

Пошаговые Руководства
Сам Себе Админ
системное администрирование
Microsoft Windows



Практика использования корпоративного антивируса

Приветствую, друзья! Сегодня я хотел бы подробно разобрать с Вами тему защиты корпоративной сети от вирусов. Мы уже касались этого вопроса в одном из наших уроков (**урок №16**), который назывался: «как защитить небольшую локальную сеть от вирусов».

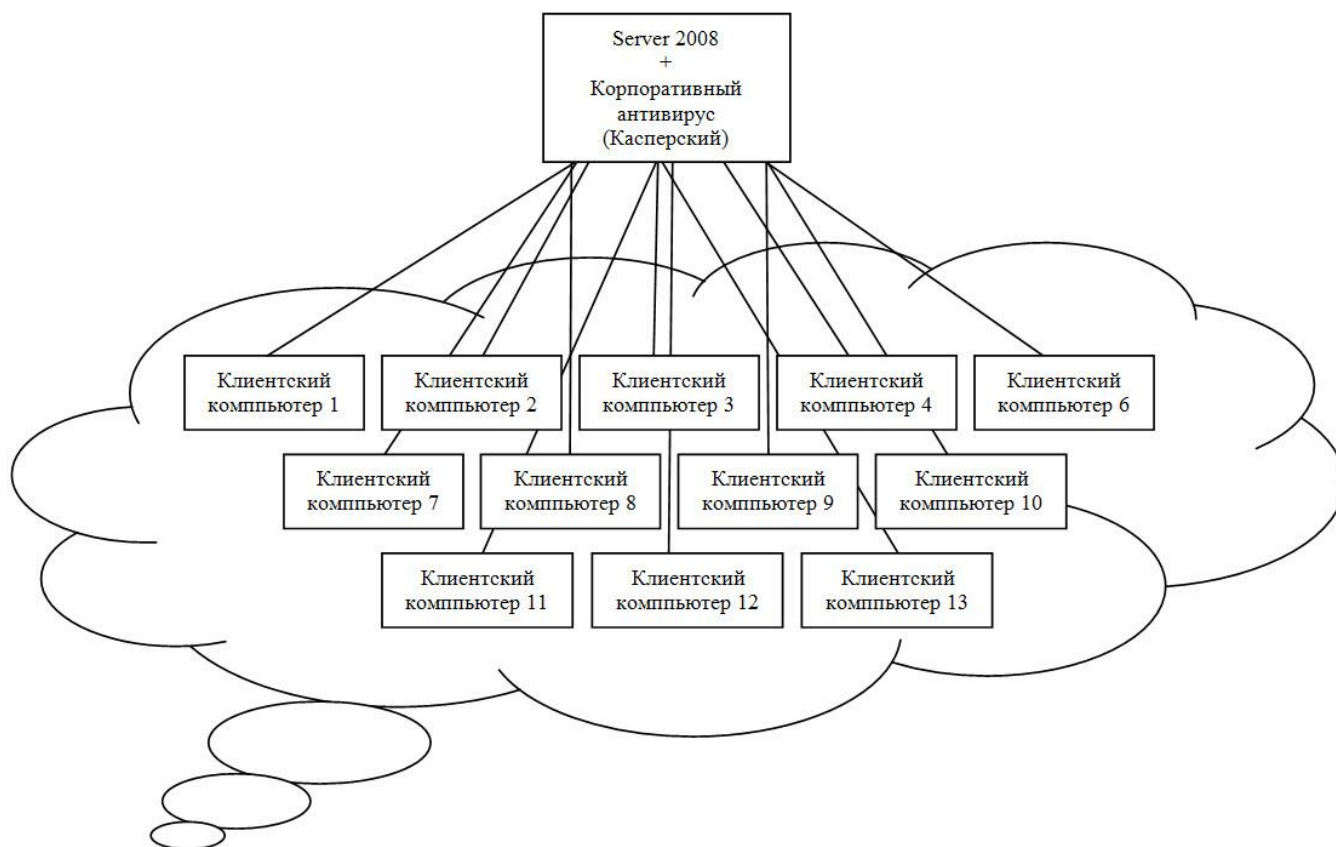
Теперь же, я бы хотел остановиться именно на одном из серьезных антивирусных решений. Мы с Вами развернем полномасштабную защиту для корпоративной сети, насчитывающей несколько сотен компьютеров. Работать мы, в данном случае, будем с продуктами лаборатории Касперского.

Сразу предупреждаю: урок будет большим, потому что в нем будет содержаться много скриншотов, на которых будет показан практически каждый шаг настройки, развертывания и установки приложений. Я решил так: показывать все скриншоты – получится много страниц и очень большой урок. Писать фразы типа: «Ну, дальше – ничего сложного, разберетесь сами...» - рука не поднимается (обязательно кто-то не так сделает, а зачем мы тогда «начинаем КВН»?) ☺ Поэтому из двух зол я постарался выбрать меньшее, - первый вариант!

Работать мы будем используя виртуальные машины. Что это такое и как с ними обращаться мы с Вами рассматривали еще в одном нашем уроке: «Что такое виртуальные машины и как с ними работать?». Там мы устанавливали Windows Server 2008 и Windows XP. Вот их и будем использовать! Зря, что ли, устанавливали? ☺

Итак, **перед любой настройкой и установкой – этап планирования!** Как все это дело будет выглядеть и работать в нашей сети?

Предлагаю начертить себе небольшую схемку (для наглядности):



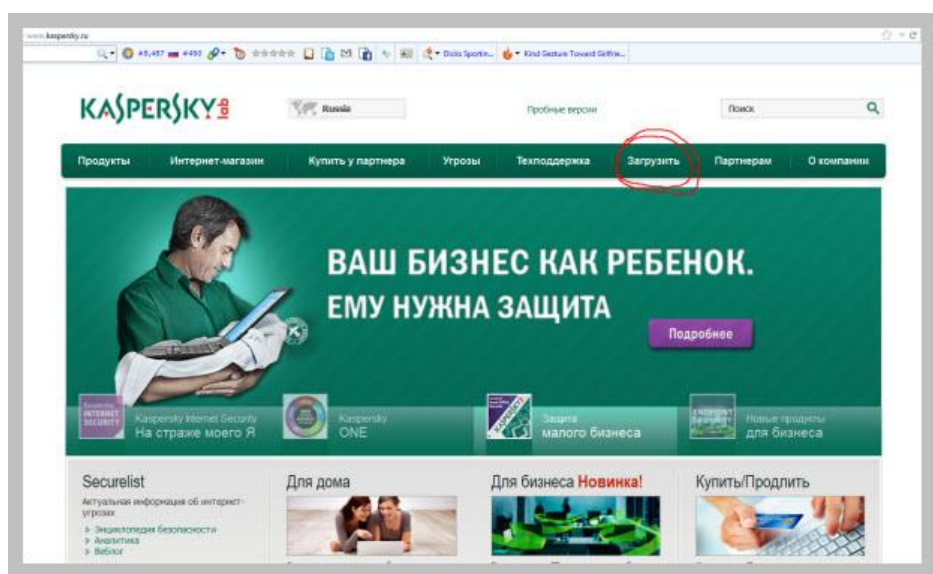
Локальная сеть

Как видим, у нас есть сервер с Windows 2008, на нем установлено корпоративное приложение антивируса Касперского. Приложение скачивает обновления антивирусных баз из Интернета (с серверов лаборатории Касперского), а все рабочие станции нашей локальной сети получают обновления своих антивирусных баз уже с НАШЕГО сервера. **НО!** Антивирусные базы еще – пол дела. Серверная часть антивирусного приложения позволяет осуществлять мониторинг клиентских (по отношению к ней) компьютеров в режиме реального времени.

Мы, как администраторы, можем видеть на каких компьютерах нашей локальной сети установлены антивирусные приложения, есть ли какие-то ошибки в функционировании некоторых из них? Можем видеть, успешно ли обновились антивирусные базы на всех компьютерах? Можем удаленно управлять практически всеми основными настройками антивируса на удаленном компьютере, а при необходимости – создать групповую задачу с определенными параметрами и удаленно запустить ее на всех клиентских машинах. Можем даже подключиться к удаленному рабочему столу пользователя и управлять его мышкой и клавиатурой ☺ И это – далеко не полный перечень того, какую выгоду мы получаем при использовании корпоративных решений.

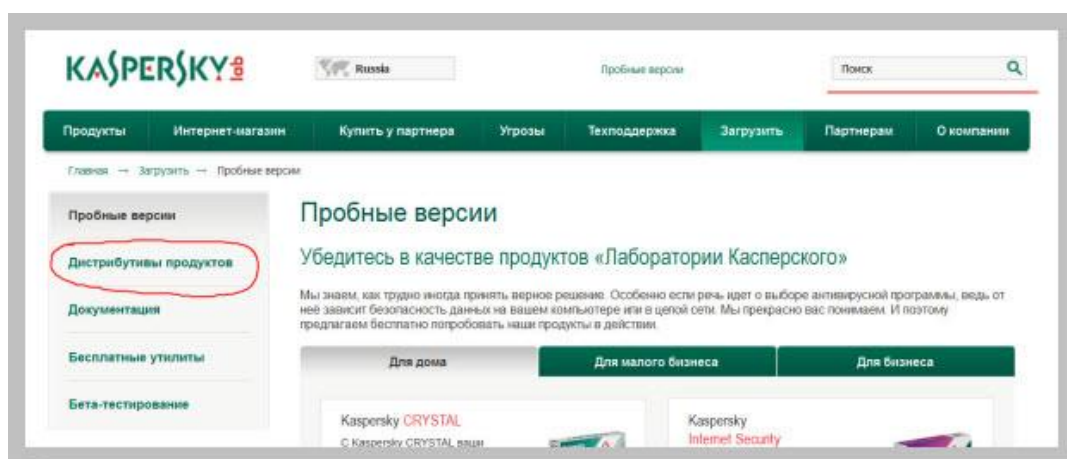
Но, прежде чем наслаждаться плодами прогресса и почувствовать себя настоящим администратором, нам нужно будет все это дело установить и настроить. Так давайте не будем медлить! Впереди – куча работы! ☺

Для начала, нам нужно будет скачать с сайта разработчика (в нашем случае – антивирусной лаборатории Касперского) необходимые нам дистрибутивы программных продуктов. Заходим на официальный сайт разработчика: лаборатории Касперского и нажимаем ссылку «загрузить».



Нам, для начала, нужно скачать весьма определенную вещь: «Kaspersky Administration Kit». Это и есть – консоль (серверная часть) управления всей антивирусной защитой корпоративной сети.

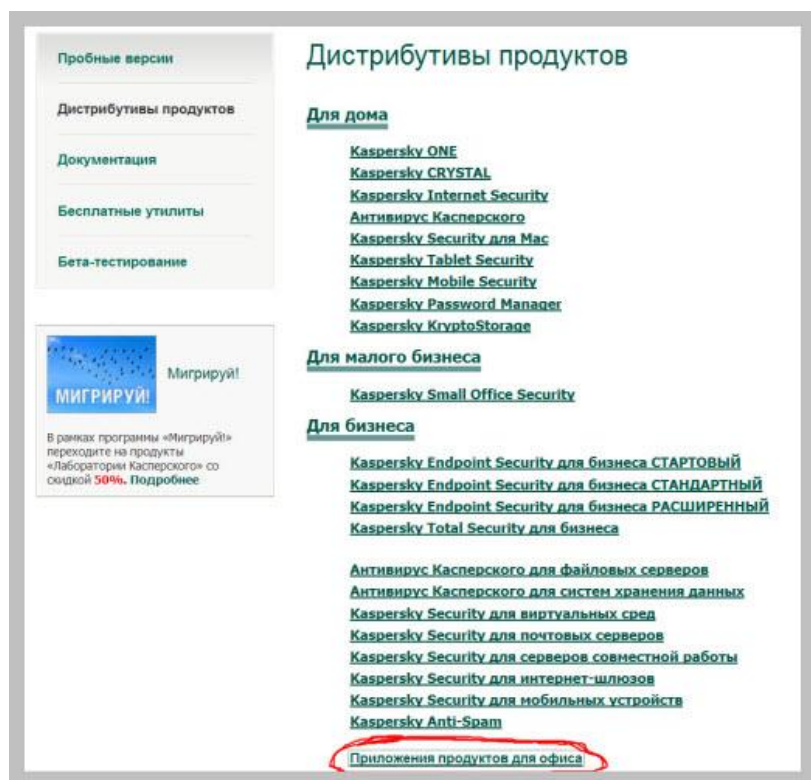
В следующем окне ищем пункт «Дистрибутивы продуктов».



Нажимаем на него и в правой части окна видим список всех программных продуктов от лаборатории Касперского.

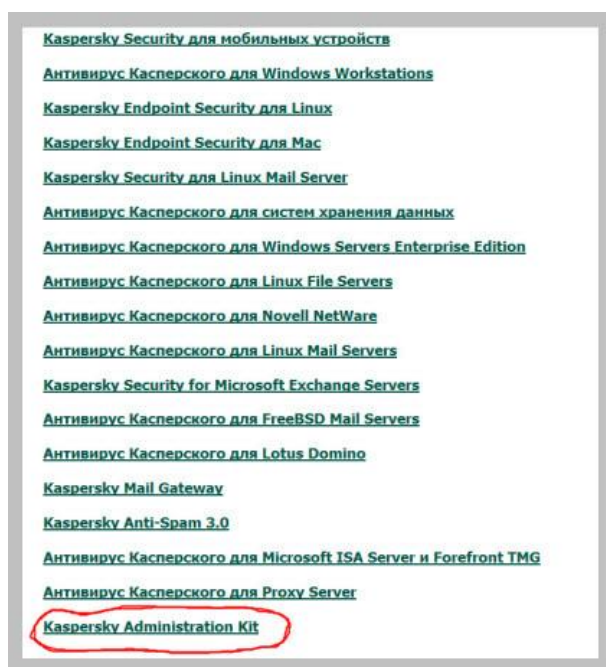
Не знаю почему там все именно так организовано, но иногда чтобы скачать что-то конкретное приходится долго лазить по списку программ и искать нужную. Может это специально так сделано, Вы не знаете? ☺

Итак, нам нужно зайти по ссылке «Приложения продуктов для офиса».



Совет: если Вам нужны корпоративные решения, то ищите в соответствующих разделах (для офиса, для бизнеса и т.д.)

И вот там – в самом низу перечня различных продуктов для корпораций обнаруживается нужная нам ссылка! Уже чувствуете себя следопытом? ☺



Нажимаем на ссылку «Kaspersky Administration Kit» и попадаем в раздел его загрузки:



Видим, что здесь есть три его версии и подраздел с документацией и руководствами в формате PDF. В большинстве случаев, лучше всегда загружать последние из доступных версии программных продуктов. Исходя из этого, мы имеем выбор между версией 8.0.2177 (Lite) и просто 8.0.2177.

Чем они отличаются? Прежде чем говорить об этом, давайте кратко рассмотрим, как работают подобные корпоративные системы антивирусной защиты? Точнее, как и где сохраняют свои данные? А сохраняют они их во внешней базе данных, которую мы, как администраторы, также должны будем установить и «связать» ее с сервером «Kaspersky Administration Kit». Согласен, звучит неприятно, но это, на самом деле, не так «страшно», как кажется ☺

База данных для Касперского, в данном случае, это – фундамент, на котором он работает. Чтобы было понятнее приведу другой пример: все современные CMS (Content Management System – системы управления контентом) на которых работает большинство сайтов в Интернете, используют базы данных. В этой базе, фактически, сохраняются все настройки сайта, вся его структура, логика взаимодействия, даже – фотографии.

На данный момент, стандартом «языка» (типа взаимодействия) пользователя с базой стал SQL (Structured Query Language) - «язык структурированных запросов», сейчас его поддерживают все современные разработки.

Но бывают исключения: например, наш проект SebeAdmin и его форум вообще не используют баз данных (а вот из принципа!) ☺

Итак, какие же есть популярные базы данных? Если говорить точнее - СУБД (системы управления базами данных), созданные по принципу клиент-серверных приложений.

В произвольном порядке:

- Ms SQL – база данных от Microsoft
- Oracle
- MySQL
- PostgreSQL
- InterBase
- FireBird
- DB2

Если то приложение, с которым Вы работаете, поддерживает (умеет работать) хотя бы с несколькими из перечисленных продуктов, то – все будет нормально. Естественно, чем большим будет этот выбор, тем лучше!

Так вот, возвращаемся к нашему антивирусу. Версия «Kaspersky Administration Kit» 8.0.2177 имеет скачиваемый объем примерно 350 мегабайт, а ее аналог 8.0.2177 (Lite) – всего около пятидесяти. Различие только в том, что в первом случае мы вместе с антивирусом скачиваем и установочные файлы базы данных для него. В данном случае это - СУБД Ms SQL. Надо сказать – «прожорливая» до системных ресурсов вещь! Версия «Lite» лишена этого «недостатка» и мы загружаем ее в чистом виде (без базы данных).

Базу к ней мы установим отдельно и не Ms SQL, а выберем что-то «полегче», например – MySQL, в народе – «**мускул**» ☺

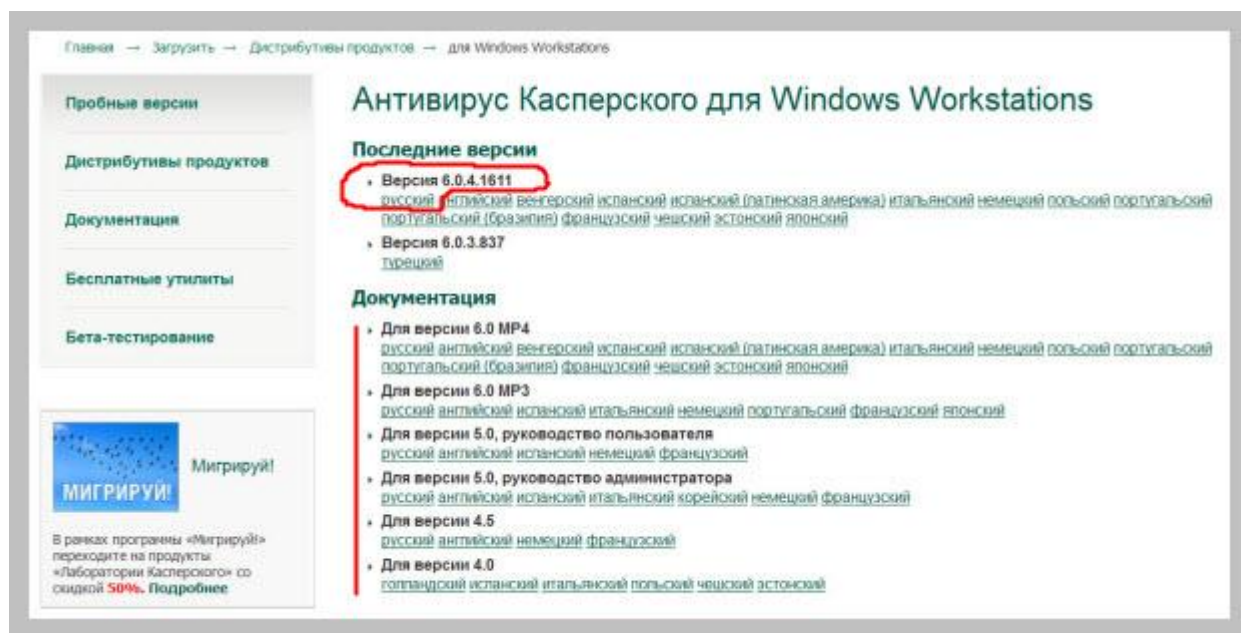
Но, не будем забегать вперед, а скачаем заодно здесь же еще одну вещь. Это – антивирус Касперского для Windows Workstation.



Почему именно его? Дело в том, что это именно та клиентская версия антивируса, которая работает вместе со скачанным нами до этого «Kaspersky Administartion Kit». Это

– пара: «админкит» устанавливаем на сервер, а антивирус WKS (Workstation) – на все остальные рабочие станции локальной сети.

