

# NOD32 – комплексная защита системы



*Андрей Бирюков*

**Антивирусная система, пожалуй, важнейший элемент защиты любой рабочей станции. Посмотрим, что нового появилось в антивирусных продуктах компании ESET.**

**А**нтивирусная система на сегодняшний день является неотъемлемой частью программного обеспечения, установленного на любом компьютере, как на корпоративном, так и на домашнем. Кроме того, думаю, сегодня сложно найти сервер электронной почты, на котором не была бы установлена какая-либо антивирусная система. Таким образом, программное обеспечение для защиты от вирусов и вредоносного кода есть практически в любой корпоративной сети. В этой статье речь пойдет о продуктах компании ESET (<http://www.eset.com>), в частности о новой версии ESET NOD32 и новом решении ESET NOD32 Smart Security.

## Функциональные возможности

Прежде всего следует сказать о возможностях антивирусных продуктов данной компании. В решении ESET NOD32 Smart Security интегрированы система антивирусной защиты, антишпион, межсетевой экран и средство защиты от нежелательной почты (ан-

тиспам). При этом в межсетевом экране реализованы все наиболее существенные функции современных персональных межсетевых экранов, включая систему обнаружения вторжений, усовершенствованную проверку трафика «на лету», поддержку IPv6, выбор портов для сканирования и проверку трафика, проходящего через нестандартные порты, и др. При установке ESET NOD32 Smart Security межсетевой экран предлагает три режима работы, которые позволяют организовать более эффективную работу с межсетевым экраном: автоматический, интерактивный и режим на основе политик, заданных пользователем. Подсистема защиты от нежелательной почты является обучаемой, позволяет легко настраивать действия при обнаружении спама, формировать «черные» и «белые» списки адресов из локальных адресных книг и на основе исходящих сообщений, задавать другие параметры системы фильтрации. Все функциональные модули ESET NOD32 Smart Security полностью интегрированы в операционную систему

и используют единый центр управления, позволяющий пользователям любой квалификации проводить тонкую настройку системы защиты и процесса обновления через простой и понятный графический интерфейс.

В корпоративную версию обоих продуктов встроен механизм взаимодействия с системой удаленного администрирования – ESET Remote Administrator версии 2.0. Это система, позволяющая централизованно устанавливать и настраивать различные версии программных продуктов компании ESET и проводить удаленную установку ПО сторонних разработчиков в крупных корпоративных сетях. Отмечу широкие возможности ESET Remote Administrator версии 2.0 по контролю событий, регистрации, формированию отчетов и управлению автоматическим обновлением антивирусных баз и ПО ESET с использованием «зеркал» в корпоративной сети. Такое средство очень удобно в использовании в крупных, корпоративных сетях, так как позволяет администраторам удаленно осуществлять установ-

ку и настройку программного обеспечения. Новые продукты ESET совместимы с MS Windows 2000, XP и Vista, наиболее популярными у корпоративных и частных пользователей. При этом поддерживаются 32- и 64-разрядные версии операционных систем. Лицензируется ESET NOD 32 Smart Security по количеству инсталляций, то есть число закупленных лицензий должно быть равно количеству установок.

## Установка

Итак, приступим непосредственно к установке и настройке данных продуктов. Прежде всего необходимо защитить файловые серверы и рабочие станции от вирусов и вредоносного кода. Для этого нам необходимо установить основной антивирусный модуль и межсетевой экран. Для защиты электронной почты от нежелательных рассылок также потребуется модуль антиспама.

Установка достаточно проста. На первом шаге необходимо выбрать режим установки: «Обычная» или «Пользовательская». Второй вариант предполагает более гибкие возможности по установке. Для большей наглядности выбираем «Пользовательскую». Далее нужно указать каталог, в который будет осуществлена установка. На следующем шаге нужно ввести те учетные данные, которые были получены вместе с дистрибутивом продукта при покупке (для коробочных версий данная информация содержится внутри комплекта ПО). Эти учетные данные необходимы для осуществления обновлений продукта. Если у вас

они отсутствуют или нет времени, то ввести их можно позже, но необходимо сделать обязательно, так как иначе могут быть проблемы с обновлениями (см. **рис. 1**).

