиентом). Также она повышает уровень доверия для получателя, а в случае обнаружения заражения предоставляет важную информацию об уровне угрозы для конкретного сообщения или отправителя.

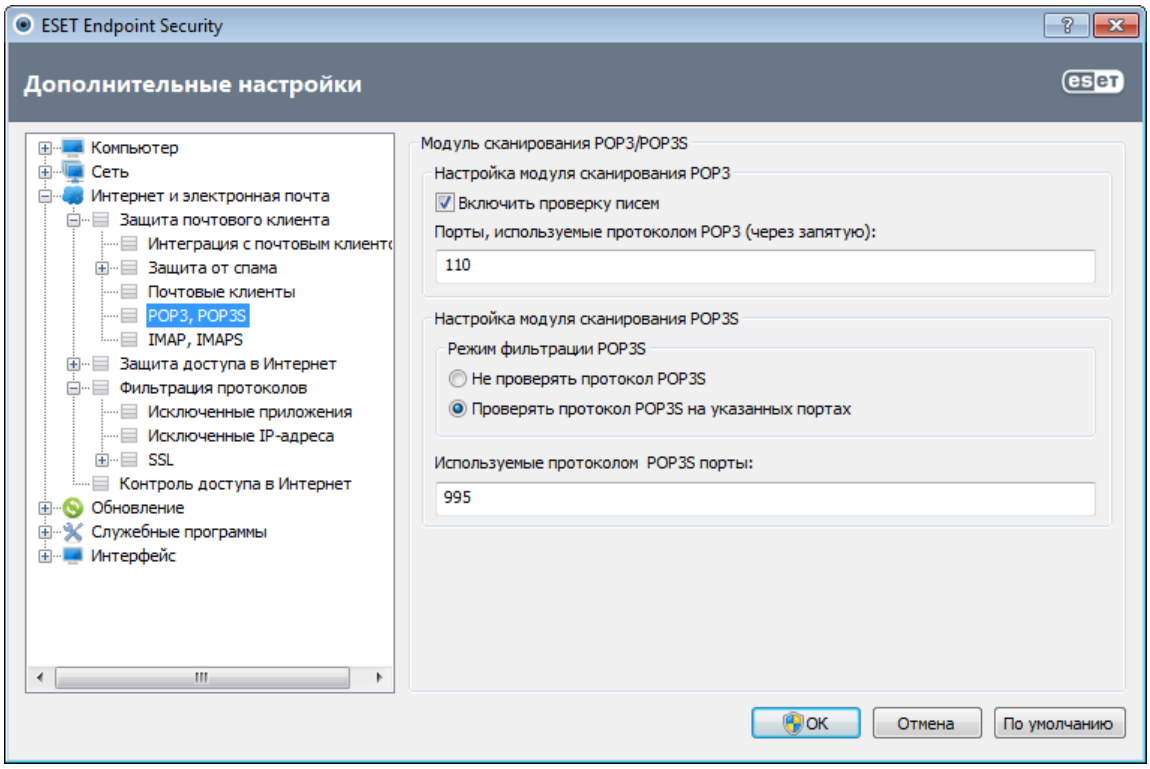
Шаблон добавления к теме зараженных писем: этот шаблон можно изменить, если нужно отредактировать формат префикса, добавляемого ко всем зараженным сообщениям. Эта функция заменит тему сообщения Hello при заданном значении префикса [virus] на такой формат: [virus] Hello. Переменная %VIRUSNAME% представляет обнаруженную угрозу.

4.3.2.1 Фильтр POP3, POP3S

POP3 — самый распространенный протокол, используемый для получения электронной почты в почтовых клиентах. ESET Endpoint 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.

Зашифрованные соединения не будут сканироваться. Чтобы включить сканирование зашифрованных соединений и просмотреть настройки модуля сканирования, нажмите Проверка протокола SSL в разделе «Дополнительные настройки» (**Интернет и электронная почта** > **Фильтрация протоколов** > **SSL**) и установите флажок **Всегда сканировать протокол SSL**.



В этом разделе можно конфигурировать проверку протоколов POP3 и POP3S.

Включить проверку писем: при включении этого параметра весь трафик, проходящий по протоколу POP3, проверяется на предмет наличия вредоносных программ.

Порты, используемые протоколом POP3: перечень портов, используемых протоколом POP3 (110 по умолчанию).

ESET Endpoint Security также поддерживает проверку протокола POP3S. В этом типе соединения для передачи информации между сервером и клиентом используется зашифрованный канал. ESET Endpoint Security проверяет соединения, использующие методы шифрования SSL и TLS.

Не проверять протокол POP3S: зашифрованные соединения не будут проверяться.

Проверять протокол POP3S на указанных портах: соединения по протоколу POP3S проверяются только на портах, указанных в параметре **Используемые протоколом POP3S порты**.

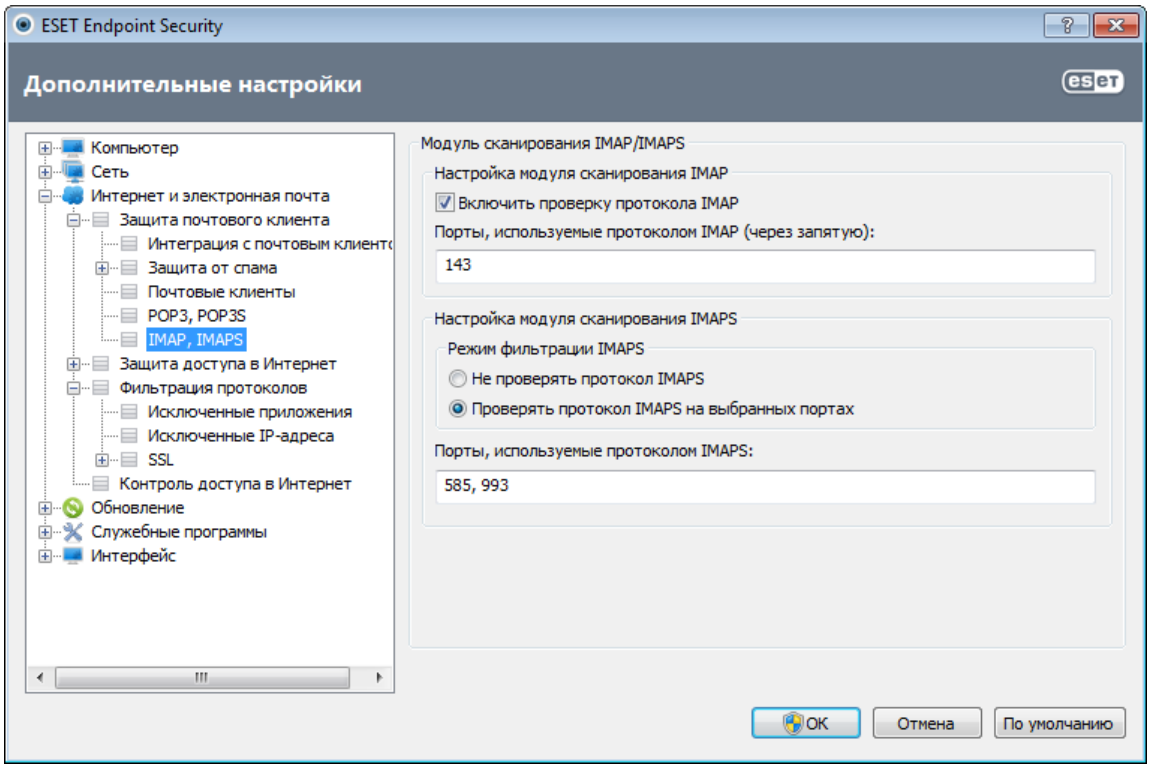
Используемые протоколом POP3S порты: перечень портов, используемых протоколом POP3S, которые следует проверять (995 по умолчанию).

4.3.2.2 Контроль протоколов IMAP, IMAPS

IMAP — еще один интернет-протокол для получения электронной почты. Он имеет определенные преимущества перед POP3. Например, сразу несколько клиентов могут одновременно подключаться к одному и тому же почтовому ящику и поддерживать сведения о состоянии сообщения, в частности о том, было ли оно прочитано или удалено, а также ответил ли пользователь на него. ESET Endpoint 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 IMAP осуществляется автоматически без необходимости в какой-либо дополнительной настройке конкретного почтового клиента. По умолчанию сканируются все соединения по порту 143, однако при необходимости могут быть добавлены и другие порты. Номера портов следует разделять запятыми.

Зашифрованные соединения не будут сканироваться. Чтобы включить сканирование зашифрованных соединений и просмотреть настройки модуля сканирования, нажмите Проверка протокола SSL в разделе «Дополнительные настройки» (**Интернет и электронная почта** > **Фильтрация протоколов** > **SSL**) и установите флажок **Всегда сканировать протокол SSL**.

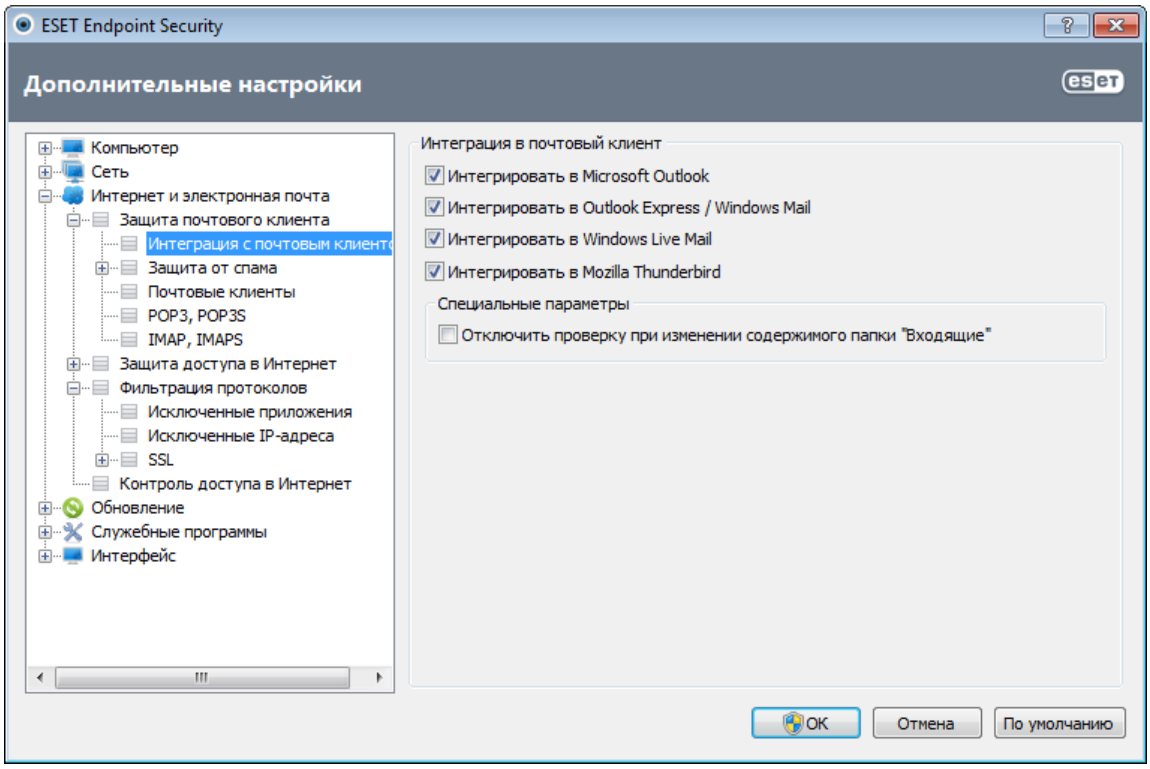


4.3.2.3 Интеграция с почтовыми клиентами

Интеграция ESET Endpoint 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 Endpoint Security. Если интеграция активирована, панель инструментов ESET Endpoint Security вставляется непосредственно в почтовый клиент, обеспечивая более эффективную защиту электронной почты. Параметры интеграции доступны в разделе **Настройка** > **Перейти к дополнительным настройкам...** > **Интернет и электронная почта** > **Защита почтового клиента** > **Интеграция с почтовым клиентом**.

В настоящий момент поддерживаются следующие почтовые клиенты: Microsoft Outlook, Outlook Express, почта Windows, почта Windows Live и Mozilla Thunderbird. Полный список поддерживаемых почтовых клиентов и их версий см. в статье базы знаний ESET.

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.



Даже если интеграция отключена, почтовые клиенты остаются защищены соответствующим модулем (для протоколов POP3, IMAP).

4.3.2.3.1 Конфигурация защиты почтового клиента

Модуль защиты электронной почты поддерживает следующие почтовые клиенты: Microsoft Outlook, Outlook Express, почта Windows, почта Windows Live и Mozilla Thunderbird. Защита электронной почты реализована в этих программах в виде подключаемого модуля. Главное преимущество подключаемого модуля заключается в том, что он не зависит от используемого протокола. При получении почтовым клиентом зашифрованного сообщения оно расшифровывается и передается модулю сканирования.

Сканируемая электронная почта

Полученные сообщения: включает или отключает проверку входящих сообщений.
Отправленные сообщения: включает или отключает проверку отправленных сообщений.
Прочитанные сообщения: включает или отключает проверку прочитанных сообщений.

Действие, которое следует применить к зараженным сообщениям

Ничего не предпринимать: в этом случае программа будет выявлять зараженные вложения, но не будет выполнять никаких действий с сообщениями электронной почты.
Удалить сообщение: программа будет уведомлять пользователя о заражениях и удалять сообщения.
Переместить сообщение в папку "Удаленные": зараженные сообщения будут автоматически перемещаться в папку **Удаленные**.
Переместить сообщение в папку: здесь можно указать собственную папку, в которую следует перемещать зараженные сообщения при их обнаружении.

Другое

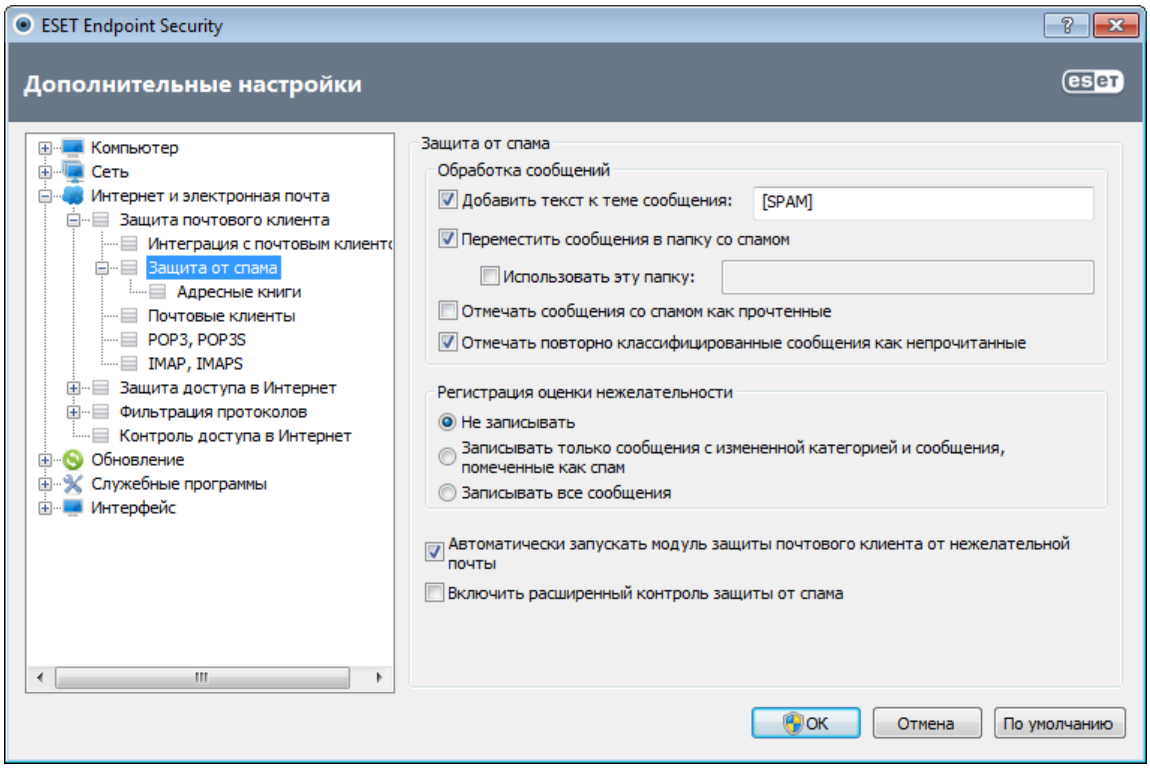
Повторить сканирование после обновления: включает или отключает повторное сканирование после обновления базы данных сигнатур вирусов.
Включить результаты сканирования другими модулями: если установлен этот флажок, модуль защиты электронной почты будет принимать результаты сканирования от других модулей защиты

4.3.2.4 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.

4.3.3 Защита от спама

Нежелательные сообщения, также называемые спамом, являются одной из самых серьезных проблем современных телекоммуникационных технологий. Доля спама в общем объеме передаваемых по электронной почте сообщений составляет около 80 %. Защита от спама ограждает от этой проблемы. Используя несколько эффективных принципов, модуль защиты от спама обеспечивает более качественную фильтрацию, чтобы поддерживать папку входящих сообщений в порядке.



Одним из важнейших принципов обнаружения спама является его распознавание на основе предварительно определенных списков доверенных («белый» список) и нежелательных («черный» список) адресов. Все адреса, найденные в адресной книге почтового клиента, автоматически попадают в «белый» список, а остальные адреса должны быть помечены пользователем как безопасные.

Основным методом, используемым для обнаружения спама, является сканирование свойств сообщения. Полученные сообщения сканируются на основные критерии защиты от спама (определения сообщения, статистические эвристики, алгоритмы распознавания и другие уникальные методы). Результатом работы этих методов является значение индекса, по которому можно с высокой степенью достоверности определить, является ли сообщение спамом.

Защита от спама в ESET Endpoint Security позволяет задать другие параметры для работы со списками рассылки. Доступны следующие параметры.

Автоматически запускать модуль защиты почтового клиента от нежелательной почты: активация или отключение защиты почтового клиента от спама.

Обработка сообщений

Добавить текст к теме сообщения: позволяет добавлять настраиваемую строку префикса в поле темы сообщений, которые классифицированы как спам. Строка по умолчанию — [SPAM].

Переместить сообщения в папку со спамом: если этот флажок установлен, нежелательные сообщения будут перемещены в папку нежелательной почты по умолчанию.

Использовать эту папку: этот параметр позволяет перемещать спам в папку, указанную пользователем.

Отмечать сообщения со спамом как прочтенные: установите этот флажок, чтобы автоматически помечать нежелательные сообщения как прочитанные. Это помогает сосредоточиться на «чистых» сообщениях.

Отмечать повторно классифицированные сообщения как непрочитанные: сообщения, первоначально классифицированные как спам, а затем помеченные как «чистые», будут отображаться как непрочитанные.

Регистрация оценки нежелательности

Ядро защиты от спама ESET Endpoint Security присваивает оценку нежелательности каждому просканированному сообщению. Данное сообщение будет записано в журнал защиты от спама (**ESET Endpoint Security** > **Служебные программы** > **Файлы журнала** > **Защита от спама**).

- **Не записывать**: ячейка **Оценка** в журнале защиты от спама останется пустой.
- **Записывать только сообщения с измененной категорией и сообщения, помеченные как спам**: если установить этот переключатель, для сообщений, помеченных как спам, будет регистрироваться оценка нежелательности.
- **Записывать все сообщения**: в журнале будут регистрироваться все сообщения вместе с оценкой нежелательности.

Автоматически запускать модуль защиты почтового клиента от нежелательной почты: если этот флажок установлен, защита от спама будет автоматически активироваться при загрузке компьютера.

Включить расширенный контроль защиты от спама: будет загружена дополнительная база данных, которая повысит эффективность защиты от нежелательной почты.

ESET Endpoint Security поддерживает защиту от спама для Microsoft Outlook, Outlook Express, почты Windows, почты Windows Live и Mozilla Thunderbird.

4.3.3.1 Добавление адресов в «белый» и «черный» списки

Адреса электронной почты, принадлежащие лицам, с которыми пользователь часто общается, можно добавить в «белый» список, чтобы отправляемые с этих адресов сообщения никогда не классифицировались как спам. Известные адреса отправителей спама можно добавить в «черный» список, чтобы отправляемые с них сообщения всегда классифицировались как спам. Для добавления нового адреса в «белый» или «черный» список щелкните сообщение правой кнопкой мыши и выберите **ESET Endpoint Security** > **Добавить в «белый» список** или **Добавить в «черный» список** или нажмите кнопку **Доверенный адрес** или **Адрес отправителя спама** в панели инструментов защиты от спама ESET Endpoint Security в почтовом клиенте.

Точно так же этот процесс может применяться к адресам отправителей спама. Если адрес электронной почты содержится в «черном» списке, каждое сообщение электронной почты, отправленное с этого адреса, будет классифицировано как спам.

4.3.3.2 Пометка сообщений как спама

Любое сообщение, просматриваемое в почтовом клиенте, может быть помечено как спам. Для этого нужно щелкнуть его правой кнопкой мыши и нажать **ESET Endpoint Security** > **Классифицировать выбранные сообщения как спам** или **Адрес отправителя спама** в панели инструментов модуля защиты от спама ESET Endpoint Security, которая расположена в верхней части окна почтового клиента.

При классификации сообщение автоматически помещается в папку спама, но адрес отправителя не вносится в «черный» список. Сходным образом происходит классификация сообщений как нормальных. Если сообщения из папки **нежелательной почты** классифицируются как полезные, они перемещаются в исходную папку. При этом адрес отправителя не вносится автоматически в «белый» список.

4.3.4 Фильтрация протоколов

Защита от вирусов протоколов приложений 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 просмотра зашифрованного соединения (SSL) выберите пункт **Фильтрация протоколов** > **SSL**.

Включить фильтрацию содержимого протоколов уровня приложений: если этот флажок установлен, все данные, обмен которыми осуществляется по протоколам HTTP(S), POP3(S) и IMAP(S), будет проверяться модулем сканирования для защиты от вирусов.

ПРИМЕЧАНИЕ. Начиная с ОС Windows Vista с пакетом обновления 1 и Windows 7, для проверки сетевых подключений используется новая архитектура платформы фильтрации Windows (WFP). Так как в технологии платформы фильтрации Windows используются особые методы отслеживания, следующие параметры недоступны.

- **Порты HTTP и POP3**: маршрутизация трафика на внутренний прокси-сервер осуществляется только для портов HTTP и POP3.
- **Приложения, помеченные как веб-браузеры и почтовые клиенты**: на внутренний прокси-сервер перенаправляется только трафик приложений, помеченных как браузеры и почтовые клиенты (**Интернет и электронная почта** > **Фильтрация протоколов** > **Клиенты Интернета и электронной почты**).
- **Порты и приложения, помеченные как веб-браузеры или почтовые клиенты**: маршрутизация трафика на внутренний прокси-сервер осуществляется как для портов HTTP и POP3, так и для приложений, помеченных как браузеры и почтовые клиенты.

4.3.4.1 Клиенты Интернета и электронной почты

ПРИМЕЧАНИЕ. Начиная с ОС Windows Vista с пакетом обновления 1 и Windows 7, для проверки сетевых подключений используется новая архитектура платформы фильтрации Windows (WFP). Так как в технологии платформы фильтрации Windows используются особые методы отслеживания, раздел **Клиенты Интернета и электронной почты** недоступен.

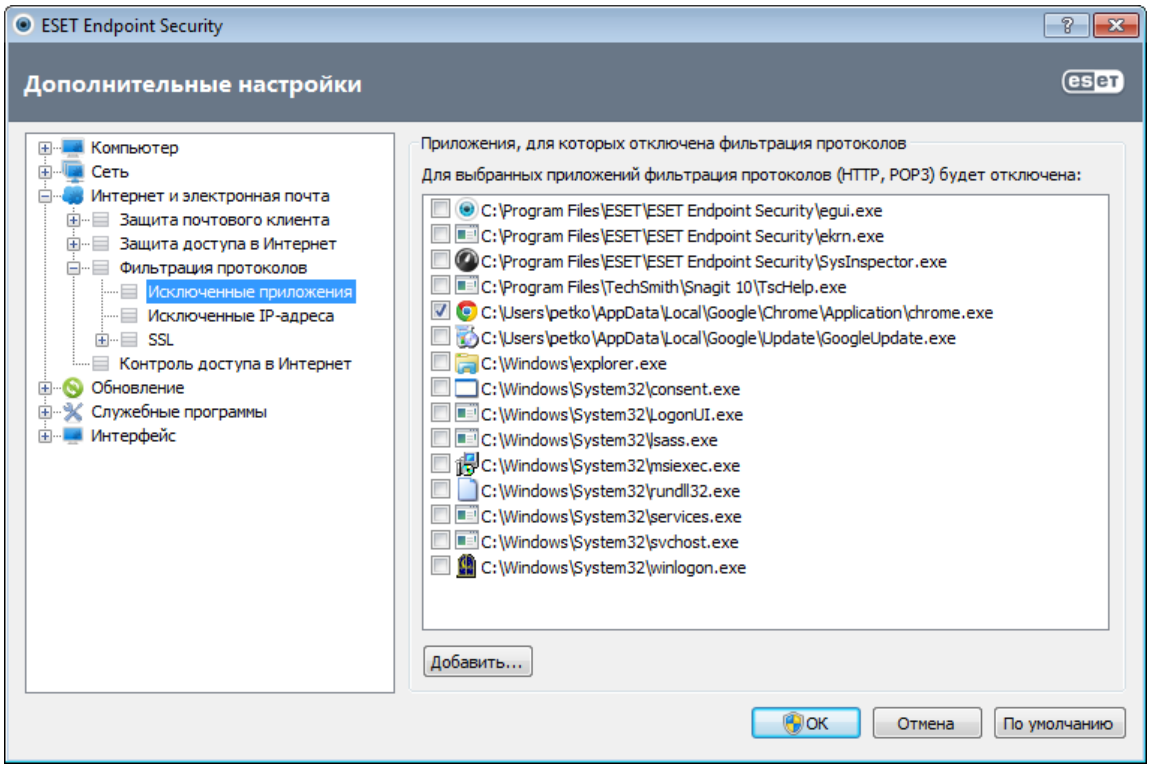
В условиях перенасыщенности Интернета вредоносными программами безопасное посещение веб-страниц является важным аспектом защиты компьютера. Уязвимости веб-браузеров и мошеннические ссылки позволяют вредоносным программам незаметно проникать в систему. Именно поэтому в программном обеспечении ESET Endpoint Security основное внимание уделяется обеспечению безопасности веб-браузеров. Каждое приложение, обращающееся к сети, может быть помечено как веб-браузер. Флажок имеет два состояния.

- **Не установлен**: соединения приложений фильтруются только для указанных портов.
- **Установлен**: соединения всегда фильтруются (даже если задан другой порт).

4.3.4.2 Исключенные приложения

Для исключения соединений определенных сетевых приложений из фильтрации содержимого выделите их в списке. Соединения выделенных приложений по протоколам HTTP/POP3/IMAP не будут проверяться на наличие угроз. Рекомендуется использовать эту возможность только для тех приложений, которые работают некорректно, если их соединения проверяются.

Запуск приложений и служб будет доступен автоматически. Нажмите кнопку **Добавить**, чтобы вручную выбрать приложение, отсутствующее в списке фильтрации протоколов.