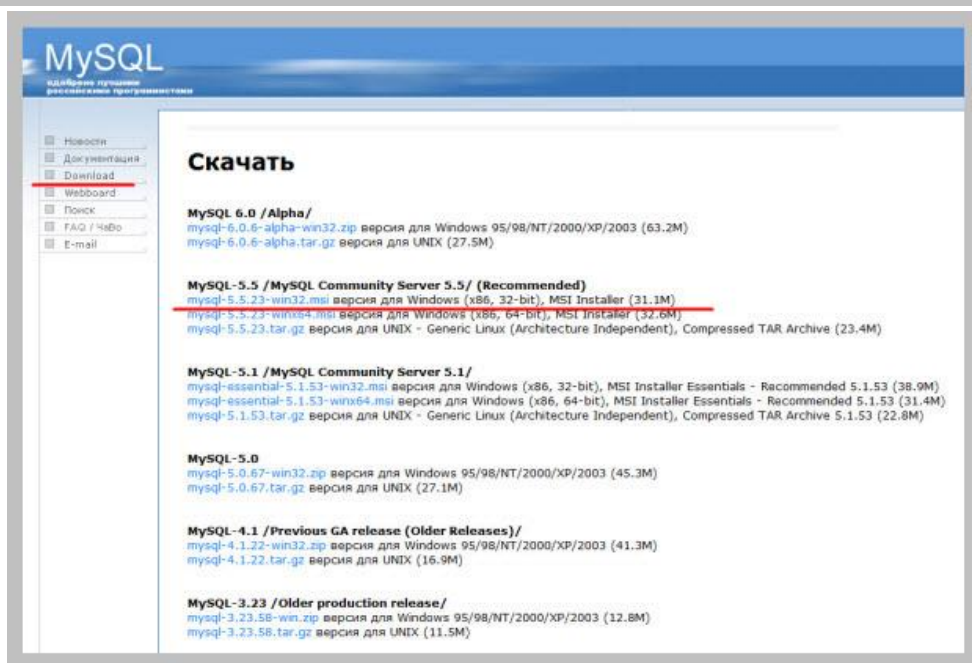
После нажатия на ссылку также попадаем в раздел загрузки WKS антивируса:



Здесь представлены также два подраздела: загрузка дистрибутива и документация и руководства к нему. Если нужно, можете скачать заодно и их. На данный момент, как видим, последняя версия Windows Workstation у нас 6.0.4.1611 Загружаем ее к себе на компьютер!

Как Вы уже поняли, пока мы собираем нужные нам компоненты (как в компьютерной игре, взяв профессию травника или алхимика) ☺ Потом нам нужно будет из всего этого добра «приготовить» правильное «зелье» – сервер администрирования лаборатории Касперского! ☺ Но для этого нам нужен еще один «ингредиент» - база данных!

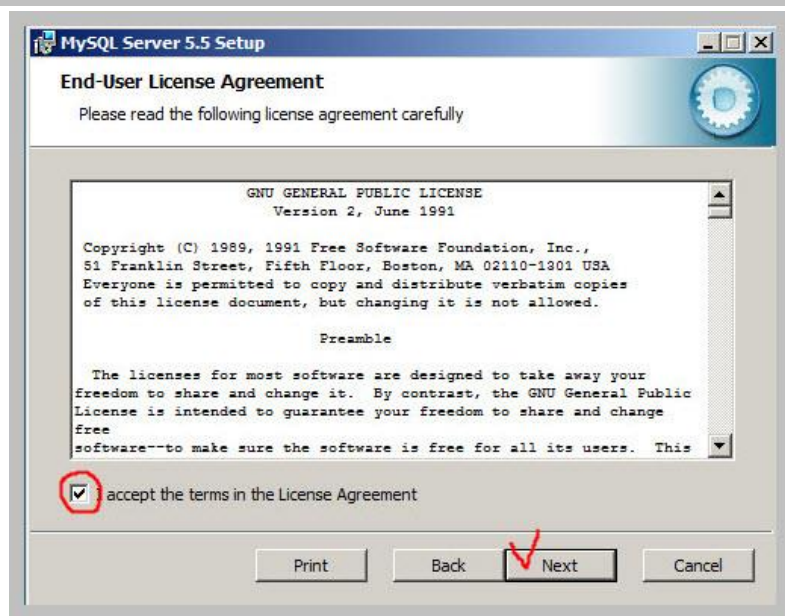
Для этого «идем» на <http://mysql.ru> и будем брать ее оттуда. Официальный сайт поддержки проекта MySQL это – <https://mysql.com>, но их база, в последнее время, занимает все больше и больше места (сто с лишним мегабайт против 31-го у mysql.ru) и «потребляет» с каждой новой версией все больше и больше ресурсов («слава» Ms SQL не дает спать – не иначе) ☺



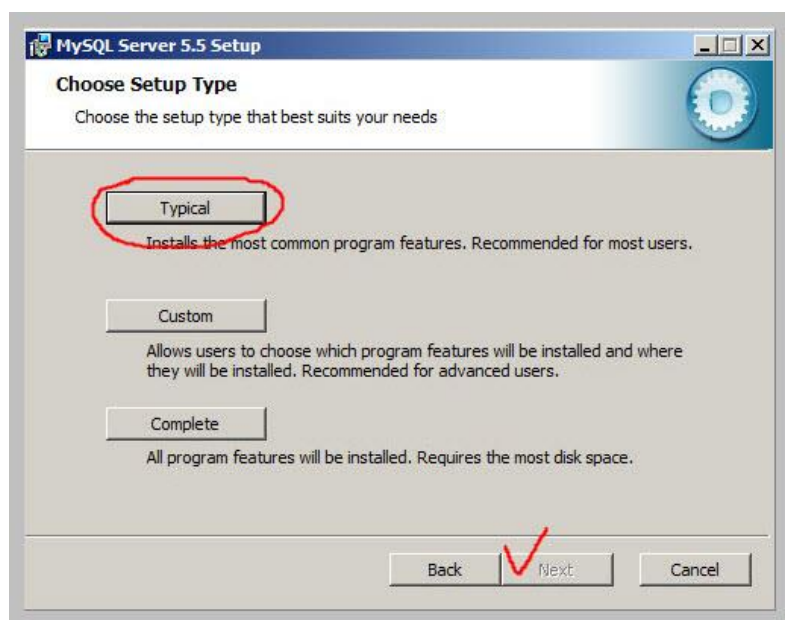
Итак, скачиваем последнюю версию дистрибутива для нашего сервера. Поскольку все три необходимые компонента мы уже загрузили, то пора с этим всем что-то таки начинать делать! ☺ Ничего сложного здесь нет, но разберем все этапы максимально подробно. Запускаем установочный файл сервера MySQL и видим мастер установки, который поможет нам преодолеть все шаги инсталляции продукта.



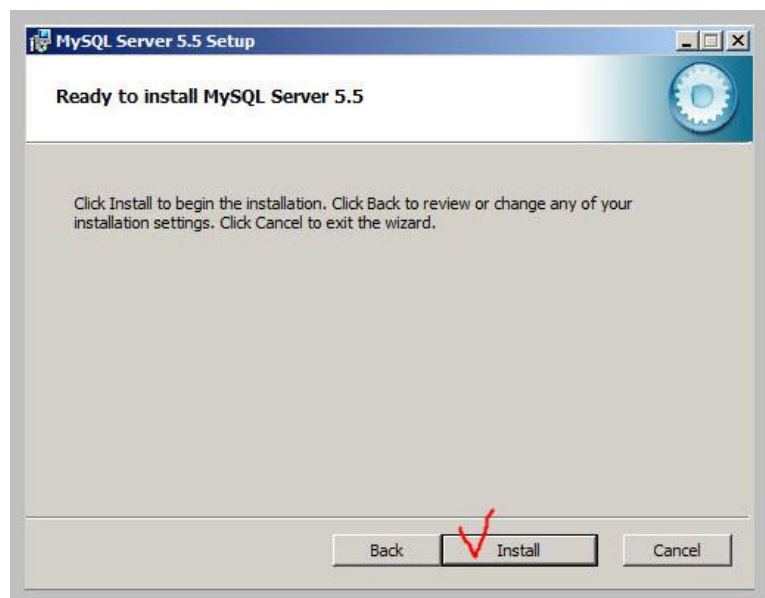
Нажимаем кнопку «Next» (Дальше) и в следующем окне нас просят принять лицензионное соглашение:



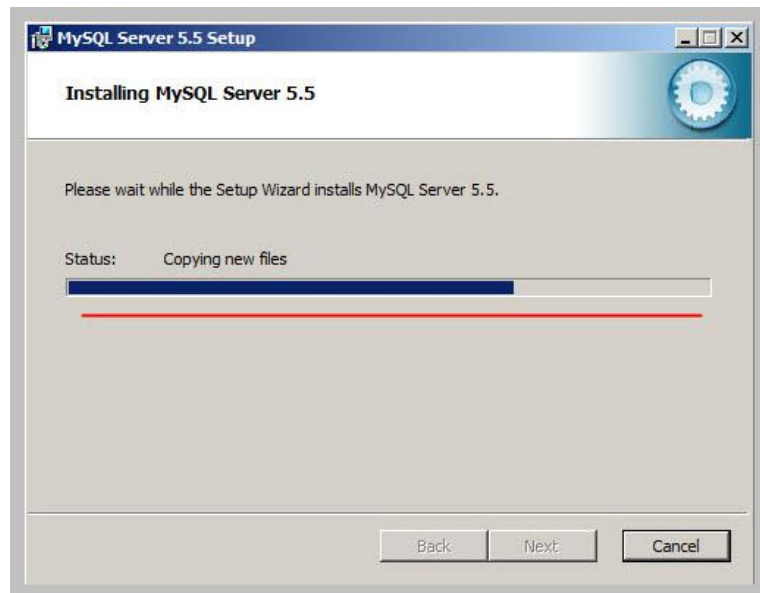
Ставим соответствующую галочку (мол - согласны) и нажимаем «Next».



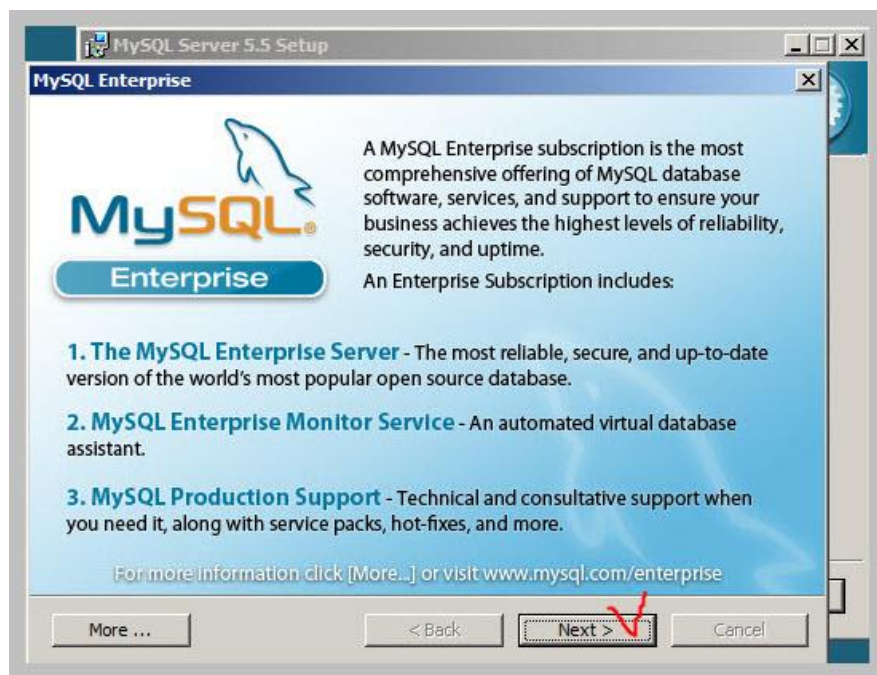
Выбираем «Typical» (стандартная конфигурация) и двигаемся дальше.



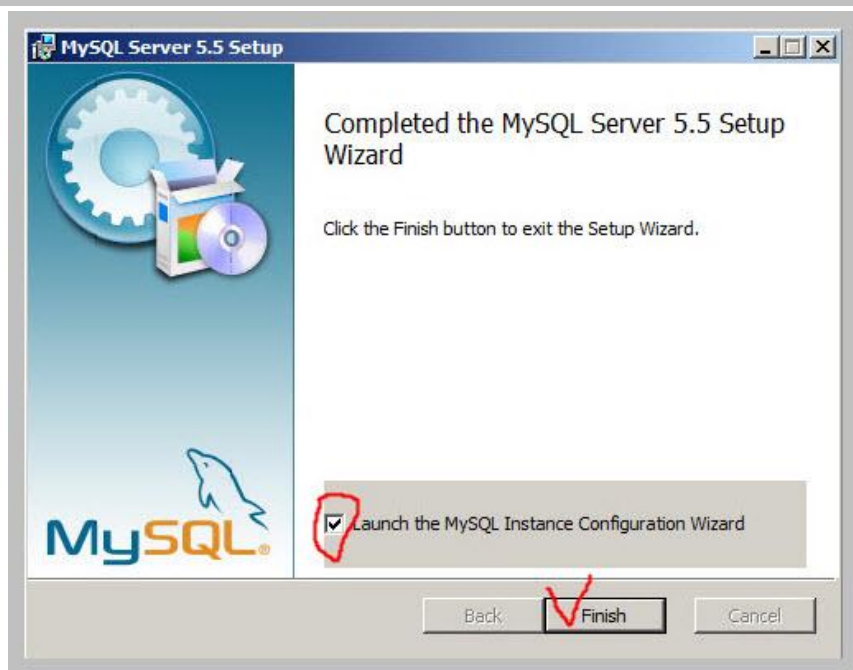
Здесь нам нужно нажать на кнопку «Install» (установка) и запустится сам процесс.



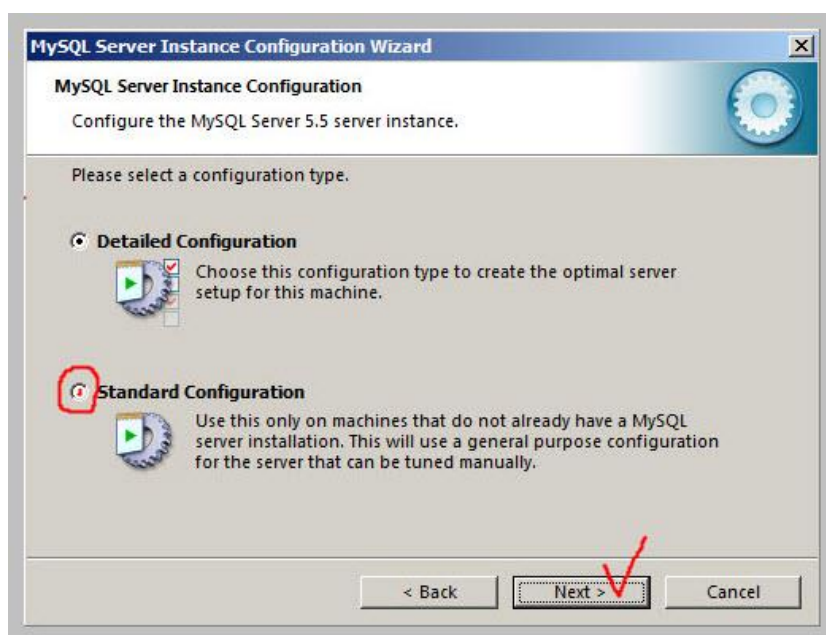
После его окончания мы увидим вот такое окно:



Идем дальше. В следующем окне подтверждаем галочкой, что мы хотим произвести первоначальную быструю настройку сервера:

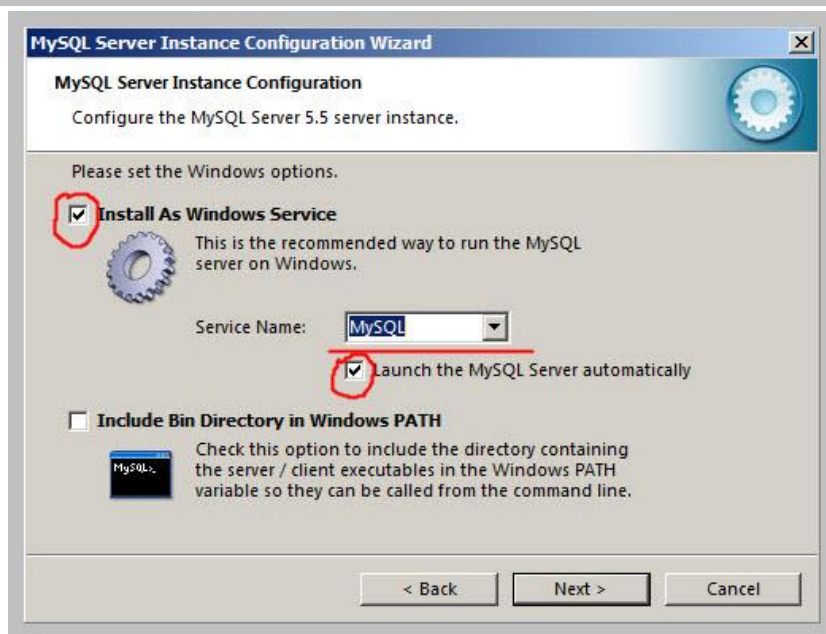


Нажимаем кнопку «Finish». После этого запустится уже мастер начальной настройки и конфигурации нашего установленного MySQL сервера:



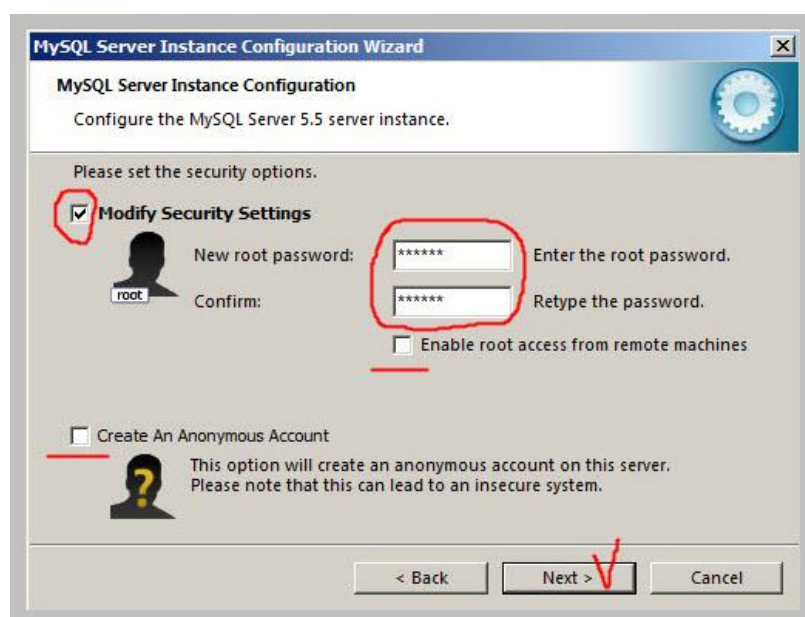
Я выбрал опцию «Standart Configuration», если хотите отвечать на много «лишних» вопросов, то можете выбрать первый вариант.

Тем не менее, некоторых вопросов и настроек избежать не удастся 😊



На скриншоте выше расставим галочки в нужном нам порядке. Первая устанавливает наш SQL сервер в систему, как службу (Install As Windows Service). Это гарантирует нам, что MySQL будет стартовать вместе с Windows. Это нам, собственно, и нужно! Поле «Service Name» дает нам возможность выбрать, как будет отображаться название системной службы базы данных в списке других служб Windows (не принципиально). Можем оставить как есть. И галочка «Launch the MySQL Server automatically» позволяет нам запускать базу данных автоматически после загрузки операционной системы.

В следующем окне нам предложат указать пароль администратора (root) к базе данных. Придумайте что-то позаковыристей, но – не забудьте! ☺

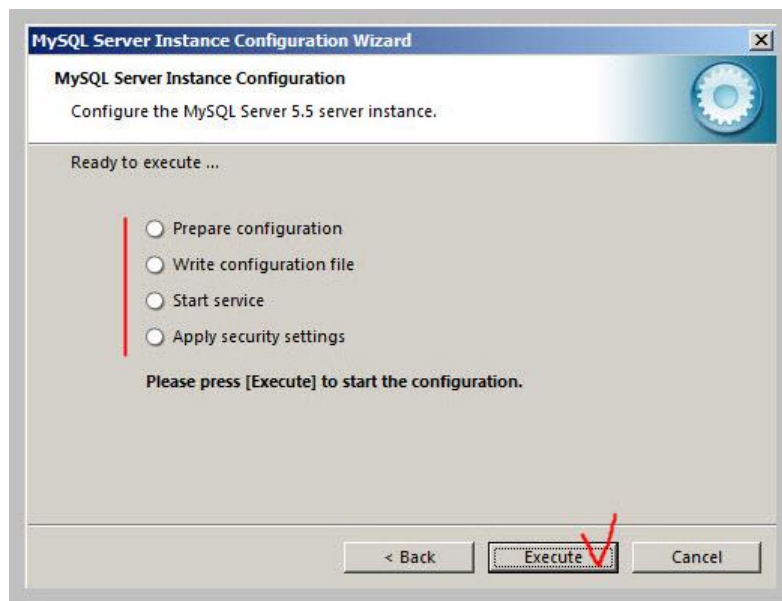


Функция «Enable root access from remote machines» позволит нам получать администраторских доступ к базе данных с удаленных компьютеров (через сеть). Для задачи развертывания корпоративной антивирусной защиты эта функция нам не нужна.

Пункт «Create an Anonymous Account» дает возможность подключаться к нашей базе данных с анонимным аккаунтом (с точки зрения безопасности – плохо, поэтому – не задействуем).