Затем нужно ввести настройки для соединения с Интернетом. После этого можно настроить расписание для автоматического обновления компонентов антивируса. Отмечу, что в данном случае речь идет об обновлении именно программных компонентов входящих в состав антивируса, а не антивирусных баз (см. **рис. 3**).

На следующем шаге можно защитить настройки конфигурации антивируса с помощью пароля. Это действие поможет защитить рабочую станцию от несанкционированного вмешательства в настройки антивирусной системы.

Далее предлагается подключить узел к «Антивирусной системе своевременного оповещения» (ThreatSense. Net Early Warning System). Фактически это средство, которое отправляет информацию о вирусных инцидентах в лабораторию ESET, данная информация может помочь своевременно предотвратить масштабную вирусную эпидемию, так что лучше оставить эту опцию включенной. Затем вам предлагается включить средство для определения потенциально нежелательных приложений (detection of potentially unwanted applications) (см. **рис. 2**). Данный режим рекомендуется включить.

На последнем шаге перед началом непосредственно установки предлагается настроить персональный межсетевой экран. По умолчанию предла-

гается использовать режим Automatic. Данный режим разрешает все исходящие соединения, но запрещает инициированные входящие. Режим Interactive позволяет пользователю самостоятельно разрешать или запрещать соединения, запрашивая разрешение или запрещение каждого нового соединения, для которого отсутствует правило. Но для администраторов крупных корпоративных сетей наиболее интересен будет режим Policy-based, который использует правила, созданные администратором.

Дальше начинается собственно процесс установки.

## Настройки и управление

Сразу после установки встроенный межсетевой экран обнаружит подключенные к компьютеру сети и предложит произвести необходимые настройки. В частности, дисковые ресурсы рабочей станции можно сделать доступными для общего доступа по сети.

После запуска консоли антивируса мы попадаем в главное окно администрирования ESET. Для тех, кто хорошо знаком с различными антивирусными продуктами, управление ESET NOD 32 не покажется сложным. Слева располагаются основные элементы управления. В частности, в разделе «Protection status» показаны состояние компонентов антивирусной системы: antivirus, firewall, antispaam, а также статистика по предотвращенным атакам и текущая версия антивирусных баз. В случае если все компоненты запущены и антивирусные базы обновлены, значок Protection Status будет све-

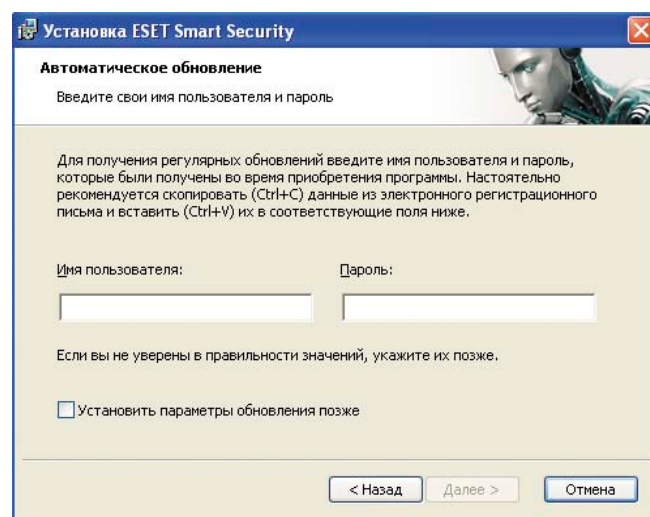


Рисунок 1. Настройки обновлений антивируса

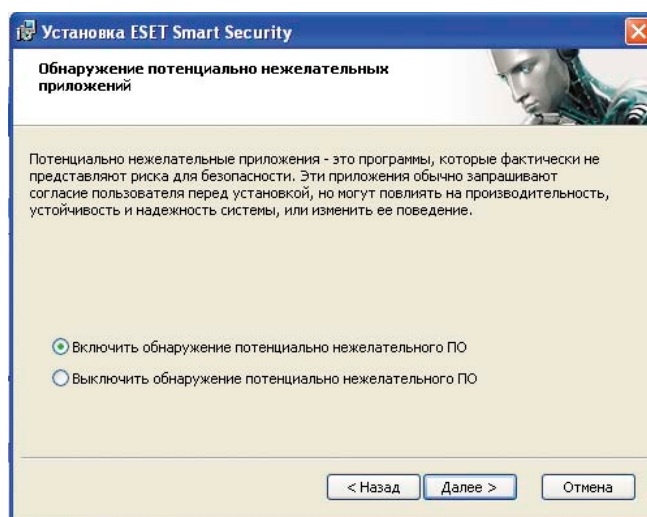


Рисунок 2. Определение потенциально опасных приложений



Рисунок 3. Настройки обновления программных компонентов

таться зеленым цветом. В противном случае цвет будет красным.