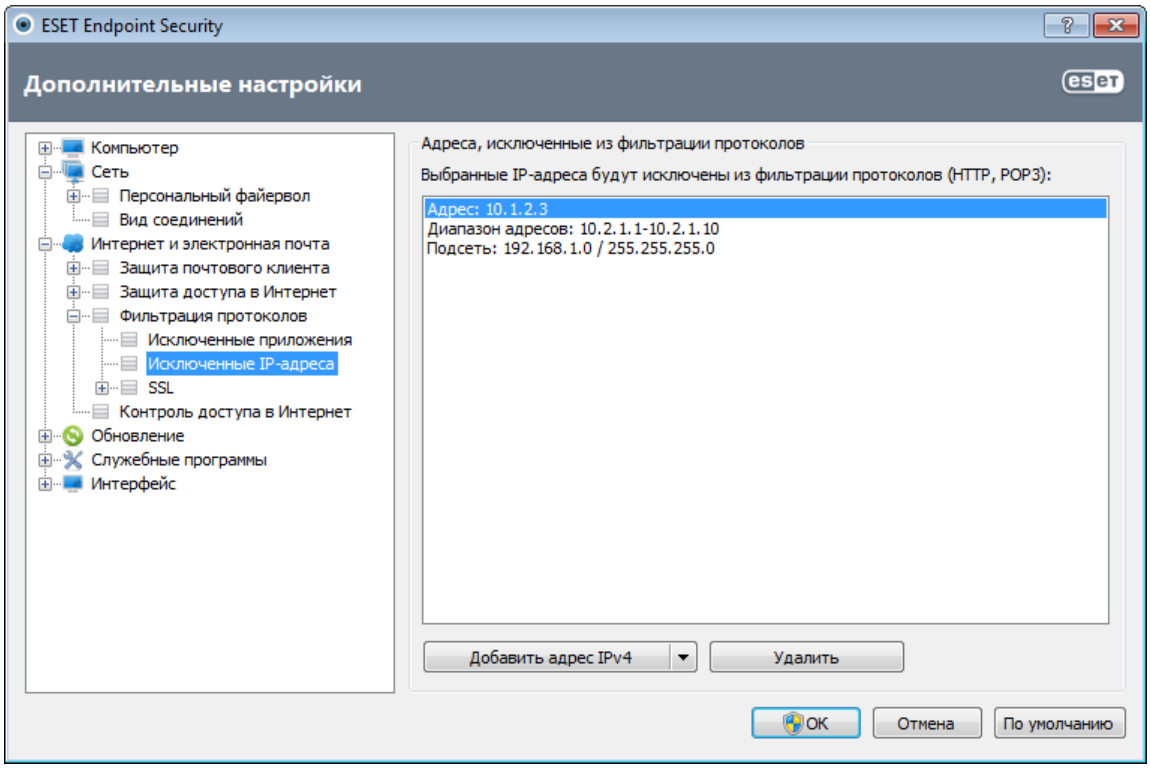


4.3.4.3 Исключенные IP-адреса

Записи в списке адресов будут исключены из фильтрации содержимого протоколов. Соединения по протоколам HTTP/POP3/IMAP, в которых участвуют выбранные адреса, не будут проверяться на наличие угроз. Этот параметр рекомендуется использовать только для заслуживающих доверия адресов.

Добавить адрес IPv4/IPv6: этот параметр позволяет добавить IP-адрес, диапазон адресов или маску подсети удаленной конечной точки, к которой должно быть применено правило.

Удалить: удаление выделенных записей из списка.



4.3.4.3.1 Добавление адреса IPv4

Эта функция позволяет добавить IP-адрес, диапазон адресов или маску подсети удаленной конечной точки, к которой должно быть применено правило. Интернет-протокол версии 4 (IPv4) — это устаревшая версия, но она до сих пор широко используется.

Отдельный адрес: добавляет IP-адрес отдельного компьютера, для которого должно быть применено правило (например, 192.168.0.10).

Диапазон адресов: введите начальный и конечный IP-адреса, чтобы задать тем самым диапазон IP-адресов (или несколько компьютеров), к которым следует применить правило (например, от 192.168.0.1 до 192.168.0.99).

Подсеть: подсеть (группа компьютеров), заданная IP-адресом и маской.

Например, 255.255.255.0 — это маска сети для префикса 192.168.1.0/24, который означает диапазон адресов от 192.168.1.1 до 192.168.1.254.

4.3.4.3.2 Добавление адреса IPv6

Этот функция позволяет добавить IPv6-адрес, диапазон адресов или маску подсети удаленной конечной точки, к которой должно быть применено правило. Это новейшая версия интернет-протокола, и в будущем она заменит более старую версию 4.

Отдельный адрес: добавляет IP-адрес отдельного компьютера, для которого должно быть применено правило (например, 2001:718:1c01:16:214:22ff:fec9:ca5).

Подсеть: подсеть (группа компьютеров), заданная IP-адресом и маской (например, 2002:c0a8:6301:1::1/64).

4.3.4.4 Проверка протокола SSL

ESET Endpoint 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 не получит уведомления, 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.

Применить созданные исключения на основе сертификатов: активирует использование при сканировании SSL-соединений исключений, указанных в исключенных и доверенных сертификатах. Для включения этого параметра выберите **Всегда сканировать протокол SSL**.

Блокировать шифрованное соединение с использованием устаревшего протокола SSL версии 2: соединения, использующие более раннюю версию протокола SSL, будут автоматически блокироваться.

4.3.4.4.1 Сертификаты

Для нормальной работы защищенных SSL-соединений в браузерах и почтовых клиентах необходимо добавить корневой сертификат ESET, spol. s r.o. в список известных корневых сертификатов (издателей). Поэтому должен быть активирован параметр **Добавить корневой сертификат к известным браузерам**. Установите этот флажок, чтобы автоматически добавить корневой сертификат ESET в известные браузеры (например, Opera, Firefox). Для браузеров, использующих системное хранилище сертификатов (например, Internet Explorer), сертификат добавляется автоматически. Для установки сертификата в неподдерживаемые браузеры выберите **Просмотреть сертификат** > **Дополнительно** > **Копировать в файл...**, а затем вручную импортируйте его в браузер.

В некоторых случаях сертификат невозможно проверить с помощью хранилища доверенных корневых сертификатов сертифицирующих органов (например, VeriSign). Это значит, что у сертификата существует собственная подпись какого-либо другого субъекта (например, администратора веб-сервера или небольшой компании) и принятие решения о выборе такого сертификата как доверенного не всегда представляет опасность. Большинство крупных компаний (например, банки) используют сертификаты, подписанные TRCA. Если установлен флажок **Запрашивать действительность сертификата** (по умолчанию), пользователю будет предложено выбрать действие, которое следует предпринять, когда устанавливается зашифрованное соединение. На экран будет выведено диалоговое окно для выбора действия, в котором можно принять решение о том, что следует сделать: пометить сертификат как доверенный или как исключенный. Если сертификат отсутствует в списке хранилища доверенных корневых сертификатов сертифицирующих органов, для оформления окна используется красный цвет. Если же сертификат есть в этом списке, окно будет оформлено зеленым цветом.

Можно выбрать вариант **Блокировать соединения, использующие сертификат**, чтобы всегда разрывать зашифрованные соединения с сайтом, использующим непроверенный сертификат.

Если этот сертификат недействителен или поврежден, это значит, что истек срок действия сертификата или же используется неверное собственное заверение. В этом случае рекомендуется блокировать соединения, использующие данный сертификат.

4.3.4.4.1.1 Доверенные сертификаты

В дополнение к встроенному хранилищу доверенных корневых сертификатов сертифицирующих органов, где ESET Endpoint Security хранит доверенные сертификаты, можно также создать собственный список доверенных сертификатов, доступный в разделе **Дополнительные настройки** (F5) > **Интернет и электронная почта** > **Фильтрация протоколов** > **SSL** > **Сертификаты** > **Доверенные сертификаты**. ESET Endpoint Security будет проверять содержимое зашифрованных соединений, используя сертификаты из этого списка.

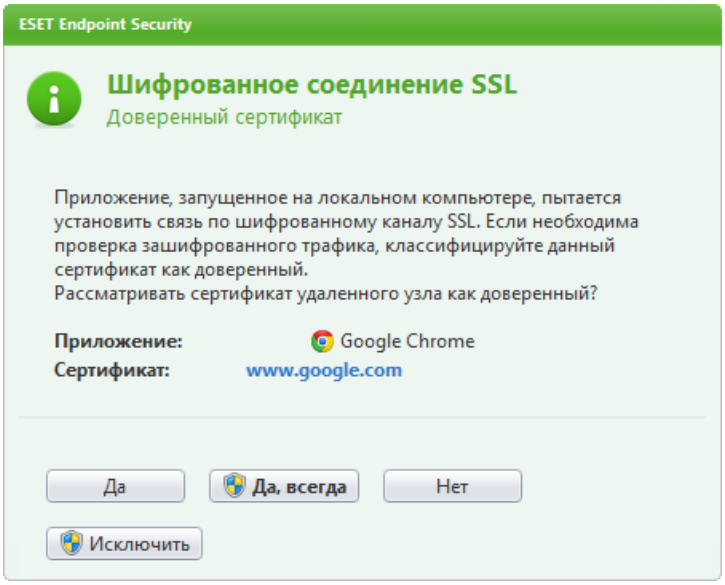
Для удаления выделенных элементов из списка нажмите кнопку **Удалить**. Установите флажок **Показать** (или дважды щелкните нужный сертификат), чтобы вывести на экран информацию о выбранном сертификате.

4.3.4.4.1.2 Исключенные сертификаты

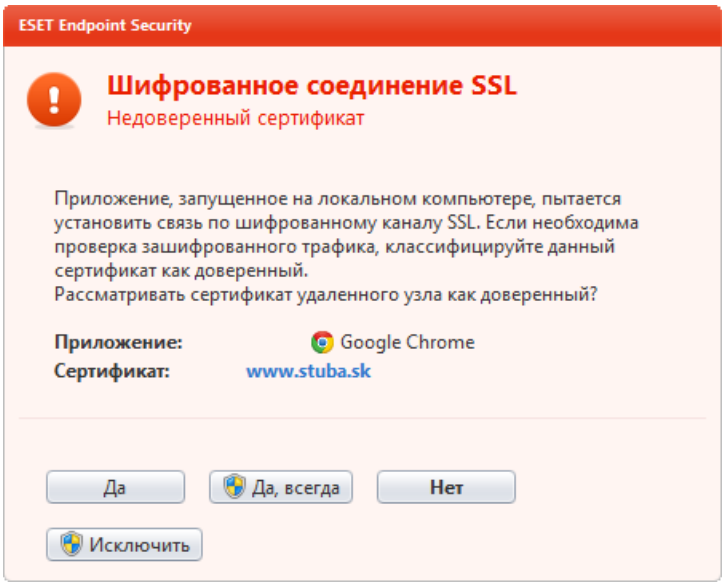
В разделе «Исключенные сертификаты» перечислены сертификаты, которые считаются безопасными. Содержимое зашифрованных соединений, использующих сертификаты из данного списка, не будет проверяться на наличие угроз. Рекомендуется исключать только те веб-сертификаты, которые гарантированно являются безопасными, а соединение с их использованием не нуждается в проверке. Для удаления выделенных элементов из списка нажмите кнопку **Удалить**. Установите флажок **Показать** (или дважды щелкните нужный сертификат), чтобы вывести на экран информацию о выбранном сертификате.

4.3.4.4.1.3 Шифрованное соединение SSL

Если компьютер сконфигурирован на сканирование протокола SSL, при попытке установить зашифрованное соединение (с использованием неизвестного сертификата) на экран может быть выведено диалоговое окно, предлагающее выбрать действие. Это диалоговое окно содержит следующие данные: название приложения, которое устанавливает соединение, и название используемого сертификата.



Если сертификат не находится в хранилище доверенных корневых сертификатов сертифицирующих органов, он считается ненадежным.



Для сертификатов доступны следующие действия.

Да: сертификат будет временно помечен как доверенный для текущего сеанса, при следующей попытке его использования окно с предупреждением не выводится.

Да, всегда: сертификат помечается как доверенный и добавляется в список доверенных сертификатов, для которых окно предупреждения не выводится.

Нет: сертификат помечается как ненадежный для текущего сеанса, при следующих попытках его использования на экран будет выведено окно предупреждения.

Исключить: сертификат добавляется в список исключенных, а данные, которые передаются по этому зашифрованному каналу, вообще не будут проверяться.

4.4 Контроль доступа в Интернет

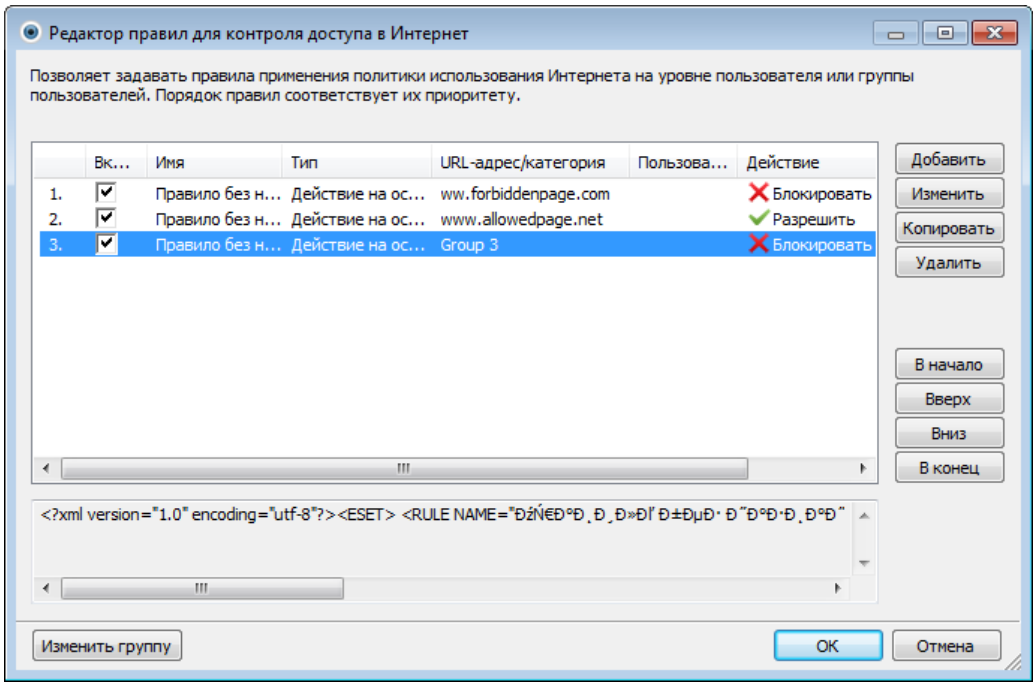
В разделе «Контроль доступа в Интернет» можно настроить параметры, которые защитят вашу компанию от опасности юридических исков. В нем указываются адреса веб-сайтов, которые нарушают права на интеллектуальную собственность. Цель заключается в предотвращении доступа сотрудников к страницам с неприемлемым или опасным содержимым, а также к ресурсам, посещение которых может отрицательно сказаться на эффективности работы.

Контроль доступа в Интернет позволяет блокировать веб-страницы, на которых могут быть потенциально нежелательные материалы. Кроме того, работодатели или системные администраторы могут запрещать доступ к более 27 предварительно заданным категориям и более 140 подкатегориям веб-сайтов.

Параметры контроля доступа в Интернет можно изменить в разделе **Дополнительные настройки** (F5) > **Контроль доступа в Интернет**. Если выбрать параметр **Интеграция с системой**, контроль доступа в Интернет будет интегрирован с ESET Endpoint Security, а также будет активирована кнопка **Настроить правила...**, позволяющая открыть окно Редактор правил для контроля доступа в Интернет.

4.4.1 Правила контроля доступа в Интернет

В окне **Редактор правил для контроля доступа в Интернет** отображаются правила для URL-адресов и категорий веб-страниц.



В списке правил представлен ряд их описаний, например имена, тип блокирования, действие, выполняемое при срабатывании правила контроля доступа в Интернет, а также вносимая в журнал серьезность.

Для управления правилом используйте кнопки **Создать** или **Изменить**. Чтобы создать правило с использованием заранее заданных параметров из другого правила, нажмите кнопку **Копировать**. XML-строки, которые отображаются, если щелкнуть правило, можно скопировать в буфер обмена. Кроме того, они могут помочь системным администраторам экспортировать или импортировать эти данные, а также использовать их, например, в ESET Remote Administrator.

Чтобы выделить несколько правил, щелкните их, удерживая нажатой клавишу CTRL. Затем их можно будет одновременно удалить либо переместить к началу или концу списка. Флажок **Включено** позволяет включить или отключить правило. Это может быть полезно, если вы не хотите полностью удалять правило, чтобы воспользоваться им позднее.

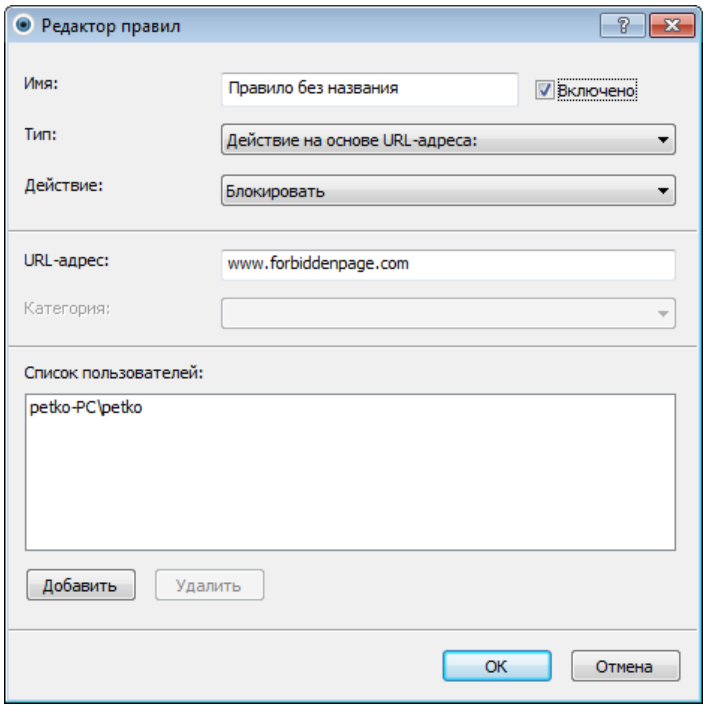
Управление основано на правилах, которые отсортированы по приоритету: правила с более высоким приоритетом находятся в начале.

Чтобы открыть контекстное меню правила, щелкните его правой кнопкой мыши. В нем для правила можно настроить степень детализации (серьезность) записей в журнале. Записи журнала можно просмотреть в главном окне ESET Endpoint Security в разделе **Служебные программы** > **Файлы журнала**.

Нажмите кнопку **Изменить группу**, чтобы открыть окно редактора групп, в котором можно добавлять и удалять заранее заданные категории и подкатегории, относящиеся к соответствующим группам.

4.4.2 Добавление правил контроля доступа в Интернет

В окне «Правила контроля доступа в Интернет» можно вручную создавать или изменять правила фильтрации для контроля доступа в Интернет.



Чтобы упростить идентификацию правила, введите его описание в поле **Имя**. Чтобы включить или отключить правило, установите или снимите флажок **Включено**. Это может быть полезно в том случае, если вы не хотите полностью удалять правило.

Тип действия

- **Действие на основе URL-адреса**: доступ к нужному веб-сайту. Введите соответствующий адрес в поле **URL-адрес**.
- **Действие на основе категории**: при активации этой функции нужно выбрать категорию в раскрывающемся меню **Категория**.

Во всех списках URL-адресов нельзя использовать специальные символы «*» (звездочка) и «?» (вопросительный знак). Например, вручную нужно вводить адреса веб-страниц с несколькими доменами верхнего уровня (examplepage.com, examplepage.sk и т. д.). При внесении домена в список все содержимое, расположенное в нем и во всех поддоменах (например, sub.examplepage.com), будет разрешено или заблокировано в зависимости от действий на основе URL-адреса.

Действие

- **Разрешить**: к адресу URL или категории будет предоставлен доступ.
- **Блокировать**: адрес URL или категория будут заблокированы.

Список пользователей

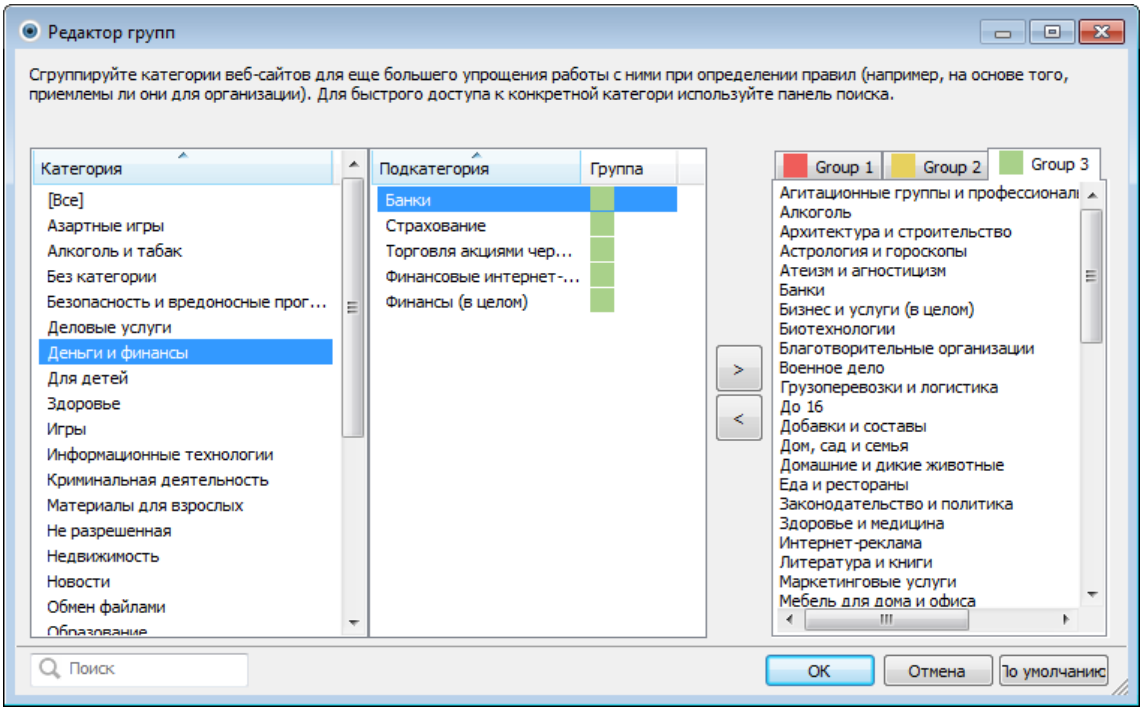
- **Добавить**: открывается диалоговое окно **Тип объекта: пользователи и группы**, в котором можно выбрать нужных пользователей.
- **Удалить**: выбранный пользователь удаляется из фильтра.

4.4.3 Редактор групп

Окно редактора групп разделено на две части. В правой представлен список категорий и подкатегорий. Чтобы просмотреть подкатегории, выберите нужную категорию в списке **Категория**. Большинство подкатегорий относятся к группам, отмеченным цветом.

В красной группе содержатся подкатегории, связанные с содержимым для взрослых или неприемлемыми материалами. В зеленой же группе, наоборот, представлены категории веб-страниц, которые признаны подходящими для просмотра.

Выделенную подкатегорию можно добавить в нужную группу или удалить из нее с помощью стрелок.



Примечание. Подкатегория может относиться только к одной группе. Некоторые подкатегории не включены в заранее заданные группы (например, «Игры»). Чтобы они использовались фильтром контроля доступа в Интернет, добавьте их в нужную группу. Если добавляемая подкатегория уже входит в другую группу, то она будет удалена из нее и перенесена в выбранную группу.

Чтобы найти группу, введите запрос в поле **Поиск** в нижнем левом углу окна.

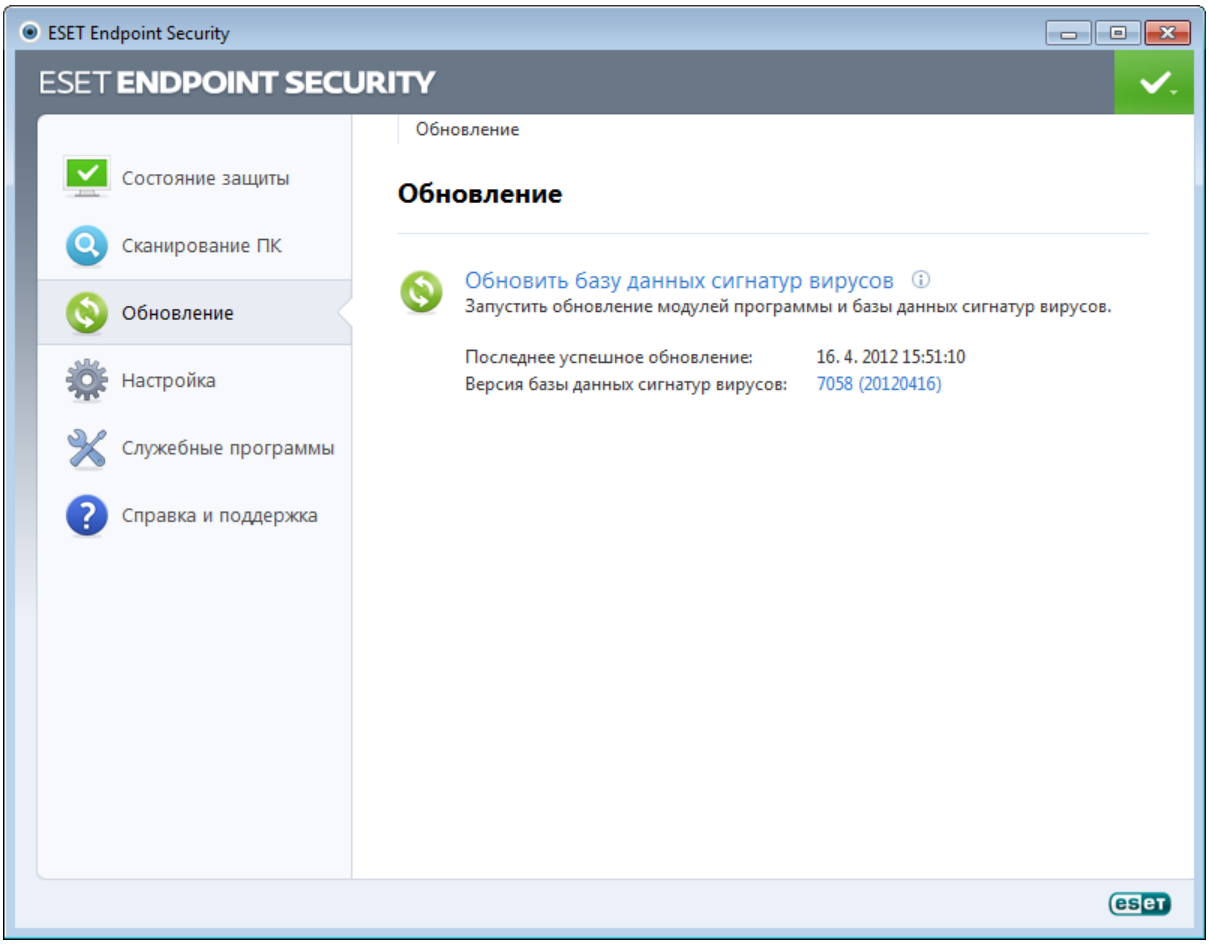
4.5 Обновление программы

Регулярное обновление ESET Endpoint Security — лучший способ добиться максимального уровня безопасности компьютера. Модуль обновления поддерживает актуальность программы двумя способами: путем обновления базы данных сигнатур вирусов и путем обновления компонентов системы.

Выбрав пункт **Обновление** в главном окне программы, 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, вы можете вручную запустить обновление — **Обновить базу данных сигнатур вирусов**. Обновление базы данных сигнатур вирусов и компонентов программы является важнейшей частью обеспечения полной защиты компьютера от злонамеренного кода. Уделите особое внимание изучению конфигурирования и работы этого процесса. Если в процессе установки не были указаны сведения о лицензии (имя пользователя и пароль), их можно ввести при обновлении, чтобы получить доступ к серверам обновлений ESET.

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

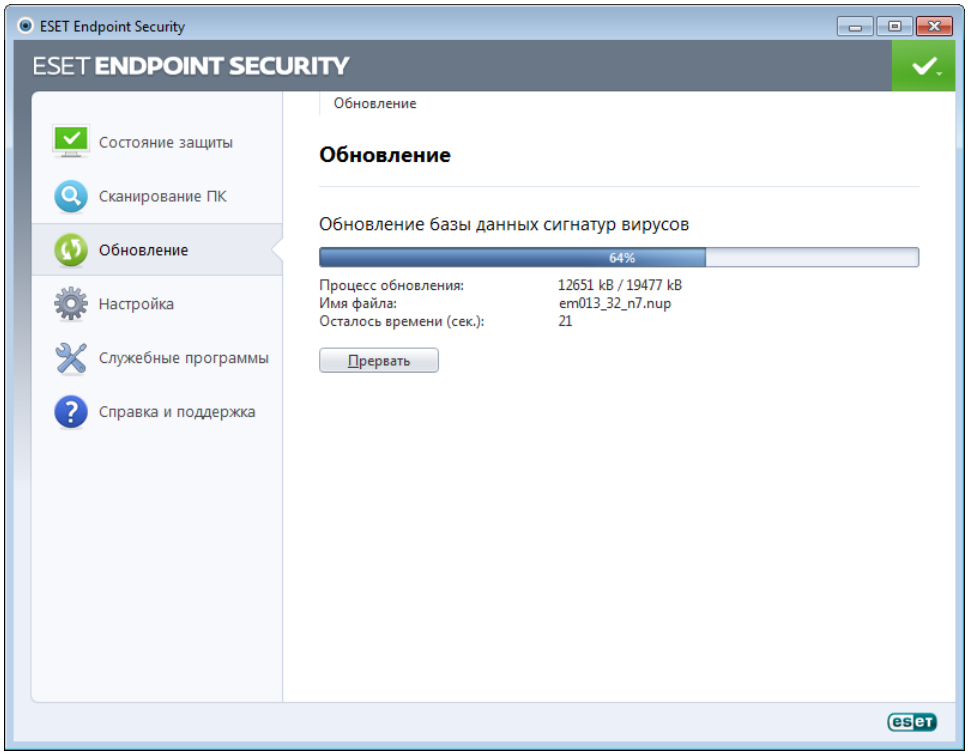


Последнее успешное обновление — дата последнего обновления. Следует убедиться, что в этом поле указана недавняя дата, поскольку это значит, что база данных сигнатур вирусов актуальна.

