ESET NOD32 Antivirus 4

для Linux Desktop

Инструкция по установке и руководство пользователя

Щелкните здесь, чтобы загрузить актуальную версию этого документа

ESET NOD32 Antivirus 4

Международная служба поддержки: www.eset.com/support

Версия 8.4.2011

Содержание

1. ESET NOD32 Antivirus

В результате роста популярности Unix-подобных операционных систем создатели вредоносных программ стали активнее разрабатывать вирусы для этой платформы. Приложение ESET NOD32 Antivirus обеспечивает мощную и эффективную защиту от угроз. Оно также может обнаруживать угрозы для Windows, защищая пользователей Linux во время взаимодействия с пользователями Windows и наоборот. Хотя вредоносные программы для Windows не представляют непосредственной угрозы для системы Linux, их деактивация на компьютере с системой Linux позволяет предотвратить заражение других компьютеров с системой Windows по локальной сети или через Интернет.

1.1 Требования к системе

Чтобы приложение ESET NOD32 Antivirus работало нормально, аппаратные средства и программное обеспечение на компьютере должны соответствовать указанным ниже требованиям.

ESET NOD32 Antivirus:

	Требования к системе
Архитектура процессора	32-разрядная либо 64-разрядная AMD® или Intel®
Система	Дистрибутивы на основе Debian или RedHat (Ubuntu, OpenSuse, Fedora, Mandriva, RedHat и т. д.) Ядро 2.6.x Библиотека GNU C 2.3 или более поздней версии GTK+ 2.6 или более поздней версии Рекомендуется обеспечить совместимость с LSB 3.1
Объем памяти	512 МБ
Свободно на диске	100 МБ

2. Установка

Прежде чем приступать к процессу установки, нужно закрыть все открытые программы. В ESET NOD32 Antivirus есть компоненты, которые могут конфликтовать с другими установленными антивирусными программами при их наличии. Компания ESET настоятельно рекомендует удалить любые другие программы, чтобы предотвратить возможные проблемы. Установить ESET NOD32 Antivirus можно с установочного компакт-диска или с помощью файла, доступного на веб-сайте ESET.

Для запуска мастера установки выполните одно из перечисленных далее действий.

- Если установка выполняется с установочного компакт-диска, вставьте этот диск в дисковод. Дважды щелкните значок установки ESET NOD32 Antivirus, чтобы запустить программу установки.
- Если установка выполняется с помощью загруженного файла, щелкните его правой кнопкой мыши, перейдите на вкладку **«Параметры» > «Разрешения»**, установите флажок **«Разрешить исполнение файла как программы»** и закройте окно. Дважды щелкните файл, чтобы запустить программу установки.

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

2.1 Обычная установка

Обычная установка выполняется с использованием параметров конфигурации, подходящих для большинства пользователей. Эти параметры обеспечивают максимальную защиту и высокую производительность системы. Обычная установка — это вариант по умолчанию; при отсутствии особых требований не следует выбирать другой способ.

Система быстрого оповещения ThreatSense.Net предназначена для своевременного информирования компании ESET о появлении новых угроз. Она помогает быстро реагировать на угрозы для защиты пользователей. Эта система предусматривает передачу образцов вредоносного кода в лабораторию ESET Threat Lab. Там они анализируются, обрабатываются и добавляются в базу данных сигнатур вирусов. По умолчанию флажок **«Включить систему быстрого оповещения ThreatSense.Net»** установлен. Для изменения параметров передачи подозрительных файлов нажмите кнопку **«Настройка»**. Дополнительную информацию см. в статье «ThreatSense.Net» 19.

Следующим действием при установке является настройка обнаружения потенциально нежелательных приложений. Приложения, относящиеся к потенциально нежелательному ПО, могут не быть вредоносными, однако они часто негативно влияют на работу операционной системы. Такие программы часто поставляются вместе с полезными, и их установку трудно заметить во время установки всего пакета программ. Хотя при установке таких приложений обычно отображается уведомление, они вполне могут быть установлены без согласия пользователя. Рекомендуется выбрать параметр **«Включить обнаружение потенциально нежелательного ПО»**, чтобы разрешить приложению ESET NOD32 Antivirus выявлять угрозы такого типа. Если включать эту функцию не нужно, установите флажок **«Отключить обнаружение потенциально нежелательного ПО»**.

Для завершения установки нажмите кнопку **«Установить»**.

2.2 Выборочная установка

Выборочная установка предназначена для опытных пользователей, которые желают изменить расширенные настройки в ходе установки приложения.

Если используется прокси-сервер, можно указать его параметры, установив флажок **«Я использую прокси-сервер»**. Введите IP-адрес или URL-адрес прокси-сервера в поле **«Адрес»**. В поле **«Порт»** укажите порт, по которому прокси-сервер принимает запросы на соединение (по умолчанию 3128). Если прокси-сервер требует аутентификации, введите правильные **имя пользователя** и **пароль**, которые необходимы для доступа к нему. Если прокси-сервер не используется, установите флажок **«Я не использую прокси-сервер»**.

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

Система быстрого оповещения ThreatSense.Net предназначена для своевременного информирования компании ESET о появлении новых угроз. Она помогает быстро реагировать на угрозы для защиты пользователей. Эта система предусматривает передачу образцов вредоносного кода в лабораторию ESET Threat Lab. Там они анализируются, обрабатываются и добавляются в базу данных сигнатур вирусов. По умолчанию флажок **«Включить систему быстрого оповещения ThreatSense.Net»** установлен. Для изменения параметров передачи подозрительных файлов нажмите кнопку **«Настройка»**. Дополнительную информацию см. в статье «ThreatSense.Net» 19.

Следующим действием при установке является настройка обнаружения потенциально нежелательных приложений. Приложения, относящиеся к потенциально нежелательному ПО, могут не быть вредоносными, однако они часто негативно влияют на работу операционной системы. Такие программы часто поставляются вместе с полезными, и их установку трудно заметить во время установки всего пакета программ. Хотя при установке таких приложений обычно отображается уведомление, они вполне могут быть установлены без согласия

пользователя. Рекомендуется выбрать параметр **«Включить обнаружение потенциально нежелательного ПО»**, чтобы разрешить приложению ESET NOD32 Antivirus выявлять угрозы такого типа.

Для завершения установки нажмите кнопку **«Установить»**.

2.3 Активация программы

Активировать копию программы ESET NOD32 Antivirus можно из самой программы. Нажмите значок ESET NOD32 Antivirus, расположенный в строке меню (в верхней части экрана), после чего выберите пункт **«Активация программы...»**.

1. Если вы приобрели коробочную розничную версию программы, к ней прилагается ключ активации, а также пошаговые инструкции по активации. Обычно ключ активации расположен внутри упаковки программного продукта или на ее тыльной стороне. Для успешного выполнения активации ключ активации нужно вводить именно в том виде, в котором он предоставлен.

2. Если имя пользователя и пароль уже получены, выберите вариант **«Активировать с помощью имени пользователя и пароля»** и введите сведения о лицензии в соответствующие поля. Этот вариант аналогичен использованию пункта **«Настройка имени пользователя и пароля...»** в окне обновления программы.

3. Если вы хотите оценить ESET NOD32 Antivirus, прежде чем покупать программу, выберите вариант **«Активировать пробную лицензию»**. Введите свое имя и **адрес электронной почты**. Данные вашей пробной лицензии будут высланы по этому адресу. Программа ESET NOD32 Antivirus будет активирована на ограниченный период времени. Каждый пользователь может активировать только одну пробную лицензию.

Если у вас нет лицензии, но вы хотите купить ее, выберите вариант **«Приобрести лицензию»**. В результате откроется веб-сайт местного распространителя ESET.

2.4 Сканирование ПК по требованию

После установки приложения ESET NOD32 Antivirus следует выполнить сканирование компьютера на наличие вредоносного кода. В главном окне программы выберите пункт **«Сканирование компьютера»**, а затем — **«Сканирование Smart»**. Дополнительную информацию о сканировании компьютера по требованию см. в разделе «Сканирование ПК по требованию» 10.

3. Руководство для начинающих

Этот раздел содержит обзор приложения ESET NOD32 Antivirus и его основных параметров.

3.1 Вводные сведения об интерфейсе пользователя: режимы

Главное окно ESET NOD32 Antivirus разделено на две основные части. Основное окно справа содержит информацию, относящуюся к параметру, выбранному в главном меню слева.

Ниже описаны пункты главного меню.

- **«Состояние защиты»**: этот пункт предоставляет информацию о состоянии защиты ESET NOD32 Antivirus. Если активирован **расширенный режим**, отображается подменю **«Статистика»**.
- **«Сканирование компьютера»**: этот пункт позволяет настроить и запустить **сканирование компьютера по требованию**.
- **«Обновление»**: выводит информацию об обновлениях базы данных сигнатур вирусов.
- **«Настройка»**: этот параметр позволяет настроить уровень безопасности компьютера. Если активирован **расширенный режим**, отображается подменю **«Защита от вирусов и шпионских программ»**.
- **«Служебные программы»**: этот пункт предоставляет доступ к **файлам журнала**, **папке карантина** и **планировщику**. Он отображается только в **расширенном режиме**.
- **«Справка»**: этот пункт предоставляет информацию о программе, а также доступ к файлам справки, базе знаний в Интернете и веб-сайту компании ESET.