В разделе «Computer Scan» можно запустить сканирование системы или отдельных ее частей на наличие вредоносного кода.

В разделе «Update» можно произвести обновление антивирусных баз.

Однако наибольший интерес представляют элементы раздела «Настройка», так как именно здесь можно более гибко настроить антивирусную систему для работы.

Начнем с компонента «Антивирус». Для настройки необходимо открыть раздел «Защита от вирусов и шпионских программ». Здесь, как и приня-

то во всех современных антивирусных системах, возможна отдельная настройка сканирования в режиме реального времени, защита электронной почты, доступа в Интернет, ручное сканирование рабочей станции, а также настройка исключений.

Как видно из рис. 4, рекомендованным действием по умолчанию для большинства компонентов является их активация. В случае активного использования сетевых ресурсов сканирование сетевых дисков лучше отключить, так как это может сказаться на производительности рабочей станции. Вообще, основываясь на собственном опыте, скажу, что по сравнению с другими антивирусными продуктами здесь доступно достаточно большое количество различных настроек, что позволяет оптимизировать работу антивирусной системы и рабочей станции в целом. Говоря об оптимизации работы системы, также хотелось бы обратить внимание на раздел «Исключения». В этом разделе можно указать те файлы и папки, сканирование которых производить не нужно. Это бывает полезно, к примеру, для баз данных или почтовых серверов, когда обращение к файлам осуществляется постоянно и антивирус существенно снижает быстродействие системы постоянным сканированием этих файлов. Кроме того, можно создать фильтры по расширению и типам файлов.

Еще один интересный раздел – это «Защита доступа в Интернет». Здесь помимо стандартного межсетевого экрана, запрещающего соединения по определенным портам, и сканирования на наличие вредоносного кода всего трафика можно также настроить запрет доступа к определенным сайтам, а также разрешить доступ в Интернет только для определенных приложений. Думаю, эти функции будут весьма полезны для администраторов крупных корпоративных сетей, где пользователи зачастую проводят слишком много времени, общаясь с помощью программ для мгновенного обмена сообщениями или посещая сайты типа [odnoklassniki.ru](http://odnoklassniki.ru). К тому же, как я упоминал ранее, настройки межсетевого экрана можно распространять централизованно, что также будет очень полезно системным администраторам.

«Защита электронной почты» представляет собой антивирусную проверку сообщений, получаемых почтовым клиентом. При этом письма, содержащие вредоносный код, можно как удалять полностью, так и доставлять, очищая от зараженных приложений, и добавлять в тело письма соответствующее сообщение о том, что из письма был удален вредоносный код. Кроме того, защита электронной почты может взаимодействовать как с конкретным почтовым клиентом (Microsoft Outlook), так и с любым приложением, работающим по протоколу POP3 (к сожалению, дополнительные настройки для других почтовых протоколов отсутствуют). Также ESET содержит средства для борьбы с нежелательной почтой. Здесь можно настроить добавление в тему сообщения соответствующего тега или перемещение письма в определенную папку. Также есть возможность самостоятельного обучения фильтра нежелательной почты.

О практическом тестировании фильтра нежелательной почты мы поговорим чуть позже.

Также еще одной интересной возможностью Smart Security является возможность централизованного управления антивирусными системами, установленными на пользовательских рабочих станциях. Для использования этой возможности необходимо разрешить удаленное администрирование в разделе настроек «Разное → Удален-

