

Пошаговые Руководства
Сам Себе Админ
системное администрирование
Microsoft Windows



Как эффективно защитить небольшую локальную сеть от вирусов?

Вот и настало время для очередного урока, Друзья ! ☺

Сегодня мы будем защищать нашу сеть от компьютерных вирусов. Поскольку сеть это – несколько, а иногда и – много компьютеров, то и подход здесь должен быть отличным от того, который большинство пользователей применяют для защиты от вирусов одного или двух ПК у себя дома.

Сегодня мы рассмотрим процесс защиты относительно небольшой сети. Думаю, компьютеров 20-30 вполне могут работать, используя схему, описанную ниже.

То, как работают антивирусные программы, мы рассматривали с Вами в одном из прошлых уроков, который назывался «Практика работы с продуктами лаборатории Касперского». В числе прочего, там мы пришли к выводу, что каким бы ни был хорошим (надежным) антивирус сам по себе, он ничего не сможет сделать, не располагая новыми сигнатурами угроз (имея устаревшие антивирусные базы).

Сейчас давайте прикинем в уме, чем же должен отличаться сам подход к защите от вирусов домашнего компьютера и небольшой офисной сети?

Во втором случае уже должен присутствовать элемент планирования, который заключается в том, что намного удобнее, экономнее по количеству Интернет-трафика и, в конечном счете, – безопаснее, если все компьютеры сети получают обновления своих антивирусных баз с одного компьютера в сети, а не скачивают их каждый самостоятельно из Интернета.

Давайте, перечислим основные преимущества такого подхода в виде списка:

1. **Удобство** – (не нужно контролировать каждый компьютер на предмет «обновился антивирус или нет»)
2. **Экономия трафика** – не загружается Интернет-канал, так как основная доля трафика обновлений ложится на локальную сеть организации
3. **Проще с лицензиями** – если мы используем не лицензионное программное обеспечение, то не нужно иметь ключ на каждый компьютер, достаточно установить один (на нужное количество компьютеров) на сервере обновлений

4. **Контроль работы антивируса** – при развертывании серьезной корпоративной антивирусной защиты можно удаленно по сети (в режиме реального времени) наблюдать за работой антивирусных программ на компьютерах пользователей.

Я решил, что четвертый пункт в данной статье мы рассматривать не будем. Прежде всего потому, что для каждой задачи должен быть свой молоток ☺ (инструмент, с помощью которого эту задачу решают). Да и если мы сейчас нагородим все в одной статье, то в голове у Вас образуется сумбур и, вместо того, чтобы стало лучше и понятнее, станет только хуже.

Помните, у нас были две подробные статьи (со схемами и фотографиями) о прокладке и построении компьютерных сетей разного масштаба. Одна из них называлась «Строим простую сеть из 20-ти компьютеров», а вторая – «Сами строим сеть стандарта СКС» ?

Я четко разнес их между собой именно для того, чтобы Вы могли определиться, для каких задач будет использоваться офисная сеть и насколько она может быть большой в далекой (или не очень) перспективе? Согласитесь, нет смысла закупать дорогие коммутационные шкафы и патч панели только для того, чтобы по всем стандартам СКС соединить в сеть пять компьютеров на этаже ☺

Эту статью я назвал: «**Как эффективно защитить небольшую локальную сеть от вирусов?**» и именно о такой небольшой сети и пойдет речь, а развертывание серьезных корпоративных антивирусных приложений мы с Вами, даст Бог, разберем в следующем уроке.

Итак, приступим! Сегодня мы организуем систему антивирусной защиты небольшой компьютерной сети с использованием антивируса NOD от компании «Eset».

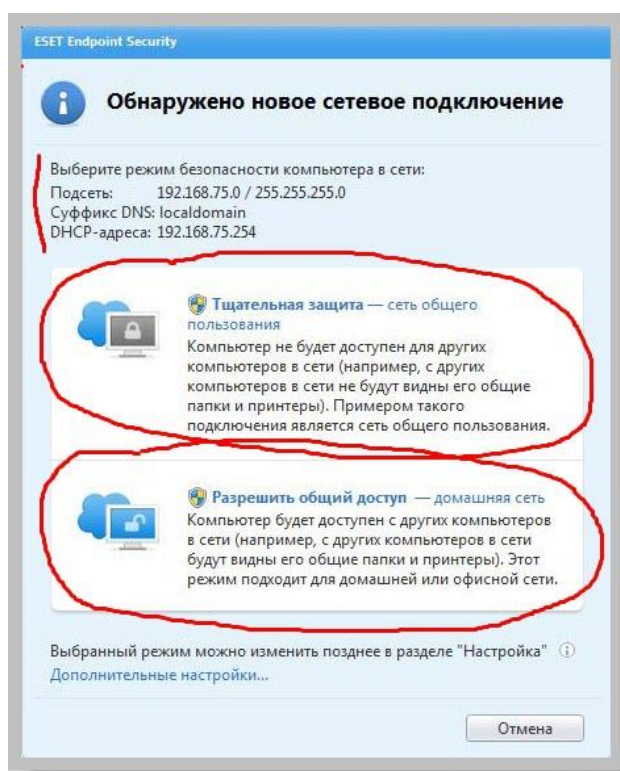
Официальный сайт компании <https://www.eset.com/> а дистрибутивы антивирусных программ, которые мы сегодня будем использовать можно скачать здесь: <https://www.eset.com/int/business/download/>

Работать сегодня мы будем с виртуальными машинами и установленной на одной из них «Windows Server 2008». Опять же, что такое виртуальные машины и как с ними обращаться мы разбирали в одном из наших предыдущих уроков ☺

На операционную систему «Windows Server 2008» мы установим приложение «Eset Endpoint Security» версии №5, сделаем этот компьютер сервером обновлений (в терминологии Eset – «зеркалом») и настроим его так, чтобы клиентские компьютеры загружали обновления антивирусных баз с него.

Сразу скажу, что все продукты антивирусной линейки от «Eset» устанавливаются и настраиваются практически аналогично и имеют почти идентичный и понятный интерфейс. Ради экономии места (в статье и так будет слишком много скриншотов) сам процесс установки антивируса на сервер мы сейчас опустим, (продублируем его чуть позже по ходу статьи) так как в нем нет ничего сложного, а перейдем сразу к настройке программы.

Сразу после инсталляции антивирус «Eset Endpoint Security 5» готов к работе. Компьютер не нужно перезагружать, как в случае с «Касперским». У нас автоматически появится вот такое окно:



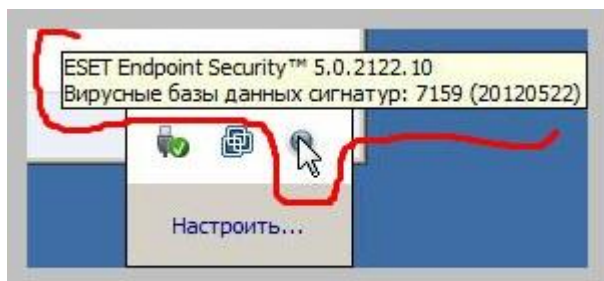
Что это такое? Это – настройки модуля файрвола антивируса (сетевое экран, он же – брандмауэр). Раньше антивирусы выпускались без него (например тот же Eset Nod Antivirus 4 Business Edition), а сейчас все чаще это дополнение для предотвращения атак через сеть стали включать в стандартную конфигурацию программных продуктов.

Итак, что мы видим на фото выше? Поскольку файрвол работает на уровне сетевого адаптера, то он, естественно, должен первым делом взять под контроль все сетевые соединения на компьютере. Вот он и «спрашивает», что мы будем делать с

подсетью 192.168. , в каком режиме ее защищать? В режиме «тщательной защиты» или – «общего доступа»? Сам сетевой адрес 192.168. это – наш местный DHCP, так что на него не обращайтесь сейчас внимания ☺

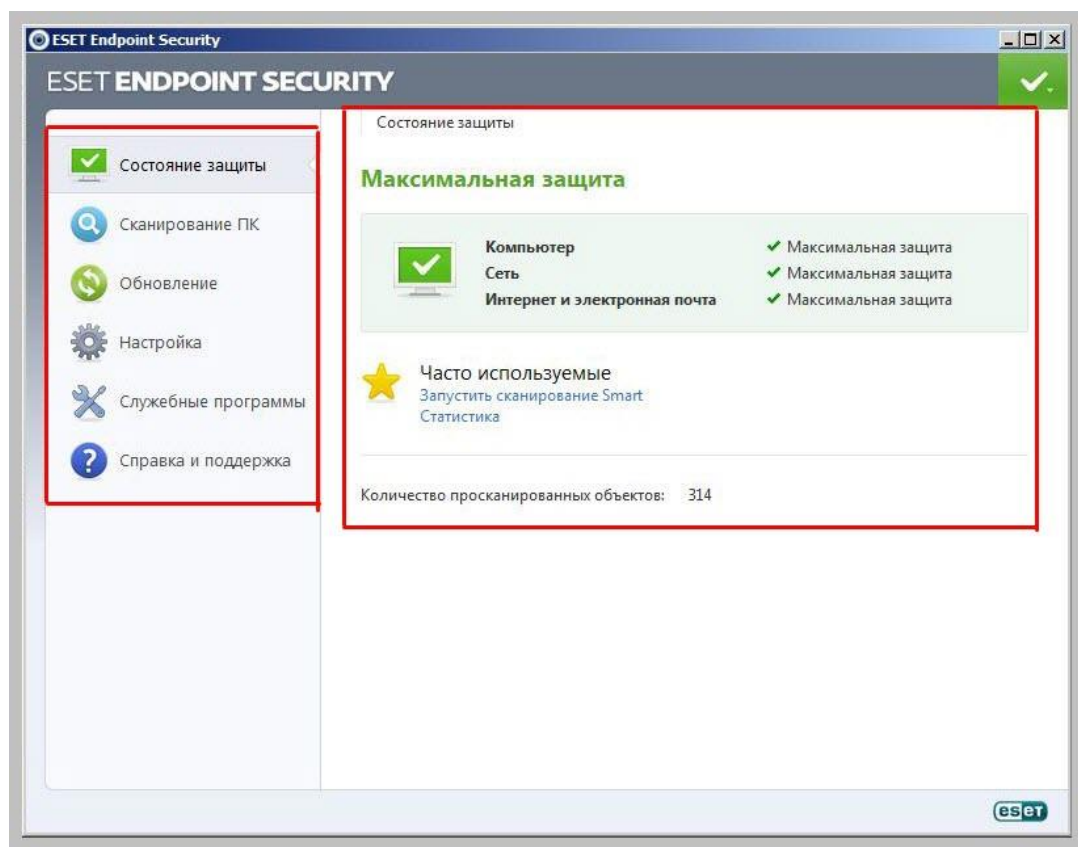
Сейчас не так важно, что мы выберем, но если Вы хотите максимальной защиты для Вашего сервера Windows 2008, то можете выбрать первый вариант.

После этого в трее (на панели задач справа внизу) появится вот такая пиктограмма:



Подведя к ней мышку, можно увидеть версию нашей антивирусной программы, а также – номер и дату выпуска ее антивирусных баз.

Два раза нажимаем левой кнопкой мыши на значке и перед нами открывается главное окно программы:



Как видим, оно разделено на две части: в левой представлены основные настройки и действия, которые может совершать программа, а в правой – дается подробная информация по каждому из пунктов.

Примечание: после инсталляции (установки) любой антивирус должен быть сразу же обновлен! Поскольку он содержит в себе антивирусные базы той актуальности, когда он был загружен с сайта производителя (или из другого источника).

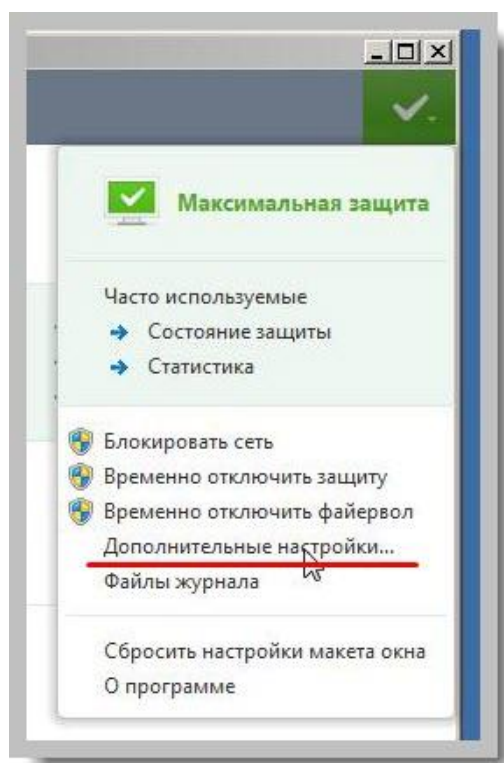
Вот давайте обновлением антивирусных баз и займемся.

Если у нас антивирус – лицензионный (купленный за деньги у дистрибьюторов компании-разработчика), то с этим проблем не будет. А если это не так? ☺

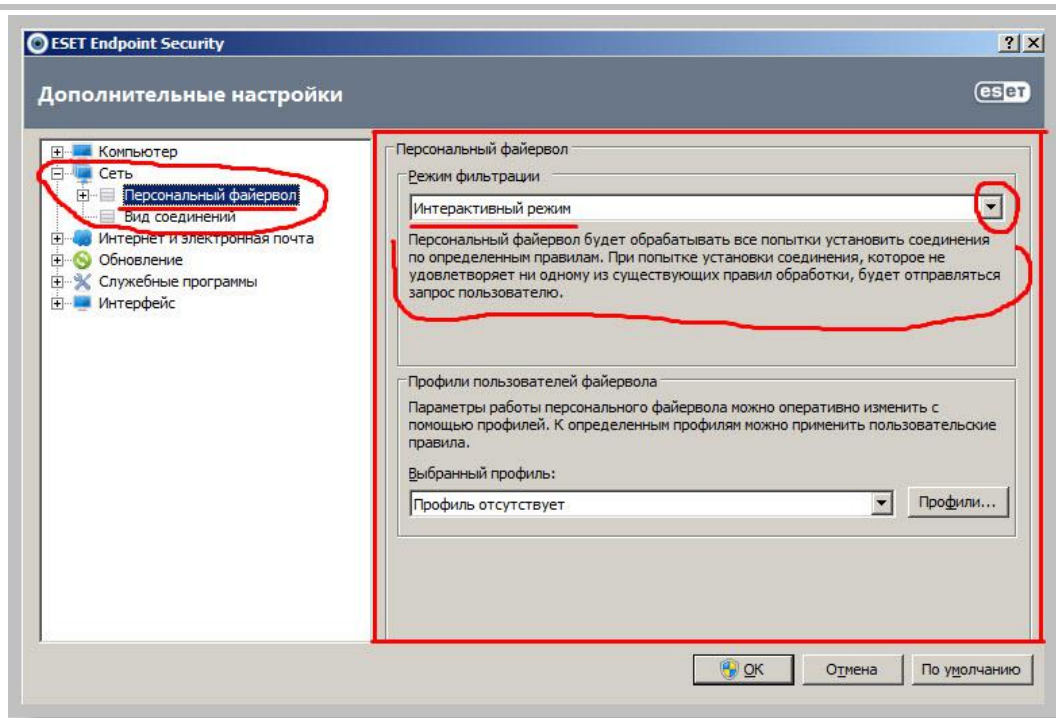
Моя позиция: Выскажу свое личное мнение и никому его навязывать не буду. Те, кто хочет (вынужден в силу обстоятельств, боится каких-то проверок, имеет свободные средства, высокоморальный человек и т.д.) – нужно подчеркнуть ☺ – покупает программное обеспечение и спокойно им пользуется. Все остальные, **полностью понимая возможные последствия, осознанно пользуются** пиратским программным обеспечением. И тут спорить не о чем, Вы либо – в числе первых, либо – во второй группе и готовы нести ответственность (или уверены, что сможете ее избежать) за свои действия.

Возвращаемся к нашей грешной действительности! ☺

Чтобы увидеть, откуда NOD антивирус берет обновления, нам нужно зайти в его настройки. Для этого – один раз щелкаем правой кнопкой мыши по значку антивируса в трее и в появившемся окне выбираем «Дополнительные настройки».



Примечание: к такому же результату приводит нажатие клавиши «F5» в главном окне программы. Очень удобно, рекомендую!



В колонке «Дополнительные настройки» мы видим все основные разделы установок программы, которые мы можем изменять. Они собраны в секции, по названиям которых можно сориентироваться, к какому из разделов программы они относятся. Например: секция «Сеть» отвечает за настройки персонального фаервола и сетевых соединений. В окне справа мы можем настраивать конечные параметры.

Примечание: для того чтобы развернуть соответствующую секцию, нужно щелкнуть мышкой по значку «+» рядом с ней.

Предлагаю Вам персональный фаервол сразу же перевести в «Интерактивный режим» (как показано на фото выше), выбрав его из раскрывающегося списка. Также обязательно прочтите (обведено красным), чем именно хорош этот режим его работы?

Идем дальше! Помните, мы хотели обновить антивирусные базы? Повторюсь, в случае лицензионного продукта – проблем с этим нет. Для второго случая предлагаю выработать альтернативную стратегию!

Прежде всего, как, в общем случае, происходит обновление антивирусных баз? Антивирус через Интернет подключается к сайту разработчика программы, там автоматически проверяется подлинность и срок истечения лицензии программы, и если претензий нет, то – автоматически начинается загрузка обновлений.

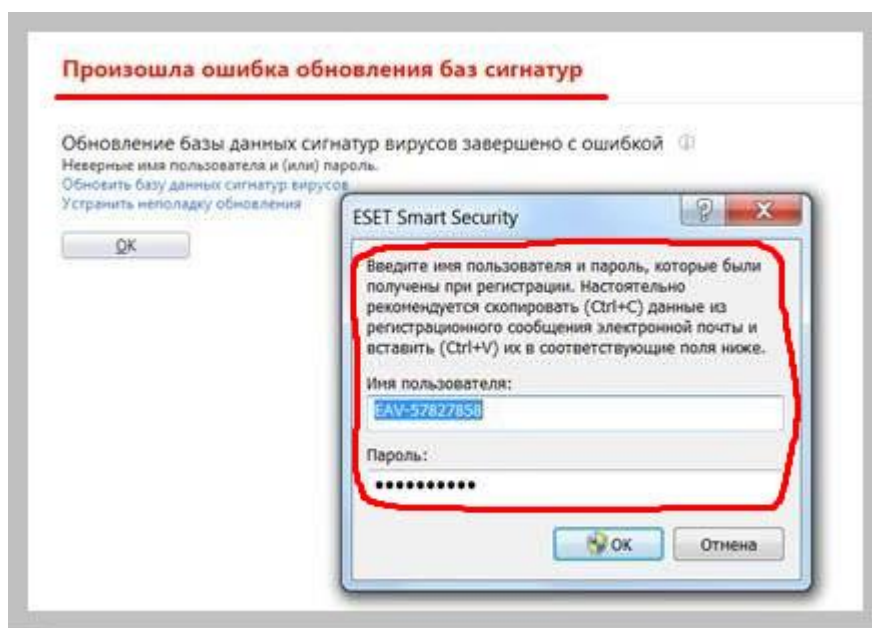
Не знаю, возможно, кому-то кажется, что если каких-то процессов не видно, то они и не происходят? ☺ Именно на этапе проверки подлинности лицензионного ключа (в случае с продуктами лаборатории Касперского) или же – проверки логина и пароля (в случае с Eset NOD) и происходит блокирование, с занесением в черный список, всех

пиратских лицензий и ключей. А если этого сразу не происходит, то – по определенным причинам (о них расскажу в следующей статье ☺). Но рано или поздно все равно ключ «забанят» (заблокируют) и нужно быть к этому готовым! А еще лучше – перестать зависеть от этого. Давайте расскажу, как делаю я?

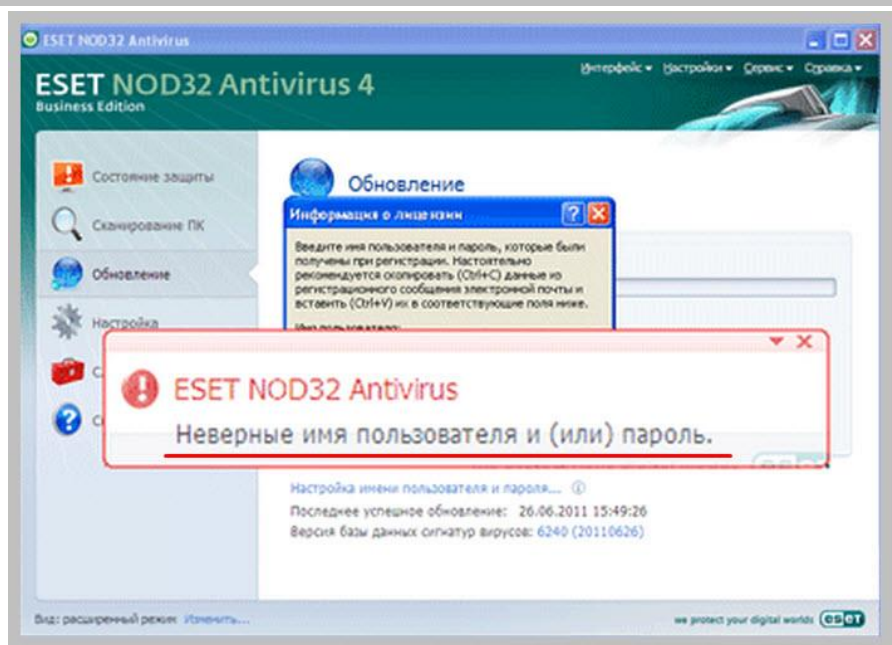
В случае с продуктами «NOD» от компании «Eset» мы имеем дело с логином (именем пользователя) и паролем, которые нам выдаются на год при покупке лицензии. Обычная практика «альтернативного» метода состоит в том, чтобы некоторое время пользоваться официальным триальным (временным) логином и паролем, которые распространяет сама компания «Eset».