База данных сигнатур вирусов: номер версии базы данных сигнатур вирусов, также являющийся активной ссылкой на веб-сайт ESET. Эту ссылку можно нажать, чтобы просмотреть все сигнатуры, добавленные в данном обновлении.

Процесс обновления

После нажатия **Обновить базу данных сигнатур вирусов** начинается процесс загрузки. На экран будут выведены индикатор выполнения загрузки и время до ее окончания. Чтобы прервать процесс обновления, нажмите **Прервать**.

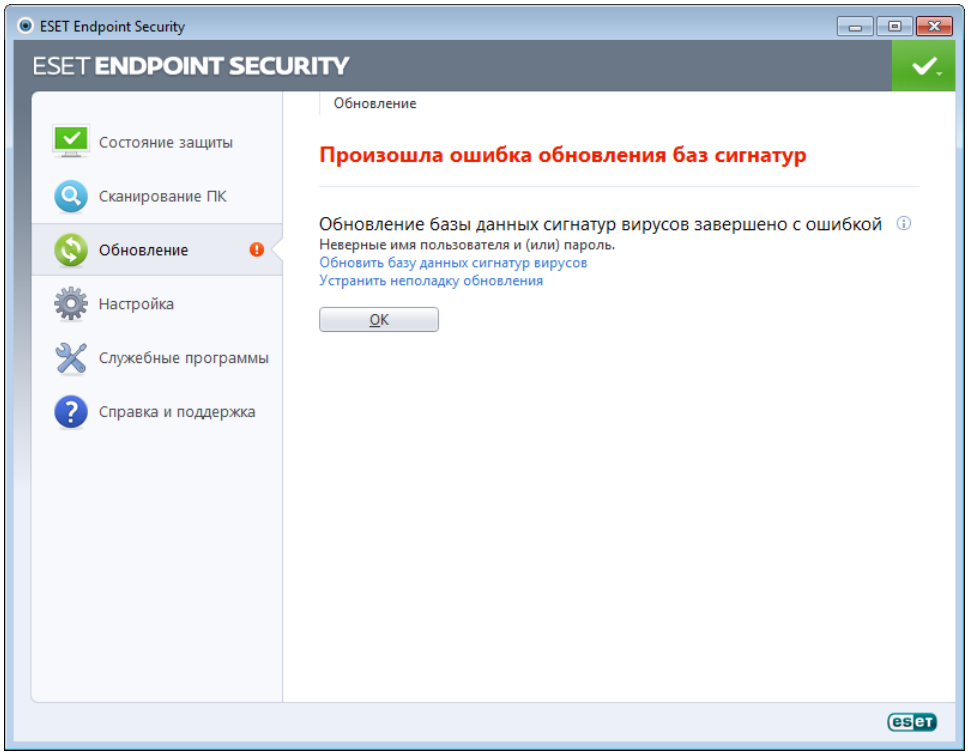


Внимание! В обычных обстоятельствах после нормального завершения загрузки в окне **Обновление** будет выведено сообщение **Обновления не требуется — установлена последняя база данных сигнатур вирусов**. Если этого сообщения нет, программа устарела. При этом повышается риск заражения. Необходимо обновить базу данных сигнатур вирусов как можно скорее. В противном случае на экран будет выведено одно из следующих сообщений.

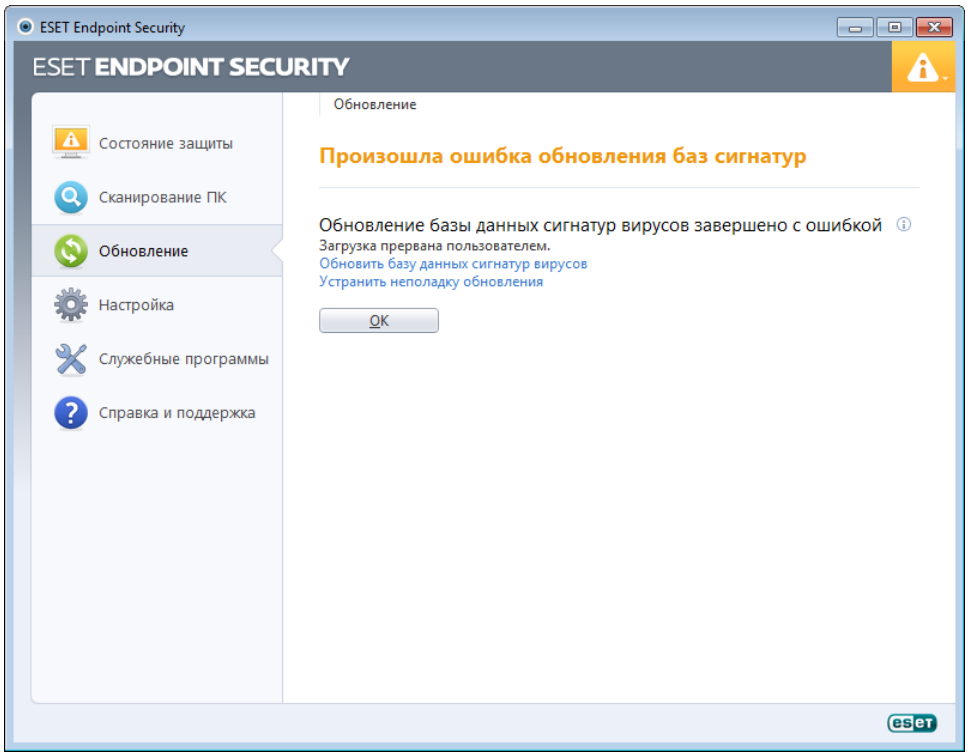
База данных сигнатур вирусов устарела: эта ошибка появится после нескольких неудачных попыток обновить базу данных сигнатур вирусов. Рекомендуется проверить параметры обновлений. Наиболее частая причина этой ошибки — неправильно введенные данные для аутентификации или неверно сконфигурированные параметры подключения.

Предыдущее уведомление связано с двумя указанными ниже сообщениями об ошибках при обновлении (**Произошла ошибка обновления баз сигнатур**).

1. **Неверные имя пользователя и (или) пароль**: указаны неправильное имя пользователя и пароль при настройке обновлений. Рекомендуется проверить данные аутентификации. В окне «Дополнительные настройки» (выберите пункт **Настройка** в главном меню, после чего нажмите **Перейти к дополнительным настройкам...** или F5 на клавиатуре) содержатся расширенные параметры обновления. Выберите **Обновление** > **Общие** в дереве расширенных параметров, чтобы ввести новые имя пользователя и пароль.



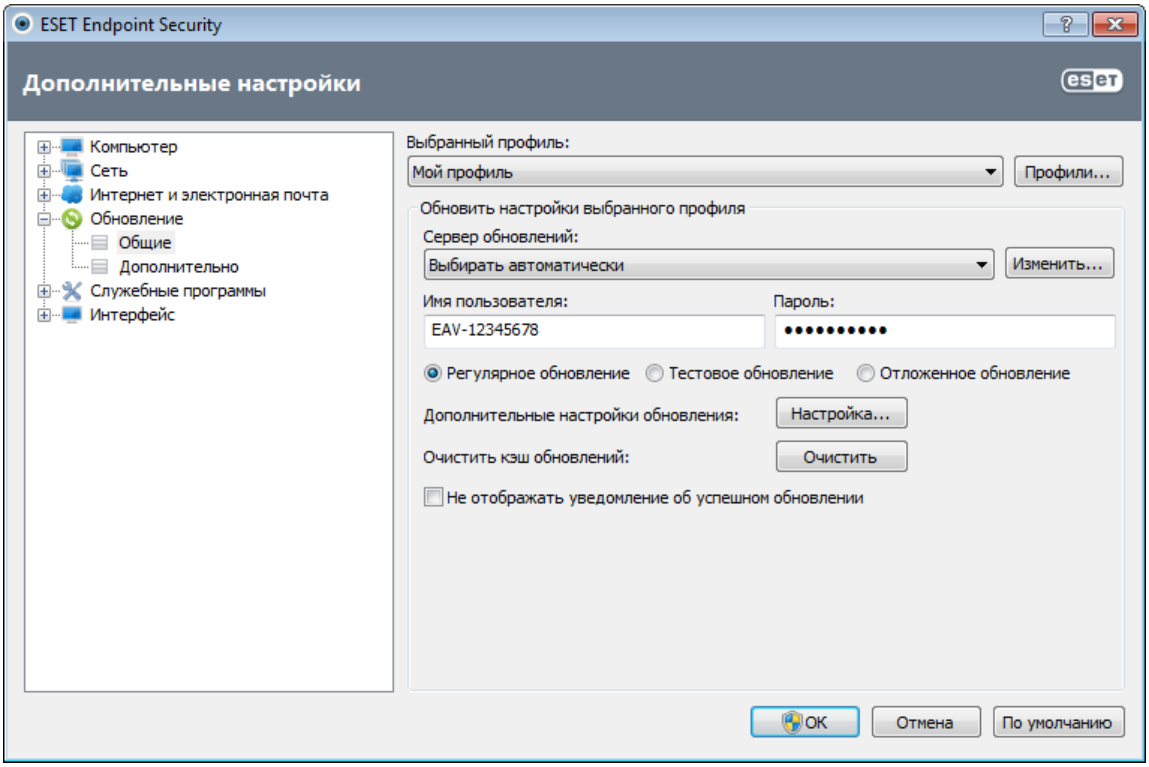
2. **Произошла ошибка при загрузке файлов обновлений**: возможная причина этой ошибки — неверные параметры подключения к Интернету. Рекомендуется проверить наличие подключения к Интернету (например, попробуйте открыть любой веб-сайт в браузере). Если веб-сайт не открывается, возможно, не установлено подключение к Интернету или на компьютере возникли какие-либо проблемы с подключением к сети. Обратитесь к своему поставщику услуг Интернета, чтобы выяснить, есть ли у вас активное подключение к Интернету.



4.5.1 Настройка обновлений

Параметры обновлений доступны в дереве **Дополнительные настройки** (клавиша F5) в разделе **Обновление** > **Общие**. В этом разделе указывается информация об источниках обновлений, таких 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 наименее загруженного сервера ESET.

Для обеспечения правильной загрузки обновлений необходимо корректно задать все эти параметры. Если используется файервол, программе должно быть разрешено обмениваться данными через Интернет (например, соединение по протоколу HTTP).



Выбранный в данный момент профиль обновлений отображается в раскрывающемся меню **Выбранный профиль**. Нажмите кнопку **Профили**, чтобы создать новый профиль.

Список доступных серверов обновлений можно просмотреть с помощью раскрывающегося меню **Сервер обновлений**. Сервер обновлений — это компьютер, на котором хранятся файлы обновлений. При использовании сервера ESET следует использовать параметр по умолчанию **Выбирать автоматически**. Для добавления нового сервера обновлений нажмите кнопку **Изменить...** в разделе **Обновить настройки выбранного профиля**, а затем кнопку **Добавить**.

При использовании локального HTTP-сервера, который также называется зеркалом, сервер обновлений должен быть указан следующим образом:
http://имя_компьютера_или_его_IP-адрес:2221.

При использовании локального HTTP-сервера с поддержкой SSL, сервер обновлений должен быть указан следующим образом:
https://имя_компьютера_или_его_IP-адрес:2221.

Для аутентификации на серверах обновлений используются **имя пользователя** и **пароль**, созданные и отправленные вам после покупки. При использовании локального сервера зеркала проверка зависит от его конфигурации. По умолчанию проверка не требуется, то есть поля **Имя пользователя** и **Пароль** остаются пустыми.

Тестовые обновления (параметр **Тестовое обновление**) — это обновления, которые уже прошли внутреннее тестирование и в ближайшее время будут доступны всем пользователям. Преимущество их использования заключается в том, что у вас появляется доступ к новейшим методам обнаружения и исправлениям. Однако такие обновления иногда могут быть недостаточно стабильны и НЕ ДОЛЖНЫ использоваться на производственных серверах и рабочих станциях, где необходимы максимальные работоспособность и стабильность. Список текущих модулей доступен в разделе **Справка и поддержка** > **О программе ESET Endpoint Security**. Неопытным пользователям рекомендуется оставить выбранный по умолчанию вариант

Регулярное обновление. Сотрудники компаний могут выбрать параметр **Отложенное обновление**. В таком случае базы данных сигнатур вирусов будут обновляться с особых серверов с задержкой не менее X часов, т. е. после того, как они будут протестированы в реальных средах и признаны стабильными.

Нажмите кнопку **Настройка...** рядом с **Дополнительные настройки обновления**, чтобы вывести на экран окно с расширенными параметрами обновлений.

При возникновении проблем с обновлениями нажмите кнопку **Очистить...**, чтобы удалить содержимое папки с временными файлами обновлений.

Не отображать уведомление об успешном обновлении: отключает уведомления на панели задач в правом нижнем углу экрана. Этот параметр удобно использовать, если какое-либо приложение или игра работает в полноэкранном режиме. Обратите внимание, что Режим презентации отключает все уведомления.

4.5.1.1 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 серверов обновлений можно просмотреть в раскрывающемся меню **Сервер обновлений**. Для добавления нового сервера обновлений нажмите кнопку **Изменить...** в разделе **Обновить настройки выбранного профиля**, а затем кнопку **Добавить**.

4.5.1.2 Дополнительные настройки обновления

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

4.5.1.2.1 Режим обновления

Вкладка **Режим обновления** содержит параметры, относящиеся к обновлениям компонентов программы. Программа позволяет предопределить ее поведение в тех случаях, когда становятся доступны обновления компонентов.

Обновления компонентов программы активируют новые функции или вносят изменения в уже существующие. Это действие может выполняться как в автоматическом режиме без вмешательства пользователя, так и с уведомлением. После установки обновления компонентов программы может потребоваться перезагрузка компьютера. В разделе **Обновление компонентов программы** доступны три описанных далее варианта.

- **Никогда не обновлять компоненты программы**: обновление компонентов программы выполняться не будет. Этот вариант подходит для серверной установки, поскольку серверы обычно перезапускаются только при техническом обслуживании.
- **Выполнять обновление компонентов программы, если доступно**: обновления компонентов программы будут автоматически загружаться и устанавливаться. Обратите внимание на то, что может потребоваться перезагрузка компьютера.
- **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 перечисленных далее вариантов.

- **Никогда не перезапускать компьютер**: запрос на перезагрузку не будет отображаться даже в тех случаях, когда это необходимо. Выбирать этот вариант не рекомендуется, так как компьютер может работать некорректно до следующей перезагрузки.
- **Предложить перезапуск компьютера, если необходимо** — параметр по умолчанию. После обновления компонентов программы будет предлагаться перезагрузить компьютер.
- **Если необходимо, перезапустить компьютер без уведомления**: после обновления компонентов

программы компьютер, если это необходимо, будет перезагружен.

ПРИМЕЧАНИЕ. 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.

Если выбран вариант **Запрашивать подтверждение перед загрузкой обновления**, на экран будет выведено уведомление, когда будет доступно новое обновление.

Если размер файла обновления больше значения, указанного в параметре **Запрашивать подтверждение, если размер обновления превышает**, на экран будет выведено уведомление.

4.5.1.2.2 Прокси-сервер

Для доступа к параметрам настройки прокси-сервера для конкретного профиля обновлений щелкните **Обновление** в дереве расширенных параметров (F5), а затем нажмите кнопку **Настройка...** справа от пункта **Дополнительные настройки обновления**. Перейдите на вкладку **Прокси HTTP** и выберите один из трех перечисленных далее вариантов.

- **Использовать общие параметры прокси-сервера**
- **Не использовать прокси-сервер**
- **Соединение через прокси-сервер**

Если выбрать вариант **Использовать общие параметры прокси-сервера**, будут использоваться параметры конфигурации прокси-сервера, уже заданные в разделе **Служебные программы** > **Прокси-сервер** дерева расширенных параметров.

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

Флажок **Соединение через прокси-сервер** должен быть установлен в следующих случаях.

- Для обновления ESET Endpoint Security должен использоваться прокси-сервер, отличный от указанного в глобальных параметрах (**Служебные программы** > **Прокси-сервер**). В этом случае нужно указать параметры: адрес (поле **Прокси-сервер**), **порт** для соединения, а также при необходимости **имя пользователя** и **пароль**.
- Не были заданы общие параметры прокси-сервера, однако ESET Endpoint Security будет подключаться к прокси-серверу для получения обновлений.
- Компьютер подключается к Интернету через прокси-сервер. Параметры берутся из Internet Explorer в процессе установки программы, но при их изменении впоследствии (например, при смене поставщика услуг Интернета) нужно убедиться в том, что параметры прокси HTTP верны, в этом окне. Если этого не сделать, программа не сможет подключаться к серверам обновлений.

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

ПРИМЕЧАНИЕ. Данные для аутентификации, такие как **имя пользователя** и **пароль**, предназначены для доступа к прокси-серверу. Заполнять эти поля необходимо только в том случае, если имя пользователя и пароль нужны. Следует обратить внимание на то, что эти поля не имеют отношения к имени пользователя и паролю для программного обеспечения ESET Endpoint Security и должны быть заполнены только в том случае, если подключение к Интернету осуществляется через защищенный паролем прокси-сервер.

4.5.1.2.3 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** доступны следующие варианты: **Учетная запись системы (по умолчанию)**, **Текущий пользователь** и **Указанный пользователь**.

Выберите вариант **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. Этот метод следует использовать в тех случаях, когда невозможно установить соединение с помощью учетной записи системы. Обратите внимание на то, что указанная учетная запись должна обладать правами на доступ к каталогу на локальном сервере, в котором хранятся файлы обновлений. В противном случае программа не сможет установить соединение и загрузить обновления.

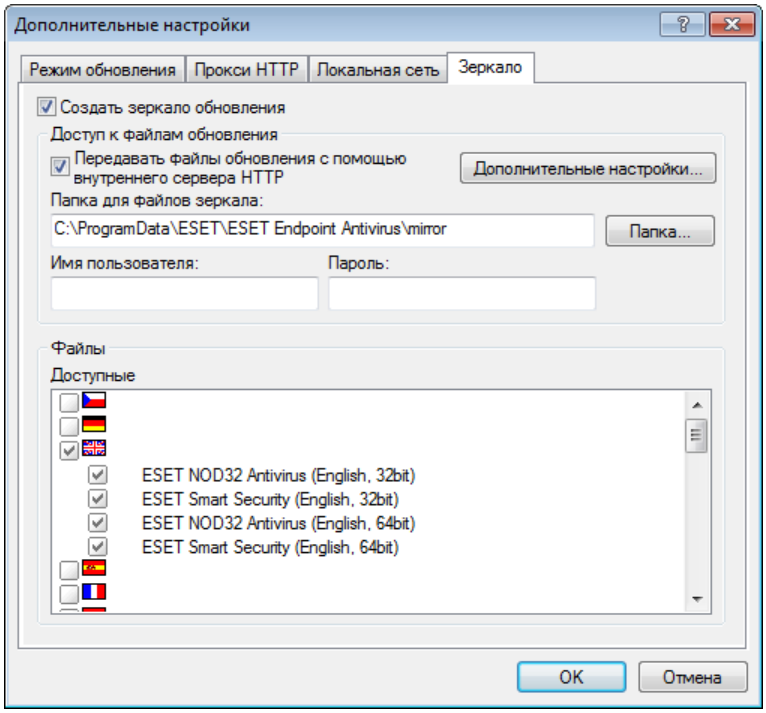
Внимание: Если выбран вариант **Текущий пользователь** или **Указанный пользователь**, может произойти ошибка при изменении учетной записи программы. В главном разделе параметров обновления рекомендуется указывать данные для аутентификации в локальной сети. В этом разделе параметров обновлений укажите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

Выберите параметр **Отключиться от сервера после завершения обновления** в том случае, если подключение к серверу остается активным после загрузки обновлений.

4.5.1.2.4 Создание копий обновлений, зеркало

ESET Endpoint Security позволяет создавать копии файлов обновлений, которые могут использоваться для обновления других рабочих станций в сети. Создание «зеркала» (копии файлов обновлений в локальной сети) — удобный способ избежать загрузки одних и тех же обновлений с сервера производителя всеми рабочими станциями. Файлы централизованно загружаются на локальный сервер зеркала, а затем распространяются на рабочие станции. Это позволяет избежать возможного перерасхода трафика. 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 Endpoint 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**, а затем 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.

Передавать файлы обновления с помощью внутреннего сервера HTTP: если этот параметр активирован,

файлы обновлений будут доступны просто по протоколу HTTP, причем имя пользователя и пароль не нужны. Для того чтобы настроить дополнительные параметры зеркала, нажмите кнопку Дополнительные настройки....

Примечание. HTTP-серверу необходима ОС Windows XP с пакетом обновления 2 или более поздней версии.

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 быть представлена как общая сетевая папка или как HTTP-сервер.

Папка, предназначенная для хранения файлов обновлений для зеркала, указывается в разделе **Папка для файлов зеркала**. 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**. Если выбранная папка назначения расположена на сетевом диске на компьютере под управлением ОС Windows NT/2000/XP, указанные имя пользователя и пароль должны принадлежать пользователю с правами на запись в указанную папку. 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. Такие языковые версии должны поддерживаться в настоящий момент сервером зеркала, сконфигурированным пользователем. Языковые версии можно настроить в списке **Доступные версии**.

4.5.1.2.4.1 Обновление с зеркала

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

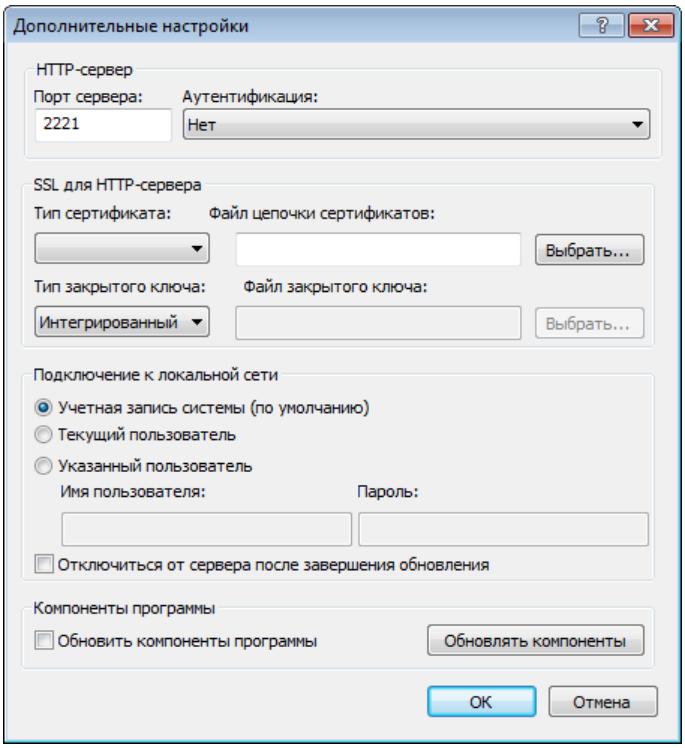
Доступ к файлам зеркала с помощью внутреннего сервера HTTP

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 указанные ниже варианты. **Ничего**, **Основное** и **NTLM**. Для того чтобы использовать кодировку 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.

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

Чтобы использовать HTTP-сервер с поддержкой протокола HTTPS (SSL), прикрепите свой **файл цепочки сертификатов** (или создайте самозаверяющий сертификат). Доступны указанные ниже типы. **ASN**, **PEM** и **PFX**. Файлы обновлений можно загружать по протоколу HTTPS, который обеспечивает дополнительный уровень защиты. При его использовании практически невозможно отследить передаваемые сведения и учетные данные. Для параметра **Файл закрытого ключа** по умолчанию установлено значение **Интегрированный** (соответственно, параметр **Файл закрытого ключа** по умолчанию неактивен). При этом закрытый ключ является частью выбранного файла цепочки сертификатов.



После завершения настройки зеркала следует воспользоваться рабочими станциями и добавить новый сервер обновлений. Для этого выполните следующие действия.

- Откройте раздел **Дополнительные настройки ESET Endpoint Security** и выберите **Обновление** > **Общие**.
- Нажмите кнопку **Изменить...** справа от раскрывающегося меню **Сервер обновлений** и добавьте адрес нового сервера в одном из указанных ниже форматов.
  http://IP_адрес_нового_сервера:2221
  https://IP_адрес_нового_сервера:2221 (при использовании SSL)
- Выберите 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 Endpoint Security из папки зеркала.

Далее необходимо указать способ доступа 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 нему. Для этого откройте в ESET Endpoint Security раздел **Дополнительные настройки** (F5) и выберите ветвь **Обновление** > **Общие**. 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 Endpoint Security и выберите **Обновление** > **Общие**.
- Нажмите кнопку **Изменить...** рядом с сервером обновления и добавьте новый в формате \\UNC-ИМЯ_КОМПЬЮТЕРА\ПУТЬ.
- Выберите вновь добавленный сервер из списка серверов обновлений.

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

Последний раздел контролирует компоненты программы (PCU). По умолчанию после загрузки они готовы для копирования на локальное зеркало. Если установлен флажок **Обновлять компоненты программы**, не нужно выбирать параметр **Обновлять компоненты**, т. к. доступные файлы автоматически копируются на локальное зеркало. Дополнительные сведения об обновлении компонентов программы см. в разделе Режим обновления.

4.5.1.2.4.2 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 Endpoint 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** в системе Windows, выберите **Выполнить**, вставьте имя папки и нажмите кнопку **OK**. На экран должно быть выведено содержимое папки.

При попытке обновления ESET Endpoint 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.

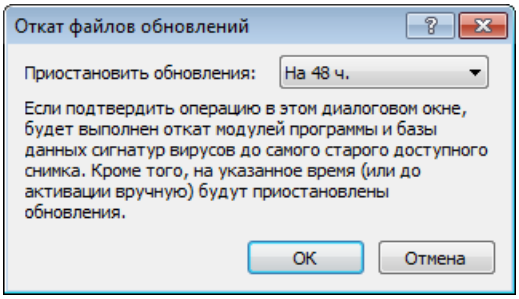
Ошибка при подключении ESET Endpoint Security к серверу зеркала: подключение к порту, указанному для доступа к HTTP-версии зеркала, блокируется.

4.5.1.3 Откат обновления

Если вы предполагаете, что последнее обновление базы данных сигнатур вирусов нестабильно или повреждено, вы можете выполнить откат к предыдущей версии, а также отключить любые обновления за выбранный период времени. Кроме того, вы можете включить ранее отключенные обновления.

ESET Endpoint Security позволяет выполнять резервное копирование и восстановление (так называемый откат) баз данных сигнатур вирусов. Чтобы включить создание их снимков, установите флажок **Создать снимки файлов обновлений**. В поле **Количество снимков в локальной системе** указывается количество снимков базы данных сигнатур вирусов, хранящихся в файловой системе локального компьютера.

После нажатия кнопки **Откат** (**Дополнительные настройки** (F5) > **Обновление** > **Дополнительно**) в раскрывающемся меню **Приостановить обновления** выберите промежуток времени, на который будет приостановлено обновление базы данных сигнатур вирусов и модулей программы.