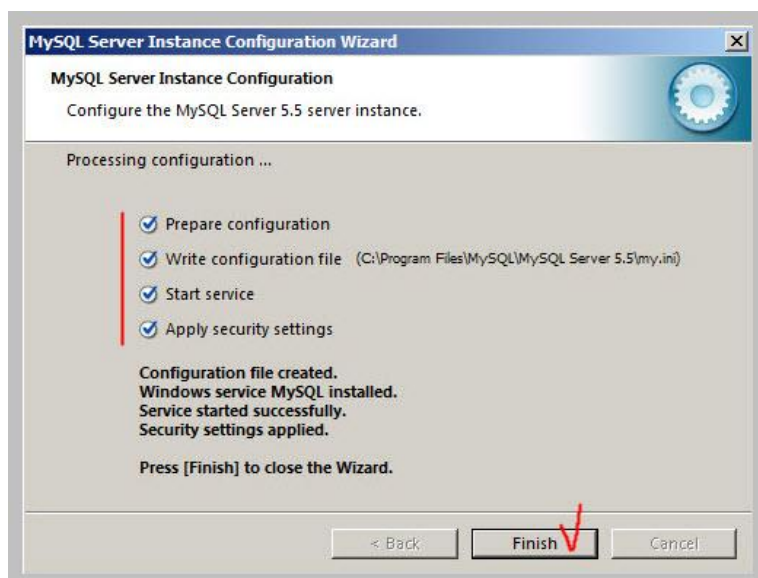
В данном окне больше делать нечего. Двигаемся дальше!

На фото ниже система отчитывается нам о том, какие действия она будет совершать в результате первоначальной автоматической само-конфигурации.



Великодушно даем свое разрешение, нажатием кнопки «Execute» (выполнить) !

После непродолжительного ожидания галочками у нас отметятся пункты, которые программа успешно выполнила:



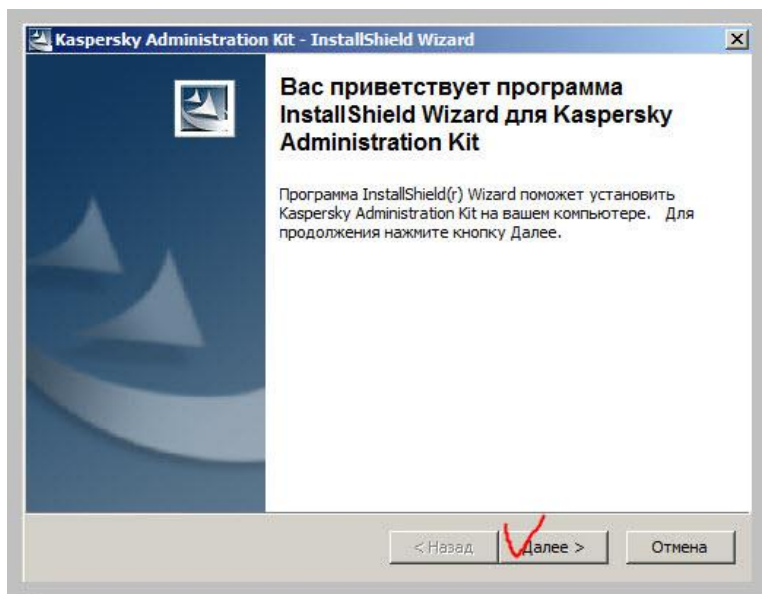
Видим, что ошибок нет, все нормально. Нажимаем «Finish» (завершить).

Все! Поздравляю! Вы только что установили сервер базы данных MySQL ! ☺

Но это еще – меньше чем пол дела! «Голая» база данных нам сама по себе не нужна. Помните, в ней должны содержаться данные другой серверной службы - «Kaspersky Administration Kit»?

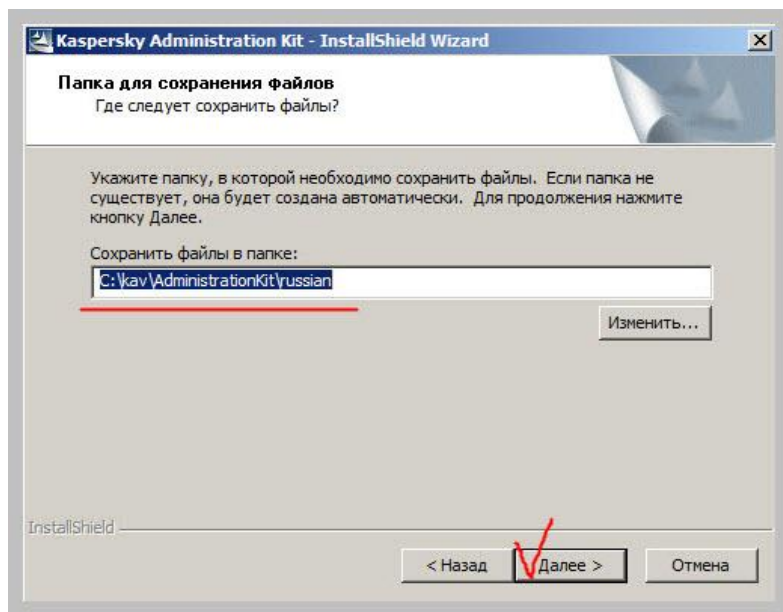
Вот его мы сейчас и будем устанавливать. Вы ведь его уже скачали, как описано в начале нашей статьи, правда? ☺

Итак, запускаем установочный файл и готовимся «общаться» еще с одним мастером установки. На этот раз – от лаборатории Касперского:



Мысленно и мы посылаем привет и нажимаем кнопку «Далее» ☺

На следующем скриншоте нас спрашивают, в какую директорию (папку) мы хотим произвести промежуточную распаковку файлов программы?

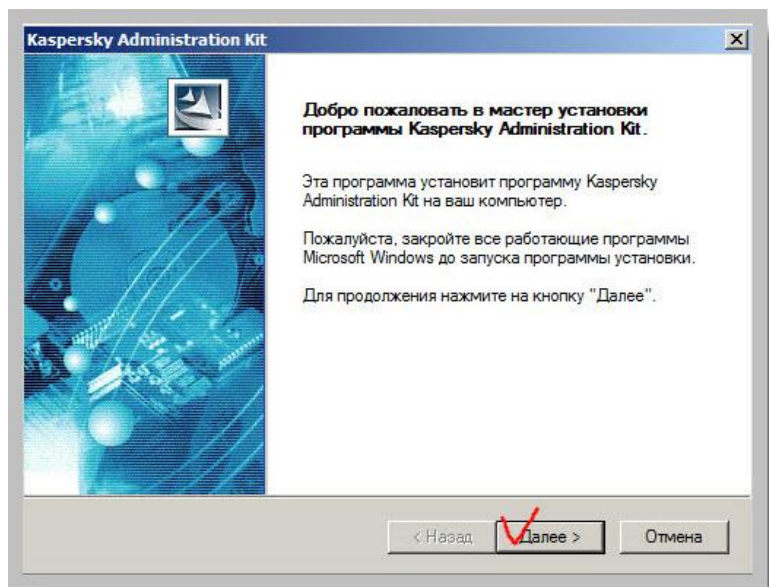


Это – не принципиально, поэтому оставляем предложенный по умолчанию вариант и нажимаем «Далее»

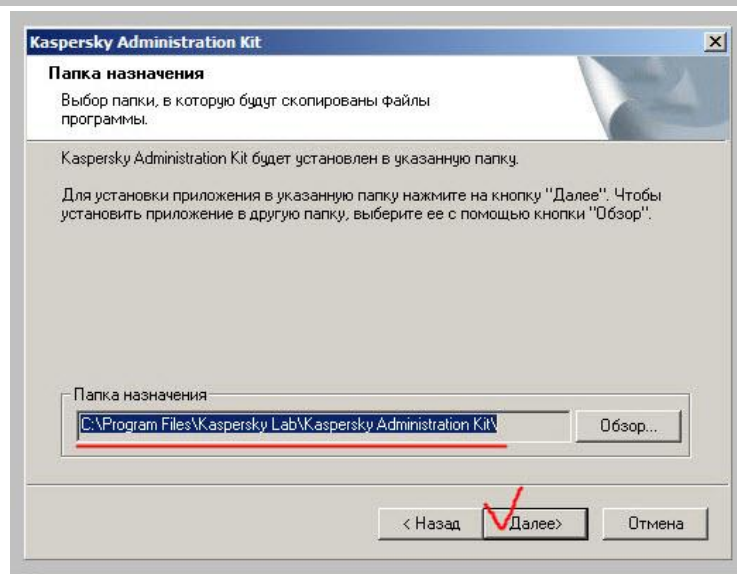
Запускается процесс распаковки и подготовки запуска мастера установки:



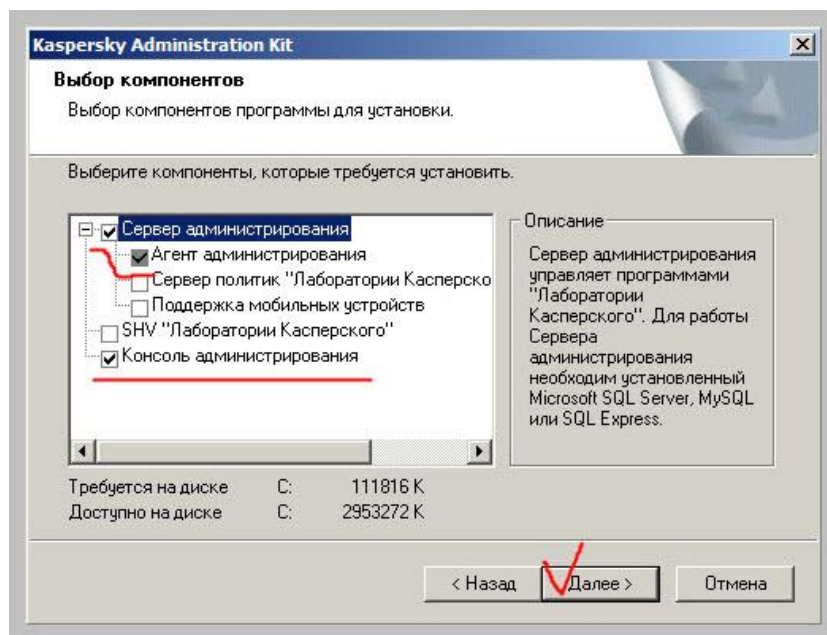
По его окончании видим следующее окно:



Опять - «Далее». Вот теперь нас спрашивают куда мы хотим установить саму программу? Я не стал ничего менять и оставил путь по умолчанию:
C:\ProgramFiles\KasperskyLab\KasperskyAdministrationKit

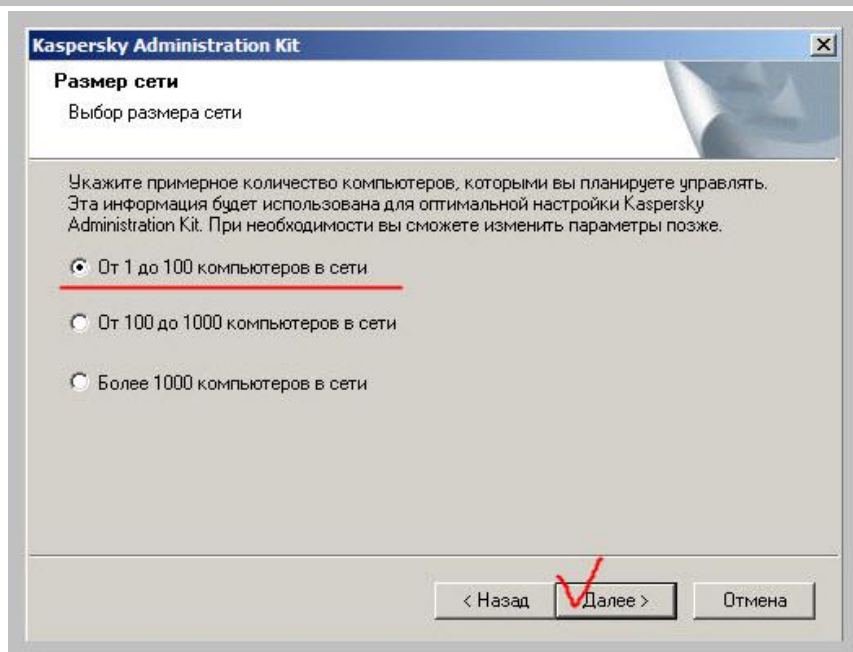


Двигаемся дальше! Вот там – уже интереснее. На скриншоте ниже мы можем выбрать те компоненты, которые хотим установить вместе с сервером администрирования лаборатории Касперского.



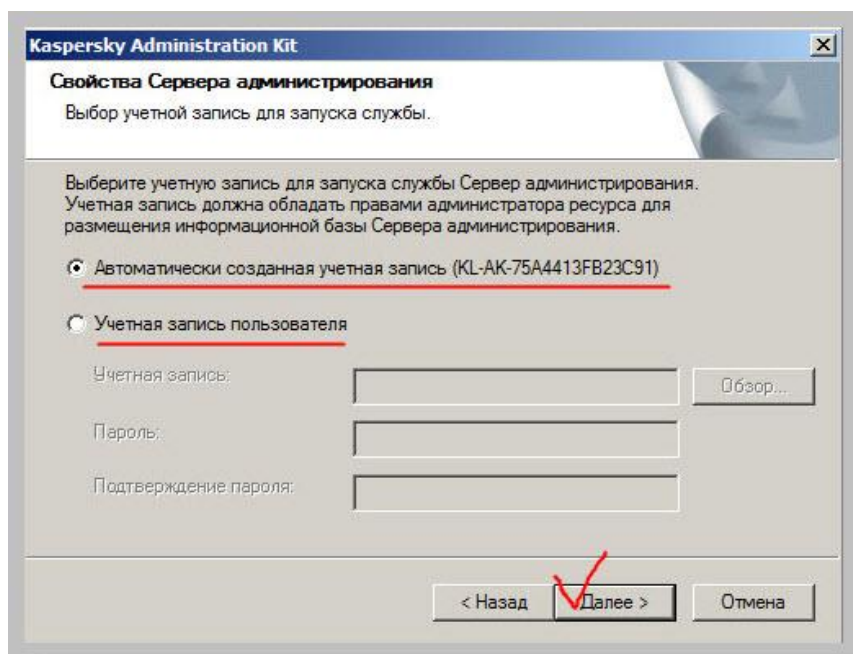
При выделении мышкой любого из пунктов в поле «Описание» мы можем видеть краткую подсказку о той или иной конкретном элементе. Лично для себя, я расставил галочки так, как показано выше. Можете поступить таким же образом, если Вам не нужны какие-то дополнительные специфические функции.

Нажимаем кнопку «Далее». На этом шаге нас спрашивают, о размере нашей локальной сети (исходя из количества компьютеров в ней)



В нашей реальной сети предприятия около 350-ти компьютеров, но поскольку я делал эти скриншоты работая в виртуальных машинах, то я выбрал первое значение. Вы, конечно же, исходите из своей ситуации.

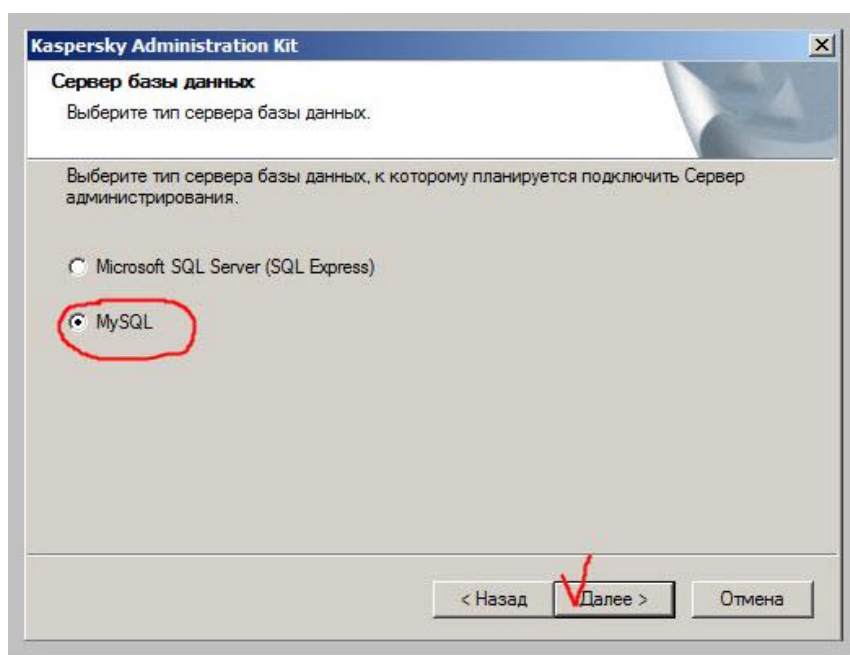
Нажимаем «Далее». Здесь нам нужно будет указать учетную запись компьютера, от имени которой будет выполняться сама служба (процесс или программа) «Kaspersky Administration Kit».



Как написано на скриншоте выше, эта учетная запись должна обладать правами администратора (входить в группу администраторов) нашего сервера. У нас есть здесь два варианта: автоматически создать учетную запись с правами локального администратора средствами самого антивируса Касперского. Я именно так и сделал! Или

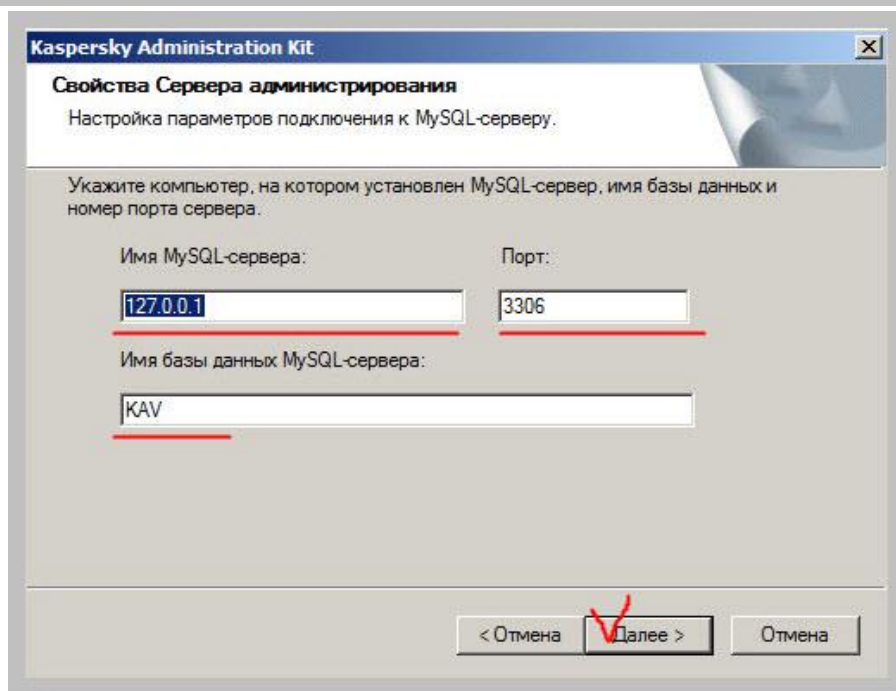
же поставить переключатель возле надписи «Учетная запись пользователя» и в ставшими доступных после этого полях, вручную (или используя кнопку «обзор») указать имя (учетную запись) и пароль уже существующего в системе пользователя с привилегиями «администратор».

В следующем окне нам пригодится то, что мы проделали ранее (наша уже установленная база данных)!



Если Вы, как мы и описывали ранее в уроке, скачали версию «Kaspersky Administration Kit **Lite**» и уже установили базу данных My SQL, то – выбор очевиден! Нажимаем кнопку «Далее».

В следующем окне, которое появится, нам будет предложено создать базу данных и выполнить настройку подключения к ней сервера «Kaspersky Administration Kit».

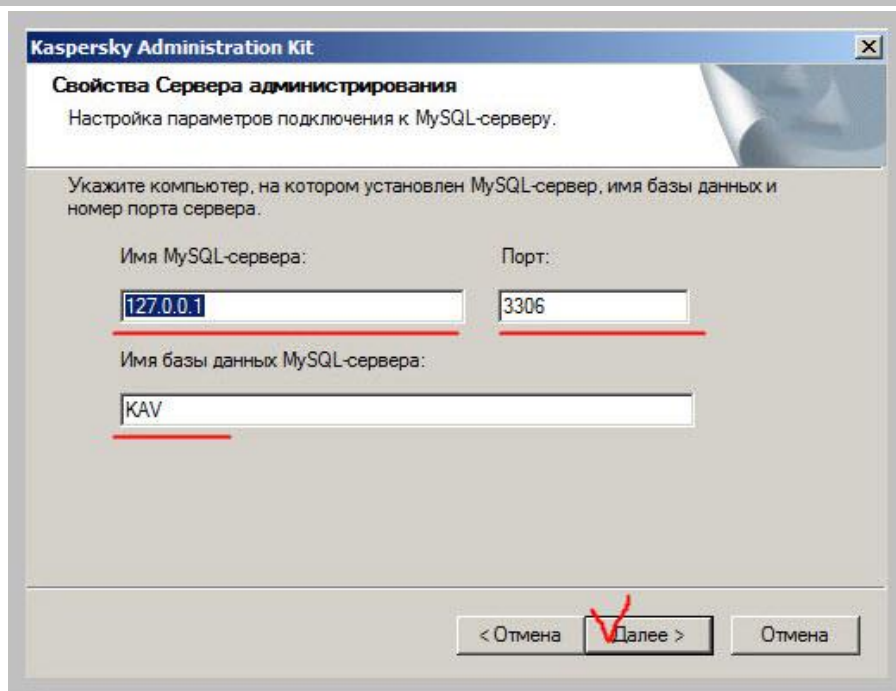


Напомним, как это все работает в связке. Создается пустая база данных, которая, по мере работы, серверной части антивируса Касперского, будет наполняться данными. Для прямого доступа к базе любой пользователь (программа или процесс) должны авторизоваться в ней (ввести свое имя и пароль). Помните, на одном из этапов установки MySQL нас просили указать пароль к базе данных?