Проблема в том, что таким методом начали пользоваться очень многие, и подобные комбинации «логин-пароль» стали очень быстро блокироваться при проверках на сайтах обновлений.

Если учетные данные заблокированы, то при попытке обновления Вы можете увидеть вот такое окно:



Вот – еще один пример:



Получается, опять нужно искать новый (не «спаленный» кем-то) пароль, найти в сотне не рабочих один единственный, по которому можно успешно обновить антивирусные базы, чтобы через несколько дней, и он оказался заблокированным! И так – по кругу. Приходит момент, когда Вы только и занимаетесь, что ищете рабочие ключи и пароли (немного утрирую, конечно, но Вы меня поняли ☺).

Я сам, в свое время, проходил эту «карусель», поэтому хорошо ее себе представляю. Сначала ключи работали по несколько месяцев, потом – недель, но когда счет пошел на дни, я понял, что нужно придумать какое-то другое (эффективное и, по возможности, простое) решение.

Локальная сеть, которую я тогда обслуживал, насчитывала около тридцати компьютеров и антивирусная защита на базе «Eset Nod32 Business Edition» успешно справлялась со всеми угрозами. Менять ничего не хотелось. Нужно было только решить возникшую проблему с обновлением.

Было решено поступить следующим образом: в Интернете есть сайты, дающие возможность бесплатно скачать **оффлайн обновления** к различным антивирусам (антивирус касперского, NOD32 и т.д.). Попробуйте ввести в строку поиска «оффлайн обновление NOD32», посмотрите, что получится ☺

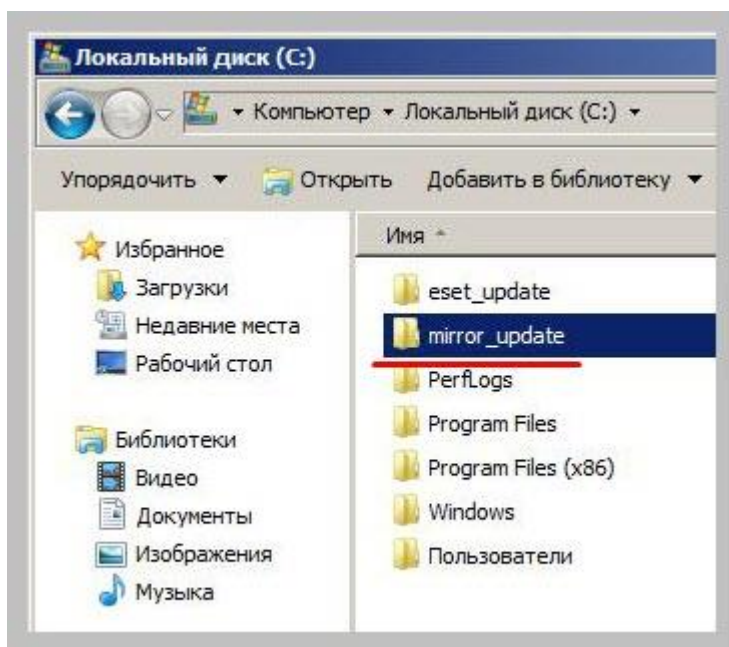
Примечание: оффлайн обновление это – архив с антивирусными базами программы, актуальными на момент выкладывания файла в сеть. Например, на 21.11.2012-го. Подобные обновления, как правило, выкладываются раз в неделю (или через день), так что, регулярно скачивая их и «скармливая» эти файлы нашему антивирусу, мы всегда будем иметь актуальные базы сигнатур и без всяких ключей!

Только нужно быть внимательным, скачивая файлы именно для Вашей версии программы! В случае с NOD32 это может выглядеть так, как показано на фото ниже:



Для версии программы «3» и «4» мы используем верхнюю ссылку, а для «5» и «6» – нижнюю. Ребята, как правило, выкладывают подобные архивы на файлообменниках, поэтому – скачиваем, разархивируем и отдаем «на съедение» нашему антивирусу ☺

Я сделал следующее: создал на сервере две папки «eset_update» и «mirror_update» (названия могут быть любыми). Пока нас будет интересовать вторая.

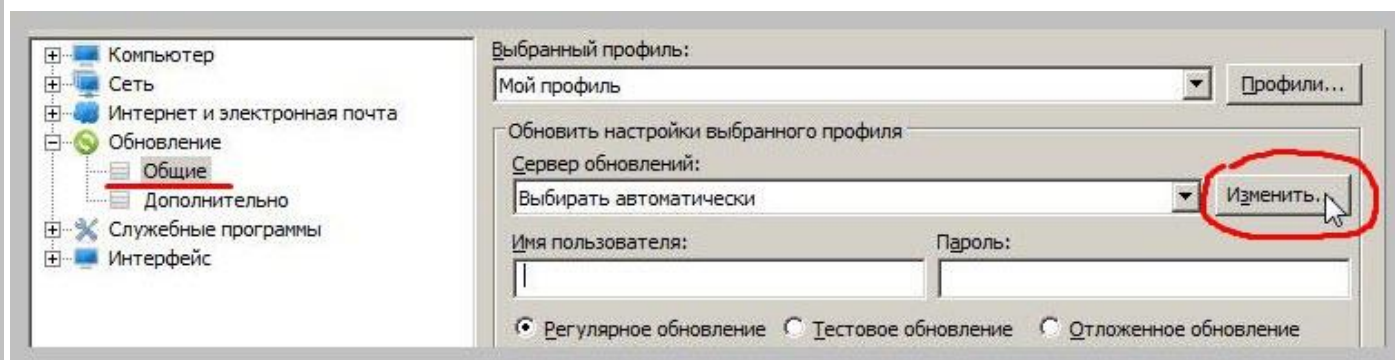


Это будет папка, в которую мы будем записывать скачанные из Интернета оффлайн обновления для нашего «Eset Endpoint Security» версии «5». Вот так должны выглядеть разархивированные файлы обновлений сигнатур, которые мы будем туда помещать.

Имя *	Дата изменения	Тип	Размер
em000_32_10.nup	21.10.2012 9:38	Файл "NUP"	55 КБ
em000_64_10.nup	21.10.2012 9:38	Файл "NUP"	66 КБ
em001_32_10.nup	21.10.2012 9:38	Файл "NUP"	502 КБ
em001_32_11.nup	21.10.2012 9:38	Файл "NUP"	22 КБ
em001_32_12.nup	21.10.2012 9:38	Файл "NUP"	62 КБ
em002_32_10.nup	21.10.2012 9:38	Файл "NUP"	34 219 КБ
em002_32_11.nup	21.10.2012 9:38	Файл "NUP"	5 509 КБ
em002_32_12.nup	21.10.2012 9:38	Файл "NUP"	789 КБ
em003_32_10.nup	21.10.2012 9:38	Файл "NUP"	735 КБ
em004_32_10.nup	21.10.2012 9:38	Файл "NUP"	809 КБ
em004_32_11.nup	21.10.2012 9:38	Файл "NUP"	22 КБ
em004_32_12.nup	21.10.2012 9:38	Файл "NUP"	20 КБ
em005_32_10.nup	21.10.2012 9:38	Файл "NUP"	29 КБ
em005_32_11.nup	21.10.2012 9:38	Файл "NUP"	42 КБ
em005_32_12.nup	21.10.2012 9:38	Файл "NUP"	13 КБ
em006_32_10.nup	21.10.2012 9:38	Файл "NUP"	11 КБ
em006_32_11.nup	21.10.2012 9:38	Файл "NUP"	87 КБ
em006_32_12.nup	21.10.2012 9:38	Файл "NUP"	11 КБ
em006_64_10.nup	21.10.2012 9:38	Файл "NUP"	11 КБ

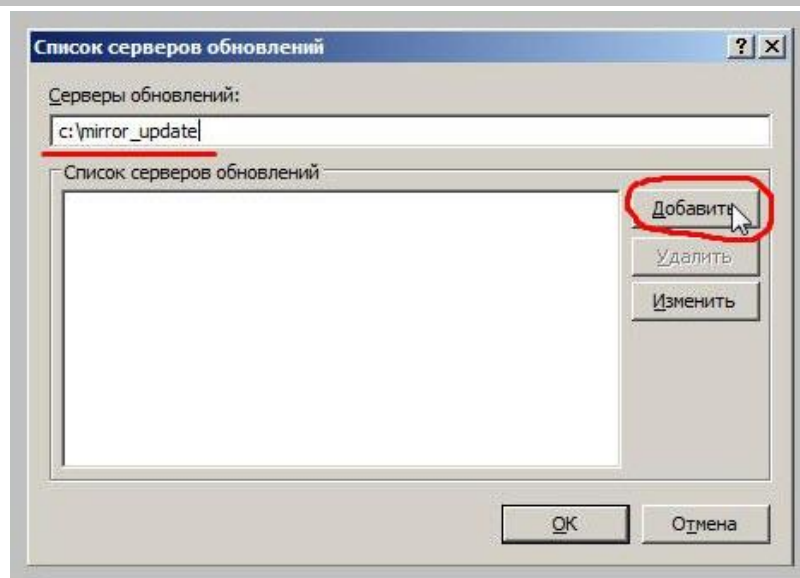
После этого нам остается только указать нашей антивирусной программе эту папку «mirror_update», как источник своего обновления.

Для этого – заходим в дополнительные настройки. Помните про клавишу «F5»? ☺ Раскрываем раздел «Обновление» и нажимаем на пункт «Общие». В правой части окна мы увидим соответствующие настройки.



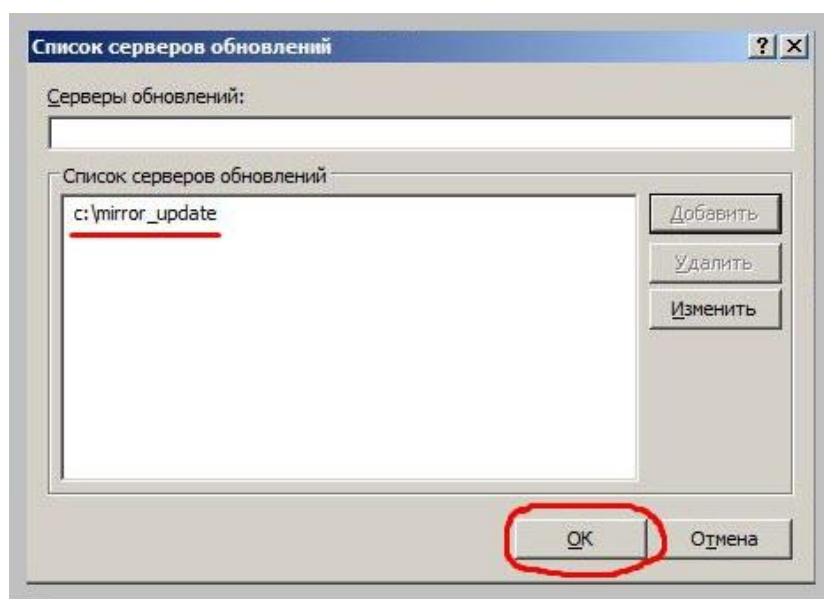
Нас будет интересовать поле «Сервер обновлений», в котором сейчас написано «Выбирать автоматически». Это – раскрывающийся список, из которого мы можем выбрать сервера обновлений компании «Eset», но к чему это (в случае отсутствия лицензии) приводит, мы рассматривали чуть выше ☺

Поэтому мы сами создадим для себя свой источник обновления! Нажимаем кнопку «Изменить» и видим вот такое окно:



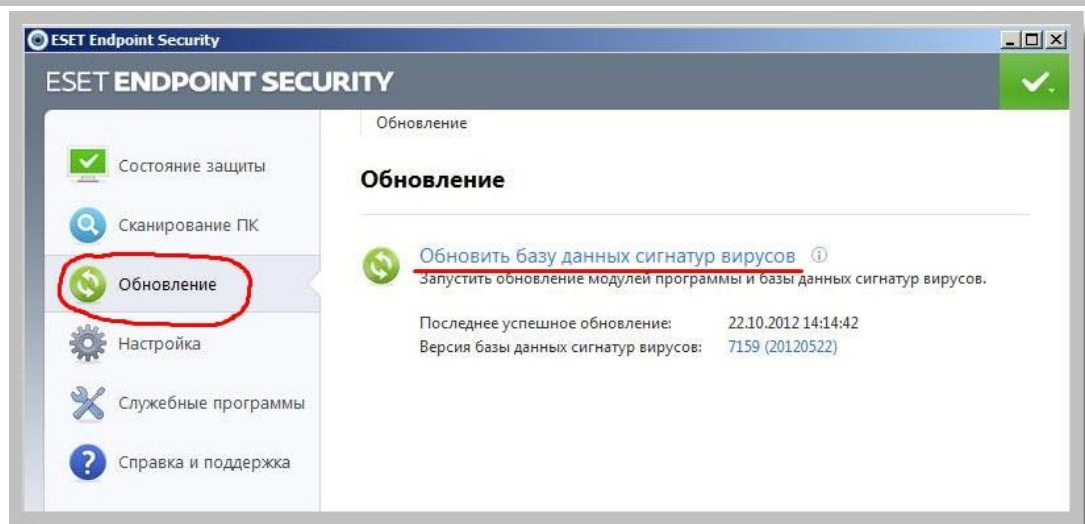
Здесь в ручном режиме, спокойно и внимательно прописываем полный путь (начиная от корня диска) к папке, в которую мы поместили наши оффлайн обновления. В моем случае это – **c:\mirror_update**

Нажимаем кнопку «Добавить» и в поле «Список серверов обновлений» появится наше расположение:

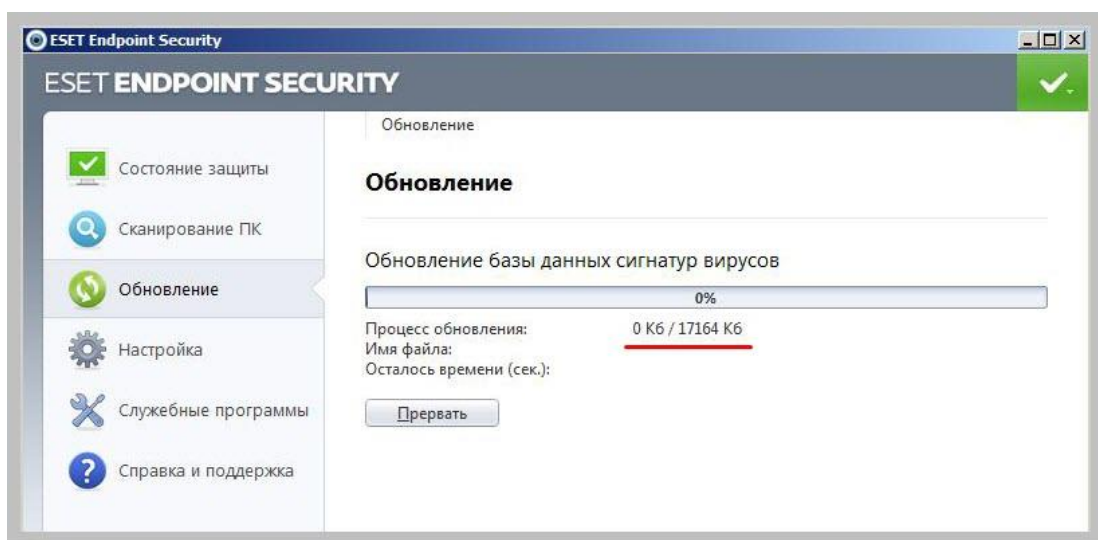


Нажимаем кнопку «ОК».

Теперь, следите внимательно, в главном окне программы переходим к пункту «Обновление» и правой части окна нажимаем на надпись «Обновить базу данных сигнатур вирусов».

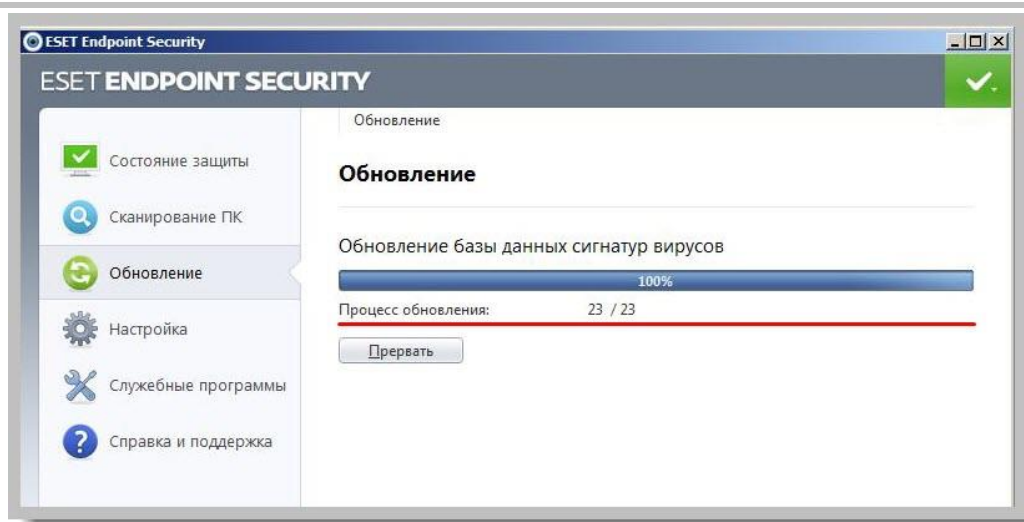


Если на предыдущих шагах настройки мы все сделали верно, то увидим вот такую картину:



Вверху расположена полоса прогресса обновления, а чуть ниже показано, сколько мегабайт антивирусных баз добавит «Eset Endpoint Security» к своим, уже существующим базам?

После загрузки, а поскольку она происходит из папки локального диска «С» - процесс пройдет быстро, мы увидим следующее:



Вот теперь – действительно все нормально и обновление прошло успешно! В самом конце вместо кнопки «Прервать» появится «ОК», а в трее справа мы увидим соответствующее всплывающее уведомление. Первый этап выполнен, можем похлопать себя по плечу 😊

Теперь, когда нам нужно будет обновить наш антивирус на сервере, мы просто загрузим из Интернета архив с новым **оффлайн обновлением**, разархивируем его, поместим в папку, которую мы установили, как сервер обновлений и обновимся с нее!

Внимание! Перед копированием новых файлов в локальную папку обновлений **все** находящиеся в ней старые файлы должны быть удалены! Иначе в процессе обновления весьма вероятна ошибка.

