

ESET NOD32 Antivirus 4

Руководство пользователя

(для продукта версии 4.2 и более поздних версий)

Microsoft® Windows® 7 / Vista / XP / NT4 / 2000 / 2003 / 2008



ESET NOD32 Antivirus 4

© ESET spol. s r.o., 2010. Все права защищены.

Антивирус ESET NOD32 разработан компанией ESET, spol. s r.o. Дополнительные сведения см. на веб-сайте компании по адресу www.eset.com.

Все права защищены. Запрещается воспроизведение, сохранение в информационных системах или передача данного документа или любой его части в любой форме и любыми средствами, в том числе электронными, механическими, с помощью фотокопирования, записи, сканирования, а также любыми другими способами без соответствующего письменного разрешения автора.

Компания ESET, spol. s r.o. оставляет за собой право изменять любые программные продукты, описанные в данной документации, без предварительного уведомления.

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

REV.20100225-008

Содержание

1. Антивирус ESET NOD32 4	4
1.1 Что нового?	4
1.2 Требования к системе	4
2. Установка	5
2.1 Обычная установка	5
2.2 Пользовательская установка	6
2.3 Использование исходных значений параметров	7
2.4 Ввод имени пользователя и пароля	8
2.5 Сканирование компьютера по требованию	8
3. Руководство для начинающих	9
3.1 Введение в пользовательский интерфейс программы: режимы	9
3.1.1 Проверка работоспособности системы	9
3.1.2 Что делать, если система не работает надлежащим образом?	10
3.2 Настройка обновлений	10
3.3 Настройка прокси-сервера	10
3.4 Защита настроек	10
4. Работа сантivirusом ESET NOD32	12
4.1 Защита от вирусов и шпионских программ	12
4.1.1 Защита файловой системы в режиме реального времени	12
4.1.1.1 Настройки контроля файловой системы	12
4.1.1.1.1 Носители для сканирования	12
4.1.1.1.2 Сканирование при определенных условиях («Сканировать при»)	12
4.1.1.1.3 Дополнительные параметры системы своевременного обнаружения ThreatSense для новых и измененных файлов	12
4.1.1.1.4 Дополнительные настройки	12
4.1.1.2 Уровни очистки	12
4.1.1.3 Когда изменять параметры защиты файловой системы в режиме реального времени	13
4.1.1.4 Проверка защиты файловой системы в режиме реального времени	13
4.1.1.5 Решение проблем, возникающих при работе защиты файловой системы в режиме реального времени	13
4.1.2 Host Intrusion Prevention System (HIPS)	13
4.1.3 Защита почтового клиента	13
4.1.3.1 Проверка POP3	14
4.1.3.1.1 Совместимость	14
4.1.3.2 Интеграция с почтовыми клиентами	14

4.1.3.2.1	Добавление уведомлений к тексту сообщений электронной почты	15
4.1.3.3	Удаление заражений	15
4.1.4	Защита доступа в Интернет	15
4.1.4.1	Протоколы HTTP, HTTPS	15
4.1.4.1.1	Управление адресами	16
4.1.4.1.2	Веб-браузеры	16
4.1.5	Сканирование компьютера	16
4.1.5.1	Тип сканирования	16
4.1.5.1.1	Обычное сканирование	17
4.1.5.1.2	Сканирование с пользовательскими настройками	17
4.1.5.2	Объекты сканирования	17
4.1.5.3	Профили сканирования	17
4.1.6	Фильтрация протоколов	18
4.1.6.1	SSL	18
4.1.6.1.1	Доверенные сертификаты	18
4.1.6.1.2	Исключенные сертификаты	18
4.1.7	Настройка параметров модуля ThreatSense	18
4.1.7.1	Настройка объектов	19
4.1.7.2	Параметры	19
4.1.7.3	Очистка	19
4.1.7.4	Расширения	20
4.1.7.5	Ограничения	20
4.1.7.6	Прочее	20
4.1.8	Действия при выявлении заражения	20
4.2	Обновление программы	21
4.2.1	Настройка обновлений	21
4.2.1.1	Профили обновлений	22
4.2.1.2	Дополнительные настройки обновления	22
4.2.1.2.1	Режим обновления	22
4.2.1.2.2	Прокси-сервер	23
4.2.1.2.3	Подключение к локальной сети	23
4.2.1.2.4	Создание зеркала обновлений	24
4.2.1.2.4.1	Обновление с зеркала	24
4.2.1.2.4.2	Устранение неполадок при обновлении с зеркала	25
4.2.2	Создание задач автоматического обновления	25
4.3	Планировщик	25
4.3.1	Назначение запланированных задач	25
4.3.2	Создание новой задачи	26
4.4	Карантин	26
4.4.1	Перемещение файлов на карантин	26
4.4.2	Восстановление из карантина	26
4.4.3	Передача файла из карантина	26
4.5	Файлы журнала	27
4.5.1	Обслуживание журнала	27
4.6	Интерфейс пользователя	27
4.6.1	Предупреждения и уведомления	28
4.7	ThreatSense.Net	29

4.7.1	Подозрительные файлы	29
4.7.2	Статистика	30
4.7.3	Передача	30
4.8	Удаленное администрирование	30
4.9	Лицензия	31
5.	Опытный пользователь	32
5.1	Настройка прокси-сервера	32
5.2	Импорт и экспорт параметров	32
5.2.1	Экспорт параметров	32
5.2.2	Импорт параметров	32
5.3	Командная строка	33
5.4	ESET SysInspector	33
5.4.1	Интерфейс пользователя и работа в приложении	34
5.4.1.1	Элементы управления программой	34
5.4.1.2	Навигация в ESET SysInspector	34
5.4.1.3	Сравнение	35
5.4.1.4	SysInspector как часть антивируса ESET NOD32 4	36
5.4.1.5	Сценарий обслуживания	36
5.4.1.5.1	Создание сценариев обслуживания	36
5.4.1.5.2	Структура сценария обслуживания	36
5.4.1.5.3	Выполнение сценариев обслуживания	37
5.5	ESET SysRescue	38
5.5.1	Минимальные требования	38
5.5.2	Создание компакт-диска аварийного восстановления	38
5.5.2.1	Папки	38
5.5.2.2	Антивирус ESET	38
5.5.2.3	Дополнительно	38
5.5.2.4	Загрузочное USB-устройство	39
5.5.2.5	Запись	39
5.5.3	Работа с ESET SysRescue	39
5.5.3.1	Использование ESET SysRescue	39
6.	Глоссарий	40
6.1	Типы заражений	40
6.1.1	Вирусы	40
6.1.2	Черви	40
6.1.3	Троянские программы	40
6.1.4	Руткиты	40
6.1.5	Рекламные программы	41
6.1.6	Шпионские программы	41
6.1.7	Потенциально опасные программы	41
6.1.8	Потенциально нежелательные программы	41

1. Антивирус ESET NOD32 4

Антивирус ESET NOD32 версии 4 пришел на смену отмеченным наградами продуктам семейства ESET NOD32 2.x. Благодаря применению новейшей версии ядра сканирования ThreatSense® программа демонстрирует скорость и точность сканирования, свойственную антивирусам ESET NOD32.

Применение передовых технологий позволяет превентивно блокировать работу вирусов, шпионского ПО, троянских и рекламных программ, а также червей и руткитов без снижения производительности системы, не вызывая раздражения у пользователя во время работы или игры на компьютере.

1.1 Что нового?

Многолетний опыт наших специалистов отражен в абсолютно новой архитектуре антивируса ESET NOD32, который обнаруживает максимальное количество злонамеренных программ при минимальных системных требованиях.

- **Модуль защиты от вирусов и шпионских программ**

В этом модуле используется ядро сканирования на основе технологии ThreatSense®, которое использовалось ранее в отмеченной наградами программе защиты от вирусов NOD 32. Ядро ThreatSense® оптимизировано и улучшено в соответствии с требованиями новой архитектуры антивируса ESET NOD32.

Возможность	Описание
Улучшенная очистка	Система защиты от вирусов высокотехнологично очищает и удаляет большую часть обнаруженных заражений без участия пользователя.
Фоновый режим сканирования	Сканирование компьютера может осуществляться в фоновом режиме, незаметном для системы и пользователя.
Уменьшенный размер файлов обновлений	Оптимизация ядра позволила сократить размер файлов обновлений по сравнению с версией 2.7. Защита файлов обновлений от повреждений также улучшена.
Защита популярных почтовых клиентов	Возможно сканирование входящей почты не только в Microsoft Outlook, но и в Outlook Express, Windows Mail, Windows Live Mail и Mozilla Thunderbird.
Множество мелких улучшений	<ul style="list-style-type: none">– Прямой доступ к файловой системе обеспечивает высокую скорость и производительность.– Блокировка доступа к зараженным файлам.– Оптимизация под требования центра безопасности Windows, включая версию для Vista.

1.2 Требования к системе

Для правильной работы антивируса ESET NOD32 система должна соответствовать перечисленным ниже аппаратным и программным требованиям.

Антивирус ESET NOD32

Операционная система Windows NT4 SP6, 2000, XP	Процессор 400 МГц, 32-разрядный (x86) или 64-разрядный (x64) 128 МБ ОЗУ 130 МБ свободного места на диске Монитор Super VGA (800 × 600)
--	---

Операционная система Windows 7, Vista	Процессор 1 ГГц, 32-разрядный (x86) или 64-разрядный (x64) 512 МБ ОЗУ 130 МБ свободного места на диске Монитор Super VGA (800 × 600)
---------------------------------------	---

Антивирус ESET NOD32 Business Edition

Операционная система Windows NT4 SP6, 2000, 2000 Server, XP, 2003 Server	Процессор 400 МГц, 32-разрядный (x86) или 64-разрядный (x64) 128 МБ ОЗУ 130 МБ свободного места на диске Монитор Super VGA (800 × 600)
--	---

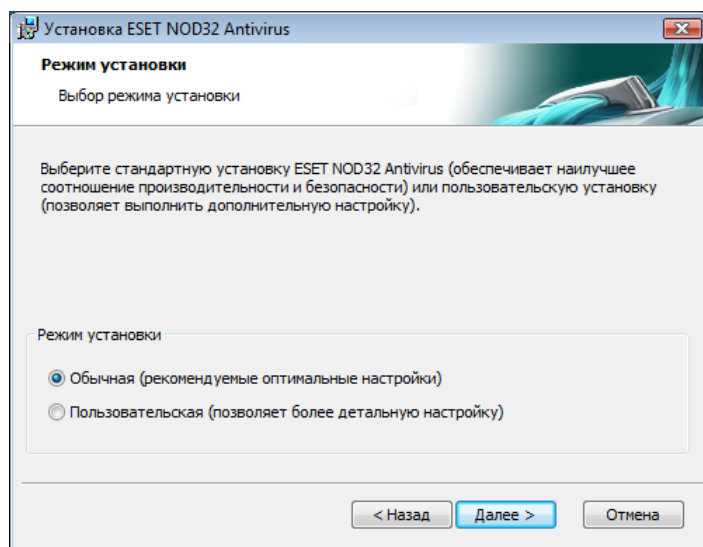
Операционная система Windows 7, Windows Vista, Windows Server 2008	Процессор 1 ГГц, 32-разрядный (x86) или 64-разрядный (x64) 512 МБ ОЗУ 130 МБ свободного места на диске Монитор Super VGA (800 × 600)
--	---

ПРИМЕЧАНИЕ. Технологии Anti Stealth и Self Defense недоступны в Windows NT4 SP6.

2. Установка

После приобретения программы установочный файл антивируса ESET NOD32 в формате пакета MSI можно загрузить с веб-узла компании ESET. Запустите установочный файл, и мастер установки поможет установить программу. Предлагается два типа установки с разным указанием сведений об установке:

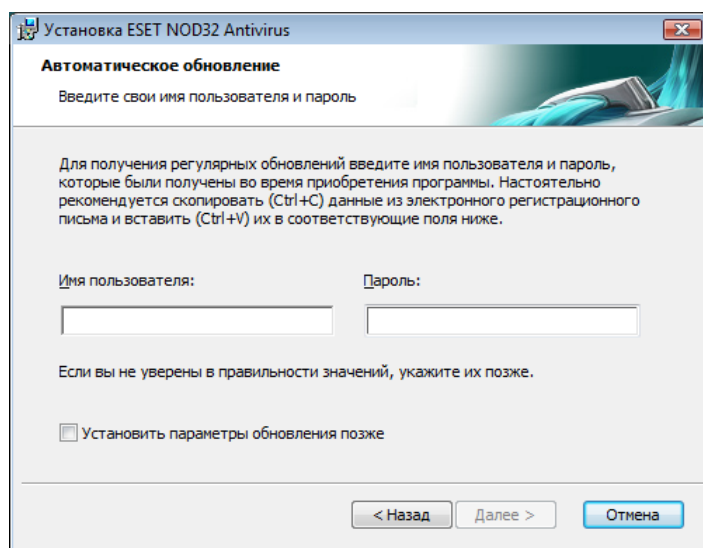
1. Обычная установка
2. Пользовательская установка



2.1 Обычная установка

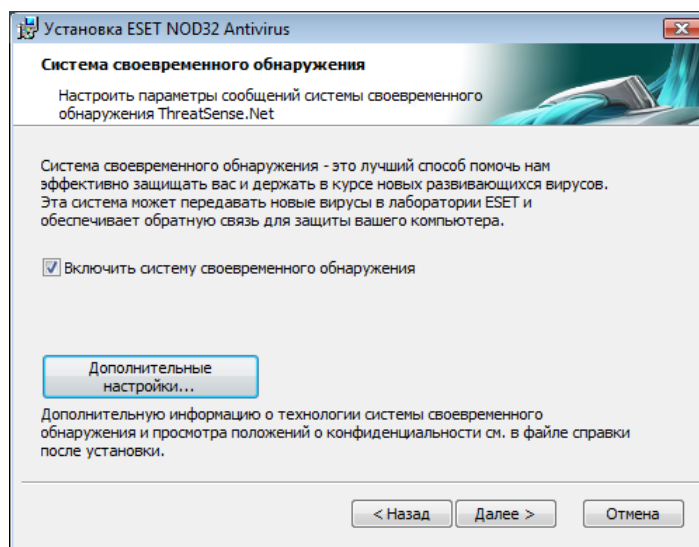
Обычная установка рекомендуется для пользователей, предпочитающих установить антивирус ESET NOD32 с параметрами по умолчанию. Параметры по умолчанию обеспечивают наивысшую степень безопасности. Этот вариант рекомендуется для пользователей, которые не хотят выполнять подробную настройку программы вручную.

На первом (очень важном) шаге установки предлагается ввести имя пользователя и пароль, необходимые для получения автоматических обновлений программы. Получение обновлений играет важнейшую роль в обеспечении непрерывной защиты компьютера.



В соответствующих полях введите свои **имя пользователя** и **пароль**, то есть те данные, которые были получены при приобретении или регистрации программы. Если имя пользователя и пароль еще неизвестны, установите флажок «Установить параметры обновления позже». Данные аутентификации могут быть указаны позже.

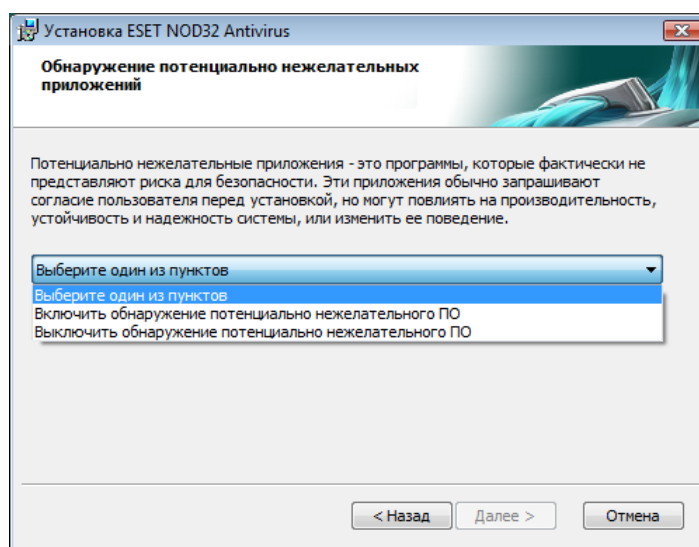
Следующим шагом является настройка системы своевременного обнаружения ThreatSense.Net. Система своевременного обнаружения ThreatSense.Net предназначена для своевременного и постоянного информирования компании ESET о появлении новых угроз. Она позволяет быстро реагировать и защищать пользователей. Система предусматривает передачу образцов злонамеренного кода в лабораторию ESET. Там они анализируются, обрабатываются и добавляются в базы данных сигнатур вирусов.



По умолчанию флажок «**Включить систему своевременного обнаружения**» установлен, что активирует данную функцию системы. Для изменения параметров передачи подозрительных файлов нажмите кнопку «**Дополнительные настройки**».

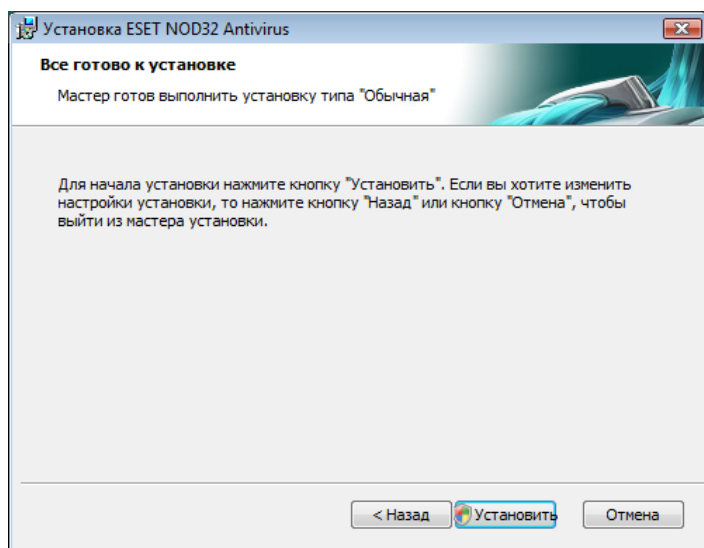
Следующим шагом установки является настройка **обнаружения потенциально нежелательного программного обеспечения**. Приложения, относящиеся к потенциально нежелательному ПО, не обязательно являются злонамеренными, однако они могут негативно влиять на работу операционной системы.

Такие программы часто поставляются в пакете совместно с другими, полезными программами, и их установку трудно заметить во время установки всего пакета программ. Хотя при установке таких приложений обычно отображается уведомление, они могут быть легко установлены без согласия пользователя.



Рекомендуется выбрать пункт «**Включить обнаружение потенциально нежелательного ПО**», чтобы разрешить обнаружение антивирусом ESET NOD32 такого типа угроз.

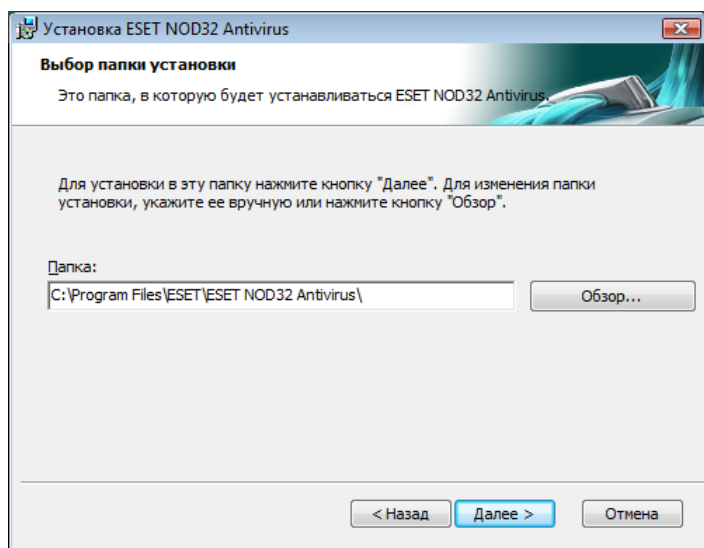
Последним шагом обычной установки является подтверждение установки. Для этого нажмите кнопку «Установить».



2.2 Пользовательская установка

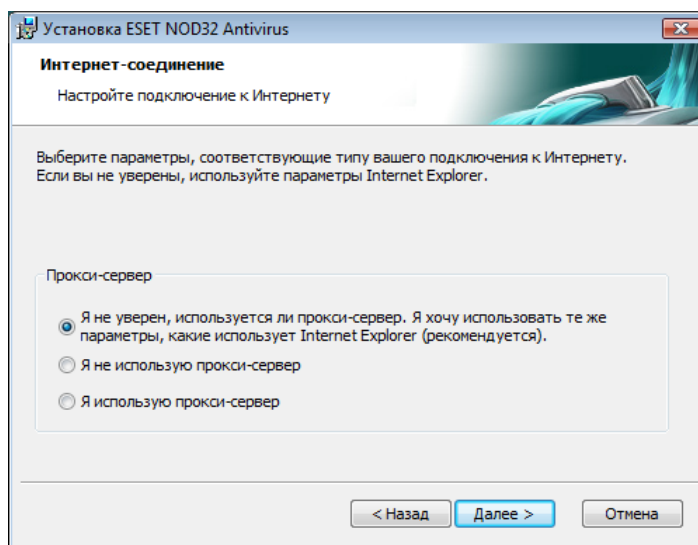
Пользовательская установка предназначена для опытных пользователей, которые могут выполнить тонкую настройку программы и хотят изменить параметры расширенной настройки во время установки.

Сначала нужно выбрать папку для установки программы. По умолчанию программа устанавливается в папку C:\Program Files\ESET\ESET NOD32 Antivirus\. Для того чтобы изменить папку установки, нажмите кнопку «Обзор» (не рекомендуется).

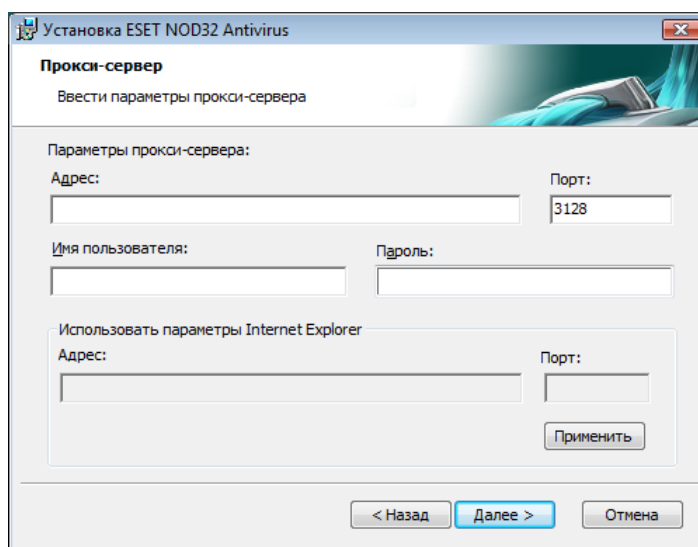


Далее **Введите имя пользователя и пароль**. Этот этап присутствует и в процедуре обычной установки (см. стр. 5).

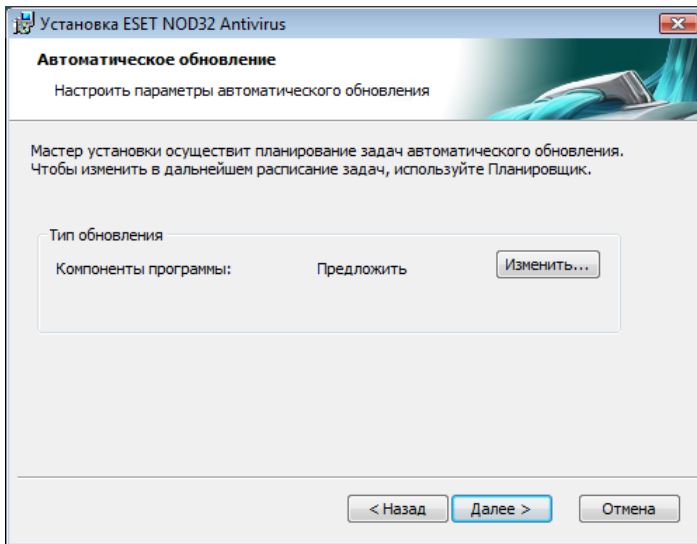
После ввода имени пользователя и пароля нажмите кнопку «Далее», чтобы **настроить подключение к Интернету**.



Если для подключения к Интернету используется прокси-сервер, для получения регулярных обновлений базы данных сигнатур вирусов необходимо правильно настроить его параметры. Если точно неизвестно, используется ли прокси-сервер для подключения к Интернету, оставьте настройку по умолчанию **«Я не знаю, используется ли прокси-сервер для выхода в Интернет. Я хочу использовать те же параметры, какие использует Internet Explorer»** и нажмите кнопку **«Далее»**. Если прокси-сервер не используется, выберите соответствующий параметр.

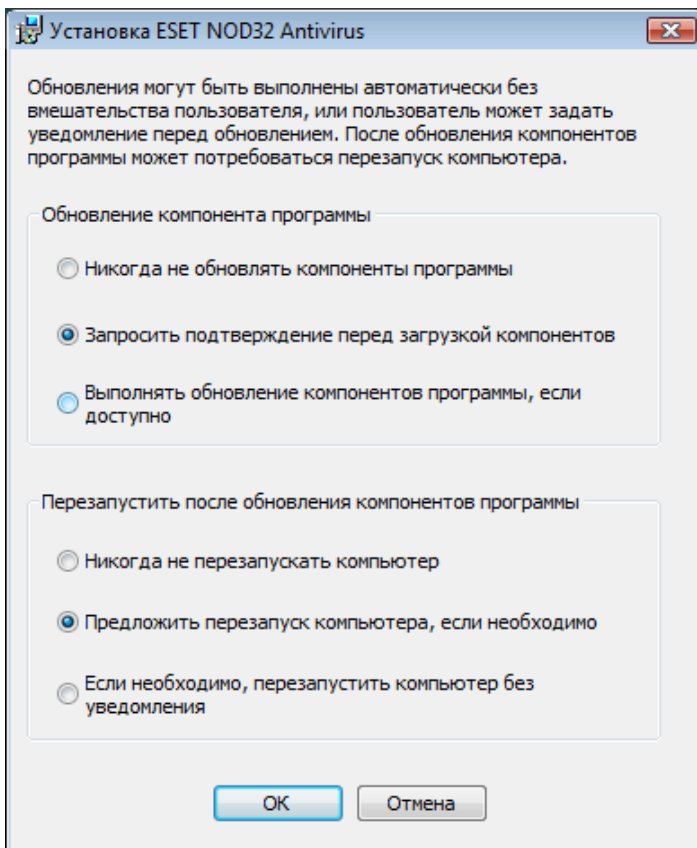


Чтобы настроить параметры прокси-сервера, выберите пункт **«Я использую прокси-сервер»** и нажмите кнопку **«Далее»**. Введите IP-адрес или адрес URL прокси-сервера в поле **«Адрес»**. В поле **«Порт»** укажите порт, по которому прокси-сервер принимает запросы на соединение (3128 по умолчанию). Если прокси-сервер требует аутентификации, введите правильные имя пользователя и пароль, которые необходимы для доступа к нему. Параметры прокси-сервера могут быть скопированы из параметров браузера Internet Explorer. Нажмите кнопку **«Применить»**, чтобы подтвердить выбор.