Наш «Kaspersky Administration Kit» для доступа к базе и работы с ней должен быть авторизован в ней под именем суперпользователя root («root» – аналог администратора в операционных системах Linux и Unix).

Теперь – продублируем наш предыдущий скриншот и разберем его подробнее:



Поле «Имя MySQL сервера». Здесь мы можем указать сетевое имя или IP адрес компьютера, на котором установлена наша база данных? Фишка в том, что база может быть установлена на одном компьютере в сети, а «Kaspersky Administration Kit» - на другом. Просто у нас (для упрощения схемы) база и «Kaspersky Administration Kit» установлены на одном физическом компьютере под управлением Windows Server 2008.

С этим – разобрались! Двигаемся дальше! Что значит запись 127.0.0.1 ? Это общепринятый IP адрес локальной машины. Попробуйте выполнить из командной строки команду **ping 127.0.0.1** Вы увидите, что пакеты успешно передались по этому адресу? Почему? А потому, что это Ваш локальный компьютер и есть! Его также иногда называют localhost – «локальная машина (хост)». Этот адрес – своеобразная «заглушка» или – «петля», если хотите, в Вашем сетевом адаптере.

Вот – выдержка из Википедии: «Как правило, интерфейс, соответствующий адресу 127.0.0.1, существует исключительно как программная абстракция на уровне ядра операционной системы. Обычно адресу 127.0.0.1 сопоставляется мнемоническое имя компьютера localhost».

Следующее поле на скриншоте выше - «Порт». Понятие порта мы рассматривали в одном из наших предыдущих уроков. Но если кратко, это – виртуальный идентификатор конкретного процесса в операционной системе. Общее количество портов – более 65-ти тысяч. Причем первые 1024, как правило, зарезервированы для различных системных служб и сервисов, а все остальные могут быть произвольно использованы (назначены) на прием или передачу сетевых данных между различными приложениями (программами).

Как правило, работа с портами для подавляющего большинства пользователей проходит абсолютно незаметно и они даже не догадываются о том, что те программы, с которыми они работают, используют какие-то там порты, но мы-то с Вами – **сами себе админы!** Поэтому знать о портах должны и, при необходимости, эти знания – применять.

Сейчас – именно такой момент! ☺

Итак – поле «Порт». По умолчанию установщик «Kaspersky Administration Kit» предлагает нам число 3306 (можете поменять на любое другое, большее 1024, но смысла в этом не вижу).

Что же именно это значит? А то, что устанавливаемая нами программа после инсталляции будет «слушать» (ожидать сетевого соединения на него) порт с номером 3306. Те, все пакеты, отправляющиеся по сети на этот компьютер и на этот порт программа (в данном случае - «Kaspersky Administration Kit») будет однозначно идентифицировать как те, которые предназначаются именно ей, а не какой-либо другой программе или службе.

Надеюсь, я понятно все это дело объяснил? ☺

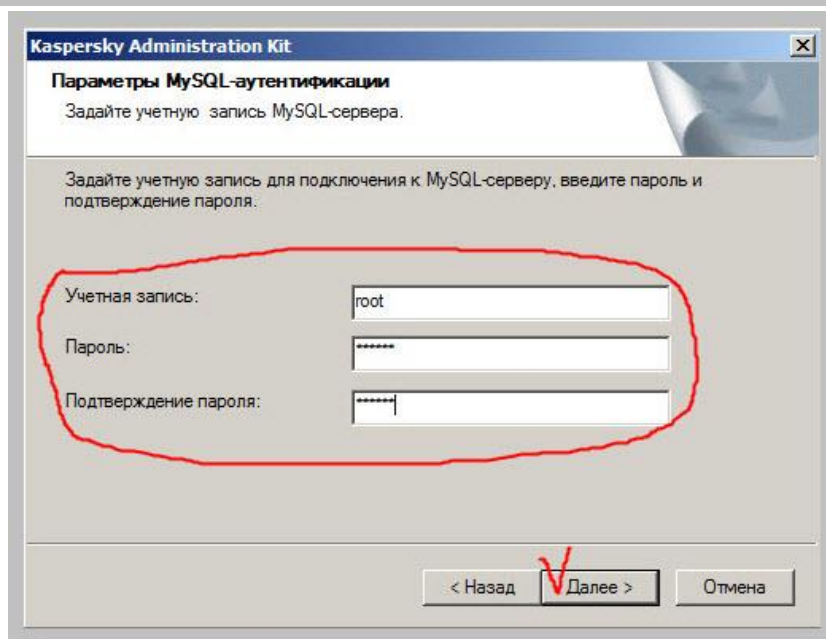
Что там у нас осталось на скриншоте выше? Поле - «Имя базы данных MySQL сервера». Что это такое? **MySQL это - сервер базы данных (а не сама база)**, и как каждый уважающий себя сервер, ☺ он может иметь много отдельных баз с данными.

При необходимости мы просто создаем еще одну под наши нужды.

Вот на фото выше «Kaspersky Administration Kit» при установке и предлагает нам создать новую базу для своих данных под именем KAV (Kaspersky Anti Virus, видимо). Можете изменить название по своему усмотрению, но, опять же, я бы оставил все, как есть. Не буду вдаваться в подробности, но я это не просто так говорю, поверьте мне на слово! ☺

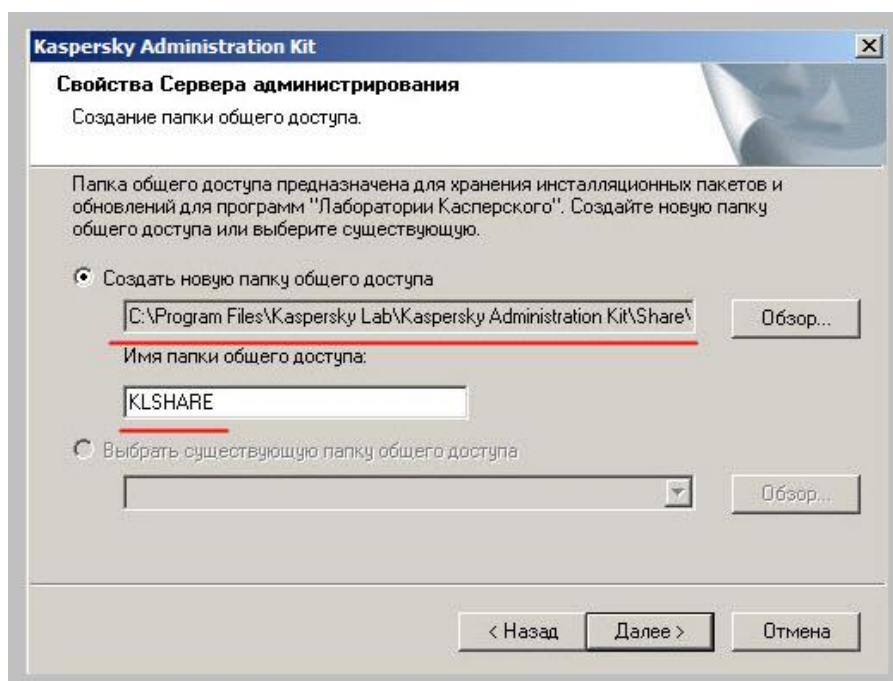
Нажимаем кнопку «Далее».

Вот в этом окне нам нужно будет сделать то, о чем мы уже немного говорили выше – прописать логин и пароль для доступа (подключения) к нашей базе данных сервера «Kaspersky Administration Kit».



Мы проделываем это только один раз. Пароль сохраняется в настройках программы и каждый раз при старте «Kaspersky Administration Kit» будет автоматически подключаться к базе MySQL сервера. Пароль и логин Вы должны помнить, так как мы указывали его при установке сервера баз данных. Вписываем эти учетные данные в соответствующие поля и нажимаем «Далее».

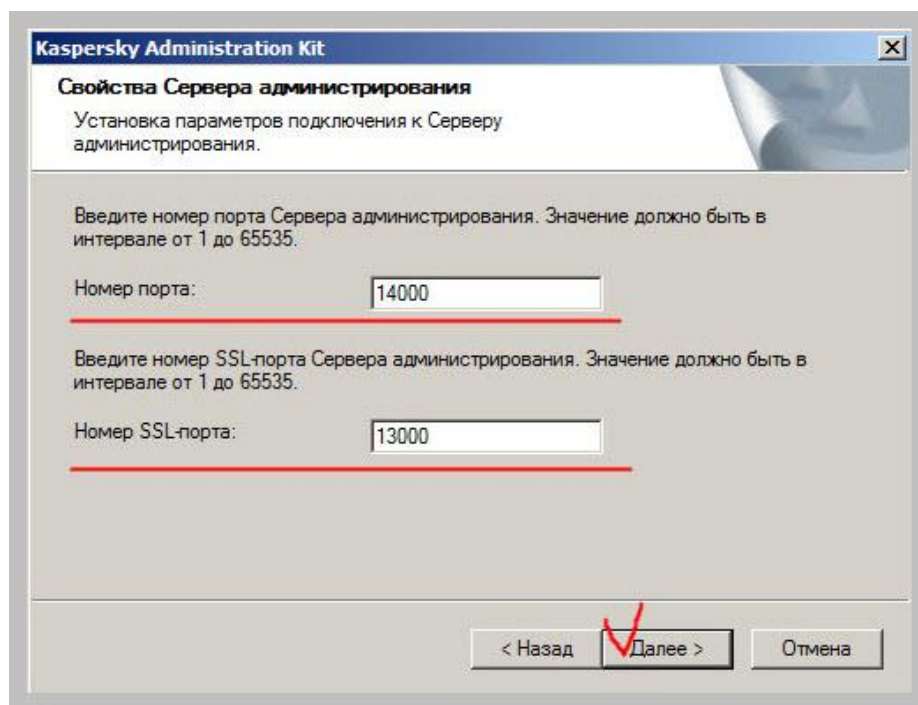
Внимательно прочтите, что сказано на скриншоте ниже:



Все скачанные из Интернета обновления антивирусных баз сервером «Kaspersky Administration Kit» будут помещаться именно в эту папку. Это – автоматически создаваемая при установке директория, с соответствующими правами для сетевого доступа к ней клиентских компьютеров всей нашей компьютерной сети.

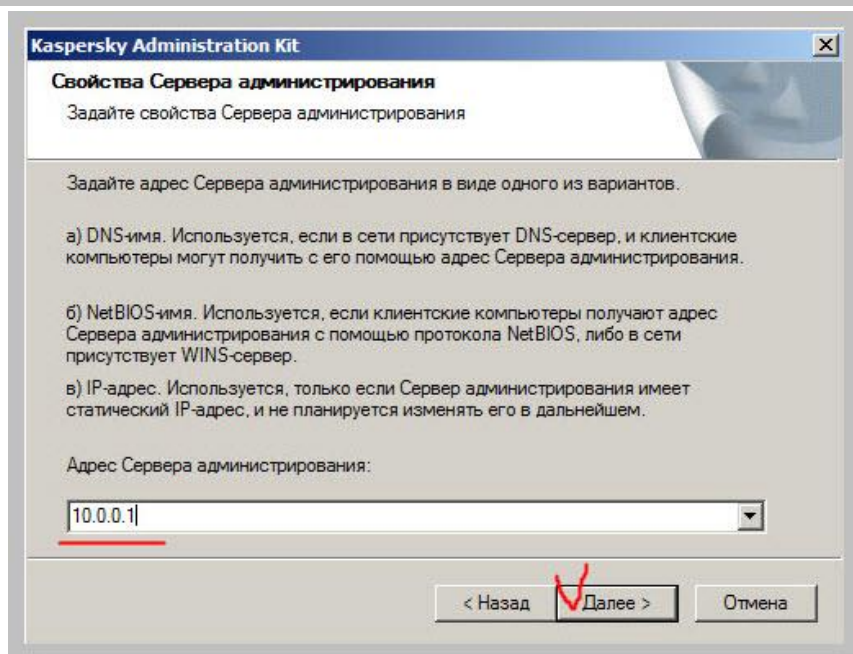
Можете, при желании, изменить место ее расположения или само ее название. Я же, как всегда, рекомендую оставить эти настройки без изменения ☺ Нажимаем «Далее».

В следующем окне нам предложат сконфигурировать (или оставить без изменений) настройки номеров портов для подключения к серверу администрирования клиентских компьютеров.



Как Вы думаете, что я посоветую Вам сделать? Правильно! Ничего не менять, а оставить, на усмотрение программы! ☺ Просто, если Вы измените здесь предустановленные значения портов, то при установке агента администрирования (мы поговорим об этом ниже) Вам каждый раз нужно будет вводить значения порта вручную. Т.е. – придется постоянно помнить его, так как программа по умолчанию настроена на работу именно с теми номерами портов, которые представлены на скриншоте. Их изменение с нашей стороны для программы будет «сюрпризом» и сама она его «переварить» не сможет, а будет продолжать попытки соединения именно по порту 14000... Ну – суть Вы уловили? Не уверен – не изменяй! ☺

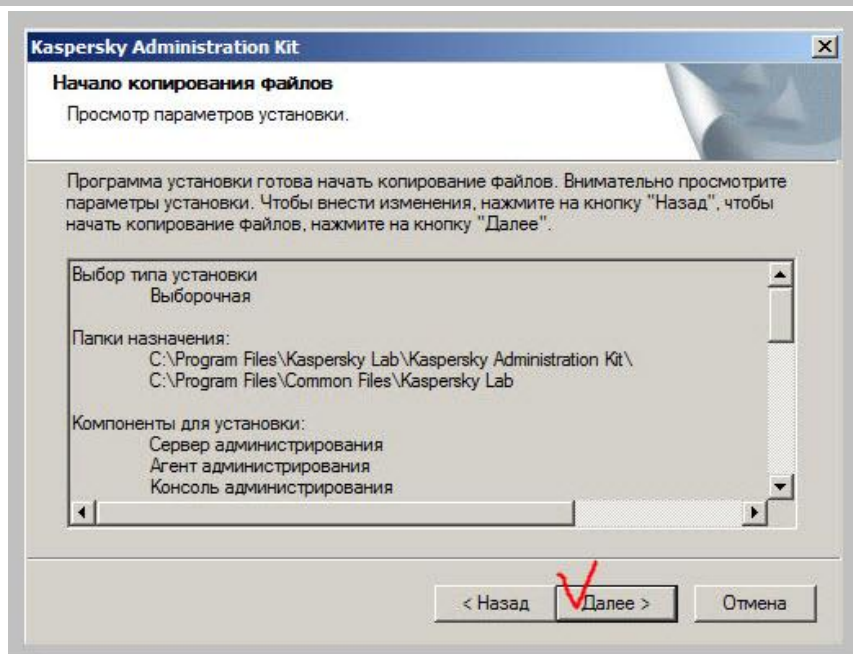
Идем «Далее».



Что нам нужно здесь знать про поле «Адрес Сервера администрирования»? Прежде всего, вдумчиво читаем все три пункта, которые указаны на скриншоте выше: «а», «б» и «в». Поскольку своего DNS сервера у нас в сети пока еще нет, то и его имя мы писать здесь не будем. Второй пункт, скорее нужен для совместимости с устаревшими компьютерами и протоколами передачи данных, поэтому – тоже пропускаем. Для нашего тестового урока как нельзя лучше подойдет третий из предложенных вариантов (в).

IP адресом нашего сервера под управлением Windows Server 2008 я заранее назначил - 10.0.0.1, так что его здесь и указываю. У Вас может быть другой вариант. Единственное, обратите внимание на предложение о том, что в этом случае адрес сервера должен быть статическим (жестко прописан вручную в свойствах сетевого адаптера), а не быть выдан динамически (DHCP) сервером локальной сети.

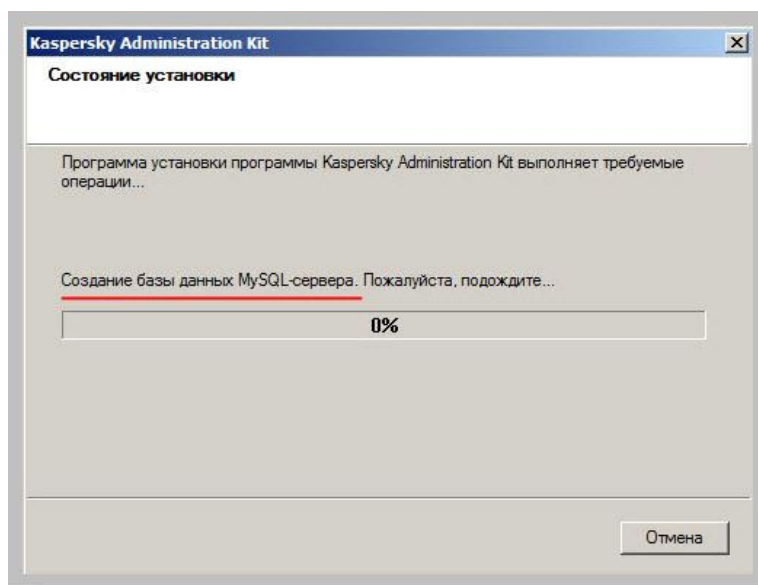
Нажимаем «Далее».



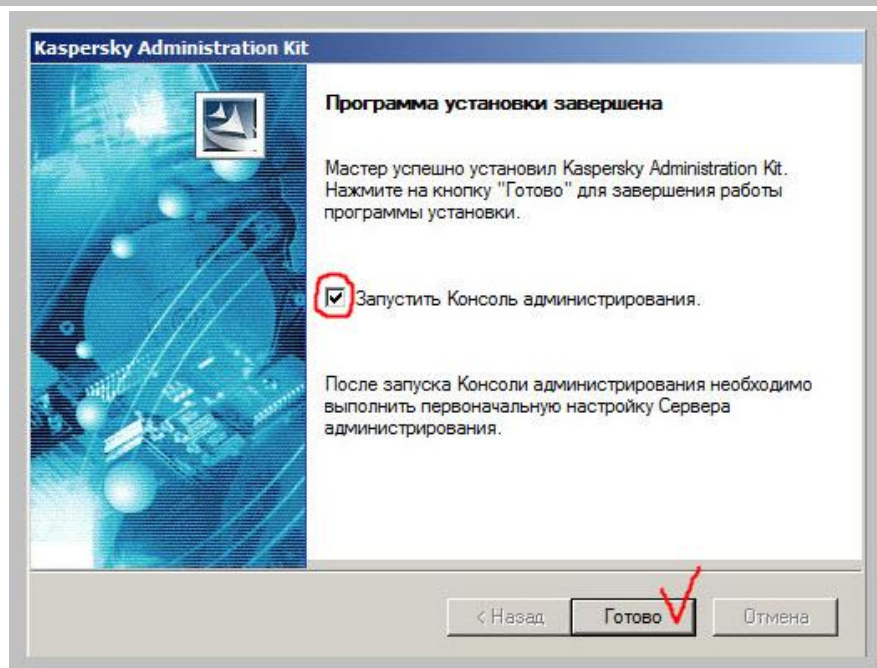
Вот теперь можем немного расслабиться! ☺ Мы передали программе установки и первоначальной настройки все необходимые ей для начала работы сведения и теперь, в который раз нажав «Далее», можем откинуться на спинку стула и наблюдать за процессом установки сервера администрирования от лаборатории Касперского.