Возможно, кто-то возразит мне, что для Eset NOD давно есть специальные программы для поиска «вечных» ключей? Не знаю, как насчет «вечных», но то, что такие программы устанавливают в операционную систему то, что я, как администратор, не могу контролировать, так это – точно! Как «оно» работает – не понятно, какие еще данные и кому передает с моего компьютера – тоже не ясно? И, к тому же, подобные программы периодически тоже «глючат» и перестают работать и что тогда делать человеку, который больше ничего не умеет, кроме как установить «супер-мега крик для всего»? 😊 Остается только судорожно искать альтернативу (другой такой же мега-крик)! А я хочу, чтобы Вы так не поступали и **сами** управляли ситуацией, а не она Вами. Короче говоря, я хочу, чтобы Вы были **сами себе админами!** 😊

Насколько же часто нужно обновлять антивирус? Для себя я решил так: один раз в неделю (или даже две) – вполне достаточно! Очень маловероятно, что Вы «подхватите» какой-то очень новый и «экзотический» вирус. Хотя, никто не мешает Вам обновляться,

хоть каждый день, главное – строго придерживайтесь того графика обновлений, который выбрали и все у Вас будет отлично! ☺

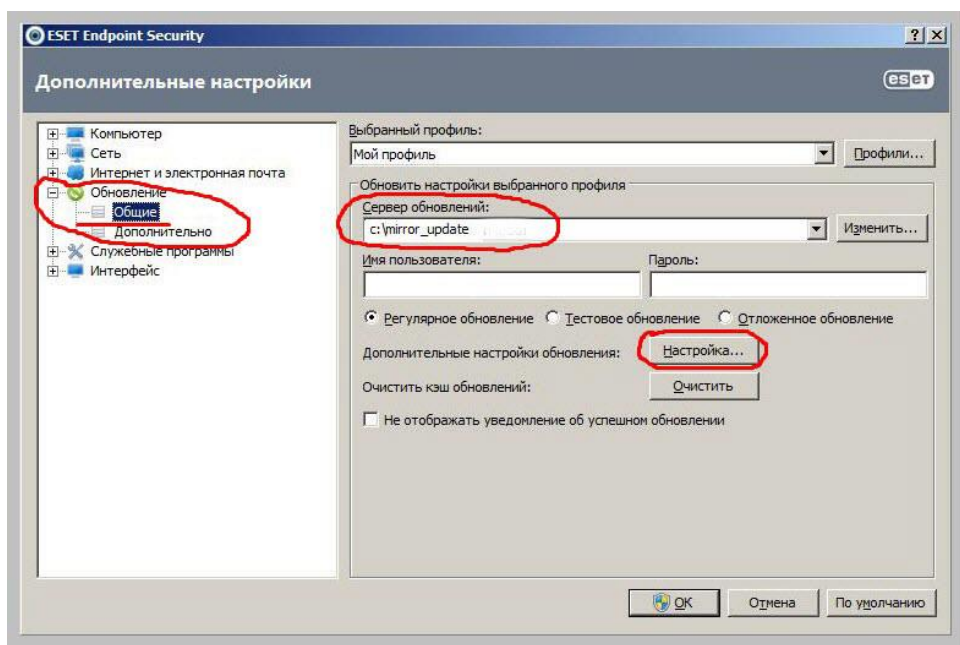
Двигаемся дальше?

Сверимся с нашими основными задачами, у нас их было две:

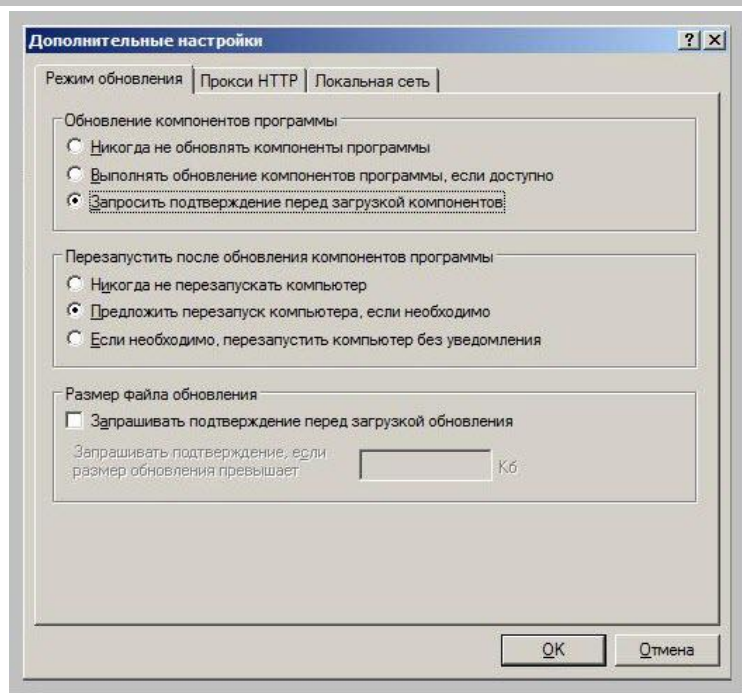
1. Настроить сервер обновлений для антивируса на Windows Server 2008
2. Сделать этот антивирус «зеркалом обновлений» для всей локальной сети

С первой мы героически справились :) беремся за вторую!

Заходим в дополнительные настройки (по «F5»), убеждаемся, что в поле «Сервер обновлений» прописано то, что нам нужно и возле надписи «Дополнительные настройки обновления» нажимаем кнопку «Настройка».

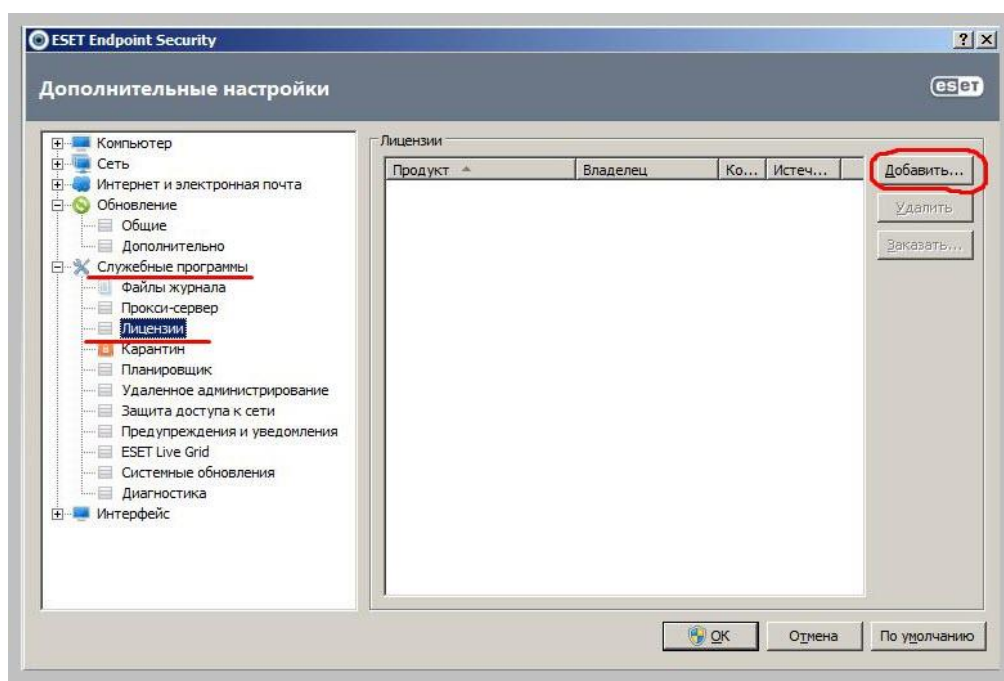


Появится вот такое окно:



Обратите внимание на три вкладки сверху. Просто запомните пока, что их – **три** ☺

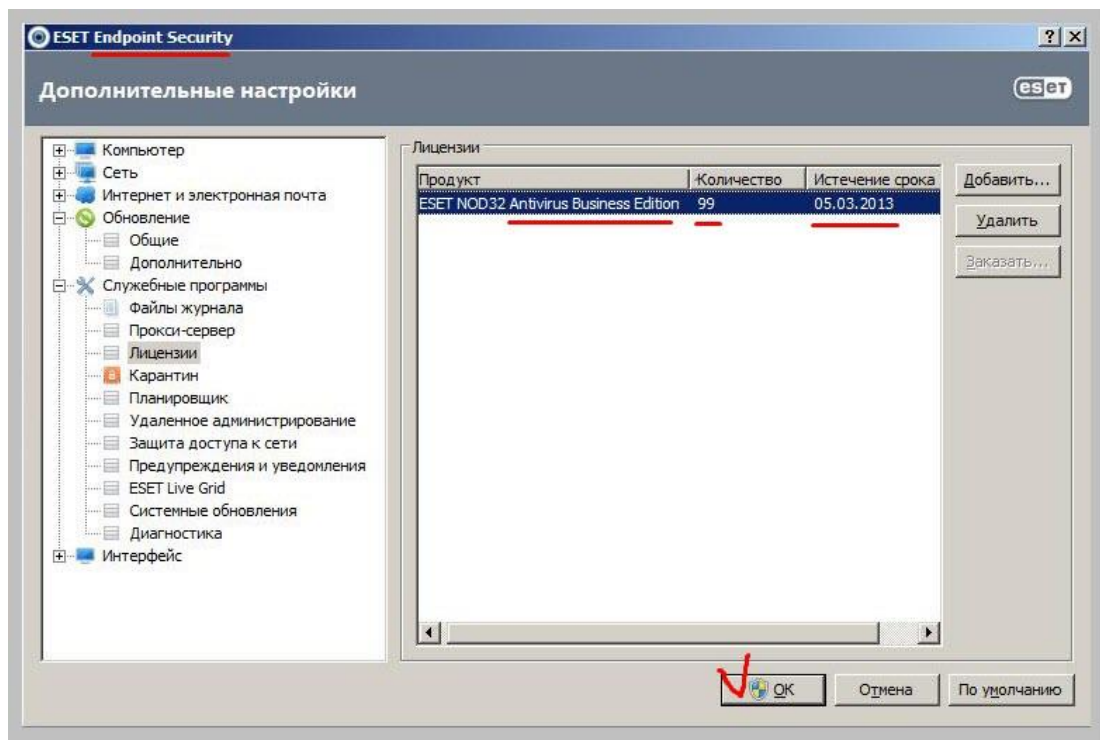
Хорошо, закрываем окно и возвращаемся к предыдущему. Разворачиваем позицию «Служебные программы» и переходим в пункт «Лицензии».



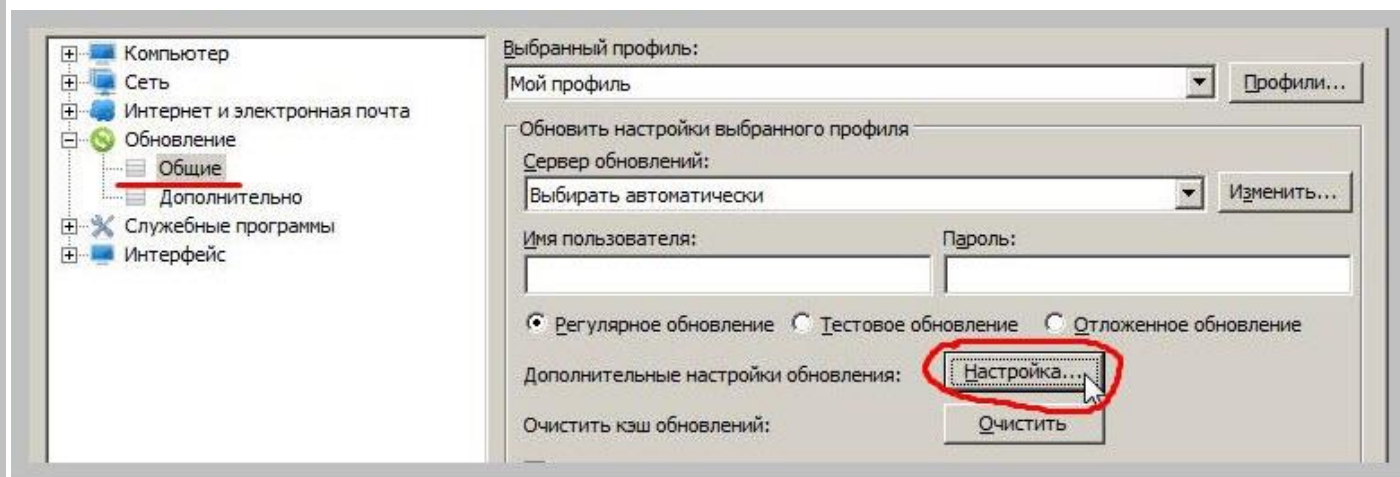
Справа сверху нажимаем на кнопку «Добавить» и выбираем файл лицензии (его размер – один килобайт), в нем указано, что данный программный продукт может использоваться в качестве зеркала обновления, и прописана информация о максимальном количестве компьютеров, которое (согласно лицензии) может обслуживать «зеркало», плюс – указана дата ее окончания.

Примечание: файл лицензии для Eset NOD32 на любое количество компьютеров и практически любую дату при наличии Интернета не является тем препятствием, которое может стать оправданием нашей с Вами лени! ☺

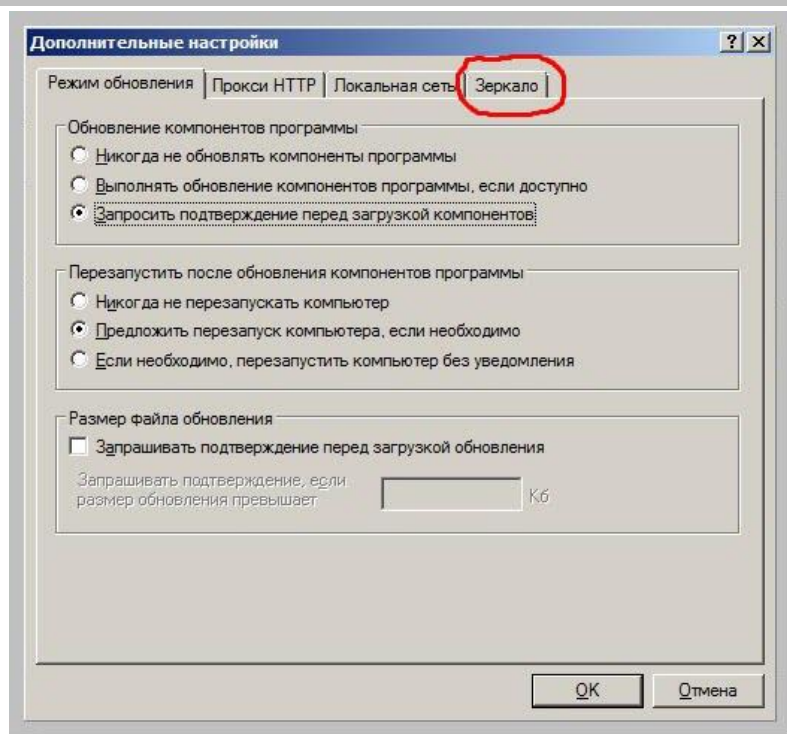
На фото ниже мы добавили файл лицензии на 99 компьютеров, срок действия которого заканчивается 05.03.2013-го года.



Нажимаем кнопку «ОК» и вот теперь, смотрим внимательно ☺



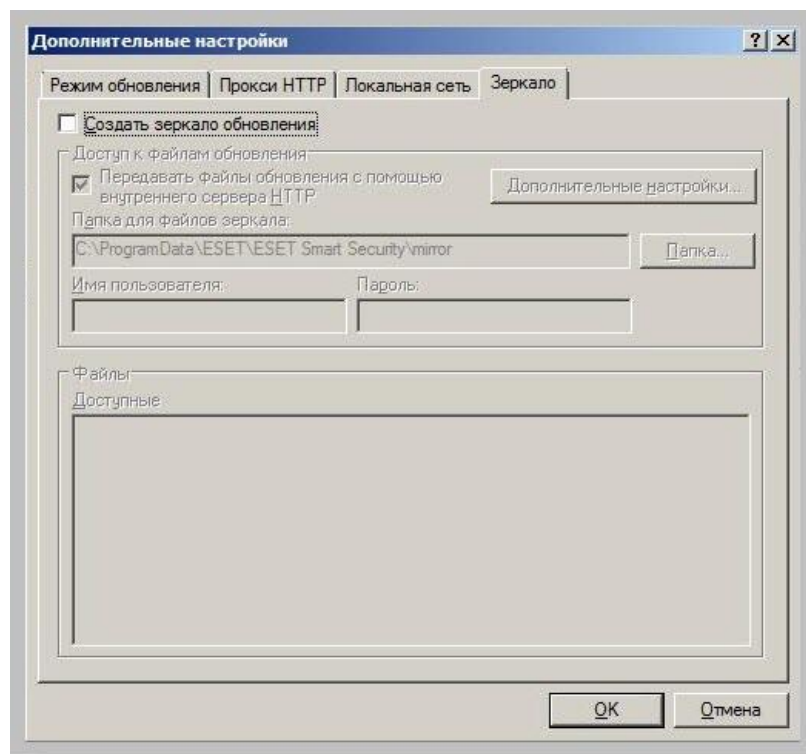
Еще раз проверим, что скрывается под кнопкой «Настройка»?



Вот чудеса! У нас появилась новая вкладка «Зеркало» (помните, до установки файла лицензии здесь было только три вкладки?).

Примечание: всегда будьте психологически готовы к тому, что после регистрации (активации) программного продукта в нем могут появиться дополнительные функции или – разблокироваться недоступная ранее функциональность.

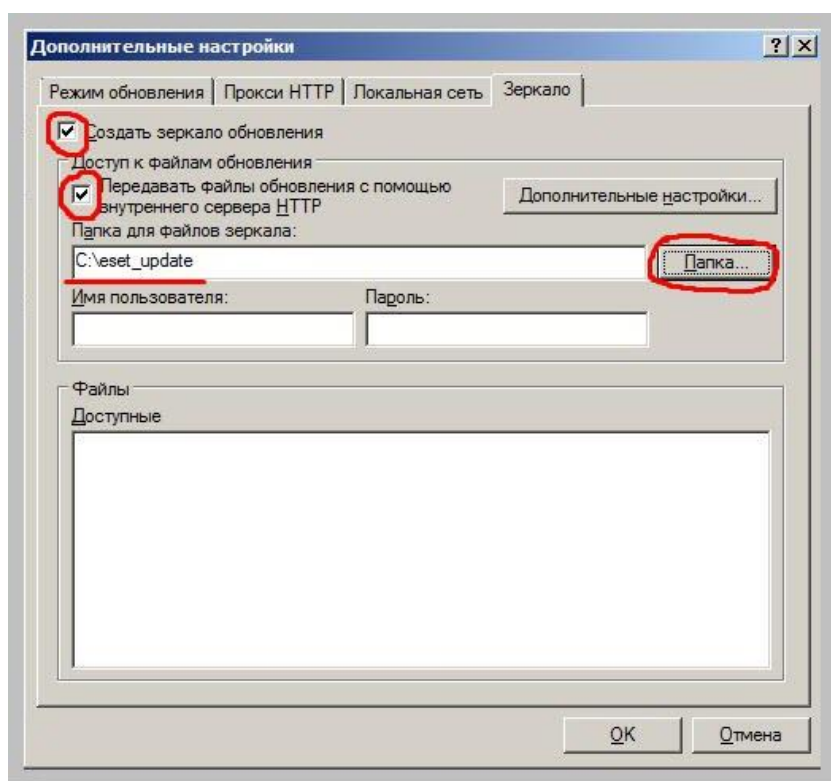
Переходим на новую вкладку, и будем создавать свое зеркало обновлений!



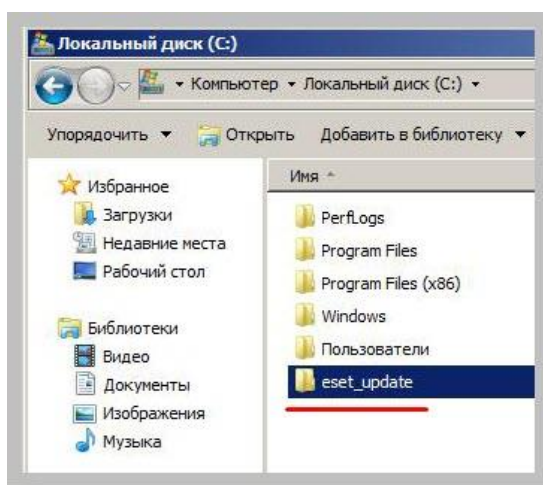
Отмечаем галочкой пункт «Создать зеркало обновления». После этого становятся активными все нужные нам опции. Также проследите, чтобы активным был второй пункт

(Передавать файлы обновления с помощью внутреннего сервера HTTP). Это – интегрированное в Eset NOD небольшое серверное приложение, которое по протоколу «http» предоставляет обновления антивирусных баз для нашей локальной сети.

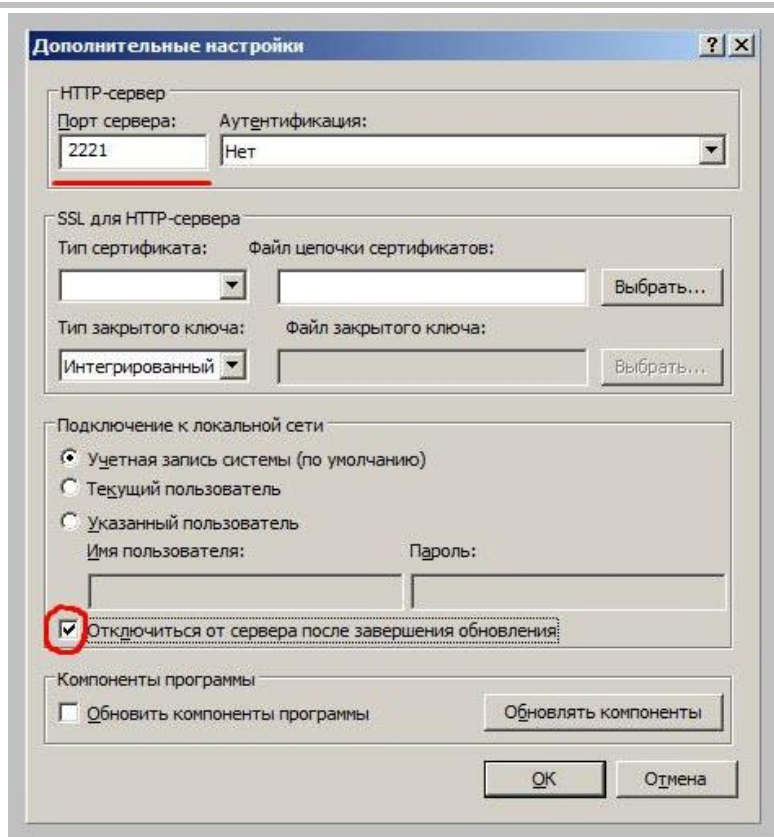
Дальше – важная настройка! В поле «Папка для файлов зеркала» нам нужно указать заранее созданный нами каталог «eset_update» (можете выбрать свой собственный). Для этого нажимаем кнопку «Папка» и в открывшемся окне проводника выбираем наш каталог.