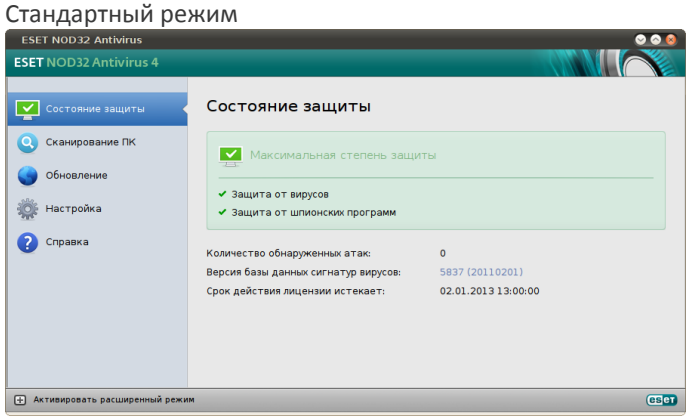
Интерфейс пользователя ESET NOD32 Antivirus позволяет переключаться между стандартным и расширенным режимами. Стандартный режим предоставляет доступ к функциям, необходимым для выполнения обычных операций. Расширенные функции при этом недоступны. Для переключения между режимами используйте значок « **+**» рядом с пунктом **«Активировать расширенный режим»** или **«Активировать стандартный режим»** в левом нижнем углу главного окна приложения.

Обычный режим предоставляет доступ ко всем функциям, необходимым для выполнения обычных операций. Расширенные функции при этом недоступны.

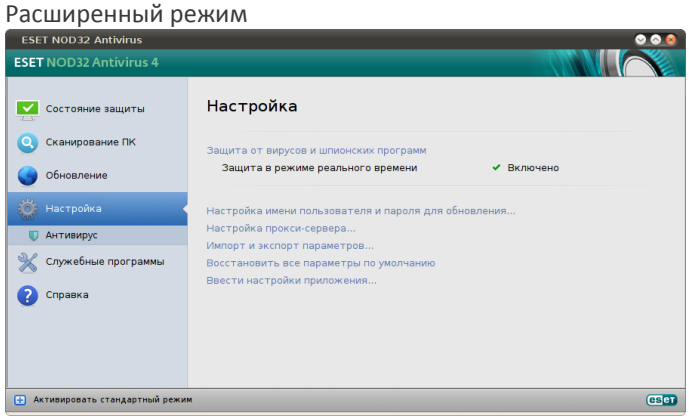
При переключении в расширенный режим в главном меню появляется пункт **«Служебные программы»**. Он позволяет использовать подменю **«Файлы журнала»**, **«Карантин»** и **«Планировщик»**.

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

Стандартный режим

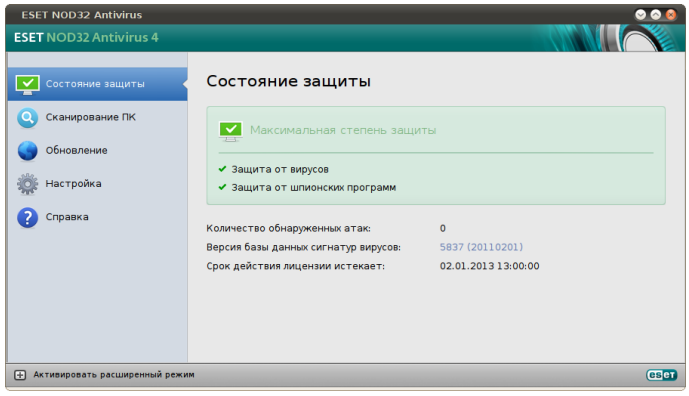


Расширенный режим



3.1.1 Проверка работоспособности системы

Чтобы просмотреть **состояние защиты**, выберите соответствующий пункт в главном меню. В главном окне появится сводная информация о работе приложения ESET NOD32 Antivirus а также подменю **статистики**. Откройте это подменю, чтобы просмотреть более подробные сведения и статистическую информацию о сканировании компьютера. Окно «Статистика» доступно только в расширенном режиме.

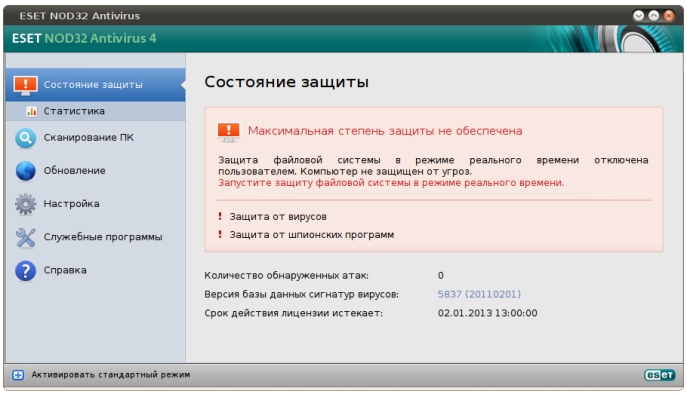


3.1.2 Действия, которые следует выполнить, если приложение не работает надлежащим образом

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

Если предложенные решения не позволяют устранить проблему, выберите пункт **«Справка»** для доступа к файлам справки или поиска в базе знаний.

Если вам потребуется помощь, обратитесь в службу поддержки компании ESET на веб-сайте ESET. Специалисты службы поддержки оперативно ответят на ваши вопросы и помогут найти решение проблемы.



4. Работает с ESET NOD32 Antivirus

4.1 Защита от вирусов и шпионских программ

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

4.1.1 Защита в режиме реального времени

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

4.1.1.1 Настройка защиты в режиме реального времени

Функция защиты в режиме реального времени проверяет все типы носителей и запускается различными событиями. Функция защиты в режиме реального времени использует разные технологии обнаружения вирусов ThreatSense, описанные в разделе «Настройка параметров модуля ThreatSense» 12. Способы обработки новых и существующих файлов этой функцией могут различаться. При обработке новых файлов могут быть применены углубленные способы контроля.

По умолчанию функция защиты в режиме реального времени запускается при загрузке системы и обеспечивает постоянное сканирование. В особых случаях (например, при возникновении конфликта с другим модулем сканирования в режиме реального времени) работу функции можно прервать, нажав значок ESET NOD32 Antivirus, расположенный в строке меню (в верхней части экрана) и выбрав вариант **«Отключить защиту файловой системы в режиме реального времени»**. Также работу функции защиты в режиме реального времени можно прервать из главного окна программы (**«Настройка»** > **«Антивирус»** > **«Отключить»**).

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

4.1.1.1.1 Сканировать при (сканирование при наступлении события)

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

4.1.1.1.2 Расширенные параметры сканирования

В этом окне можно определить типы объектов, которые будет сканировать модуль ThreatSense, включить или отключить **расширенную эвристику**, а также изменить настройки архивов и файлового кэша.

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

Можно включить или отключить расширенное эвристическое сканирование ThreatSense по отдельности для запускаемых, создаваемых или изменяемых файлов, установив флажок **«Расширенная эвристика»** в соответствующих разделах параметров ThreatSense.

Чтобы свести к минимуму влияние защиты в режиме реального времени на систему, можно задать размер кэша оптимизации. Эта функция активна, если используется параметр **«Включить очистку файлового кэша»**. Если он отключен, все файлы сканируются каждый раз при доступе к ним. Файлы не будут сканироваться повторно после кэширования (если они не были изменены), пока не превышен указанный размер кэша. Файлы сканируются повторно сразу после обновления базы данных сигнатур вирусов.

Чтобы включить или отключить эту функцию, используйте параметр **«Включить очистку файлового кэша»**. Чтобы задать объем кэшируемых файлов, введите нужное значение в поле ввода **«Размер кэша»**.

В окне **«Настройка модуля ThreatSense»** можно настроить дополнительные параметры сканирования, например можно определить типы **объектов**, которые необходимо сканировать, используемые **параметры** и уровень **очистки**, а также указать **расширения** и **ограничения** размера файлов для защиты в режиме реального времени. Окно настройки модуля ThreatSense можно открыть, нажав кнопку **«Настройка»** рядом с элементом **«Модуль ThreatSense»** в окне расширенной настройки. Дополнительную информацию о параметрах модуля ThreatSense см. в разделе «Настройка параметров модуля ThreatSense» 12.

4.1.1.1.3 Исключения из сканирования

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

- **«Путь»**: путь к исключаемым файлам и папкам.
- **«Угроза»**: если рядом с исключаемым файлом указано имя угрозы, файл не сканируется только на предмет этой угрозы, а не всегда. Если файл окажется заражен другой вредоносной программой, модуль защиты от вирусов ее обнаружит.

- **«Добавить»**: команда, исключающая объекты из сканирования. Введите путь к объекту (допускается использование знаков подстановки * и ?) либо выберите файл или папку в древовидной структуре.
- **«Изменить...»**: команда, изменяющая выделенные записи.
- **«Удалить»**: команда, удаляющая выделенные записи.
- **«По умолчанию»**: команда, отменяющая все исключения.