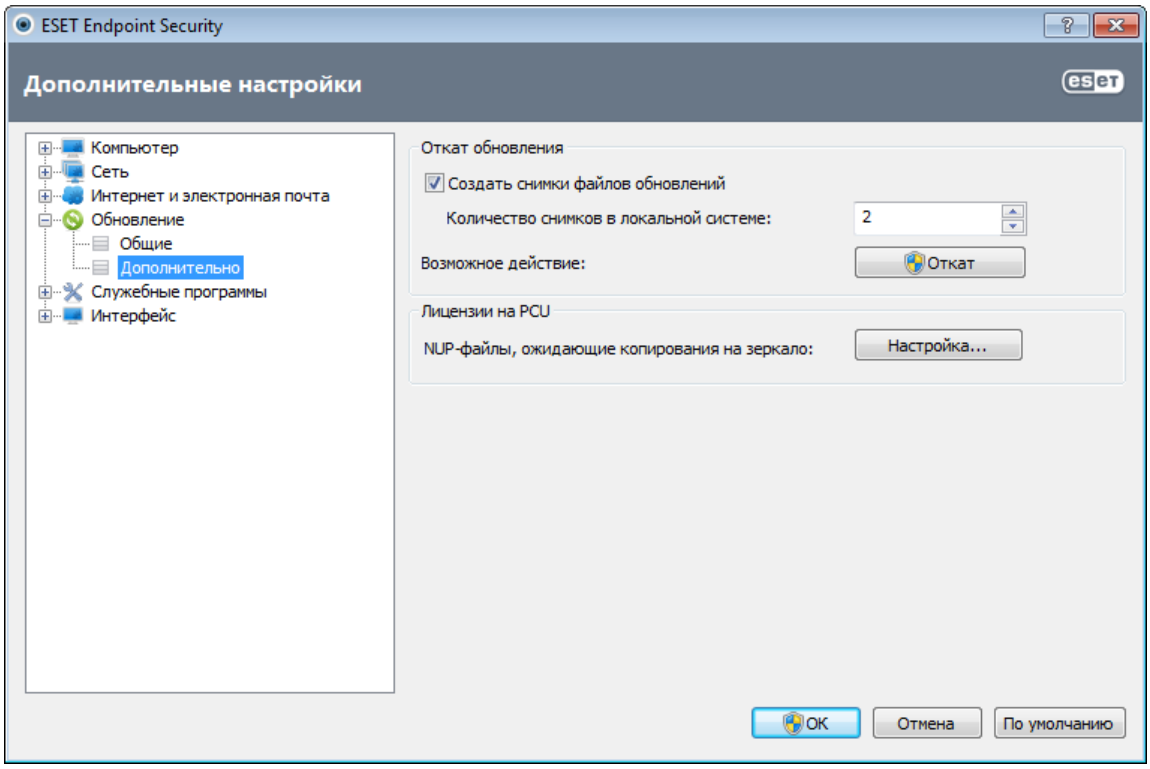


Чтобы регулярные обновления можно было возобновить только вручную, выберите вариант **До отзыва**. Поскольку он подвергает систему опасности, его не рекомендуется использовать.

После отката кнопка **Откат** заменяется на **Разрешить обновления**. На протяжении периода времени, выбранного в раскрывающемся меню «Время», обновления не производятся. Программа возвращается к самой старой версии базы данных сигнатур вирусов, которая хранится в качестве снимка в файловой системе локального компьютера.

Пример. Предположим, последней версии базы данных сигнатур вирусов присвоен номер 6871. Версии 6870 и 6868 хранятся в качестве снимков. Также учтем, что версия 6869 не загружена, поскольку, например, компьютер долго был выключен. Если в поле **Количество снимков в локальной системе** ввести значение 2 и нажать кнопку **Откат**, программа вернется к версии 6868 базы данных сигнатур вирусов. Это может занять некоторое время. Чтобы проверить, произведен ли откат к предыдущей версии, в главном окне ESET Endpoint Security откройте раздел Обновление.

Параметры конфигурации локального сервера зеркала становятся доступны после добавления действительного лицензионного ключа в менеджере лицензий, который расположен в разделе «Дополнительные настройки» ESET Endpoint Security. Если рабочая станция используется в качестве зеркала, перед созданием копий обновлений нужно принять условия последней версии лицензионного соглашения с конечным пользователем. Это требуется, поскольку в ходе данного процесса изменяются файлы, которые используются для обновления других рабочих станций в сети. При наличии новой версии лицензионного соглашения ее условия можно принять в диалоговом окне, которое появляется на 60 секунд. Чтобы сделать это вручную, нажмите кнопку **Настройка...** в разделе **Лицензии на PCU** этого окна.



4.5.2 Создание задач обновления

Обновление можно запустить вручную, нажав **Обновить базу данных сигнатур вирусов** в основном окне, которое появляется после выбора пункта **Обновление** в главном меню.

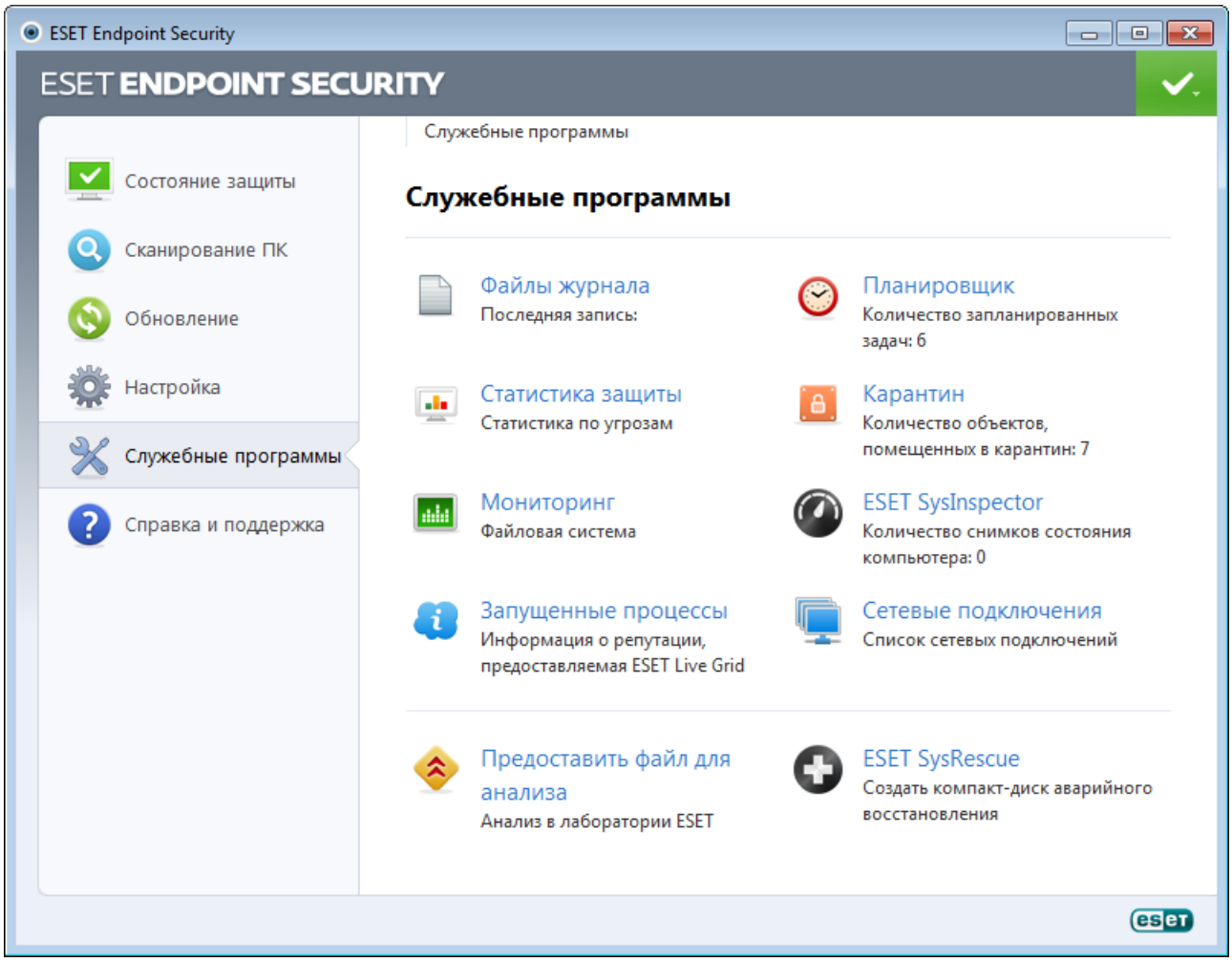
Обновления также можно выполнять как запланированную задачу. Для конфигурирования запланированной задачи перейдите в раздел **Служебные программы** > **Планировщик**. По умолчанию в ESET Endpoint Security активированы указанные ниже задачи.

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

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

4.6 Служебные программы

В меню **Служебные программы** перечислены модули, которые позволяют упростить процесс администрирования программы и содержат дополнительные возможности администрирования для опытных пользователей.



В этом меню представлены следующие служебные программы.

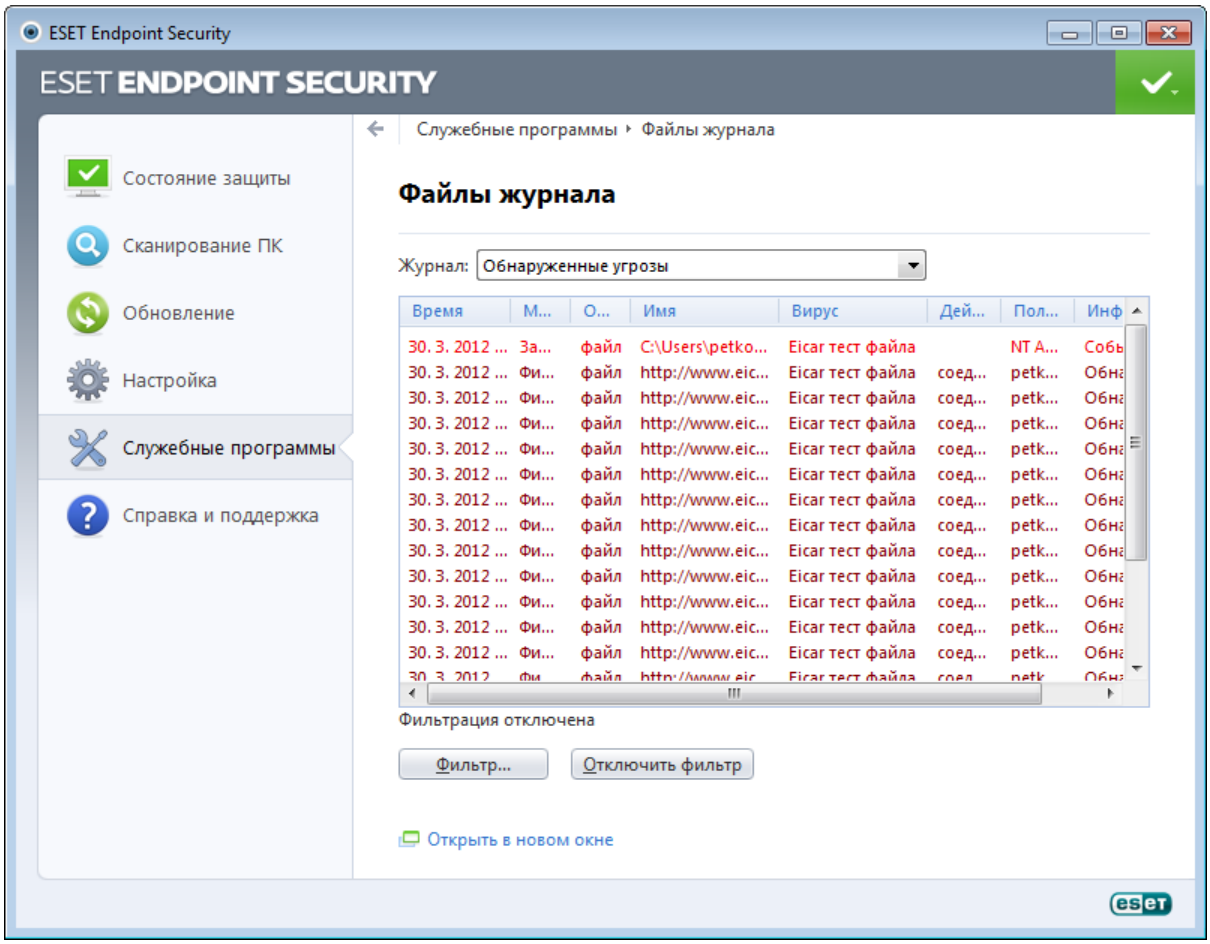
- Файлы журнала
- Статистика защиты
- Наблюдение
- Запущенные процессы
- Планировщик
- Карантин
- Сетевые подключения
- ESET SysInspector

Предоставить файл для анализа: позволяет отправить подозрительный файл на анализ в вирусную лабораторию ESET. Диалоговое окно, открывающееся при использовании этой функции, описано в разделе Отправка файлов на анализ.

ESET SysRescue: запуск мастера создания ESET SysRescue.

4.6.1 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 файлы журнала, а также архивировать их можно непосредственно в среде ESET Endpoint Security.



Получить доступ к файлам журнала можно из главного окна программы с помощью команды **Служебные программы** > **Файлы журнала**. Выберите нужный тип журнала в раскрывающемся меню **Журнал**. Доступны указанные ниже журналы.

- **Обнаруженные угрозы**: журнал угроз содержит подробную информацию о заражениях, обнаруженных модулями ESET Endpoint Security. Регистрируется информация о времени обнаружения, название угрозы, место обнаружения, выполненные действия и имя пользователя, который находился в системе при обнаружении заражения. Дважды щелкните запись журнала для просмотра подробного содержимого в отдельном окне.
- **События**: в журнале событий регистрируются все важные действия, выполняемые программой ESET Endpoint Security. Он содержит информацию о событиях и ошибках, которые произошли во время работы программы. Он должен помогать системным администраторам и пользователям решать проблемы. Зачастую информация, которая содержится в этом журнале, оказывается весьма полезной при решении проблем, возникающих в работе программы.
- **Сканирование компьютера**: в этом окне отображаются результаты всех выполненных вручную или запланированных операций сканирования. Каждая строка соответствует одной проверке компьютера. Чтобы получить подробную информацию о той или иной операции сканирования, дважды щелкните соответствующую запись.
- **Система предотвращения вторжений на узел**: содержит записи о конкретных правилах, которые были помечены для регистрации. Протокол показывает приложение, которое вызвало операцию, результат (было правило разрешено или запрещено) и имя созданного правила.
- **Персональный файервол**: в журнале событий файервола отображаются все попытки атак извне, которые

были обнаружены персональным файерволом. В нем находится информация обо всех атаках, которые были направлены на компьютер пользователя. В столбце Событие отображаются обнаруженные атаки. В столбце источник указываются сведения о злоумышленнике. В столбце Протокол перечисляются протоколы обмена данными, которые использовались для атак. Анализ журнала файервола может помочь вовремя обнаружить попытки заражения компьютера, чтобы предотвратить несанкционированный доступ на компьютер.

- **Защита от спама**: содержит записи, связанные с сообщениями электронной почты, которые были помечены как спам.
- **Контроль доступа в Интернет**: содержит список заблокированных или разрешенных URL-адресов и категорий соответствующих веб-страниц. В столбце Предпринятое действие указывается, какие правила фильтрации были применены.
- **Контроль устройств**: содержит список подключенных к компьютеру съемных носителей и устройств. В журнале регистрируются только те устройства, которые соответствуют правилу контроля. В противном случае в журнале не создаются записи о них. Также здесь отображаются такие сведения, как тип устройства, серийный номер, название поставщика и размер носителя (при его наличии).

Чтобы скопировать в буфер обмена информацию из любого раздела журнала, выделите нужную запись и нажмите кнопку **Копировать** или клавиши CTRL + C. Для выделения нескольких записей можно использовать клавиши CTRL и SHIFT.

Щелчок по записи правой кнопкой мыши выводит на экран контекстное меню. В контекстном меню доступны перечисленные ниже параметры.

- **Фильтровать записи того же типа**: после активации этого фильтра будут показаны только записи одного типа (диагностические, предупреждения и т. д.).
- **Фильтровать.../Найти...**: использование одной из этих команд выводит на экран окно **Фильтрация журнала**, в котором можно задать критерии фильтрации.
- **Отключить фильтр**: удаляются все параметры фильтра (созданные, как описано выше).
- **Копировать все**: копируется информация обо всех записях, присутствующих в окне.
- **Удалить/Удалить все**: удаляются выделенные записи или все записи в окне; для этого действия нужны права администратора.
- **Экспорт**: экспорт информации о записях в файл в формате XML.
- **Прокрутить журнал**: этот флажок следует оставить установленным, чтобы использовалась автоматическая прокрутка старых журналов, а на экран в окне **Файлы журнала** выводились активные журналы.

4.6.1.1 Обслуживание журнала

Конфигурацию файлов журнала ESET Endpoint Security можно открыть из главного окна программы. Нажмите **Настройка** > **Перейти к дополнительным настройкам...** > **Служебные программы** > **Файлы журнала**. Раздел «Файлы журнала» используется для настройки управления журналами. Программа автоматически удаляет старые файлы журналов, чтобы сэкономить дисковое пространство. Для файлов журнала можно задать параметры, указанные ниже.

Автоматически удалять записи старше, чем (дн.):: записи в журнале старше указанного количества дней будут автоматически удалены.

Оптимизировать файлы журналов автоматически: если этот флажок установлен, файлы журналов будут автоматически дефрагментироваться в тех случаях, когда процент фрагментации превышает значение, указанное в параметре **Если количество неиспользуемых записей превышает (%)**.

Нажмите **Оптимизировать сейчас**, чтобы запустить дефрагментацию файлов журналов. При этом удаляются все пустые записи журналов, что улучшает производительность и скорость обработки журналов. Такое улучшение особенно заметно, если в журналах содержится большое количество записей.

Минимальная степень детализации журнала: определяет минимальный уровень детализации записей о событиях.

- **Диагностика**: регистрируется информация, необходимая для тщательной настройки программы, а также все перечисленные выше записи.
- **Информационные**: 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**: регистрируется информация об ошибках загрузки файлов и критических ошибках.
- **Критические**: регистрируются только критические ошибки (ошибки запуска защиты от вирусов, персонального файерволаи т. п.).

Выберите вариант **Включить текстовый протокол** для хранения журналов в другом формате файлов без использования файлов журнала.

- **Тип**: если выбрать **Обычный** формат, журналы будут храниться как текстовые файлы с разделителями-знаками табуляции. Если выбрать вариант **CSV**, то журналы будут храниться как файлы с разделителями-запятыми. В случае выбора параметра **Событие** журналы будут храниться в журнале событий Windows (который можно открыть с помощью средства просмотра событий на панели управления), а не в файле.
- **Целевой каталог**: место, в котором будут сохранены файлы (только для форматов «Обычный»/CSV). Каждый раздел журнала имеет собственный файл с предопределенным именем (например, virlog.txt для раздела **Обнаруженные угрозы** в файлах журнала в случае, если журналы сохраняются в формате обычного текстового файла).

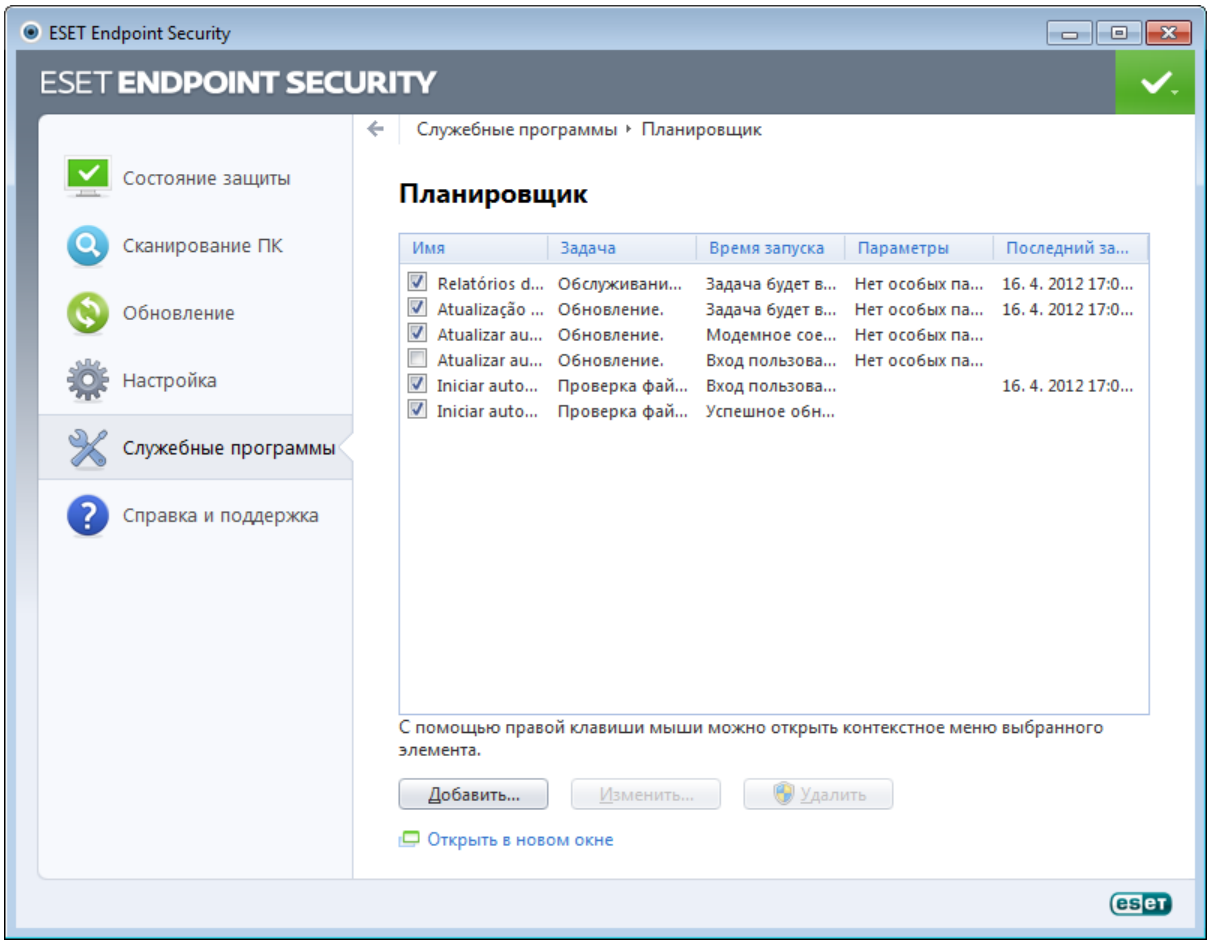
Кнопка **Удалить журнал** используется для очистки всех сохраненных журналов, которые в данный момент выбраны в раскрывающемся меню **Тип**.

4.6.2 Планировщик

Планировщик управляет запланированными задачами и запускает их с предварительно заданными параметрами и свойствами.

Перейти к планировщику можно из главного окна программы ESET Endpoint Security, открыв раздел меню **Служебные программы** > **Планировщик**. **Планировщик** содержит полный список всех запланированных задач и свойства конфигурации, такие как предварительно заданные дата, время и используемый профиль сканирования.

Планировщик предназначен для планирования выполнения следующих задач: обновление базы данных сигнатур вирусов, сканирование, проверка файлов, исполняемых при запуске системы, и обслуживание журнала. Добавлять и удалять задачи можно непосредственно в главном окне планировщика (кнопки **Добавить...** и **Удалить** в нижней части окна). С помощью контекстного меню окна планировщика можно выполнить следующие действия: отображение подробной информации, выполнение задачи немедленно, добавление новой задачи и удаление существующей задачи. Используйте флажки в начале каждой записи, чтобы активировать или отключить соответствующие задачи.



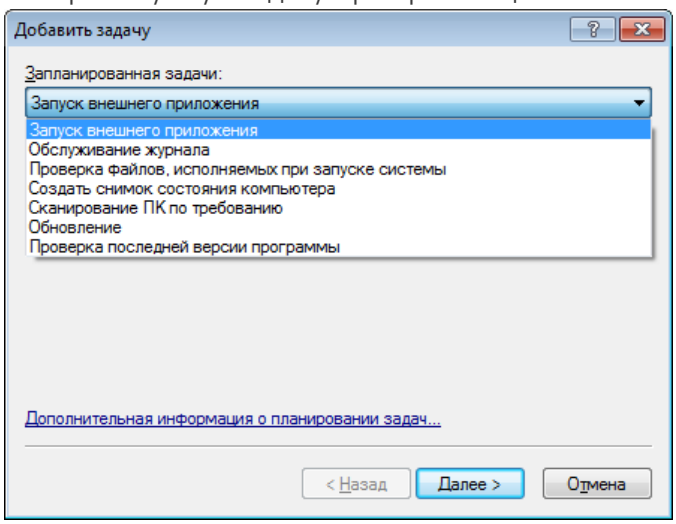
По умолчанию в **планировщике** отображаются следующие запланированные задачи.

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

Для того чтобы изменить параметры запланированных задач (как определенных по умолчанию, так и пользовательских), щелкните правой кнопкой мыши нужную задачу и выберите в контекстном меню команду **Изменить...** или выделите задачу, которую необходимо изменить, а затем нажмите кнопку **Изменить...**.

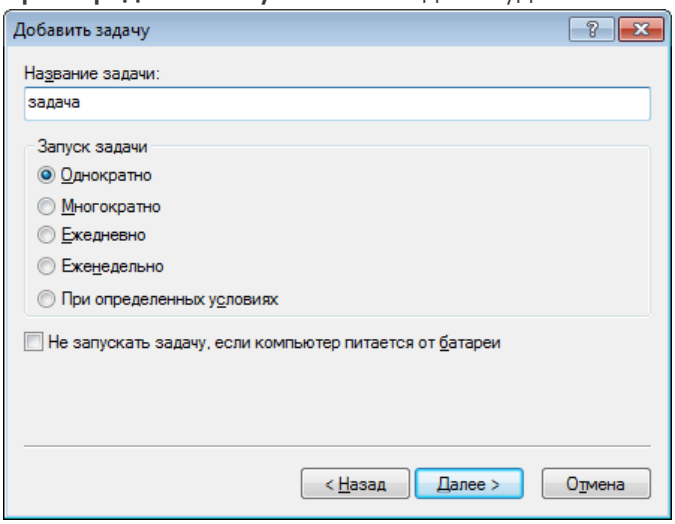
Добавление новой задачи

1. Нажмите **Добавить...** в нижней части окна.
2. Выберите нужную задачу в раскрывающемся меню.



3. Введите имя задачи и выберите один из режимов времени выполнения.

   - **Однократно**: задача будет выполнена однократно в установленную дату и время.
   - **Многократно**: задача будет выполняться регулярно через указанный промежуток времени (в часах).
   - **Ежедневно**: задача будет выполняться раз в сутки в указанное время.
   - **Еженедельно**: задача будет выполняться один или несколько раз в неделю в указанные дни и время.
   - **При определенных условиях**: задача будет выполнена при возникновении указанного события.



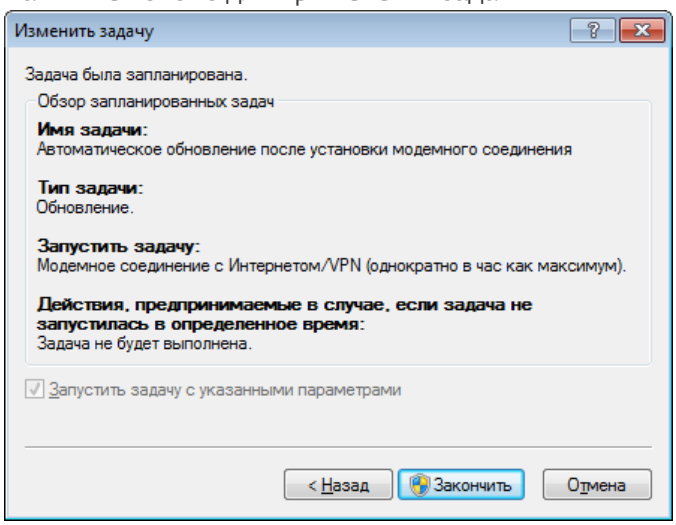
4. В зависимости от выбранного в предыдущем действии режима времени выполнения на экран будет выведено одно из следующих диалоговых окон.

   - **Однократно**: задача будет выполнена однократно в установленную дату и время.
   - **Многократно**: задача будет выполняться регулярно через указанный промежуток времени.
   - **Ежедневно**: задача будет многократно выполняться каждые сутки в указанное время.
   - **Еженедельно**: задача будет выполняться в выбранный день недели в указанное время.

5. Если задача не могла быть выполнена в отведенное ей время, можно указать, когда будет предпринята следующая попытка запуска задачи.

   - Ждать до следующего намеченного момента
   - Выполнить задачу как можно скорее
   - Выполнить задачу немедленно, если время, прошедшее с последнего запуска, превысило указанный интервал (в часах).