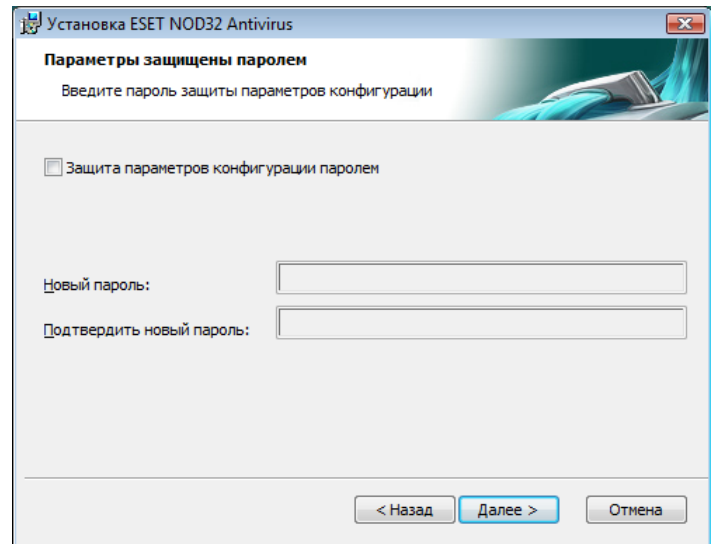
Нажмите кнопку «Далее», чтобы перейти к окну «**Настройка параметров автоматического обновления**». На этом этапе можно указать, как должна работать функция автоматического обновления программных компонентов. Для доступа к расширенным параметрам нажмите кнопку «Изменить».

Если нет необходимости получать обновления программных компонентов, выберите пункт «**Никогда не обновлять компоненты программы**». Параметр «**Запросить подтверждение перед загрузкой компонентов**» включает вывод окна подтверждения перед загрузкой программных компонентов. Для того чтобы включить автоматическое обновление программных компонентов без запроса подтверждения, выберите пункт «**Выполнять обновление компонентов программы, если доступно**».



ПРИМЕЧАНИЕ. После обновления программных компонентов обычно требуется перезагрузка компьютера. Рекомендуется выбрать вариант «**Если необходимо, перезапустить компьютер без уведомления**».

На следующем шаге нужно ввести пароль для защиты параметров программы. Укажите пароль, которым будут защищены параметры программы. Введите пароль повторно для подтверждения.

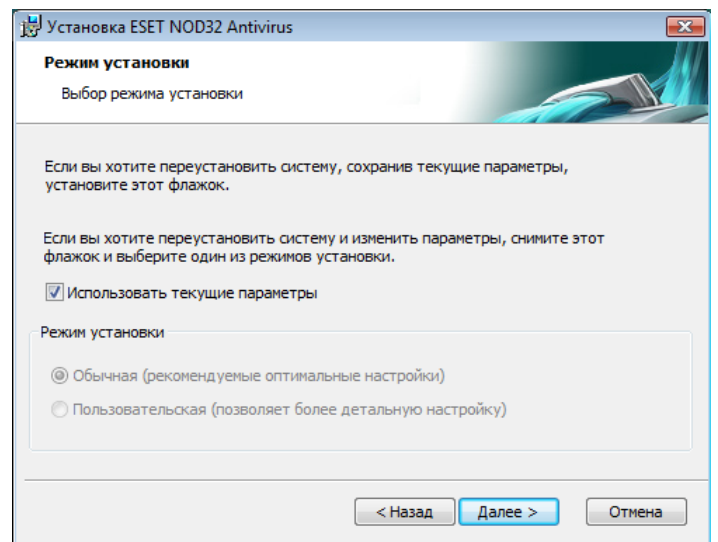


Шаги «**Настройка системы своевременного обнаружения**» и «**Обнаружение потенциально нежелательного ПО**» совпадают с соответствующими шагами в процедуре обычной установки и не описаны здесь (см. стр. 5).

На последнем шаге отображается окно с запросом на подтверждение установки.

2.3 Использование исходных значений параметров

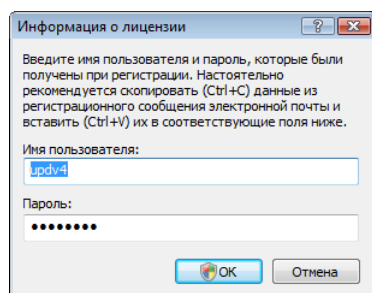
Если выполняется переустановка антивируса ESET NOD32, отображается флажок «**Использовать текущие параметры**». Установите этот флажок, чтобы перенести параметры исходного процесса установки в текущий процесс.



2.4 Ввод имени пользователя и пароля

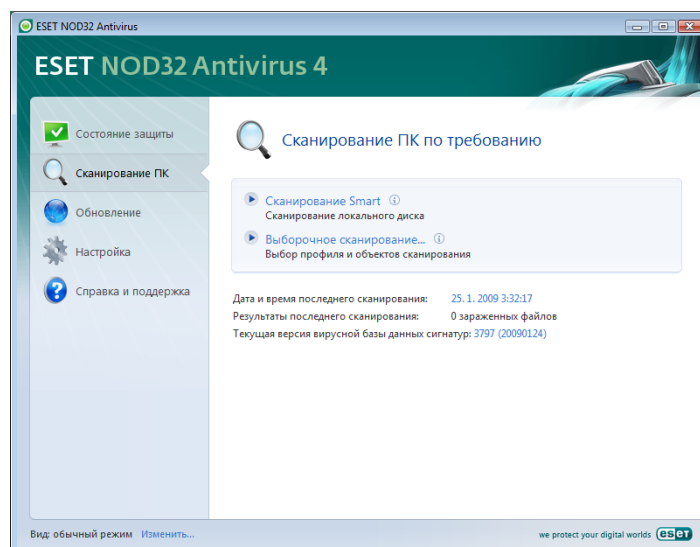
Для того чтобы использовать программу наилучшим образом, необходимо регулярно обновлять ее. Это возможно только при наличии правильных имени пользователя и пароля, которые указываются в параметрах обновления.

Если имя пользователя и пароль не указаны при установке, это можно сделать позже. В главном окне программы выберите последовательно пункты «**Обновление**» и «**Настройка имени пользователя и пароля**». В окне «**Информация о лицензии**» введите данные, полученные вместе с лицензией на программу.



2.5 Сканирование компьютера по требованию

После установки антивируса ESET NOD32 нужно выполнить сканирование компьютера на наличие злонамеренного кода. Для быстрого запуска сканирования в главном меню последовательно выберите пункты «**Сканирование компьютера**» и «**Обычное сканирование**». Дополнительную информацию о сканировании компьютера см. в разделе «Сканирование компьютера».



3. Руководство для начинающих

Эта глава содержит обзор основных функций и настроек антивируса ESET NOD32.

3.1 Введение в пользовательский интерфейс программы: режимы

Главное окно антивируса ESET NOD32 разделено на две области. Левый столбец содержит удобное для использования главное меню программы. Правая часть окна предназначена для отображения информации в зависимости от выбранного пункта меню в левой части.

Ниже приведено описание кнопок главного меню.

«**Состояние защиты**» — в этом разделе в понятной форме отображается информация о состоянии системы защиты антивируса ESET NOD32. Если включен расширенный режим, отображается состояние всех модулей защиты по отдельности. Щелкните по модулю, чтобы просмотреть подробную информацию о его текущем состоянии.

«**Сканирование компьютера**» — в этом разделе пользователь может настроить и запустить сканирование компьютера по требованию.

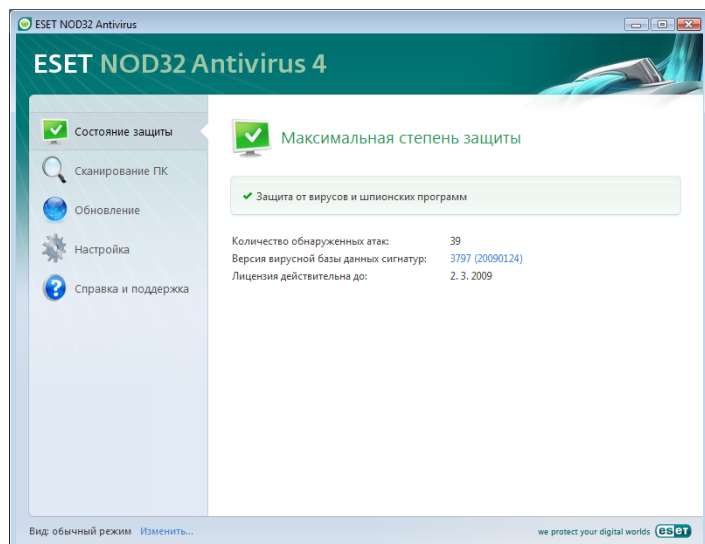
«**Обновление**» — в этом разделе предоставлен доступ к модулю, который управляет процессом обновления базы данных сигнатур вирусов.

«**Настройки**» — этот раздел предназначен для управления уровнем безопасности компьютера. Если включен расширенный режим, отображаются подменю модуля защиты от вирусов и шпионских программ.

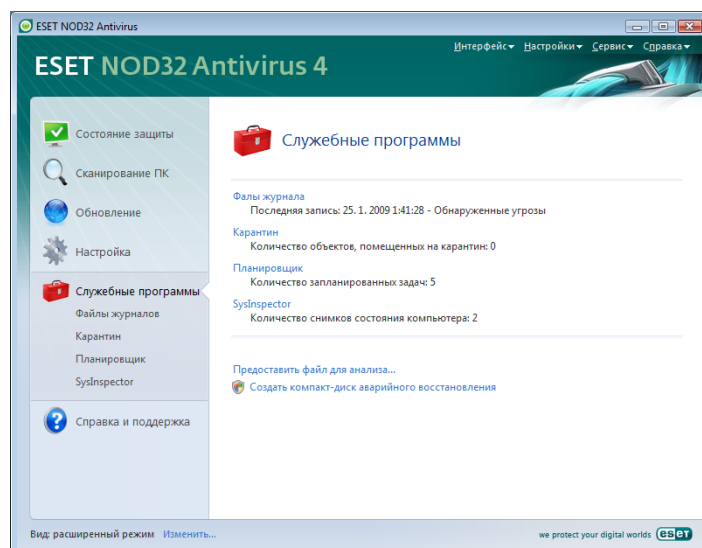
«**Служебные программы**» — этот раздел доступен только в расширенном режиме и предназначен для доступа к файлам журналов, карантину и планировщику.

«**Справка и поддержка**» — кнопка предназначена для перехода к справочной системе, к статьям базы знаний и веб-сайту компании ESET, а также для доступа к системе размещения запросов в службу поддержки.

Интерфейс антивируса ESET NOD32 позволяет пользователям переключаться между обычным и расширенным режимами. Для переключения между режимами предназначена ссылка «**Показать**», расположенная в нижнем левом углу главного окна антивируса ESET NOD32. Нажмите эту кнопку, чтобы выбрать необходимый режим отображения.



Обычный режим предоставляет доступ ко всем функциям, необходимым для выполнения обычных операций. Доступ к расширенным функциям при этом отсутствует.

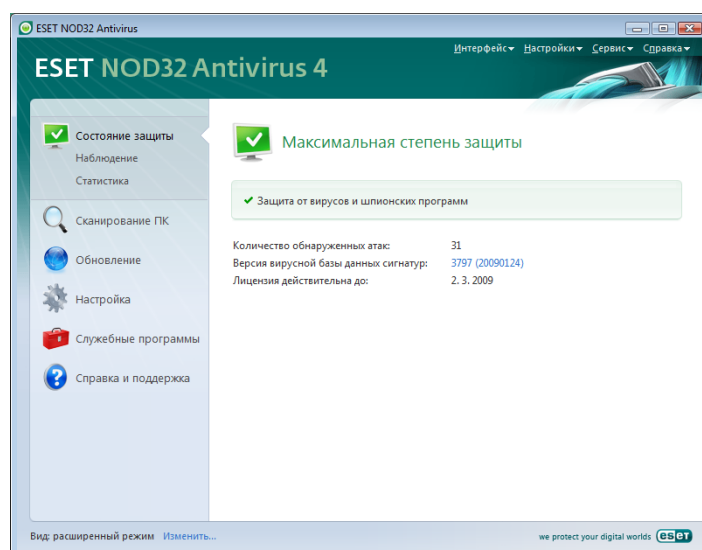


При переключении в расширенный режим в главном меню появляется пункт «**Служебные программы**». Раздел «Служебные программы» предоставляет доступ к планировщику, карантину и файлам журналов антивируса ESET NOD32.

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

3.1.1 Проверка работоспособности системы

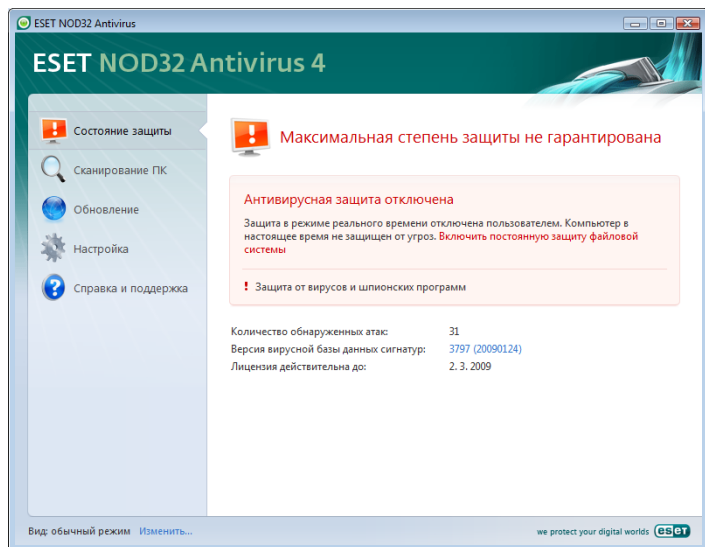
Для того чтобы получить информацию о **состоянии защиты**, выберите соответствующий пункт главного меню. При этом ниже появляется подменю «**Защита от вирусов и шпионских программ**», а в главном окне программы отображается отчет о состоянии системы защиты от вирусов ESET NOD32. Выберите «Защита от вирусов и шпионских программ» для просмотра сведений о состоянии отдельных модулей защиты в главном окне программы.



Зеленый флажок обозначает, что в работе модулей нет проблем. При возникновении проблем отображается оранжевый значок уведомления или красный восклицательный знак, а также дополнительные сведения в верхней части окна. Кроме того, предлагается решение проблемы. Для того чтобы изменить состояние отдельного модуля, щелкните пункт главного меню «**Настройки**» и выберите необходимый модуль.

3.1.2 Что делать, если система не работает надлежащим образом?

Если антивирус ESET NOD32 обнаруживает проблему в каком-либо модуле защиты, это отражается в окне «Состояние защиты». Там же предлагается возможное решение проблемы.

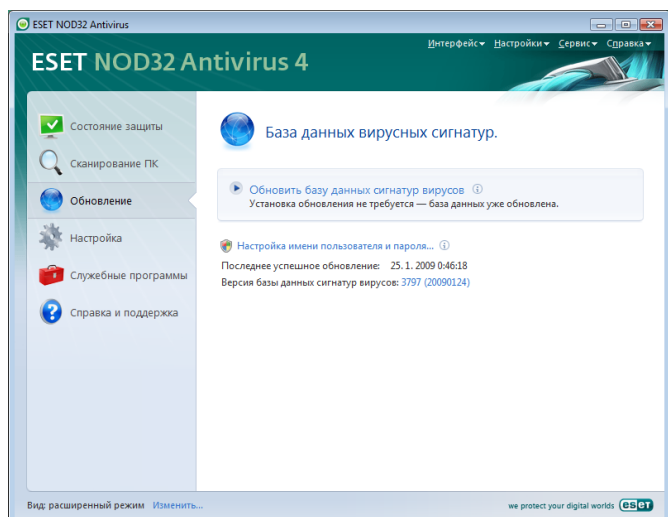


Если решить проблему с помощью предлагаемых мер не удастся, выберите пункт «Справка и поддержка» для доступа к файлам справки или для поиска в базе знаний. Если по-прежнему не удастся решить проблему, отправьте запрос в службу технической поддержки компании ESET. На основе полученных от пользователя сведений специалисты службы поддержки могут быстро определить причину проблемы и предложить ее решение.

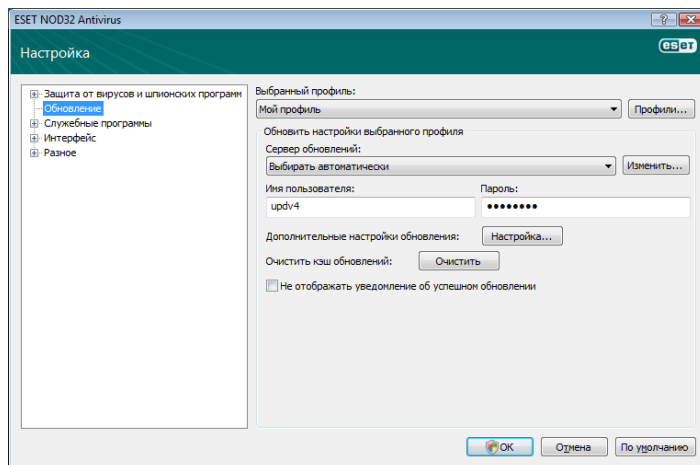
3.2 Настройка обновлений

Процесс обновления базы данных сигнатур вирусов и компонентов программы является важнейшей частью обеспечения защиты компьютера от злонамеренного кода. Уделите особое внимание изучению настройки и работы этого процесса. Чтобы незамедлительно проверить доступность обновления базы данных сигнатур вирусов, в главном меню программы нажмите «Обновить» и «Обновить базу данных сигнатур вирусов». Диалоговое окно «Настройка имени пользователя и пароля» предназначено для ввода имени пользователя и пароля, которые были получены в момент приобретения программного продукта.

Если имя пользователя и пароль были указаны во время установки антивируса ESET NOD32, то они не будут запрошены на этом этапе.

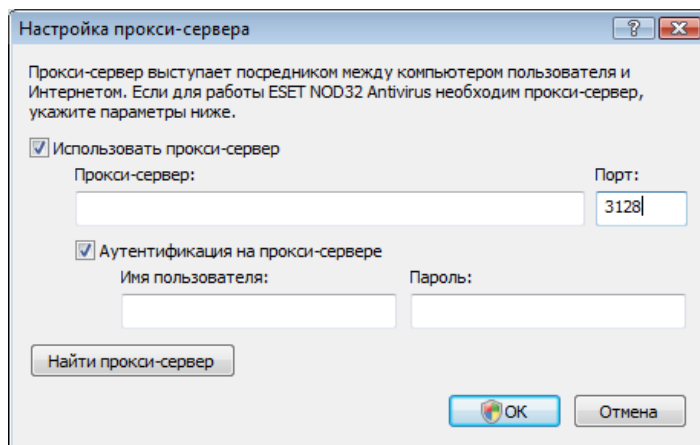


Окно «Дополнительные настройки» (для доступа нажмите клавишу F5) содержит дополнительные параметры обновления. «Сервер обновлений»: в раскрывающемся списке выберите пункт «Выборить автоматически». Для настройки дополнительных параметров обновления, например режима обновлений, доступа к прокси-серверу, получения обновлений с локального сервера и создания копий сигнатур вирусов (в антивирусе ESET NOD32 Business Edition), нажмите кнопку «Настройки».



3.3 Настройка прокси-сервера

Если для подключения к Интернету используется прокси-сервер, это должно быть указано в дополнительных параметрах (клавиша F5). Для доступа к окну настроек прокси-сервера в дереве расширенных параметров программы выберите «Разное» > «Прокси-сервер». Установите флажок «Использовать прокси-сервер», введите IP-адрес и номер порта прокси-сервера, а также данные аутентификации для доступа к серверу.



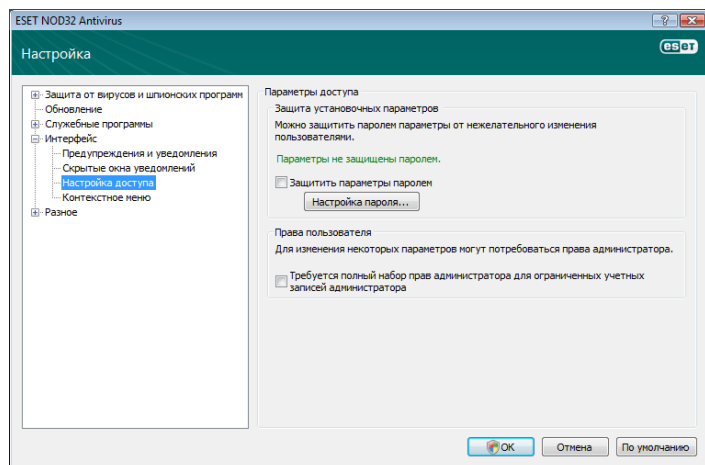
Если эти сведения отсутствуют, можно попробовать автоматически определить параметры прокси-сервера для антивируса ESET NOD32, нажав кнопку «Найти прокси-сервер».

ПРИМЕЧАНИЕ. Параметры прокси-сервера для различных профилей обновления могут различаться. В этом случае настройте прокси-сервер в разделе дополнительных настроек обновления.

3.4 Защита настроек

Настройки антивируса ESET NOD32 могут быть очень важны с точки зрения политики безопасности организации. Несанкционированное изменение параметров может нарушить стабильность системы и ослабить ее защиту. Для защиты параметров паролем в главном меню программы выберите «Настройки» > «Ввод всего дерева расширенных параметров» > «Интерфейс» > «Защита параметров» и нажмите кнопку «Введите пароль».

Введите пароль, введите его повторно для подтверждения, а затем нажмите **ОК**. Этот пароль потребуется для любого изменения параметров антивируса ESET NOD32 в будущем.



4. Работа с антивирусом ESET NOD32

4.1 Защита от вирусов и шпионских программ

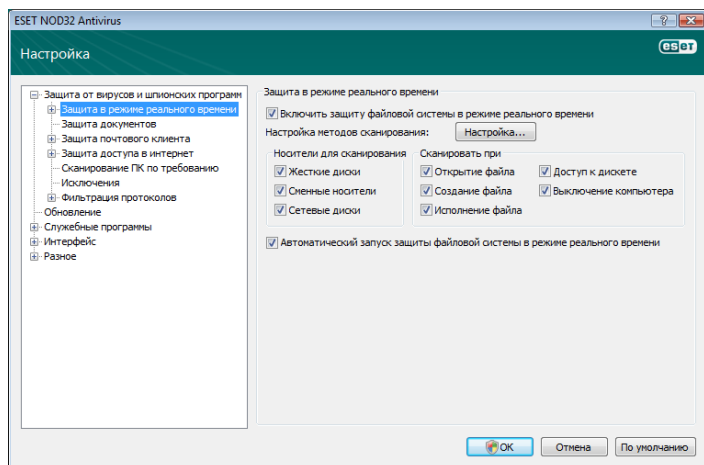
Защита от вирусов и шпионских программ предназначена для ограждения системы от вредоносных атак с помощью проверки содержимого файлов, сообщений электронной почты и обмена данными через Интернет. Если вредоносный код обнаружен, модуль защиты от вирусов и шпионских программ обезвреживает его, сначала блокируя его исполнение, а затем очищая, удаляя или перемещая на карантин.

4.1.1 Защита файловой системы в режиме реального времени

Защита файловой системы в режиме реального времени управляет всеми событиями в системе, относящимися к защите от вирусов. Все файлы сканируются на наличие вредоносного кода в момент их открытия, создания или запуска. Защита файловой системы в режиме реального времени запускается во время загрузки операционной системы.

4.1.1.1 Настройки контроля файловой системы

Защита файловой системы в режиме реального времени проверяет все типы носителей. Контроль включается в зависимости от различных событий. Контроль использует методы технологии своевременного обнаружения (подробнее см. раздел «Настройка методов сканирования»). Метод контроля может изменяться в зависимости от того, создается ли новый файл или происходит работа с уже существующим. Для вновь созданных файлов возможно применение углубленных методов контроля.



4.1.1.1.1 Носители для сканирования

По умолчанию все доступные носители проверяются на наличие возможных угроз безопасности.

«**Жесткие диски**» – все жесткие диски компьютера.

«**Съемные носители**» – дискеты, накопители USB и т. д.

«**Сетевые диски**» – все подключенные сетевые диски.

Рекомендуется изменять эти параметры только в особых случаях (например, если сканирование определенных носителей приводит к значительному замедлению скорости передачи данных).

4.1.1.1.2 Сканирование при определенных условиях («Сканировать при»)

По умолчанию все файлы сканируются при открытии, исполнении или создании. Рекомендуется сохранять установки по умолчанию, поскольку они обеспечивают максимальный уровень безопасности компьютера.

Функция «**Доступ к дискете**» обеспечивает контроль содержимого загрузочного сектора дискеты, находящейся в приводе. Функция «**Выключение компьютера**» обеспечивает проверку загрузочных секторов жестких дисков компьютера во время его выключения. Несмотря на то, что загрузочные вирусы в настоящее время встречаются редко, рекомендуется включить эту функцию.