4.1.1.2 Изменение параметров защиты в режиме реального времени

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

После установки ESET NOD32 Antivirus все параметры оптимизированы для максимальной защиты системы. Чтобы восстановить параметры по умолчанию, нажмите кнопку **«По умолчанию»** в левом нижнем углу окна **«Защита в режиме реального времени»** (диалоговое окно **«Настройка»** > **«Ввести настройки приложения...»** > **«Защита»** > **«Защита в режиме реального времени»**).

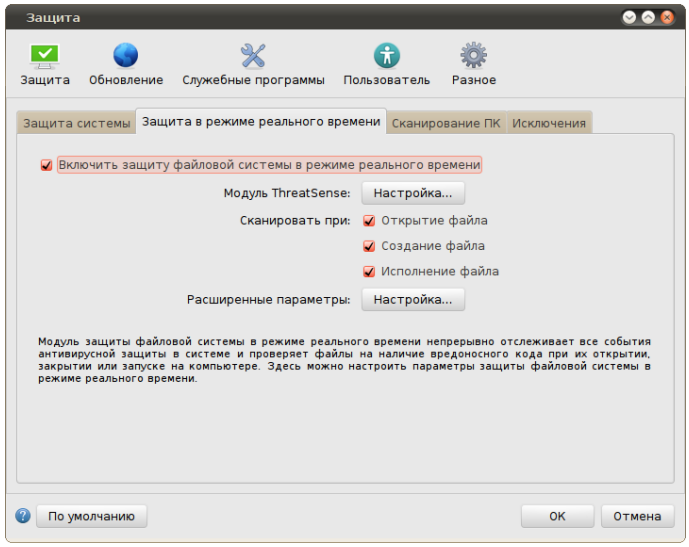
4.1.1.3 Проверка защиты в режиме реального времени

Чтобы проверить работоспособность и эффективность защиты в режиме реального времени, воспользуйтесь тестовым файлом eicar.com. Это специальный безвредный файл, обнаруживаемый всеми антивирусными программами. Он создан институтом EICAR (Европейский институт антивирусных компьютерных исследований) для тестирования функциональности антивирусных программ.

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

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

Защита в режиме реального времени отключена
Если защита в режиме реального времени была случайно отключена пользователем, ее нужно включить. Чтобы включить защиту в режиме реального времени, перейдите на страницу **«Настройка»** > **«Защита от вирусов и шпионских программ»** и щелкните ссылку **«Включить защиту в режиме реального времени»** справа в главном окне приложения. Кроме того, защиту в режиме реального времени можно включить в диалоговом окне расширенной настройки в разделе **«Защита»** > **«Защита в режиме реального времени»**, выбрав параметр **«Включить защиту в режиме реального времени»**.



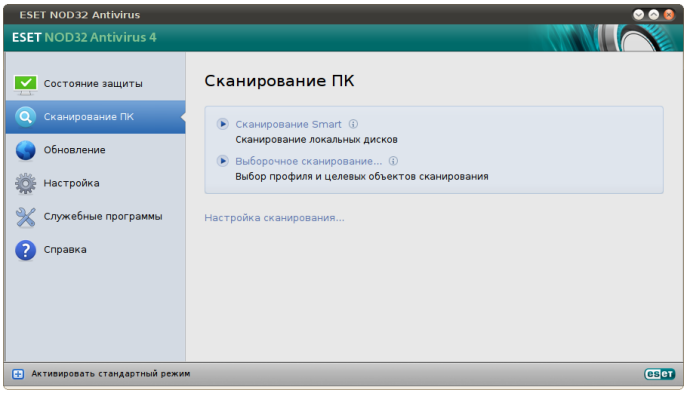
Функция защиты в режиме реального времени не обнаруживает вирусы
Убедитесь, что на компьютере не установлено другое антивирусное приложение. При одновременной работе двух систем защиты от вирусов в режиме реального времени могут возникать конфликты. Рекомендуется удалить все другие антивирусные приложения.

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

4.1.2 Сканирование ПК по требованию

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

Рекомендуется запускать сканирование компьютера по требованию хотя бы раз в месяц. Можно настроить сканирование так, чтобы оно запускалось по расписанию (**«Служебные программы»** > **«Планировщик»**).



4.1.2.1 Тип сканирования

Доступны два типа сканирования компьютера по требованию. Тип **«Сканирование Smart»** позволяет быстро проверить систему без настройки каких-либо параметров. Тип **«Выборочное сканирование»** позволяет выбрать предопределенный профиль сканирования и указать объекты, которые нужно проверить.

4.1.2.1.1 Сканирование Smart

Режим сканирования Smart позволяет быстро запустить сканирование компьютера и очистить зараженные файлы без вмешательства пользователя. Главным преимуществом этого метода является простота использования без детальной настройки параметров сканирования. Функция сканирования Smart проверяет все файлы во всех папках и автоматически очищает или удаляет обнаруженные вирусы. При этом автоматически используется уровень очистки по умолчанию. Дополнительную информацию о типах очистки см. в разделе «Очистка» 13.

4.1.2.1.2 Выборочное сканирование

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

Чтобы указать объекты сканирования, выберите пункт **«Сканирование компьютера»** > **«Выборочное сканирование»** и отметьте нужные **объекты сканирования** в древовидной структуре. Объекты сканирования можно также определить более точно. Для этого укажите пути к папкам и файлам, подлежащим сканированию. Если требуется только просканировать систему без выполнения дополнительных действий по ее очистке, выберите параметр **«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.

4.1.2.2 Объекты сканирования

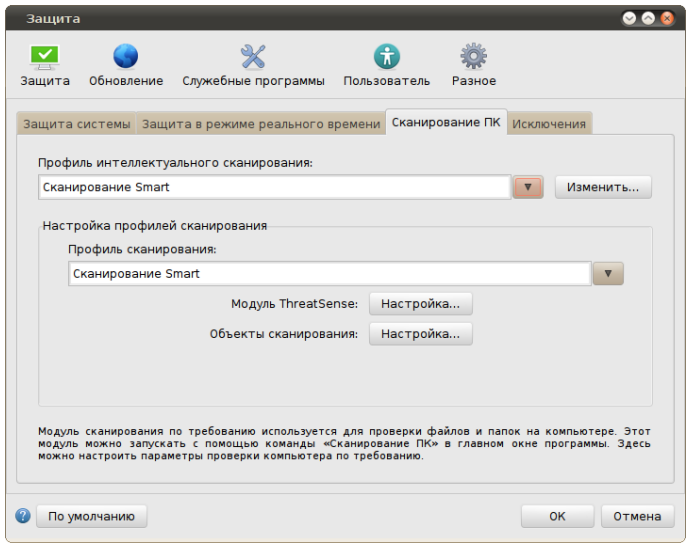
Дерево объектов сканирования позволяет выбрать файлы и папки, которые необходимо проверить на наличие вирусов. Выбор папок может также осуществляться в соответствии с параметрами профиля.

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

4.1.2.3 Профили сканирования

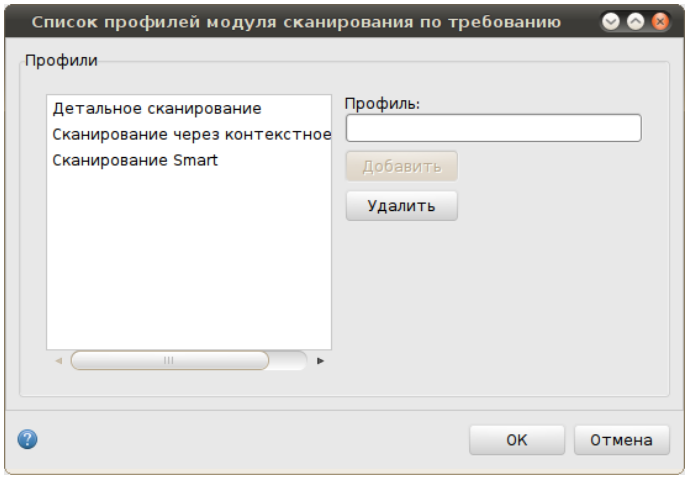
Предпочтительные настройки сканирования можно сохранить для использования в будущем. Рекомендуется создать отдельный профиль для каждого регулярно используемого набора параметров (с различными объектами и методами сканирования и т. д.).

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



Информацию о создании профиля, соответствующего конкретным требованиям, и описание каждого параметра сканирования см. в разделе «Настройка параметров модуля ThreatSense» 12.

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



4.1.3 Настройка параметров модуля ThreatSense

ThreatSense — это технология, объединяющая ряд способов обнаружения угроз. Она является проактивной, т. е. защищает даже от новых угроз. При этом используется сочетание методов (анализ кода, моделирование кода, обобщенные сигнатуры, сигнатуры вирусов), которое значительно повышает уровень безопасности компьютера. Модуль сканирования может контролировать несколько потоков данных одновременно, что повышает эффективность обнаружения угроз. Кроме того, технология ThreatSense эффективна против руткитов.