6. На последнем этапе предоставляется возможность просмотреть информацию о планируемой задаче. Нажмите **Готово** для применения задачи.



4.6.2.1 Создание новой задачи

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**: планирование выполнения внешнего приложения.
- **Обслуживание журнала**: в файлах журнала также содержатся остатки удаленных записей. Эта задача регулярно оптимизирует записи в файлах журнала для эффективной работы.
- **Проверка файлов, исполняемых при запуске системы**: проверка файлов, исполнение которых разрешено при запуске или входе пользователя в систему.
- **Создать снимок состояния компьютера**: создание снимка состояния компьютера в ESET SysInspector, для которого собираются подробные сведения о компонентах системы (например, драйверах, приложениях) и оценивается уровень риска для каждого их них.
- **Сканирование компьютера**: сканирование файлов и папок на компьютере.
- **Обновление**: планирование задачи обновления, в рамках которой обновляется база данных сигнатур вирусов и программные модули.

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 указанные ниже варианты. **Однократно**, **Многократно**, **Ежедневно**, **Еженедельно** и **При определенных условиях**. Установите флажок **Не запускать задачу, если компьютер питается от батареи**, чтобы свести к минимуму потребление системных ресурсов, когда ноутбук работает от аккумулятора. 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 варианты:

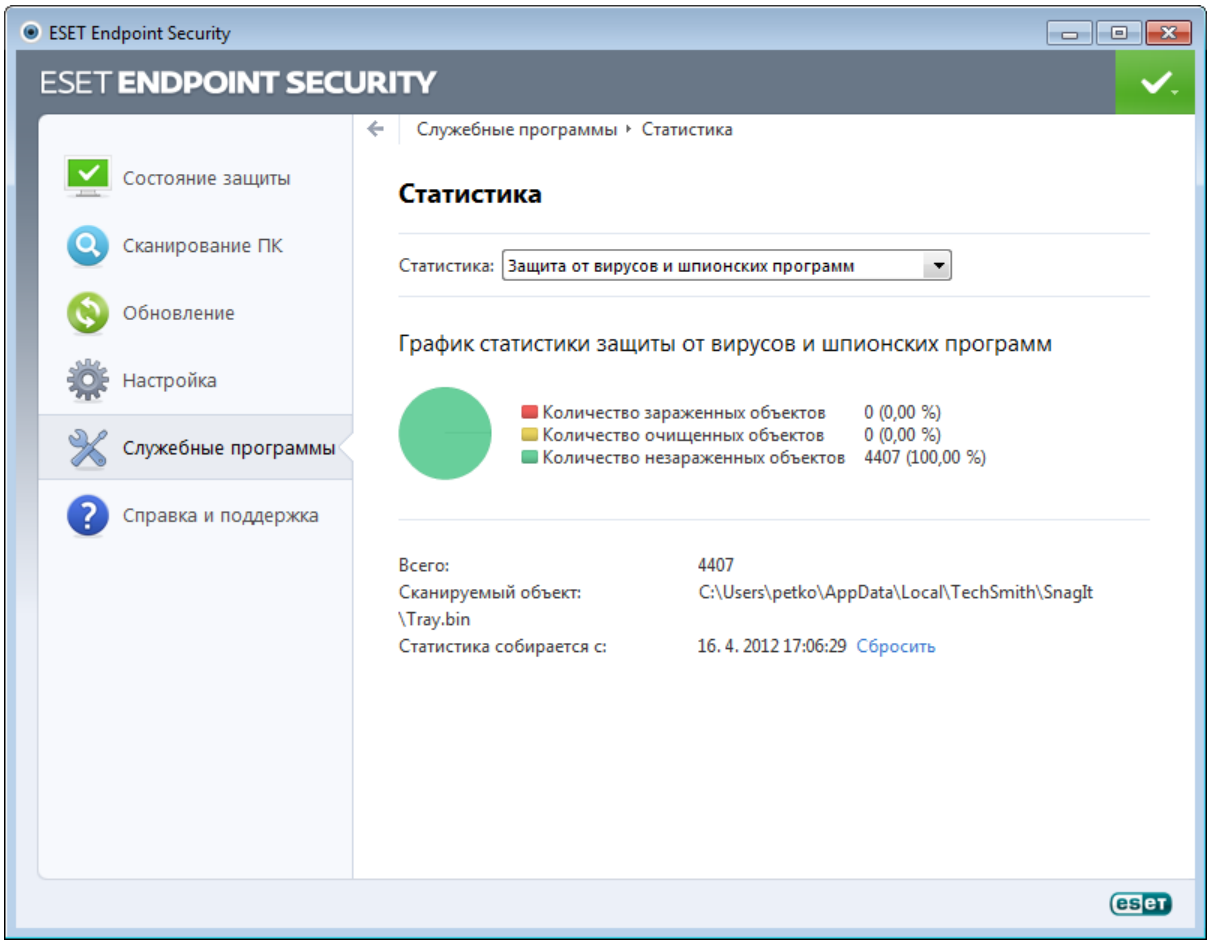
- **Ждать до следующего намеченного момента**
- **Выполнить задачу как можно скорее**
- **Выполнить задачу немедленно, если время, прошедшее с последнего запуска, превысило указанный интервал** (интервал можно указать с помощью параметра «Минимальный интервал между задачами»).

На следующем этапе отображается окно сводной информации о текущей планируемой задаче. Пункт **Запустить задачу с указанными параметрами** должен быть 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 **ОК** в окне **Профили обновления**. Новая задача появится в списке существующих запланированных.

4.6.3 Статистика защиты

Для просмотра диаграммы статистических данных, связанных с модулями защиты ESET Endpoint Security, нажмите **Служебные программы** > **Статистика защиты**. Выберите интересующий вас модуль защиты в раскрывающемся меню **Статистика**, в результате чего на экран будет выведена соответствующая диаграмма и легенда. Если навести указатель мыши на элемент в легенде, на диаграмме отобразятся данные только для этого элемента.



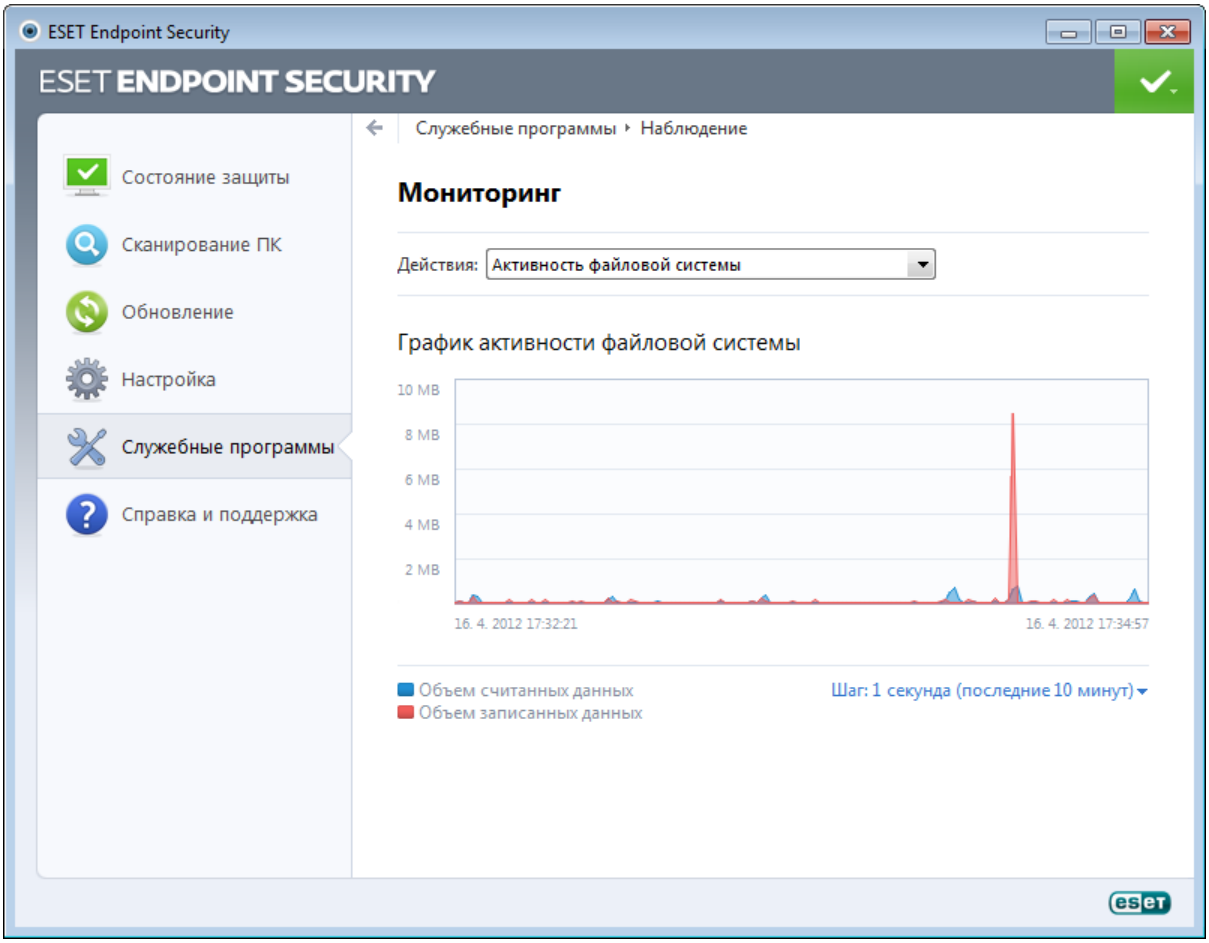
Доступны следующие статистические диаграммы.

- **Защита от вирусов и шпионских программ**: отображение количества зараженных и очищенных объектов.
- **Защита файловой системы**: отображение только объектов, считанных из файловой системы или записанных в нее.
- **Защита почтового клиента**: отображение только объектов, отправленных или полученных почтовыми клиентами.
- **Защита доступа в Интернет**: отображение только объектов, загруженных веб-браузерами.
- **Защита почтового клиента от спама**: отображение статистики защиты от спама с момента последнего запуска.

Под статистическими диаграммами показано общее количество просканированных объектов, последний просканированный объект и метка времени статистики. Нажмите **Сброс**, чтобы удалить всю статистическую информацию.

4.6.4 Наблюдение

Чтобы просмотреть текущую **активность файловой системы** в графическом виде, выберите **Служебные программы** > **Наблюдение**. В нижней части диаграммы находится временная шкала, на которой отображается активность файловой системы в режиме реального времени за выбранный временной интервал. Для изменения интервала времени нажмите **Шаг в 1...** в правом нижнем углу окна.



Доступны указанные ниже варианты.

- **Шаг: 1 секунда (последние 10 минут)**: диаграмма обновляется каждую секунду, временная шкала охватывает последние 10 минут.
- **Шаг: 1 минута (последние 24 часа)**: диаграмма обновляется каждую минуту, временная шкала охватывает последние 24 часа.
- **Шаг: 1 час (последний месяц)**: диаграмма обновляется каждый час, временная шкала охватывает последний месяц.
- **Шаг: 1 час (выбранный месяц)**: диаграмма обновляется каждый час, временная шкала охватывает последние X месяцев.

На вертикальной оси **графика активности файловой системы** отмечаются прочитанные (синий цвет) и записанные (красный цвет) данные. Оба значения измеряются в КБ (килобайтах)/МБ/ГБ. Если навести указатель мыши на прочитанные или записанные данные в легенде под диаграммой, на графике отобразятся данные только для выбранного типа активности.

В раскрывающемся меню **Активность** также можно переключиться в режим отображения **сетевой активности**. Вид диаграмм и параметры для режимов **Активность файловой системы** и **Сетевая активность** одинаковы за тем исключением, что для последней отображаются полученные (синий цвет) и отправленные (красный цвет) данные.

4.6.5 ESET SysInspector

ESET SysInspector — это приложение, которое тщательно проверяет компьютер и собирает подробные сведения о компонентах системы, такие как установленные драйверы и приложения, сетевые подключения и важные записи реестра, а также оценивает уровень риска для каждого компонента. Эта информация способна помочь определить причину подозрительного поведения системы, которое может быть связано с несовместимостью программного или аппаратного обеспечения или заражением вредоносными программами.

В окне SysInspector отображаются такие данные о созданных журналах.

- **Время**: время создания журнала.
- **Комментарий**: краткий комментарий.
- **Пользователь**: имя пользователя, создавшего журнал.
- **Состояние**: состояние создания журнала.

Доступны перечисленные далее действия.

- **Сравнить**: сравнение двух существующих журналов.
- **Создать...**: создание журнала. Дождитесь окончания создания журнала ESET SysInspector (в поле **Состояние** показано «Создан»).
- **Удалить**: удаление выделенных журналов из списка.

В контекстном меню, которое открывается, если щелкнуть правой кнопкой мыши один или несколько выделенных журналов, доступны перечисленные ниже действия.

- **Показать**: открытие выделенного журнала в ESET SysInspector (аналогично двойному щелчку).
- **Удалить все**: удаление всех журналов.
- **Экспорт...**: экспорт журнала в файл или архив в формате XML.

4.6.6 ESET Live Grid

ESET Live Grid (следующее поколение ESET ThreatSense.Net) — это расширенная система своевременного обнаружения, защищающая от вновь появляющихся угроз на основе репутации. За счет потоковой передачи в режиме реального времени информации из облака вирусная лаборатория ESET поддерживает актуальность средств защиты для обеспечения постоянной безопасности. Пользователь может проверять репутацию запущенных процессов и файлов непосредственно в интерфейсе программы или в контекстном меню, благодаря чему становится доступна дополнительная информация из ESET Live Grid. Существует два варианта работы.

1. Можно принять решение на включать ESET Live Grid. Функциональность программного обеспечения при этом не ограничивается, и пользователь все равно получает наилучшую защиту.
2. Можно сконфигурировать ESET Live Grid так, чтобы отправлялась анонимная информация 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.

ESET Live Grid 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.

По умолчанию программа ESET Endpoint Security отправляет подозрительные файлы в вирусную 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.

Меню настройки ESET Live Grid позволяет воспользоваться рядом параметров для включения и отключения системы ESET Live Grid, которая служит для отправки подозрительных файлов и анонимной статистической информации в лабораторию ESET. Эти параметры доступны через дерево расширенных параметров в разделе **Служебные программы** > **ESET Live Grid**.

Принять участие в ESET Live Grid : включает или отключает систему ESET Live Grid, которая служит для отправки подозрительных файлов и анонимной статистической информации в лабораторию ESET.

Не отправлять статистику: установите этот флажок, если системе ESET Live Grid не следует отправлять анонимную информацию о компьютере. Эта информация связана со вновь обнаруженными угрозами и может содержать имя заражения, информацию о дате и времени обнаружения, версии ESET Endpoint Security,

информацию о версии операционной системы компьютера и параметрах местоположения. Обычно статистика передается на сервер ESET один или два раза в день.

Не отправлять файлы: подозрительные файлы, содержимое или поведение которых напоминает заражение, не отправляются в ESET на анализ средствами технологии ESET Live Grid.

Дополнительные настройки...: открывается окно с дальнейшими параметрами ESET Live Grid.

Если система ESET Live Grid использовалась ранее, но была отключена, могут существовать пакеты данных, предназначенные для отправки. Эти пакеты будут отправлены в ESET при первой возможности даже после выключения системы. После этого новые пакеты создаваться не будут.

4.6.6.1 Подозрительные файлы

На вкладке **Файлы** расширенных параметров ESET Live Grid можно сконфигурировать, как угрозы будут отправляться в вирусную 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.

Фильтр исключения: этот вариант позволяет исключить из отправки определенные файлы или папки. Перечисленные в этом списке файлы никогда не будут передаваться в ESET на анализ, даже если они содержат подозрительный код. 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.

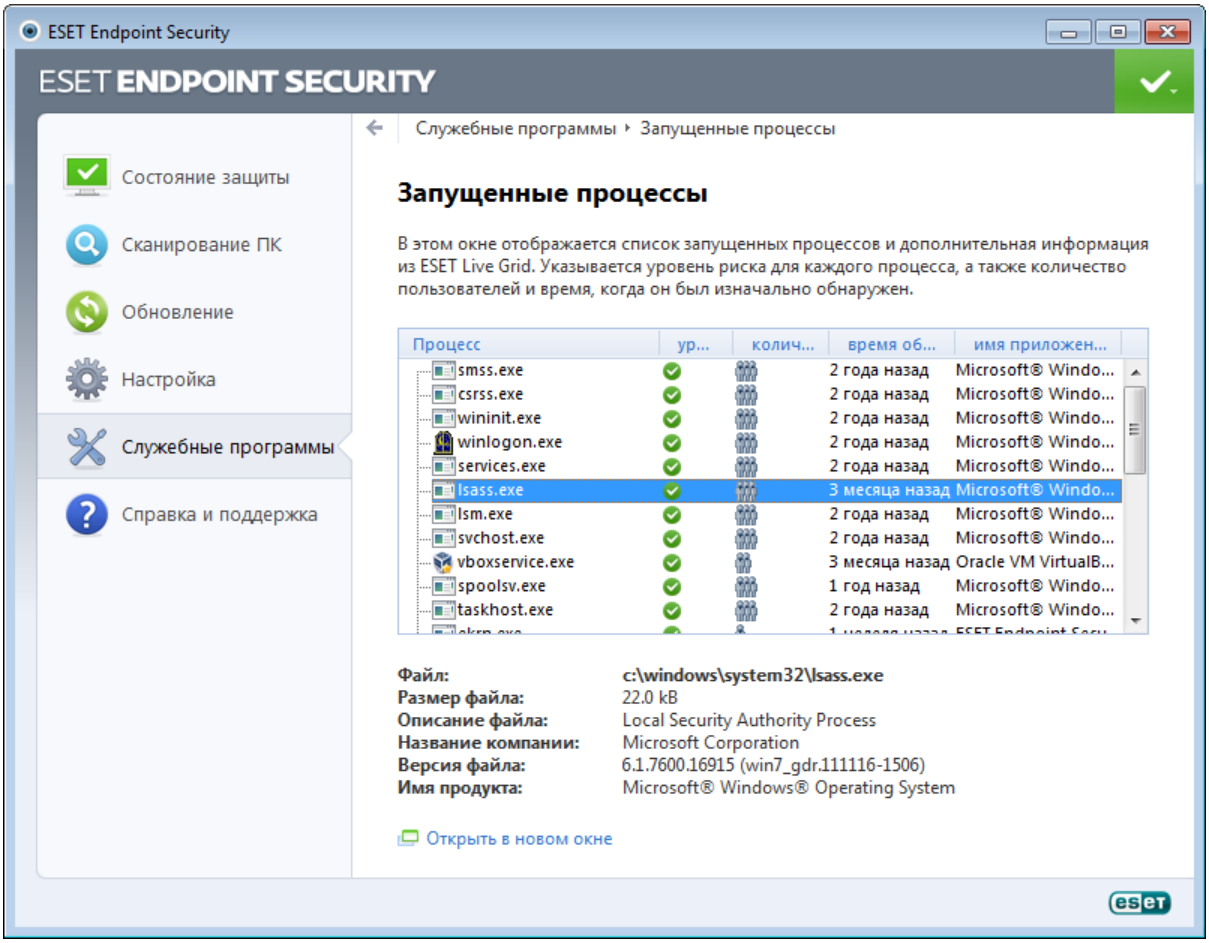
Ваш адрес электронной почты (необязательно): можно отправить адрес электронной почты вместе с подозрительными файлами, чтобы специалисты ESET могли обратиться к вам, если для анализа потребуется дополнительная информация. Имейте в виду, что компания ESET не отправляет ответы пользователям без необходимости.

В этом разделе также можно выбрать, будут ли файлы и статистическая информация отправляться с помощью ESET Remote Administrator или непосредственно в ESET. Чтобы подозрительные файлы и статистическая информация гарантированно доставлялись в ESET, выберите пункт **Средствами удаленного администрирования или непосредственно в ESET**. В таком случае они будут отправляться всеми доступными способами. При отправке подозрительных файлов и статистики средствами удаленного администрирования данные доставляются на соответствующий сервер, с которого они затем передаются в вирусные лаборатории ESET. Если выбрать вариант **Непосредственно в ESET**, все подозрительные файлы и статистическая информация будут отправляться в вирусную лабораторию ESET прямо из программы.

Установите флажок **Вести журнал**, чтобы создать журнал событий для регистрации фактов отправки файлов и статистической информации. В журнал событий будут вноситься записи при каждой отправке файлов или статистики.

4.6.7 Запущенные процессы

В разделе «Запущенные процессы» отображаются выполняемые на компьютере программы или процессы. Кроме того, он позволяет оперативно и непрерывно уведомлять компанию ESET о новых заражениях. ESET Endpoint Security предоставляет подробные сведения о запущенных процессах для защиты пользователей с помощью технологии ESET Live Grid.



Процесс: имя образа программы или процесса, запущенных в настоящий момент на компьютере. Для просмотра всех запущенных на компьютере процессов также можно использовать диспетчер задач Windows. Диспетчер задач также можно открыть, щелкнув правой кнопкой мыши в пустой области на панели задач, после чего выбрав пункт «Диспетчер задач», или же воспользовавшись сочетанием клавиш CTRL + SHIFT + ESC.

Уровень риска: в большинстве случаев ESET Endpoint Security и технология ESET Live Grid присваивают объектам (файлам, процессам, разделам реестра и т. п.) уровни риска на основе наборов эвристических правил, которые изучают характеристики каждого объекта и затем оценивают вероятность их вредоносной деятельности. На основе такого эвристического анализа объектам присваивается уровень риска от 1 — безопасно (зеленый) до 9 — опасно (красный).

ПРИМЕЧАНИЕ. Известные приложения, помеченные как 1 — безопасно (зеленый), точно являются безопасными (внесены в «белый» список) и исключаются при сканировании, благодаря чему ускоряется сканирование компьютера по запросу или защита файловой системы в режиме реального времени.

Количество пользователей: количество пользователей данного приложения. Эта информация собирается технологией ESET Live Grid.

Время обнаружения: время, прошедшее с момента обнаружения приложения технологией ESET Live Grid.

ПРИМЕЧАНИЕ.Если для приложения выбран уровень безопасности неизвестно (оранжевый), оно не обязательно является вредоносной программой. Обычно это просто новое приложение. Если вы не уверены в безопасности какого-либо файла, его можно отправить на анализ в вирусную лабораторию ESET. Если файл окажется вредоносным приложением, необходимая для его обнаружения информация будет включена в последующие обновления.

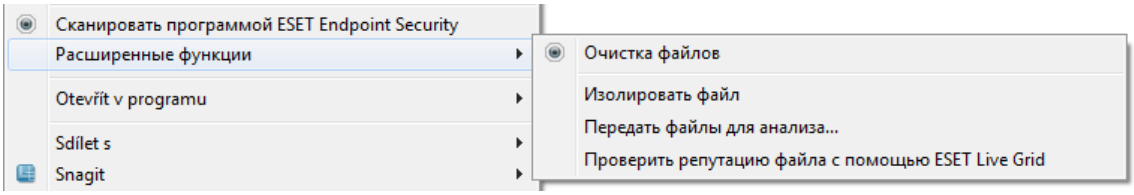
Имя приложения: конкретное имя программы или процесса.

Открыть новое окно: сведения о запущенных процессах будут открыты в новом окне.

Если выбрать определенное приложение внизу, будет выведена указанная ниже информация.

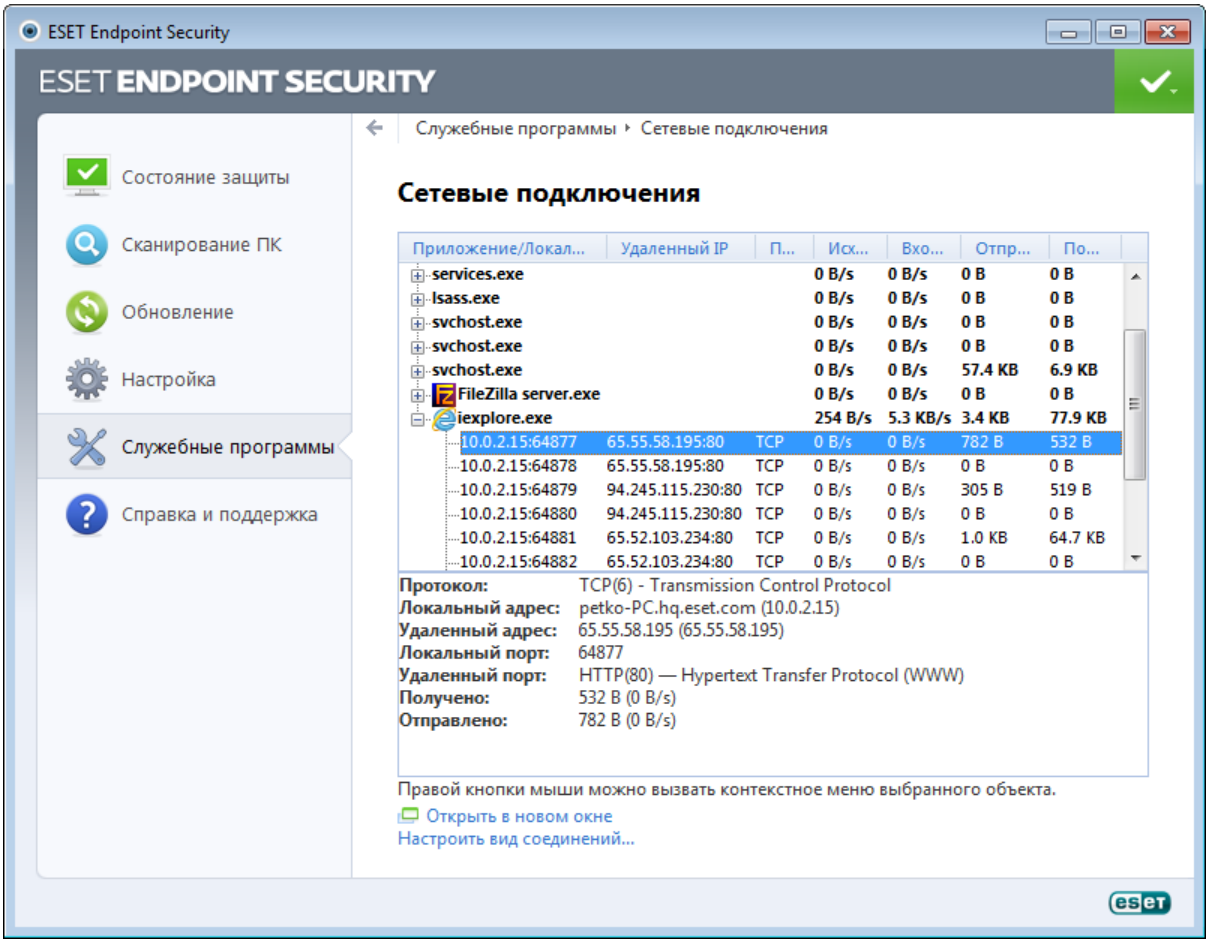
- **Файл**: расположение приложения на компьютере.
- **Размер файла**: Размер файла в КБ (килобайтах) или МБ (мегабайтах).
- **Описание файла**: характеристики файла на основе его описания в операционной системе.
- **Название компании**: название поставщика или процесса приложения.
- **Версия файла**: информация, предоставленная издателем приложения.
- **Имя продукта**: имя приложения и/или наименование компании.

ПРИМЕЧАНИЕ. Также вы можете проверить репутацию файлов, которые не являются запущенными программами или процессами. Для этого пометьте нужные файлы, щелкните их правой кнопкой мыши и в контекстном меню выберите параметры **Расширенные функции** > **Проверить репутацию файла с помощью ESET Live Grid**.



4.6.8 Сетевые подключения

В разделе «Сетевые подключения» отображается список активных и отложенных соединений. Это позволяет управлять всеми приложениями, пытающимися установить исходящие соединения.



Первая строка содержит имя приложения и скорость установленного соединения. Для просмотра всего списка соединений отдельного приложения, а также более подробной информации нажмите **+**.

Приложение/Локальный IP: наименование приложения, локальные IP-адреса и порты, по которым происходит обмен данными.

Удаленный IP: IP-адрес и номер порта соответствующего удаленного компьютера.

Протокол: используемый протокол передачи данных.

Исходящая скорость/Входящая скорость: текущая скорость обмена данными в соответствующих направлениях.

Отправлено/Получено: объем переданных данных с начала соединения.

Открыть новое окно: позволяет отобразить информацию в новом окне.

При нажатии на кнопку **Настроить вид соединений...** на экране Сетевые подключения открываются описанные ниже расширенные параметры для этого раздела, позволяющие изменить отображение подключений.