4.1.1.1.3 Дополнительные параметры системы своевременного обнаружения ThreatSense для новых и измененных файлов

Возможность заражения недавно созданных или измененных файлов выше по сравнению с уже существующими файлами. По этой причине такие файлы сканируются с учетом дополнительных параметров. Одновременно с обычными методами сканирования, основанными на поиске в базе данных сигнатур вирусов, применяются методы расширенной эвристики. Это значительно увеличивает вероятность обнаружения вирусов. Кроме недавно созданных файлов, такое сканирование выполняется для самораспаковывающихся файлов (SFX) и файлов упаковщиков в режиме реального времени (внутренне упакованных исполняемых файлов). По умолчанию архивы проверяются до десятого уровня вложенности вне зависимости от фактического размера файла. Для того чтобы изменить параметры сканирования архивов, снимите флажок «**Параметры сканирования архива по умолчанию**».

4.1.1.1.4 Дополнительные настройки

Для минимизации помех при работе компьютера защита файловой системы в режиме реального времени не сканирует повторно файлы, которые уже проверены, если они не были изменены. Файлы сканируются повторно сразу после обновления базы данных сигнатур вирусов. Такое поведение настраивается с помощью функции «**Оптимизированное сканирование**». Если она отключена, все файлы сканируются каждый раз при доступе к ним.

По умолчанию защита файловой системы в режиме реального времени запускается во время загрузки операционной системы и предназначена для непрерывного сканирования файлов. В особых случаях (например, в случае конфликта с другим модулем сканирования в режиме реального времени) защита файловой системы в режиме реального времени может быть отключена путем отключения параметра «**Автоматический запуск защиты файловой системы в режиме реального времени**».

По умолчанию расширенная эвристика не используется при запуске файлов на исполнение. Тем не менее в некоторых случаях можно включить эту функцию, установив флажок «**Расширенная эвристика запуска файлов**». Следует обратить внимание на то, что из-за повышенных требований к системе расширенная эвристика может замедлить выполнение некоторых программ.

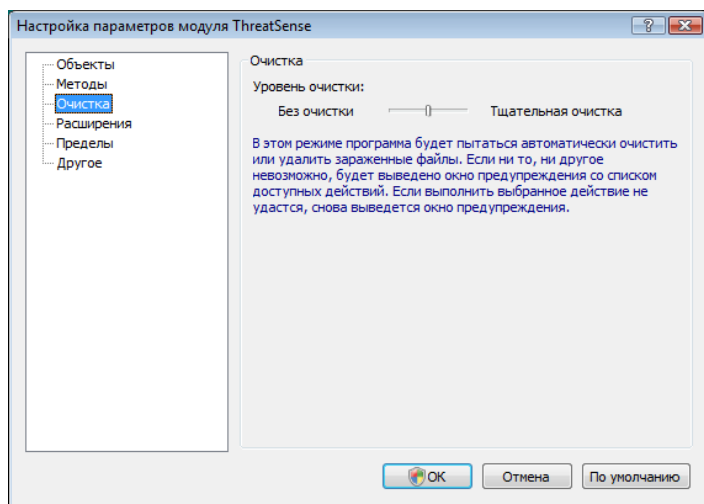
4.1.1.2 Уровни очистки

Защита в режиме реального времени предусматривает три уровня очистки (для доступа к настройкам нажмите кнопку «**Настройки**» в разделе «**Защита файловой системы в режиме реального времени**» и перейдите к ветке «**Очистка**»).

- В режиме первого уровня программа показывает окно уведомления и предлагает на выбор действия для каждого из случаев заражения. Пользователь должен выбрать действие для каждого заражения отдельно. Этот уровень разработан для опытных пользователей, которые знают, как поступать в каждом конкретном случае.
- В режиме среднего уровня программа автоматически выбирает и выполняет предварительно определенное действие (в зависимости от типа заражения). Обнаружение и удаление зараженных файлов сопровождается информационным сообщением, располагающимся в правом

нижнем углу экрана. Однако автоматические действия не предпринимаются в случае обнаружения заражения в архивах, которые содержат, помимо зараженных, файлы без вредоносного кода, а также если действий для этого случая не предусмотрено.

- В режиме третьего, наиболее «агрессивного» уровня все зараженные объекты удаляются. Так как этот уровень может привести к потере полезной информации, рекомендуется использовать его только в особых случаях.



4.1.1.3 Когда изменять параметры защиты файловой системы в режиме реального времени

Защита файловой системы в режиме реального времени является наиболее существенным компонентом всей системы защиты. Поэтому необходимо соблюдать осторожность при изменении ее параметров. Рекомендуется изменять ее параметры только в особых случаях. Например, это можно делать при возникновении конфликтов с какими-либо приложениями или модулями сканирования в режиме реального времени других антивирусных программ.

После установки антивируса ESET NOD32 все параметры настроены оптимально и обеспечивают максимальный уровень защиты системы. Для того чтобы восстановить параметры по умолчанию, нажмите кнопку «По умолчанию» в нижней части окна «Защита файловой системы в режиме реального времени» («Дополнительные настройки» > «Защита от вирусов и шпионских программ» > «Защита файловой системы в режиме реального времени»).

4.1.1.4 Проверка защиты файловой системы 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 по адресу <http://www.eicar.org/download/eicar.com>.

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

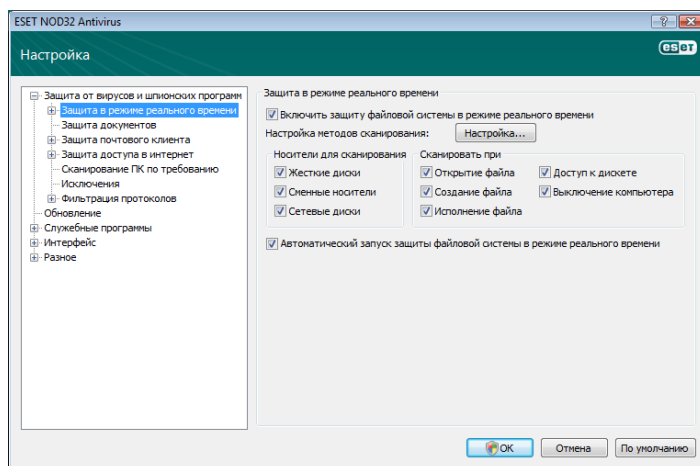
В этой главе рассказывается о проблемах, которые могут возникать при работе защиты файловой системы в режиме реального времени, и о способах их разрешения.

Защита файловой системы в режиме реального времени отключена

Если защита файловой системы в режиме реального времени непреднамеренно была отключена пользователем, ее нужно включить. Для того чтобы включить защиту файловой системы в режиме реального времени, перейдите на страницу «Настройки» > «Защита от вирусов и шпионских программ»

и нажмите «Включить» в разделе «Защита файловой системы в режиме реального времени» главного окна программы.

Если защита файловой системы в режиме реального времени не запускается при загрузке операционной системы, возможно, отключена функция «Автоматический запуск защиты файловой системы в режиме реального времени». Для того чтобы включить эту функцию, перейдите в окно «Дополнительные настройки» (клавиша F5) и выберите в дереве расширенных параметров «Защита файловой системы в режиме реального времени». В разделе «Дополнительные настройки» в нижней части окна установите флажок «Автоматический запуск защиты файловой системы в режиме реального времени».



Защита файловой системы в режиме реального времени не обнаруживает вирусы

Убедитесь в том, что на компьютере не установлено другое антивирусное приложение. При одновременной работе двух систем защиты от вирусов могут возникнуть конфликты. Рекомендуется удалять все прочие антивирусные приложения.

Защита файловой системы в режиме реального времени не 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 к специалистам службы технической поддержки ESET.

4.1.2 Host Intrusion Prevention System (HIPS)

Host Intrusion Prevention System (HIPS) защищает от попыток внешнего воздействия, способных негативно повлиять на безопасность вашего компьютера. Для мониторинга процессов, файлов и ключей реестра HIPS использует сочетание технологий поведенческого анализа с возможностями сетевого фильтра, что позволяет эффективно детектировать, блокировать и предотвращать подобные попытки вторжения.

4.1.3 Защита почтового клиента

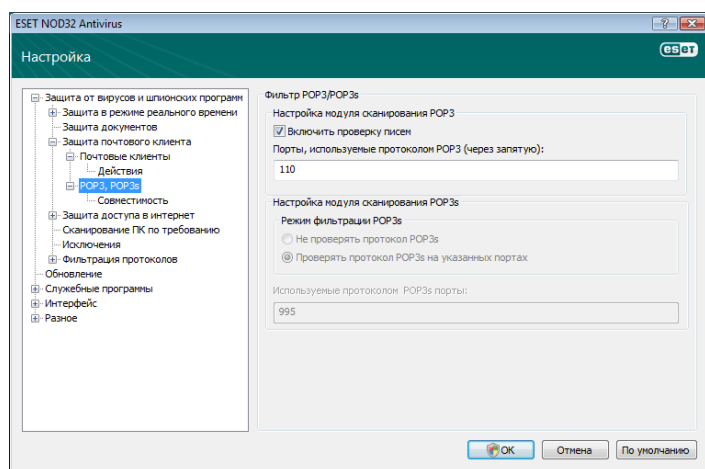
Защита электронной почты обеспечивает контроль безопасности обмена данных по протоколу POP3. Использование подключаемого модуля антивируса ESET NOD32 для программы Microsoft Outlook позволяет контролировать весь трафик почтового клиента по протоколам POP3, MAPI, IMAP и HTTP. При проверке входящих сообщений программа использует все методы глубокого сканирования технологии своевременного обнаружения ThreatSense. Это позволяет обнаруживать попытки проникновения вредоносных программ даже до того, как данные о них попадают в базу данных сигнатур вирусов. Процесс сканирования обмена данных по протоколу POP3 происходит независимо от типа используемого клиента.

4.1.3.1 Проверка POP3

Протокол POP3 является самым распространенным протоколом получения сообщений почтовыми клиентами. Антивирус ESET NOD32 обеспечивает защиту этого протокола независимо от используемого клиента.

Модуль, обеспечивающий эту функцию, загружается при запуске операционной системы и остается активным в системной памяти. Для нормальной работы модуля убедитесь в том, что он включен. Для проверки протокола POP3 перенастройка под конкретного почтового клиента не требуется. По умолчанию сканируется весь трафик, проходящий через порт 110, однако может быть настроена и проверка других портов. Номера портов при перечислении разделяются запятыми.

Шифрованный трафик не проверяется.



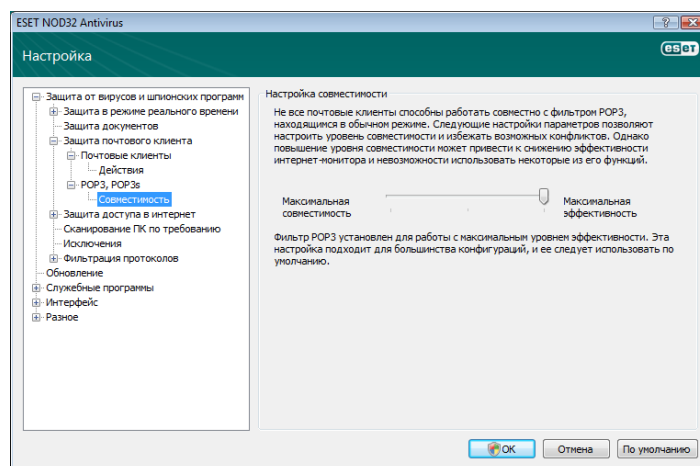
4.1.3.1.1 Совместимость

В некоторых почтовых клиентах могут возникать проблемы при фильтрации пакетов POP3 (например, при медленном соединении с сервером процесс получения сообщений может прерываться). В этом случае измените способ контроля трафика. Снижение уровня контроля может увеличить скорость очистки. Для настройки уровня контроля POP3 воспользуйтесь командой «Защита от вирусов и шпионских программ» > «Защита электронной почты» > «POP3» > «Совместимость».

Если включен режим «Максимальная эффективность», вредоносный код удаляется из зараженных сообщений, а информация о заражении вставляется перед исходной темой письма (если включены функции «Удалить» или «Очистить» либо включен уровень **тщательной** очистки или очистки **по умолчанию**).

Режим «Средняя совместимость» изменяет способ получения сообщений. Сообщения постепенно отправляются почтовому клиенту и сканируются только после получения последней части. Однако при этом возрастает риск заражения. Уровень очистки и применение уведомлений (текстовой информации, прикрепляемой к теме или телу сообщения) остаются теми же, что и для режима наибольшей эффективности.

В режиме «Максимальная совместимость» программа выводит окно с уведомлением о получении зараженного сообщения. При этом не добавляется уведомлений к теме или телу сообщения, а вирусы автоматически не удаляются. Удаление заражения должно производиться пользователем вручную в почтовом клиенте.

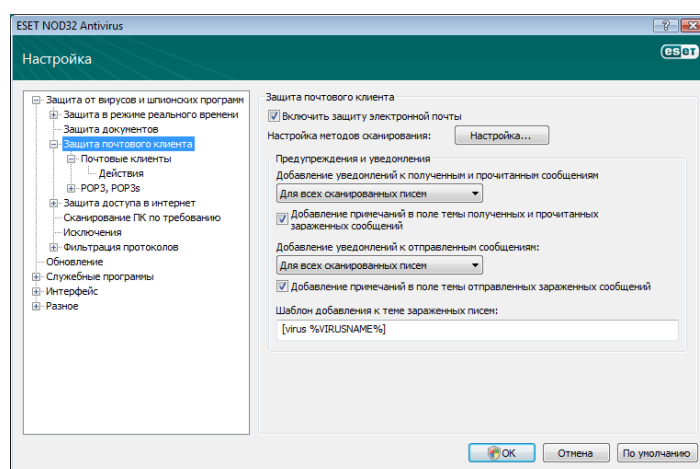


4.1.3.2 Интеграция с почтовыми клиентами

Интеграция антивируса ESET NOD32 и почтовых клиентов увеличивает степень активного противодействия вредоносному коду, распространяемому через сообщения электронной почты. Если почтовый клиент содержится в списке поддерживаемых, можно включить режим интеграции с антивирусом ESET NOD32. После включения режима интеграции панель инструментов антивируса ESET NOD32 встраивается в почтовый клиент, что обеспечивает более эффективную защиту обмена данными по электронной почте. Параметры интеграции доступны в разделе «Настройки» > «Ввод всего дерева расширенных параметров» > «Разное» > «Интеграция с почтовыми клиентами». Диалоговое окно позволяет пользователю включить интеграцию с поддерживаемыми почтовыми клиентами. Список поддерживаемых почтовых клиентов содержит такие программы, как Microsoft Outlook, Outlook Express, Windows Mail, Windows Live Mail и Mozilla Thunderbird.

Если при работе с почтовым клиентом производительность системы снижается, установите флажок «Отключить проверку при изменении содержимого папки «Входящие»». Такие проблемы могут возникать при загрузке сообщений с узла Kerio Outlook Connector Store.

Защиту электронной почты можно включить, установив флажок «Включить защиту электронной почты» в разделе «Дополнительные настройки» (клавиша F5) > «Защита от вирусов и шпионских программ» > «Защита электронной почты».



4.1.3.2.1 Добавление уведомлений к тексту сообщений электронной почты

Каждое сообщение, проверяемое антивирусом ESET NOD32, может быть отмечено прикрепленным к теме или тексту сообщения уведомлением. Эта функция поднимает уровень доверия со стороны адресата, а в случае возникновения заражения предоставляет важную информацию о степени заражения и опасности, исходящей от отправителя.

Параметры этой функции доступны в разделе «Дополнительные настройки» > «Защита от вирусов и шпионских программ» > «Защита почтового клиента». Программа содержит функцию «Добавление уведомлений к полученным и прочитанным сообщениям», а также «Добавление уведомлений к отправленным сообщениям». Пользователь может указать, добавлять ли уведомления ко всем сообщениям, только к зараженным сообщениям или не добавлять уведомлений вообще.

Антивирус ESET NOD32 позволяет пользователю добавлять уведомления к теме сообщения. Для этого используйте функции «Добавление примечаний в поле темы полученных и прочитанных зараженных сообщений» и «Добавление примечаний в поле темы отправленных зараженных сообщений».

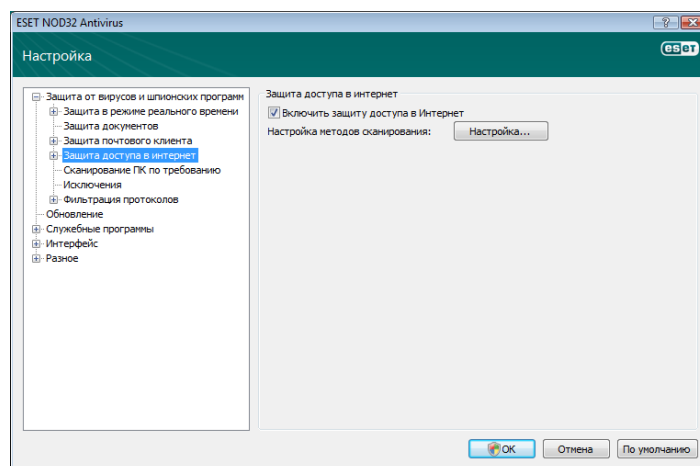
Содержимое уведомлений можно настроить в поле «Шаблон», добавленном к теме зараженных писем. Вышеупомянутые изменения помогают автоматизировать процесс фильтрации зараженных сообщений электронной почты и позволяют пользователю отбирать почту с указанной темой в отдельную папку (если это поддерживается почтовым клиентом).

4.1.3.3 Удаление заражений

В случае обнаружения зараженного сообщения электронной почты выводится окно уведомления. Окно уведомления содержит имя отправителя, адрес его электронной почты и название угрозы. В нижней части окна находятся функции, которые можно применить обнаруженному объекту, а именно: «Очистить», «Удалить» и «Пропустить». В большинстве случаев рекомендуется выбирать вариант «Очистить» или «Удалить». В особых ситуациях, если есть желание принять зараженный объект, выберите «Пропустить». Если выбран режим «Тщательная очистка», информационное окно не предоставляет возможность выбора действия.

4.1.4 Защита доступа в Интернет

Подключение к Интернету является стандартной возможностью современного компьютера. К сожалению, Интернет является одним из основных носителей злонамеренного кода. По этой причине необходимо уделять особое внимание защите доступа в Интернет. Настоятельно рекомендуется установить флажок «Включить защиту доступа в Интернет». Этот параметр расположен в разделе «Дополнительные настройки» (F5) > «Защита от вирусов и шпионских программ» > «Защита доступа в Интернет».



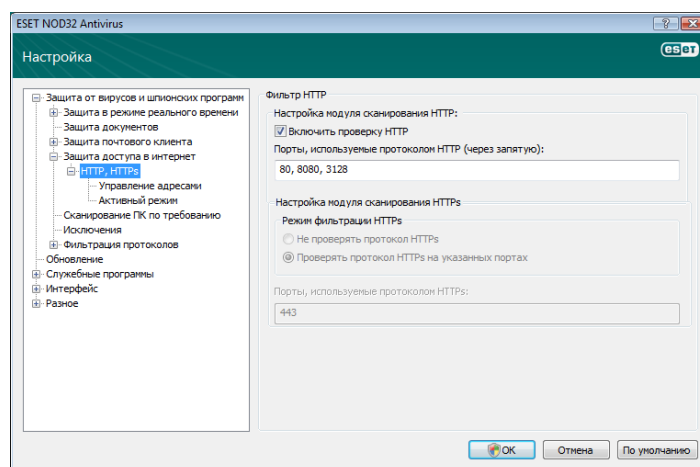
4.1.4.1 Протоколы HTTP, HTTPS

Защита доступа в Интернет заключается в контроле процесса обмена данными между веб-браузерами и удаленными серверами в соответствии с правилами протоколов HTTP и HTTPS (шифрованный трафик). Антивирус ESET NOD32 по умолчанию настроен на работу со стандартами, которые поддерживаются большинством веб-браузеров. Однако некоторые из параметров проверки трафика HTTP могут быть изменены в разделе «Защита доступа в Интернет» > «Протоколы HTTP, HTTPS». В главном окне фильтра HTTP пользователь может установить или снять флажок «Включить проверку HTTP». Кроме того, можно указать номера портов, которые используются при обмене данными по протоколу HTTP. По умолчанию определены следующие номера портов: 80, 8080 и 3128. Проверка протокола HTTPS может осуществляться в перечисленных ниже режимах.

«Не проверять протокол HTTPS»:
обмен шифрованными данными не проверяется.

«Проверять протокол HTTPS на указанных портах»:
проверка данных HTTPS осуществляется только при использовании указанных портов.

«Проверять протокол HTTPS для приложений, отмеченных как интернет-браузеры, на указанных портах»:
проверка только тех приложений, которые содержатся в списке интернет-браузеров и используют порты из списка «Порты, используемые протоколом HTTP».

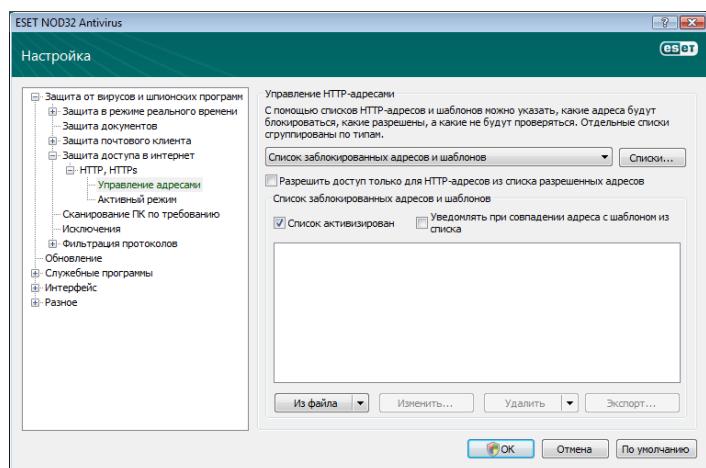


4.1.4.1.1 Управление адресами

В этом разделе можно указать адреса HTTP для блокировки, разрешения или исключения из проверки.

Для формирования списков адресов используйте кнопки «Добавить», «Изменить», «Удалить» и «Экспорт». Веб-сайты из списка заблокированных адресов будут недоступны. Веб-сайты из списка исключенных адресов загружаются без проверки на вредоносный код. Если включить функцию «Разрешить доступ только для HTTP-адресов из списка разрешенных адресов», будут доступны только веб-сайты с адресами из списка разрешенных, а остальные адреса будут заблокированы.

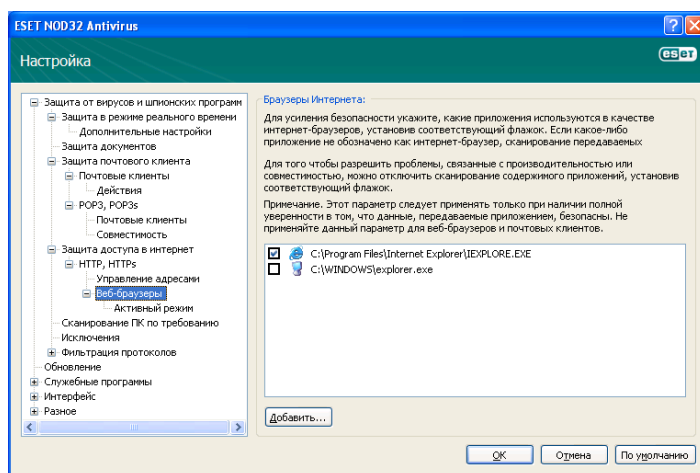
Во всех списках допустимо использование символов шаблона «*» (звездочка) и «?» (вопросительный знак). Символ звездочки обозначает любую последовательность символов, а вопросительный знак – любой символ. Работать с содержимым списка исключенных адресов необходимо с особой тщательностью, так как он должен содержать только проверенные и безопасные адреса. В связи с этим необходимо быть уверенным в правильности использования символов шаблона в этом списке. Для того чтобы активировать список, установите флажок «Список активен». Если требуется получать уведомления при вводе адреса из списка, установите флажок «Уведомлять при совпадении адреса с шаблоном из списка».



4.1.4.1.2 Веб-браузеры

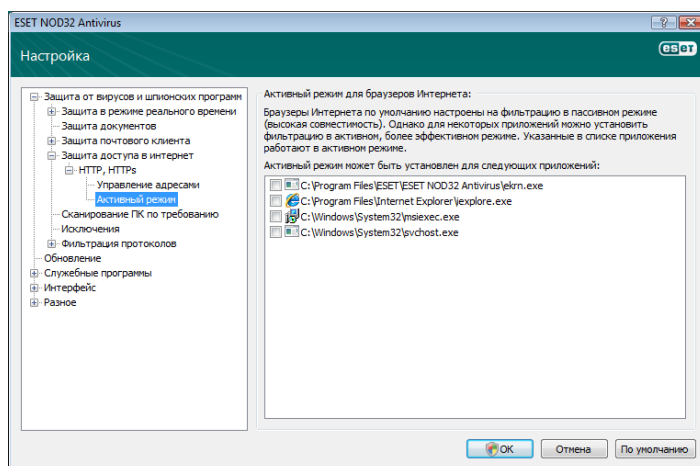
Антивирус ESET NOD32 содержит функцию **Веб-браузеры**, которая позволяет пользователю указать, является ли приложение веб-браузером. Если приложение классифицируется как веб-браузер, весь обмен данными с этим приложением отслеживается вне зависимости от портов, используемых в сетевом соединении.

Эта функция дополняет функцию проверки протокола HTTP, так как проверка HTTP контролирует только определенные порты. Многие службы в Интернете используют динамическое распределение портов или неизвестные заранее значения портов. С помощью функции указания веб-браузеров можно контролировать сетевые соединения вне зависимости от параметров соединения.



Список приложений, классифицированных как веб-браузеры, доступен в подменю «Веб-браузеры» в ветке «HTTP». Этот раздел также содержит подменю «Активный режим», которое определяет режим проверки для интернет-браузеров.