Начинается мой любимый в этом деле процесс, когда я отдыхаю, а ОНО само все делает! ☺

На скриншоте ниже мы можем видеть как программа, согласно нашим инструкциям, создает базу данных MySQL, настраивает подключение к ней, потом устанавливает сам «Kaspersky Administration Kit», и конфигурирует его. Короче говоря – картина маслом: «Вкалывают роботы, а не человек!» ☺



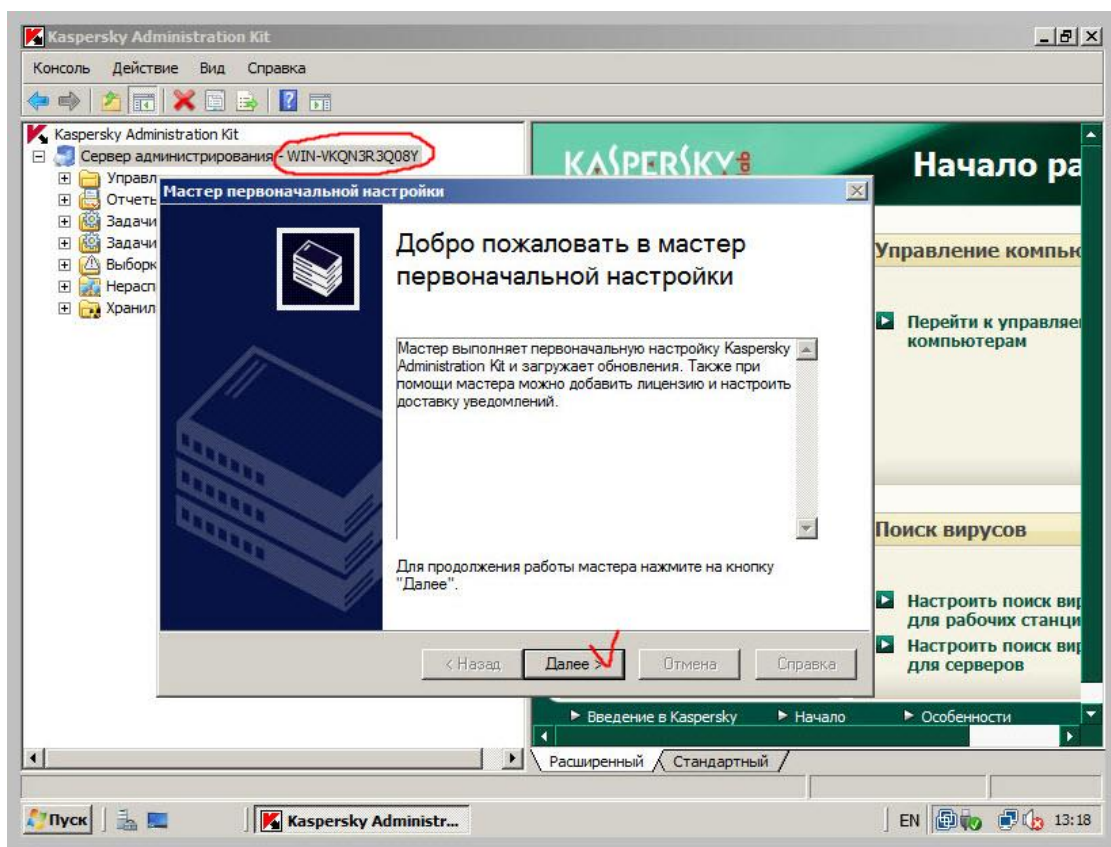
По окончании этого увлекательного процесса, мы увидим вот такое окно:



Можем сразу отметить галочкой пункт «Запустить Консоль администрирования» и нажать кнопку «Готово».

После этого (приготовьте фотоаппараты, чтобы увековечить этот момент) запустится сама консоль! ☺

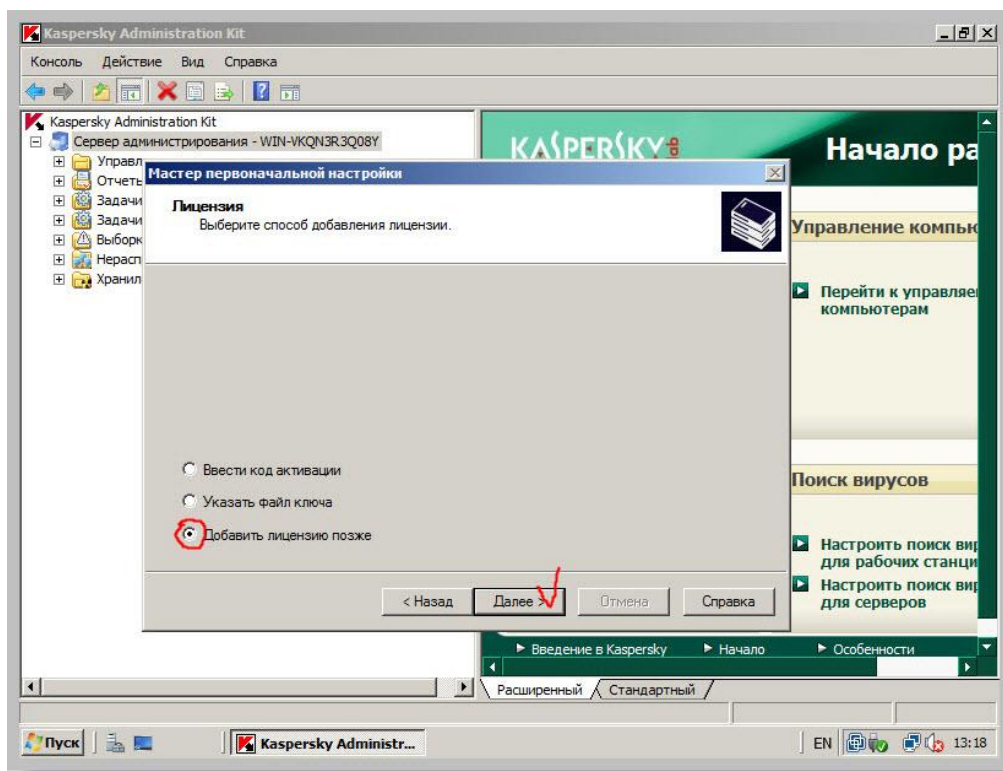
Примечание: по другому ее можно запустить с рабочего стола, нажав на иконку красного цвета «Ярлык для CS Admin Kit».



Как видите, красным на фото выше я обвел имя нашего виртуального сервера с Windows 2008. Выглядит оно – крайне неудобоваримо, поэтому для последующих наших скриншотов я планирую переименовать его в «Server», так что наблюдательный читатель обязательно это заметит ☺

Итак, для нас запустится отдельный мастер (мастер первоначальной настройки Admin Kit), который поможет нам совершить начальное развертывание антивирусной защиты корпоративной компьютерной сети.

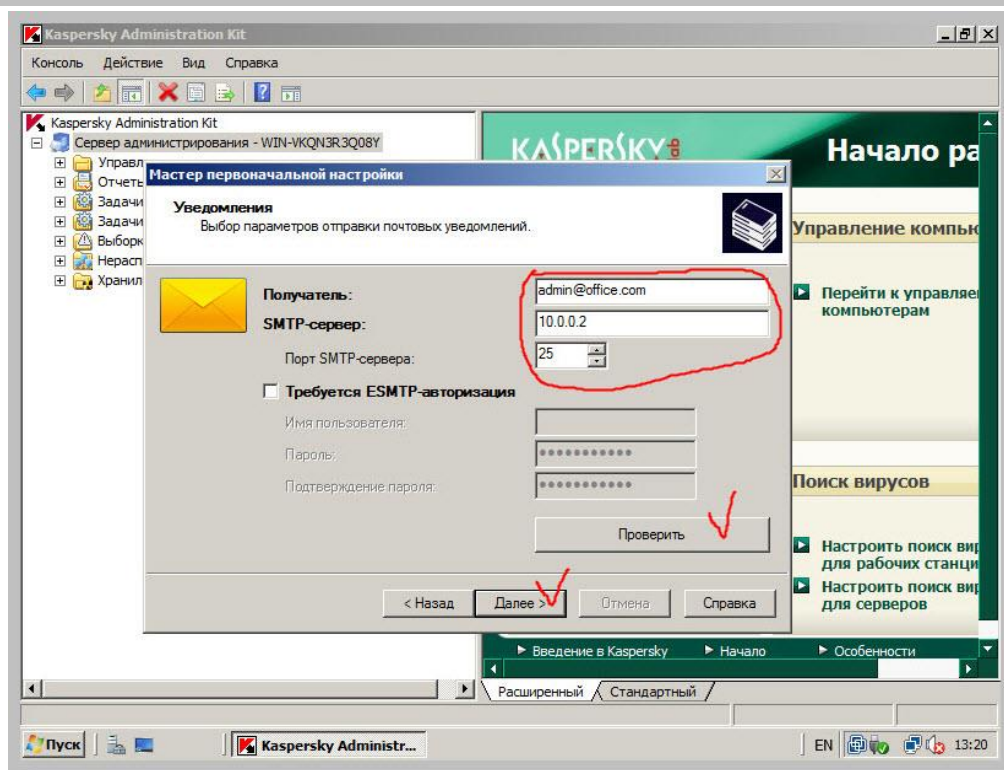
До рези в глазах знакомая нам кнопка «Далее» ☺ Нажимаем ее.



В окне выше нас просят указать код активации или указать файл ключа для КЛИЕНТСКИХ компьютеров. Сам «Kaspersky Administration Kit» распространяется бесплатно, так что если у Вас есть лицензионный ключ на определенное количество рабочих станций – можете добавить его сюда. Если же нет, как видите, CS Adminkit не настаивает и любезно предлагает пункт «Добавить лицензию позже» ☺

Нажимаем кнопку «Далее».

В следующем окне мы можем указать адреса электронной почты и самого почтового сервера.



Зачем это нужно? При условии наличия в сети сервера почты и рабочего e-mail адреса (адрес на скриншоте я указал просто как пример) мы можем оперативно получать исчерпывающую информацию о критических событиях (заражение клиента вирусом, повреждение антивирусных сигнатур, проблемы лицензии и т.д.) на почту.

Вот как это выглядит на рабочей системе в нашей локальной сети организации.

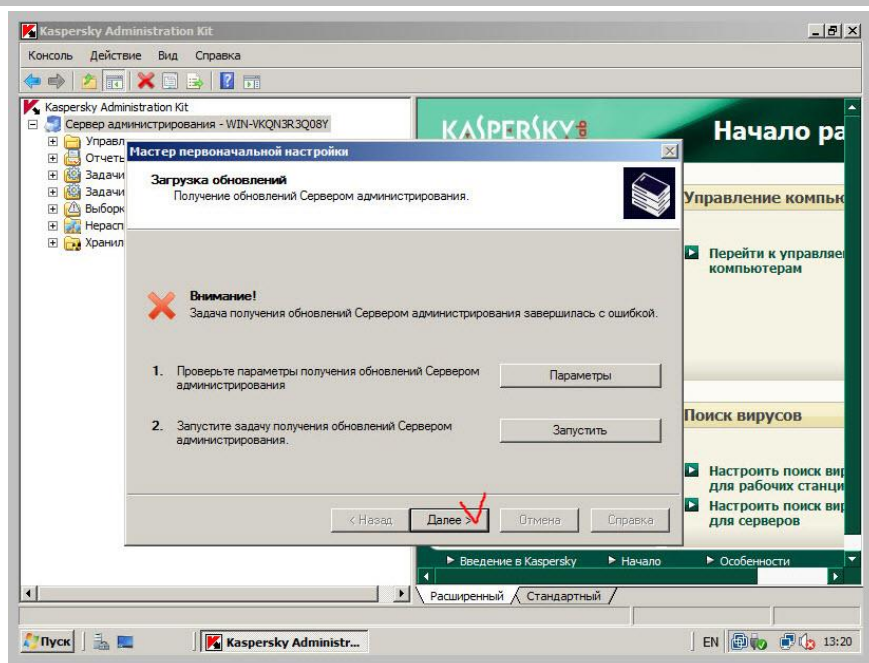
От: [REDACTED]@ [REDACTED] Кому: [REDACTED]@ [REDACTED]
Тема: Kaspersky AdminKit

Событие Обнаружение вирусов, червей, троянских и хакерских программ произошло на компьютере SUPPLY09 в домене [REDACTED] в 22 марта 2013 г. 16:07:54 (GMT+02:00)
Файл E:\програми.exe, обнаружено: вирус 'Worm.Win32.AutoRun.hrm'. Пользователь: [REDACTED]\luciv, компьютер:localhost.

Как Вы понимаете, из соображений корпоративной этики я замалевал реальные адреса и название домена на скриншоте выше. С помощью такой своевременной системы оповещения мы практически в режиме реального времени будем «видеть», что (с точки зрения вирусной безопасности) происходит в нашей сети? Какие именно вирусы выявляются системой безопасности и какие действия предпринимаются? Если происходит сетевая атака (скажем, вируса-червя по типу знаменитого «kido»), то - с какого именно IP адреса? В каком состоянии находятся антивирусные базы на клиентских компьютерах сети (актуальны ли они)? И много чего еще.

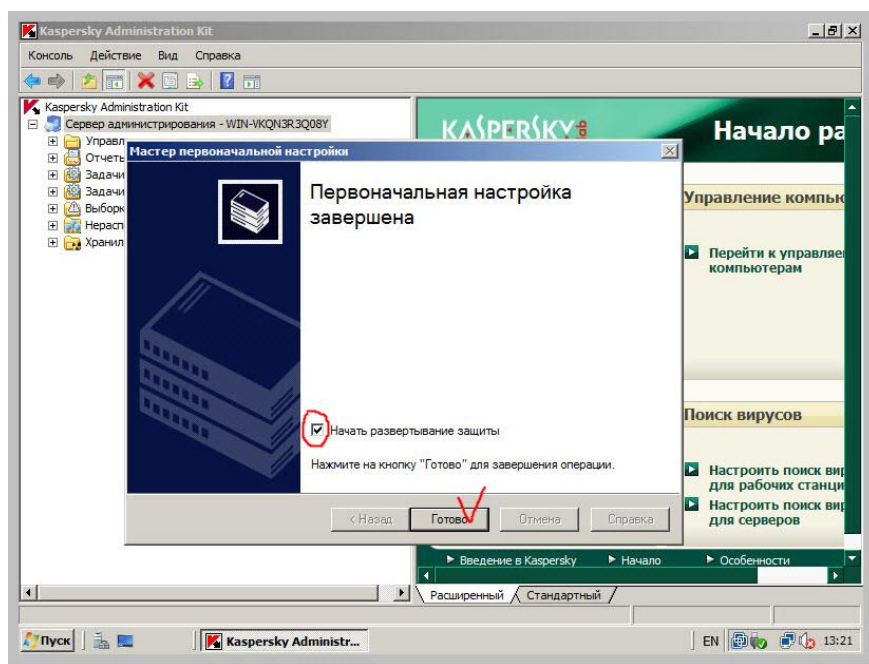
Да что я Вас уговариваю!? Поставите, настроите и сами все увидите! ☺

При переходе к следующему окну нам сообщат, что задача получения обновлений антивирусных баз сервером администрирования завершилась с ошибкой.



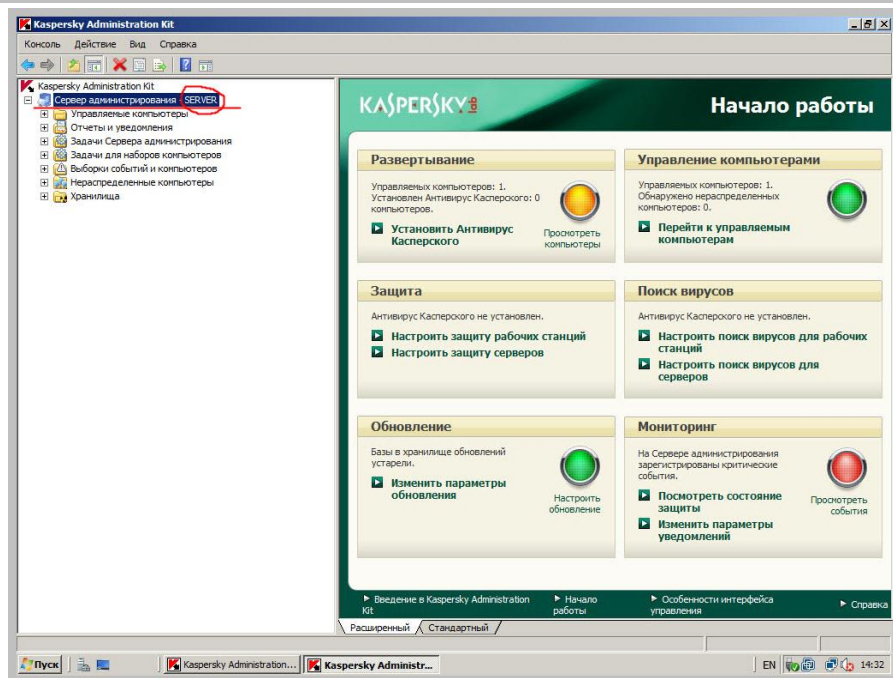
Это – не страшно, поскольку получение обновлений мы скоро настроим сами и все будет в порядке! ☺

На следующем скриншоте ставим галочку возле надписи «Начать развертывание защиты» и нажимаем кнопку «Готово».



После этого мы (наконец-то) вырвемся из под «родительской» опеки бесконечной вереницы «мастеров» (нянек) и нам предоставят возможность начать делать что-то самостоятельно! Первые шаги, так сказать ☺

Вот она – консоль управления Admin Kit полностью в нашем распоряжении!



Имя сервера, как видите, я уже поменял ☺

В левой части оснастки у нас находится древовидная структура управления всей антивирусной защитой. В правой – параметры и настройки того конкретного пункта, который отмечен слева.

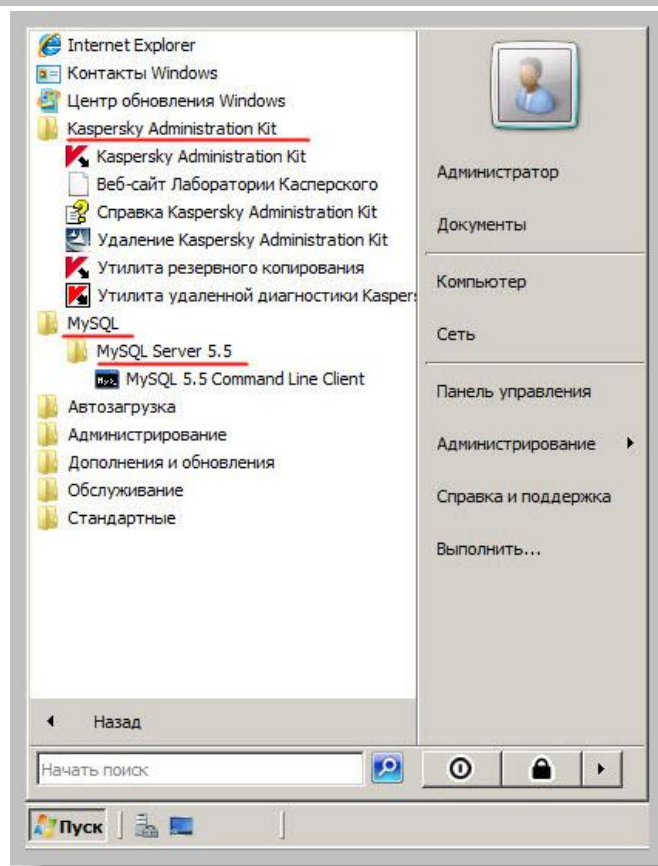
Нажимая на значок «+» (в левой колонке) мы можем раскрыть дополнительные подпункты любого из семи разделов:

- Управляемые компьютеры
- Отчеты и уведомления
- Задачи Сервера администрирования
- Задачи для наборов компьютеров
- Выборки событий и компьютеров
- Нераспределенные компьютеры
- Хранилища

Раскройте весь список и ознакомьтесь с ним!

Предлагаю сейчас открыть (через кнопку «Пуск») весь список установленных программ и посмотреть, что же мы имеем на нашем сервере на данный момент?

Посмотрите на фото ниже:



У нас установлен MySQL Server версии 5.5 и Kaspersky Administration Kit с набором дополнительных утилит и справкой на русском языке. Ознакомьтесь, при случае.

Утилита резервного копирования, к примеру, – очень полезна в том случае, если Вы захотите сделать полный бэкап (резервную копию) клиентской базы компьютеров, базы данных MySQL и настроек самого сервера администрирования.

Зачем это может понадобиться? А вдруг Вы задумаете «переезд» на новый сервер или что-то случится со старым и придется заново устанавливать на нем систему? Вот тут очень пригодится утилита резервного копирования!

Итак, что мы имеем на данном этапе?

1. Установленный сервер баз данных MySQL
2. Установленный и связанный с ним сервер антивирусной защиты Admin Kit

Теперь нам нужно где-то «взять» клиентские компьютеры и установить на них антивирус, который будет самостоятельно обновляться с сервера администрирования и передавать ему всю необходимую информацию для управления антивирусной защитой нашей сети.