Разрешать имена компьютеров: все сетевые адреса, если это возможно, отображаются в формате DNS, а не в числовом формате IP-адресов.

Показывать только соединения по TCP: в списке отображаются только подключения по протоколу TCP.

Показывать соединения по открытым портам, на которых компьютер ожидает соединения: установите этот флажок для отображения только подключений, по которым в настоящий момент не происходит обмена данными, но для которых система уже открыла порты и ожидает подключения.

Показывать внутренние соединения: установите этот флажок, чтобы отобразить только те соединения, в которых удаленной стороной является локальный компьютер (так называемые локальные соединения).

Щелкните подключение правой кнопкой мыши, чтобы просмотреть дополнительные параметры, среди которых есть следующие.

Запретить обмен данными для соединения: разрывает установленное соединение. Этот параметр доступен, только если щелкнуть активное подключение.

Показать подробности: выберите эту функцию для отображения подробной информации о выделенном подключении.

Обновить скорость: выберите периодичность обновления активных подключений.

Обновить сейчас: перезагрузка окна «Сетевые подключения».

Представленные ниже возможности доступны, только если щелкнуть приложение или процесс, а не активное подключение.

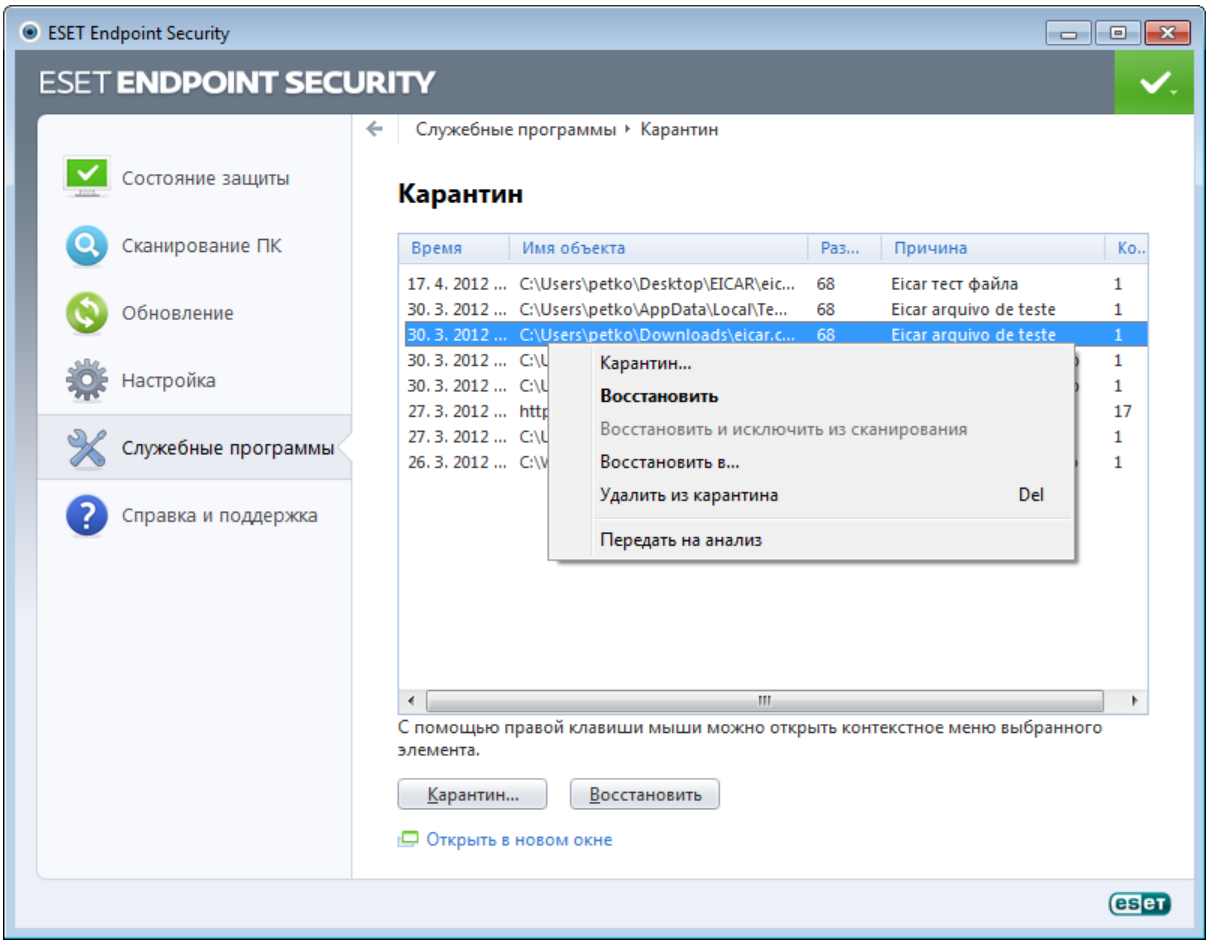
Временно запретить сетевое соединение для процесса: запретить текущие соединения данного приложения. При создании нового соединения файервол использует предопределенное правило. Описание параметров см. в разделе Правила и зоны.

Временно разрешить сетевое соединение для процесса: разрешить текущие соединения данного приложения. При создании нового соединения файервол использует предопределенное правило. Описание параметров см. в разделе Правила и зоны.

4.6.9 Карантин

Карантин предназначен в первую очередь для изоляции и безопасного хранения зараженных файлов. Файлы следует помещать на карантин, если их нельзя вылечить или безопасно удалить либо если они отнесены программой ESET Endpoint Security к зараженным по ошибке.

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 в вирусную лабораторию ESET на анализ.



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, объект добавлен пользователем) и количество угроз (например, если архив содержит несколько заражений).

Помещение файлов на карантин

Программа ESET Endpoint 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, щелкнув правой кнопкой мыши окно **Карантин** и выбрав пункт **Карантин...**.

Восстановление из карантина

Файлы, находящиеся на карантине, можно восстановить в исходном месте. Для этого предназначена функция **Восстановить**, доступная в контекстном меню окна карантина. Если файл помечен как потенциально нежелательная программа, становится активным параметр **Восстановить и исключить из сканирования**. Дополнительную информацию об этом типе приложения см. в глоссарии. 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 сканирования после восстановления и отправьте его в службу поддержки клиентов ESET.

Отправка файла из карантина

Если на карантин помещен файл, угроза в котором не распознана программой, или файл неверно квалифицирован как зараженный (например, в результате ошибки эвристического метода) и изолирован, передайте файл в вирусную лабораторию ESET. Чтобы отправить файл из карантина, щелкните его правой кнопкой мыши и выберите пункт **Передать на анализ**.

4.6.10 Отправка файлов на анализ

Диалоговое окно отправки файлов позволяет отправить файл в ESET на анализ. Для доступа к этому окну выберите **Служебные программы** > **Предоставить файл для анализа**. При обнаружении на компьютере файла, проявляющего подозрительную активность, его можно отправить в вирусную лабораторию ESET. Если файл окажется вредоносным приложением, необходимая для его обнаружения информация будет включена в последующие обновления.

Другим способом отправки является электронная почта. Если этот способ для вас удобнее, заархивируйте файлы с помощью программы WinRAR или WinZIP, защитите архив паролем «infected» и отправьте его по адресу samples@eset.com. Помните, что тема письма должна описывать проблему, а текст должен содержать как можно более полную информацию о файле (например, адрес веб-сайта, с которого он был загружен).

ПРИМЕЧАНИЕ. Прежде чем отправлять файл в ESET, убедитесь в том, что проблема соответствует одному из следующих критериев:
- файл совсем не обнаруживается;
- файл неправильно обнаруживается как угроза.

Ответ на подобный запрос будет отправлен только в том случае, если потребуется дополнительная информация.

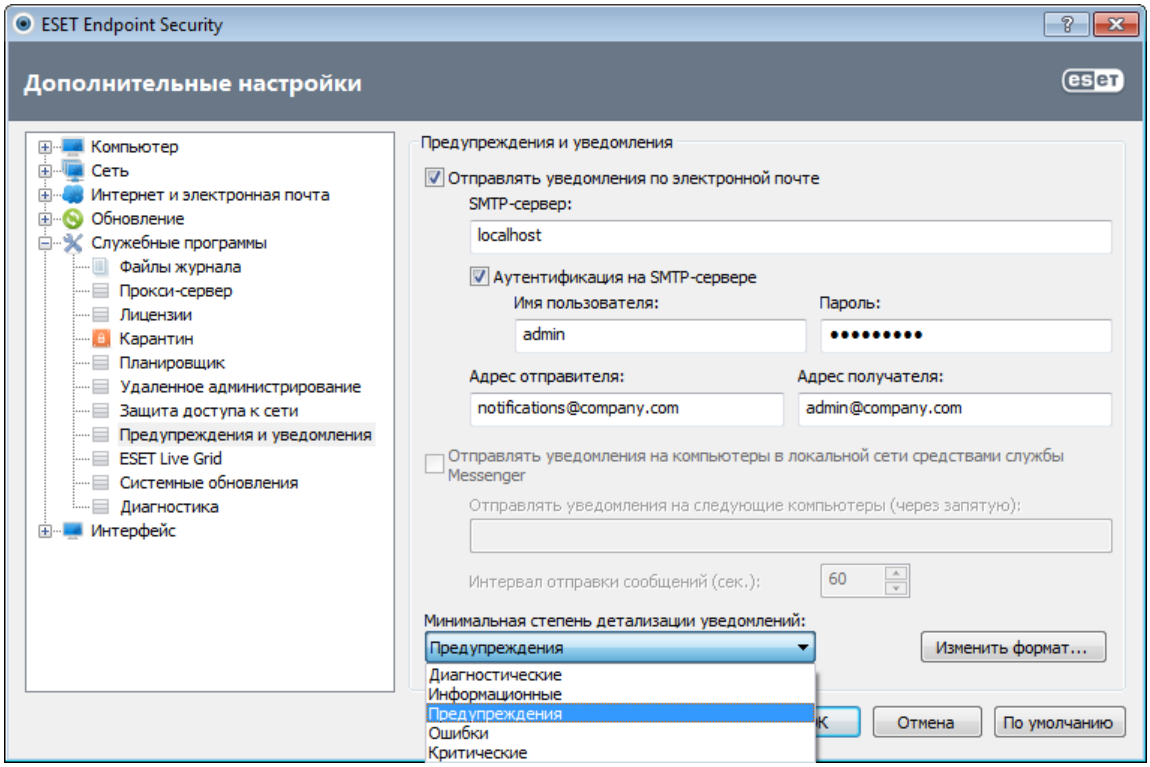
В раскрывающемся меню **Причина отправки файла** выберите наиболее подходящее описание своего сообщения.
- **Подозрительный файл**;
- **Ложное срабатывание** (файл признан зараженным, хотя не является таковым);
- и **Другое**.

Файл — путь к файлу, который вы намерены отправить.

Адрес электронной почты: адрес отправляется в ESET вместе с подозрительными файлами и может использоваться для запроса дополнительной информации, необходимой для анализа. Указывать адрес электронной почты необязательно. Поскольку каждый день на серверы ESET поступают десятки тысяч файлов, невозможно отправить ответ на каждый запрос. Вам ответят только в том случае, если для анализа потребуется дополнительная информация.

4.6.11 Предупреждения и уведомления

ESET Endpoint Security поддерживает отправку сообщений электронной почты при возникновении событий с заданной степенью детализации. Чтобы включить эту функцию и активировать отправку сообщений, установите флажок **Отправлять уведомления по электронной почте**.



SMTP-сервер: SMTP-сервер, используемый для отправки уведомлений.

Примечание. ESET Endpoint Security не поддерживает SMTP-серверы, использующие шифрование SSL/TLS.

Аутентификация на SMTP-сервере: если требуется аутентификация на SMTP-сервере, укажите действительные имя пользователя и пароль для доступа к нему.

Адрес отправителя: в этом поле указывается адрес отправителя, который будет отображаться в заголовке писем с уведомлением.

Адрес получателя: в этом поле указывается адрес получателя, который будет отображаться в заголовке писем с уведомлением.

Отправлять уведомления на компьютеры в локальной сети средствами службы Messenger: если установить этот флажок, уведомления будут отправляться на компьютеры в локальной сети с помощью службы сообщений Windows®.

Отправлять уведомления на следующие компьютеры (через запятую): введите имена компьютеров, на которые будут отправляться уведомления с помощью службы сообщений Windows®.

Интервал отправки сообщений (сек.): для изменения интервала между уведомлениями, отправляемыми по локальной сети, введите необходимое значение в секундах.

Минимальная степень детализации уведомлений: определяет минимальный уровень детализации уведомлений, которые следует отправлять.

Изменить формат...: обмен данными между программой и удаленным пользователем или системным администратором осуществляется посредством электронной почты или уведомлений в локальной сети (служба сообщений Windows®). Формат предупреждений и уведомлений, установленный по умолчанию, будет оптимален в большинстве случаев. В некоторых случаях может понадобиться изменить формат сообщений. Для этого нажмите Изменить формат....

4.6.11.1 Формат сообщений

В этом окне можно настроить формат сообщений о событиях, отображающихся на удаленных компьютерах.

Предупреждения об угрозе и уведомления по умолчанию имеют предопределенный формат. Изменять этот формат не рекомендуется. Однако в некоторых случаях (например, при наличии системы автоматизированной обработки электронной почты) может понадобиться изменить формат сообщений.

Ключевые слова (строки, разделенные символом %) в сообщении замещаются реальной информацией о событии. Доступны следующие ключевые слова.

- **%TimeStamp%**: дата и время события.
- **%Scanner%**: задействованный модуль.
- **%ComputerName%**: имя компьютера, на котором произошло событие.
- **%ProgramName%**: программа, создавшая предупреждение.
- **%InfectedObject%**: имя зараженного файла, сообщения и т. п.
- **%VirusName%**: идентифицирующие данные заражения.
- **%ErrorDescription%**: описание события, не имеющего отношения к вирусам.

Ключевые слова **%InfectedObject%** и **%VirusName%** используются только в предупреждениях об угрозах, а **%ErrorDescription%** — только в сообщениях о событиях.

Использовать символы местного алфавита: преобразование сообщений с использованием кодировки ANSI на основе региональных параметров Windows (например, windows-1250). Если не устанавливать этот флажок, сообщение будет преобразовано с использованием 7-битной кодировки ACSII (например, «á» будет преобразовано в «a», а неизвестные символы — в «?»).

Использовать местную кодировку символов: сообщение будет преобразовано в формат Quoted Printable (QP), в котором используются знаки ASCII, что позволяет правильно передавать символы национальных алфавитов по электронной почте в 8-битном формате (áéíóú).

4.6.12 Обновления системы

Функция обновления Windows является важной составляющей защиты пользователей от вредоносных программ. По этой причине обновления Microsoft Windows следует устанавливать сразу после появления. Программное обеспечение ESET Endpoint Security уведомляет пользователя об отсутствующих обновлениях в соответствии с выбранным уровнем. Доступны следующие уровни.

- **Без обновлений**: не будет предлагаться загрузить обновления системы.
- **Необязательные обновления**: будет предлагаться загрузить обновления, помеченные как имеющие низкий и более высокий приоритет.
- **Рекомендованные обновления**: будет предлагаться загрузить обновления, помеченные как имеющие обычный и более высокий приоритет.
- **Важные обновления**: будет предлагаться загрузить обновления, помеченные как важные и имеющие более высокий приоритет.
- **Критические обновления**: пользователю будет предлагаться загрузить только критические обновления.

Для сохранения изменений нажмите кнопку **OK**. После проверки статуса сервера обновлений на экран будет выведено окно «Обновления системы», поэтому данные об обновлении системы могут быть недоступны непосредственно после сохранения изменений.

4.6.13 Диагностика

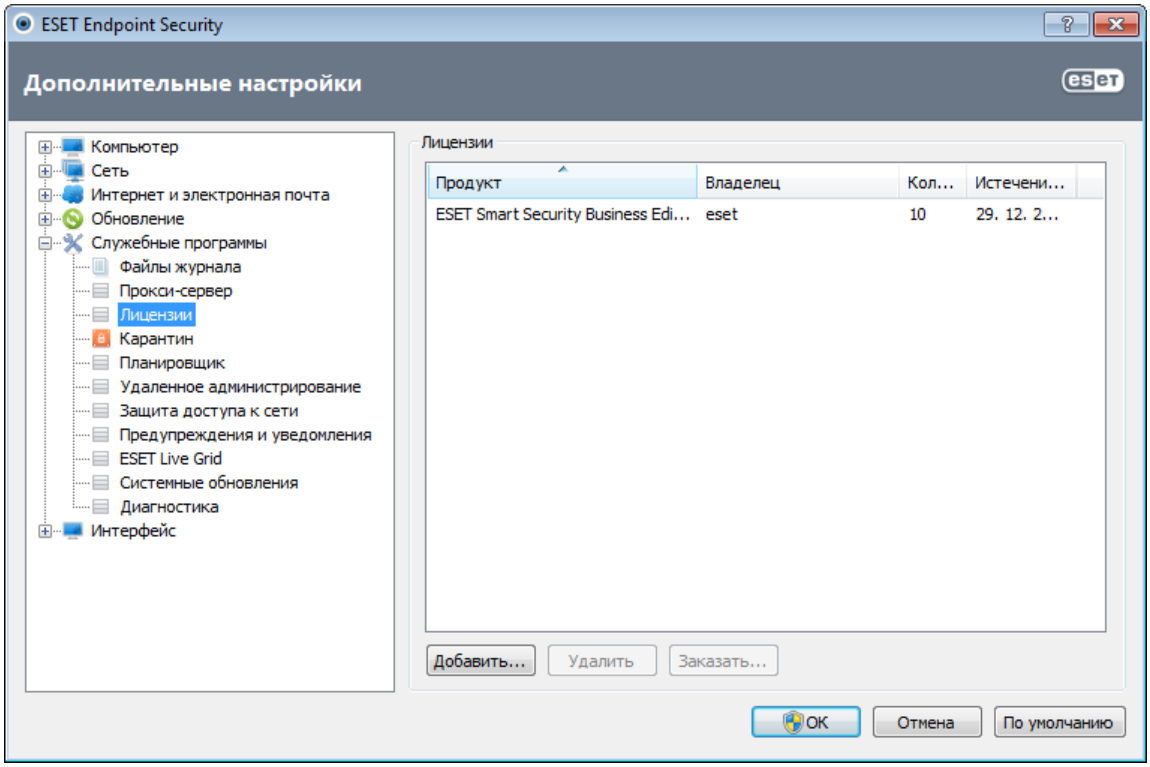
Функция диагностики формирует аварийные дампы приложения процессов ESET (например, ekrn). Если происходит сбой приложения, формируется дамп памяти. Это может помочь разработчикам выполнять отладку и устранять различные проблемы ESET Endpoint Security. Существует два типа дампов.

- **Полный дамп памяти**: регистрируется все содержимое системной памяти, когда неожиданно прекращается работа приложения. Полный дамп памяти может содержать данные процессов, которые выполнялись в момент создания дампа.
- **Минидамп**: регистрируется самый малый объем полезной информации, которая может помочь выявить причину неожиданного сбоя приложения. Этот тип файла дампа может быть удобно использовать, если место на диске ограничено. Однако ограниченный объем включенной в него информации может не позволить при анализе такого файла обнаружить ошибки, которые не были вызваны непосредственно потоком, выполнявшимся в момент возникновения проблемы.
- Установите флажок **Не создавать дамп памяти** (по умолчанию), чтобы отключить эту функцию.

Целевой каталог: каталог, в котором будет создаваться дамп при сбое. Нажмите **Открыть папку...**, чтобы открыть этот каталог в новом окне проводника.

4.6.14 Лицензии

В ветви **Лицензии** можно управлять лицензионными ключами для ESET Endpoint Security и других программных продуктов ESET, таких как ESET Remote Administrator и прочие. После покупки лицензионные ключи доставляются вместе с именем пользователя и паролем. Чтобы **добавить/удалить** лицензионный ключ нажмите соответствующую кнопку в окне менеджера лицензий (**Лицензии**). Менеджер лицензий можно открыть через дерево расширенных параметров в разделе **Служебные программы** > **Лицензии**.



Лицензионный ключ представляет собой текстовый файл, содержащий информацию о приобретенном продукте: владелец лицензии, количество лицензий и дата окончания срока действия.

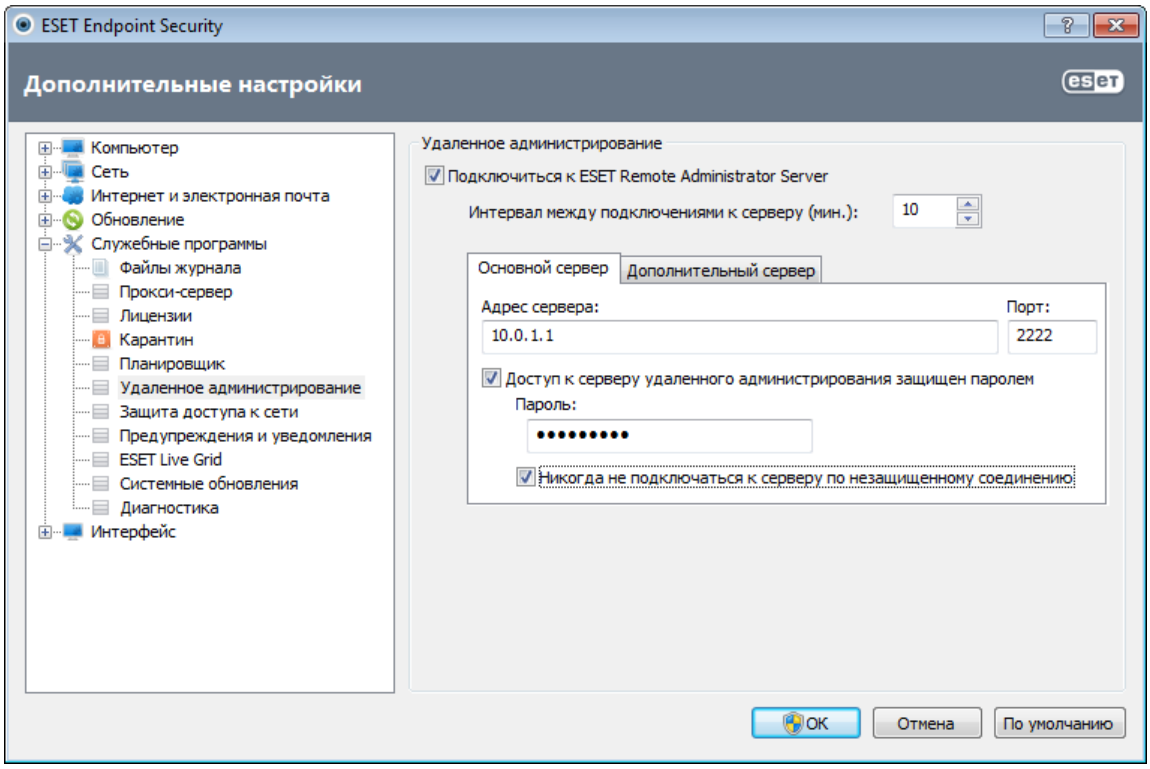
В окне менеджера лицензий можно загрузить и просмотреть содержимое лицензионного ключа, нажав кнопку **Добавить...**, после чего на экран будет выведена соответствующая информация. Для того чтобы удалить файлы лицензии из списка, выделите их и нажмите **Удалить**.

Если срок действия лицензионного ключа истек и вы хотите продлить лицензию, нажмите кнопку **Заказать...**, после чего вы перейдете в наш интернет-магазин.

4.6.15 Удаленное администрирование

ESET Remote Administrator (ERA) — это полезное средство, используемое для управления политикой безопасности и получения общих сведений о безопасности сети. Оно особенно полезно в больших сетях. Средство ERA не только повышает уровень безопасности, но и облегчает администрирование ESET Endpoint Security на клиентских рабочих станциях. В таком режиме можно устанавливать и конфигурировать программы, просматривать журналы, запланировать задачи по обновлению, задачи по сканированию и т. д. Для обмена данными между ESET Remote Administrator (ERAS) и продуктами обеспечения безопасности ESET нужно правильно выполнить конфигурирование на обеих конечных точках.

Параметры удаленного администрирования доступны из главного окна программы ESET Endpoint Security. Нажмите **Настройка** > **Перейти к дополнительным настройкам...** > **Служебные программы** > **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.): это значение определяет, как часто продукт обеспечения безопасности ESET будет подключаться к ERAS для передачи данных.

«Основной сервер», «Дополнительный сервер»: обычно достаточно сконфигурировать только основной сервер. Если в сети несколько серверов ERA Server, можно также добавить дополнительное подключение к другому, дополнительному серверу ERA Server. Он будет использоваться как резервное решение. То есть в том случае, если основной сервер станет недоступен, программа ESET автоматически обратится к дополнительному серверу ERA. Впоследствии она будет пытаться восстановить подключение к основному серверу. После восстановления этого подключения решение ESET для обеспечения безопасности переключится обратно на основной сервер. Настройка двух профилей сервера удаленного администрирования — наиболее удачное решение для мобильных клиентов, которые подключаются к серверу как из локальной сети, так и через Интернет.

Адрес сервера: укажите или DNS-имя, или IP-адрес сервера, на котором работает сервер удаленного администрирования ESET.

Порт: в этом поле указывается предварительно заданный порт сервера, используемый для подключения. Рекомендуется не изменять порт по умолчанию (2222).

Интервал между подключениями к серверу (мин.): частота, с которой программа ESET Endpoint Security подключается к ERA Server. Если установлено значение 0, данные отправляются каждые 5 секунд.

Доступ к серверу удаленного администрирования защищен паролем: позволяет ввести пароль для подключения к ERA Server, если это необходимо.

Никогда не подключаться к серверу по незащищенному соединению: установите этот флажок, чтобы запретить подключение к серверам ERA Server, на которых включен доступ без аутентификации (см. **ERA Console** > **Параметры сервера** > **Безопасность** > **Включить доступ без аутентификации для клиентов**).

Нажмите кнопку **OK**, чтобы подтвердить внесение изменений, и примените параметры. ESET Endpoint Security будет использовать эти параметры для подключения к ERA Server.

4.7 Интерфейс

В разделе **Интерфейс** можно конфигурировать поведение графического интерфейса пользователя программы.

С помощью служебной программы Графика можно изменить внешний вид программы и используемые эффекты.

Путем настройки параметров в разделе Предупреждения и уведомления можно изменить поведение предупреждений об обнаруженных угрозах и системных уведомлений. Их можно настроить в соответствии со своими потребностями.

Если принять решение о том, что некоторые уведомления не должны отображаться, они будут присутствовать в области Скрытые окна уведомлений Здесь можно проверить их состояние, просмотреть дополнительные сведения или удалить их из данного окна.

Для обеспечения максимального уровня безопасности программного обеспечения можно предотвратить несанкционированное изменение, защитив параметры паролем с помощью служебной программы Параметры доступа.

Щелчок по выделенному объекту правой кнопкой мыши открывает контекстное меню. Эта возможность позволяет интегрировать элементы управления ESET Endpoint Security в контекстное меню.

Режим презентации удобен для пользователей, которые хотят работать с приложениями, не отвлекаясь на всплывающие окна, запланированные задачи и любые компоненты, которые могут загрузить процессор и оперативную память.

4.7.1 Графика

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

В разделе **Элементы интерфейса** следует снять флажок **Графический интерфейс пользователя**, если графические элементы снижают производительность компьютера или вызывают 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.