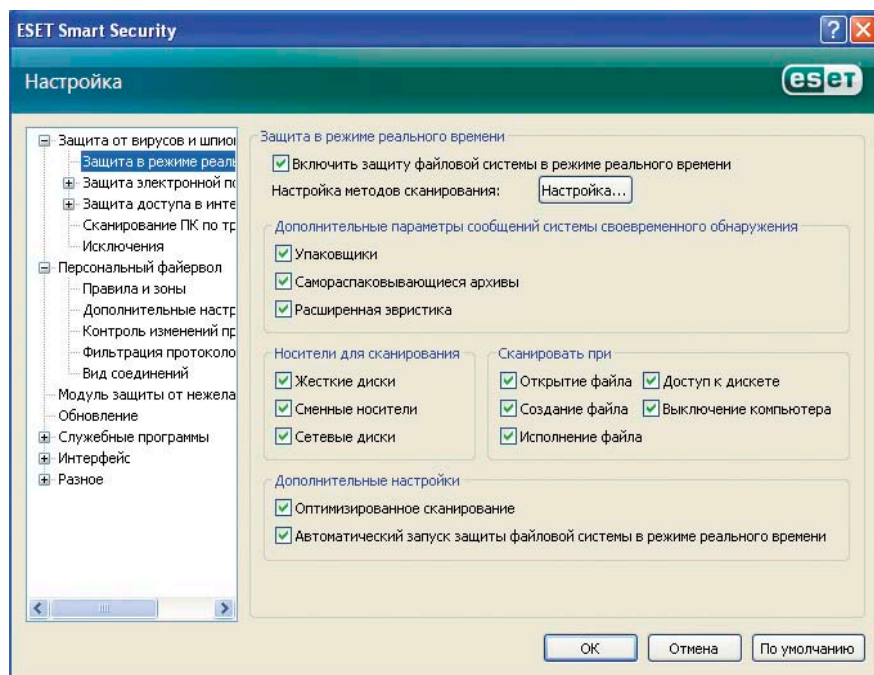


Рисунок 4. Настройка компонентов антивирусной защиты



ное администрирование». Для удаленного управления лучше использовать аутентификацию, в особенности в рамках крупных корпоративных сетей.

## Работа в боевом режиме

Итак, я описал основные возможности ESET NOD32 Smart Security, а также внешний вид, имеющихся интерфейсов и их настройки. Однако описание антивирусной системы было бы не совсем полным, если бы я не привел результаты практических испытаний различных компонентов антивирусной системы. Что касается качества сканирования в различных режимах, то я не стал ограничиваться обнаружением тестовой сигнатуры Eicar, с помощью которой обычно тестируют все антивирусные продукты. В качестве тестовой станции мной была выбрана виртуальная машина под управлением Windows XP SP2, которая использовалась для скачивания файлов из сомнительных источников. Очень часто при посещении различных сайтов на рабочую станцию


пытаются проникнуть и иногда проникают различные вредоносные приложения, так что данная виртуальная машина содержала несколько «нежелательных приложений». Таким образом тестирование проводилось в самых что ни на есть боевых условиях.

После того как на данной машине был установлен Eset NOD 32 Smart Security, на ней было обнаружено более десятка вредоносных и AdWare-приложений. Так что антивирус показал себя очень неплохо, тем более что после очистки с помощью NOD32 я также сканировал данную систему с помощью других антивирусных продуктов, однако не один вредоносный код не был найден. Затем я произвел другой тест: я подключил внешний носитель, содержащий одну из модификаций вируса «Mal\_torun». Антивирус тут же обнаружил данный вредоносный код и успешно его удалил. Также был успешно удален вирус, находящийся в RAR-архиве. Попытка пересылки зараженного файла с помощью

почтового клиента Outlook Express также не удалась, письмо пришло без прикрепленного файла, но с сообщением о том, что вирус был успешно удален.

Что касается практического тестирования работы фильтра нежелательной почты, то для системы, расположенной на рабочей станции пользователя, были получены вполне приличные результаты. В частности, все те сообщения, которые попали в папку в моем бесплатном почтовом ящике, также были обнаружены и фильтром ESET. При этом почтовые сообщения, содержащие спам в виде картинок, также были успешно отфильтрованы.

## Заключение

Завершая свой рассказ об антивирусной системе ESET NOD 32 Smart Security, хотелось бы отметить, что данный продукт является достаточно мощным средством защиты от различных угроз и способен эффективно защитить как рабочую станцию, так и домашний компьютер. 

[Осень...]

Каждую минуту падают сотни, тысячи систем...

...холодный ветер дует в окна...

...и все, что только что двигалось...

...застывает

Реклама

Есть только тысяча и 1 способ сохранить покой в душе  
ВСЕ О СВОБОДНОМ ПРОГРАММНОМ ОБЕСПЕЧЕНИИ

**LINUX**  
**FORMAT**