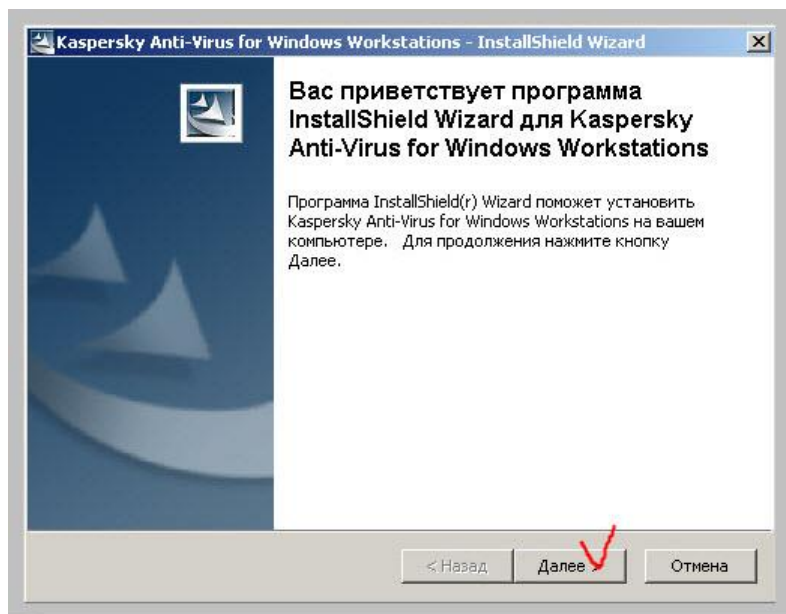
Нет ничего проще! ☺ Создаем еще одну виртуальную машину с Windows XP (мы делали это в одном из прошлых уроков, поэтому я просто скопировал ее оттуда), присваиваем ей IP адрес из того же диапазона, что и наш сервер, проверяем с помощью

команды «ping» (тоже - разбирали) наличие сетевого соединения между сервером и клиентом.

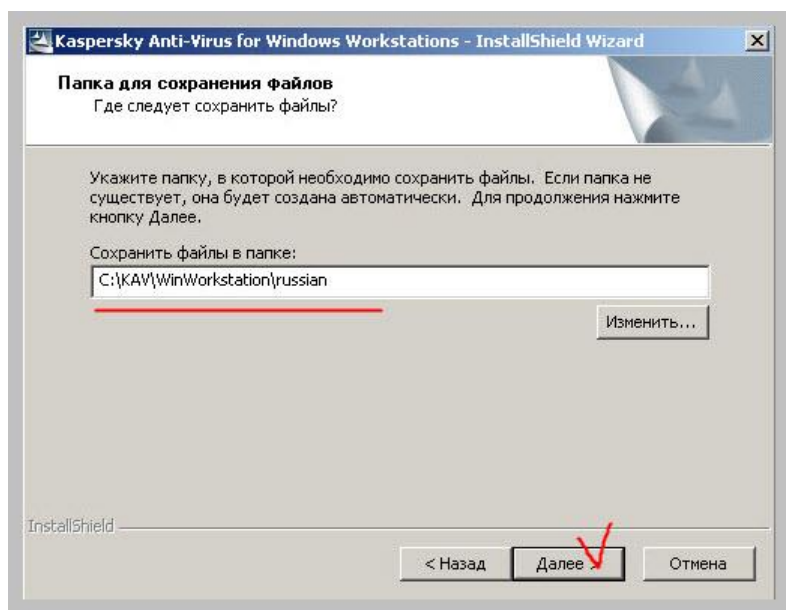
В моем случае адрес сервера: 10.0.0.1 маска подсети 255.0.0.0 и рабочая группа «office». У первого клиентского компьютера: 10.0.0.2 маска 255.0.0.0 и рабочая группа «office».

Теперь установим на компьютер с Windows XP антивирус Касперского для Windows Workstation который мы также загрузили с официального сайта.

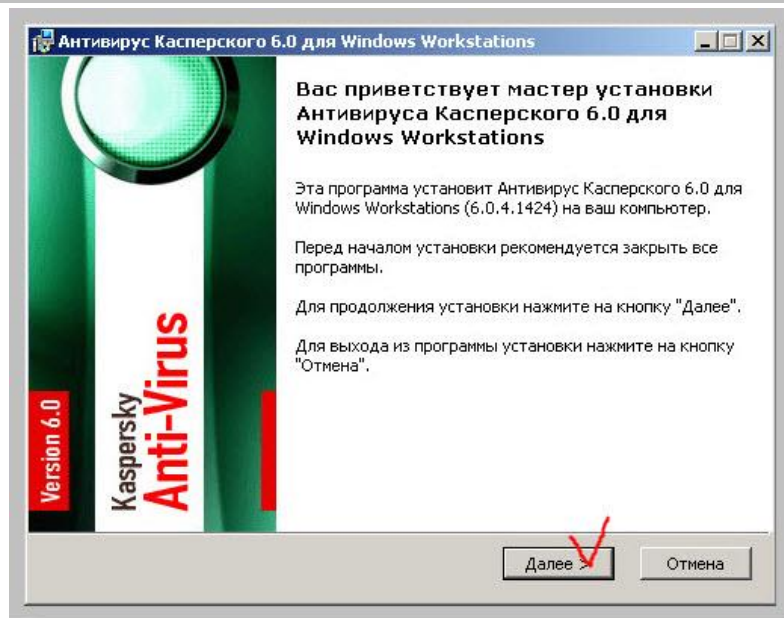
Запускаем его установщик:



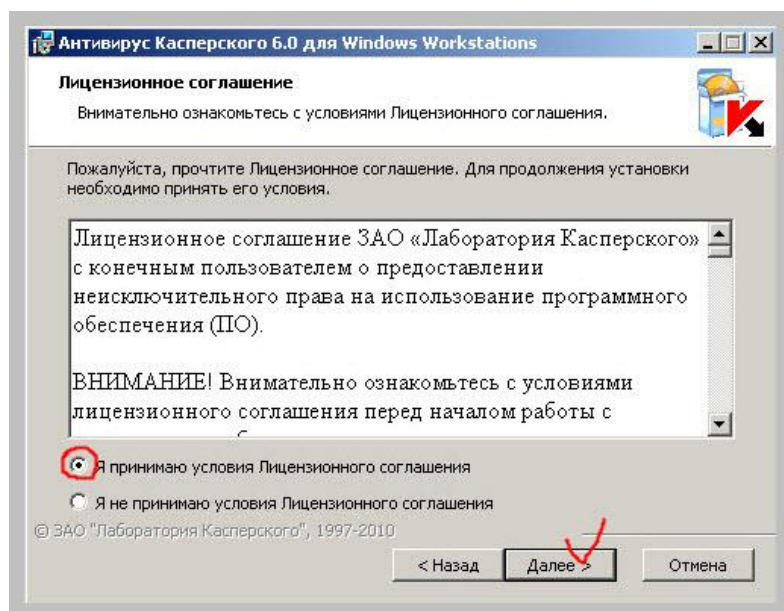
Нажимаем кнопку «Далее».



Соглашаемся с тем, куда программа предлагает нам распаковывать свои компоненты и нажимаем «Далее».

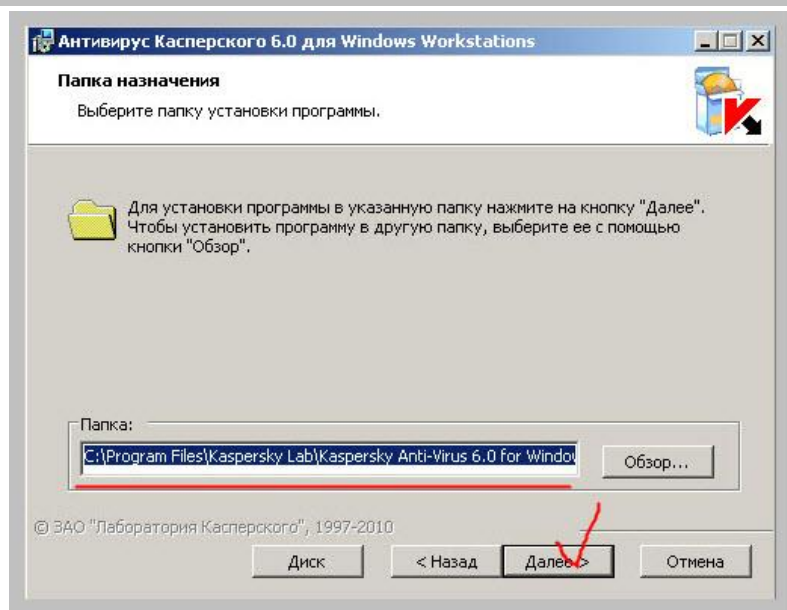


Видим окно мастера установки.

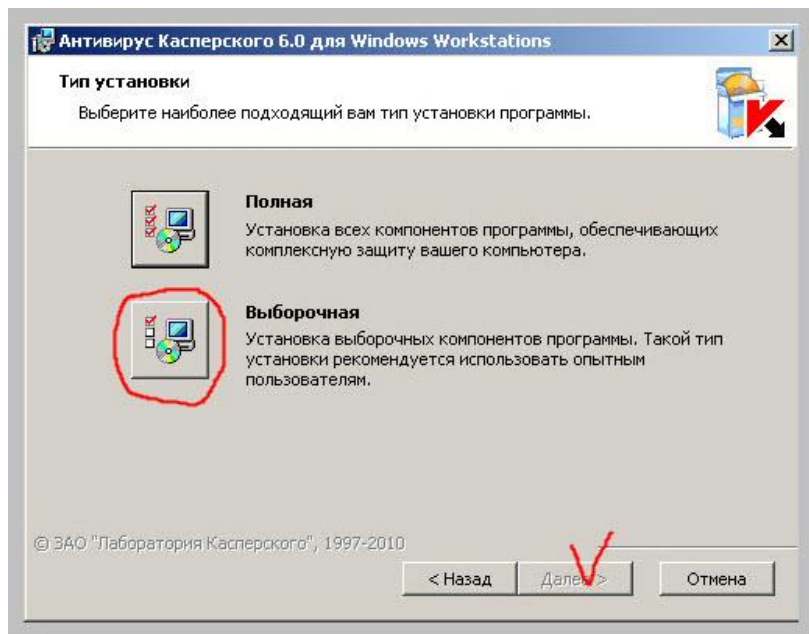


Принимаем и продолжаем !

Я бы не рекомендовал изменять папку установки антивируса:

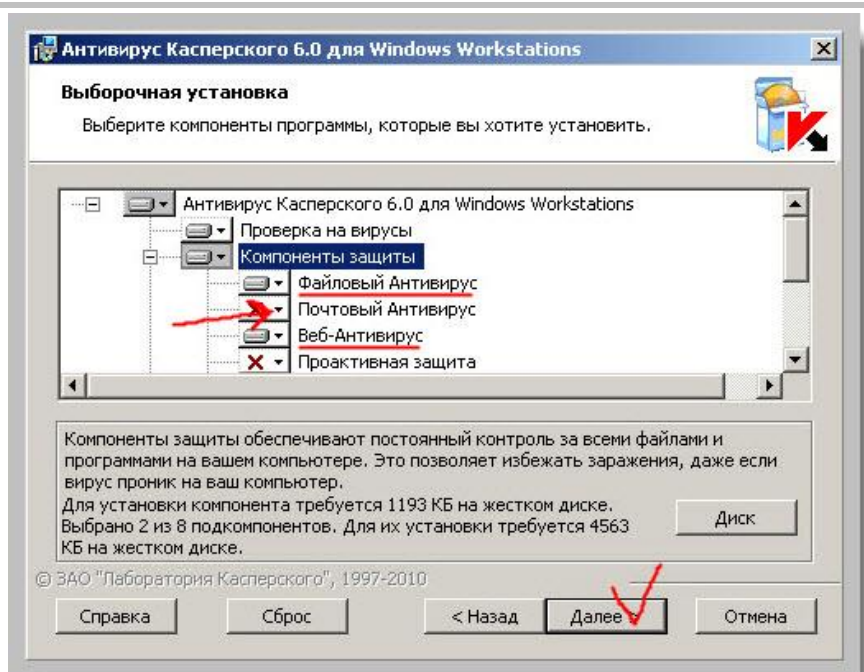


Нажимаем «Далее»:



Вот тут предлагаю притормозить и нажать кнопку «выборочная» установка компонентов. Сейчас я расскажу Вам почему я так советую сделать.

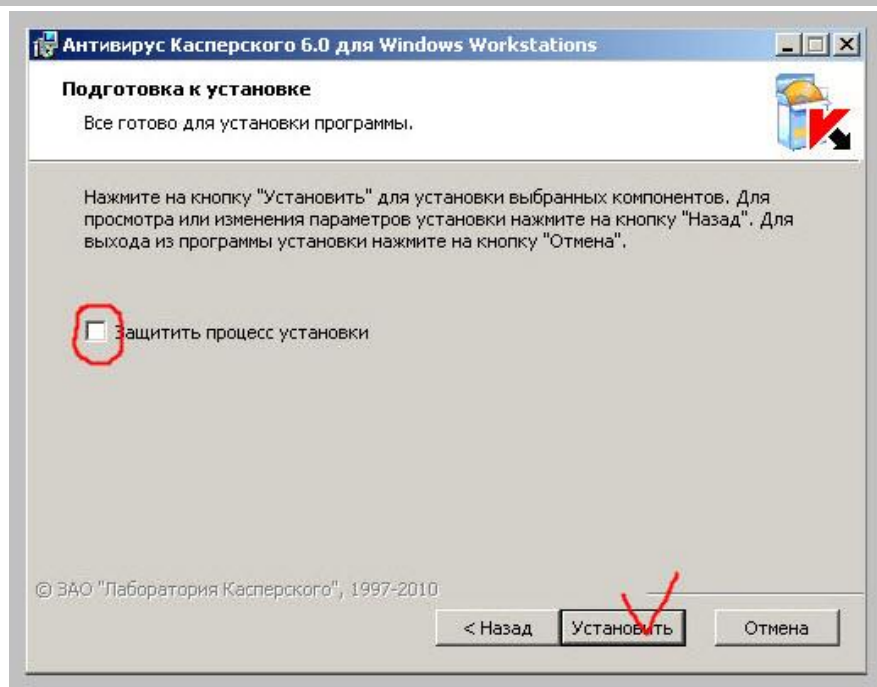
После нажатия на пункт «выборочная» у нас появится окно, как на фото ниже:



Давайте с ним разберемся! Здесь нам предоставляется возможность выбрать те компоненты защиты, которые будут установлены и задействованы на клиентской части антивируса. Нажав возле нужного компонента на треугольник, обозначенный стрелкой, мы можем вызвать меню и выбрать в нем пункт «отключить». После этого возле компонента появится красный крестик и данный компонент не будет установлен в процессе инсталляции. На работе мы устанавливаем только два компонента (оба они подчеркнуты на фото выше).

Как вариант, можно еще задействовать компонент «Антихакер». Тогда наш антивирус обзаведется еще и сетевым экраном (файрволом). Все остальное можете отключить. Особенно это касается компонента «Проактивная защита». Это – модуль эвристического анализа с такими параноидальными наклонностями, который будет «кричать: **Вирусы!**» по любому поводу и даже без него ☺

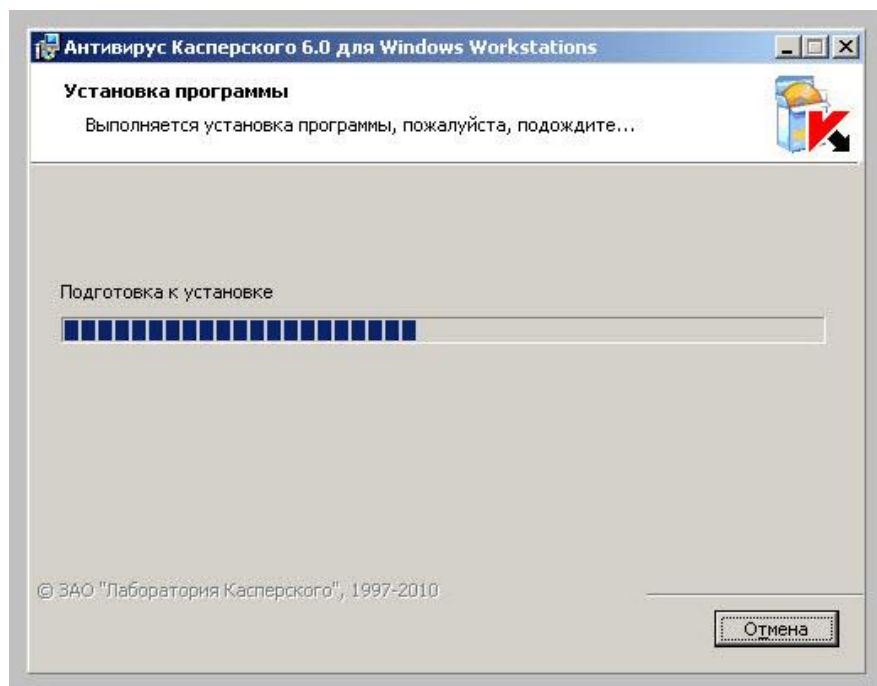
Не забываем читать, что написано в самих окнах мастера установки – пригодится!
Двигаемся дальше.



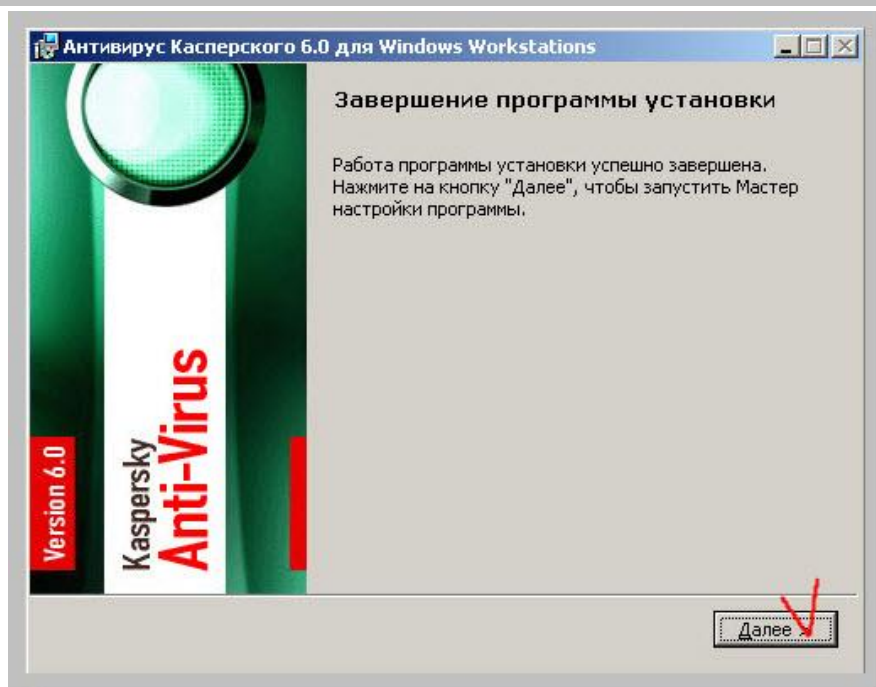
В окне выше нам предложат защитить процесс установки. Можете поставить эту галочку (в том случае, если у Вас есть некоторые сомнения относительно того, что на компьютере, на который мы устанавливаем антивирус, могут быть вирусы). Тогда Касперский обезопасит свою установку, исключив возможность блокирования себя какой-то посторонней программой или процессом.

После этого нажимаем кнопку «Установить».

Начнется установка антивируса.