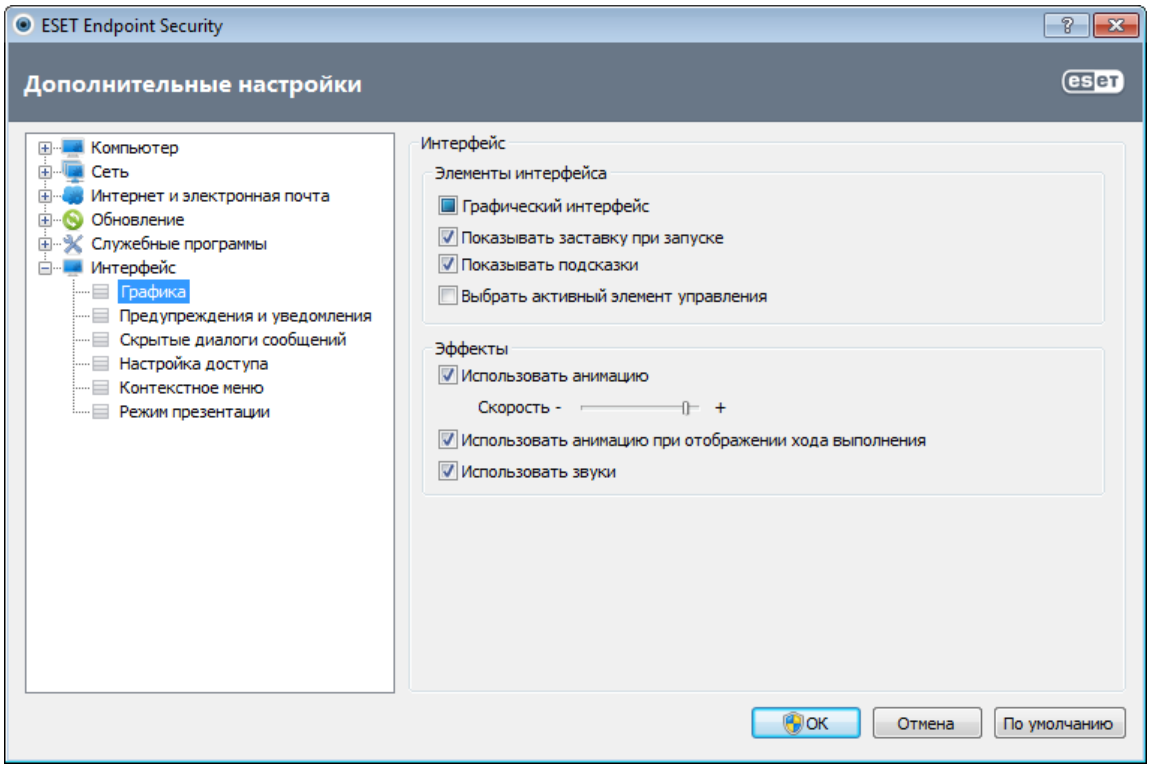
Для того чтобы отключить заставку ESET Endpoint Security, снимите флажок **Показывать заставку при запуске**.

Если установлен флажок **Показывать подсказки**, при наведении указателя мыши на элемент управления отображается 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 звук при возникновении важного события, установите флажок **Использовать звуки**. Обратите внимание, что звук будет воспроизводиться только тогда, когда сканирование компьютера выполняется или завершилось.



4.7.2 Предупреждения и уведомления

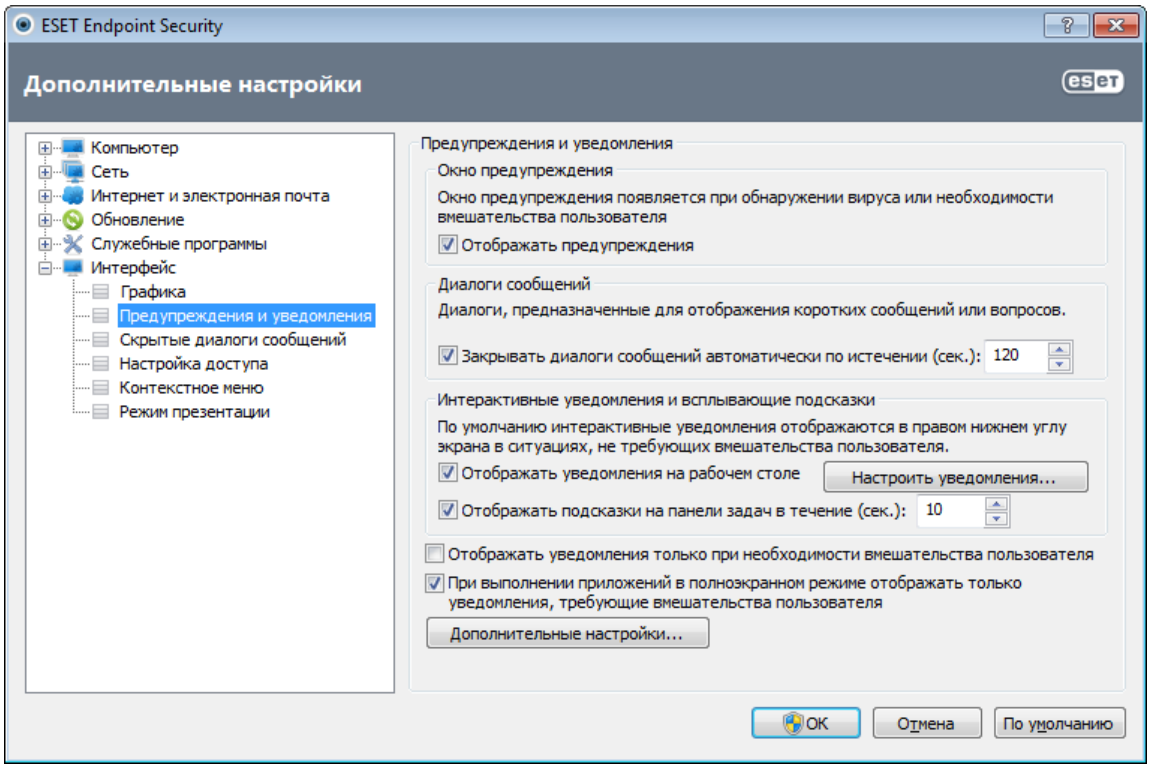
Раздел **Предупреждения и уведомления** окна **Интерфейс** дает возможность сконфигурировать, каким образом в ESET Endpoint Security обрабатываются предупреждения об угрозах и системные уведомления (например, сообщения об успешном выполнении обновлений). Здесь также можно настроить время отображения и уровень прозрачности уведомлений на панели задач (применяется только к системам, поддерживающим уведомления на панели задач).

Первый пункт — **Отображать 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 уведомления на рабочем столе, установите флажок **Отображать уведомления на рабочем столе**. Более подробные параметры, такие как время отображения и прозрачность окна уведомлений, можно изменить, нажав кнопку **Настроить уведомления...**. Для предварительного просмотра уведомлений нажмите кнопку **Просмотр**.

Для того чтобы настроить время отображения всплывающих подсказок, активируйте параметр **Отображать подсказки на панели задач в течение (сек.)** и введите нужное значение в расположенное рядом поле.



Параметр **Отображать уведомления только при необходимости вмешательства пользователя** позволяет включать и отключать отображение предупреждений и уведомлений, которые не требуют вмешательства пользователя. Установите флажок **При выполнении приложений в полноэкранном режиме отображать только уведомления, требующие вмешательства пользователя**, чтобы запретить все неинтерактивные уведомления.

Нажмите **Дополнительные настройки...**, чтобы перейти к расширенным параметрам **предупреждений и уведомлений**.

4.7.2.1 Дополнительные настройки

В раскрывающемся меню **Минимальная детализация отображаемых событий** можно выбрать начальный уровень серьезности предупреждений и уведомлений, которые следует отображать.

- **Диагностика**: регистрируется информация, необходимая для тщательной настройки программы, а также все перечисленные выше записи.
- **Информационные**: 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**: регистрируется информация об ошибках загрузки файлов и критических ошибках.
- **Критические**: регистрируются только критические ошибки (ошибки запуска защиты от вирусов, персонального файерволаи т. п.).

Последний параметр этого раздела позволяет сконфигурировать, кто именно должен получать уведомления в многопользовательской среде. В поле **В многопользовательских системах отображать уведомления для пользователя** указывается пользователь, который будет получать системные и прочие уведомления, если одновременно может быть подключено несколько пользователей. Обычно это системный или сетевой администратор. Эта функция особенно полезна для терминальных серверов при условии, что все системные уведомления отправляются администратору.

4.7.3 Скрытые окна уведомлений

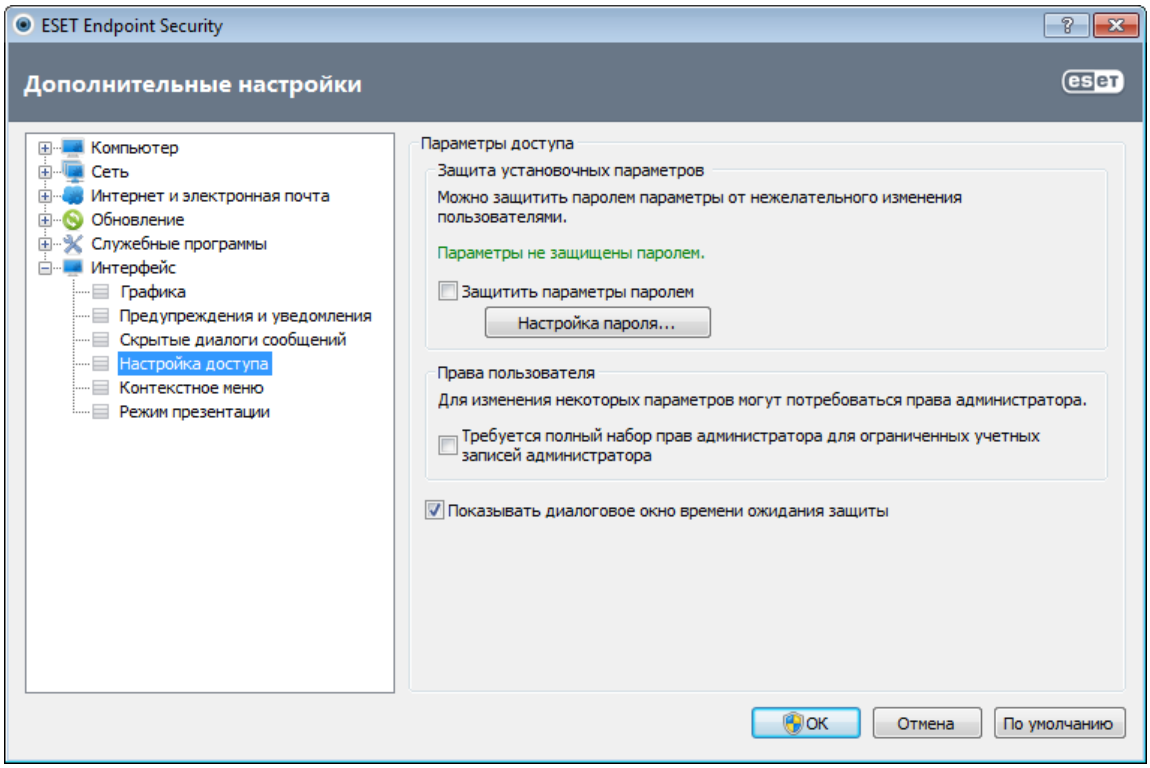
Если для одного из показанных ранее окон уведомлений (предупреждений) был выбран параметр **Не показывать это сообщение**, данное окно появится в списке скрытых окон уведомлений. Действия, которые в настоящий момент выполняются автоматически, отображаются в столбце с заголовком **Подтвердить**.

Показать: предварительный просмотр окон уведомлений, которые сейчас не отображаются и для которых сконфигурировано автоматическое действие.

Удалить: удаление элементов из списка **Скрытые диалоговые окна**. Все окна уведомлений, удаленные из списка, снова будут отображаться.

4.7.4 Настройка доступа

Для обеспечения максимальной безопасности компьютера нужно, чтобы программное обеспечение ESET Endpoint Security было правильно сконфигурировано. Неквалифицированное изменение параметров может привести к потере важных данных. Этот параметр расположен в подменю **Настройка доступа** раздела **Интерфейс** в дереве расширенных параметров. Для предотвращения несанкционированного изменения параметры ESET Endpoint Security можно защитить паролем.



Параметры защищены паролем: включает или отключает защиту параметров программы. Установите или снимите этот флажок, чтобы открыть окно настройки пароля.

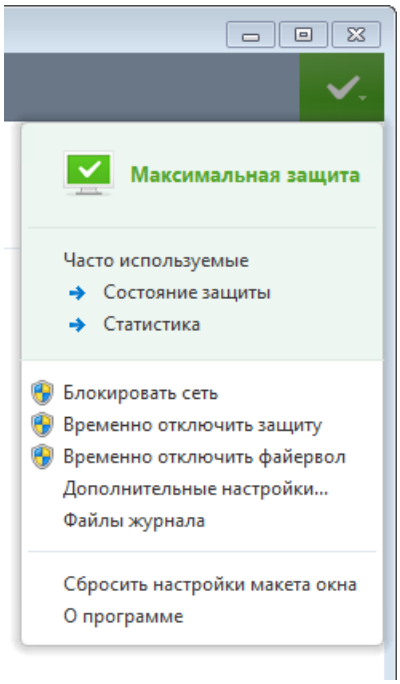
Для установки или изменения пароля для защиты параметров нажмите **Настройка пароля...**.

Требуется полный набор прав администратора для ограниченных учетных записей администратора: установите этот флажок, чтобы при изменении определенных параметров системы текущему пользователю в случае, если у такого пользователя нет прав администратора, предлагалось ввести имя и пароль администратора (аналогично контролю учетных записей в Windows Vista). К изменениям относится отключение модулей защиты или файервола.

Показывать диалоговое окно времени ожидания защиты: если этот флажок установлен, при временном отключении защиты через меню программы или раздел **ESET Endpoint Security** > **Настройка** на экран будет выведено специальное окно. Раскрывающееся меню **Период времени** в окне **Временно отключить защиту** представляет тот период времени, на который будут отключены все выбранные части защиты.

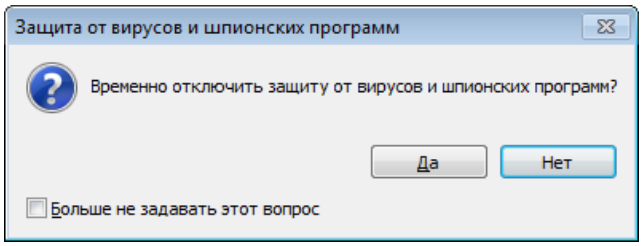
4.7.5 Меню программы

Некоторые наиболее важные функции и параметры доступны в главном меню программы.

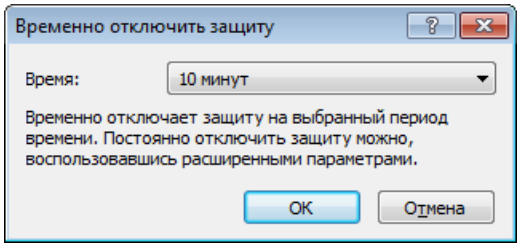


Часто используемые: на экран выводятся наиболее часто используемые части ESET Endpoint Security. К ним можно быстро перейти через меню программы.

Временно отключить защиту: на экран выводится диалоговое окно с подтверждением. В нем можно отключить защиту от вирусов и шпионских программ, которая предотвращает вредоносные атаки на компьютер, контролируя файлы, обмен данными через Интернет и электронную почту. Если установить флажок **Больше не задавать этот вопрос**, это сообщение больше не появится.



В раскрывающемся меню **Время** указывается период времени, на которое будет полностью отключена защита от вирусов и шпионских программ.



Блокировать сеть: персональный файервол будет блокировать весь исходящий и входящий обмен данными по сети и через Интернет.

Временно отключить файервол: файервол переводится в неактивное состояние. Для получения дополнительных сведений см. главу Интеграция в систему персонального файервола.

Дополнительные настройки...: установите этот флажок для просмотра дерева **Дополнительные настройки**. Также существуют и другие способы открыть ее, такие как нажатие клавиши F5 или использование меню **Настройка** > **Перейти к дополнительным настройкам...**.

Файлы журнала: файлы журнала содержат информацию обо всех важных программных событиях и предоставляют общие сведения об обнаруженных угрозах.

Сбросить настройки макета окна: для окна ESET Endpoint Security восстанавливаются размер и положение на экране по умолчанию.

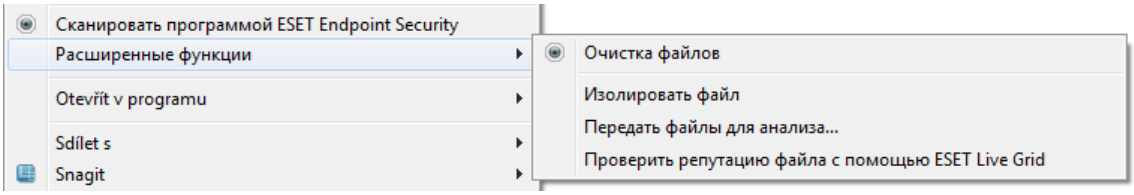
О программе: отображение системной информации, сведений об установленной версии ESET Endpoint Security и модулях программы. Также здесь показана дата окончания срока действия лицензии. В нижней части окна представлена информация об операционной системе и системных ресурсах.

4.7.6 Контекстное меню

Щелчок по выделенному объекту правой кнопкой мыши открывает контекстное меню. В этом меню перечислены все применимые к объекту команды.

Элементы управления ESET Endpoint Security можно интегрировать в контекстное меню. Более детальная настройка этих функций выполняется в дереве расширенных параметров, в разделах **Интерфейс** > **Контекстное меню**.

Интегрировать с контекстным меню: можно интегрировать элементы управления ESET Endpoint Security в контекстное меню.



В раскрывающемся меню **Тип меню** доступны следующие варианты.

- **Полное (сначала сканирование)**: активация всех функций контекстного меню; в главном меню появится пункт **Сканировать программой ESET Endpoint Security**.
- **Полное (сначала очистка)**: активация всех функций контекстного меню; в главном меню появится пункт **Очистить программой ESET Endpoint Security**.
- **Только сканирование**: в контекстном меню появится только пункт **Сканировать программой ESET Endpoint Security**.
- **Только очистка**: в контекстном меню появится только пункт **Очистить программой ESET Endpoint Security** .

4.7.7 Режим презентации

Режим презентации — это функция для тех, кто стремится избежать каких-либо перерывов в работе программного обеспечения и отвлекающих от дел всплывающих окон, а также желает свести к минимуму нагрузку на процессор. Режим презентации также можно использовать во время презентаций, которые нельзя прерывать деятельностью модуля защиты от вирусов. При включении этой функции отключаются все всплывающие окна, а работа планировщика полностью останавливается. Защита системы по-прежнему работает в фоновом режиме, но не требует какого-либо вмешательства со стороны пользователя.

Вы можете включить или отключить режим презентации в главном окне программы, выбрав пункт **Настройка** > **Компьютер**, а затем — **Включить** в разделе **Режим презентации** доступен в дереве расширенных параметров (F5). Чтобы активировать его, разверните раздел **Интерфейс**, выберите **Режим презентации** и установите флажок **Включить Режим презентации**. Включая режим презентации вы подвергаете систему угрозе, поэтому значок состояния защиты на панели задач станет оранжевого цвета, чтобы тем самым предупредить вас. Также этот значок наряду с оранжевой надписью Режим презентации включен появится в главном окне программы.

Если установить флажок **Автоматически включать Режим презентации при выполнении приложений в полноэкранном режиме**, Режим презентации будет включаться при запуске какого-либо приложения в полноэкранном режиме и автоматически выключаться после выхода из такого приложения. Это особенно удобно, если Режим презентации нужно включить сразу после запуска игры, открытия какого-либо приложения в полноэкранном режиме или начала работы с презентацией.

Также можно установить флажок **Автоматически отключать Режим презентации через X мин** и указать время (значение по умолчанию — 1 минута). Эта возможность используется, если режим презентации нужен только на определенное время, по окончании которого его следует автоматически отключить.

ПРИМЕЧАНИЕ. Если персональный файервол работает в интерактивном режиме и включен режим презентации , возможны проблемы при подключении к Интернету. Это может представлять сложности, если запускается игра, в которой используется подключение к Интернету. Обычно пользователю предлагается

подтвердить нужное действие (если не задано никаких правил или исключений для подключения), но в режиме презентации. В качестве решения можно задать правило подключения для каждого приложения, которое может конфликтовать с таким поведением, или использовать другой режим фильтрации в персональном файерволе. Также следует помнить о том, что при включенном режиме презентации может быть заблокирован переход на веб-страницу или использование приложения, которые способны представлять угрозу для безопасности, но при этом на экран не будет выведено никакого пояснения или предупреждения, поскольку взаимодействие с пользователем отключено.

5. Для опытных пользователей

5.1 Настройка прокси-сервера

В больших локальных сетях подключение компьютеров к Интернету может осуществляться через прокси-сервер. В этом случае необходимо задать описанные ниже параметры. Если этого не сделать, программа не сможет обновляться автоматически. В ESET Endpoint Security настройку прокси-сервера можно выполнить в двух разных разделах дерева расширенных параметров.

Во-первых, параметры прокси-сервера можно конфигурировать в разделе **Дополнительные настройки**, доступном через **Служебные программы** > **Прокси-сервер**. Настройка прокси-сервера на этом уровне позволяет задать его параметры для программы ESET Endpoint 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**, а также укажите номер его **порта** в соответствующем 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 подставить 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.

Параметры прокси-сервера также можно настроить в расширенных параметрах обновления (ветвь **Обновление** дерева **Дополнительные настройки**). Эти параметры применяются к конкретному профилю обновления и рекомендуются для ноутбуков, которые часто получают обновления сигнатур вирусов из разных источников. Для получения дополнительных сведений об этих параметрах см. раздел Дополнительные настройки обновления.

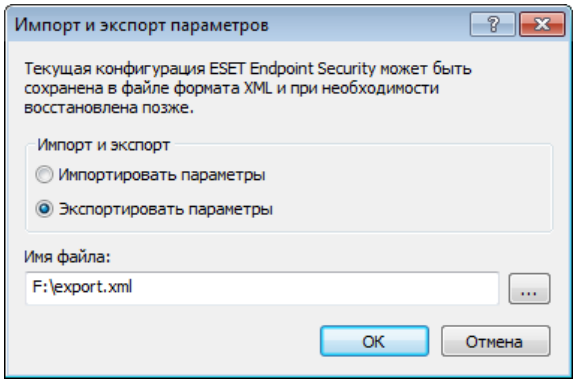
5.2 Импорт и экспорт параметров

Импорт и экспорт конфигурации ESET Endpoint Security можно выполнить в разделе **Настройка**.

И для импорта, и для экспорта используются файлы в формате XML. Импорт и экспорт удобны, если нужно создать резервную копию текущей конфигурации ESET Endpoint Security для дальнейшего использования. Экспорт параметров также полезен, если необходимо использовать выбранную конфигурацию ESET Endpoint Security на нескольких компьютерах. Для этого файл XML можно легко импортировать для переноса нужных параметров.

Импортировать конфигурацию несложно. В главном окне программы выберите пункт **Настройка** > **Импорт и экспорт параметров...**, а затем — команду **Импортировать параметры**. Введите путь к файлу конфигурации или нажмите кнопку **...**, чтобы выбрать нужный файл конфигурации, который следует импортировать.

Процедура экспорта конфигурации похожа на ее импорт. В главном меню выберите пункт **Настройка** > **Импорт и экспорт параметров...**. Выберите функцию **Экспорт параметров** и введите **Имя файла** для файла конфигурации (например, export.xml). С помощью проводника выберите место на компьютере для сохранения файла конфигурации.



5.3 Сочетания клавиш

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

Ctrl + G	отключение графического интерфейса пользователя в программе
Ctrl + I	переход на страницу ESET SysInspector
Ctrl + L	переход на страницу файлов журнала
Ctrl + S	переход на страницу планировщика
Ctrl + Q	переход на страницу карантина
Ctrl + U	вывод на экран диалогового окна, в котором можно задать имя пользователя и пароль
Ctrl + R	восстановление размеров окна и его положения на экране по умолчанию

Для более удобной навигации в программе обеспечения безопасности ESET можно использовать следующие сочетания клавиш.

F1	вызов справки
F5	вызов дополнительных параметров
Вверх/вниз	переход по элементам в программе
*	разворачивание узла дерева расширенных параметров
-	сворачивание узла дерева расширенных параметров
TAB	перемещение курсора по окну
Esc	закрытие активного диалогового окна

5.4 Командная строка

Модуль защиты от вирусов ESET Endpoint Security может быть запущен из командной строки вручную (с помощью команды «ecls») или в пакетном режиме (с помощью файла BAT-файла). Использование модуля сканирования командной строки ESET:

```
ecls [ПАРАМЕТРЫ..] ФАЙЛЫ..
```

Следующие параметры и аргументы могут использоваться при запуске сканера по требованию из командной строки.

Параметры

/base-dir=ПАПКА	загрузить модули из ПАПКИ
/quar-dir=ПАПКА	ПАПКА карантина
/exclude=МАСКА	исключить из сканирования файлы, соответствующие МАСКЕ
/subdir	сканировать вложенные папки (по умолчанию)
/no-subdir	не сканировать вложенные папки
/max-subdir-level=УРОВЕНЬ	максимальная степень вложенности папок для сканирования
/symlink	следовать по символическим ссылкам (по умолчанию)
/no-symlink	пропускать символические ссылки
/ads	сканировать ADS (по умолчанию)
/no-ads	не сканировать ADS
/log-file=ФАЙЛ	вывод журнала в ФАЙЛ
/log-rewrite	перезаписывать выходной файл (по умолчанию добавлять)
/log-console	вывод журнала в окно консоли (по умолчанию)
/no-log-console	не выводить журнал в консоль
/log-all	регистрировать также незараженные файлы
/no-log-all	не регистрировать незараженные файлы (по умолчанию)
/aind	показывать индикатор работы
/auto	сканирование и автоматическая очистка всех локальных дисков

Параметры модуля сканирования

/files	сканировать файлы (по умолчанию)
/no-files	не сканировать файлы
/memory	сканировать память

/boots	сканировать загрузочные секторы
/no-boots	не сканировать загрузочные секторы (по умолчанию)
/arch	сканировать архивы (по умолчанию)
/no-arch	не сканировать архивы
/max-obj-size=РАЗМЕР	сканировать файлы, только если их размер не превышает РАЗМЕР в мегабайтах (по умолчанию 0 = без ограничений)
/max-arch-level=УРОВЕНЬ	максимальная степень вложенности архивов для сканирования
/scan-timeout=ОГРАНИЧЕНИЕ	сканировать архивы не более указанного в ОГРАНИЧЕНИИ количества секунд
/max-arch-size=РАЗМЕР	сканировать файлы в архивах, только если их размер не превышает РАЗМЕР (по умолчанию 0 = без ограничений)
/max-sfx-size=РАЗМЕР	сканировать файлы в самораспаковывающихся архивах, только если их размер не превышает РАЗМЕР в мегабайтах (по умолчанию 0 = без ограничений)
/mail	сканировать файлы электронной почты (по умолчанию)
/no-mail	не сканировать файлы электронной почты
/mailbox	сканировать почтовые ящики (по умолчанию)
/no-mailbox	не сканировать почтовые ящики
/sfx	сканировать самораспаковывающиеся архивы (по умолчанию)
/no-sfx	не сканировать самораспаковывающиеся архивы
/rtp	сканировать упаковщики (по умолчанию)
/no-rtp	не сканировать упаковщики
/adware	сканировать рекламные/шпионские/опасные программы (по умолчанию)
/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 (по умолчанию)
/unwanted	сканировать на наличие потенциально нежелательных приложений
/no-unwanted	не сканировать на наличие потенциально нежелательных приложений (по умолчанию)
/pattern	использовать сигнатуры (по умолчанию)
/no-pattern	не использовать сигнатуры
/heur	включить эвристический анализ (по умолчанию)
/no-heur	отключить эвристический анализ
/adv-heur	включить расширенную эвристику (по умолчанию)
/no-adv-heur	отключить расширенную эвристику
/ext=РАСШИРЕНИЯ	сканировать только файлы с РАСШИРЕНИЯМИ, указанными через двоеточие
/ext-exclude=РАСШИРЕНИЯ	исключить из сканирования файлы с РАСШИРЕНИЯМИ, указанными через двоеточие
/clean-mode=РЕЖИМ	использовать РЕЖИМ очистки для зараженных объектов. Возможны следующие варианты: нет, стандартная (по умолчанию), тщательная, наиболее тщательная, удаление
/quarantine	копировать зараженные файлы, если они очищены, в карантин (дополнительно к действию, выполняемому при очистке)
/no-quarantine	не копировать зараженные файлы в карантин

Общие параметры

/help	показать справку и выйти
/version	показать сведения о версии и выйти
/preserve-time	сохранить последнюю отметку о времени доступа

Коды завершения

0	угроз не обнаружено
1	угроза обнаружена и очищена
10	некоторые файлы не удалось просканировать (могут быть угрозами)
50	угроза найдена
100	ошибка

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

5.5 ESET SysInspector

5.5.1 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 Security версию, а, во-вторых, загрузить самостоятельную версию (SysInspector.exe) бесплатно с веб-сайта ESET. Обе версии аналогичны по своим функциям и имеют одинаковые элементы управления программой. Единственное отличие заключается в том, как осуществляется управление результатами. И отдельная, и интегрированная версии позволяют экспортировать снимки системы в файл в формате XML и сохранять его на диске. Однако интегрированная версия также дает возможность хранить снимки системы прямо в разделе **Служебные программы** > **ESET SysInspector** (за исключением ESET Remote Administrator).