Функция «Активный режим» весьма полезна для полной проверки всего трафика. Если она отключена, обмен данными контролируется в пакетном режиме. Это снижает эффективность проверки передачи данных, но обеспечивает лучшую совместимость с перечисленными приложениями. Если проблем с совместимостью нет, рекомендуется использовать активный режим, установив соответствующий флажок рядом с нужным приложением.



4.1.5 Сканирование компьютера

При обнаружении симптомов возможного заражения компьютера (необычное поведение и т. п.) запустите сканирование компьютера по требованию. С точки зрения обеспечения безопасности целесообразно запускать сканирование регулярно, а не только при возникновении подозрительных симптомов. Регулярное сканирование помогает обнаружить заражение, если оно не было обнаружено защитой файловой системы в режиме реального времени в момент попадания вредоносного кода в систему. Это может произойти в том случае, если в тот момент модуль сканирования в режиме реального времени был отключен или база данных сигнатур вирусов устарела.

Рекомендуется запускать сканирование по требованию не реже одного или двух раз в месяц. Сканирование можно запускать по расписанию из окна «Службные программы» > «Планировщик».

4.1.5.1 Тип сканирования

Доступно два типа сканирования. Тип «Обычное сканирование» предназначен для быстрой проверки системы. При этом не нужно настраивать никакие параметры. Тип «Выборочное сканирование» позволяет пользователю выбирать необходимые профили сканирования и указывать объекты, подлежащие сканированию.



4.1.5.1.1 Обычное сканирование

Обычное сканирование является интуитивно понятным методом, позволяющим пользователю запускать сканирование компьютера и очищать зараженные файлы без участия самого пользователя. Главным преимуществом этого метода является простота эксплуатации без расширенного управления параметрами сканирования. Обычное сканирование проверяет все файлы на локальных дисках и автоматически очищает или удаляет обнаруженный вредоносный код. Уровень очистки автоматически установлен на уровень по умолчанию. Дополнительную информацию о типах очистки см. в разделе «Очистка» (стр. 18).

Стандартный профиль очистки разработан для пользователей, желающих быстро и просто просканировать компьютеры. Он предлагает эффективное решение для сканирования и очистки без углубленной настройки процесса.

4.1.5.1.2 Сканирование с пользовательскими настройками

Сканирование с пользовательскими настройками является оптимальным решением в том случае, когда нужно указать параметры сканирования (например, объекты сканирования и методы сканирования). Преимуществом такого сканирования является возможность подробной настройки. Наборы параметров могут быть сохранены в виде пользовательских профилей сканирования, которые особенно полезны при регулярном сканировании с одинаковыми параметрами.

Для того чтобы выбрать объекты сканирования, используйте меню быстрого выбора объектов или выберите объекты в дереве объектов, доступных для сканирования. Пользователь может задать три уровня очистки в меню «**Настройки**» > «**Очистка**». Если необходимо сканирование без выполнения дополнительных действий, установите флажок «**Сканировать без очистки**».

Сканирование с пользовательскими настройками подходит для опытных пользователей систем защиты от вирусов.

4.1.5.2 Объекты сканирования

Раскрывающееся меню «Объекты сканирования» служит для выбора файлов, папок и устройств (накопителей) для сканирования.

Можно выбрать следующие объекты сканирования:

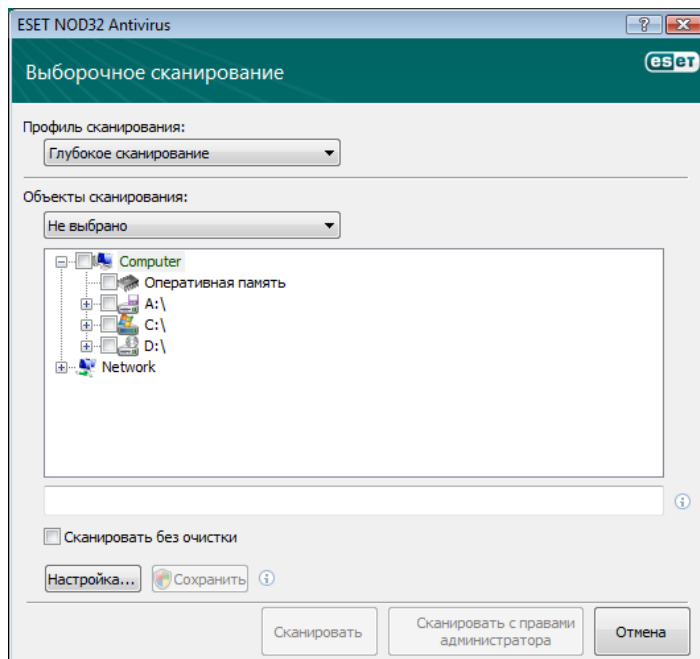
«**По параметрам профиля**» — объекты сканирования, указанные в выбранном профиле;

«**Съемные носители**» — дискеты, накопители USB, приводы CD/DVD и т. д.;

«**Жесткие диски**» — все жесткие диски компьютера;

«**Сетевые диски**» — все подключенные сетевые диски;

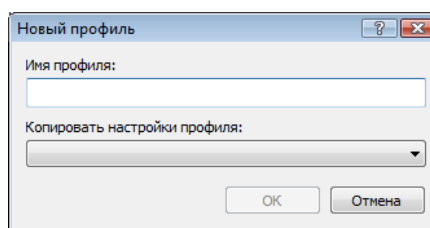
«**Ничего не выбирать**» — отменить выбор объектов сканирования.



Объекты сканирования могут быть определены более точно. Для этого укажите пути к папкам и файлам, подлежащим сканированию. Выберите объекты сканирования в дереве, содержащем доступные на компьютере устройства.

4.1.5.3 Профили сканирования

Набор предпочитаемых параметров сканирования компьютера может быть сохранен в виде профиля. С помощью профилей сканирования можно сохранить параметры и использовать их в будущем. Рекомендуется создать профили для каждого из регулярно используемых наборов параметров (для различных объектов сканирования, методов сканирования и прочих параметров).



Для того чтобы создать новый профиль, который будет использоваться в будущем на регулярной основе, откройте окно «**Дополнительные настройки**» (F5) > «**Сканирование компьютера по требованию**». Нажмите кнопку «**Профили**», расположенную в правой части. В результате отобразится список существующих профилей сканирования. Выберите создание нового профиля. В разделе «**Настройка методов сканирования**» подробно описан каждый из параметров сканирования. Эта информация может пригодиться при формировании профиля сканирования.

Пример.

Предположим, необходимо создать отдельный профиль сканирования, а конфигурация профиля «**Разумное сканирование**» частично подходит. Однако дополнительно необходимо включить сканирование файлов упаковщиков в режиме реального времени и потенциально опасного ПО, а также применить режим «**Тщательная очистка**». В окне «**Конфигурационные профили**» нажмите кнопку «**Добавить**». Введите имя нового профиля в поле «**Имя профиля**» и выберите «**Разумное сканирование**» в разделе «**Копировать настройки профиля:**». Настройте остальные необходимые параметры.

4.1.6 Фильтрация протоколов

Защита от вирусов для протоколов POP3 и HTTP обеспечивается модулем сканирования ThreatSense, который объединяет в себе все передовые технологии сканирования на наличие злонамеренного кода. Контроль осуществляется автоматически, независимо от используемого веб-браузера и почтового клиента. Если установлен флажок **«Включить фильтрацию содержимого протоколов уровня приложений»**, доступны следующие функции фильтрации протоколов:

«Порты HTTP и POP3» — сканирование только соединений через известные порты HTTP и POP3;

«Приложения, классифицированные как интернет-браузеры или почтовые клиенты» — фильтрация соединений только для приложений, классифицированных как интернет-браузеры («Защита доступа в Интернет» > HTTP, HTTPS > «Веб-браузеры») и почтовые клиенты («Защита почтового клиента» > POP3, POP3S > «Почтовые клиенты»);

«Порты и приложения, классифицированные как браузеры Интернета или почтовые клиенты» — на наличие вредоносного кода проверяются как порты, так и веб-браузеры.

Примечание.

Начиная с систем Windows Vista с пакетом обновления 1 (SP1) и Windows Server 2008, используется новая технология фильтрации сетевого трафика. Поэтому раздел фильтрации протоколов недоступен.

4.1.6.1 SSL

Антивирус ESET NOD32 4 позволяет выполнять проверку инкапсулированных в SSL протоколов. Для соединений, защищенных протоколом SSL с помощью доверенных сертификатов, неизвестных сертификатов или сертификатов, которые исключены из процесса проверки, предусмотрены различные режимы сканирования.

«Всегда сканировать протокол SSL (исключенные и доверенные сертификаты остаются действительными)» — данный режим предназначен для сканирования всех соединений SSL, кроме соединений, защищенных сертификатами, которые исключены из процесса проверки. При установлении нового соединения с неизвестным подписанным сертификатом пользователь об этом не уведомляется, а соединение подвергается автоматической фильтрации. Когда пользователь пытается соединиться с сервером, который использует ненадежный сертификат, классифицированный пользователем как доверенный (добавленный в список доверенных сертификатов), соединение с сервером разрешается, а обмен данными по установленному каналу фильтруется.

«Запрашивать о новых сайтах (неизвестные сертификаты)» — при посещении нового веб-сайта, защищенного SSL (с неизвестным сертификатом), будет отображаться диалоговое окно выбора. Этот режим позволяет создать список сертификатов SSL, которые должны быть исключены из сканирования.

«Не сканировать протокол SSL» — сканирование соединений, защищенных SSL, отключено.

Если сертификат невозможно проверить с помощью хранилища доверенных корневых сертификатов сертифицирующих органов, используются следующие режимы:

«Запрашивать действительность сертификата» — пользователю предлагается выбрать действие;

«Блокировать соединения, использующие данный сертификат» — соединение с сайтом, использующим данный сертификат, разрывается.

Если сертификат недействителен или поврежден:

«Запрашивать действительность сертификата» — пользователю предлагается выбрать действие;

«Блокировать соединения, использующие данный

сертификат» — соединение с сайтом, использующим данный сертификат, разрывается.

4.1.6.1.1 Доверенные сертификаты

Кроме интегрированного хранилища доверенных корневых сертификатов сертифицирующих органов, в котором антивирус ESET NOD32 4 хранит доверенные сертификаты, можно создать пользовательский список доверенных сертификатов, для просмотра которого нужно последовательно выбрать пункты **«Настройка» (F5) > «Фильтрация протоколов» > SSL > «Доверенные сертификаты»**.

4.1.6.1.2 Исключенные сертификаты

В разделе «Исключенные сертификаты» перечислены сертификаты, которые считаются безопасными. Программа не будет проверять содержимое зашифрованного соединения, использующего сертификаты из данного списка. Рекомендуется устанавливать только гарантированно безопасные веб-сертификаты, чтобы исключить необходимость фильтрации содержимого.

4.1.7 Настройка параметров модуля ThreatSense

ThreatSense — это технология, которая содержит комплекс методов обнаружения угроз. Эта технология является проактивной, т. е. она защищает от новой угрозы в первые часы ее распространения. При этом используется комбинация методов (анализ кода, моделирование кода, обобщенные сигнатуры, сигнатуры вирусов), которые работают совместно, значительно повышая уровень безопасности компьютера. Модуль сканирования способен контролировать несколько потоков данных одновременно. Это увеличивает эффективность обнаружения. Кроме того, технология ThreatSense эффективна против руткитов.

Пользователь может настроить несколько параметров сканирования:

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

Для того чтобы открыть окно настроек, нажмите кнопку **«Настройка»** в окне параметров любого модуля, который использует технологию ThreatSense (см. ниже). Различные сценарии обеспечения безопасности требуют различных настроек. Именно поэтому технология ThreatSense позволяет настраивать параметры отдельно для каждого из следующих модулей:

- «Защита файловой системы в режиме реального времени»;
- «Проверка файлов, исполняемых при запуске системы»;
- «Защита электронной почты»;
- «Защита доступа в Интернет»;
- «Сканирование компьютера по требованию».

Параметры ThreatSense хорошо оптимизированы для каждого из модулей, и их изменение ведет к значительным изменениям поведения 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). Таким образом, рекомендуется воздержаться от изменения настроек методов сканирования для всех модулей, кроме модуля «Сканирование компьютера».

4.1.7.1 Настройка объектов

Раздел «**Объекты**» позволяет определять, какие компоненты и файлы компьютерной системы должны быть проверены на заражение.

«**Оперативная память**» — сканирование оперативной памяти на наличие вирусов и прочих угроз.

«**Загрузочные секторы**» — сканирование загрузочных секторов на наличие вирусов в MBR.

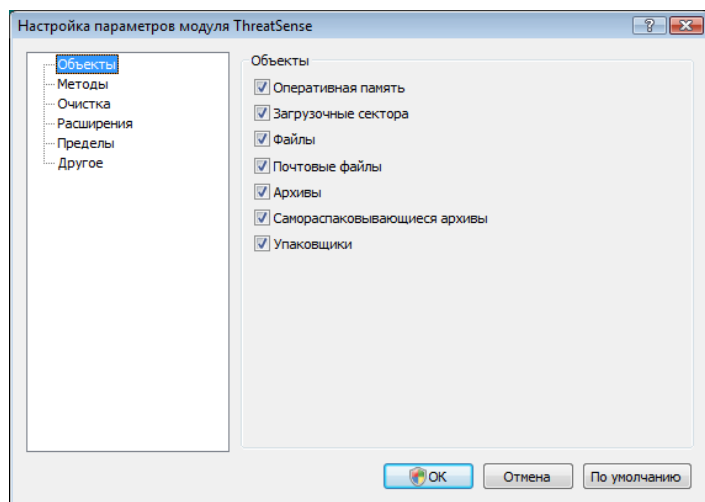
«**Файлы**» — сканирование всех широко используемых типов файлов (программ, изображений, звуковых и видеофайлов, файлов баз данных и т. п.).

«**Почтовые файлы**» — сканирование специальных файлов, предназначенных для хранения сообщений электронной почты.

«**Архивы**» — сканирование сжатых файлов в архивах (RAR, ZIP, ARJ, TAR и т. п.).

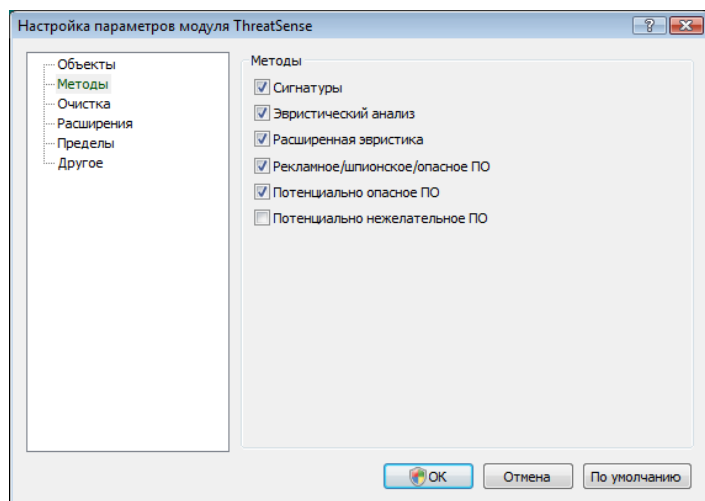
«**Самораспаковывающиеся архивы**» — сканирование файлов, содержащихся в архивах, которые распаковываются при запуске и, как правило, имеют расширение EXE.

«**Упаковщики**» — программы-упаковщики, которые отличаются от стандартных упаковщиков и распаковывают файлы динамически в системную память (UPX, yoda, ASPack, FGS и т. д.).



4.1.7.2 Параметры

В разделе «**Параметры**» пользователь может выбрать методы проверки системы на заражение. Ниже перечислены доступные варианты.



«**Сигнатуры**» — надежный и точный метод обнаружения и классификации вредоносного кода с помощью базы данных сигнатур вирусов.

«**Эвристика**» — алгоритм, анализирующий злонамеренную активность программ. Основным преимуществом метода эвристического анализа является способность обнаруживать новое вредоносное программное обеспечение, сведения о котором еще не попали в базу данных сигнатур вирусов.

«**Расширенная эвристика**» — метод основан на уникальном эвристическом алгоритме, разработанном компанией ESET и оптимизированном для обнаружения компьютерных червей и «троянских коней», написанных на языках программирования высокого уровня. Благодаря методу расширенной эвристики способность системы защиты правильно определять угрозу значительно возрастает.

«**Рекламное/шпионское/опасное ПО**» — эта категория включает в себя программы, собирающие информацию о пользователе без его согласия. Кроме того, сюда относятся программы, отображающие рекламные материалы.

«**Потенциально опасное ПО**» — коммерческие, легитимные приложения могут быть классифицированы как потенциально опасное ПО. Категория включает в себя такие программы, как средства доступа. Поэтому по умолчанию эта функция отключена.

«**Потенциально нежелательное ПО**» — эти приложения не обязательно являются злонамеренными, но они могут тем или иным образом снижать производительность системы. Такие приложения обычно требуют согласия пользователя при установке. После их установки поведение системы изменяется (по сравнению с тем, как она вела себя до установки этих программ). Наиболее значительные изменения касаются возникновения нежелательных всплывающих окон, запуска и работы скрытых процессов, увеличения использования системных ресурсов, изменения результатов поисковых запросов, обмена данными с удаленными серверами.

4.1.7.3 Очистка

Параметры процесса очистки определяют поведение модуля сканирования во время очистки зараженных файлов. Предусмотрено три уровня очистки.

«Без очистки»

Зараженные файлы не будут очищаться автоматически. Программа выводит предупреждение и предлагает пользователю выбрать действие.

«Уровень по умолчанию»

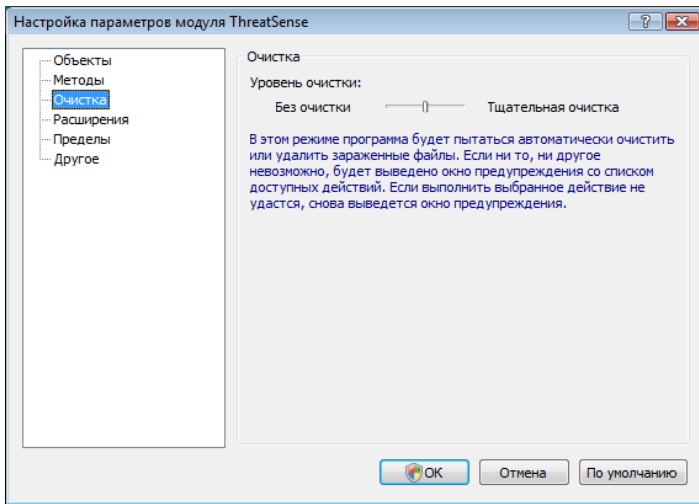
Программа будет пытаться автоматически очистить или удалить зараженный файл. При невозможности выбрать необходимое действие автоматически программа предлагает пользователю сделать выбор. Выбор предоставляется пользователю и в том случае, если предопределенное действие не может быть выполнено.

«Тщательная очистка»

Программа будет очищать или удалять все зараженные файлы, в том числе и архивы. Единственное исключение составляют системные файлы. Если это невозможно, пользователю выводится предупреждение с предложением выполнить определенное действие.

Предупреждение.

В режиме по умолчанию архив удаляется целиком, если содержит только зараженные файлы. Если в архиве имеются и незараженные файлы, он не будет удален. Если зараженный архив обнаружен в режиме тщательной очистки, весь архив удаляется, даже если присутствуют файлы без вредоносного кода.



4.1.7.4 Расширения

Расширением называется часть имени файла, отделенная от основной части точкой. Обычно расширение обозначает тип файла или его содержимого. Этот раздел параметров системы своевременного обнаружения позволяет определить типы файлов, подлежащих сканированию.

По умолчанию сканируются все файлы независимо от их расширения. Любое расширение можно добавить к списку исключений из сканирования. Если флажок **«Проверять все файлы»** не установлен, в списке отображаются расширения всех файлов, подлежащих сканированию в настоящее время. С помощью кнопок **«Добавить»** и **«Удалить»** можно изменять содержимое списка, запрещая или разрешая сканирование для тех или иных расширений.

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

Исключение файлов предназначено для тех случаев, когда сканирование файлов определенного типа приводит к ошибкам в работе программ, которые их используют. Например, эта ситуация возможна для файлов с расширениями EDB, EML и TMP, которые используются сервером Microsoft Exchange.

4.1.7.5 Ограничения

Этот раздел предназначен для указания максимального размера объектов сканирования и уровня вложенности сканируемых архивов.

«Максимальный размер объекта, в байтах»

Определяет максимальный размер объектов сканирования. Данный модуль антивируса будет сканировать только объекты меньше указанного размера. Не рекомендуется изменять объем по умолчанию без особых причин. Этот параметр предназначен для опытных пользователей, которые имеют определенные причины для исключения больших объектов из процесса сканирования.

«Максимальное время сканирования, в секундах»

Определяет максимальное время сканирования одного объекта. Если пользователем определено это значение, модуль антивируса прерывает процесс сканирования текущего объекта по истечении указанного промежутка времени вне зависимости от того, завершено ли сканирование.

«Уровень вложенности архива»

Определяет максимальную глубину сканирования архивов. Не рекомендуется изменять значение по умолчанию, равное 10, так как в обычных условиях для этого нет причин. Если сканирование преждевременно прерывается из-за превышения степени вложенности архивов, архив остается непроверенным.

«Максимальный размер файла в архиве, в байтах»

Определяет наибольший размер хранящихся в архиве файлов (в несжатом виде), которые подлежат сканированию. Если сканирование преждевременно прерывается из-за превышения данного параметра, архив остается непроверенным.

4.1.7.6 Прочее

«Сканировать потоки данных ADS»

Альтернативные потоки данных (ADS) используются файловой системой NTFS при работе с файлами и папками, которые не видны для обычного процесса сканирования. Многие вредоносные программы используют альтернативные потоки данных для того, чтобы избежать обнаружения.

«Запустить фоновое сканирование с низким приоритетом»

Каждый процесс сканирования потребляет некоторое количество системных ресурсов. Если пользователь использует программы с высокими требованиями к системным ресурсам, можно запустить сканирование в режиме низкого приоритета и освободить ресурсы для других приложений.

«Регистрировать все объекты»

При выборе этого параметра в журнале будет содержаться информация обо всех проверенных файлах, включая незараженные.

«Сохранить отметку о времени последнего доступа»

Используйте этот параметр для сохранения исходного времени доступа к сканируемым файлам, не обновляя его (например, для правильного функционирования систем резервного копирования).

Оптимизация Smart

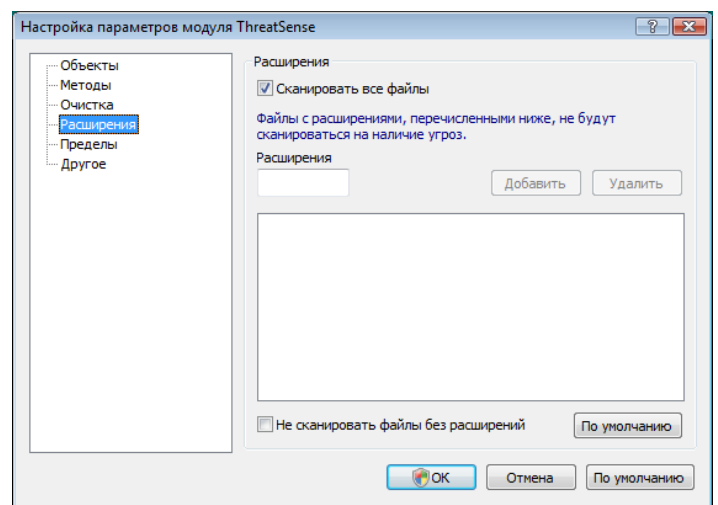
Оптимизация Smart упрощает сканирование Вашей системы на наличие вредоносного кода. Когда опция включена, увеличивается скорость сканирования без ущерба для безопасности вашей системы.

«Прокрутить журнал сканирования»

Эта функция позволяет включать и отключать прокрутку журнала. Если прокрутка включена, свежая информация всегда находится в нижней части экрана.

«Показывать уведомление о завершении сканирования в отдельном окне»

Открывает отдельное окно для отображения результатов сканирования.



4.1.8 Действия при выявлении заражения

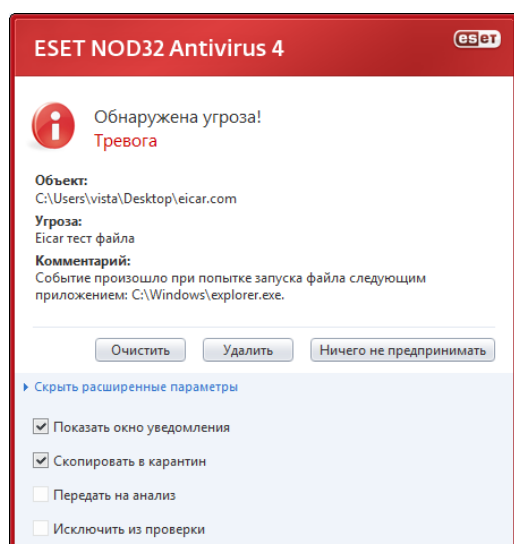
Система может получить вредоносный код из различных источников – веб-сайты, папки общего доступа, электронная почта или сменные носители (USB, внешние диски, компакт-диски, диски DVD и т. д.).

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

- Откройте антивирус ESET NOD32 и выберите пункт **«Сканирование компьютера»**.
- Нажмите кнопку **«Обычное сканирование»** (дополнительную информацию см. в разделе «Обычное сканирование»).
- После завершения сканирования просмотрите журнал на предмет количества проверенных, зараженных и вылеченных объектов.

Если необходимо проверить только часть диска, выберите **«Сканирование с пользовательскими настройками»** и укажите объекты для сканирования.

Чтобы проиллюстрировать, что происходит, когда антивирус ESET NOD32 находит заражение, предположим, что заражение обнаружено модулем защиты файлов в режиме реального времени, который используется в режиме очистки по умолчанию. Модуль пытается очистить или удалить файл. Если действие по умолчанию для модуля защиты в режиме реального времени не определено, запрос отправляется пользователю. Обычно предоставляется выбор из действий **«Очистить»**, **«Удалить»** и **«Пропустить»**. Не рекомендуется использовать действие **«Пропустить»**, так как зараженный файл останется на компьютере. Это действие следует использовать только тогда, когда есть полная уверенность в том, что файл безвреден и попал под подозрение по ошибке.