Технология ThreatSense позволяет настроить несколько параметров сканирования:

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

Чтобы открыть окно настройки, выберите пункт **«Настройка»** > **«Защита от вирусов и шпионских программ»** > **«Расширенная настройка параметров защиты от вирусов и шпионских программ»** и нажмите кнопку **«Настройка...»** в разделах **«Защита системы»**, **«Защита в режиме реального времени»** и **«Сканирование компьютера»**, в которых применяется технология ThreatSense (см. ниже). Разные сценарии обеспечения безопасности требуют различных настроек, поэтому технологию ThreatSense можно настроить отдельно для каждого из следующих модулей защиты:

- **«Защита системы»** > «Автоматическая проверка файлов, исполняемых при запуске системы»;
- **«Защита в реальном времени»** > «Защита в режиме реального времени»;
- **«Сканирование компьютера»** > «Сканирование компьютера по требованию».

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

4.1.3.1 Объекты

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

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

4.1.3.2 Параметры

В разделе **«Параметры»** можно выбрать методы, которые будут использоваться при сканировании системы на предмет заражения. Доступны следующие варианты:

- **«База данных сигнатур вирусов»**: сигнатуры вирусов позволяют точно и надежно обнаруживать и идентифицировать заражения по имени.
- **«Эвристический анализ»**: эвристические алгоритмы анализируют активность программ на предмет вредоносных действий. Основным преимуществом эвристического анализа является возможность обнаруживать новое вредоносное программное обеспечение, сведения о котором еще не попали в базу данных сигнатур вирусов.
- **«Расширенная эвристика»**: этот метод основан на уникальном эвристическом алгоритме, разработанном компанией ESET и оптимизированном для обнаружения компьютерных червей и «троянских коней», написанных на языках программирования высокого уровня. Применение расширенной эвристики существенно улучшает возможности обнаружения вредоносных программ.

- **«Рекламное/шпионское/опасное ПО»**: эта категория включает программы, собирающие важную информацию о пользователях без их согласия. Кроме того, к ней относятся программы, показывающие рекламу.
- **«Потенциально нежелательное ПО»**: не все потенциально нежелательные приложения являются вредоносными, однако они могут тем или иным образом снижать производительность системы. Такие приложения обычно запрашивают при установке согласие пользователя. После их установки работа системы изменяется. Наиболее заметны такие изменения, как появление нежелательных всплывающих окон, запуск скрытых процессов, увеличение степени использования системных ресурсов, изменение результатов поисковых запросов и обмен данными с удаленными серверами.
- **«Потенциально опасное ПО»**: в эту категорию входят коммерческие законные приложения, которыми могут воспользоваться злоумышленники, если такие приложения были установлены без ведома пользователя. Это в том числе средства удаленного доступа. По умолчанию этот параметр отключен.

4.1.3.3 Очистка

Параметры очистки определяют способ очистки зараженных файлов модулем сканирования. Есть три уровня очистки, указанных ниже.

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

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

4.1.3.4 Расширения

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, которые не нужно сканировать.

По умолчанию сканируются все файлы независимо от их расширения. Любое расширение можно добавить в список исключений из сканирования. С помощью кнопок **«Добавить»** и **«Удалить»** можно изменять содержимое списка, отключая или включая сканирование для тех или иных расширений.

Исключение файлов из сканирования может потребоваться, если сканирование файлов некоторых типов мешает нормальной работе программы, которая их использует. Например, иногда целесообразно исключить из сканирования файлы с расширениями *.log*, *.cfg* и *.tmp*.

4.1.3.5 Ограничения

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

- **Максимальный размер:**: определяет максимальный размер сканируемых объектов. После установки этого ограничения модуль защиты от вирусов будет проверять только объекты меньше указанного размера. Не рекомендуется изменять значение этого параметра по умолчанию, если для этого нет особой причины. Он предназначен для опытных пользователей, которым необходимо исключить большие объекты из сканирования.
- **Максимальное время сканирования:**: определяет максимальное время сканирования объекта. Если пользователь определил это значение, модуль защиты от вирусов прерывает сканирование текущего объекта по истечении указанного интервала времени независимо от того, завершено ли оно.
- **Максимальный уровень вложенности:**: определяет максимальную глубину сканирования архивов. Не рекомендуется изменять значение этого параметра по умолчанию, равное 10; в обычных условиях для этого нет особой причины. Если сканирование преждевременно прерывается из-за превышения уровня вложенности, архив остается непроверенным.
- **Максимальный размер файла:**: определяет максимальный размер файлов в архиве (после извлечения), подлежащих сканированию. Если из-за этого ограничения сканирование прерывается до его завершения, архив остается непроверенным.

Если нужно отключить сканирование управляемых системой папок (*/proc* и */sys*), установите флажок **«Исключить из сканирования системные папки»** (этот параметр недоступен для сканирования файлов, исполняемых при запуске системы).

4.1.3.6 Другие

При включенном параметре «Оптимизация Smart» используются оптимальные настройки для обеспечения самого эффективного уровня сканирования с сохранением его высокой скорости. Разные модули защиты выполняют интеллектуальное сканирование, применяя отдельные методы для различных типов файлов. Оптимизация Smart не определена в продукте жестким образом. Коллектив разработчиков компании ESET постоянно вносит в нее изменения, которые можно интегрировать в ESET NOD32 Antivirus с помощью регулярных обновлений. Если оптимизация Smart отключена, при сканировании

используются только пользовательские настройки ядра ThreatSense каждого модуля.

«Сканировать альтернативные потоки данных»: применимо только к модулю сканирования по требованию.
Альтернативные потоки данных используемые файловой системой — это связи файлов и папок, недоступные для обычных методик сканирования. Многие вредоносные программы выдают себя за альтернативные потоки данных, чтобы не быть обнаруженными.

«Сохранить отметку о времени последнего доступа»: применимо только к модулю сканирования по требованию.
Используйте этот параметр для сохранения исходного времени доступа к сканируемым файлам без его обновления (например, для использования с системами резервного копирования данных).

4.1.4 Действия при выявлении заражения

Вредоносный код может быть получен из разных источников: с веб-страниц, из общих папок, по электронной почте или со сменных носителей (USB-накопителей, внешних дисков, компакт- или DVD-дисков, дискет и т. п.).

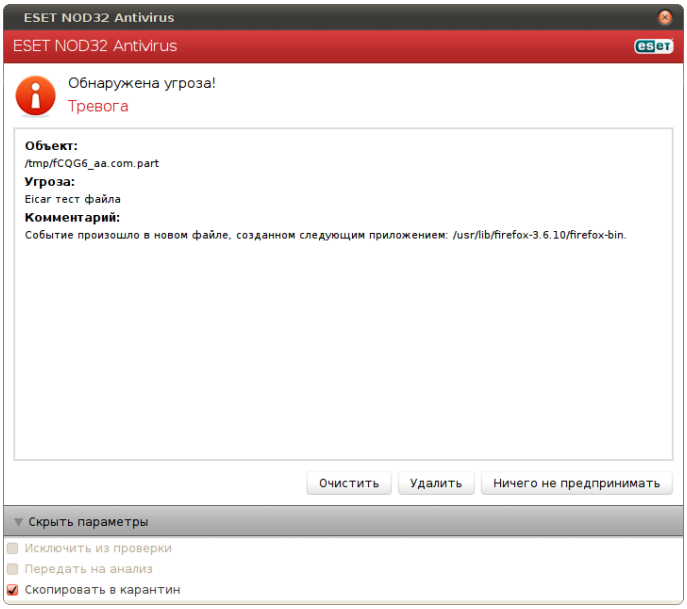
Если наблюдаются признаки заражения компьютера (например, он стал медленнее работать, часто «зависает» и т. п.), рекомендуется выполнить действия, описанные ниже.

1. Откройте ESET NOD32 Antivirus и выберите команду **«Сканирование компьютера»**.
2. Выберите параметр **«Сканирование Smart»** (дополнительную информацию см. в разделе «Сканирование Smart» 11).
3. По завершении сканирования просмотрите в журнале количество проверенных, зараженных и очищенных файлов.

Если необходимо проверить только часть диска, выберите параметр **«Выборочное сканирование»** и укажите объекты, которые нужно проверить.

Ниже описано, что происходит, когда система ESET NOD32 Antivirus выявляет заражение. Предположим, что заражение обнаружено модулем защиты файловой системы в режиме реального времени при уровне очистки по умолчанию. Сначала модуль пытается очистить или удалить файл. Если действие по умолчанию для модуля защиты в режиме реального времени не определено, его предлагается выбрать пользователю. Обычно можно выбрать действие **«Очистить»**, **«Удалить»** или **«Ничего не предпринимать»**. Действие **«Ничего не предпринимать»** выбирать не рекомендуется, так как в этом случае зараженный файл останется на компьютере. Исключением может быть ситуация, когда имеется полная уверенность в том, что файл безвреден и попал под подозрение по ошибке.

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



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

4.2 Обновление приложения

Для обеспечения максимального уровня безопасности необходимо регулярно обновлять приложение ESET NOD32 Antivirus. Модуль обновления поддерживает актуальное состояние приложения, обновляя базу данных сигнатур вирусов.