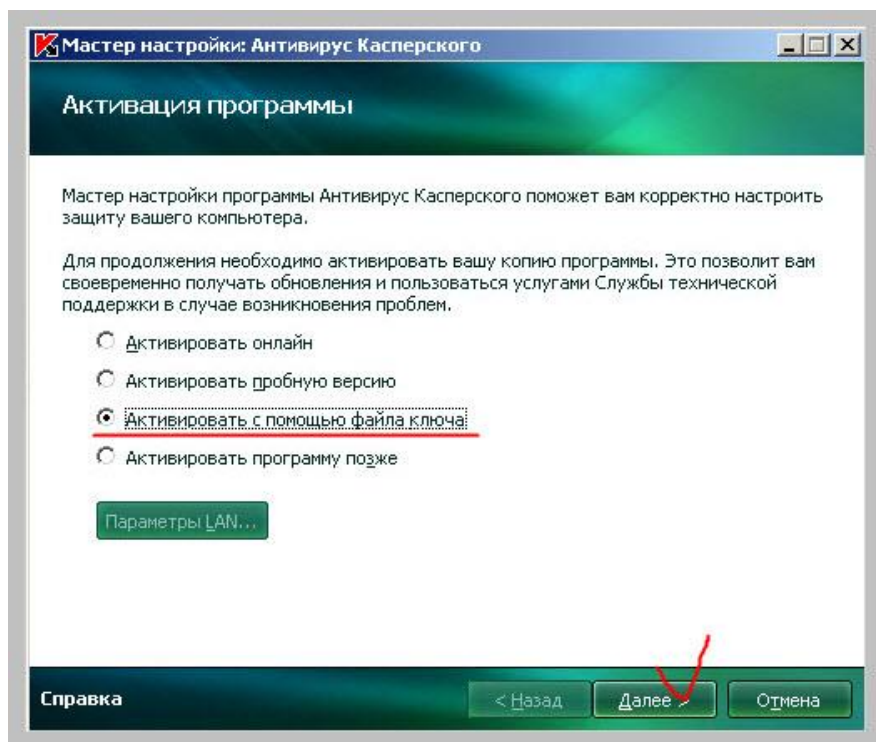


После ее завершения мы увидим вот такое окно:



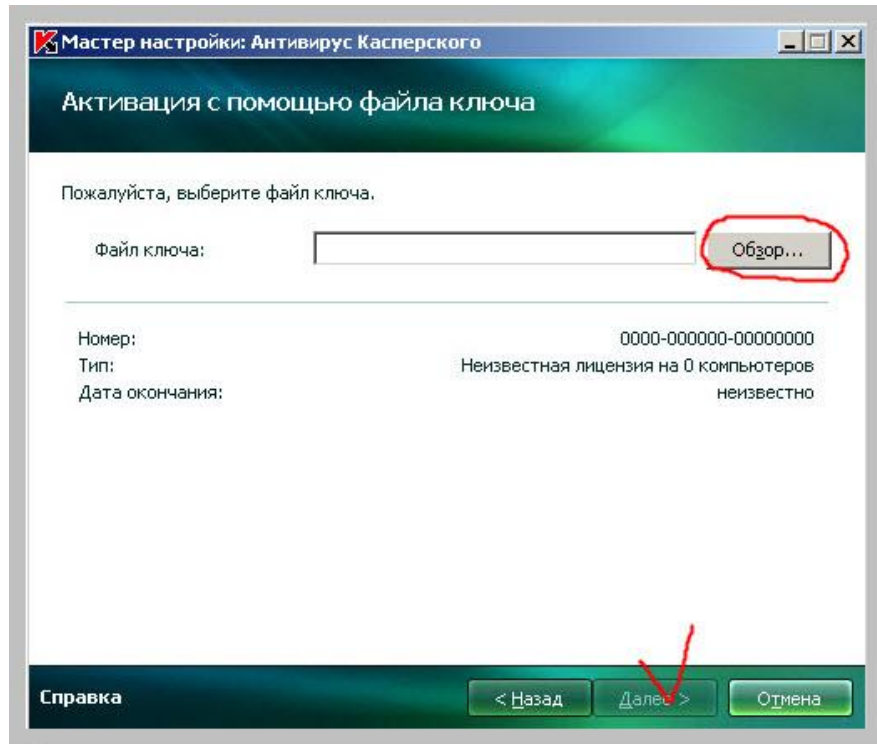
После чего нам будет предложено запустить мастер первоначальной настройки программы. Поскольку возможности отказаться нас все равно лишили, то нажимаем кнопку «Далее» ☺

Немного «подумав» программа покажет нам вот такое окно:



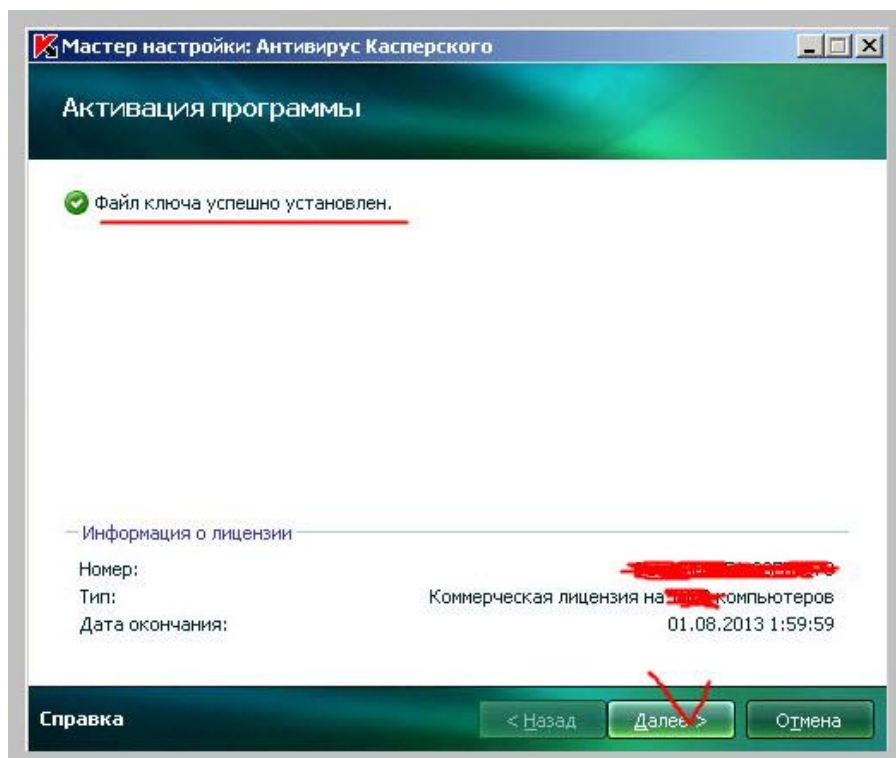
Если у Вас есть лицензионный ключ или регистрационная информация в любом другом виде, то выберите один из вариантов, которые Вам подходят (свой вариант я подчеркнул). В крайнем случае можете выбрать пункт «Активировать программу позже».

Окно, которое показано на фото ниже, появится только в том случае если Вы (как и я в примере) выберете «Активировать с помощью ключа».



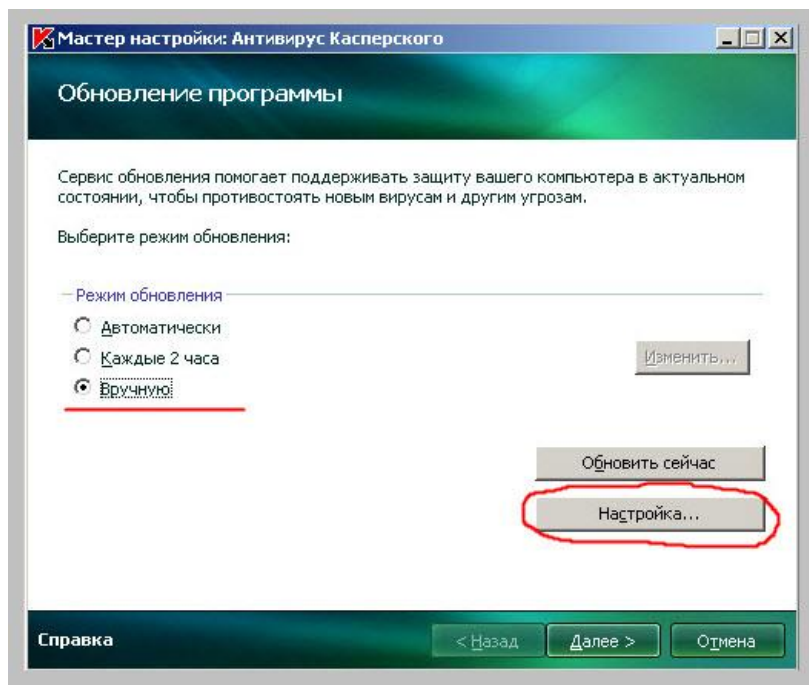
Нажимаем кнопку «Обзор» и в окне проводника Windows, которое появится, выбираем файл ключа регистрации. После этого кнопка «Далее» станет активной и мы сможем нажать на нее.

Если все прошло удачно, то мы увидим вот такое окно с надписью «Файл ключа успешно установлен».



Внизу окна отображается информация о типе лицензии, количестве компьютеров на которые она распространяется (один ключ может использоваться на нескольких сотнях или даже тысячах компьютеров), также указана дата окончания лицензии.

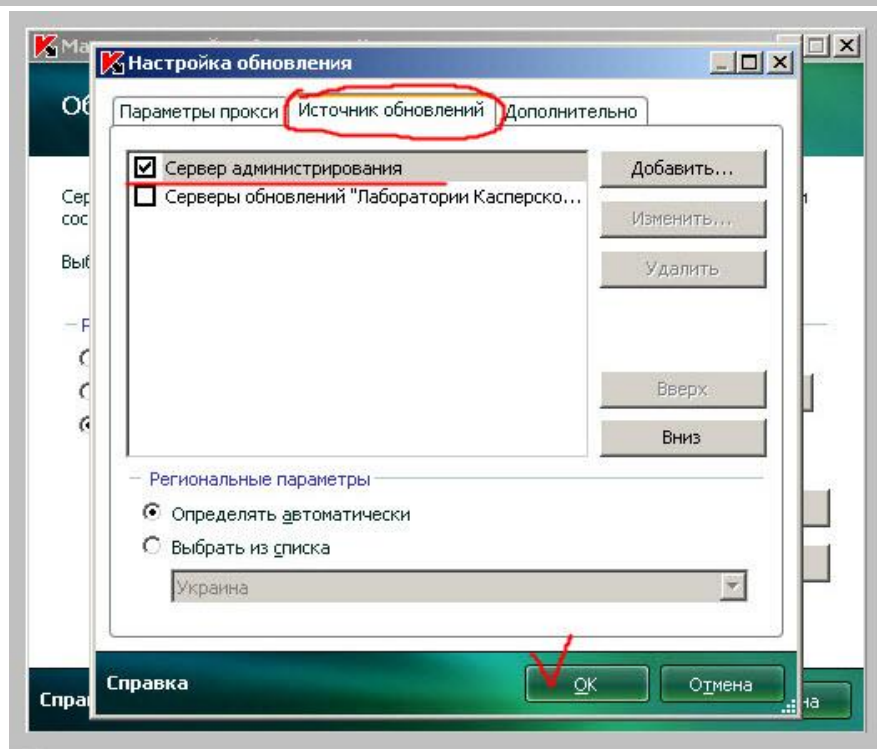
После нажатия на кнопку «Далее» нам предложат выбрать режим обновления антивирусных баз приложения.



Рекомендую Вам сделать именно так, как показано на скриншоте выше: «Вручную». Почему именно так? Дело в том, что режим «Автоматически» (предлагаемый по умолчанию) может стать для нас «подводным камнем». Смотрите, если мы создадим впоследствии групповую задачу обновления для всех компьютеров нашей сети (я покажу, как это делается), то этот режим «Автоматически» будет срабатывать независимо от групповой задачи и дополнительно запускать обновление на клиенте. А зачем нам такое дублирование?!

Итак, выставляем «Вручную» и нажимаем кнопку «Настройка».

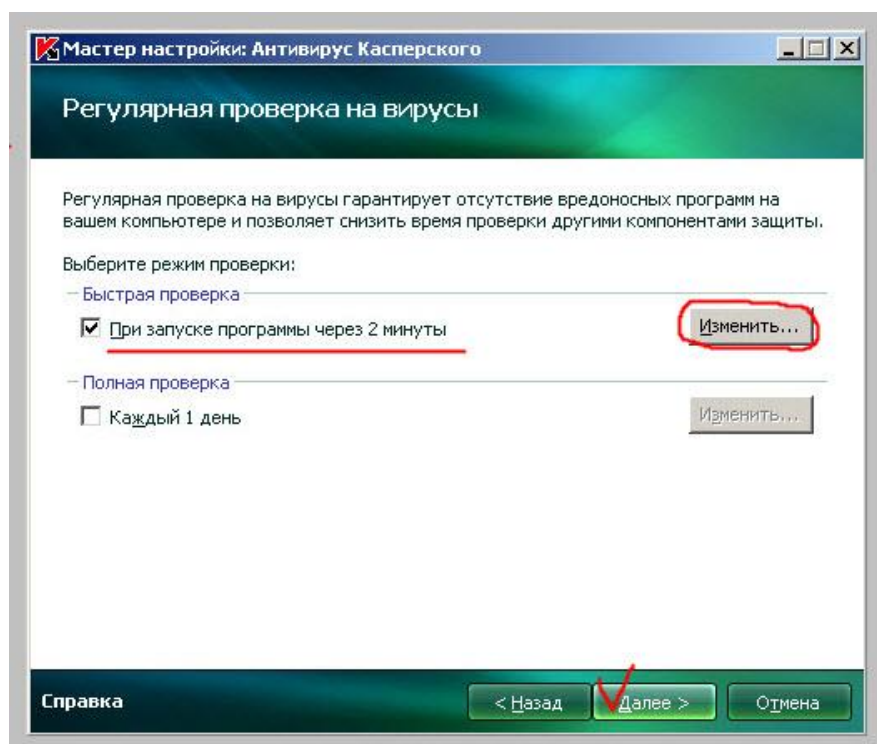
В следующем окне, которое появится, переходим на вкладку «Источник обновлений»



Здесь выставляем все так, как показано на скриншоте выше. В случае необходимости используем кнопки «Вверх» и «Вниз», для того чтобы выставить «Сервер администрирования» первым в списке серверов обновления для наших рабочих станций. Галочку ставим только одну – возле него же!

Нажимаем кнопку «ОК».

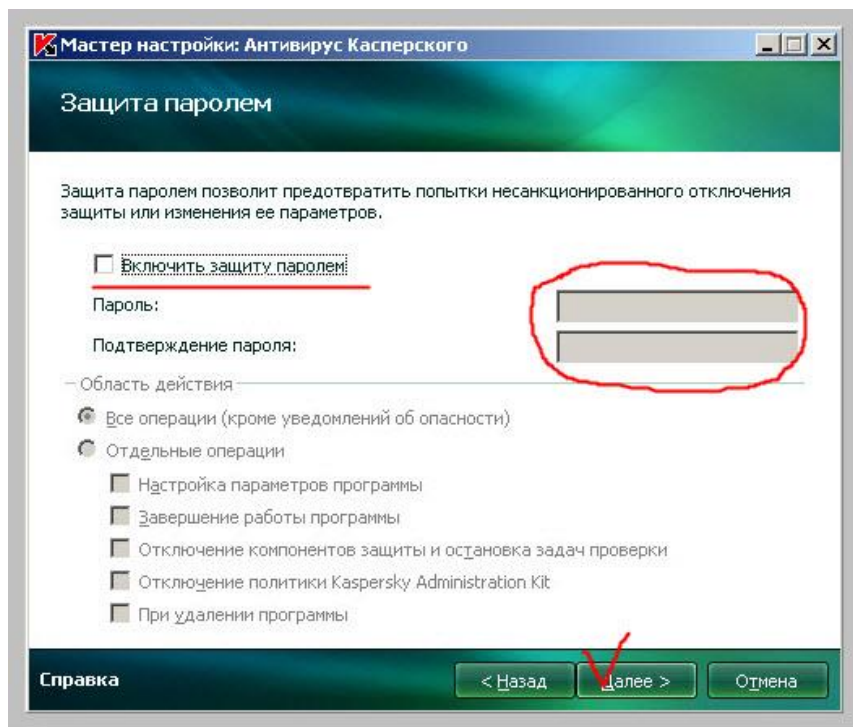
На фото ниже нам предложат изменить (или оставить как есть) временной интервал после запуска компьютера, после которого на клиенте автоматически запустится быстрая проверка критически важных для работы системы областей и файлов.



Как видим, по умолчанию стоит значение: 2 минуты. Если хотите, можете изменить его, нажав на одноименную кнопку.

Двигаемся дальше:

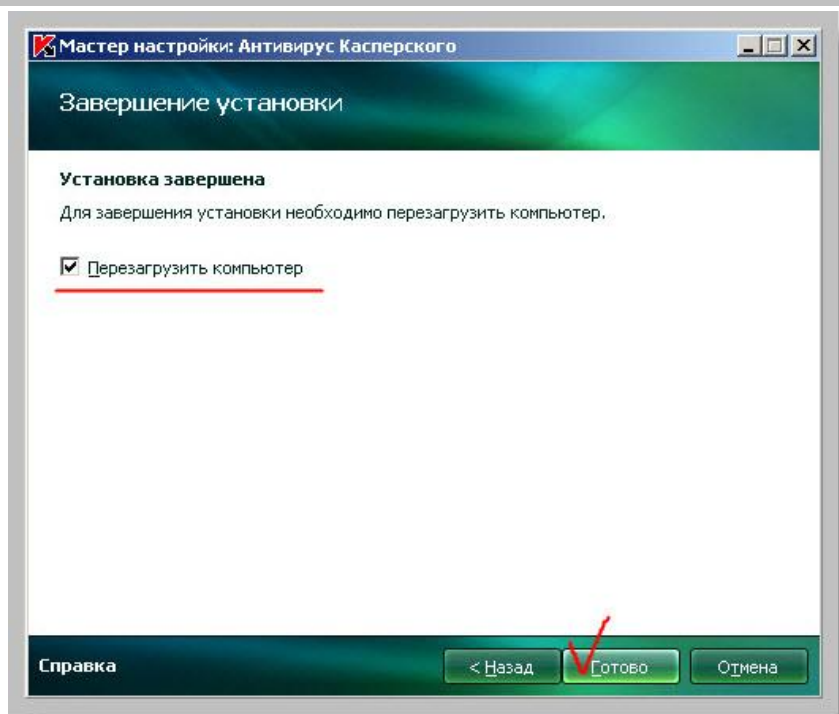
Нам предложат возможность защиты конфигурации программы паролем.



Зачем это может понадобиться? Представьте: мы установили антивирус на машине пользователя, настроили его, все так красиво сделали. А пользователь (когда мы ушли) взял и поменял в нем какие-то настройки или – вообще его выключил! Думаю, нам, как администраторам, такой вариант развития событий не понравится? ☺

Вот для предотвращения несанкционированного изменения настроек программы, отключения ее отдельных функций или даже полной деинсталляции, и предусмотрен вариант защиты паролем. НО! Не спешите задействовать эту функцию! Дальше я покажу Вам, как сделать это с помощью групповой политики через сервер администрирования: настроить нужно только один раз, а применится эффект сразу ко всем компьютерам сети!

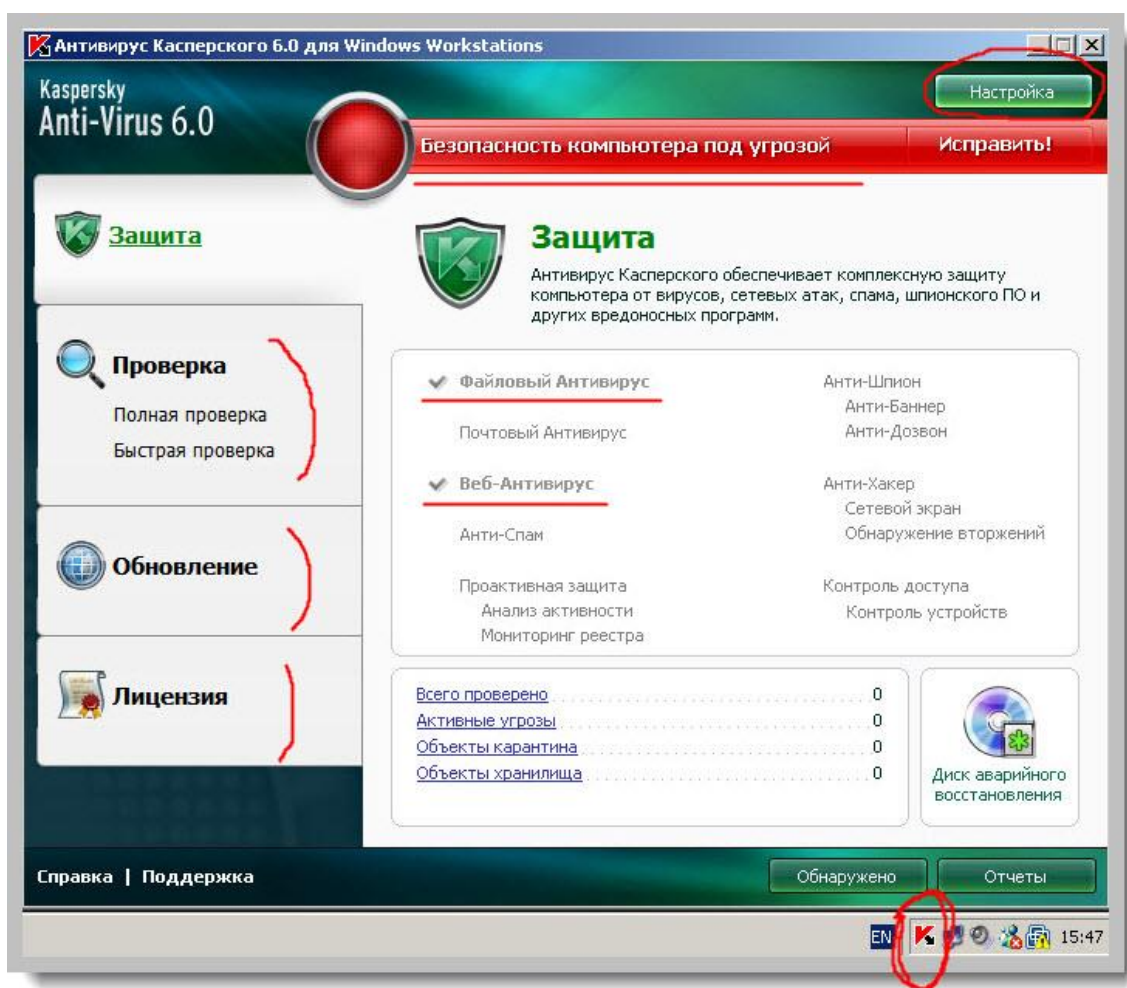
Так что, просто нажимаем «Далее» и видим следующее окно (крепитесь, уже почти закончили) ☺



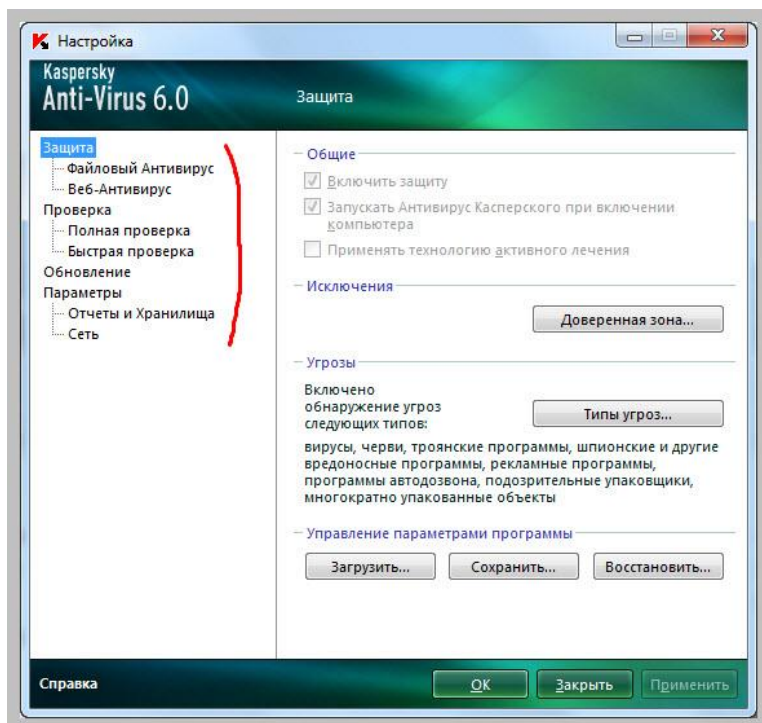
Ставим галочку «Перезагрузить компьютер» и нажимаем кнопку «Готово».