Очистка и удаление

Примените очистку, если полезный файл был атакован вирусом, который добавляет вредоносный код к полезному. В этом случае в первую очередь следует попытаться очистить файл, чтобы восстановить его первоначальное состояние. Если файл содержит только вредоносный код, его следует удалить.

Если зараженный файл заблокирован или используется системным процессом, его удаление возможно только после его освобождения. Это обычно происходит после перезапуска системы.

Удаление файлов из архивов

По умолчанию архив удаляется целиком, если содержит только зараженные файлы и не содержит файлов без вредоносного кода. Другими словами, архивы, которые содержат незараженные файлы, не удаляются. Тем не менее при сканировании в режиме «Тщательная очистка» архив удаляется, если содержит как минимум один зараженный файл, независимо от состояния других файлов в архиве.

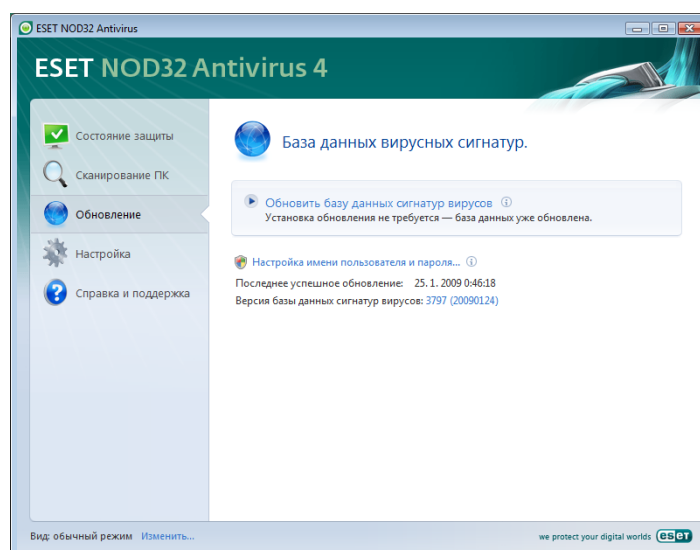
4.2 Обновление программы

Регулярные обновления системы являются основой для обеспечения максимально возможного уровня безопасности, который предоставляется антивирусом ESET NOD32. Модуль обновления предназначен для получения регулярных обновлений программы. При этом обновляются как базы данных сигнатур вирусов, так и компоненты системы.

Для получения сведений о текущем состоянии обновления, в том числе о текущей версии базы данных сигнатур вирусов и о необходимости выполнить обновление, выберите пункт **«Обновление»**. Можно также запустить процесс обновления немедленно с помощью функции **«Обновить базу данных сигнатур вирусов»**. Кроме того, там расположены основные параметры обновления, например имя пользователя и пароль для доступа к серверам обновлений компании ESET.

Информационная часть содержит такие полезные данные, как дата и время последнего удачного обновления и количество вирусов, информация о которых содержится в базе данных сигнатур. Числовой индикатор является активной ссылкой на список всех сигнатур, добавленных в базу в текущем обновлении, который расположен на веб-сайте компании ESET.

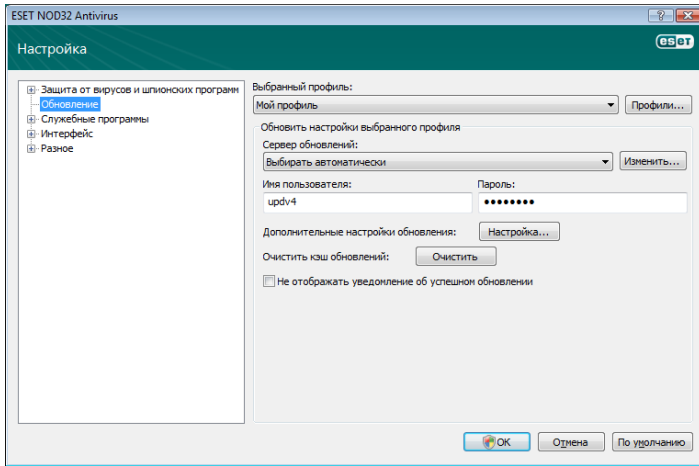
Для того чтобы получить доступ к форме регистрации новой лицензии в компании ESET и получить данные аутентификации по электронной почте, воспользуйтесь ссылкой **«Зарегистрировать»**.



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

4.2.1 Настройка обновлений

Раздел параметров обновления содержит информацию об источниках обновлений, такую как адреса серверов обновлений и данные аутентификации для этих серверов. По умолчанию поле **«Сервер обновлений»** содержит значение **«Выбирать автоматически»**. Это означает, что все файлы обновлений будут автоматически загружаться с сервера компании ESET в моменты наименьшей загрузки сети. Параметры обновлений доступны в дереве «Дополнительные настройки» (F5), в разделе **«Обновление»**.



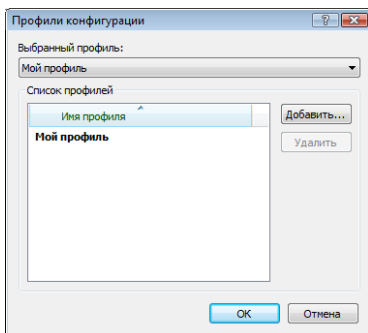
Список существующих серверов обновлений доступен в раскрывающемся меню **«Сервер обновлений»**. Для того чтобы добавить новый сервер обновлений, в разделе **«Обновить настройки выбранного профиля»** нажмите **«Изменить»**, а затем нажмите кнопку **«Добавить»**.

Аутентификация на серверах обновлений осуществляется с помощью **имени пользователя** и **пароля**, которые формируются автоматически и отправляются пользователю при приобретении лицензии на использование программы.

4.2.1.1 Профили обновлений

Для различных наборов параметров обновления можно создавать пользовательские профили, которые будут использоваться для заданной задачи обновления. Создание различных профилей особенно необходимо для пользователей портативных компьютеров, так как в этом случае параметры подключения к Интернету постоянно изменяются. С помощью настройки задачи обновления пользователь портативного компьютера может указать альтернативный профиль обновления, который используется, если не удалось выполнить обновление с основным, указанным в разделе **«Мой профиль»**.

В раскрывающемся меню **«Выбранный профиль»** отображается текущий выбранный профиль. По умолчанию отображается профиль, указанный в поле **«Мой профиль»**. Для создания нового профиля нажмите кнопку **«Профили»**, затем кнопку **«Добавить»** и введите выбранное **«Имя профиля»**. При создании профиля можно скопировать параметры из уже существующего профиля с помощью команды меню **«Копировать настройки профиля»**.



В параметрах профиля можно указать сервер обновлений, с которого программа будет загружать обновления. Доступен выбор любого сервера из списка или настройка нового. Список существующих серверов обновлений доступен в раскрывающемся меню **«Сервер обновлений»**. Для того чтобы добавить новый сервер, в разделе **«Обновить настройки выбранного профиля»** нажмите кнопку **«Изменить»**, а затем нажмите кнопку **«Добавить»**.

4.2.1.2 Дополнительные настройки обновления

Для просмотра **дополнительных настроек обновления** нажмите кнопку **«Настройки»**. Дополнительные настройки обновлений включают в себя параметры **режима обновления, прокси HTTP, подключения к локальной сети и сервера зеркалирования**.

4.2.1.2.1 Режим обновления

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

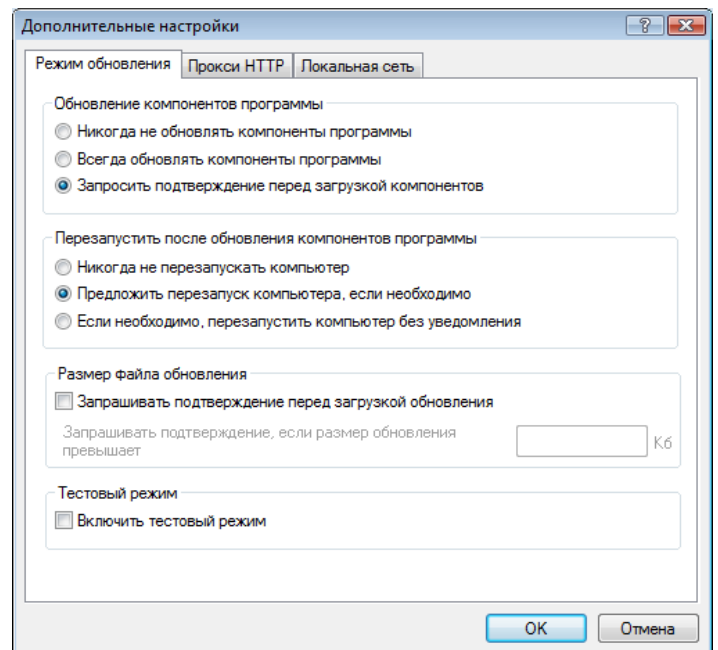
В разделе **«Обновление компонентов программы»** доступны три варианта:

- **«Никогда не обновлять компоненты программы»;**
- **«Всегда обновлять компоненты программы»;**
- **«Запросить подтверждение перед загрузкой компонентов».**

Если выбран вариант **«Никогда не обновлять компоненты программы»**, то при выпуске компанией ESET обновлений компонентов они не будут загружаться. В результате ни один из компонентов программы на компьютере пользователя обновляться не будет. Если выбран вариант **«Всегда обновлять компоненты программы»**, то программа обновляется всегда при появлении новых доступных обновлений на серверах ESET. При этом компоненты программы будут обновлены сразу же после загрузки.

Если выбран вариант **«Запросить подтверждение перед загрузкой компонентов»**, то программа запрашивает у пользователя подтверждение загрузки обновлений программных компонентов при их появлении на серверах компании. В этом случае открывается диалоговое окно, содержащее информацию о новых обновлениях. В этом окне можно подтвердить обновление или отказаться от него. Если пользователь разрешает обновление, начинается процесс загрузки и обновления программных компонентов.

По умолчанию выбран вариант **«Запросить подтверждение перед загрузкой компонентов»**.



После установки обновления программных компонентов необходима перезагрузка системы, чтобы изменения вступили в силу и все модули заработали должным образом. В разделе **«Перезапустить после обновления компонентов программы»** можно выбрать один из трех вариантов:

- **«Никогда не перезапускать компьютер»;**
- **«Предложить перезапуск компьютера, если необходимо»;**

- «Если необходимо, перезапустить компьютер без уведомления».

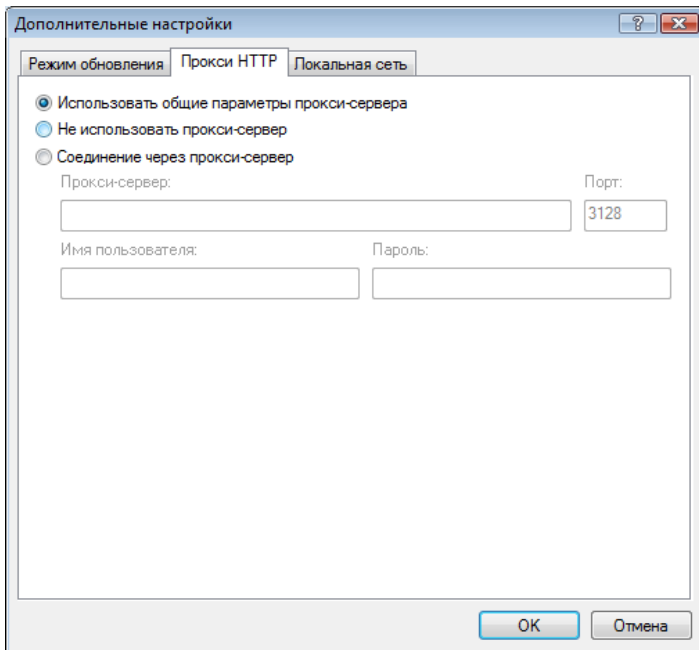
По умолчанию выбран вариант «Предложить перезапуск компьютера, если необходимо». Выбор наиболее приемлемых параметров для обновлений программных компонентов на вкладке «Режим обновления» зависит от многих факторов и условий эксплуатации компьютера. Необходимо помнить о том, что существует разница между рабочими станциями и серверами. Например, перезагрузка сервера в автоматическом режиме после обновления программы может привести к серьезным проблемам.

4.2.1.2.2 Прокси-сервер

Для получения доступа к параметрам прокси-сервера для выбранного профиля обновления выполните следующие действия: выберите пункт «Обновление» в дереве «Дополнительные настройки» (F5), а затем нажмите кнопку «Настройки» справа от элемента «Дополнительные настройки обновления». На вкладке «Прокси HTTP» можно выбрать один из трех вариантов:

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

Если выбран вариант «Использовать общие параметры прокси-сервера», применяются параметры прокси-сервера, указанные в дереве расширенных параметров в ветке «Разное» > «Прокси-сервер».



Выберите вариант «Не использовать прокси-сервер», чтобы явно указать на то, что прокси-сервер при обновлении антивируса ESET NOD32 не используется.

Вариант «Соединение через прокси-сервер» следует выбирать в том случае, если для обновления антивируса ESET NOD32 нужно использовать прокси-сервер, параметры которого отличаются от указанных в общих параметрах программы («Разное» > «Прокси-сервер»). Если выбран этот вариант, укажите следующие параметры: адрес прокси-сервера, порт обмена данными, а также имя пользователя и пароль для авторизации (при необходимости).

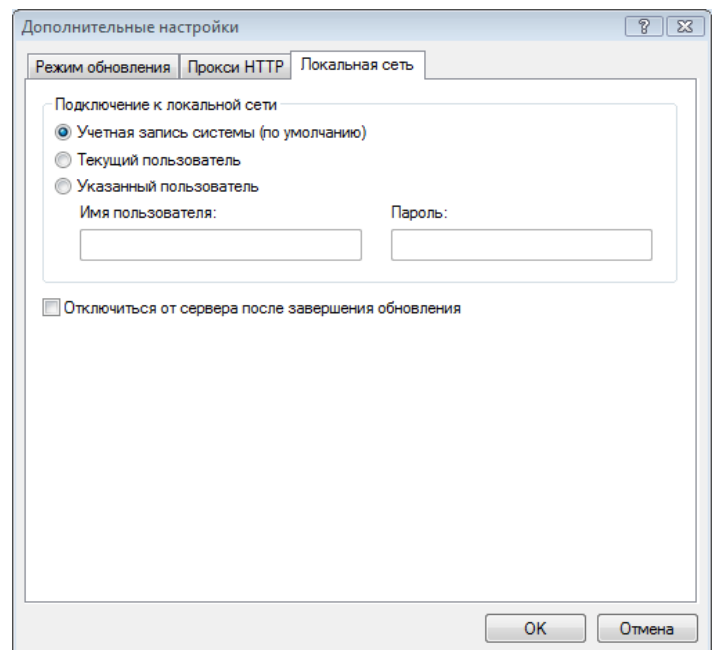
Этот вариант используется также в случае, если в общих параметрах прокси-сервер не указан, но модуль обновления антивируса ESET NOD32 подключается к Интернету через прокси-сервер.

По умолчанию установлен вариант «Использовать общие параметры прокси-сервера».

4.2.1.2.3 Подключение к локальной сети

При обновлении с сервера локальной сети средствами операционной системы на основе NT по умолчанию требуется аутентификация всех сетевых соединений. Чаще всего прав локальной системной учетной записи недостаточно для доступа к папке на сервере, в которой хранятся файлы обновлений. В этом случае введите имя пользователя и пароль в разделе параметров обновления или укажите уже существующую учетную запись, которая позволит программе получить доступ к обновлениям.

Для того чтобы настроить такую учетную запись, перейдите на вкладку «Локальная сеть». Раздел «Подключение к локальной сети» содержит параметры «Учетная запись системы (по умолчанию)», «Текущий пользователь» и «Указанный пользователь».



Выберите вариант «Учетная запись системы», 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 данные аутентификации текущего пользователя, выберите пункт «Текущий пользователь». Недостаток этого метода состоит в том, что программа не может подключиться к серверу, если в текущий момент пользователей на компьютере нет.

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

По умолчанию значением параметра подключения к локальной сети является «Учетная запись системы».

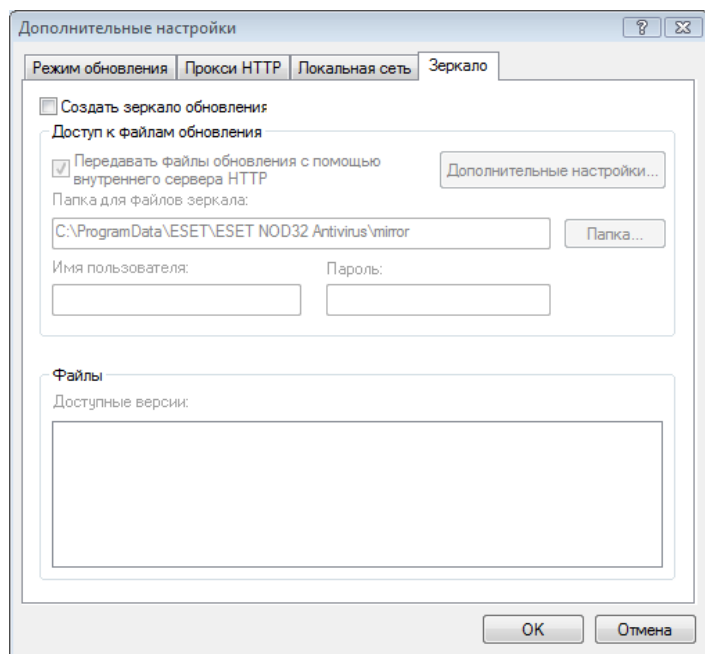
Предупреждение.

Если выбран вариант «Текущий пользователь» или «Указанный пользователь», может произойти ошибка при изменении учетной записи программы. Поэтому на главной странице параметров обновления рекомендуется указывать данные аутентификации пользователя локальной сети. В этом разделе параметров обновлений укажите данные аутентификации следующим образом: домен\имя_пользователя (а для рабочей группы: рабочая_группа\имя_пользователя) и пароль. При обновлении по протоколу HTTP с сервера локальной сети аутентификации не требуется.

4.2.1.2.4 Создание зеркала обновлений

Антивирус ESET NOD32 Business Edition позволяет пользователю создавать копии файлов обновления, которые могут использоваться для обновлений других рабочих станций в сети. Обновление рабочих станций с зеркала оптимизирует трафик во внутренней сети и сокращает нагрузку на внешний канал в Интернет.

Параметры зеркала в локальной сети доступны в разделе «Дополнительные настройки обновления» (если указан правильный лицензионный ключ в менеджере лицензий, который расположен в разделе дополнительных настроек программы ESET NOD32 Antivirus Business Edition). Для доступа к этому разделу нажмите клавишу F5 и щелкните элемент «Обновление» в дереве расширенных параметров. Затем нажмите кнопку «Настройки» рядом с элементом «Дополнительные настройки обновления» и выберите вкладку «Зеркало».



На первом шаге настройки зеркала обновлений установите флажок «Создать зеркало обновления». После этого становятся доступны другие параметры, такие как способ доступа к файлам обновлений и путь к файлам в системе.

Методы организации зеркала обновлений подробно описаны в главе «Варианты доступа к зеркалу обновлений». Существует два основных варианта доступа к файлам зеркала обновлений. Папка обновлений может быть представлена как папка общего доступа сети NT или как зеркало сервера HTTP.

Папка, предназначенная для хранения файлов обновлений, указывается в разделе «Папка для дублируемых файлов». Нажмите кнопку «Папка» для выбора папки на локальном компьютере или папки общего доступа в сети. При необходимости авторизации данные аутентификации могут быть указаны в полях «Имя пользователя» и «Пароль». Имя пользователя и пароль должны быть указаны в формате *домен/имя_пользователя* или *рабочая_группа/имя_пользователя*. Не забудьте ввести соответствующие пароли.

При подробной настройке зеркала пользователь может указать языковые версии продуктов, для которых необходимо получать обновления. Языковые версии доступны в разделе «Файлы» > «Доступные версии».

4.2.1.2.4.1 Обновление с зеркала

Существует два основных способа доступа к файлам зеркала обновлений – папка обновлений может быть представлена как папка общего доступа сети NT или как зеркало сервера HTTP.

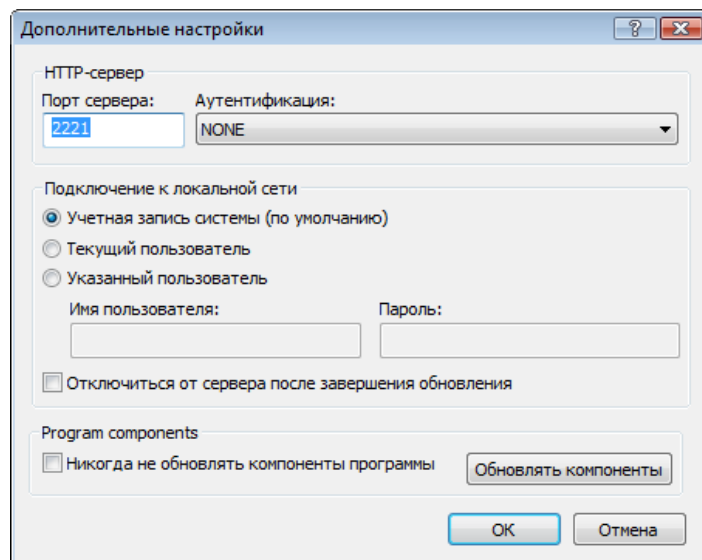
Доступ к файлам зеркала с помощью внутреннего сервера HTTP

Этот способ заранее задан в конфигурации программы и используется по умолчанию. Для предоставления доступа к файлам обновлений с помощью сервера HTTP перейдите в раздел «Дополнительные настройки обновления» (вкладка «Зеркало») и установите флажок «Создать зеркало обновления».

В разделе «Дополнительные настройки» вкладки «Зеркало» можно указать «Порт сервера», через который сервер HTTP будет принимать запросы на соединение, а также настроить параметр «Аутентификация» для использования сервером HTTP. По умолчанию параметр «Порт сервера» имеет значение 2221. Параметр «Аутентификация» определяет метод аутентификации пользователя для доступа к файлам обновлений. Доступны следующие варианты: «Нет», Basic и NTLM. Для того чтобы использовать кодирование base64 и упрощенную аутентификацию по имени пользователя и паролю, выберите Basic. Аутентификация NTLM использует возможности протокола NTLM повышенной безопасности компании Microsoft. Для аутентификации используется учетная запись пользователя, который предоставляет доступ к файлам общего использования. По умолчанию задано значение «Нет». Это дает возможность получать обновления без аутентификации.

Предупреждение.

Если планируется организовать доступ к файлам с помощью сервера HTTP, папка с копиями обновлений должна находиться на том же компьютере, что и экземпляр антивируса ESET NOD32, который ее создает.



После настройки зеркала обновлений укажите на рабочих станциях адрес нового сервера обновлений в формате **http://IP_адрес_сервера:2221**. Для этого выполните следующие действия:

- откройте «Дополнительные параметры антивируса ESET NOD32» и выберите ветку «Обновление»;
- справа от раскрывающегося меню «Сервер обновлений» нажмите кнопку «Изменить» и добавьте новый сервер в формате: `http://IP_адрес_нового_сервера:2221`;
- выберите новый сервер из списка серверов.

Доступ к файлам обновлений средствами общего доступа

Сначала необходимо создать папку общего доступа на локальном или сетевом диске. 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 антивируса ESET NOD32 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». Эта функция включена по умолчанию после установки программы.

Если папка общего доступа расположена на другом компьютере в сети, необходимо указать данные аутентификации для доступа к этому компьютеру. Для этого откройте раздел «Дополнительные параметры антивируса ESET NOD32» (F5) и перейдите в ветку «Обновление». Нажмите кнопку «Настройки» и перейдите на вкладку «Локальная сеть». Этот параметр настраивается так же, как описано в главе «Подключение к локальной сети».

После окончания настройки зеркала укажите на рабочих станциях адресного сервера обновлений в формате \\UNC-ИМЯ_КОМПЬЮТЕРА\ПУТЬ. Для этого выполните следующие действия:

- откройте расширенные параметры антивируса ESET NOD32 и нажмите «Обновление»;
- в разделе «Сервер обновлений» нажмите «Изменить» и добавьте новый сервер в формате \\UNC-ИМЯ_КОМПЬЮТЕРА\ПУТЬ;
- выберите новый сервер из списка серверов.

ПРИМЕЧАНИЕ: Путь к зеркалу в этом случае указывается в формате UNC. Обновления с сетевых дисков могут не работать.

4.2.1.2.4.2 Устранение неполадок при обновлении с зеркала

В зависимости от способа доступа к папке обновлений могут возникать различные проблемы. В большинстве случаев проблемы вызваны одной или несколькими из следующих причин: неверное указание расположения файлов обновлений в системе, неверные данные аутентификации для доступа к файлам обновлений, неверные параметры обновляемой программы на рабочих станциях, а также комбинация этих причин. Ниже приведен краткий обзор проблем, наиболее часто возникающих при обновлении с зеркала.

- **Ошибка при подключении антивируса ESET NOD32 к серверу зеркала** — обычно происходит при указании неправильных данных сервера обновлений (сетевое пути к папке обновлений) на рабочей станции, с которой осуществляется доступ. Для того чтобы проверить путь к папке, откройте в Windows меню «Пуск», затем нажмите «Выполнить», введите или скопируйте путь в открывшееся окно и нажмите **ОК**. Должна открыться папка обновлений.
- **При попытке обновления антивирус ESET NOD32 запрашивает имя пользователя и пароль** — неправильно введены данные аутентификации (имя пользователя и пароль) в разделе параметров обновлений. Имя пользователя и пароль используются для доступа к серверу обновлений, с которого программа загружает файлы обновлений. Убедитесь в том, что данные аутентификации указаны верно и в правильном формате. Например, имя пользователя в формате «Домен/Имя» или «Рабочая группа/Имя» и соответствующий пароль. Если зеркало сервера обновлений доступно 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, указание доменного имени пользователя и пароля в настройках обновления необходимо.
- **Ошибка при подключении антивируса ESET NOD32 к серверу зеркала** – обмен данными по указанному порту подключения к серверу обновлений HTTP блокируется.