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

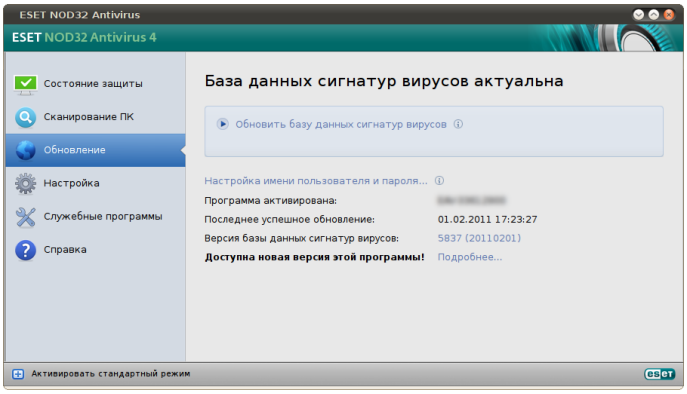
В обычной ситуации после нормального завершения загрузки в окне обновления выводится сообщение **«База данных сигнатур вирусов актуальна»**. Если обновить базу данных сигнатур вирусов невозможно, рекомендуется проверить настройки обновления 15, так как самая распространенная причина этой ошибки — неверно введенные данные для аутентификации (имя пользователя и пароль) или некорректно выбранные параметры подключения 21.

В окне обновления также выводятся сведения о версии базы данных сигнатур вирусов. Числовой индикатор представляет собой активную ссылку на список всех сигнатур, добавленных в базу данных в текущем обновлении, на веб-сайте компании ESET.

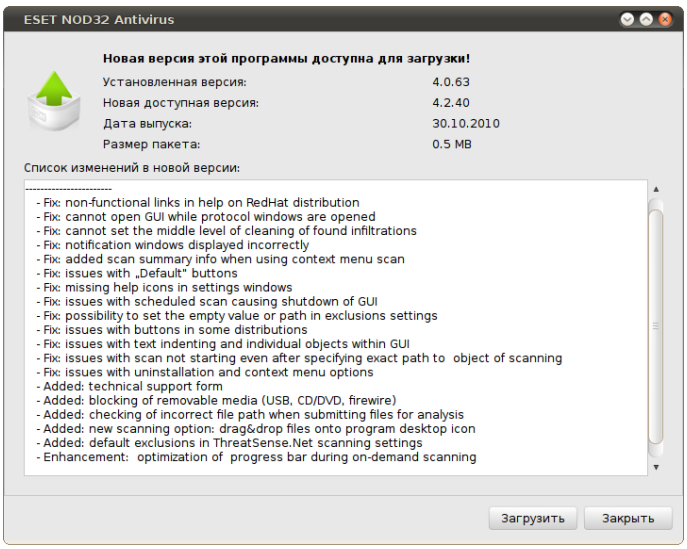
ПРИМЕЧАНИЕ. Имя пользователя и пароль предоставляются компанией ESET после приобретения приложения ESET NOD32 Antivirus.

4.2.1 Обновление до новой сборки

Для обеспечения максимальной защиты важно использовать новейшую сборку ESET NOD32 Antivirus. Чтобы проверить наличие новой версии, выберите пункт **«Обновление»** из главного меню в левой части окна. Если доступна новая сборка, в нижней части окна будет выведено сообщение *«Доступна новая версия этой программы!»*. Нажмите **«Подробнее...»**, чтобы вывести на экран новое окно с информацией о номере версии доступной сборки и перечнем изменений.



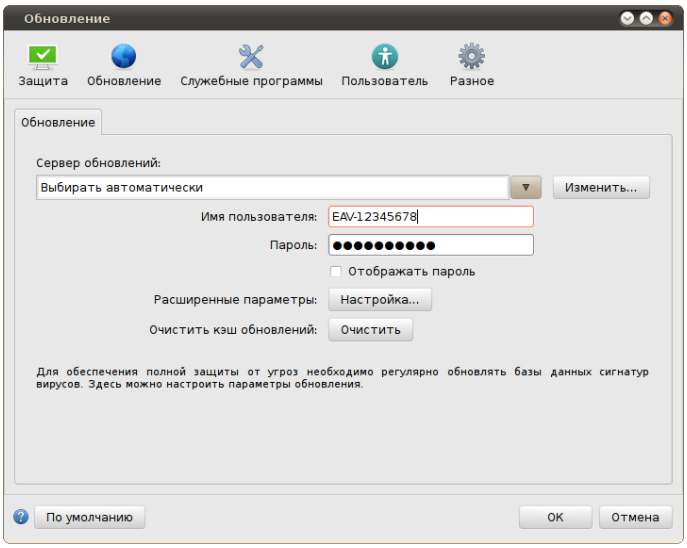
Нажмите кнопку **«Загрузить»**, чтобы загрузить новейшую сборку. Нажмите кнопку **«Закрыть»**, чтобы закрыть это окно и загрузить обновление позднее.



Если нажать кнопку **«Загрузить»**, файл будет загружен в папку загрузок (или в выбранную в браузере папку по умолчанию). Когда файл будет загружен, запустите его и следуйте указаниям по установке. Ваши имя пользователя и пароль будут автоматически перенесены в новую установленную версию. Рекомендуется регулярно проверять наличие обновлений, особенно при выполнении установки ESET NOD32 Antivirus с компакт- или DVD-диска.

4.2.2 Настройка обновления

Раздел параметров обновления содержит информацию об источниках обновлений, такую как адреса серверов обновлений и данные аутентификации для них. По умолчанию в раскрывающемся меню **«Сервер обновлений»** выбран параметр **«Выбирать автоматически»**, обеспечивающий автоматическую загрузку файлов обновлений с сервера ESET с минимальным расходом трафика.



Список доступных серверов обновлений можно просмотреть с помощью раскрывающегося меню **«Сервер обновлений»**. Чтобы добавить в список новый сервер, нажмите кнопку **«Изменить»**. Затем введите адрес сервера в поле **«Сервер обновлений»** и нажмите кнопку **«Добавить»**. Для аутентификации при входе на серверы обновлений используйте **имя пользователя** и **пароль**, полученные после покупки приложения.

Чтобы включить тестовый режим (для загрузки тестовых обновлений), нажмите кнопку **«Настройка»** рядом с **расширенными параметрами** и установите флажок **«Включить тестовые обновления»**. Чтобы отключить отображение уведомлений на панели задач после каждого успешно выполненного обновления, установите флажок **«Не отображать уведомление об успешном обновлении»**.

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

4.2.3 Создание задач обновления

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

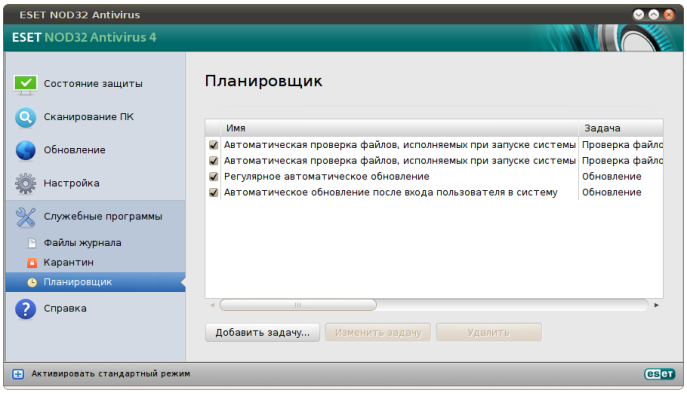
Кроме того, обновление можно выполнять как запланированную задачу. Чтобы настроить запланированную задачу, перейдите в раздел **«Служебные программы»** > **«Планировщик»**. По умолчанию в ESET NOD32 Antivirus активированы указанные ниже задачи.

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

Каждую из указанных выше задач 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» 16.

4.3 Планировщик

Планировщик доступен, если в ESET NOD32 Antivirus активирован расширенный режим. Перейти к планировщику можно через главное меню ESET NOD32 Antivirus, воспользовавшись пунктом **«Служебные программы»**. **Планировщик** содержит полный список всех запланированных задач и их параметры запуска (дату, время и используемый профиль сканирования).



По умолчанию в планировщике отображаются следующие запланированные задачи:

- Регулярное автоматическое обновление
- Автоматическое обновление после входа пользователя в систему
- «Автоматическая проверка файлов, исполняемых при запуске системы»;
- «Автоматическая проверка файлов после обновления базы данных сигнатур вирусов»;
- «Обслуживание журналов» (после установки флажка **«Показывать системные задачи»** при настройке планировщика).