Вот таким образом:



Теперь давайте заглянем в «Дополнительные настройки» (кнопка возле надписи «Передавать файлы обновления с помощью внутреннего сервера HTTP»)



Что нам здесь интересно? По умолчанию сервер обновлений (зеркало) будет ожидать входящих соединений по сети от станций-клиентов (с целью обновления) на порт под номером «2221». При желании можете его поменять (лично я оставил, как есть).

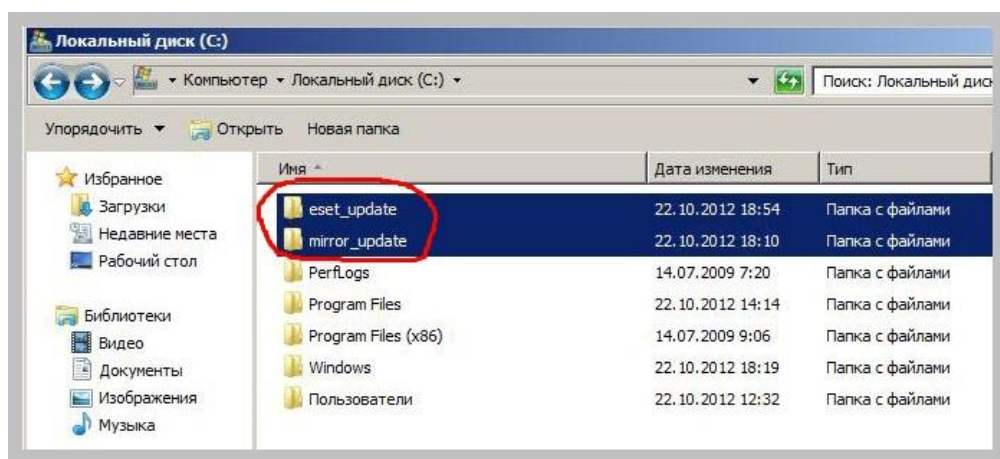
Примечание: что такое порт? Представим себе, что на одном компьютере установлено большое количество разных программ (так оно, как правило, и бывает). Некоторая часть из них взаимодействует с сетью (локальной или Интернет) и эти программы должны обмениваться с сетью какими-то данными, что-то принимать, отсылать и т.д. И получается так, что сетевой IP адрес у компьютера один, а программ, которые работают с сетью – много. Если бы внешняя сеть, пересылая данные для этого компьютера, просто отправляла их на его IP адрес, то программы не смогли бы разобраться, для какой именно из них предназначены те или иные пакеты данных? Для устранения этой неразберихи и было введено понятие «порты». Это – виртуальное пространство адресов (всего - **65536**), из которого каждая программа, которой это нужно, может брать любой понравившийся (установленный программистом при ее создании) порт и работать с ним. Как видим, зеркало обновлений нашего Eset NOD работает через 2221-й порт. Что это значит? Если из сети приходит запрос на порт номер 2221, то Eset «знает», что этот запрос предназначенся именно ему и начинает с ним работать (в данном случае – предоставляет обновления антивирусных баз). Другая программа может использовать любой другой порт и «слушает» ожидает сетевого соединения именно по

этому номеру порта. Есть начальный диапазон портов (первые 1024), которые зарезервированы системой под «стандартные» протоколы и программы. Например: за «http» сервером, как правило, закреплён порт номер «80» (хотя никто не запрещает поменять этот номер в процессе настройки самого сервера), для «ftp» доступа существует стандартный порт «21», безопасное «SSH» сетевое соединение работает с портом «22» и т.д.

Итак, с портами разобрались, двигаемся дальше!

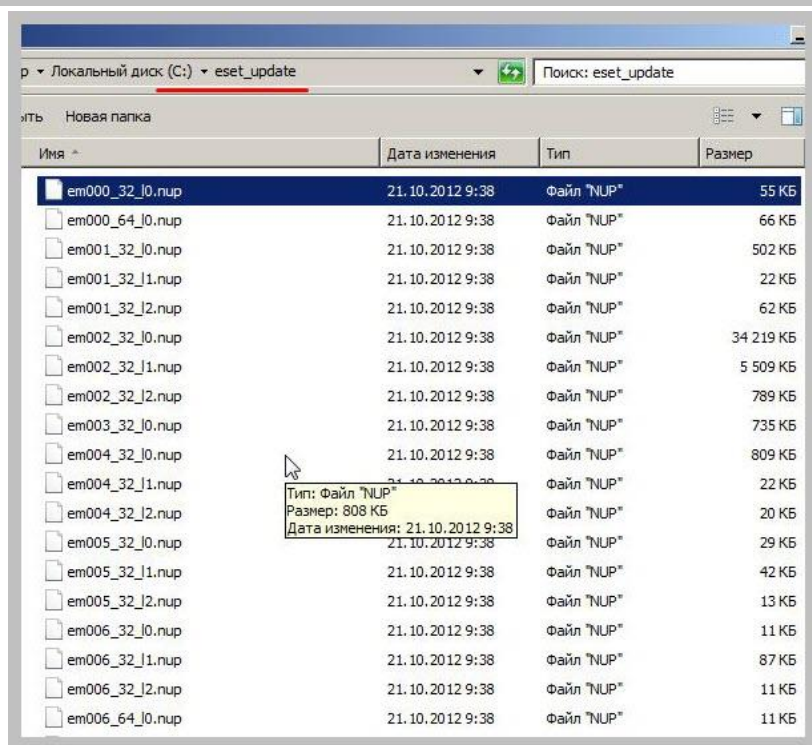
На скриншоте выше можете поставить галочку напротив пункта «Отключиться от сервера после завершения обновления». Зачем нам поддерживать лишнее активное сетевое соединение с «клиентом» (компьютером пользователя), который уже получил обновление? Включать аутентификацию я смысла не вижу. Мы ведь хотим упростить задачу распространения антивирусных баз, а не усложнить ее ☺

Закрепим ещё раз то, что мы проделали на данном этапе: мы создали на диске «С» две папки: «eset_update» и «mirror_update».



В «mirror_update» мы разархивируем скачанные нами из Интернета оффлайн обновления антивирусных баз и обновляем с этой папки наш «Eset Endpoint Security 5», а каталог «eset_update» - является «зеркалом обновления» для всей локальной сети. Компьютеры пользователей автоматически (по расписанию) по «http» протоколу подключаются к серверу обновлений на порт 2221 и скачивают недостающие базы.

Если Вы заглянете в эти папки после первого обновления, то увидите, что находящиеся там файлы – абсолютно идентичны (Eset NOD просто дублирует свои базы в папку сетевого «зеркала»).

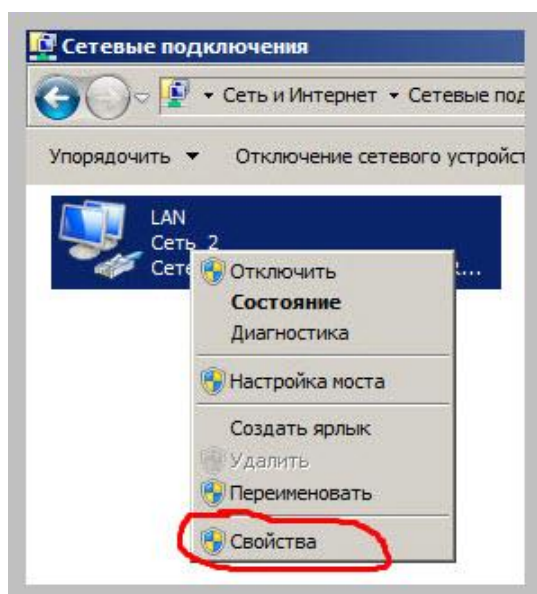


Отлично, процесс обновления и настройку «зеркала» мы закончили, теперь давайте будем проверять, как это все работает на практике! ☺

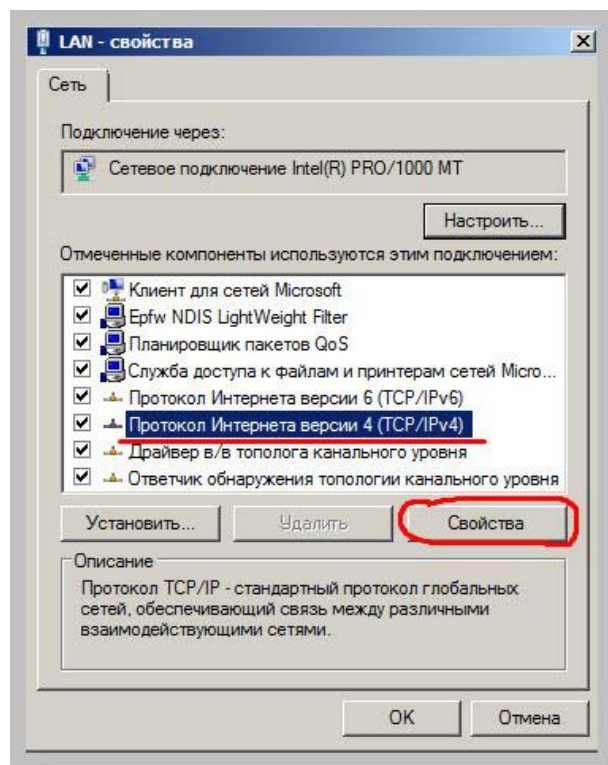
Для начала, организуем сеть между нашим Windows Server 2008 и клиентским компьютером под управлением Windows XP (под Windows 7 все точно, так же, просто она занимает больше оперативной памяти на виртуальной машине, а у меня ее, – всего 2 гигабайта).

Давайте присвоим нашему серверу персональный IP адрес и дадим гордое имя ☺

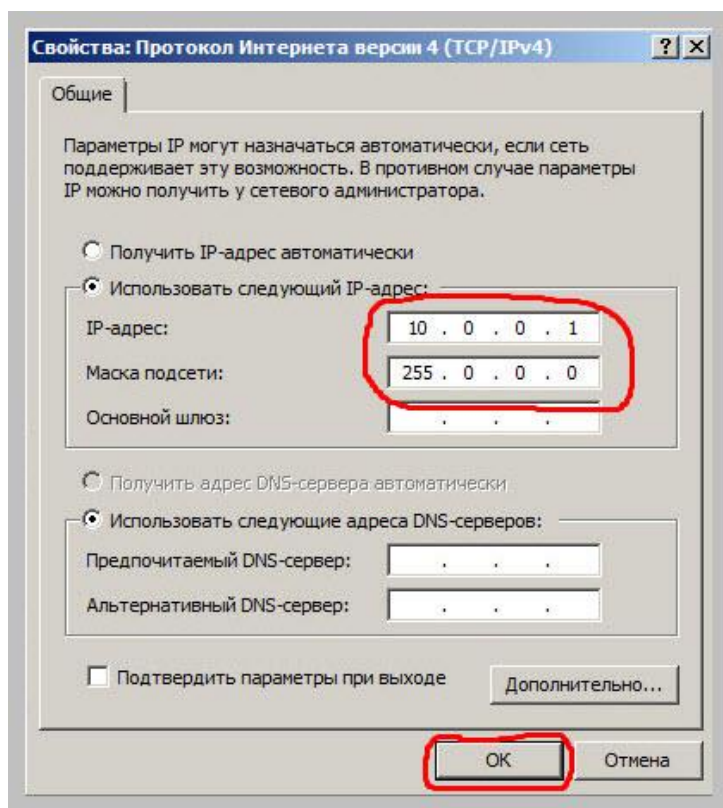
«Идем» в наши сетевые соединения, нажимаем правой кнопкой мыши на подключении. Из раскрывшегося меню выбираем пункт «Свойства».



Отмечаем «Протокол Интернета версии 4 (TCP/IPv4)» и нажимаем кнопку «Свойства».



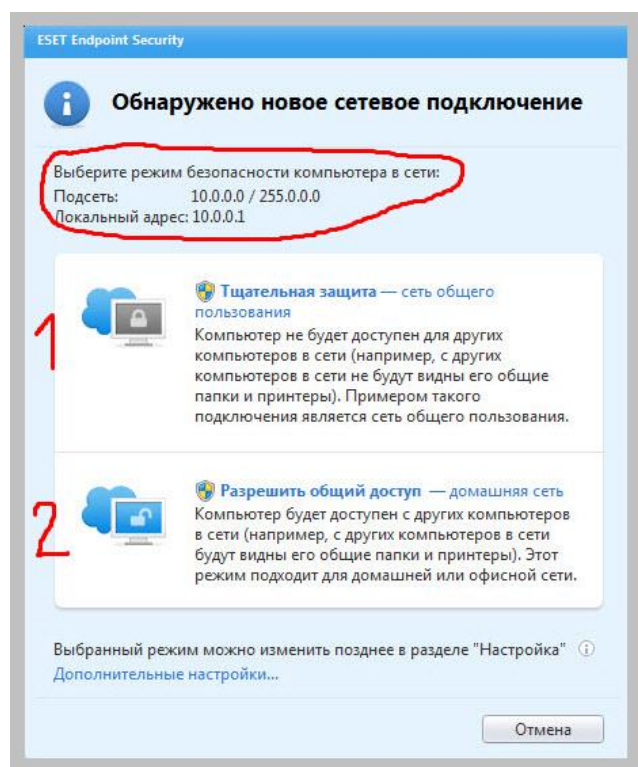
Попадаем в окно установки сетевого адреса ОС:



Отмечаем радиобокс «Использовать следующий IP-адрес» и в открывшемся поле вводим 10.0.0.1, щелкнув в поле «Маска подсети», видим, что «маска» проставилась

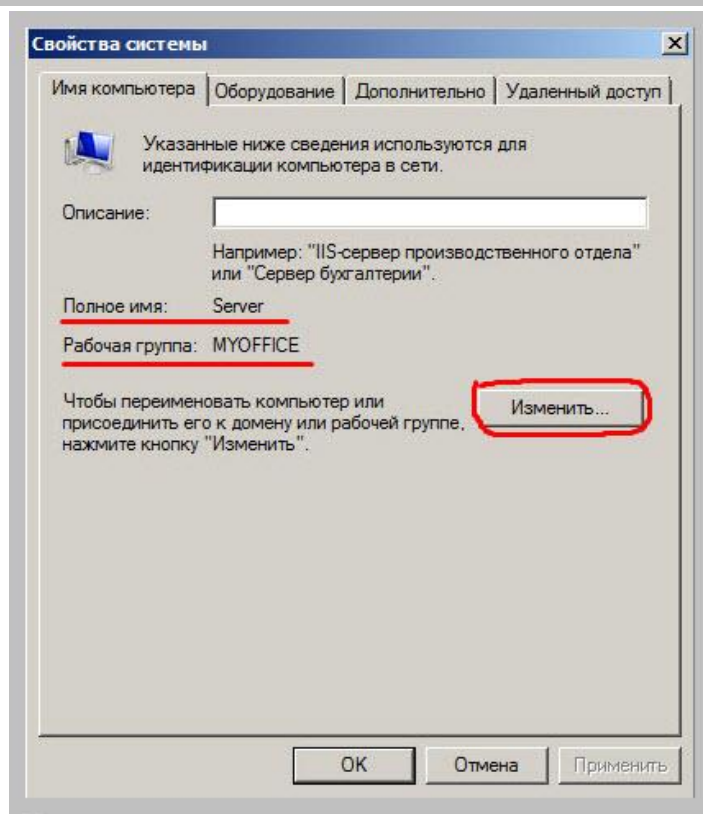
автоматически (в соответствии с типом выбранной нами сети класса «А» - 10.0.0.1). Нажимаем кнопку «ОК», завершая настройки.

Сразу после этого у нас перед глазами появляется вот такое окно:



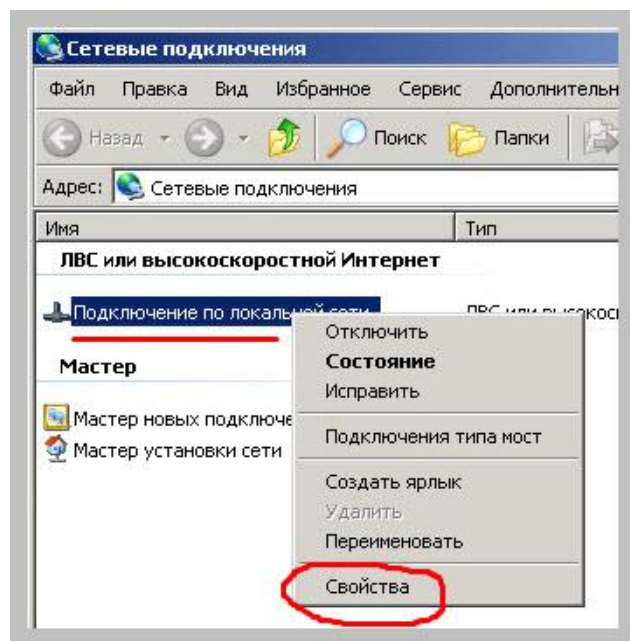
Это – следствие установленного вместе с антивирусом модуля фаервола (он «увидел», что сетевые настройки изменились, и предлагает нам выбрать режим защиты для этого «нового» для него соединения). Какой из вариантов (первый или второй) Вы здесь выберете – решайте сами, тем более, что все это можно изменить впоследствии и по необходимости.

А сейчас – зайдем в дополнительные параметры системы и, для порядка, поменяем имя нашего Windows Server 2008. Нажимаем там на кнопку «Изменить» и задаем параметры по желанию.

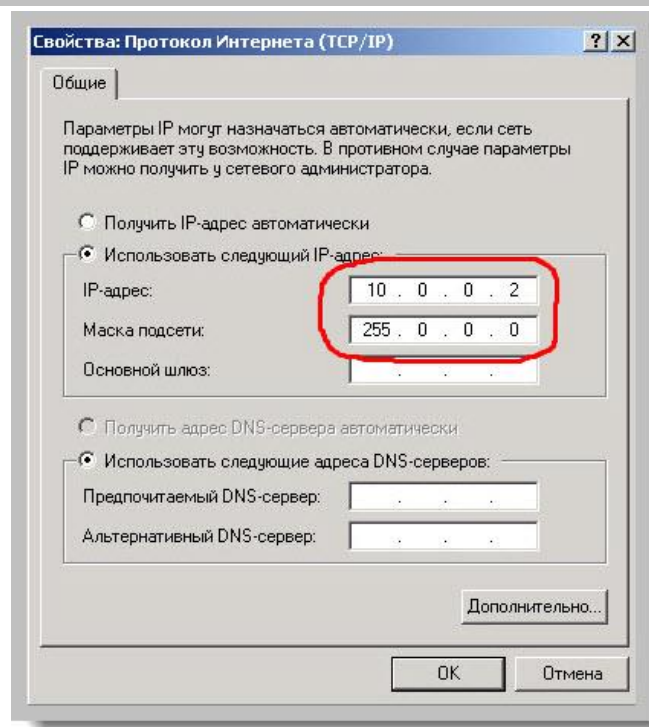


Как видите, у меня имя компьютера – «Server», а рабочая группа – «MYOFFICE». Для применения изменений операционная система предложит нам перезагрузиться, соглашаемся и отправляем наш Windows Server 2008 в «ребут», а пока займемся настройкой клиентского компьютера с Windows XP.