4.2.2 Создание задач автоматического обновления

Обновление может быть запущено вручную с помощью функции «Обновить базу данных сигнатур вирусов» в информационном окне после выбора пункта «Обновление» в главном меню.

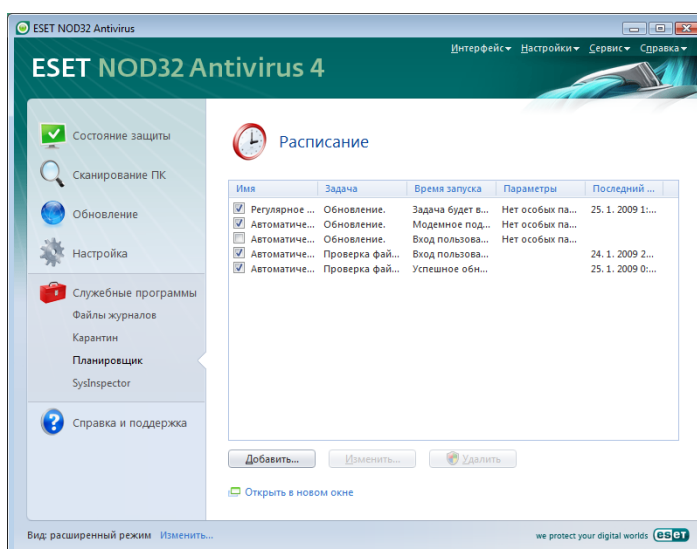
Обновления могут запускаться по расписанию: для планирования задач обновлений перейдите в раздел «Служебные программы» > «Планировщик». По умолчанию в антивирусе ESET NOD32 сформированы следующие задачи:

- «Регулярное автоматическое обновление»;
- «Автоматическое обновление после установки модемного соединения»;
- «Автоматическое обновление после входа пользователя в систему».

Каждая из перечисленных выше задач может быть настроена под текущие нужды пользователя. Кроме задач по умолчанию пользователь может создавать новые задачи обновления и определять их настройки. Дополнительную информацию о создании и настройке задач обновления см. в главе «Планировщик».

4.3 Планировщик

Планировщик доступен, если включен расширенный режим антивируса ESET NOD32. Для доступа к **планировщику** в главном меню антивируса ESET NOD32 откройте раздел «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 установки модемного соединения»;
- «Автоматическое обновление после входа пользователя в систему»;
- «Автоматическая проверка файлов, исполняемых при запуске системы»;
- «Автоматическая проверка файлов после обновления базы данных сигнатур вирусов».

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».

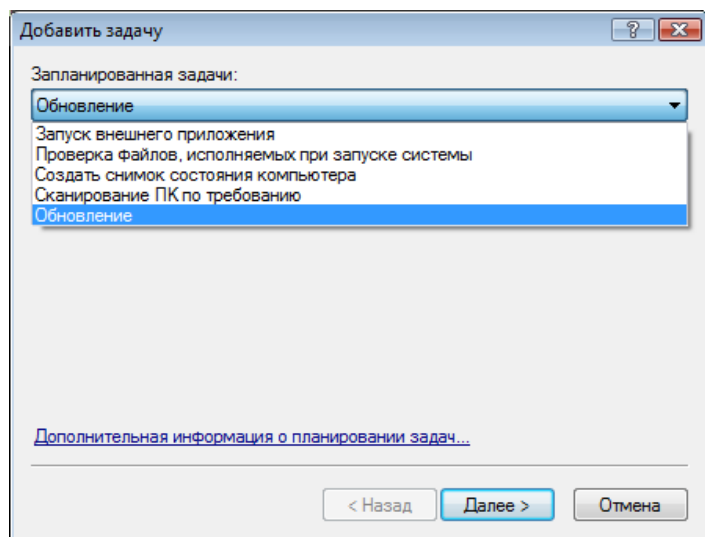
4.3.1 Назначение запланированных задач

Планировщик управляет задачами и запускает их по расписанию с predetermined параметрами. Параметры содержат информацию, такую как дата и время исполнения, а также профили обновления, которые используются во время выполнения задачи.

4.3.2 Создание новой задачи

Для того чтобы создать новую задачу в планировщике, нажмите кнопку **«Добавить»** или щелкните правой кнопкой мыши и выберите команду **«Добавить»** в контекстном меню. Доступны пять типов задач:

- **«Запуск внешнего приложения»;**
- **«Обслуживание журнала»;**
- **«Проверка файлов, исполняемых при запуске системы»;**
- **«Сканирование компьютера по требованию»;**
- **«Обновление».**



Так как наиболее часто используемыми задачами являются **«Сканирование компьютера по требованию»** и **«Обновление»**, ниже описано создание задачи обновления.

В раскрываемом меню **«Запланированные задачи»** выберите пункт **«Обновление»**. Нажмите кнопку **«Далее»** и введите название задачи в поле **«Название задачи»**. Выберите частоту запуска задачи. Доступны следующие варианты: **«Однократно»**, **«Многократно»**, **«Ежедневно»**, **«Еженедельно»** и **«При определенных условиях»**. В зависимости от указанной частоты запуска будут запрошены различные параметры обновления. Далее укажите, какое действие следует предпринять, если задача не выполнена или не завершена успешно 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»** (при выборе этого варианта доступна настройка параметра **«Интервал времени»**).

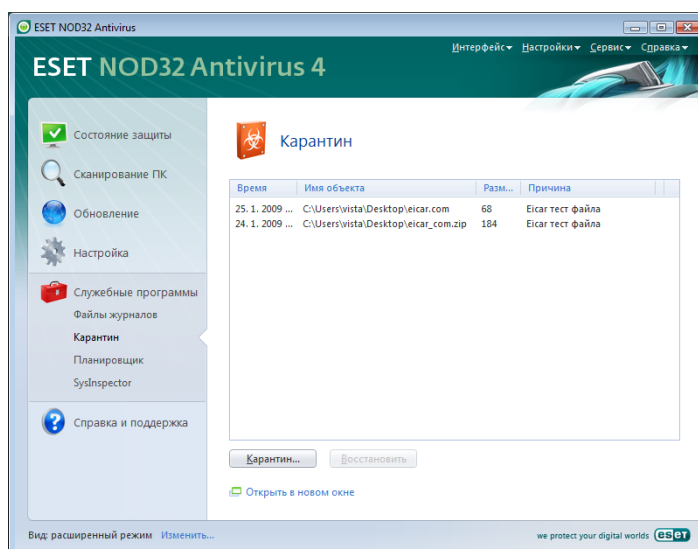
На следующем шаге отображается окно сводной информации о текущей планируемой задаче. Пункт **«Запустить задачу с указанными параметрами»** автоматически выбран. Нажмите кнопку **«Готово»**.

В открывшемся окне выберите профиль, используемый при выполнении задачи. Можно выбрать основной профиль и альтернативный, который будет использоваться, если запуск задачи с помощью основного профиля пройдет неудачно. Подтвердите настройки, нажав кнопку **ОК** в окне профиля обновления. Новая задача появится в списке запланированных.

4.4 Карантин

Главное назначение карантина состоит в изоляции и безопасном хранении зараженных файлов. Файлы должны помещаться на карантин, если они не могут быть вылечены или безопасно удалены, или если удаление не рекомендуется, или если они ошибочно отнесены антивирусом ESET NOD32 к зараженным.

Пользователь может поместить на карантин любой файл по выбору. Рекомендуется помещать на карантин файлы с подозрительной активностью, которые, тем не менее, не определяются модулем сканирования как зараженные. Изолированные файлы могут быть переданы в лабораторию ESET для дальнейшего анализа.



Информация о файлах, помещенных на карантин, находится в таблице. Она содержит дату и время помещения на карантин, путь к исходному расположению файла в системе, его размер в байтах, причину помещения на карантин (**помещен пользователем**) и количество обнаруженных вирусов (полезно, если файл содержит несколько вирусов).

4.4.1 Перемещение файлов на карантин

Программа автоматически помещает удаленные файлы на карантин (если эта функция не отключена пользователем). Любой подозрительный файл можно поместить на карантин вручную с помощью кнопки **«Карантин»**. При этом исходная копия файла не удаляется. Контекстное меню, которое также может использоваться для этих целей, доступно в окне карантина и содержит пункт **«Добавить»**.

4.4.2 Восстановление из карантина

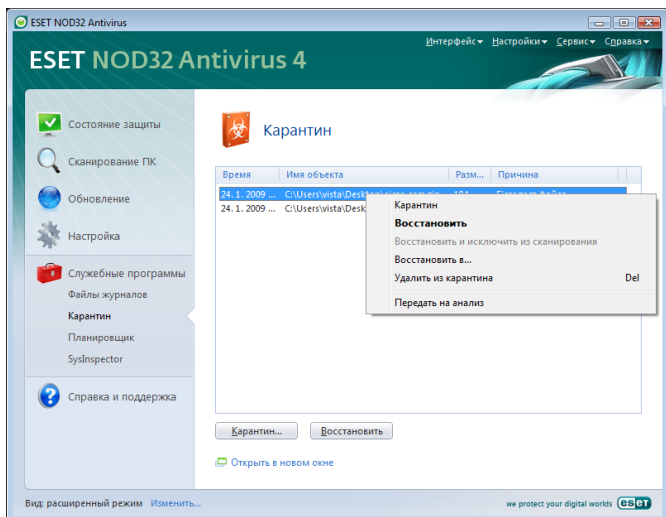
Изолированные файлы могут быть восстановлены в исходное местоположение в системе. Для этого предназначена функция **«Восстановить»**, доступная в контекстном меню окна карантина. Кроме того, контекстное меню содержит функцию **«Восстановить в»**, которая позволяет восстанавливать файлы в другое местоположение, отличное от исходного.

ПРИМЕЧАНИЕ:

Если программа поместила файл на карантин по ошибке, исключите файл из процесса сканирования и отправьте образец в службу поддержки клиентов ESET с соответствующими пояснениями.

4.4.3 Передача 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. Для того чтобы передать файл из карантина, выберите его и используйте пункт **«Передать на анализ»** контекстного меню.

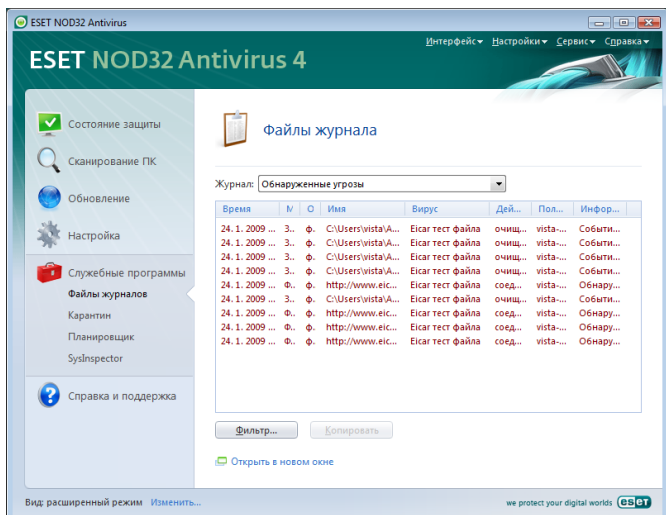


4.5 Файлы журнала

Файлы журнала содержат информацию о важных произошедших программных событиях и позволяют просматривать сводную информацию об обнаруженных угрозах. Регистрация событий является важнейшим инструментом для анализа, обнаружения угроз и поиска неисправностей. Ведение журнала выполняется в фоновом режиме без вмешательства пользователя. Данные сохраняются в соответствии с текущими параметрами степени детализации журнала. Просмотр текстовых сообщений и файлов журнала, а также их архивирование могут осуществляться непосредственно в среде антивируса ESET NOD32.

Получить доступ к файлам журнала можно в главном окне антивируса ESET NOD32 с помощью команды меню «Служебные программы» > «Файлы журнала». Укажите необходимый тип журнала в меню «Журнал», которое находится в верхней части окна. Ниже перечислены доступные журналы.

1. «Обнаруженные угрозы» — используется для просмотра всех данных о событиях, имеющих отношение к обнаружению проникновений.
2. «События» — этот журнал предназначен для решения проблем системными администраторами и пользователями. Все важные действия антивируса ESET NOD32 регистрируются в этом журнале.
3. «Сканирование по требованию» — в этом окне отображаются результаты всех выполненных процессов сканирования. Чтобы получить подробную информацию о том или ином сканировании по требованию, дважды нажмите соответствующую запись.

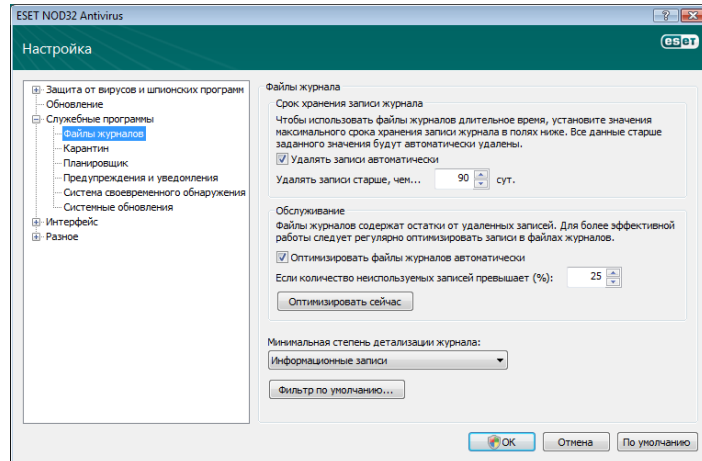


Чтобы скопировать в буфер обмена информацию из любого раздела журнала, выберите необходимую запись и нажмите кнопку «Копировать». Для выбора нескольких записей используйте клавиши CTRL и SHIFT.

4.5.1 Обслуживание журнала

Параметры ведения журнала антивируса ESET NOD32 доступны из главного окна программы. Перейдите к разделу «Настройки» > «Ввод всего дерева расширенных параметров» > «Служебные программы» > «Файлы журналов». Можно задать параметры, перечисленные ниже.

- «Удалять записи автоматически»: записи старше указанного количества суток автоматически удаляются.
- «Оптимизировать файлы журналов автоматически»: включает автоматическую дефрагментацию файлов журнала, если указано предельное содержание неиспользуемых записей в процентах.
- «Минимальная степень детализации журнала»: задает степень детализации журнала. Доступные параметры:
 - «Критические ошибки» — регистрировать только сведения о критических ошибках (ошибка запуска защиты от вирусов и т. д.);
 - «Ошибки» — регистрировать только информацию о критических ошибках и ошибках типа «Ошибка загрузки файла»;
 - «Предупреждения» — регистрировать информацию обо всех критических ошибках, ошибках и предупреждениях;
 - «Информационные записи» — регистрировать все информационные сообщения, включая сообщения о выполненных обновлениях, и все сообщения, описанные выше;
 - «Диагностические записи» — регистрировать всю информацию, необходимую для тонкой настройки программы, и все сообщения, описанные выше.



4.6 Интерфейс пользователя

Пользовательский интерфейс антивируса ESET NOD32 можно настроить под собственные нужды. Параметры интерфейса доступны в ветке «Интерфейс» дерева расширенных параметров антивируса ESET NOD32.

При необходимости в разделе «Элементы интерфейса» пользователи могут переключаться в расширенный режим. Расширенный режим предоставляет доступ к большему числу параметров и функций антивируса ESET NOD32.

Графический интерфейс пользователя может быть отключен, если отображение графических элементов значительно влияет на быстродействие компьютера или вызывает другие проблемы. Кроме того, графический интерфейс пользователя может быть отключен, если отображение графических элементов мешает восприятию для пользователей с ослабленным зрением, так как он может конфликтовать со специальными приложениями, используемыми для работы с текстом.

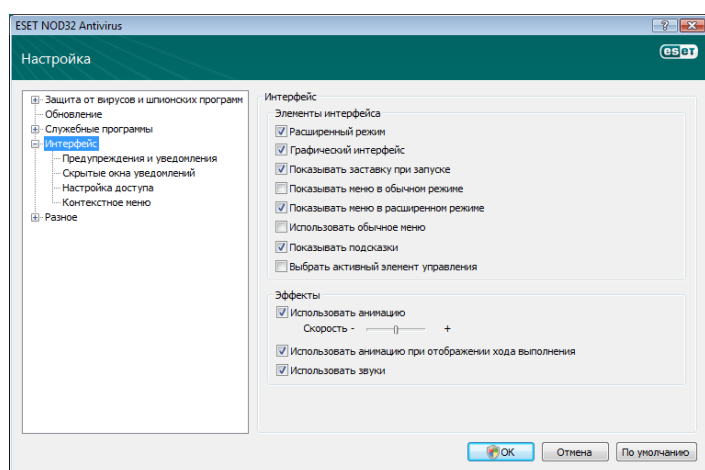
Можно отключить заставку антивируса ESET NOD32, сняв флажок «Показывать заставку при запуске».

В верхней части экрана антивируса ESET NOD32 располагается обычное меню, которое может быть включено или отключено с помощью параметра «Использовать обычное меню».

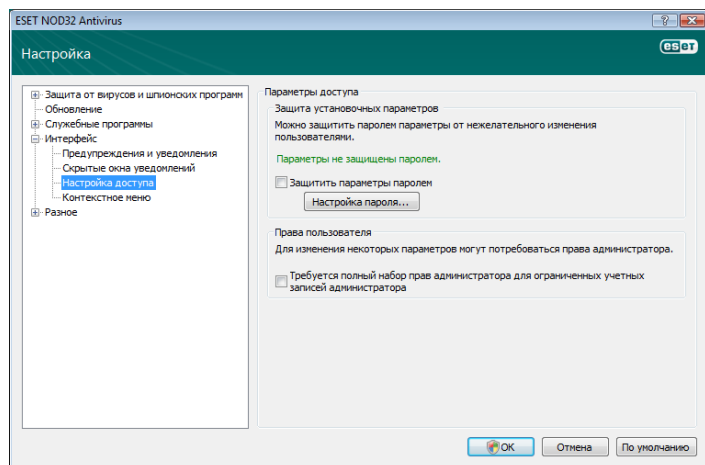
Если установлен флажок «Показывать подсказки», при наведении курсора на элемент управления отображается краткое описание. Параметр «Выбрать активный элемент управления» предназначен для выделения элементов управления при наведении на них курсора мыши. Выделенный элемент будет активирован при щелчке клавиши мыши.

Для того чтобы изменить скорость анимации интерфейса, установите флажок «Использовать анимацию» и передвиньте ползунок «Скорость» вправо или влево.

Для того чтобы включить анимацию значков, отображающих выполнение различных операций, установите флажок «Использовать анимацию при отображении хода выполнения». Можно включить звуковые уведомления о важных событиях, установив флажок «Использовать звуки».



Параметры **пользовательского интерфейса** позволяют указать пароль для доступа к параметрам антивируса ESET NOD32. Эта функция располагается в подменю «Защита параметров» меню «Интерфейс». Для максимальной безопасности системы программа должна быть правильно настроена. Несанкционированное изменение параметров может привести к потере важных данных. Для того чтобы установить защиту параметров паролем, нажмите кнопку «Введите пароль».



4.6.1 Предупреждения и уведомления

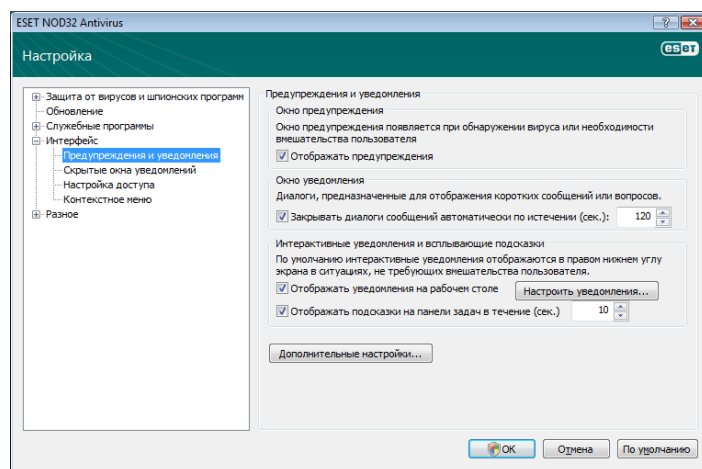
В разделе «Предупреждения и уведомления» меню «Интерфейс» можно настраивать порядок уведомления пользователя о появлении угроз.

Первый пункт – это «**Окно предупреждения**». Если соответствующий флажок снят, окна предупреждений не отображаются. Такой режим подходит только для узкого круга особых ситуаций. Не рекомендуется изменять этот параметр без крайней необходимости; лучше оставить его значение по умолчанию (включено).

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

Уведомления на рабочем столе и всплывающие подсказки являются информационными и не требуют участия пользователя. Они отображаются в области уведомлений в правой нижней части экрана. Для того чтобы включить уведомления на рабочем столе, установите флажок «**Отображать уведомления на рабочем столе**». Более подробные параметры – время отображения и прозрачность окна – доступны с помощью кнопки «**Конфигурация уведомлений**».

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



Выберите пункт «**Дополнительные настройки**» для настройки дополнительных параметров **предупреждений и уведомлений**, в том числе параметра «**Отображать уведомления только при необходимости вмешательства**». Он позволяет включать или выключать отображение уведомлений, которые не требуют вмешательства со стороны пользователя. Установите флажок «Отображать только требующие вмешательства пользователя уведомления при запуске приложений в полноэкранном режиме» для подавления всех сообщений, не требующих ответа пользователя. Раскрывающееся меню «Минимальная степень детализации сообщений» предназначено для выбора минимального уровня серьезности предупреждений и уведомлений, которые должны отображаться на экране.

Последний параметр этого раздела предназначен для определения адресатов уведомлений в многопользовательской среде. В поле «**В многопользовательских системах отображать уведомления для пользователя**» можно указать пользователя, который будет получать важную информацию о работе антивируса ESET NOD32 4. Обычно это системный или сетевой администратор. Эта функция особенно полезна для терминальных серверов, в которых все уведомления предназначаются администратору.

4.7 ThreatSense.Net

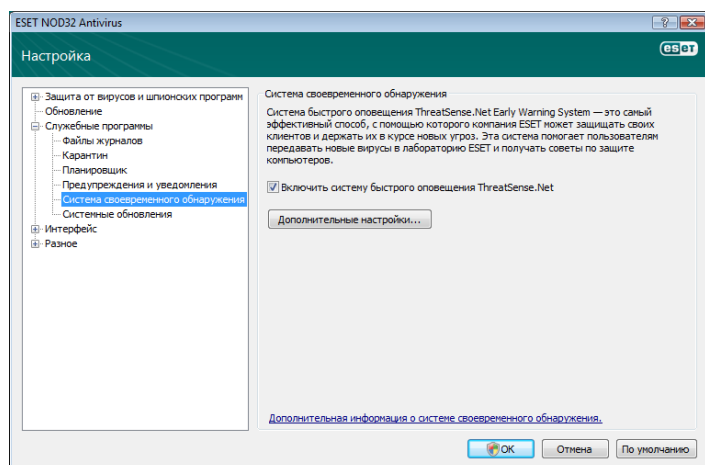
Система своевременного обнаружения ThreatSense.Net является инструментом немедленного и быстрого информирования компании ESET о появлении новых угроз. Действующая в обоих направлениях система своевременного обнаружения имеет единственное предназначение — сделать защиту компьютера пользователя еще более надежной. Лучшим способом обнаружить новые угрозы сразу после их появления является сбор информации от как можно большего числа пользователей для дальнейшего использования собранных данных в продуктах защиты. Существует два варианта, описанных ниже.

1. Пользователь отключает систему своевременного обнаружения. При этом пользователь не теряет никаких возможностей программы, и его компьютер защищен настолько хорошо, насколько это возможно.
2. Пользователь разрешает системе своевременного обнаружения передавать анонимную информацию о появлении новых угроз и, если угрозы обнаружены, отправлять файл, содержащий злонамеренный код. Файл передается в лабораторию ESET для тщательного анализа. Изучение этих угроз поможет компании ESET обновить средства обнаружения угроз. Система своевременного обнаружения собирает анонимную информацию о компьютерах пользователей, которая может иметь отношение к недавно появившимся угрозам. Эта информация может содержать образец кода или копию файла, в котором появилась угроза, путь к местоположению файла, имя файла, дату и время обнаружения, имя процесса, в котором обнаружена угроза, и информацию об операционной системе пользователя. Некоторые из этих данных могут содержать личную информацию о пользователе, например имя пользователя в названиях папок и тому подобные случайные включения личных данных. Пример передаваемой информации приведен в этом справочном документе.

Так как существует вероятность того, что в отправляемую информацию непреднамеренно могут попасть личные сведения о пользователе и его компьютере, компания ESET заверяет, что передаваемая информация не будет использована ни в каких иных целях, кроме целей раннего обнаружения новых угроз.

По умолчанию антивирус ESET NOD32 запрашивает разрешение на передачу подозрительных файлов в лабораторию ESET. Файлы с такими расширениями, как DOC или XLS, не передаются, даже если в них обнаружены угрозы. Можно указать любые другие типы файлов, которые следует исключить из передачи.

Параметры системы своевременного обнаружения доступны в разделе дерева расширенных настроек «**Службные программы**» > «**Система своевременного обнаружения**». Установите флажок «**Включить систему своевременного обнаружения**». Это позволит активировать функцию. Затем нажмите кнопку «**Дополнительные настройки**».

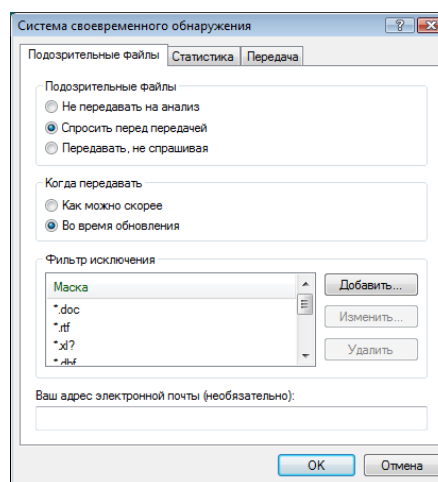


4.7.1 Подозрительные файлы

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

Если пользователь выявил подозрительный файл, он может передать его в лабораторию компании для дальнейшего анализа. Если файл содержит злонамеренный код, информация о нем будет включена в следующую версию базы данных сигнатур вирусов.