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

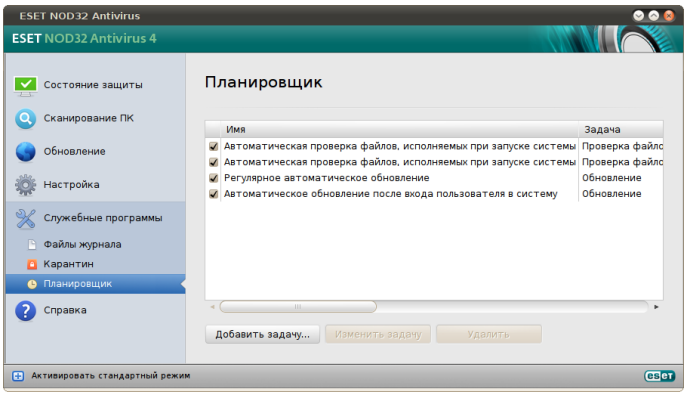
4.3.1 Назначение запланированных задач

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

4.3.2 Создание задачи

Чтобы создать задачу в планировщике, нажмите кнопку **«Добавить задачу...»** или щелкните правой кнопкой мыши и выберите в контекстном меню команду **«Добавить»**. Доступны пять типов запланированных задач. Они указаны ниже.

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



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

В раскрывающемся меню **«Запланированная задача»** выберите пункт **«Обновление»**. Введите имя задачи в поле **«Название задачи»**. Укажите частоту выполнения задачи в раскрывающемся меню **«Выполнить задачу»**. Доступны следующие варианты: **«Определяется пользователем»**, **«Однократно»**, **«Регулярно»**, **«Ежедневно»**, **«Еженедельно»** и **«При наступлении события»**. В зависимости от указанной частоты запуска будут запрошены различные параметры обновления. Затем укажите, какое действие следует предпринимать, если задача не будет выполнена в установленное время. Доступны указанные ниже варианты.

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

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

Новая задача появится в списке запланированных.

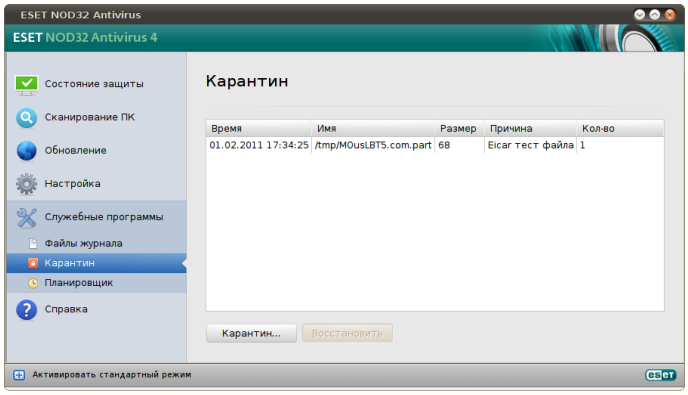
По умолчанию система включает запланированные задачи, которые обеспечивают правильную работу приложения. Изменить эти задачи нельзя, и по умолчанию они скрыты. Чтобы сделать эти задачи видимыми, выберите по очереди пункты **«Настройка»** > **«Ввести настройки**

приложения...» > **«Служебные программы»** > **«Планировщик»** и установите флажок **«Показывать системные задачи»**.

4.4 Карантин

Главное назначение карантина состоит в изоляции и безопасном хранении зараженных файлов. Файлы следует помещать на карантин, если они не могут быть излечены или безопасно удалены, если удалять их не рекомендуется или если они ошибочно отнесены приложением ESET NOD32 Antivirus к зараженным.

Поместить на карантин можно любой файл. Рекомендуется помещать на карантин файлы с подозрительной активностью, которые, тем не менее, не определяются модулем сканирования как зараженные. Файлы на карантине можно предоставить в лабораторию ESET для дальнейшего анализа.



Информацию о файлах, помещенных на карантин, можно просмотреть в виде таблицы, содержащей дату и время помещения файла на карантин, путь к его исходному расположению, его размер в байтах, причину помещения файла на карантин (например, мнение пользователя) и количество обнаруженных угроз (например, если архив содержит несколько вирусов). Папка карантина с изолированными файлами (*/var/opt/eset/esets/cache/quarantine*) остается в системе даже после удаления приложения ESET NOD32 Antivirus. В папке карантина файлы хранятся в безопасном зашифрованном виде. Их можно восстановить после повторной установки приложения ESET NOD32 Antivirus.

Если нужно автоматически сканировать помещенные в папку карантина файлы после каждого обновления базы данных сигнатур вирусов, установите флажок **«Повторно сканировать файлы в папке карантина после обновлений»** в разделе **«Настройка»** > **«Ввести настройки приложения...»** > **«Служебные программы»** > **«Карантин»** .

4.4.1 Помещение файлов на карантин

Приложение ESET NOD32 Antivirus автоматически помещает удаленные файлы на карантин (если эта функция не была отключена пользователем в окне предупреждения). При желании любой подозрительный файл можно поместить на карантин вручную с помощью кнопки **«Карантин»**. Для этого также можно использовать контекстное меню. Щелкните правой кнопкой мыши в окне **карантина**, выберите файл, который нужно поместить на карантин, и нажмите кнопку **«Открыть»**.

4.4.2 Восстановление из карантина

Файлы, находящиеся на карантине, можно восстановить в исходном месте. Для этого воспользуйтесь кнопкой **«Восстановить»**; кроме того, восстановить файл можно с помощью его контекстного меню в окне **«Карантин»**. Контекстное меню содержит также функцию **«Восстановить в...»**, которая позволяет восстановить файл в месте, отличном от исходного.

4.4.3 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 лабораторию ESET. Чтобы отправить файл из карантина, щелкните его правой кнопкой мыши и выберите пункт **«Предоставить файл для анализа»**.

4.5 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 NOD32 Antivirus .

Получить доступ к файлам журнала можно из главного окна ESET NOD32 Antivirus с помощью команды **«Служебные программы»** > **«Файлы журнала»**. Выберите нужный тип журнала в раскрывающемся меню **«Журнал»** в верхней части окна. Доступны указанные ниже журналы.

1. **«Обнаруженные угрозы»**: позволяет просмотреть все данные о событиях, имеющих отношение к обнаружению заражений.
2. **«События»**: этот журнал упрощает устранение проблем. В нем регистрируются все важные действия, выполняемые приложением ESET NOD32 Antivirus.
3. **«Сканирование компьютера»**: в этом окне отображаются результаты всех выполненных операций сканирования. Чтобы получить подробную информацию о той или иной операции сканирования по требованию, дважды щелкните соответствующую запись.

Чтобы скопировать в буфер обмена информацию из любого раздела журнала, выделите необходимую запись и нажмите кнопку **«Копировать»**.

4.5.1 Обслуживание журнала

Конфигурация журнала ESET NOD32 Antivirus доступна из главного окна приложения. Нажмите **Настройка** > **Ввести настройки приложения...** > **Служебные программы** > **Файлы журнала**. Для файлов журнала можно задать параметры, указанные ниже.

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

Чтобы настроить **фильтр записей журналов, заданный по умолчанию**, нажмите кнопку **«Изменить»** и выберите нужные типы журналов.

4.5.2 Фильтрация журнала

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

Ниже указаны типы журналов, используемые чаще всего.

- **«Критические предупреждения»**: в эти журналы записываются критические системные ошибки (например, сбой запуска модуля защиты от вирусов).
- **«Ошибки»**: в эти журналы записываются ошибки типа *«Не удалось загрузит ь файл»* и критические ошибки.
- **«Предупреждения»**: в эти журналы записываются сообщения с предупреждениями.
- **«Информационные записи»**: в эти журналы записываются информационные сообщения, в том числе сообщения о выполненных обновлениях, предупреждения и т. д.
- **«Диагностические записи»**: в эти журналы записываются данные, необходимые для точной настройки программы, а также все описанные выше записи.
- **«Все фильтры»**: этот флажок позволяет выбрать указанные выше типы журналов или отменить их выбор.

4.6 Интерфейс пользователя

Параметры интерфейса пользователя ESET NOD32 Antivirus позволяют настроить рабочую среду в соответствии с конкретными требованиями. Эти параметры конфигурации доступны в разделе **«Настройка»** > **«Ввести настройки приложения...»** > **«Пользователь»** > **«Интерфейс»**.

В этом разделе можно переключиться в расширенный режим, в котором отображаются более детальные настройки и дополнительные элементы управления ESET NOD32 Antivirus.

Чтобы включить заставку, которая отображается при запуске, установите флажок **«Показывать заставку при запуске»**.

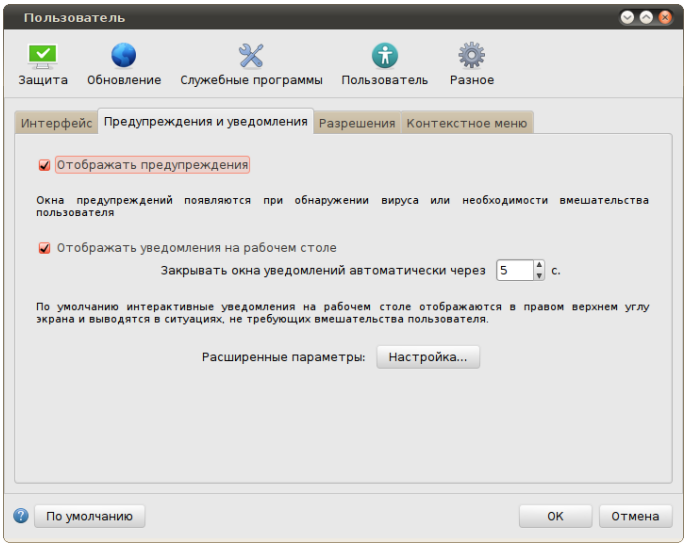
В разделе **«Использовать обычное меню»** можно установить флажки **«В стандартном режиме»** и **«В расширенном режиме»**, чтобы включить использование стандартного меню в главном окне программы в соответствующем режиме.