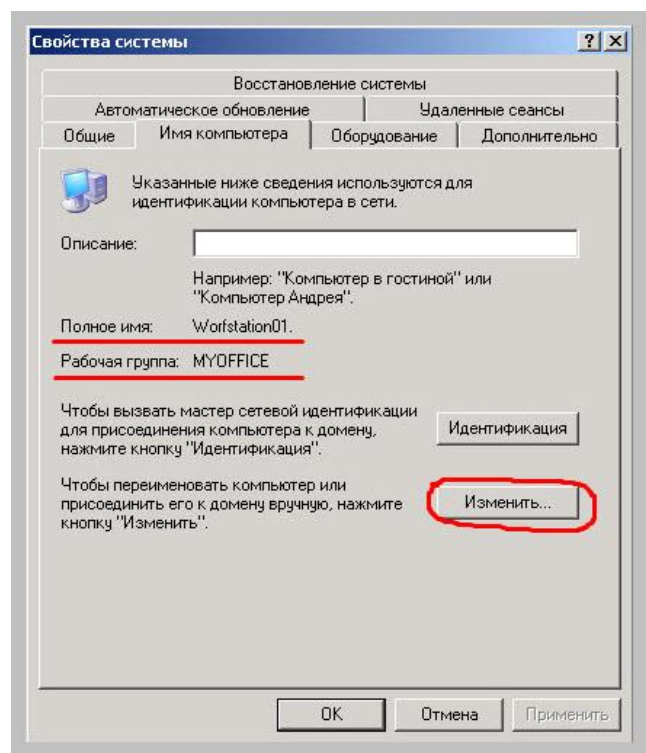
Продельываем те же самые операции, только на другой виртуальной машине:



Появляется окно «Свойства протокола Интернета (TCP/IP)» и там давайте выставим IP адрес на единицу больший, чем у сервера – 10.0.0.2 Помните, что двух одинаковых сетевых адресов в одной сети быть не может?

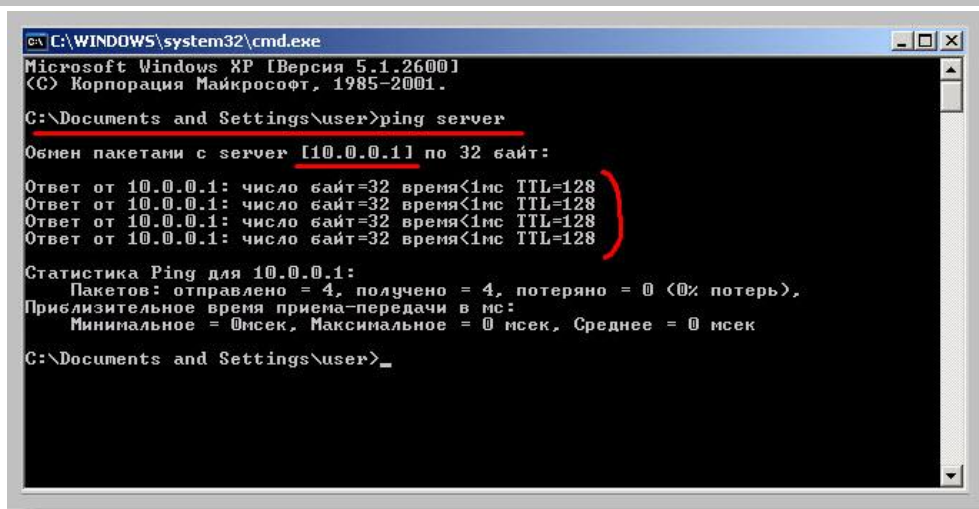


Та же самая «маска» подсети. И переходим в окно «Свойства системы», по нажатию кнопки «Изменить» задаем имя компьютера (я написал «Workstation01») и рабочую группу (та же, что и на сервере – «myoffice»).



Перезагружаем виртуальную рабочую станцию.

Проверяем, чтобы обе виртуальные машины (сервер и рабочая станция) были запущены и выполняем команду «ping» (мы рассматривали ее в одном из предыдущих уроков) с компьютера «Workstation01» на наш сервер: ping server



```
C:\WINDOWS\system32\cmd.exe
Microsoft Windows XP [Версия 5.1.2600]
(C) Корпорация Майкрософт, 1985-2001.

C:\Documents and Settings\user>ping server

Обмен пакетами с server [10.0.0.1] по 32 байт:

Ответ от 10.0.0.1: число байт=32 время<1мс TTL=128
Ответ от 10.0.0.1: число байт=32 время<1мс TTL=128
Ответ от 10.0.0.1: число байт=32 время<1мс TTL=128
Ответ от 10.0.0.1: число байт=32 время<1мс TTL=128

Статистика Ping для 10.0.0.1:
    Пакетов: отправлено = 4, получено = 4, потеряно = 0 (0% потерь),
Приблизительное время приема-передачи в мс:
    Минимальное = 0мсек, Максимальное = 0 мсек, Среднее = 0 мсек

C:\Documents and Settings\user>
```

Как видим, в ответе от сервера указан его IP адрес (10.0.0.1), все пакеты успешно достигли адресата, значит, - сетевое соединение работает!

Что нам нужно сделать теперь? Установить на клиентский компьютер Eset NOD Antivirus пятой версии и обновить его антивирусные базы с нашего сервера.

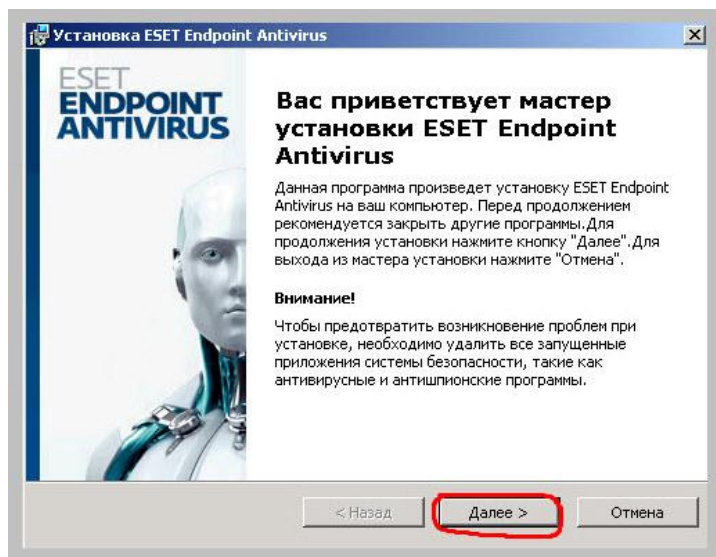
Приступаем! Для пущего интереса предлагаю сделать так: взять две виртуальные машины (эмулируя два пользовательских компьютера) и установить на одном из них «Eset Endpoint Antivirus 5», а на другом - «Eset Endpoint Security 5». Это – немного отличающиеся программные продукты и я хочу на этом примере показать Вам, что можно успешно обновлять их антивирусные базы с одного и того же «зеркала».

Вообще, политика разграничения программных продуктов от компании «Eset» не «страдает» излишней прозрачностью ☺ На сайте разработчика представлены решения для дома (персональные антивирусы, которые не поддерживают работу через сервера обновлений, отличные от Eset). К таким можно отнести: «ESET Smart Security» и «ESET NOD32 Antivirus». Для бизнеса (офиса с локальной сетью) имеются «ESET Endpoint Security», «ESET Endpoint Antivirus», «ESET Smart Security Business Edition» и т.д.

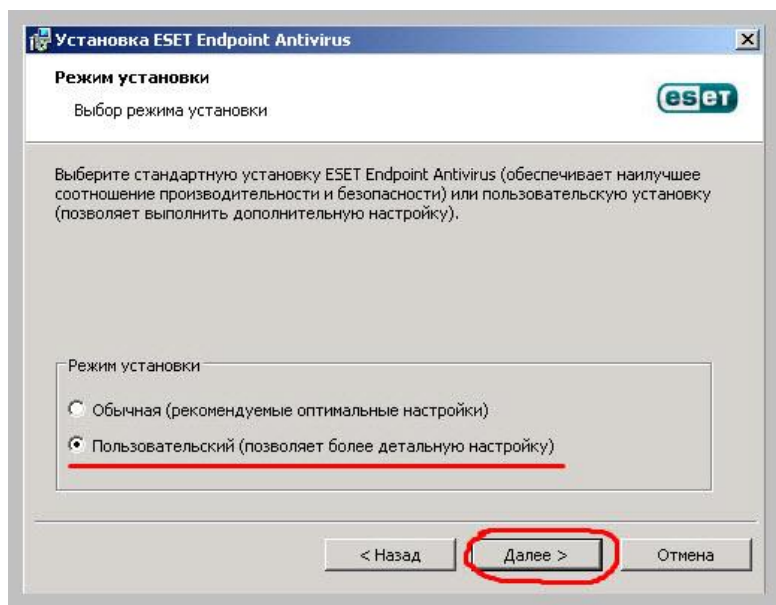
Каких-то кардинальных отличий (даже в самом интерфейсе) между этими продуктами Вы вряд ли обнаружите. Различие только в дополнительных модулях (более настраиваемый фаервол, различные антишпионские приложения, более гибкие настройки отдельных модулей, возможность выбрать свой сервер обновлений и возможность обновляться с «зеркала»).

Поэтому договоримся так: я показываю Вам что 100% сработало лично у меня, а если Вы знаете еще какие-то варианты, то отпишитесь мне на почту (возможно, я расширю данную статью Вашими примерами?)

Итак, начинаем устанавливать «Eset Endpoint Antivirus» на «клиенте».

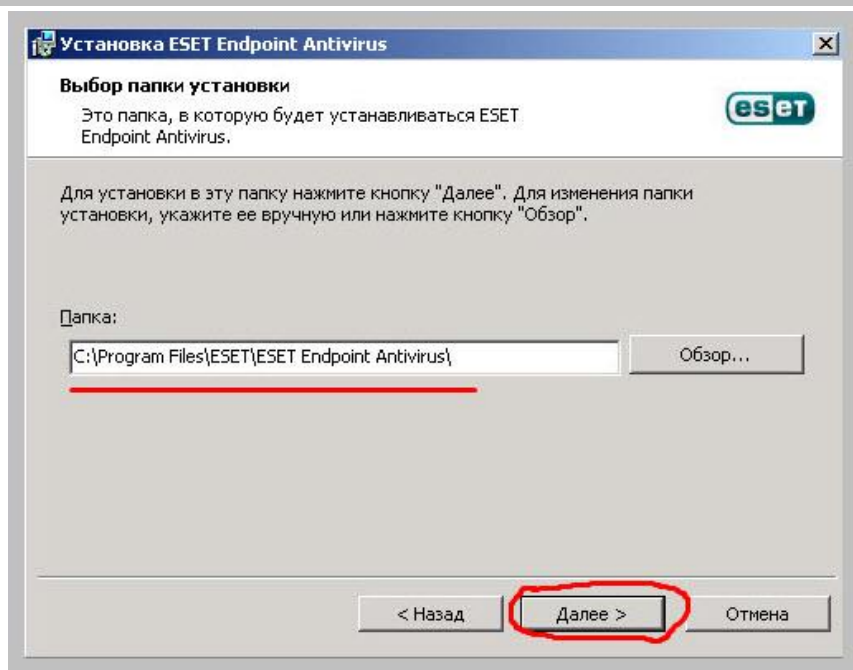


В первом окне нажимаем кнопку «Далее» и переходим к следующему:

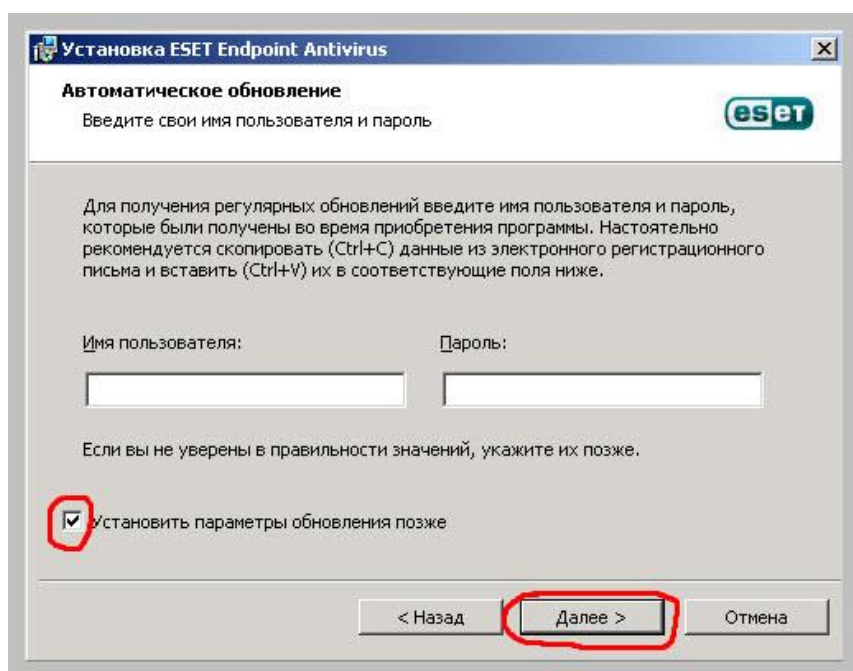


Чтобы лучше ознакомиться с вариантами первоначальной настройки данного антивируса, предлагаю перевести его в режим пользовательской установки. Так мы сможем **увидеть** больше настроек и **понять**, с чем мы имеем дело?

Указываем путь, по которому будет установлен антивирус:

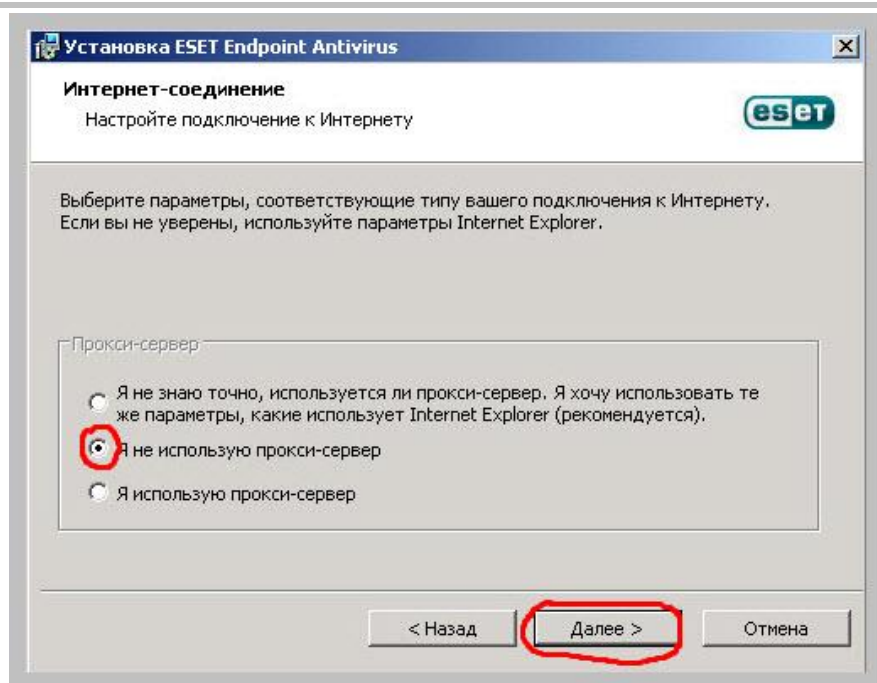


Нажимаем кнопку «Далее»:



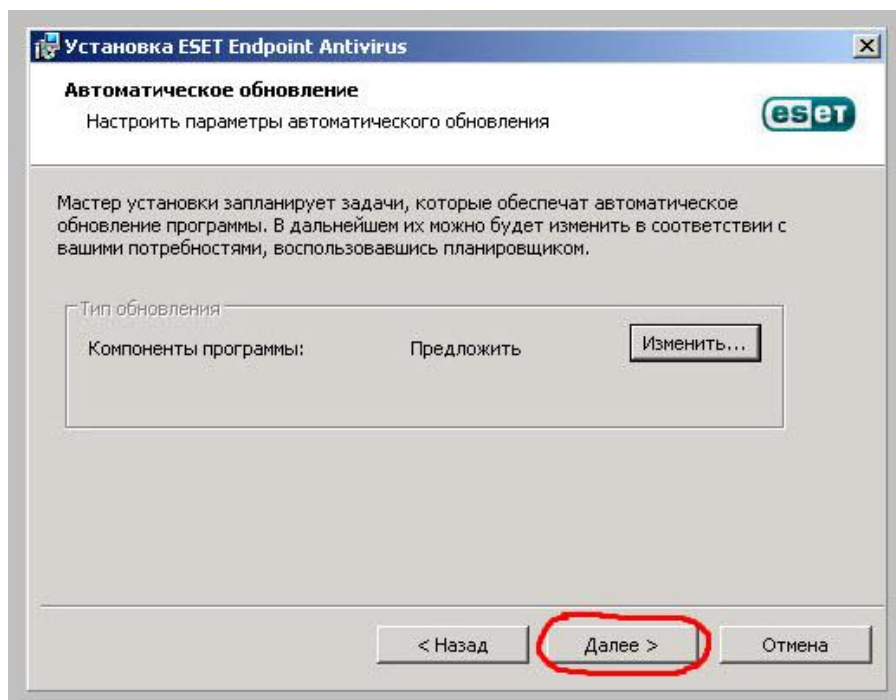
Рекомендую Вам (если у вас – не лицензионная копия программы) поставить галочку возле пункта: «Установить параметры обновления позже». Все равно мы этот момент будем настраивать сами.

В следующем окне выбираем соответствующий пункт. Для обновления с «зеркала», расположенного в нашей же локальной сети, я рекомендую Вам всегда выбирать вариант, обозначенный на скриншоте ниже:

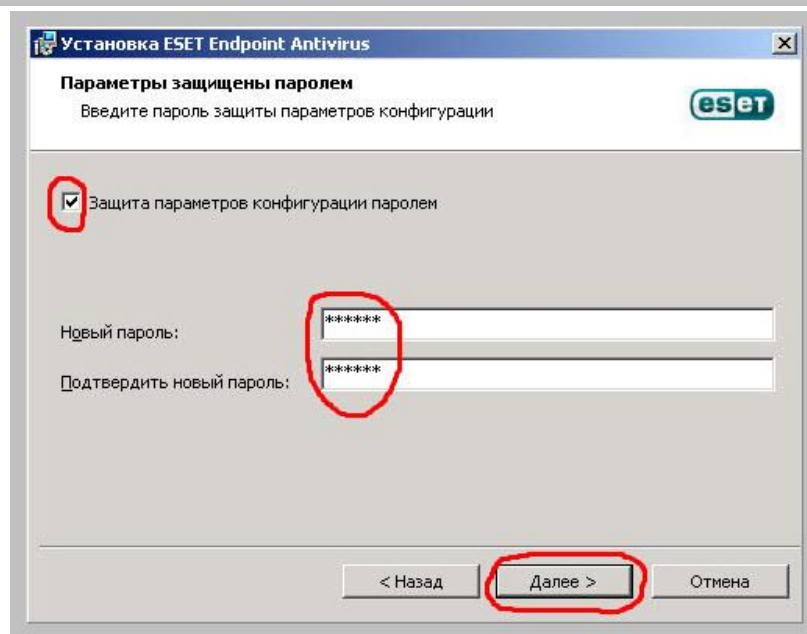


Программное обеспечение прокси-сервера, как правило, используется для контроля выхода пользователей из корпоративной сети в сеть Интернет. Если при доступе к глобальной сети вы видите перед собой окно для ввода логина и пароля, то это – «проделки» прокси-сервера ☺

Нажимаем кнопку далее:



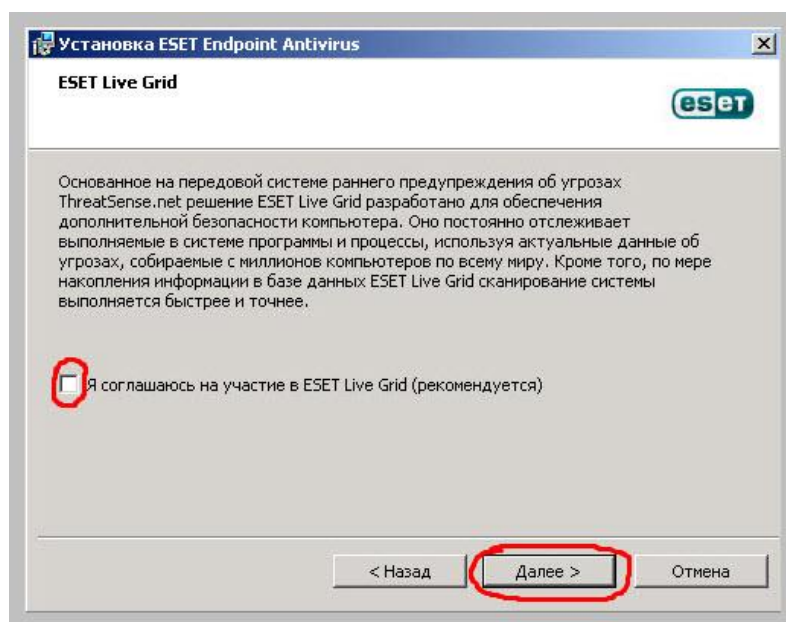
В окне, которое показано на фото выше, нажав кнопку «Изменить» мы можем выбрать, будут ли обновляться вместе с антивирусными базами и компоненты самой антивирусной программы и прочие настройки. Выбирайте на свое усмотрение. Нажимаем «Далее».