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.

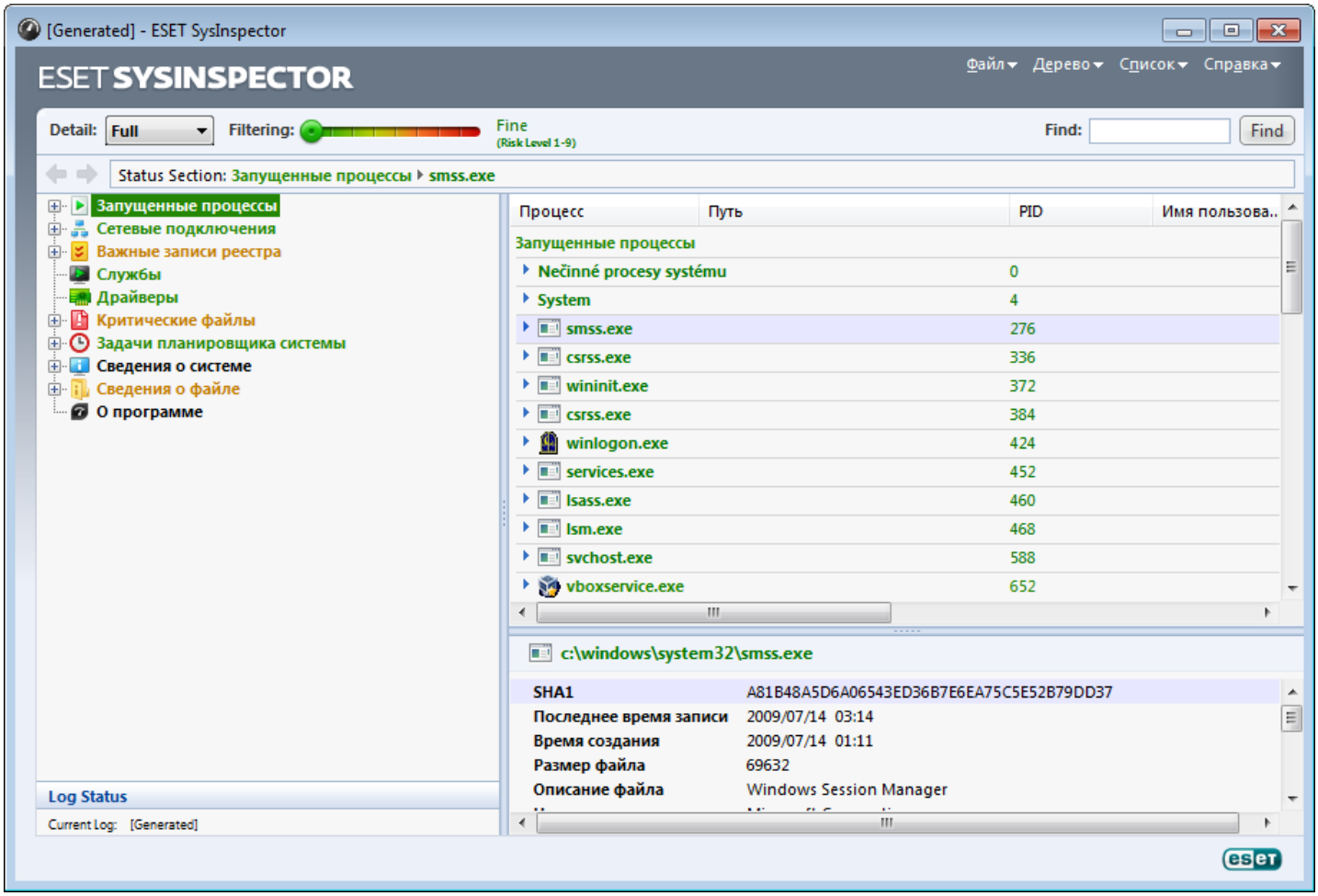
5.5.1.1 Запуск ESET SysInspector

Чтобы запустить ESET SysInspector, достаточно выполнить файл SysInspector.exe, загруженный с веб-сайта ESET.

Подождите, пока программа проверяет систему: это может занять несколько минут в зависимости от оборудования и собираемых данных.

5.5.2 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.).



5.5.2.1 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, рекомендуем просканировать компьютер с помощью ESET Online Scanner после нахождения любых таких элементов программой ESET SysInspector. 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.

5.5.2.2 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.

Задачи планировщика системы

Содержит список задач, запускаемых планировщиком заданий Windows в указанное время или через заданные интервалы.

Информация о системе

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

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 версии ESET SysInspector и список модулей программы.

5.5.2.2.1 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	создание стандартного снимка состояния компьютера
Ctrl + H	создание снимка состояния компьютера, в котором может быть зарегистрирована 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

5.5.2.3 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.

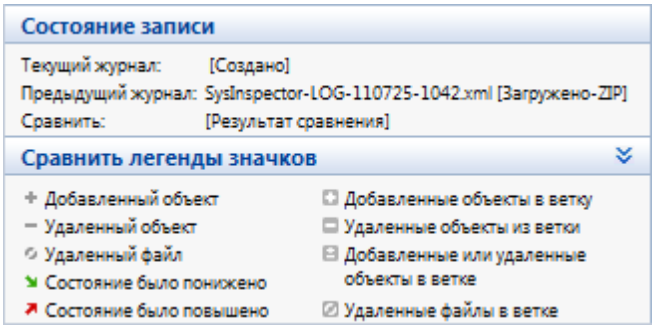
Напротив отображенных элементов ESET SysInspector выводит символы, обозначающие различия между сравниваемыми журналами.

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

5.5.3 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.

5.5.4 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 Shift, а затем выберите последний элемент, чтобы пометить все элементы.
- Щелкните выделенные объекты правой кнопкой мыши и в контекстном меню выберите пункт **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, перейдите в раздел **Файл** > **Запустить сценарий службы** и введите путь к своему сценарию.
- Нажмите кнопку **OK**, чтобы запустить сценарий.

5.5.4.1 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.

5.5.4.2 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 останавливаются выбранные драйверы. Учтите, что некоторые драйверы не позволяют останавливать себя.

O9) Critical files (Критические файлы)

Этот раздел содержит информацию о файлах, критически необходимых для правильной работы 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.

5.5.4.3 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.

5.5.5 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, решение ESET SysInspector подписано цифровой подписью («сертификатом»), которая гарантирует, что издателем данного программного обеспечения является компания ESET и оно 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 атакована злонамеренным кодом, который ведет себя как руткит, пользователь подвергается риску потери или хищения 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. При ее обнаружении файл проверяется с помощью этой информации. В противном случае 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.

5.5.6 ESET SysInspector как часть ESET Endpoint Security

Для того чтобы открыть ESET SysInspector в ESET Endpoint 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, создания 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 **Показать**. 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 журнала. Эта функция удобна, если нужно найти различия между текущим и более старым журналом. Для сравнения необходимо выбрать два снимка состояния.
- **Создать...**: создание 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 имеют состояние **Создано**.
- **Удалить/Удалить все**: удаление записей из списка.
- **Экспорт...**: сохранение выделенной записи в файл в формате XML (также есть возможность создания заархивированной версии).

5.6 ESET SysRescue

ESET SysRescue — это утилита для создания загрузочного диска, содержащего одно из решений ESET Security (ESET NOD32 Antivirus, ESET Smart Security или даже некоторые продукты для серверов). Главным преимуществом ESET SysRescue является то, что программа ESET 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.

5.6.1 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 (http://go.eset.eu/AIK) необходимо установить Windows AIK. Поскольку поддержка среды предустановки Windows ограничивается ее 32-разрядной версией, необходимо использовать 32-разрядный установочный пакет ESET Security при создании ESET SysRescue в 64-разрядных операционных системах. Средство ESET SysRescue поддерживает пакет Windows AIK версии 1.1 и более поздних.

ПРИМЕЧАНИЕ. Поскольку размер Windows AIK превышает 1 ГБ, для загрузки этого пакета требуется высокоскоростное интернет-соединение.

Средство ESET SysRescue доступно в составе ESET 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

5.6.2 Создание компакт-диска аварийного восстановления

Чтобы запустить мастер ESET SysRescue, выберите в меню **Пуск** > **Программы** > **ESET** > **ESET Endpoint 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 неправильно или поврежден, мастер предложит установить этот пакет или ввести путь к папке с Windows AIK (http://go.eset.eu/AIK).

ПРИМЕЧАНИЕ. Поскольку размер Windows AIK превышает 1 ГБ, для загрузки этого пакета требуется высокоскоростное интернет-соединение.

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

5.6.3 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.

5.6.4 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)
- Записывающее устройство (когда в качестве объекта выбран дисковод компакт- или DVD-дисков)

Кнопка **Создать** будет неактивна, если не указан установочный пакет MSI или на компьютере нет решений ESET Security. 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.

5.6.4.1 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.

5.6.4.2 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 установлено решение ESET Security.

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 установленного решения ESET Security.

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

ПРИМЕЧАНИЕ. Программа ESET 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.

5.6.4.3 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.

5.6.4.4 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**.

5.6.4.5 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.

5.6.4.6 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.

5.6.5 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 запущено решение ESET Security. Поскольку средство ESET SysRescue используется лишь в особых случаях, некоторые модули защиты и функции программы, имеющиеся в стандартной версии ESET 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.

5.6.5.1 Использование ESET SysRescue

Предположим, что компьютеры в сети были заражены вирусом, который вносит изменения в исполняемые файлы (.exe). ESET 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 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.

6. Глоссарий

6.1 Типы заражений

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

6.1.1 Вирусы

Компьютерный вирус — это фрагмент злонамеренного кода, который добавляется в начало или конец файлов на компьютере. Название было выбрано из-за сходства с биологическими вирусами, так как они используют похожие методы для распространения с компьютера на компьютер. Часто термином «вирус» неверно обозначают любые типы угроз. Однако постепенно он выводится из употребления, и на смену ему приходит более точный термин «вредоносная программа».

Компьютерные вирусы атакуют в основном исполняемые файлы и документы. Компьютерный вирус функционирует следующим способом: после запуска зараженного файла вызывается и выполняется злонамеренный код. Это происходит до выполнения исходного приложения. Вирус способен заразить все файлы, на запись в которые у пользователя есть права.

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.

Если ваш компьютер заражен вирусом, который не удается очистить, отправьте соответствующие файлы в лабораторию ESET для изучения. В ряде случаев зараженные файлы изменяются настолько, что их невозможно очистить. В таком случае их нужно заменять чистыми копиями.

6.1.2 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 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.

6.1.3 Троянские программы

Исторически троянскими программами называли такой класс угроз, которые пытаются маскироваться под полезные программы, тем самым заставляя пользователя запускать их.

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

- **Загрузчик**— вредоносная программа, способная загружать другие угрозы из Интернета.
- **Dropper**— вредоносная программа, которая предназначена для заражения компьютеров другими вредоносными программами.
- **Backdoor**— вредоносная программа, которая обменивается данными со злоумышленниками, позволяя им получить доступ к компьютеру и контроль над ним.
- **Клавиатурный шпион** — программа, которая регистрирует все, что пользователь набирает на клавиатуре, и отправляет эту информацию злоумышленникам.
- **Программа дозвона** — вредоносная программа, которая предназначена для подключения к номерам с

высокими тарифными планами, а не к поставщику интернет-услуг пользователя. При этом пользователь практически не может заметить, что создано новое подключение. Программы дозвона могут нанести вред только пользователям модемов. К счастью, модемы уже не распространены столь широко, как раньше.

Если на компьютере обнаружен файл, классифицированный как троянская программа, рекомендуется удалить его, так как он с большой вероятностью содержит злонамеренный код.

6.1.4 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 системного реестра. По этой причине их активность невозможно обнаружить стандартными методами проверки.

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 Endpoint Security есть преимущества технологии Anti-Stealth, которая позволяет обнаружить и устранить активные руткиты.

6.1.5 Рекламные программы

Под рекламной программой понимается программное обеспечение, существующее за счет рекламы. Программы, демонстрирующие пользователю рекламные материалы, относятся к этой категории. Рекламные приложения часто автоматически открывают всплывающие окна с рекламой в веб-браузере или изменяют домашнюю страницу. 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 стоить уделить особое внимание установке программы. Чаще всего программа установки предупреждает об установке дополнительной рекламной программы. Зачастую пользователь имеет возможность отказаться от его установки и установить необходимую программу без рекламной.

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 он с большой вероятностью содержит злонамеренный код.

6.1.6 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 технологии служат для изучения требований и интересов пользователей и позволяют создавать рекламные материалы, более соответствующие 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 известного бесплатного программного обеспечения, вместе с которым поставляется шпионское, могут служить клиенты пиринговых (P2P) сетей. Программы Spyfalcon и Spy Sheriff (и многие другие) относятся к особой подкатегории шпионских программ. Утверждается, что они предназначены для защиты от шпионских программ, но на самом деле 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.

6.1.7 Потенциально опасные приложения

Существует множество нормальных программ, предназначенных для упрощения администрирования подключенных к сети компьютеров. Однако злоумышленники могут использовать их для причинения вреда. Программное обеспечение ESET Endpoint 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, записывающие 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.

6.1.8 Потенциально нежелательные приложения

Потенциально нежелательные приложения не всегда являются вредоносными, однако могут негативно повлиять 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 (всплывающие окна, реклама).
- Активируются и выполняются скрытые процессы.
- Повышается уровень потребления системных ресурсов.
- Появляются изменения в результатах поиска.
- Приложение обменивается данными с удаленными серверами.

6.2 Типы удаленных атак

Существует множество специальных технологий, с помощью которых злоумышленники могут атаковать удаленные компьютеры. Они подразделяются на несколько категорий.

6.2.1 DoS-атаки

DoS-атаки (атаки типа отказ в обслуживании) представляют собой попытку сделать компьютер или сеть недоступными тем пользователями, для которых они предназначены. Обмен данными между пользователями пораженного компьютера затруднен или невозможен в приемлемом режиме. Компьютеры, подвергшиеся действию DoS-атаки, обычно должны быть перезагружены для восстановления нормальной работы.

В большинстве случаев объектами этой атаки становятся веб-серверы, а целью является вывод их из строя и, как следствие, их недоступность на некоторое время.

6.2.2 Атака путем подделки записей кэша DNS

Атака путем подделки записей кэша DNS (сервер доменных имен) позволяет хакерам убедить DNS-сервер любого компьютера в том, что предоставляемые подложные данные являются истинными. Ложная информация кэшируется на определенное время, давая злоумышленникам возможность перезаписать ответы DNS-сервера с IP-адресами. В результате при попытке посещения веб-сайтов пользователь загружает компьютерные вирусы и черви вместо исходного содержимого.

6.2.3 Атаки червей

Компьютерные черви — это содержащие злонамеренный код программы, которые атакуют главные компьютеры и распространяются через сеть. Сетевые черви используют сетевые уязвимости различных приложений. Благодаря Интернету они распространяются по всему земному шару за считаные часы после запуска в сеть. В некоторых случаях счет идет на минуты.

Многих из атак червей (Sasser, SqlSlammer) можно избежать, используя настройки персонального файервола по умолчанию или с помощью блокировки незащищенных и неиспользуемых портов. Очень важно регулярно устанавливать новейшие пакеты обновления операционной системы.

6.2.4 Сканирование портов

Сканирование портов используется, чтобы определить, какие порты компьютера открыты на узле сети. Сканер портов представляет собой программное обеспечение, которое предназначено для поиска таких портов.

Компьютерный порт является виртуальной точкой, которая управляет сетевым трафиком в обоих направлениях. Это является критичным с точки зрения сетевой безопасности. В больших сетях данные, которые собираются с помощью сканера портов, могут помочь выявить потенциальные уязвимости компьютерных систем. Такое использование является допустимым.

Однако сканеры часто используются злоумышленниками для взлома систем безопасности. Первым шагом отправляется серия пакетов на каждый из портов. В зависимости от полученных ответов определяется, какой из портов можно использовать. Сканирование не причиняет вреда само по себе, но следует иметь в виду, что такая активность зачастую является признаком попытки выявления уязвимости и последующей атаки злоумышленников на систему.

Сетевые администраторы обычно советуют блокировать все неиспользуемые порты и защищать используемые от неавторизованного доступа.

6.2.5 TCP-десинхронизация

TCP-десинхронизация — это метод, используемых в атаках подмены одного из участников TCP-соединения. Этот метод основан на процессах, которые происходят, когда порядковый номер приходящего пакета отличается от ожидаемого. Пакеты с неожиданными номерами пропускаются (или сохраняются в специальном буфере, если они попадают в текущее окно соединения).

При десинхронизации обе стороны обмена данными пропускают полученные пакеты. В этот момент злоумышленники могут заразить и передать пакеты с правильным порядковым номером. Злоумышленники могут даже манипулировать обменом данных и вносить в него изменения.

В атаках путем подмены одного из участников целью является внедрение в двухсторонний обмен данными между сервером и клиентом. Многие атаки в этом случае могут быть предотвращены путем использования аутентификации для каждого из сегментов TCP. Кроме того, следует использовать рекомендуемые параметры для сетевых устройств.

6.2.6 SMB Relay

SMBRelay и SMBRelay2 являются особыми программами, которые способны атаковать удаленные компьютеры. Эти программы используют уязвимость протокола SMB, который встроен в NetBIOS. Если пользователь предоставляет общий доступ к каким-либо папкам через локальную сеть, скорее всего это осуществляется с помощью протокола SMB.

В рамках обмена данными по локальной сети происходит обмен данными хеш-таблиц паролей.

SMBRelay принимает соединения по UDP на портах 139 и 445, транслирует пакеты, которыми обменивается клиент и сервер, и подменяет их. После подключения и аутентификации соединение с клиентом прерывается. SMBRelay создает новый виртуальный IP-адрес. Новый адрес доступен с помощью следующей команды: net use \\192.168.1.1. После этого доступ к адресу открыт для любой сетевой функции Windows. SMBRelay транслирует весь обмен данными через себя, кроме процессов установления соединения и аутентификации. Удаленная атакующая сторона может использовать IP-адрес, пока подключен клиентский компьютер.

SMBRelay2 работает на основе того же принципа, что и SMBRelay, но использует имена NetBIOS вместо IP-адресов. Обе программы используют атаки «злоумышленник в середине». Эти атаки позволяют удаленной атакующей стороне считывать, вставлять и изменять сообщения между двумя сторонами, не обнаруживая

себя. Атакованные таким методом компьютеры зачастую прекращают отвечать на запросы пользователя или внезапно перезагружаются.

Для того чтобы избежать проблем подобного рода, рекомендуется использовать пароли для аутентификации или ключи.

6.2.7 Атаки по протоколу ICMP

Протокол ICMP является популярным и широко используемым протоколом Интернета. Применяется он преимущественно подключенными к сети компьютерами для отправки сообщений об ошибках.

Удаленные злоумышленники пытаются использовать уязвимости протокола ICMP. Протокол ICMP предназначен для передачи данных в одном направлении без аутентификации. Это позволяет злоумышленникам организовывать DoS-атаки (отказ в обслуживании) или атаки, предоставляющие не имеющим на это права лицам доступ ко входящим и исходящим пакетам.

Типичными примерами атак по протоколу ICMP являются ping-флуд, флуд эхо-запросов по протоколу ICMP и smurf-атаки. Компьютеры, подвергающиеся атаке по протоколу ICMP, значительно замедляют свою работу (это касается всех приложений, использующих Интернет), и у них возникают проблемы при подключении к Интернету.

6.3 Электронная почта

Электронная почта является современным средством общения, которое применяется во многих областях. Она отличается гибкостью, высокой скоростью и отсутствием посредников и сыграла ключевую роль в распространении Интернета в начале 90-х годов прошлого века.

К сожалению, вследствие высокого уровня анонимности электронная почта и Интернет оставляют пространство для незаконных действий, таких как рассылка спама. К спаму относятся нежелательные рекламные объявления, мистификации и сообщения, предназначенные для распространения вредоносных программ. Доставляемые пользователю неудобства и опасность увеличиваются из-за того, что стоимость рассылки минимальна, а в распоряжении авторов спама есть множество средств для получения новых адресов электронной почты. Кроме того, количество и разнообразие спама сильно затрудняют контроль над ним. Чем дольше используется адрес электронной почты, тем выше вероятность того, что он попадет в базы данных, используемые для рассылки спама. Вот некоторые советы, помогающие избежать этого.

- По возможности не размещайте свой адрес электронной почты в Интернете.
- Давайте свой адрес только тем, кому полностью доверяете.
- Если возможно, не используйте распространенные слова в качестве псевдонимов (чем сложнее псевдоним, тем труднее отследить адрес).
- Не отвечайте на полученный спам.
- Будьте осторожны при заполнении форм на веб-сайтах (особенно если они содержат пункты типа «Да, я хочу получать информацию»).
- Используйте «специализированные» адреса электронной почты (например, заведите один адрес для работы, другой для общения с друзьями и т. д.).
- Время от времени меняйте адрес электронной почты.
- Используйте какое-либо решение для защиты от спама.

6.3.1 Рекламные объявления

Реклама в Интернете является одним из наиболее бурно развивающихся видов рекламы. Ее преимуществами являются минимальные затраты и высокая вероятность непосредственного общения с потребителем. Кроме того, сообщения доставляются практически мгновенно. Многие компании используют электронную почту в качестве эффективного маркетингового инструмента для общения со своими существующими и потенциальными клиентами.

Этот вид рекламы является нормальным, так как потребители могут быть заинтересованы в получении коммерческой информации о некоторых товарах. Однако многие компании занимаются массовыми рассылками нежелательных коммерческих сообщений. В таких случаях реклама по электронной почте выходит за границы допустимого, и эти сообщения классифицируются как спам.

Количество нежелательных сообщений уже стало проблемой, и при этом никаких признаков его сокращения не наблюдается. Авторы нежелательных сообщений часто пытаются выдать спам за нормальные сообщения.

6.3.2 Мистификации

Мистификацией называется ложная информация, распространяющаяся через Интернет. Обычно мистификации рассылаются по электронной почте или с помощью таких средств общения, как ICQ и Skype. Собственно сообщение часто представляет собой шутку или городскую легенду.

Связанные с компьютерными вирусами мистификации направлены на то, чтобы вызвать в получателях страх, неуверенность и мнительность, побуждая их верить в то, что «не поддающийся обнаружению вирус» удаляет их файлы, крадет пароли или выполняет какие-либо другие крайне нежелательные действия с компьютерами.

Некоторые мистификации работают, предлагая получателям переслать сообщение своим знакомым, за счет чего увеличивается масштаб мистификации. Существуют мистификации, которые передаются через мобильные телефоны, мистификации, представляющие собой просьбы о помощи, предложения получить деньги из-за границы, и прочие. Часто бывает невозможно понять мотивацию создателя мистификации.

Если сообщение содержит просьбу переслать его всем знакомым, это сообщение с большой вероятностью является мистификацией. Существует большое количество веб-сайтов, которые могут проверить, является ли сообщение нормальным. Прежде чем пересылать сообщение, которое кажется вам мистификацией, попробуйте найти в Интернете информацию о нем.

6.3.3 Фишинг

Термин «фишинг» обозначает преступную деятельность, в рамках которой используются методы социальной инженерии (манипулирование пользователем, направленное на получение конфиденциальной информации). Целью фишинга является получение доступа к таким конфиденциальным данным, как номера банковских счетов, PIN-коды и т. п.

Попытка получения информации обычно представляет собой отправку сообщения якобы от доверенного лица или компании (такой как финансового учреждения или страховой компании). Сообщение может казаться благонадежным и содержать изображения и текст, которые могли изначально быть получены от источника, якобы являющегося отправителем данного сообщения. Под разными предлогами (проверка данных, финансовые операции) предлагается предоставить какую-либо личную информацию, такую как номера банковских счетов, имена пользователя, пароли и т. д. Если такие данные предоставляются, они легко могут быть украдены и использованы в преступных целях.

Банки, страховые компании и другие легитимные организации никогда не запрашивают имена пользователей и пароли в незапрошенных сообщениях электронной почты.

6.3.4 Распознавание мошеннических сообщений

Вообще существует несколько признаков, которые могут помочь распознать спам (нежелательные сообщения) в почтовом ящике. Если сообщение соответствует хотя бы нескольким из этих критериев, оно, наиболее вероятно, является нежелательным.

- Адрес отправителя отсутствует в адресной книге получателя.
- Предлагается получить большую сумму денег, но сначала нужно оплатить небольшую сумму.
- Под разными предлогами (проверка данных, финансовые операции) предлагается предоставить какие-либо личные данные, такие как номера банковских счетов, имя пользователя, пароль и т. д.
- Сообщение написано на иностранном языке.
- Предлагается покупка продукции, в которой получатель не заинтересован. Однако если получателя заинтересовало предложение, следует проверить, является ли отправитель надежным поставщиком (например, проконсультироваться с представителем производителя продукции).
- Некоторые из слов намеренно написаны с ошибками, чтобы обмануть фильтр спама. Например, «веагро» вместо «виагра» и т. п.

6.3.4.1 Правила

В контексте решений для защиты от спама и почтовых клиентов под правилами понимаются инструменты обработки электронной почты. Правило состоит из двух логических частей:

1. условие (например, получение сообщения с определенного адреса);
2. действие (например, удаление сообщения, перемещение его в указанную папку).

Количество и сочетания правил зависят от конкретного решения по защите от спама. Правила предназначены для борьбы со спамом (нежелательными сообщениями). Стандартные примеры приведены далее.

- 1. Условие: во входящем сообщении содержатся некоторые слова, часто присутствующие в нежелательных сообщениях.
  2. Действие: удалить сообщение.
- 1. Условие: у входящего сообщения есть вложение с расширением .exe.
  2. Действие: удалить вложение и доставить сообщение в почтовый ящик.
- 1. Условие: входящее сообщение отправлено сотрудником компании, в которой работает пользователь.
  2. Действие: переместить сообщение в папку «Работа».

Рекомендуется использовать сочетание правил в программах защиты от спама, чтобы упростить администрирование и более эффективно отфильтровывать спам.

6.3.4.2 «Белый» список

Вообще под «белым» списком понимается перечень объектов или лиц, которые являются приемлемыми или имеют доступ. Термин «"белый" список электронной почты» означает список адресов пользователей, от которых разрешено получать сообщения. Такого рода списки создаются на основе поиска по ключевым словам в адресах электронной почты, именах домена или IP-адресах.

Если «белый» список работает в «исключительном» режиме, сообщения с других адресов, доменов или IP-адресов получаться не будут. Если же «белый» список не является исключительным, такие сообщения не будут удаляться, а будут обрабатываться каким-либо другим способом.

«Белый» список обладает противоположным «черному» списку назначением. «Белые» списки сравнительно просто поддерживать, значительно проще, чем «черные». Для большей эффективности фильтрации спама рекомендуется использовать и «белый», и «черный» списки.

6.3.4.3 «Черный» список

В общем случае «черный» список является списком неприемлемых или запрещенных объектов или лиц. В виртуальном мире это метод, позволяющий принимать сообщения, которые приходят от всех пользователей, отсутствующих в таком списке.

Существует два типа «черных» списков. К первому типу относятся списки, созданные самими пользователями, в их приложениях для защиты от спама, а ко второму — профессиональные регулярно обновляемые «черные» списки, которые создаются специализированными учреждениями и распространяются через Интернет.

Принципиально важно использовать «черный» список для блокировки спама, но при этом вести такой список сложно, так как новые объекты блокирования появляются ежедневно. Рекомендуется использовать и «белый», и «черный» список, чтобы максимально эффективно отфильтровывать спам.

6.3.4.4 Контроль на стороне сервера

Контроль на стороне сервера — это метод выявления массовых рассылок спама на основе количества полученных сообщений и реакции пользователей на них. Каждое сообщение оставляет уникальный цифровой «отпечаток», который основан на его содержимом. Уникальный идентификационный номер ничего не говорит о содержимом сообщения. Однако два одинаковых сообщения имеют одинаковые отпечатки, тогда как два различающихся — разные.

Если сообщение помечено как спам, его отпечаток отправляется на сервер. Если сервер получает и другие идентичные отпечатки (соответствующие одному и тому же нежелательному сообщению), этот отпечаток сохраняется в базе данных отпечатков спама. При сканировании входящих сообщений программа отправляет отпечатки сообщений на сервер. Сервер возвращает данные о тех отпечатках, которые соответствуют сообщениям, уже помеченным пользователями как спам.