Передача файлов может выполняться автоматически. Если выбрана эта функция, подозрительные файлы отправляются в фоновом режиме. Для того чтобы знать, какие файлы отправляются для анализа, и подтверждать их отправку, выберите пункт «**Спросить перед передачей**».



Чтобы запретить передачу файлов, выберите пункт «**Не передавать на анализ**». Примечание: запрет на передачу файлов не влияет на передачу статистической информации в ESET. Передача статистики настраивается в отдельном разделе, который описан в следующей главе.

Когда передавать

Подозрительные файлы передаются в лабораторию ESET при первой же возможности. Рекомендуется использовать выделенное подключение к Интернету. В этом случае подозрительные файлы будут передаваться без задержек. Можно передавать подозрительные файлы **во время обновления**. Если выбрана эта функция, подозрительные файлы будут накапливаться и загружаться на серверы лаборатории ESET во время обновления.

Фильтр исключения

Не все файлы должны передаваться в лабораторию ESET. Фильтр исключения позволяет исключить из передачи определенные файлы или папки. Например, можно исключить файлы, содержащие конфиденциальную информацию (документы или электронные таблицы). Самые распространенные типы файлов исключены по умолчанию (Microsoft Office, OpenOffice). При необходимости список исключений можно расширить.

Адрес электронной почты

Адрес электронной почты передается в ESET вместе с подозрительным файлом и может быть использован для запроса дополнительной информации, необходимой для анализа переданных файлов. Если вопросов нет, пользователь не получит никакого ответа на передачу файлов.

4.7.2 Статистика

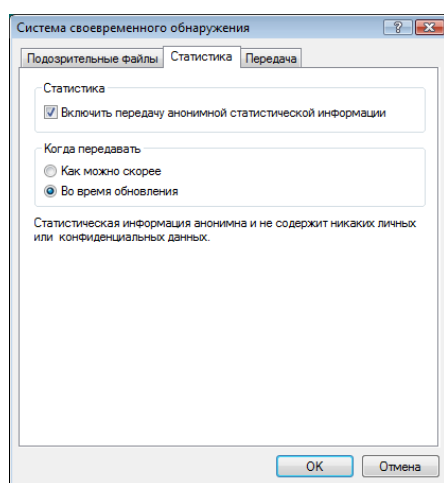
Система своевременного обнаружения ThreatSense.Net собирает анонимную информацию о компьютерах пользователей, которая может иметь отношение к недавно появившимся угрозам. Эта информация может содержать имя вируса, дату и время обнаружения, версию антивируса ESET NOD32, версию операционной системы компьютера и информацию о его расположении. Обычно статистика передается на сервер ESET один или два раза в день.

Пример передаваемого пакета со статистикой:

```
# utc_time=2005-04-14 07:21:28
# country="Russia"
# language="RUSSIAN"
# osver=5.1.2600 NT
# engine=5417
# components=2.50.2
# moduleid=0x4e4f4d41
# filesize=28368
# filename=C:\Documents and Settings\Administrator\
Local Settings\Temporary Internet Files\Content.IE5\
C14J8NS7\rdgFR1463[1].exe
```

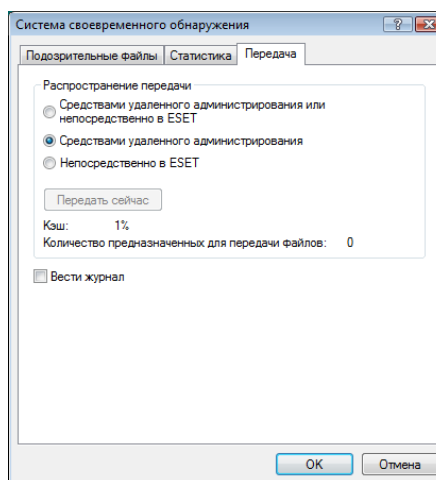
Когда передавать

В разделе «**Когда передавать**» можно настроить время передачи статистики. Если выбран вариант «**Как можно скорее**», статистическая информация отправляется сразу после создания. Этот вариант подходит для систем с постоянным подключением к Интернету. Если выбран вариант «**Во время обновления**», статистическая информация сохраняется и передается во время обновления.



4.7.3 Передача

В этом разделе можно выбрать способ передачи файлов и статистической информации средствами удаленного администрирования ESET или непосредственно в ESET. Для того чтобы подозрительные файлы и статистическая информация доставлялись в ESET, выберите параметр «**Средствами удаленного администрирования или непосредственно в ESET**». Если этот параметр установлен, файлы и статистика будут передаваться всеми доступными средствами. При передаче подозрительных файлов средствами удаленного администрирования они попадают на сервер удаленного администрирования, а затем передаются в лабораторию ESET. При выборе варианта «**Непосредственно в ESET**» подозрительные файлы и статистика отправляются программой в лабораторию ESET напрямую.



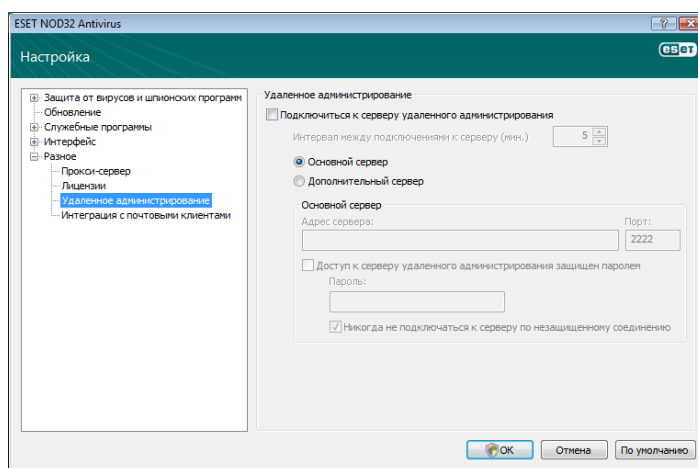
Для передачи отложенных файлов используйте кнопку «**Передать сейчас**». Нажмите эту кнопку, чтобы передать файлы и статистику незамедлительно.

Установите флажок «**Вести журнал**», чтобы включить регистрацию событий передачи информации и файлов. После каждой передачи подозрительных файлов или статистической информации создается запись в журнале событий.

4.8 Удаленное администрирование

Удаленное администрирование является мощным инструментом для поддержки политики безопасности и получения информации об общем уровне безопасности в сети. Это особенно полезно в больших сетях. Удаленное администрирование помогает не только повысить уровень безопасности, но и упростить управление антивирусом ESET NOD32 на рабочих станциях.

Настройки удаленного администрирования доступны из главного окна антивируса ESET NOD32. Перейдите к разделу «**Настройки**» > «**Ввод всего дерева расширенных параметров**» > «**Разное**» > «**Удаленное администрирование**».



Для того чтобы включить режим удаленного администрирования, в окне настроек установите флажок «**Подключиться к серверу удаленного администрирования**». Затем можно настроить нижеперечисленные параметры.

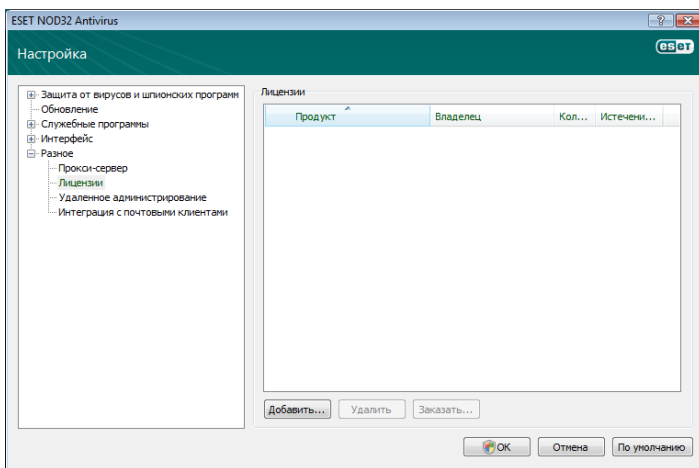
- «**Адрес сервера**» — сетевой адрес сервера удаленного администрирования.
- «**Порт**» – порт, используемый для подключения к серверу удаленного администрирования. Рекомендуется оставить порт по умолчанию – 2222.

- **«Интервал между подключениями к серверу (мин.)»** — частота, с которой антивирус ESET NOD32 подключается к серверу удаленного администрирования для отправки данных. Другими словами, поле содержит временной интервал отправки информации на сервер. Если установлено значение 0, данные отправляются с интервалом в 5 секунд.
- **«Доступ к серверу удаленного администрирования защищен паролем»** — позволяет ввести пароль для подключения к серверу удаленного администрирования (если это необходимо).

Нажмите кнопку **ОК**, чтобы подтвердить изменения и применить параметры. Они будут использованы антивирусом ESET NOD32 для подключения к серверу удаленного администрирования.

4.9 Лицензия

Ветка **«Лицензия»** служит для управления лицензионными ключами к антивирусу ESET NOD32 и другим продуктам ESET. После приобретения продукта вместе с ключами предоставляются имя пользователя и пароль. Для того чтобы **добавить или удалить** лицензионный ключ, нажмите соответствующую кнопку в окне менеджера лицензий. Менеджер лицензий доступен в дереве расширенных параметров в разделе **«Разное» > «Лицензии»**.



Лицензионный ключ является текстовым файлом, содержащим информацию о приобретенном продукте (владелец лицензии, количество лицензий и дата истечения срока действия лицензии).

Окно менеджера лицензий позволяет загружать и просматривать содержимое лицензионных ключей с помощью кнопки **«Добавить»**. Содержимое лицензионного ключа отображается в окне менеджера. Для того чтобы удалить файлы лицензии из списка, нажмите кнопку **«Удалить»**.

Если срок действия лицензионного ключа истек и необходимо продолжить использование продукта, нажмите кнопку **«Заказать»**. В результате откроется соответствующий раздел веб-сайта компании ESET.

5. Опытный пользователь

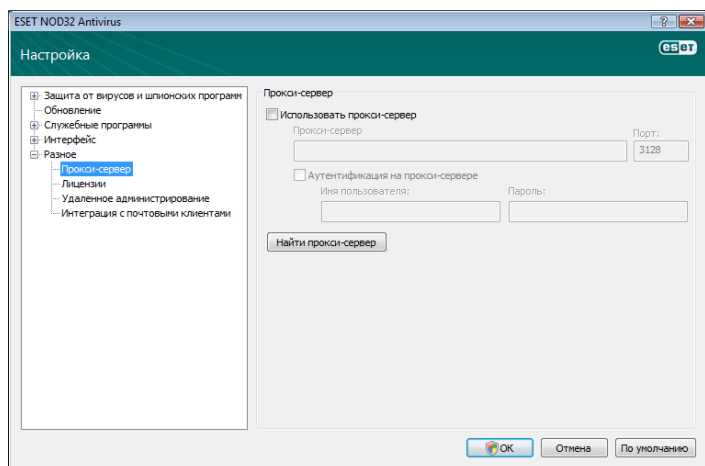
Данная глава содержит описание функций антивируса ESET NOD32, которые могут оказаться полезными для большинства опытных пользователей. Эти параметры и функции доступны только в расширенном режиме. Для переключения в расширенный режим нажмите кнопку «**Переключиться в расширенный режим**» в левом нижнем углу главного окна программы или нажмите клавиши CTRL + M на клавиатуре.

5.1 Настройка прокси-сервера

В антивирусе ESET NOD32 настройки прокси-сервера расположены в двух различных разделах дерева расширенных параметров.

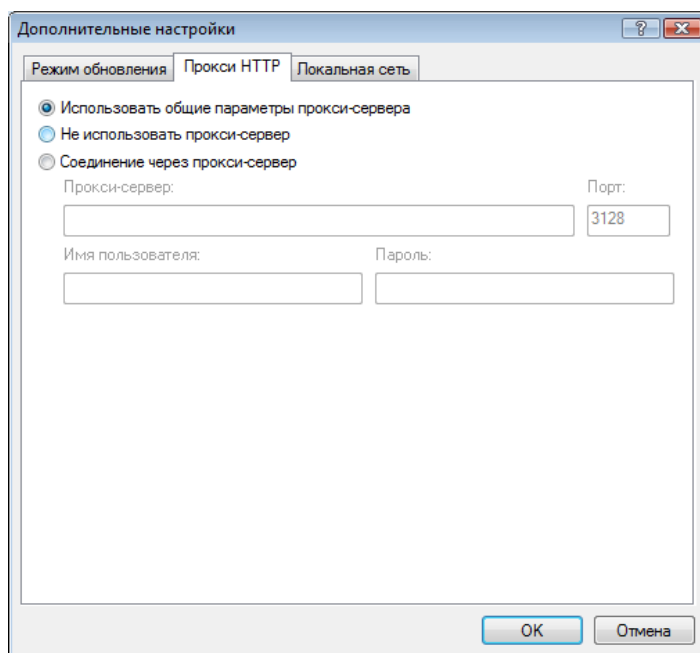
Параметры прокси-сервера можно настроить в разделе «**Разное**» > «**Прокси-сервер**». Эти настройки прокси-сервера являются общими для всего антивируса ESET NOD32. Эти параметры используются всеми модулями программы, которым требуется подключение к Интернету.

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 номер порта прокси-сервера в поле «**Порт**».



Если требуется аутентификация на прокси-сервере, установите флажок «**Аутентификация на прокси-сервере**», а затем укажите правильное **имя пользователя** и **пароль** в соответствующих полях. Нажмите кнопку «**Найти прокси-сервер**», чтобы автоматически определить и вставить параметры прокси-сервера. Будут скопированы параметры, которые используются веб-браузером Internet Explorer. Следует заметить, что данные аутентификации (имя пользователя и пароль) при этом не копируются, и пользователь должен указать их вручную.

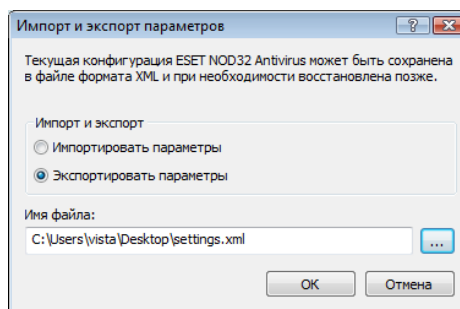
Кроме того, параметры прокси-сервера можно настроить в разделе «**Дополнительные настройки обновления**» (ветка «**Обновление**» дерева расширенных параметров). Эти параметры применяются только для данного профиля обновления и рекомендуются для использования на переносных компьютерах, которым необходимо получать обновления сигнатур вирусов из различных местоположений. Дополнительные сведения об этих параметрах см. в разделе 4.4 «Обновление системы».



5.2 Импорт и экспорт параметров

Импорт и экспорт текущей конфигурации антивируса ESET NOD32 доступен только в расширенном режиме в разделе «**Настройки**».

Как при импорте, так и при экспорте используются файлы формата XML. Процедуры импорта и экспорта полезны для резервного копирования текущей конфигурации антивируса ESET NOD32 при необходимости использовать ее в дальнейшем (по любой причине). Кроме того, экспорт параметров полезен, если нужно перенести опробованную конфигурацию антивируса ESET NOD32 на несколько систем. В этом случае на других системах нужно просто импортировать файл XML.



5.2.1 Экспорт параметров

Экспортировать настройки очень легко. Для сохранения текущей конфигурации антивируса ESET NOD32 перейдите к разделу «**Настройки**» > «**Импорт и экспорт параметров**». Выберите пункт **Экспортировать параметры** и введите имя файла конфигурации. Используйте проводник для указания местоположения файла конфигурации.

5.2.2 Импорт параметров

Процедура импорта похожа на процедуру экспорта. Перейдите к разделу «**Импорт и экспорт параметров**», а затем выберите пункт «**Импортировать параметры**». Нажмите кнопку «**...**» и укажите файл конфигурации, который необходимо импортировать.

5.3 Командная строка

Модуль защиты от вирусов антивируса ESET NOD32 может быть запущен из командной строки вручную (с помощью команды `cls`) или в пакетном режиме (с помощью BAT-файла).

При запуске сканирования по требованию из командной строки можно использовать перечисленные ниже параметры и аргументы.

Общие параметры:

- `help` показать справку и выйти
- `version` показать версию и выйти
- `base dir = ПАПКА` загрузить модули из ПАПКИ
- `quar-dir = ПАПКА` ПАПКА карантина
- `aind` показывать индикатор активности
- `auto` сканировать все жесткие диски в режиме очистки

Объекты:

- `files` сканировать файлы (по умолчанию)
- `no files` не сканировать файлы
- `boots` сканировать загрузочные сектора (по умолчанию)
- `no boots` не сканировать загрузочные сектора
- `arch` сканировать архивы (по умолчанию)
- `no arch` не сканировать архивы
- `max archive level = УРОВЕНЬ` максимальный УРОВЕНЬ вложенности архивов
- `scan-timeout = ИНТЕРВАЛ` сканировать архивы не дольше указанного ИНТЕРВАЛА времени в секундах. По достижении указанного предела сканирование архива останавливается и начинается сканирование следующего файла
- `max arch size = РАЗМЕР` сканировать только первые РАЗМЕР байт в архивах (по умолчанию «0» — без ограничения)
- `mail` сканировать файлы электронной почты
- `no mail` не сканировать файлы электронной почты
- `sfx` сканировать самораспаковывающиеся архивы
- `no sfx` не сканировать самораспаковывающиеся архивы
- `rtp` сканировать упаковщики в режиме реального времени
- `no rtp` не сканировать упаковщики в режиме реального времени
- `exclude = ПАПКА` не сканировать ПАПКУ
- `subdir` сканировать вложенные папки (по умолчанию)
- `no subdir` не сканировать вложенные папки
- `max archive level = УРОВЕНЬ` максимальный УРОВЕНЬ вложенности папок (по умолчанию «0» — без ограничения)
- `symlink` следовать по символическим ссылкам (по умолчанию)
- `no symlink` пропускать символические ссылки
- `ext-remove = РАСШИРЕНИЯ` исключить из сканирования файлы с указанными РАСШИРЕНИЯМИ (разделенными двоеточиями)
- `ext-exclude = РАСШИРЕНИЯ`

Методы:

- `adware` проверять на наличие рекламного, шпионского и опасного ПО
- `no adware` не проверять на наличие рекламного, шпионского и опасного ПО
- `unsafe` проверять на наличие потенциально опасного ПО

- `no unsafe` не проверять на наличие потенциально опасного ПО
- `unwanted` проверять на наличие потенциально нежелательного ПО
- `no unwanted` не проверять на наличие потенциально нежелательного ПО
- `pattern` использовать сигнатуры
- `no pattern` не использовать сигнатуры
- `heur` включить эвристику
- `no heur` отключить эвристику
- `adv heur` включить расширенную эвристику
- `no adv heur` отключить расширенную эвристику

Очистка:

- `action = ДЕЙСТВИЕ` выполнить ДЕЙСТВИЕ с зараженными объектами. Возможные действия: `none` (ничего), `clean` (очистить), `prompt` (запросить)
- `quarantine` копировать зараженные файлы в карантин (в дополнение к ДЕЙСТВИЮ)
- `no quarantine` не копировать зараженные файлы в карантин

Журналы:

- `log file = ФАЙЛ` записывать информацию о событии в ФАЙЛ
- `log rewrite` перезаписывать файл журнала (по умолчанию — дополнять)
- `log all` фиксировать данные о незараженных файлах
- `no log all` не фиксировать данные о незараженных файлах (по умолчанию)

Возможные коды завершения:

- 0 — угроз не обнаружено
- 1 — угроза найдена, но не удалена
- 10 — остались зараженные файлы
- 101 — ошибка архива
- 102 — ошибка доступа
- 103 — внутренняя ошибка

ПРИМЕЧАНИЕ:

Код завершения больше 100 означает, что файл не был просканирован и может быть заражен.

5.4 ESET SysInspector

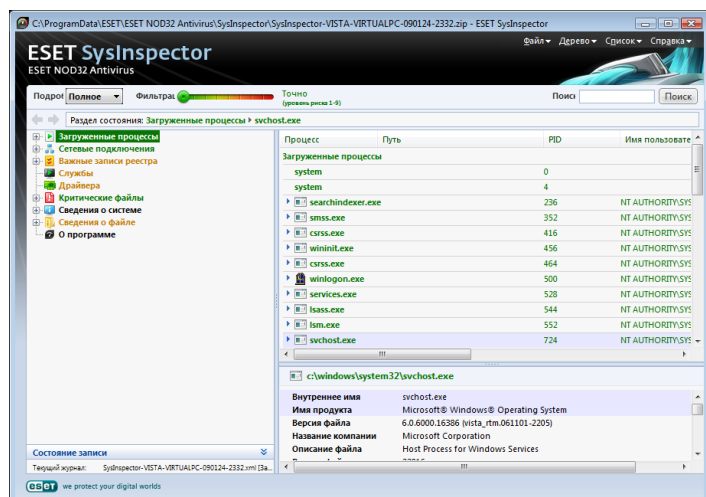
ESET SysInspector – это приложение, которое тщательно проверяет компьютер и отображает собранные данные в обобщенном виде. Такая информация как данные об установленных драйверах и приложениях, сетевых соединениях и важных записях в реестре позволяет определить причину неожиданного поведения системы, которое могло иметь место, например, вследствие несовместимости программного или аппаратного обеспечения или заражения вредоносными программами.

Компания ESET предлагает средство SysInspector в двух вариантах. Отдельное приложение (SysInspector.exe) можно загрузить с веб-сайта компании ESET. Интегрированная версия включена в пакет антивируса ESET NOD32 4. Для того чтобы открыть раздел SysInspector, перейдите в расширенный режим отображения (левый нижний угол окна) и выберите пункт «Службные программы» > SysInspector. Функциональные возможности и элементы управления обеих версий одинаковы. Единственное отличие заключается в способе обработки выходных данных. Отдельное приложение позволяет экспортировать снимок состояния системы в XML-файл и сохранить его на диск. Это возможно и в интегрированной версии SysInspector. Кроме того, можно воспользоваться удобной функцией сохранения снимков состояния системы непосредственно в окне «Антивирус ESET NOD32 4» > «Службные программы» > «SysInspector» (дополнительные сведения см. в разделе «5.4.1.4. SysInspector как часть антивируса ESET NOD32»).

Подождите, пока средство ESET SysInspector сканирует компьютер. Это может занять от 10 секунд до нескольких минут и зависит от конфигурации оборудования, операционной системы и количества установленных приложений.

5.4.1 Интерфейс пользователя и работа в приложении

Для простоты использования главное окно разделено на четыре части: сверху находятся элементы управления программой, слева – окно навигации, справа по центру – окно описания, а справа внизу – окно подробных сведений.



5.4.1.1 Элементы управления программой

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

«Файл»

Позволяет сохранить текущий отчет для последующего изучения или открыть ранее сохраненный отчет. Если отчет предназначен для публикации, рекомендуется создать его в формате, подходящем для отправки. В отчете такого типа отсутствует конфиденциальная информация.

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

«Дерево»

Позволяет развернуть или свернуть все узлы.

«Список»

Содержит функции, облегчающие перемещение в пределах программы, а также прочие функции (например, для поиска информации в Интернете).

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

«Справка»

Содержит сведения о приложении и его функциях.

«Подробнее»

Дополняет сведения, отображаемые в других секциях главного окна, упрощая тем самым работу с программой. В «базовом» режиме пользователь имеет доступ к информации, необходимой для поиска решений стандартных проблем в системе. В «среднем» режиме ESET SysInspector отображает сведения, которые используются реже, а в «полном» отображается вся информация, необходимая для решения наиболее нестандартных проблем.

«Фильтрация элементов»

Используется для поиска подозрительных файлов или записей в реестре системы. 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 отобразит только те элементы, уровень подозрительности которых выше отображаемого уровня. Если ползунок находится в крайнем правом положении, программа отображает только определенно вредоносные элементы.

Все элементы с уровнем риска от 6 до 9 могут быть опасными для системы. Если не используется ни одно решение для обеспечения безопасности от компании ESET, рекомендуется после нахождения программной такой элемента проверить систему онлайн-сканером ESET. Онлайн-сканер ESET распространяется бесплатно и доступен на странице <http://www.eset.eu/online-scanner>.

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

«Поиск»

Функция поиска используется для быстрого нахождения конкретного 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.

«Раздел состояния»

Отображает текущий узел в окне навигации.

5.4.1.2 Навигация в ESET SysInspector

ESET SysInspector распределяет разнообразную информацию в несколько базовых разделов, называемых узлами. Чтобы получить дополнительные сведения о каком-либо из разделов, разверните вложенные узлы соответствующего узла. Чтобы открыть (развернуть) узел, дважды щелкните по названию узла либо щелкните значок  или  рядом с названием узла. 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 в окне подробной информации отображаются дополнительные сведения о нем.

Ниже представлены описания главных узлов в окне навигации и относящейся к ним информации в окнах описания и подробных сведений.

«Запущенные процессы»

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

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

Примечание: Любая операционная система состоит из нескольких важных компонентов, которые постоянно выполняются и обеспечивают работу базовых и жизненно важных функций для других пользовательских приложений. В отдельных случаях такие процессы отображаются в программе ESET SysInspector с путем, начинающимся с символов «\?». Эти символы обеспечивают оптимизацию до запуска таких процессов и с точки зрения системы являются безопасными и правильными.

«Сетевые соединения»

В окне описания перечислены процессы и приложения, обменивающиеся данными через сеть с использованием протокола, выбранного в окне навигации (TCP или UDP), а также удаленные адреса, с которыми эти приложения устанавливают соединения. Можно также проверить присвоение доменов IP-адресам.

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

«Важные записи в реестре»

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

В окне описания также могут быть перечислены файлы, связанные с отдельными 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 проверить способ запуска службы, а также некоторую дополнительную информацию.

«Драйверы»

Список драйверов, установленных в системе.

«Критические файлы»

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

«Информация о системе»

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

«Сведения о файле»

Список важных системных файлов и файлов из папки Program Files. В окнах описания и подробных сведений может отображаться дополнительная информация о файлах.