На фото выше мы обязательно должны поставить галочку «Защита параметров конфигурации паролем» и в открывшихся полях ввести (и подтвердить) любой пароль на наше усмотрение. **Не забудьте его!**

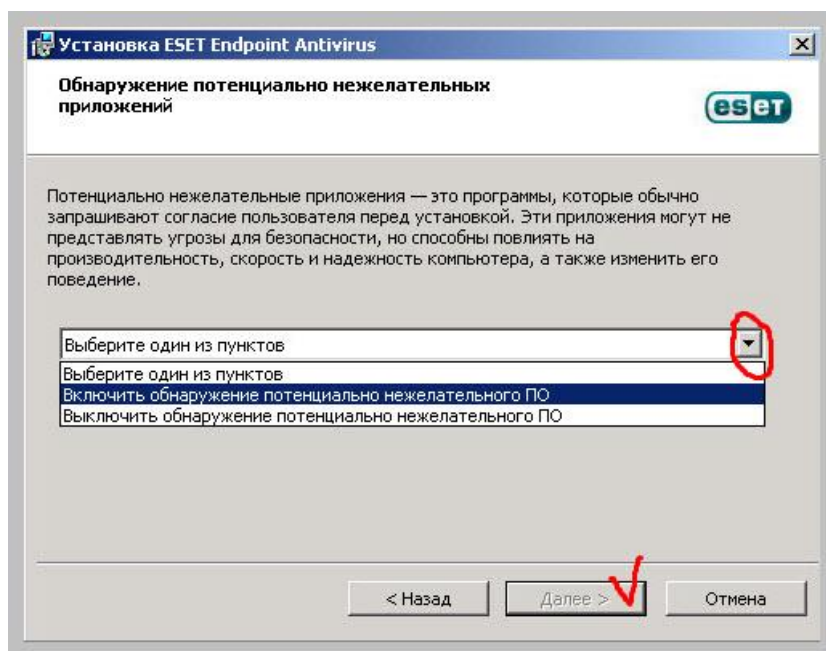
Подсказка! Паролить таким образом мы должны каждую клиентскую копию Eset NOD. Это нужно для того, чтобы пользователь не смог войти в дополнительные настройки программы и изменить там какие-то критически важные параметры (отключить файрвол или всю антивирусную защиту, изменить сервер обновления и т.д.) Даже входя на локальном компьютере в группу «Администраторы», он не сможет удалить программное обеспечение антивируса без ввода пароля, который мы здесь укажем!

Нажимаем «Далее».

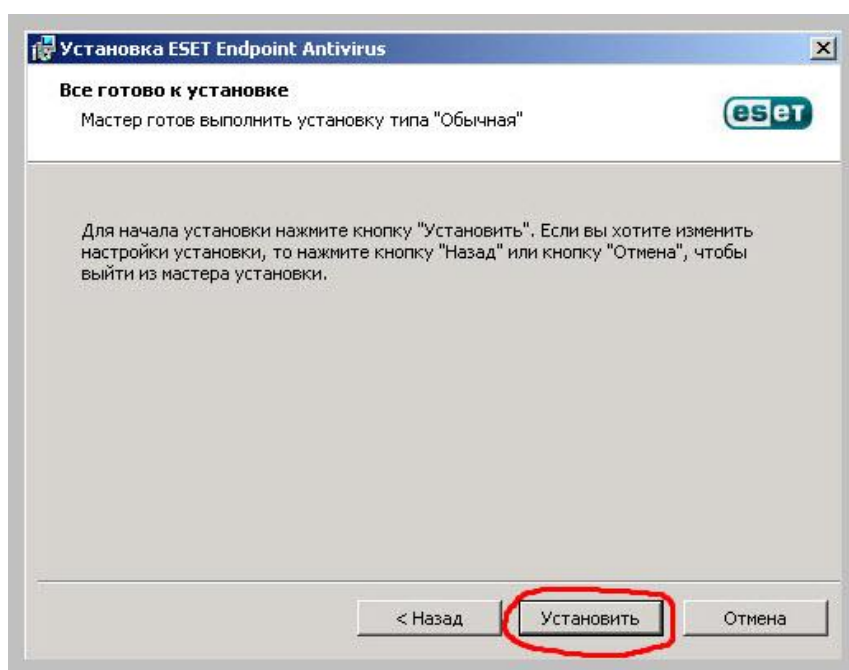


Вот эту галочку я бы Вам настоятельно рекомендовал убрать. Если Вы ее оставите, антивирус начнет передавать компании «Eset» какие-то данные, которые («якобы») помогут улучшить их продукт. Ее наличие это - одна из причин, по которой в черный список так быстро попадают пароли, которые «еще вчера хорошо работали» ☺

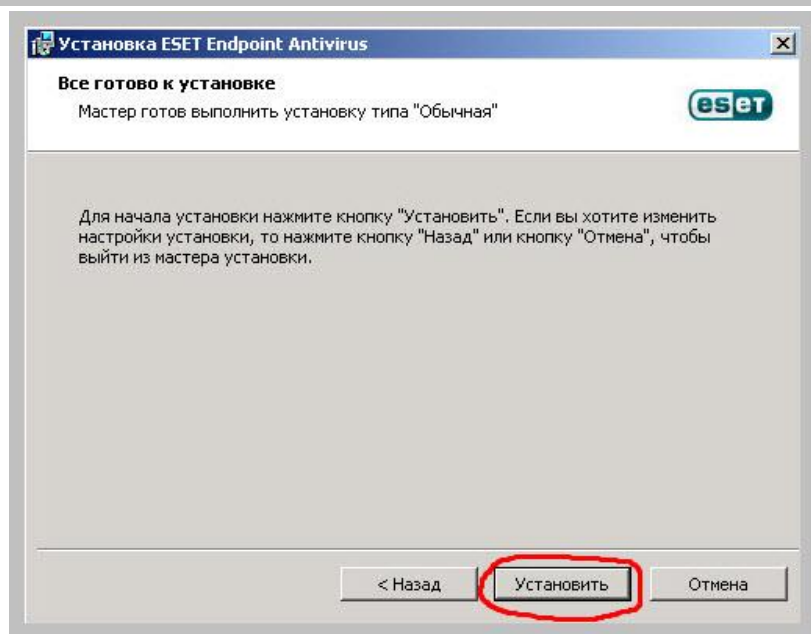
В следующем окне можем включить режим обнаружение потенциально опасного ПО (различные spyware, malware и т.д.) Рекомендую включить.



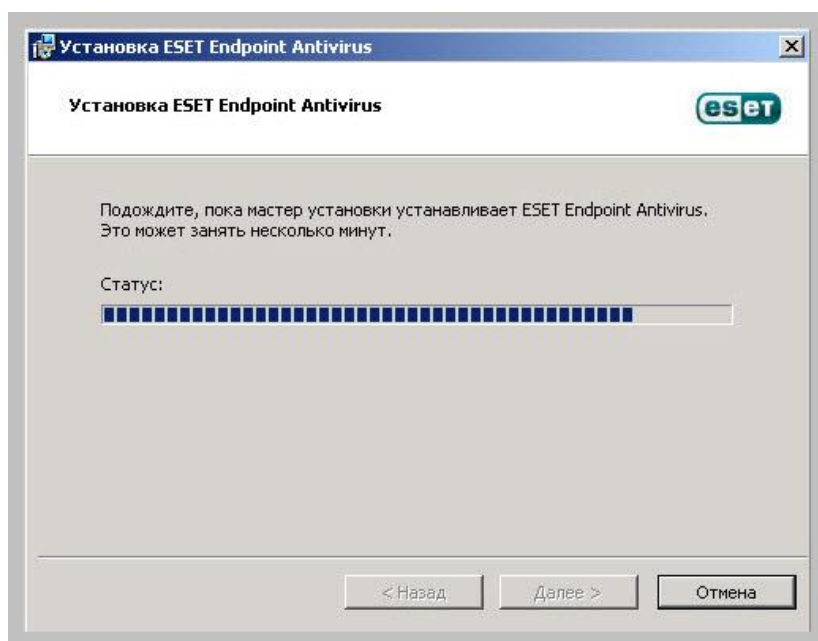
После выбора из списка одного из пунктов, кнопка «Далее» станет активной. Нажимаем ее.



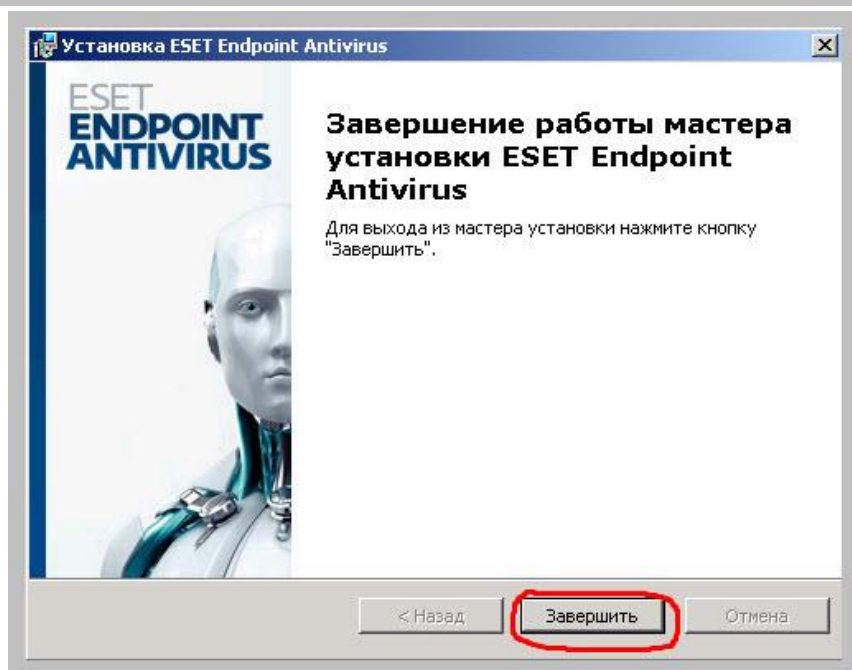
Приступаем к установке. Нажимаем одноименную кнопку ☺



Запускается процесс инсталляции:



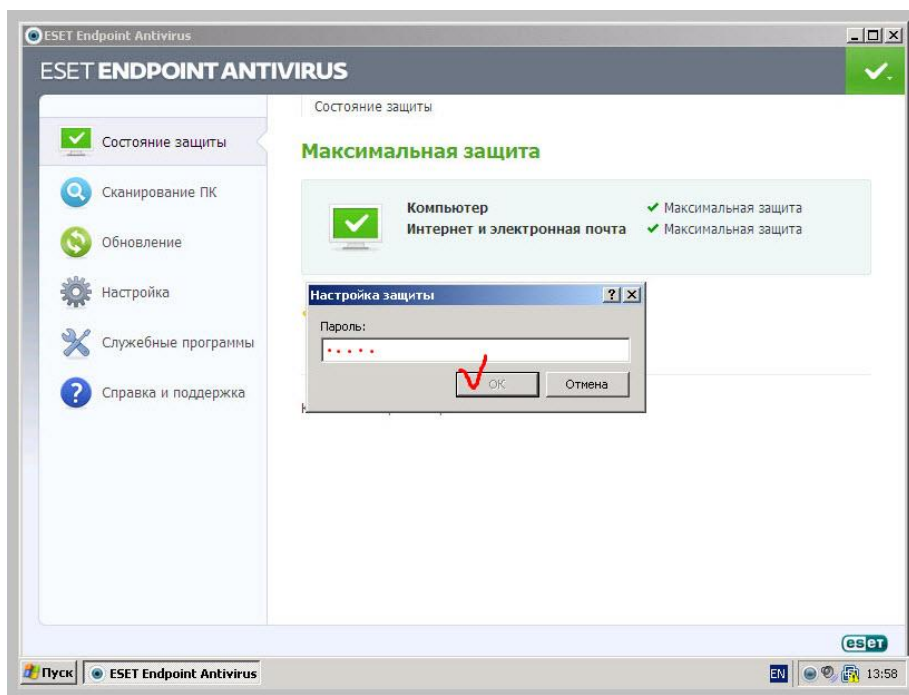
Если все прошло успешно, то по завершении видим вот такую картину:



Нажимаем кнопку «Завершить».

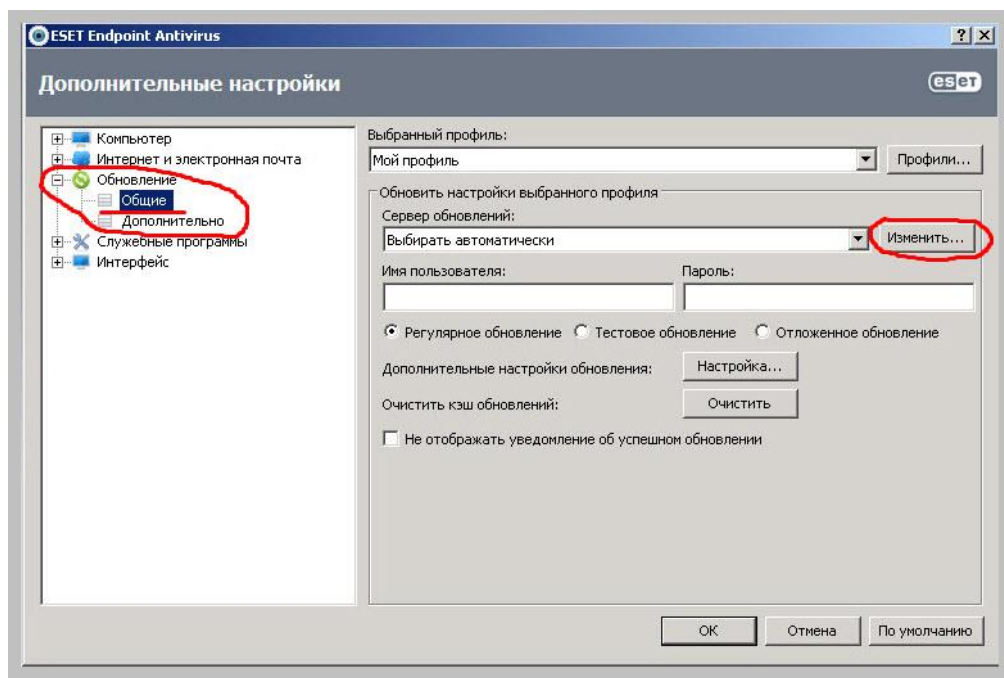
Я столь подробно остановился на процессе установки и начальной настройке антивируса именно потому, что у компании «Eset» она очень схожа для всей линейки продуктов и изучив, как это работает для одного, можно быть уверенным, что и с остальными Вы не поспорите 😊

Итак, можем сразу же, без перезагрузки ОС зайти в главное окно программы и войти в расширенные настройки: «F5».

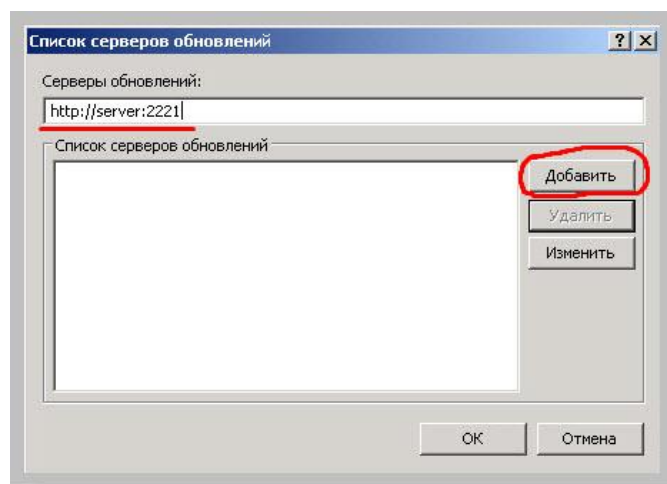


У нас появилось окошко «Настройки защиты» с предложением ввести пароль доступа к настройкам. Помните, на одном из этапов установки мы защищали критически важные опции антивируса от изменения пользователями? Вот так это и работает!

Вводим наш пароль и попадаем в «Дополнительные настройки»:



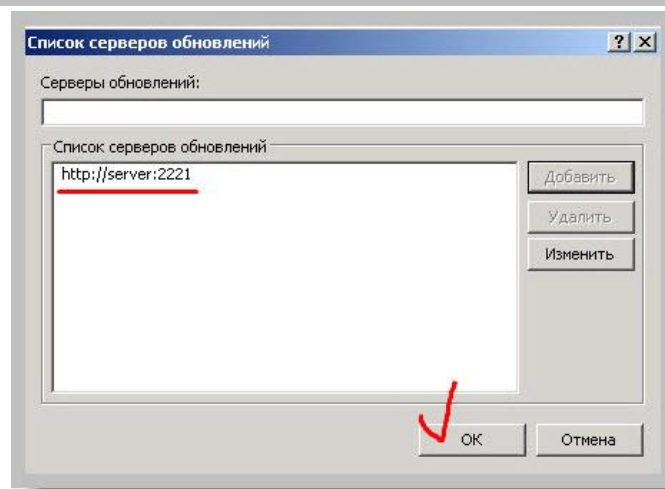
Здесь нам нужно раскрыть раздел «Обновление» и перейти в пункт «Общие». Возле поля «Сервер обновлений» нажимаем кнопку «Изменить» и попадаем в знакомое нам уже окно:



Здесь прописываем удаленный сервер обновлений, расположенный в нашей локальной сети. Как Вы помните, это – компьютер под именем «server», где установлен «Esen Endpoint Security 5», слушающий (ожидающий) соединения на 2221-й порт по протоколу «http»?

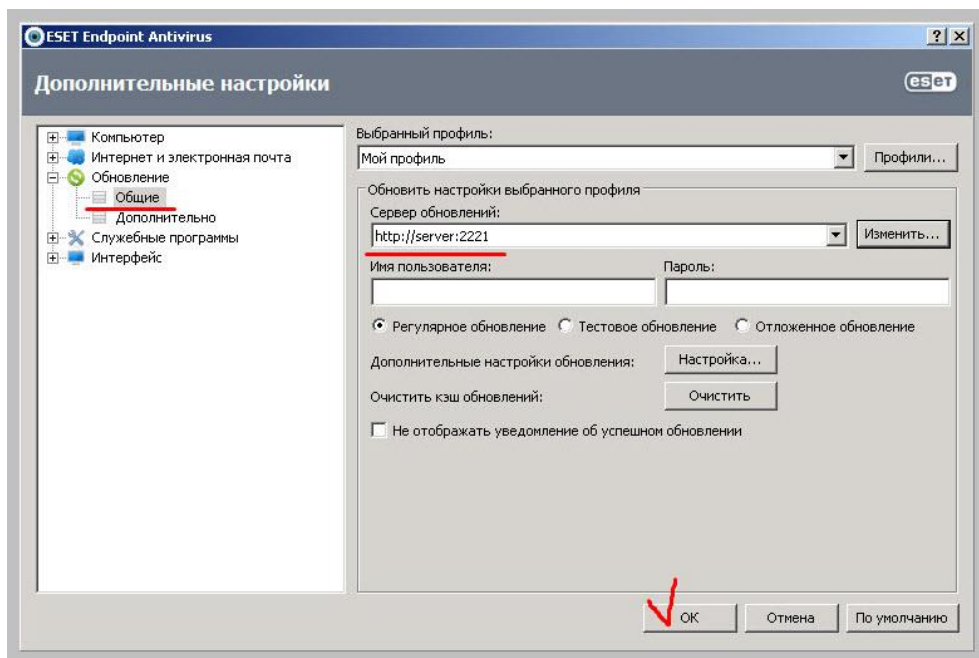
Вот так и пишем **http://server:2221** (если мы хотим обратиться к компьютеру по определенному порту, то перед номером порта всегда ставим двоеточие).

Нажимаем кнопку «Добавить»:



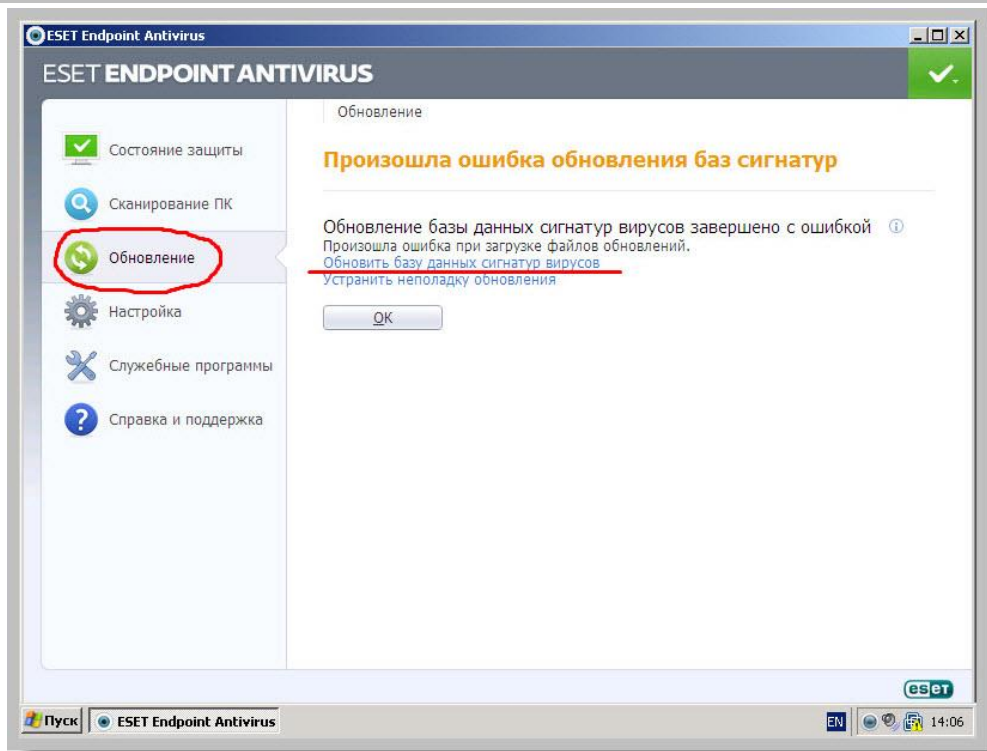
Видим, что в списке серверов обновления появилась наша запись. Жмем «ОК»!