Чтобы включить вывод подсказок, задайте параметр **«Показывать подсказки»**. Параметр **«Показывать скрытые файлы»** позволяет просматривать и выбирать скрытые файлы при настройке **объектов сканирования**.

4.6.1 Предупреждения и уведомления

Раздел **«Предупреждения и уведомления»** позволяет настроить обработку системных уведомлений и предупреждений об угрозах в приложении ESET NOD32 Antivirus.

Если снять флажок **«Отображать предупреждения»**, предупреждения выводиться не будут, поэтому делать это без особых причин не рекомендуется. В большинстве случаев лучше оставить этот параметр без изменений (включен).



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

4.6.1.1 Расширенная настройка предупреждений и уведомлений

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

Отображать уведомления только в случае необходимости вмешательства пользователя при выполнении приложений в полноэкранном режиме
Этот параметр полезен при проведении презентаций, при играх и выполнении других программ, использующих весь экран.

4.6.2 Права

Настройки ESET NOD32 Antivirus могут иметь большое значение для политики безопасности организации. Несанкционированное изменение параметров может нарушить стабильность работы системы и ослабить ее защиту. Поэтому можно выбрать пользователей, которым разрешено изменять конфигурацию приложения.

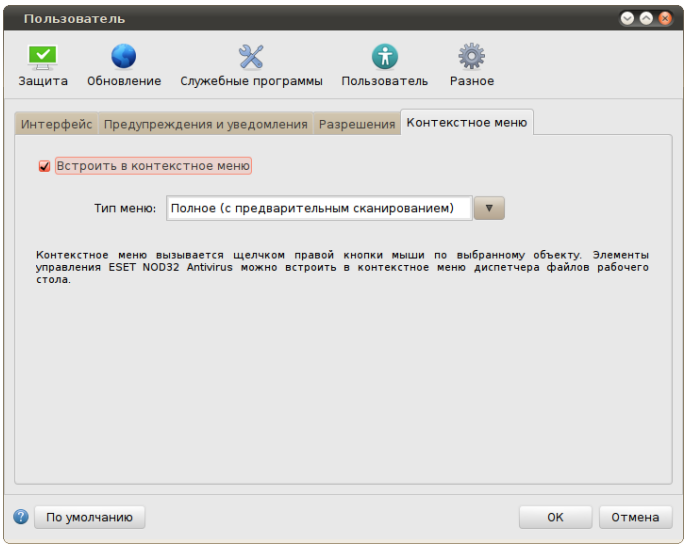
Чтобы указать пользователей с правами, воспользуйтесь пунктом меню **«Настройка»** > **«Ввести настройки приложения...»** > **«Пользователь»** > **«Разрешения»**.

Для обеспечения максимальной безопасности системы необходимо правильно настроить приложение ESET Smart Security. Несанкционированное изменение параметров может привести к потере важных данных. Для составления списка пользователей с правами выберите их в списке **«Пользователи»** в левой части окна и нажмите кнопку **«Добавить»**. Чтобы удалить пользователя, выберите его в списке пользователей с правами в правой части окна и нажмите кнопку **«Удалить»**.

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

4.6.3 Контекстное меню

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



ПРИМЕЧАНИЕ. Для включения интеграции элементов в контекстное меню необходимо расширение функций Nautilus.

4.7 Система быстрого оповещения ThreatSense.Net

Система быстрого оповещения ThreatSense.Net оперативно уведомляет компанию ESET о новых угрозах. Она является двунаправленной и имеет целью повышение надежности защиты компьютера пользователя. Лучшим способом обнаружения новых угроз сразу после их появления является сбор информации от как можно большего числа пользователей. При этом возможны два варианта, указанных ниже.

1. Можно отключить систему быстрого оповещения ThreatSense.Net. Функциональность приложения при этом не ограничивается, и пользователь все равно получает наилучшую защиту.
2. Можно разрешить системе быстрого оповещения передавать анонимную информацию о новых угрозах и опасном коде. В этом случае соответствующий файл передается в лабораторию ESET для тщательного анализа. Исследование этих угроз помогает компании ESET обновлять базу данных угроз и улучшать средства их обнаружения.

Система быстрого оповещения ThreatSense.Net собирает также информацию о компьютерах пользователей, которая может иметь отношение к недавно появившимся угрозам. Она может включать образец кода или копию файла, в котором была обнаружена угроза, путь к файлу, его имя, дату и время обнаружения угрозы, имя процесса, в котором она обнаружена, и версию операционной системы пользователя.

Поскольку в отправляемую информацию могут случайно попасть сведения о пользователе и его компьютере (например, имя пользователя в пути к файлу), компания ESET заверяет, что они не будут использованы ни в каких иных целях, кроме как для раннего выявления и устранения новых угроз.

Параметры системы быстрого оповещения ThreatSense.Net доступны в окне расширенных настроек в разделе **«Служебные программы»** > **«ThreatSense.Net»**. Установите флажок **«Включить систему быстрого оповещения ThreatSense.Net»** и нажмите кнопку **«Настройка»** рядом с надписью «Расширенные параметры».

4.7.1 Подозрительные файлы

Параметр «Подозрительные файлы» позволяет настроить способ передачи вредоносного кода в лабораторию ESET для анализа.

При обнаружении подозрительного файла его можно отправить в лабораторию ESET. Если это вредоносное приложение, информация о нем будет включена в следующую версию базы данных сигнатур вирусов.

«Передача подозрительных файлов»: файлы можно отправить в лабораторию ESET **в процессе обновления**. Кроме того, их можно отправлять **по мере возможности**; этот параметр следует выбрать при постоянном подключении к Интернету.

Если вы не хотите отправлять файлы для анализа, установите флажок **«Не передавать»**. Если выбрать этот параметр, статистическая информация все равно будет отправляться (эта функция настраивается в другом месте).

Система быстрого оповещения ThreatSense.Net собирает анонимную информацию о компьютерах пользователей, которая может иметь отношение к недавно появившимся угрозам. Она может включать имя вредоносной программы, дату и время ее обнаружения, версию приложения ESET, версию операционной системы компьютера и информацию о его расположении. Обычно статистика отправляется на серверы ESET один или два раза в день.

Пример отправляемого пакета со статистикой:

```
# utc_time=2009-04-14 07:21:28
# country="Russia"
# language="ENGLISH"
# osver=2.6.18-128.e5
# engine=5417
# components=2.50.2
# moduleid=0x4e4f4d41
# filesize=28368
# filename=/home/user/Documents/Incoming/rdgFR1463
[1].zip
```

«Передача анонимной статистической информации»: этот параметр позволяет определить условия передачи статистической информации. Если выбрать вариант **«По мере возможности»**, статистическая информация будет отправляться сразу после сбора. Этот параметр подходит для систем с постоянным подключением к Интернету. Если выбрать вариант **«В процессе обновления»**, вся статистическая информация будет отправляться во время обновления после ее сбора.

Чтобы отключить отправку анонимной статистической информации, установите флажок **«Не передавать»**.

«Фильтр исключения»: этот вариант позволяет исключить из передачи определенные файлы или папки. Например, это можно сделать для файлов, содержащих конфиденциальную информацию (документы или электронные таблицы). Файлы наиболее распространенных типов (*.doc* и т. д.) по умолчанию не отправляются. Можно добавить их в список исключений.

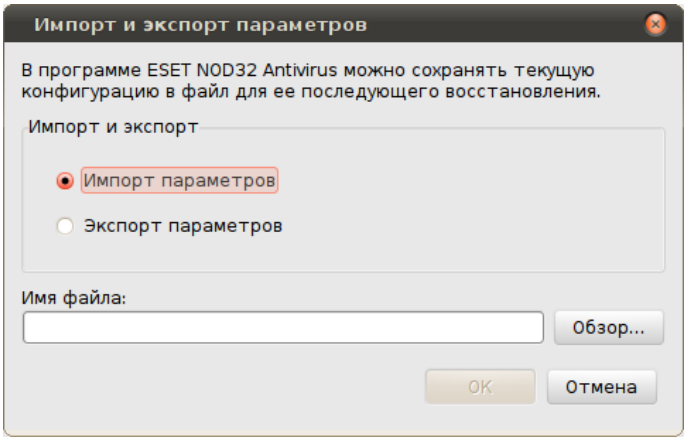
«Адрес электронной почты (необязательно)»: можно отправить адрес электронной почты вместе с подозрительными файлами, чтобы специалисты ESET могли связаться с вами, если им для анализа потребуется дополнительная информация. Имейте в виду, что компания ESET не связывается с пользователями без необходимости.