«О программе»

Сведения о программе ESET SysInspector.



5.4.1.3 Сравнение

Функция сравнения позволяет пользователю сравнить два существующих журнала. Результатом выполнения этой команды является набор элементов, не совпадающих в этих журналах. Это позволяет отслеживать изменения в системе – таким образом можно, например, обнаружить деятельность вредоносных программ.









После запуска приложение создает новый журнал, отображаемый в новом окне. Чтобы сохранить журнал в файл, выберите пункт **«Файл» > «Сохранить журнал»**. Файлы журнала можно открыть и просмотреть позже. Чтобы открыть существующий журнал, выберите пункт меню **«Файл» > «Открыть журнал»**. В главном окне программы ESET SysInspector всегда отображается только один журнал.

Принцип сравнения двух журналов заключается в сравнении активного журнала с журналом из файла. Для сравнения журналов воспользуйтесь командой **«Файл» > «Сравнить журнал»** и выберите пункт **«Выбрать файл»**. Выбранный журнал будет сравнен с активным журналом в главном окне программы. Будет отображен так называемый сравнительный журнал, содержащий различия между двумя сравниваемыми журналами.

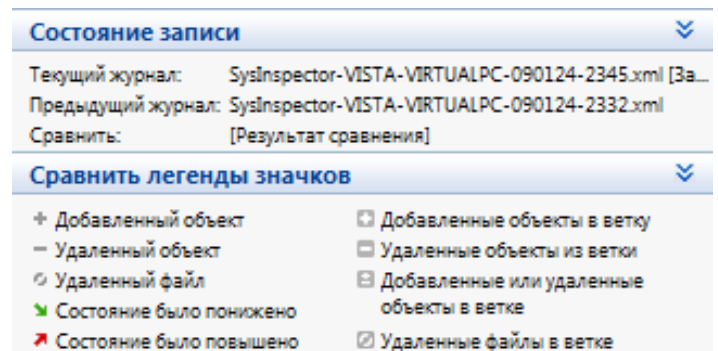
Примечание. Для сравнения двух журналов выберите пункт **«Файл» > «Сохранить журнал»** и сохраните журнал как ZIP-файл. Будут сохранены оба файла. Если позже открыть такой файл, автоматически будет выполнено сравнение содержащихся в нем журналов.

Рядом с отображаемыми элементами в SysInspector помещаются символы, обозначающие различия между журналами. Элементы, отмеченные знаком , находятся только в активном журнале и отсутствуют в журнале, открытом для сравнения. Элементы, отмеченные знаком , присутствуют только в открытом журнале и отсутствуют в активном.

Описание всех символов, которые могут отображаться напротив элементов:

-  новое значение, отсутствует в предыдущем журнале;
-  в разделе древовидной структуры содержатся новые значения;
-  удаленное значение, присутствует только в предыдущей версии журнала;
-  в разделе древовидной структуры содержатся удаленные значения;
-  значение или файл были изменены;
-  в разделе древовидной структуры содержатся измененные значения или файлы;
-  уровень риска снизился или был выше в предыдущей версии журнала;
-  уровень риска увеличился или был ниже в предыдущей версии журнала.

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



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

Пример.

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

Чтобы отследить различия между этими двумя журналами, перейдите в меню **«Файл» > «Сравнить журнал»**. Программа создаст сравнительный журнал, содержащий различия между сравниваемыми журналами.

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

```
SysInspector.exe текущий.xml предыдущий.xml
```

5.4.1.4 SysInspector как часть антивируса ESET NOD32 4

Для того чтобы открыть раздел SysInspector в антивирусе ESET NOD32 4, выберите пункт «**Служебные программы**» > **SysInspector**. Элементы управления в окне SysInspector похожи на элементы в окне журнала сканирования или в окне запланированных задач. Все операции со снимками состояния системы (создание, просмотр, сравнение, удаление и экспорт) выполняются посредством одного или двух щелчков мыши.

Окно SysInspector содержит основные сведения о созданных снимках состояния, такие как время, краткое примечание, имя создавшего снимок пользователя, а также состояние снимка.

Для **сравнения, добавления и удаления** снимков используйте соответствующие кнопки, расположенные в окне SysInspector под списком снимков. Эти функции также можно вызвать из контекстного меню. Для просмотра выбранного снимка состояния системы воспользуйтесь командой контекстного меню «**Просмотреть**». Чтобы экспортировать снимок в файл, щелкните его правой кнопкой и выберите «**Экспорт**». Ниже приведено подробное описание каждой из функций.

«**Сравнить**» — сравнение двух журналов и просмотр списка различий между текущим журналом и его более старой версией. Для сравнения необходимо выбрать два снимка состояния.

«**Добавить**» — добавление новой записи. Перед созданием записи требуется ввести к ней короткое примечание. В столбце «Состояние» отображается ход создания снимка состояния системы в процентах; все уже созданные снимки состояния помечены надписью «Создано».

«**Удалить**» — удалить записи из списка.

«**Отобразить**» — вывод выбранного снимка на экран. Вместо этого можно дважды щелкнуть выбранную запись.

«**Экспорт...**» — сохранение выбранного снимка в формате XML с возможностью упаковки в архив ZIP.

5.4.1.5 Сценарий обслуживания

Сценарий обслуживания — это средство, непосредственно взаимодействующее с операционной системой и установленными приложениями и позволяющее выполнять другие сценарии, которые удаляют проблемные компоненты системы, включая вирусы и их остатки, заблокированные файлы, вирусные записи в реестре и т. д. Сценарий хранится в текстовом файле, созданном на основе заранее подготовленного XML-файла. Данные в текстовом файле сценария упорядочены интуитивно понятным образом, что упрощает работу с ними. Изначально сценарий предполагает нейтральное поведение. Иными словами, в своем исходном состоянии он не оказывает никакого воздействия на систему. Для того чтобы добиться того или иного эффекта, необходимо внести в него изменения.

Внимание!

Это средство предназначено для опытных пользователей. Его неправильное использование может привести к повреждению программ или операционной системы.

5.4.1.5.1 Создание сценариев обслуживания

Для того чтобы создать сценарий, щелкните правой кнопкой любой объект в древовидном меню в левой панели основного окна SysInspector. В контекстном меню выберите команду «**Экспортировать все разделы в сценарий обслуживания**» или «**Экспортировать выбранные разделы в сценарий обслуживания**».

5.4.1.5.2 Структура сценария обслуживания

В первой строке заголовка сценария содержатся данные о версии ядра (ev), версии интерфейса (gv) и версии журнала (lv). Эти данные можно использовать для отслеживания изменений в XML-файле, используемом для создания сценария. Они гарантируют согласованность версий на этапе выполнения. Эту часть сценария изменять не следует.

Остальное содержимое файла разбито на разделы, объекты в которых можно менять. Те из них, которые должны учитываться сценарием, следует пометить. Для этого символ «-» перед объектом надо заменить символом «+». Разделы отделены один от другого пустой строкой. Каждый раздел имеет собственный номер и название.

01) Running Processes (выполняемые процессы)

Этот раздел содержит список процессов, выполняющихся в системе. Каждый процесс идентифицируется по UNC-пути, а также по 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 выбран (помечен символом «+») процесс module32.exe, который будет завершен при выполнении сценария.

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\khibehb.dll
- c:\windows\system32\advapi32.dll
[...]
```

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

03) TCP connections (TCP-соединения)

В этом разделе содержится информация о существующих TCP-соединениях.

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 этого сценария обнаруживается владелец сокета помеченных TCP-соединений и сокет останавливается, высвобождая системные ресурсы.

04) UDP endpoints (конечные точки UDP)

В этом разделе содержится информация 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 и 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 в реестре)

В этом разделе содержится информация о важных записях в реестре.

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 запуске сценария помеченные записи будут удалены, сведены к 0-разрядным значениям или сброшены к значениям по умолчанию. Действия, применяемые к конкретным записям, зависят от категории и значения ключа в определенной записи реестра.

07) Services (службы)

Этот раздел содержит список служб, зарегистрированных в системе.

Пример

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

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

08) Drivers (драйверы)

В этом разделе перечислены установленные драйверы.

Пример

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

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

09) Critical files (важные файлы)

В этом разделе содержится информация о файлах, играющих важную роль с точки зрения 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
[...]
```

Выбранные объекты будут или удалены или возвращены к исходным значениям.

5.4.1.5.3 Выполнение сценариев обслуживания

Пометьте нужные объекты, сохраните и закройте сценарий. Запустите измененный сценарий непосредственно из основного окна SysInspector с помощью команды **«Запуск сценария обслуживания»** в меню «Файл». При открытии сценария появится следующее сообщение: **«Выполнить сценарий обслуживания "%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 появится подтверждение о выполнении сценария.

Если сценарий может быть обработан только частично, отобразится следующее сообщение: **«Сценарий обслуживания выполнен частично. Показать отчет об ошибке?»** Для того чтобы просмотреть полный отчет об ошибке, в котором перечислены невыполненные действия, нажмите кнопку **«Да»**.

Сценарий был признан недопустимым и не был выполнен, если отображается следующее сообщение: **«Проблемы целостности сценария (поврежденный заголовок, измененное название раздела, пропущена пустая разделительная строка и т. д.)»**. В этом случае откройте файл сценария и исправьте ошибки либо создайте новый сценарий обслуживания.

5.5 ESET SysRescue

Средство создания аварийного компакт-диска ESET (ERCD) предназначено для создания загрузочного диска, содержащего антивирус ESET NOD32 4 (ENA). Главным преимуществом этого диска является то, что приложение ENA запускается 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.

5.5.1 Минимальные требования

Средство ESET SysRescue (ESR) работает в среде предустановки Microsoft Windows (Windows PE) версии 2.x, созданной на базе системы Windows Vista. Windows PE является частью свободно распространяемого пакета автоматической установки Windows (Windows AIK), поэтому перед созданием ESR необходимо установить Windows AIK. В связи с тем, что поддержка среды Windows PE ограничивается ее 32-разрядной версией, ESR создается только в 32-разрядных версиях ENA. Средство ESR поддерживает пакет Windows AIK версии 1.1 и выше и доступно в составе пакета ENA версии 4.0 и выше.

5.5.2 Создание компакт-диска аварийного восстановления

При условии соответствия минимальным требованиям к созданию компакт-диска ESET SysRescue (ESR) процесс его создания достаточно прост. Для запуска мастера ESR последовательно выберите в меню пункты **«Пуск» > «Программы» > ESET > «Антивирус ESET NOD32 4» > ESET SysRescue**.

На первом этапе мастер определяет наличие в системе установленного средства Windows AIK и подключенного к компьютеру подходящего устройства записи для создания загрузаемого носителя.

На следующем этапе предлагается выбрать носитель для размещения на нем файлов ESR. Помимо CD, DVD или USB, образ диска ESR можно сохранить в файл 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).

На последнем этапе, после указания всех параметров, пользователю предоставляется возможность просмотреть отчет о работе мастера ESET SysRescue, проверить правильность параметров и приступить к созданию диска. Доступны следующие варианты:

«Папки»;
«Антивирус ESET»;
«Дополнительно»;
«Загрузочное устройство USB»;
«Запись».

5.5.2.1 Папки

«Временная папка» — это рабочий каталог для файлов, необходимый при создании диска ESET SysRescue.

«Папка с ISO» — это папка, в которую сохраняется полученный ISO-файл.

В списке на этой вкладке перечислены все локальные и сетевые диски с указанием свободного места на них. Если какие-то из папок располагаются на диске с недостатком свободного места, рекомендуется выбрать другой диск, на котором места достаточно. В противном случае недостаток свободного места не позволит создать образ диска.

«Внешние приложения»

Позволяет указать дополнительные программы, которые будут запущены или установлены после загрузки с носителя SysRescue.

«Включать внешние приложения» — позволяет добавлять внешние программы в набор программ SysRescue.

«Выбранная папка» — папка, содержащая программы, которые нужно добавить на диск SysRescue.

5.5.2.2 Антивирус ESET

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

«Папка ENA» — файлы, уже содержащиеся в папке, в которую установлен программный продукт ESET;

«MSI-файл» — файлы, которые содержатся в установщике MSI.

«Профиль» — источником имени пользователя и пароля может послужить один из двух следующих вариантов:

«Установленный ENA» — имя пользователя и пароль копируются из установленных продуктов (антивирус ESET NOD32 4 или ESET NOD32);

«От пользователя» — имя пользователя и пароль вводятся в соответствующие текстовые поля, расположенные ниже.

Примечание. Антивирус ESET NOD32 4 и антивирус ESET NOD32 на компакт-диске ESET SysRescue обновляются из Интернета или из пакета безопасности ESET, установленного на компьютере, на котором запускается компакт-диск ESET SysRescue.

5.5.2.3 Дополнительно

На вкладке **«Дополнительно»** можно настроить параметры компакт-диска ESET SysRescue в соответствии с объемом оперативной памяти компьютера. Чтобы записать содержимое компакт-диска в оперативную память (ОЗУ), выберите пункт **«512 МБ и больше»**. Если выбрать пункт **«Меньше 512 МБ»**, при работе WinPE будет постоянно происходить обращение к компакт-диску восстановления.

«Внешние драйверы» — в этом разделе можно добавить драйверы для особого оборудования (обычно для сетевой карты). Хотя система WinPE создана на основе ОС Windows Vista SPI, поддерживающей самое разное аппаратное обеспечение, иногда оборудование не распознается и драйвер для него приходится добавлять вручную. Существует два способа добавления драйвера на диск ESET SysRescue: вручную (кнопка **«Добавить»**) и автоматически (кнопка **«Автопоиск»**). При добавлении драйвера вручную необходимо указать путь к соответствующему INF-файлу (в этой папке также должен находиться SYS-файл). В режиме автоматического добавления драйвер находится в операционной системе данного компьютера автоматически. Автоматическое добавление рекомендуется применять только в случае, если SysRescue используется на компьютере с такой же сетевой картой, как и на компьютере, на котором был создан диск SysRescue. При создании диска ESET SysRescue драйвер добавляется в сборку, поэтому пользователю впоследствии не приходится его искать.

5.5.2.4 Загрузочное USB-устройство

Если в качестве носителя назначения было выбрано USB-устройство, на вкладке «Загрузочное USB-устройство» можно выбрать один из доступных USB-носителей (если доступно несколько USB-устройств).

Предупреждение: *Выбранное USB-устройство будет отформатировано при создании ESET SysRescue, что означает, что все данные с него будут удалены.*

5.5.2.5 Запись

Если в качестве диска назначения выбран компакт-диск или DVD-диск, на вкладке «Запись» можно задать дополнительные параметры записи.

«Удалить ISO-файл» — установите этот флажок, чтобы удалить ISO-файлы после создания компакт-диска аварийного восстановления ESET.

«Включить удаление» — позволяет сделать выбор между быстрой и полной очисткой диска.

«Устройство записи» — выберите диск, 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» представлены сведения о диске в дисковом.

«Скорость записи» — выберите нужную скорость из раскрывающегося списка. При выборе скорости необходимо учитывать возможности записывающего устройства и тип компакт- или DVD-диска.

5.5.3 Работа с ESET SysRescue

Для эффективного использования функции аварийного восстановления с носителей CD, DVD и USB необходимо загрузить компьютер с соответствующего носителя. Порядок загрузки настраивается в параметрах BIOS. Кроме того, на этапе запуска компьютера можно вызвать меню загрузки; обычно оно вызывается с помощью клавиш F9 – F12, в зависимости от версии системной платы и BIOS.

После загрузки запускается программа ENA. Поскольку средство ESET SysRescue используется лишь в особых случаях, некоторые модули защиты и функции ENA не требуются и их список включает только функции сканирования компьютера и обновления, а также некоторые разделы настроек. Возможность обновления базы данных сигнатур вирусов является наиболее важной функцией ESET SysRescue. Перед началом сканирования компьютера рекомендуется обновить программу.

5.5.3.1 Использование ESET SysRescue

Представим себе ситуацию, когда компьютеры в сети заражены вирусами, поражающими исполняемые файлы (EXE). Система ENA способна излечить все инфицированные файлы, кроме файла проводника explorer.exe, который не может быть излечен даже в безопасном режиме.

Это связано с тем, что файл explorer.exe, как один из основных компонентов системы Windows, загружается и используется даже в безопасном режиме. Система ENA не может выполнять никаких действий с этим файлом, поэтому он остается зараженным.

В такой ситуации проблему может решить средство ESET SysRescue. Для работы средства ESET SysRescue не требуется ни один компонент операционной системы компьютера, поэтому оно способно обрабатывать (очищать, удалять) любые файлы на диске.

6. Глоссарий

6.1 Типы заражений

Заражение представляет собой попытку проникновения злонамеренного ПО на компьютер пользователя и причинение вреда.

6.1.1 Вирусы

При заражении компьютера вирусами происходит порча файлов. Название категории возникло вследствие сходства таких программ с биологическими вирусами, так как они используют сходную технику для передачи своего кода с компьютера на компьютер.

Компьютерные вирусы атакуют в основном исполняемые файлы и документы. Для размножения вирус присоединяет свое «тело» к концу заражаемого файла. Вот краткое описание цикла размножения: после запуска зараженного файла вирус активируется (это происходит перед активацией самого приложения) и выполняет атакующие действия. Только после этого происходит запуск самого приложения. Вирус не может заразить компьютер, пока пользователь (по ошибке или намеренно) собственноручно не запустит злонамеренную программу.

Компьютерные вирусы могут различаться по активности и степени опасности. Некоторые из вирусов особо опасны, так как могут уничтожать файлы на компьютере. С другой стороны, некоторые из вирусов не приводят к серьезным повреждениям. Они просто досаждают пользователю своей деятельностью, которая призвана демонстрировать навыки их разработчиков.

Важно заметить, что вирусы постепенно становятся редкостью по сравнению с троянскими программами или шпионским ПО, так как они коммерчески малоэффективны для авторов злонамеренных программ. Таким образом, термин «вирус» зачастую неверно используется для других типов заражений. В настоящее время он постепенно выходит из употребления, и на смену ему приходит более точный термин «злонамеренное ПО».

Если компьютер заражен вирусом, необходимо восстановить зараженные файлы в их исходное состояние, т. е. очистить их с помощью антивирусной программы.

Примеры вирусов: OneHalf, Tenga и Yankee Doodle.

6.1.2 Черви

Компьютерные черви – это злонамеренные программы, которые атакуют компьютеры и распространяются через сеть. Основная разница между вирусами и червями заключается в том, что черви могут воспроизводиться и распространять сами себя по сети. Они не зависят от файлов-носителей (или загрузочных секторов).

Черви распространяются с помощью электронной почты или сетевых пакетов. С учетом этого черви могут быть разделены на две категории:

- **почтовые** – рассылают себя по адресам, найденным в адресной книге пользователя;
- **сетевые** – используют сетевые уязвимости приложений.

Черви намного более подвижны, чем компьютерные вирусы. Благодаря Интернету они распространяются по всему земному шару за считанные часы после запуска в сеть. В некоторых случаях счет идет даже на минуты. Эта характерная способность распространяться быстро и независимо делает червей очень опасными, значительно опаснее, чем вирусы и другие типы злонамеренных программ.

Действующий в системе червь может доставить множество неудобств пользователю: он может удалять файлы, снижать производительность системы или мешать работе программ. Его природа позволяет ему выступать в качестве «транспортного средства» для заражений других типов.

Если компьютер заражен компьютерным червем, рекомендуется удалить инфицированные файлы, так как они содержат злонамеренный код.

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

6.1.3 Троянские программы

Исторически троянскими программами называется обособленная группа злонамеренных программ, которые выглядят как полезные. Пользователь, не зная о злонамеренном коде, производит запуск такой программы. Однако стоит заметить, что на сегодняшний день это определение устарело, и троянские программы больше не нуждаются в подобной рода маскировке. Целью таких программ являются как можно более простое проникновение в систему и выполнение злонамеренного кода. Термин «троянский конь» стал обозначать обширный класс заражений, которые не попадают в классификацию обычных вирусов.

Так как эта категория весьма обширна, ее часто разбивают на несколько подкатегорий. Широко известны следующие:

- **downloader** (программа-загрузчик) – злонамеренная программа, которая загружает другие угрозы из Интернета;
- **dropper** (программа-бомба) – тип троянской программы, которая разработана для заражения компьютеров другими опасными программами;
- **backdoor** (утилита удаленного администрирования) – приложение, которое обменивается данными с атакующей стороной, позволяя получить доступ к системе и контроль над ней;
- **keylogger** (клавиатурный шпион) – программа записывает все, что набирает пользователь на клавиатуре, и отправляет эту информацию удаленной атакующей стороне;
- **dialer** (программа дозвона) – программа, которая пытается набирать номера телефонов, звонки на которые оплачивает вызывающий абонент. При этом пользователю почти незаметно, что создано новое соединение. Программы дозвона могут нанести вред только пользователям модемов. К счастью, модемы уже не распространены столь широко, как раньше.

Троянская программа обычно представляет собой исполняемый файл с расширением exe. Если на компьютере обнаружен файл, принадлежащий к категории троянских программ, рекомендуется удалить его, так как он с большой вероятностью содержит злонамеренный код.

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

6.1.4 Руткиты

Руткитом называется злонамеренная программа, которая предоставляет атакующей стороне возможность получения полного удаленного доступа через Интернет ко всем ресурсам компьютера, не проявляя при этом своего присутствия в системе. При доступе к системе через бреши в ее безопасности руткиты используют функции операционной системы, чтобы избежать обнаружения антивирусными приложениями: используются механизмы маскировки процессов, файлов и данных системного реестра. По этой причине их активность невозможно обнаружить стандартными средствами системы.

Для профилактики атаки с помощью руткитов необходимо помнить о двух уровнях обнаружения, описанных ниже.

1. Обнаружение при попытке проникновения в систему. Если злоумышленник не может проникнуть, он безопасен. Многие системы защиты от вирусов способны предотвратить проникновение руткитов на этом уровне (так как они могут быть обнаружены в содержимом файлов, которое возможно проверить).
2. Обнаружение при попытке скрыться во время обычной проверки системы. Пользователи антивируса ESET могут использовать технологию Anti-Stealth, которая позволяет вовремя обнаружить и удалить активные руткиты.

6.1.5 Рекламные программы

Рекламное ПО — краткое название программного обеспечения, поддерживаемого рекламой (adware). Программы, демонстрирующие пользователю рекламу, попадают в эту категорию. Чаще всего признаками работы рекламного ПО становятся всплывающие окна рекламы в веб-браузере или смена домашней страницы. Рекламное ПО зачастую распространяется совместно с бесплатными пакетами программного обеспечения. Это позволяет их создателям покрывать расходы на разработку полезных, как правило, программ.

Само по себе рекламное ПО не опасно, но оно доставляет неудобства пользователям. Опасность заключается в том, что в рекламном ПО могут быть реализованы дополнительные функции слежения, подобно шпионским программам.

Если пользователь решает использовать свободно распространяемый программный продукт, ему стоит уделить особое внимание установке программы. Чаще всего программа установки предупреждает о наличии рекламного ПО. Зачастую пользователь имеет возможность отказаться от его установки и установить необходимую программу без рекламного ПО. Однако иногда программы нельзя установить без рекламной части или их функционал оказывается неполным. Это приводит к тому, что рекламное ПО получает доступ к системе на «законных» основаниях, так как пользователь согласился на его установку. В этом случае лучше заранее обезопасить себя, чем потом пожалеть.

Если на компьютере обнаружен файл, который относится к рекламному ПО, рекомендуется удалить его, так как он с большой вероятностью содержит злонамеренный код.

6.1.6 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 (например, список посещаемых веб-сайтов, адреса электронной почты в адресных книгах или набираемый на клавиатуре текст).

Авторы шпионского программного обеспечения утверждают, что эти технологии направлены на изучение потребностей и интересов пользователей и позволяют лучше управлять рекламой. Проблема заключается в том, что нет четкой границы между полезными и злонамеренными приложениями, и никто не гарантирует, что собираемая информация не будет использована во вред. Данные, полученные шпионскими приложениями, могут содержать пароли пользователя, PIN-коды, номера счетов и т. д. Шпионское программное обеспечение зачастую поставляется в комплекте со свободно распространяемыми программами. Это позволяет авторам возместить расходы на разработку программ или проводить стимуляцию продаж ПО. Часто пользователи информируются о присутствии шпионского программного обеспечения во время установки основной программы. При этом в платной версии программы этого программного обеспечения нет.

Примерами хорошо известного программного обеспечения, которое поставляется в комплекте со шпионским, являются клиенты пиринговых (P2P) сетей. Программы Spyfalcon и Spy Sheriff (и многие другие) принадлежат к особой подкатегории шпионского ПО. Об этих программах заявляется, что они предназначены для борьбы со шпионским ПО, но на самом деле они сами являются таковым.

Если на компьютере обнаружен файл, принадлежащий к шпионским программам, рекомендуется удалить его, так как он с большой вероятностью содержит злонамеренный код.

6.1.7 Потенциально опасные программы

Существует множество программ, предназначенных для упрощения администрирования сетевых компьютеров. Однако в руках злоумышленника они могут быть использованы во вредоносных целях. По этой причине они отнесены в отдельную категорию в классификации ESET. Пользователи могут указать, должна ли система защиты от вирусов обнаруживать такие программы или нет.

Коммерческие, легитимные 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, отслеживающие последовательность клавиш, нажимаемых пользователем на клавиатуре).

Если такая программа обнаружена на компьютере, но пользователь не устанавливал ее, следует обратиться к администратору сети за консультацией или удалить ее.

6.1.8 Потенциально нежелательные программы

Приложения, относящиеся к потенциально нежелательному ПО, не обязательно являются злонамеренными. Однако они могут тем или иным образом снижать производительность системы. Такие приложения обычно требуют согласия пользователя при установке. После их установки поведение системы изменяется (по сравнению с тем, как она вела себя до установки этих программ). Наиболее заметными изменениями являются следующие:

- открываются новые окна, которых не было ранее;
- активируются и выполняются скрытые процессы;
- повышается уровень использования системных ресурсов;
- появляются изменения в результатах поиска;
- приложения подключаются к удаленным серверам.