В окне дополнительных настроек проконтролируем, что все правильно и еще раз нажимаем «ОК».

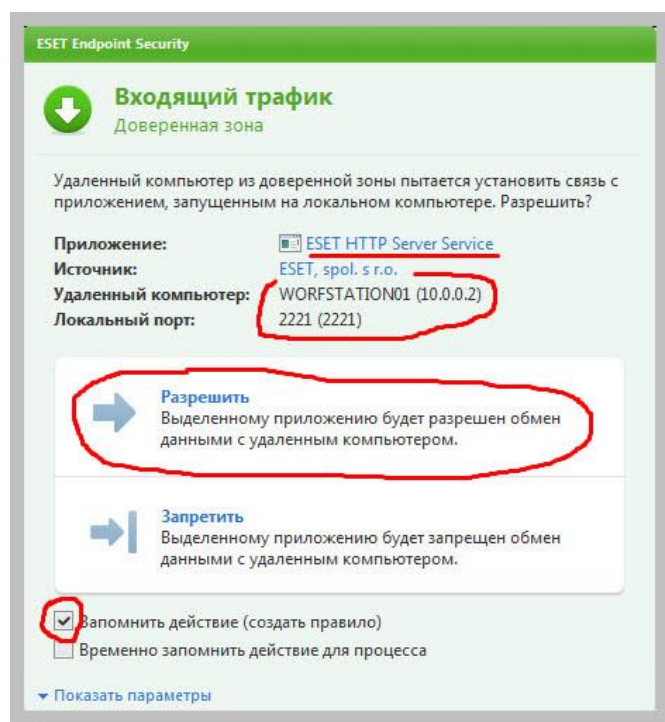


Вот теперь – самое интересное! ☺

В главном окне программы на «клиенте» перейдем в раздел «Обновление» и нажмем на ссылку «Обновить базу данных сигнатур вирусов».



Важный для понимания момент! После этого на компьютере с Windows Server 2008 у нас появится приблизительно вот такое окно:

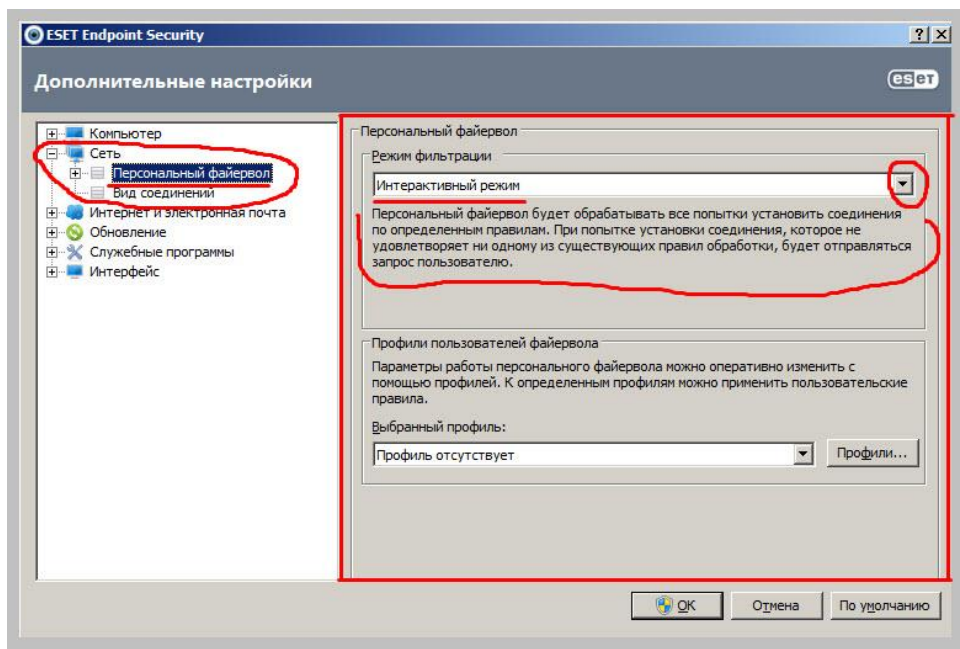


Посмотрите на него внимательнее. Это работает наш сетевой экран. Вверху обозначено приложение, которое пытается установить сетевое соединение с нашим сервером, показано имя удаленного компьютера (Workstation01), его сетевой IP адрес (10.0.0.2) и порт, по которому удаленная программа пытается соединиться (2221).

Здесь нам обязательно нужно нажать ссылку «Разрешить» и поставить галочку возле пункта «Запомнить действие (создать правило)». Это укажет программе на то, что

в будущем для подобных соединений надо разрешать доступ (для этого она создаст в настройках своего сетевого экрана исключение, называемое «правилом»)

Вообще, это окно – следствие наших предыдущих действий. Помните, на одном из ранних этапов настройки антивируса на сервере мы переводили модуль его файрвола в интерактивный режим?

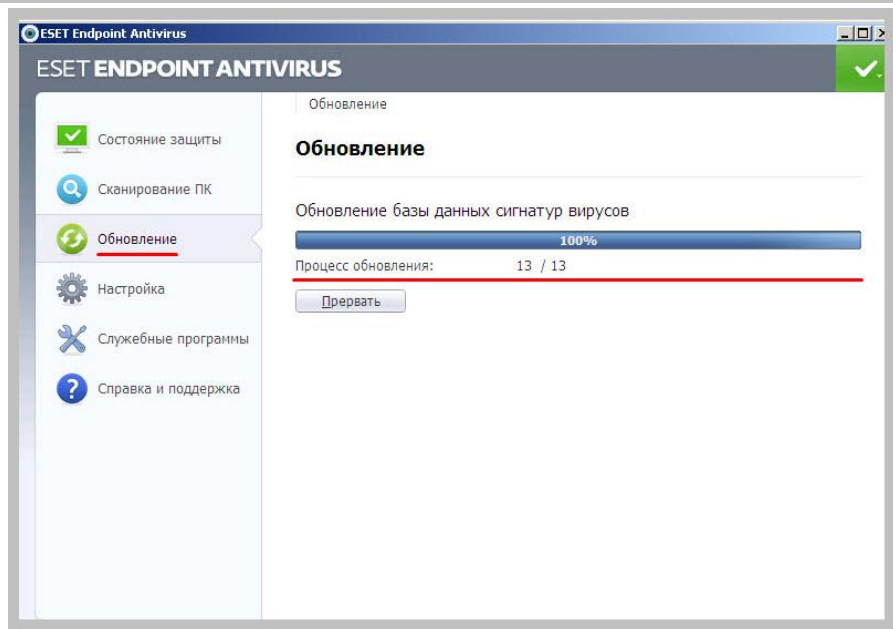


И теперь при проявлении «подозрительной» сетевой активности файрвол антивируса будет спрашивать нас, хотим ли мы разрешить данное соединение или заблокировать его. Исключения (правила) можно создавать и самим вручную, а можно с помощью вот такого интерактивного режима самообучения программы.

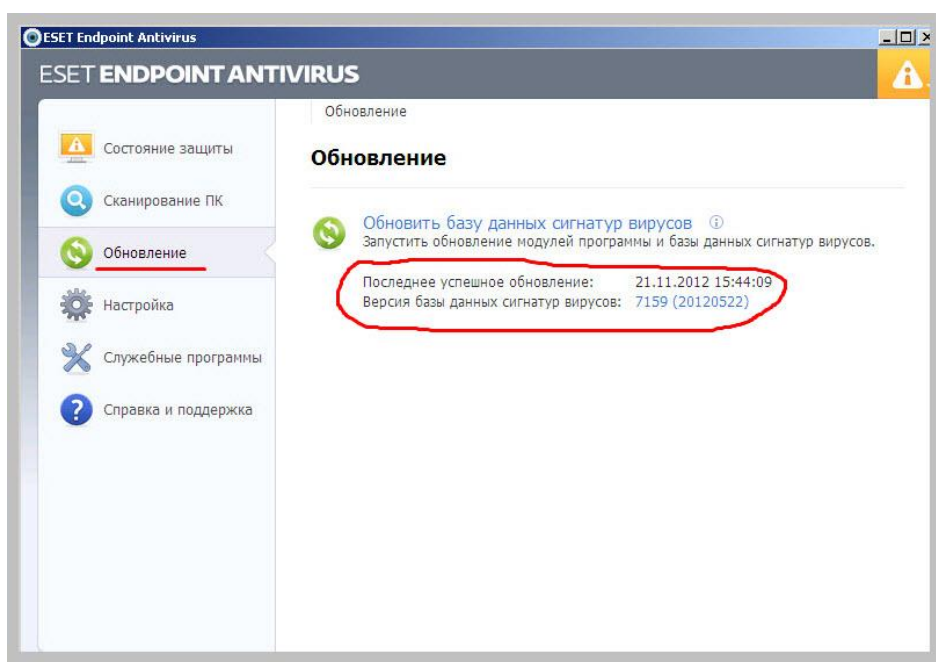
Весьма вероятно, что первый запуск обновления с «клиентского» компьютера именно по этой причине пройдет неудачно. До создания «правила-исключения» в соединении с сервером ему будет просто отказано, но после применения галочки «запомнить действие» все должно измениться.

После этого обновление пойдет успешно и в будущем (по крайней мере, до переустановки антивируса на сервере или изменений его сетевых настроек) никаких дополнительных манипуляций производить будет не нужно.

Запускаем процесс обновления с «клиента» еще раз и видим, что на этот раз оно идет успешно:



По завершении, вместо кнопки «Прервать» у нас появится «ОК» и мы сможем увидеть дату последнего успешного обновления, а также убедиться, что версия базы данных сигнатур вирусов теперь совпадает с версией на сервере!

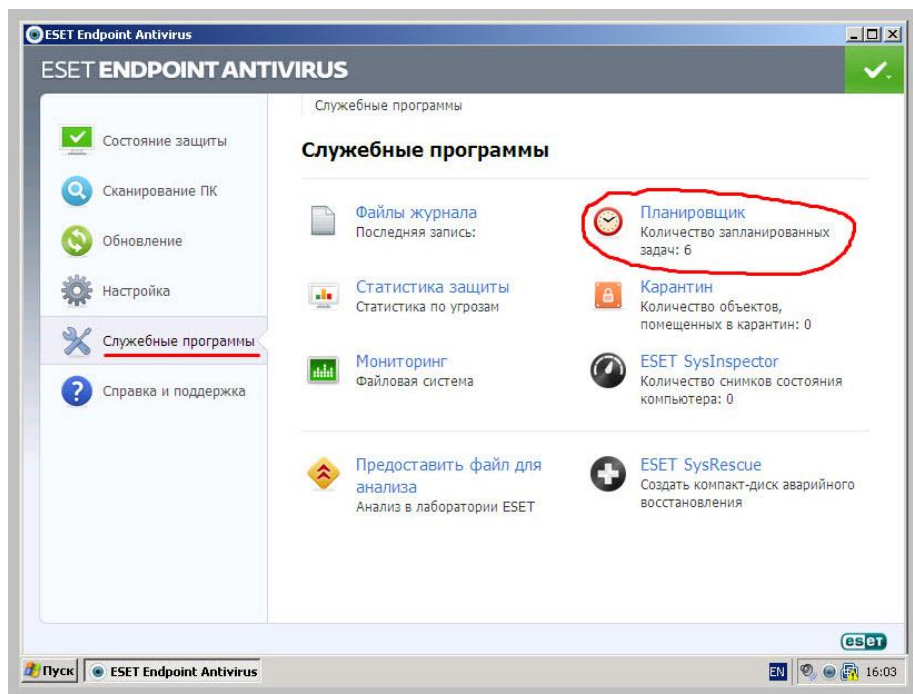


Вот так мы только что обновили наш антивирус по сети через собственное «зеркало обновлений»!

Теперь пришло время произвести на «клиентах» еще одну маленькую, но очень ответственную настройку ☺ Нам, как администраторам, нужно быть уверенным, что рабочие станции пользователей будут четко обновлять свои антивирусные базы и без нашего участия. Наше дело – следить, чтобы на сервере все было в порядке!

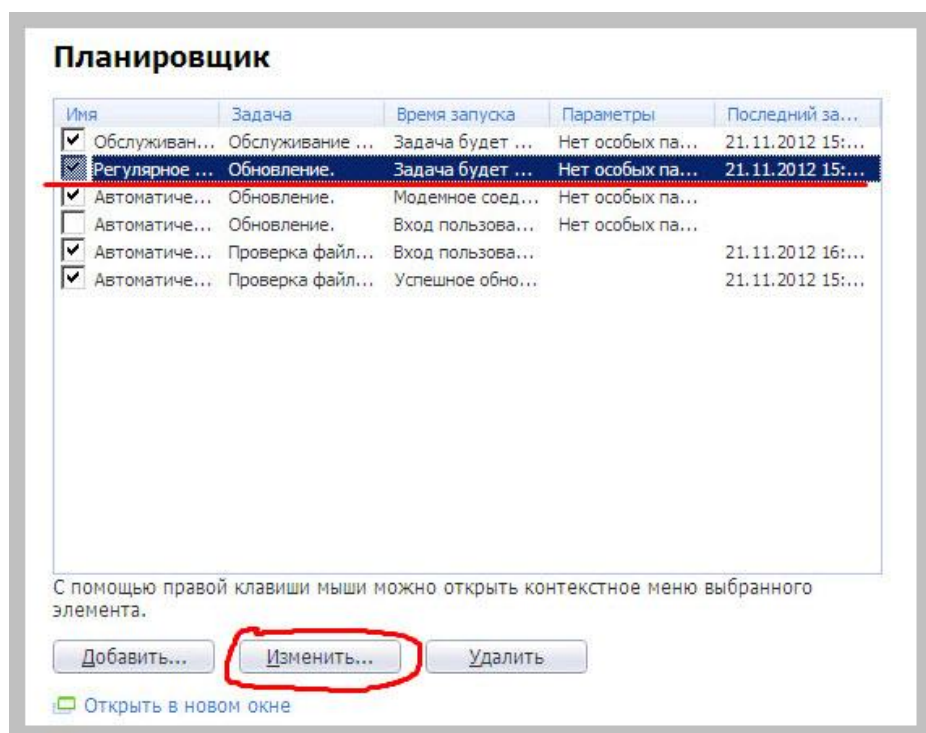
Что, для собственного спокойствия в будущем, нам нужно сделать? В главном окне заходим в раздел «Служебные программы» и в правой его части нажимаем на ссылку «Планировщик».

Примечание: даже если в других версиях антивируса NOD он будет располагаться немного не там, то все равно – ищите «Планировщик» ☺



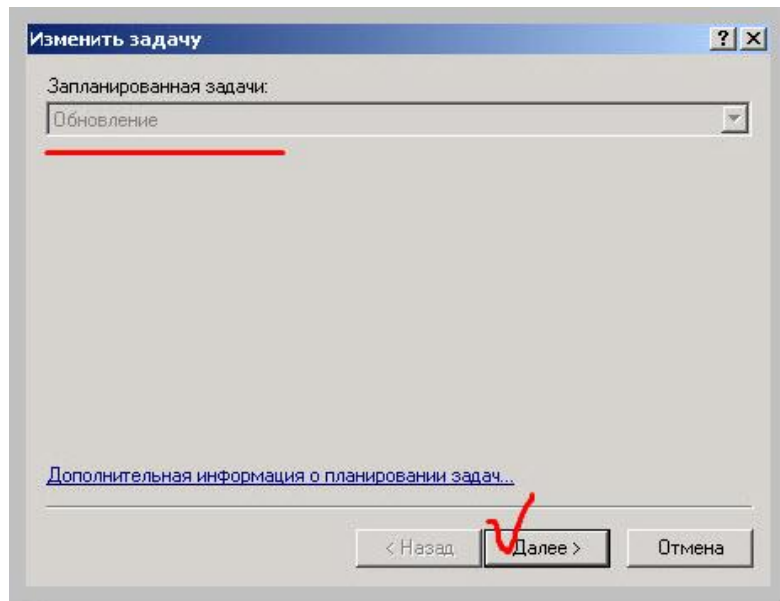
Заходим в него и видим активные задания, отмеченные галочками. Это – те действия, которое антивирус будет выполнять в автоматическом режиме в заданное время.

Давайте подправим задачу регулярного автоматического обновления!

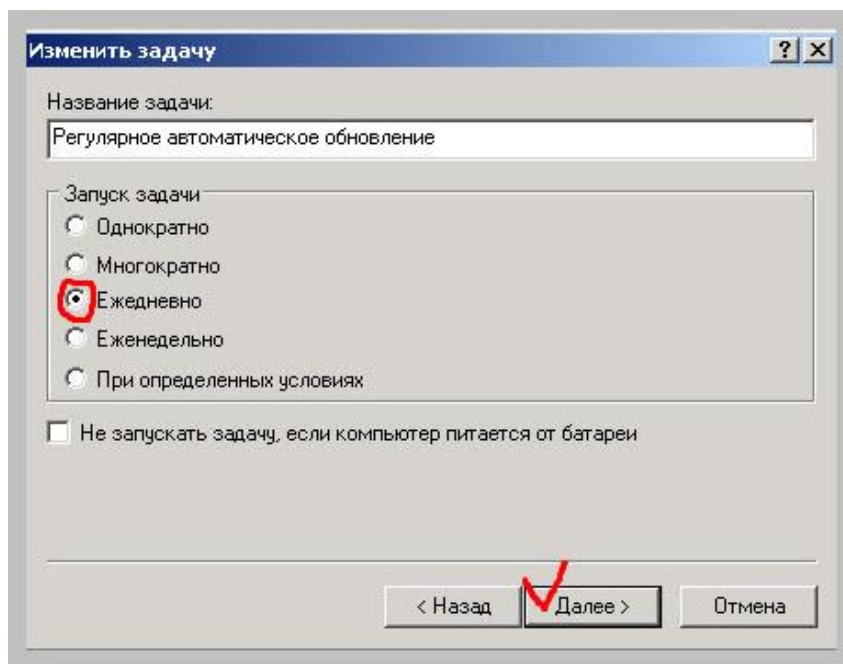


Выделяем ее и нажимаем кнопку «Изменить».

Запустится мастер редактирования условий задачи «Обновление».