5. Для опытных пользователей

5.1 Импорт и экспорт параметров

Импорт или экспорт конфигурации ESET NOD32 Antivirus можно выполнить в расширенном режиме в разделе **«Настройка»**.

Для хранения конфигурации при импорте и экспорте используются файлы архивов. Импорт и экспорт полезны, если необходимо создать резервную копию текущей конфигурации ESET NOD32 Antivirus. Экспорт параметров также полезен, если необходимо использовать выбранную конфигурацию ESET NOD32 Antivirus на нескольких системах, поскольку файл конфигурации можно легко импортировать для переноса нужных настроек.



5.1.1 Импорт параметров

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

5.1.2 Экспорт параметров

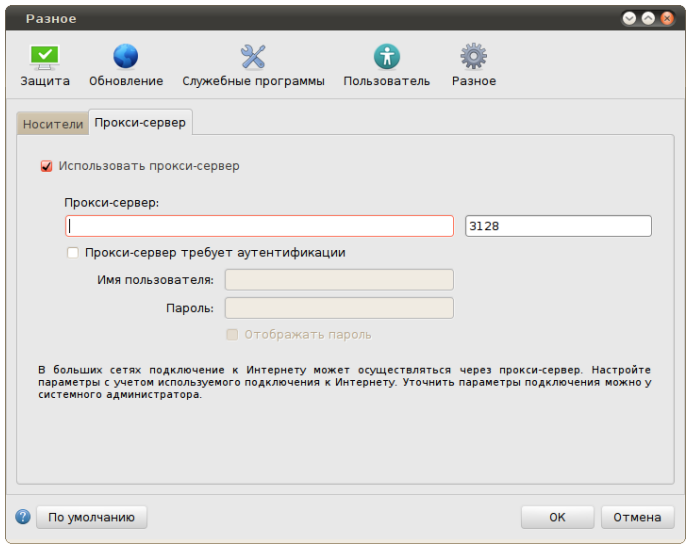
Процедура экспорта параметров похожа на их импорт. В главном меню выберите пункт **«Настройка»** > **«Импорт и экспорт параметров...»**. Выберите пункт **Экспортировать параметры** и введите имя файла конфигурации. Выберите место для сохранения файла.

5.2 Настройка прокси-сервера

Параметры прокси-сервера можно настроить в разделе **«Разное»** > **«Прокси-сервер»**. Эти параметры являются общими для всего приложения ESET NOD32 Antivirus. 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»** вместе с номером его порта.

Если требуется аутентификация на прокси-сервере, установите флажок **«Прокси-сервер требует аутентификации»**, а затем укажите **имя пользователя** и **пароль** в соответствующих полях.



5.3 Блокирование сменных носителей

Сменные носители (например, компакт-диски или USB-накопители) могут содержать вредоносный код и подвергать компьютер риску. Чтобы заблокировать их, установите флажок **«Включить блокирование сменных носителей»**. Чтобы разрешить доступ к носителям определенного типа, снимите соответствующие флажки.

6. Глоссарий

6.1 Типы заражений

Заражение представляет собой попытку проникновения вредоносного программного обеспечения на компьютер пользователя и (или) причинения ему вреда.

6.1.1 Вирусы

Компьютерные вирусы портят файлы на компьютере. Их назвали так из-за сходства с биологическими вирусами, так как они используют похожие способы для распространения с компьютера на компьютер.

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

Компьютерные вирусы могут различаться по принципам работы и степени опасности. Некоторые из вирусов особо опасны, так как могут удалять файлы с компьютера. С другой стороны, некоторые вирусы не причиняют никакого вреда. Они просто досаждают пользователю, демонстрируя возможности своих авторов.

Важно отметить, что вирусы постепенно становятся все более редкими по сравнению с троянскими или шпионскими программами, так как разрабатывать их экономически невыгодно для авторов. Кроме того, термин «вирус» часто неправильно используют для описания других типов заражений. Он постепенно выходит из употребления, и на смену ему приходит более точный термин «вредоносное программное обеспечение».

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

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

6.1.2 Черви

Компьютерные черви — это вредоносные программы, которые атакуют компьютеры, распространяясь по сети. Основное различие между вирусами и червями заключается в том, что черви могут воспроизводиться и распространяться самостоятельно — они не зависят от зараженных файлов или загрузочных секторов. Черви распространяются, используя адресную книгу пользователя или уязвимости сетевых приложений.

Черви намного более жизнеспособны, чем компьютерные вирусы. Благодаря Интернету они могут распространиться по всему земному шару за считанные часы после запуска в сеть. В некоторых случаях счет идет даже на минуты. Из-за этой способности к быстрому и независимому распространению черви опаснее вредоносных программ других типов.

Работающий в системе червь может доставить много неудобств пользователю: он может удалять файлы, снижать производительность системы или мешать работе других программ. Кроме того, он может служить «транспортным средством» для вредоносного кода других типов.

Если компьютер заражен червем, рекомендуется удалить инфицированные файлы, поскольку они содержат вредоносный код.

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

6.1.3 Троянские программы

Исторически троянскими программами называют особую группу вредоносных программ, которые выдают себя за полезные, чтобы пользователи запускали их. Сегодня троянские программы не нуждаются в подобной маскировке. Единственная их цель — как можно проще проникнуть в систему и запустить вредоносный код. Троянскими программами стали называть широкий класс вредоносных программ, которые не получается отнести к какому-либо классу вирусов.

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

- Downloader (программа-загрузчик) — вредоносная программа, которая загружает другие вредоносные модули из Интернета.
- Dropper (программа-бомба) — тип троянских программ, разработанных для заражения компьютеров другими вредоносными программами.
- Backdoor (утилита удаленного администрирования) — приложение, которое обменивается данными со злоумышленниками, позволяя им получить доступ к системе и контроль над ней.
- Keylogger (клавиатурный шпион) — такие программы записывают все, что пользователь набирает на клавиатуре, и отправляют эту информацию злоумышленникам.
- Dialer (программа дозвона) — программы, которые пытаются набирать номера телефонов, звонки на которые оплачивает вызывающий абонент. При этом пользователю практически невозможно заметить, что создается новое подключение. Программы дозвона могут причинить вред только пользователям модемов. К счастью, модемы распространены не столь широко, как раньше.
- Как правило, троянские программы распространяются в виде исполняемых файлов. Если на компьютере будет обнаружен файл, относящийся к категории троянских программ, рекомендуется удалить его, так как он скорее всего содержит вредоносный код.

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

6.1.4 Рекламные программы

Рекламными программами называют программное обеспечение, распространение которого частично обеспечивается за счет рекламы. Программы, демонстрирующие пользователю рекламу, попадают в эту категорию. Частыми признаками работы рекламных программ являются появление всплывающих окон с рекламой в веб-браузере или изменение домашней страницы. Рекламные программы часто распространяются с бесплатными пакетами программного обеспечения. Это позволяет их создателям покрывать расходы на разработку полезных (как правило) программ.

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

Если принято решение использовать свободно распространяемый программный продукт, стоить уделить особое внимание программе установки. Чаще всего программа установки предупреждает о наличии рекламного ПО. При этом часто предлагается отказаться от его установки и установить необходимую программу без рекламного ПО.

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

6.1.5 Шпионские программы

К этой категории относятся программы, которые отправляют личные данные злоумышленнику без ведома и согласия их владельца. Они используют функции слежения для отправки статистической информации, такой как список посещаемых веб-сайтов, адреса электронной почты в адресных книгах 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 в том, что нет четкой границы между полезными и вредоносными приложениями, и никто не гарантирует, что собираемая информация не будет использована во вред. Данные, полученные шпионскими программами, могут содержать пароли пользователя, PIN-коды, номера счетов и т. д. Шпионские программы зачастую распространяются в комплекте со свободно распространяемыми программами самими авторами, чтобы возместить расходы на разработку или разрекламировать свое программное обеспечение. Часто пользователей информируют о наличии шпионских программ во время установки основной программы. При этом в платной версии программы этого программного обеспечения нет.

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 шпионского ПО. Утверждается, что они предназначены для борьбы со шпионским ПО, но на самом деле они сами являются таковым.

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

6.1.6 Потенциально опасное ПО

Существует множество программ, предназначенных для упрощения администрирования сетевых компьютеров. Однако злоумышленники могут использовать их для причинения вреда. Приложение ESET NOD32 Antivirus позволяет выявлять такие угрозы.

Коммерческие законные приложения могут быть классифицированы как потенциально опасное ПО. В эту категорию входят такие программы, как средства удаленного доступа, приложения для взлома паролей и клавиатурные шпионы (программы, записывающие нажатия клавиш на клавиатуре).

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

6.1.7 Потенциально нежелательное ПО

Не все приложения, относящиеся к потенциально нежелательному ПО, являются вредоносными, однако они могут тем или иным образом снижать производительность системы. Такие приложения обычно запрашивают при установке согласие пользователя. После их установки работа системы изменяется. Наиболее заметны следующие изменения:

- открываются новые окна, которые не появлялись ранее;
- активируются и выполняются скрытые процессы;
- повышается степень использования системных ресурсов;
- изменяются результаты поиска;
- приложение подключается к удаленным серверам.