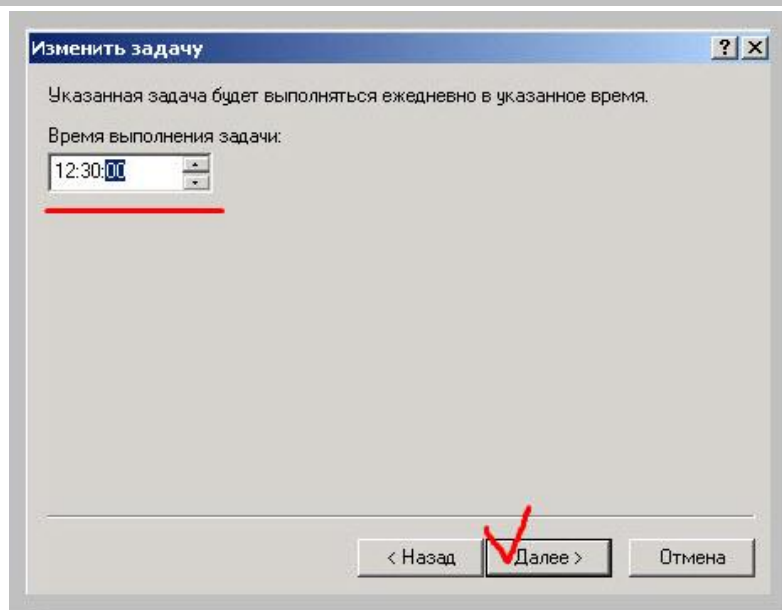


Нажимаем кнопку «Далее»:



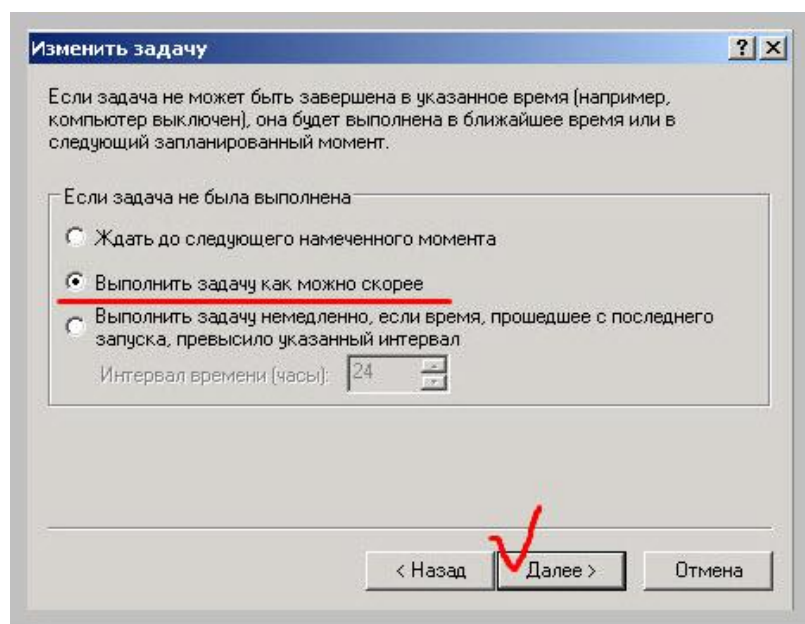
Название задачи – «Регулярное автоматическое обновление» мы можем не менять (это ни на что не влияет), а вот режим запуска я рекомендую выставить в «Ежедневно». Первое условие: задача обновления будет выполняться ежедневно. То, что нам нужно! Двигаемся «Далее» ☺

В следующем окне нам предложат ввести время выполнения задачи:



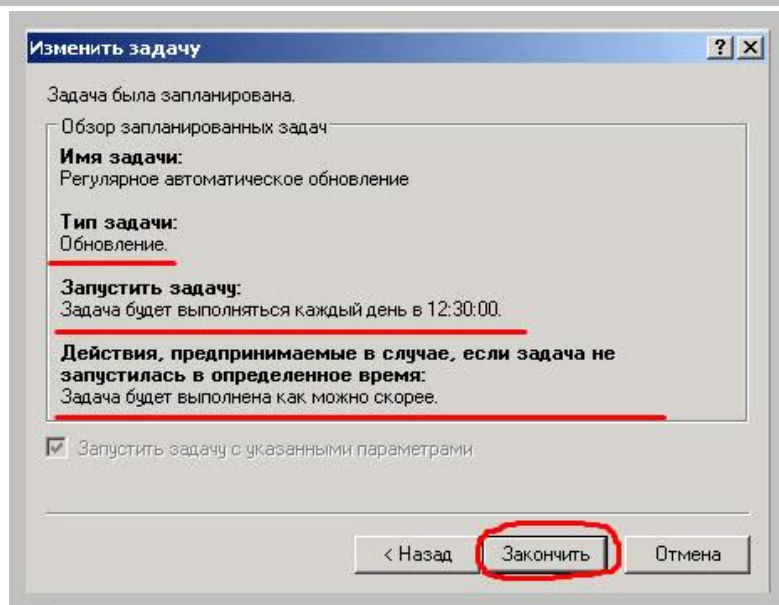
Как видите, я указал 12:30 дня. Это – обеденный перерыв и обновление, не будет никому мешать работать. Нажимаем кнопку «Далее».

На следующем шаге я, опять же, порекомендую Вам выбрать вариант «Выполнить задачу как можно скорее».



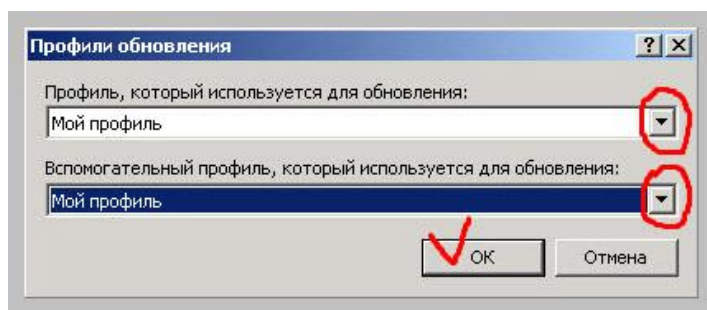
Какие преимущества, по сравнению с другими, он нам дает? Если последнее обновление по расписанию по каким-либо причинам не было выполнено: клиентский компьютер был выключен или в это время пропало электричество и задача была сорвана, то при возобновлении нормальной работы компьютера и сети антивирус приступит к обновлению немедленно, не дожидаясь следующего дня (в который тоже что-то может произойти) или следующего цикла обновления.

Еще раз нажимаем «Далее» и видим всю сводную информацию по данной задаче:



Что мы имеем? Тип задачи – «Обновление». Когда запускать? – каждый день в 12:30. Что делать, если не получилось обновиться? – запустить повторно, как можно скорее! Все просто и логично и не оставляет осадка двусмысленности или недосказанности. А главное – работает именно так, как и написано, проверено ☺

В последнем окне «мастера» нам предложат выбрать профиль, к которому мы применим данные настройки. Я ничего не выдумывал и ставлю все по умолчанию, как показано на скриншоте ниже:



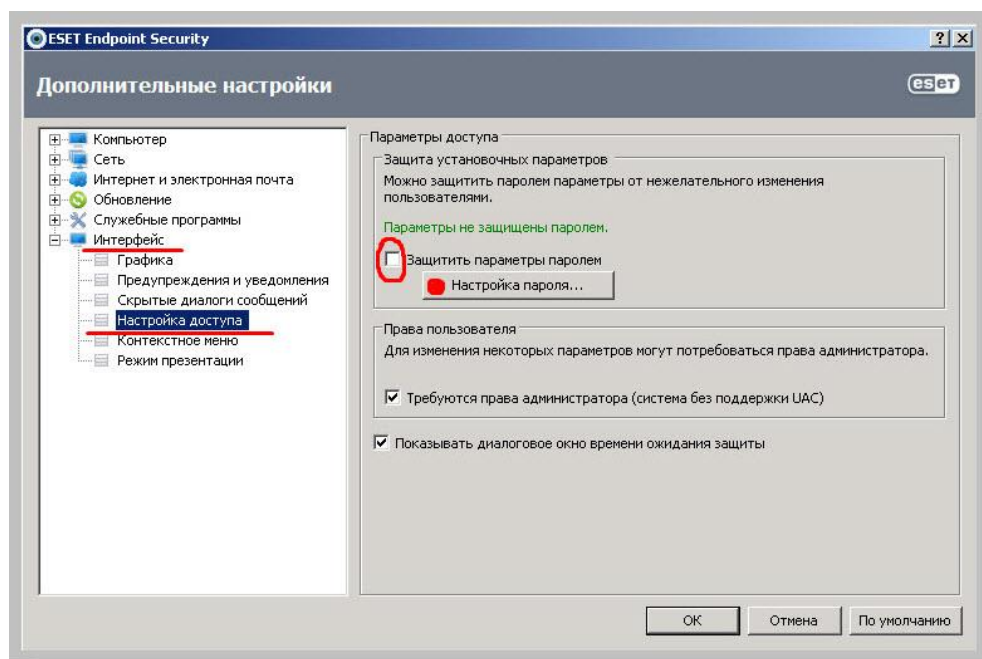
Вот, собственно и все! ☺

Возможно, получилось слишком много скриншотов, но с меньшим их количеством я бы не был уверен, что всем все будет ясно, а объяснять словами то, что можно показать на картинке – не эффективно. Конечно, было бы еще лучше (и экономнее по времени), если бы я записал все тоже самое, как видеоурок, но здесь уже сказывается первое (филологическое) образование и душа требует самовыражения письменным словом ☺

Давайте я Вам, в завершении, покажу еще пару скриншотов, раскрывающих кое-какие нюансы, опущенные в статье. Помните, мы говорили, что установим на клиентские компьютеры два разных продукта от «Eset» (Eset Endpoint Antivirus и Eset Endpoint

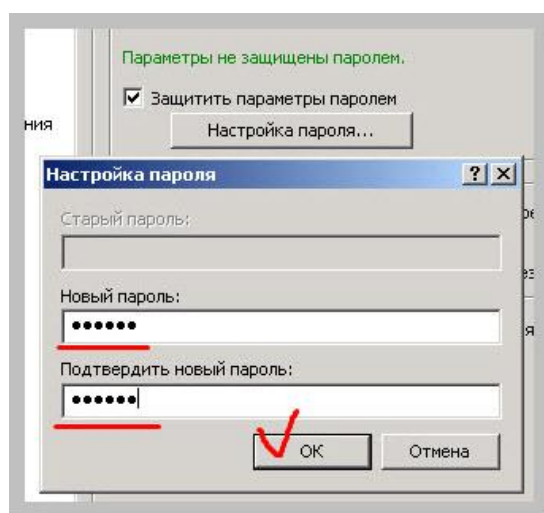
Security)? Они оба успешно обновляются с одного и того же «зеркала». Нюанс состоит в том, что второй продукт при установке не предлагает защитить свои настройки паролем.

Для того чтобы это сделать, нам нужно зайти в дополнительные настройки, развернуть раздел «Интерфейс» и перейти к пункту «Настройка доступа».



В правой части окна нужно поставить галочку напротив пункта «Защитить параметры паролем» или – нажать на кнопку «Настройка пароля».

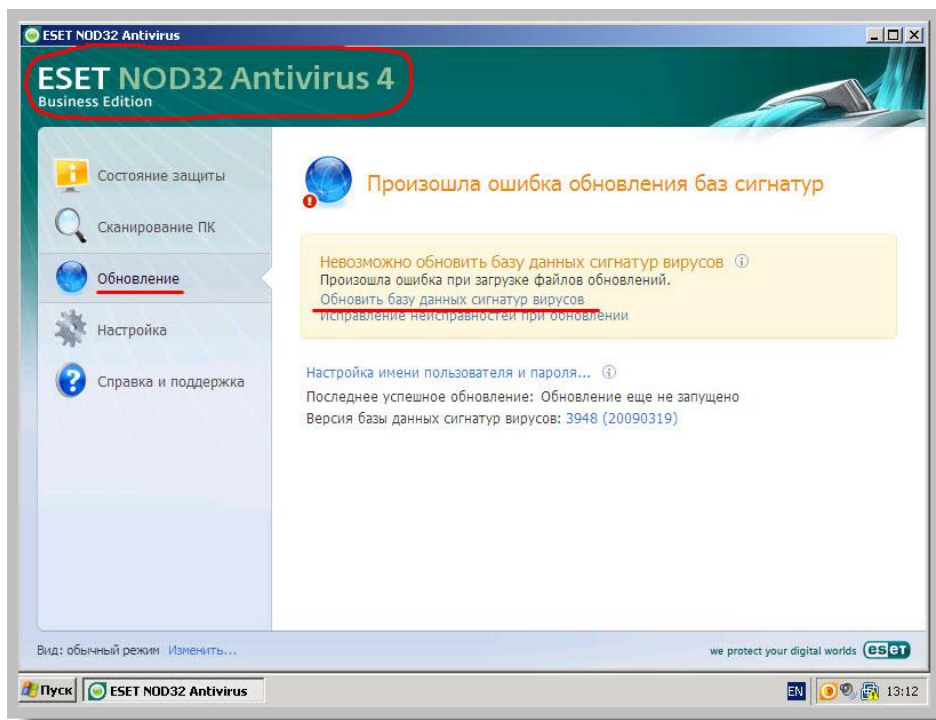
Появится окно, в котором нам нужно будет указать наш пароль, который защитит антивирус от изменения настроек неопытным пользователем.



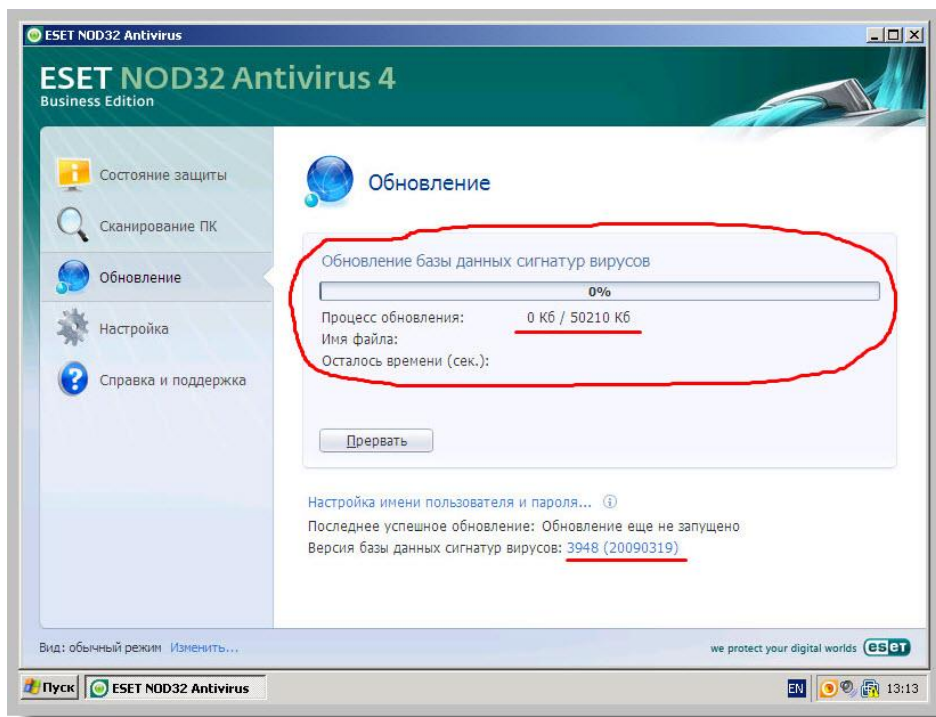
Давайте еще, для полноты охвата момента, попробуем установить на один из компьютеров версию Eset NOD предыдущего (четвертого) поколения: «Eset NOD32 Antivirus Business Edition».

Хорошая, в свое время, была система. Никакой мороки с файрволом (он там просто отсутствовал ☺), минималистичный интерфейс – красота! Если ничего не изменилось, то одна небольшая компьютерная сеть (машин двадцать пять) до сих пор на нем работает.

Итак, устанавливаем программу на виртуальную машину, настраиваем сеть, прописываем зеркало обновления (все, как в предыдущих примерах) и пробуем обновиться с сервера:



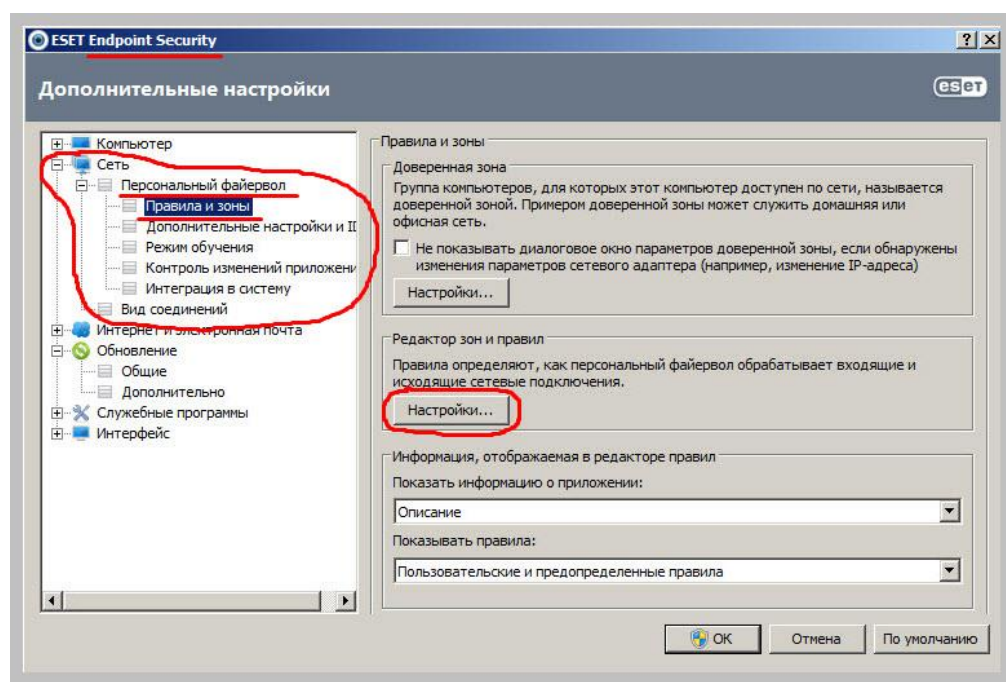
Нажимаем на ссылку «Обновить базу данных сигнатур вирусов», видим, что программа успешно определила размер скачиваемого обновления и начала процесс:



НО! Через некоторое время мы получаем сообщение о том, что программа не смогла обновить антивирусные базы из за ошибки. А «ошибка» и состоит в том, что мы пытаемся обновить четвертую версию программы с сервера обновления, работающего на версии номер «5». **Так что всегда имейте подобные нюансы в виду!**

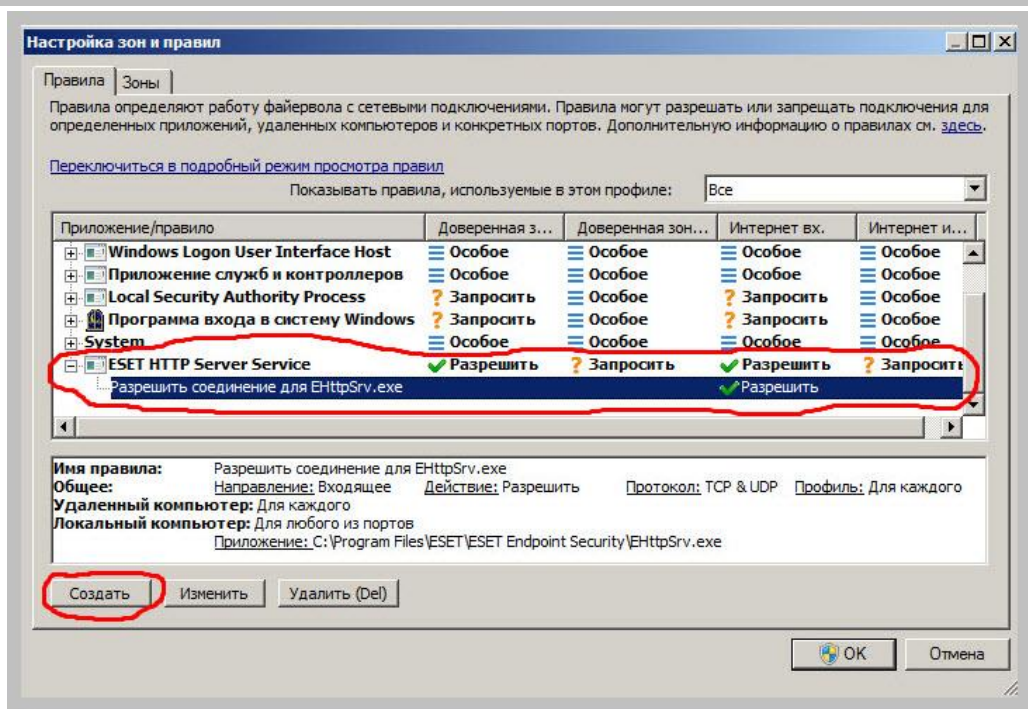
Сейчас, предлагаю Вам более внимательно посмотреть на настройки модуля фаервола антивирусной защиты на нашем сервере. Помните, когда мы перевели сетевой экран в интерактивный режим, то после попытки соединения с «клиента» у нас появилось окно, в котором мы создали правило-исключение для подобного типа соединений?

Было бы уместным, сейчас взглянуть, где и что именно было прописано в этот момент на сервере. Итак, - «Дополнительные настройки», раскрываем раздел «Персональный фаервол» и выбираем пункт «Правила и зоны».



В правой части окна есть кнопка «Настройки». Щелкнув по ней, можно попасть в редактор правил для сетевого экрана.

Вот как он выглядит:



Как видите, последним пунктом у нас стоит правило, касающееся соединения для приложений ESET (EhttpSrv.exe) по протоколу HTTP. Далее идут пункты, разрешающие данный вид соединений или предлагающие «Запросить» такое разрешение. Чуть ниже – указаны разрешенные сетевые протоколы передачи данных (TCP и UDP) и - направление передачи.

Кнопка «Создать» позволяет самостоятельно (в ручном режиме) ввести свое собственное правило обработки любого из сетевых соединений для произвольного типа приложения. Но это уже – совсем другая история, и рассказывать ее мы будем на одной из наших следующих встреч! ☺

Урок взят с сайта: <https://sebeadmin.thelogos.in.ua>

До встречи в следующих уроках !