После перезагрузки запустим главное окно нашего антивируса на клиенте, щелкнув два раза левой кнопкой мыши на его иконке в трее.

Специально сделал большой скриншот, чтобы Вы могли все хорошо рассмотреть.



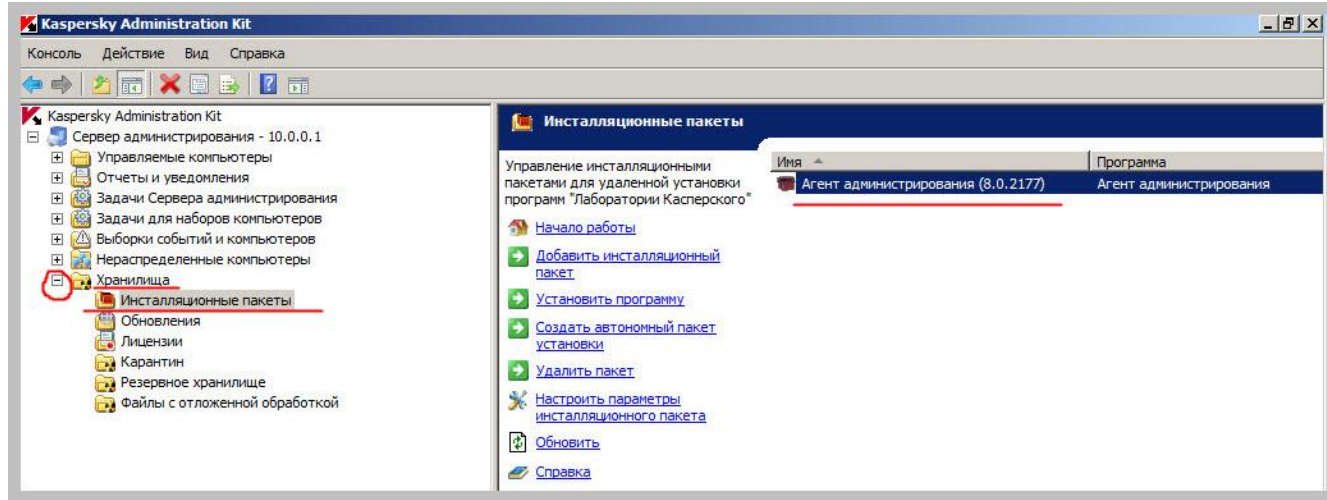
Структура окна – стандартная: в левой части представлены основные функции и возможности программы, а в правой – их детализация. Галочками отмечены установленные компоненты программы (помните, мы выбирали их из списка компонентов для установки?) Справа верху расположена кнопка «Настройки», нажав на которую, можно попасть в отдельное окно со всеми настройками антивируса:



Так, с клиентским компьютером мы разобрались: установили на него «Антивирус Касперского для Windows Workstation» **НО!** Для эффективного автоматического обновления клиентских компьютеров на каждом из них должен быть установлен еще один компонент: «Kaspersky Net Agent». Именно через него и происходит все сетевое взаимодействие между клиентским антивирусом и сервером.

Теперь займемся самым интересным! Я покажу Вам, как удаленно (по сети) установить Net Agent-ы на рабочие станции пользователей! Фактически, мы будем управлять «клиентом» с сервера администрирования (компьютера под управлением Windows Serve 2008 с установленным на нем Kaspersky Administration Kit).

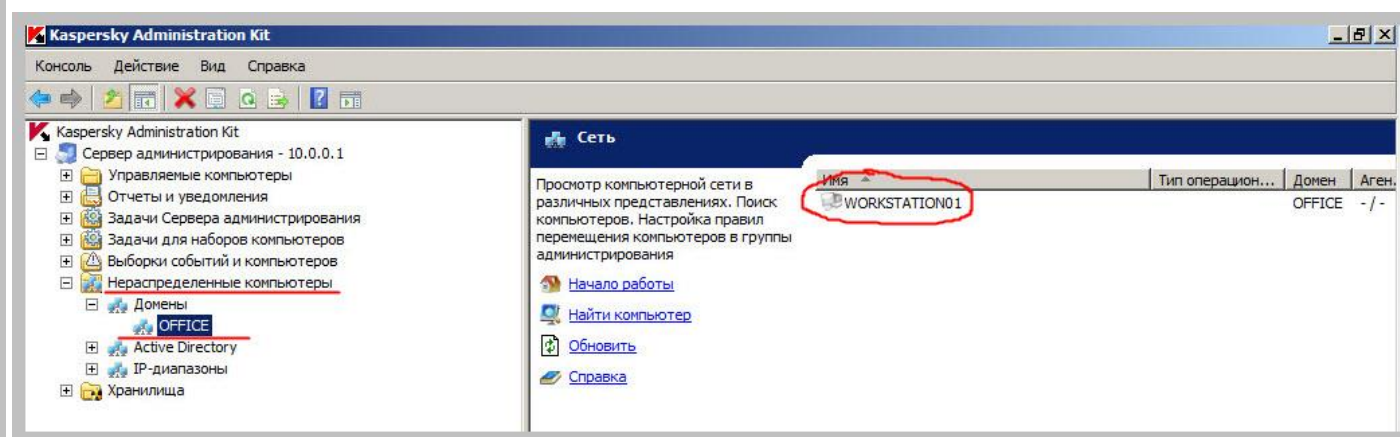
Зайдем в консоль управления Admin Kit-ом и перейдем в раздел «Хранилища», «Инсталляционные пакеты»:



Здесь хранятся установочные пакеты программ, готовых для распространения (установки) по сети. В правой части окна мы увидим инсталляционный пакет «Агент администрирования» (версия 8.0.2177). При желании и по мере необходимости, мы можем сами создавать здесь свои дистрибутивы программных продуктов с целью их последующей установки на управляемые компьютеры. Так, к примеру, можно удаленно поставить и сам антивирус!

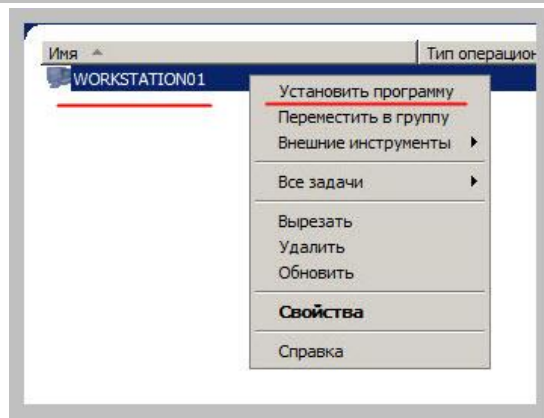
Итак, **ЧТО** мы будем устанавливать мы увидели, теперь давайте посмотрим, **КУДА** будем проводить инсталляцию.

В консоли сервера переходим в раздел «Нераспределенные компьютеры». Раскроем его «дерево» и найдем там свою рабочую группу или домен. Домена у нас в примере нет, а рабочая группа называется (если помните) «office». В нее и заходим!

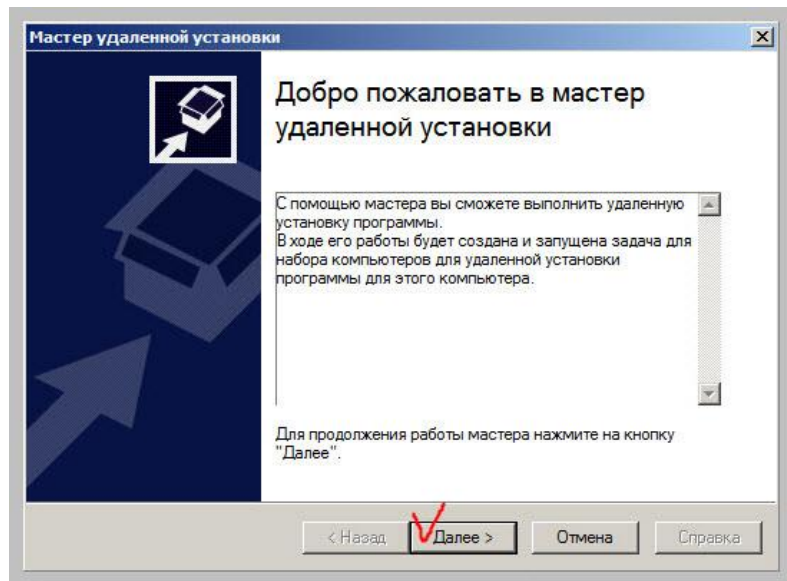


Если мы до этого все делали правильно, то в правой части окна мы должны увидеть наш клиентский компьютер (в нашем случае это ПК с сетевым именем Workstation01).

Нажимаем на нем правой кнопкой мыши и из раскрывшегося меню выбираем пункт: «Установить программу»:

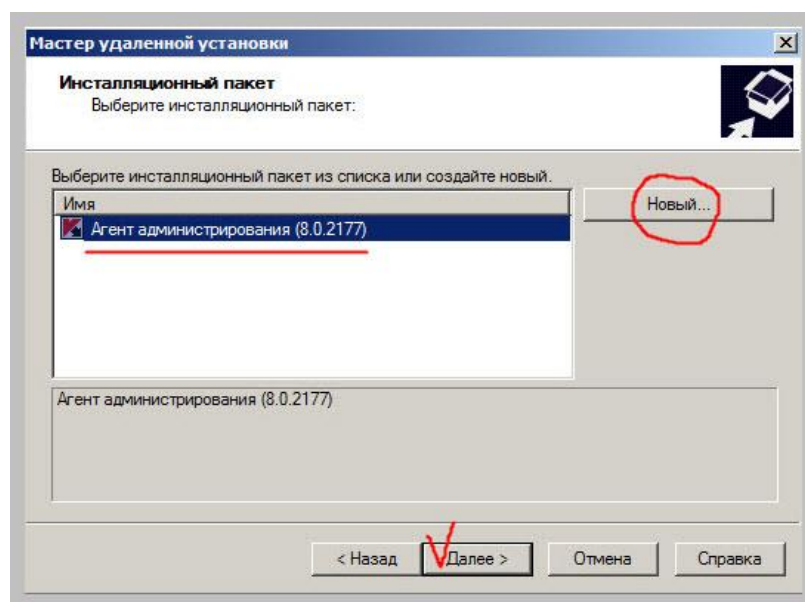


После этого у нас запустится очередной мастер: «Мастер удаленной установки»



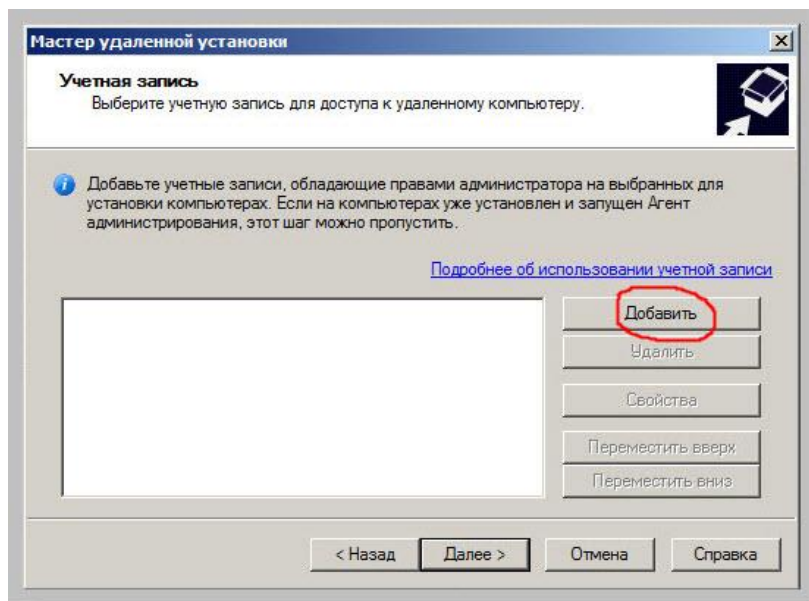
Нажимаем кнопку «Далее»

В белой области слева у нас будет список пакетов, готовых для распространения по сети.



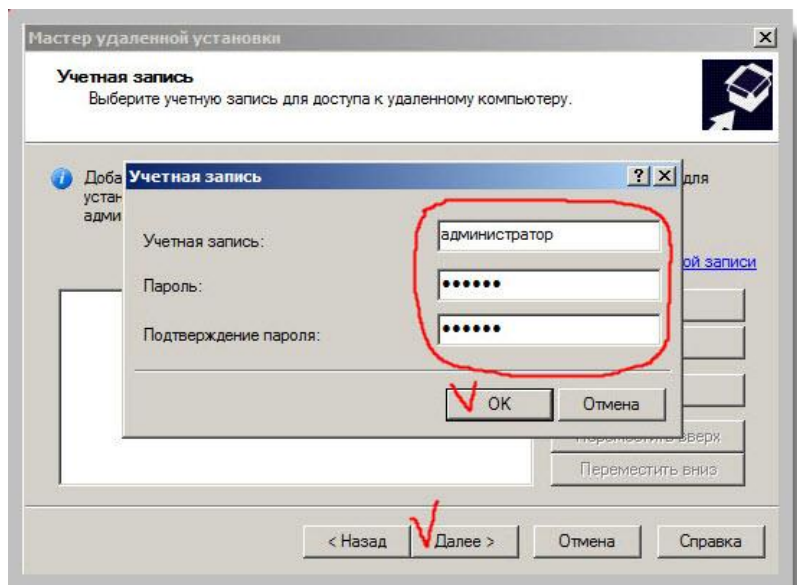
Сейчас, как видите, у нас здесь только один «Агент администрирования», но нам пока этого вполне достаточно! Если же захотите добавить сюда свои пакеты, то просто нажмите кнопку «Новый».

Выделяем нужный и нажимаем кнопку «Далее».



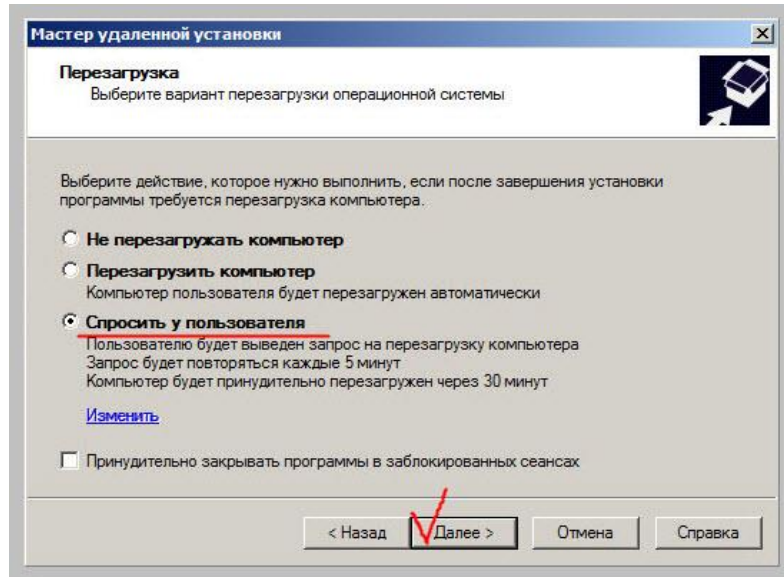
Смотрим на фото выше и внимательно читаем, что написано на самом скриншоте! Нам нужно указать здесь логин и пароль того пользователя, который имеет привилегии администратора на удаленном компьютере. Это – логично. Программе ведь нужно установиться, а из под учетной записи пользователя с ограниченными правами она этого сделать не сможет, поэтому и просит нас заранее указать логин и пароль администратора для установки.

Нажимаем кнопку «Добавить», появится вот такое окошко:



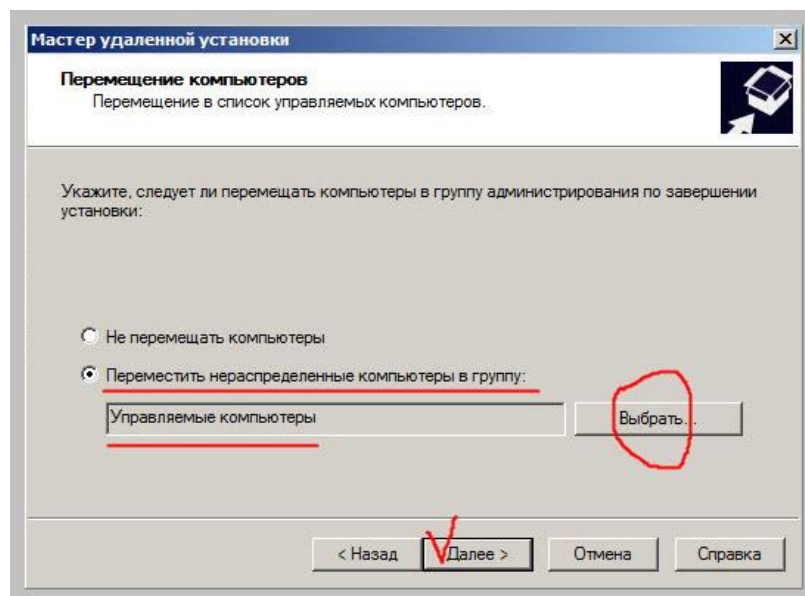
В нем нам нужно указать имя и пароль пользователя, который является администратором на удаленном компьютере. При наличии доменной структуры можете указать здесь сразу логин и пароль администратора домена.

В следующем окне мы можем выбрать нужное нам действие, если после установки приложения потребуется перезагрузить компьютер пользователя.



Реальный выбор здесь возможен между вторым и третьим вариантом. Если Вы – настоящий суровый админ, то выбор – очевиден: принудительная перезагрузка! ☺ Третий вариант – более человечен (по отношению к пользователю) и позволит ему спокойно закончить свою текущую работу.

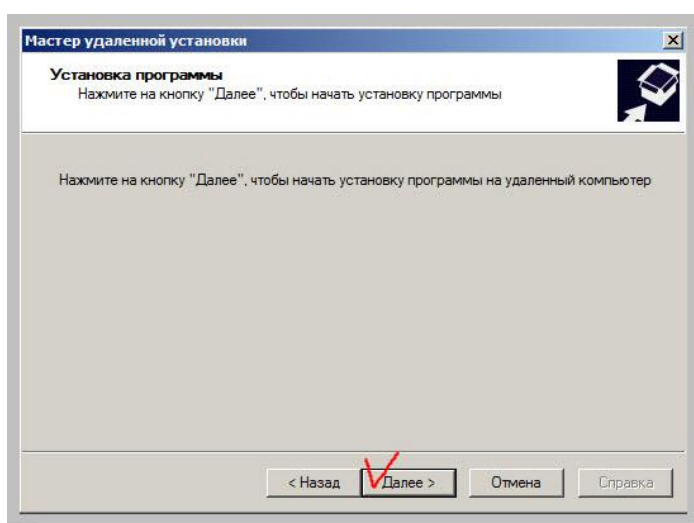
Нажимаем «Далее» и переходим к следующему окну:



Здесь нам нужно выбрать пункт «Переместить нераспределенные компьютеры в группу» и выбрать группу. По умолчанию выбрана группа «Управляемые компьютеры».

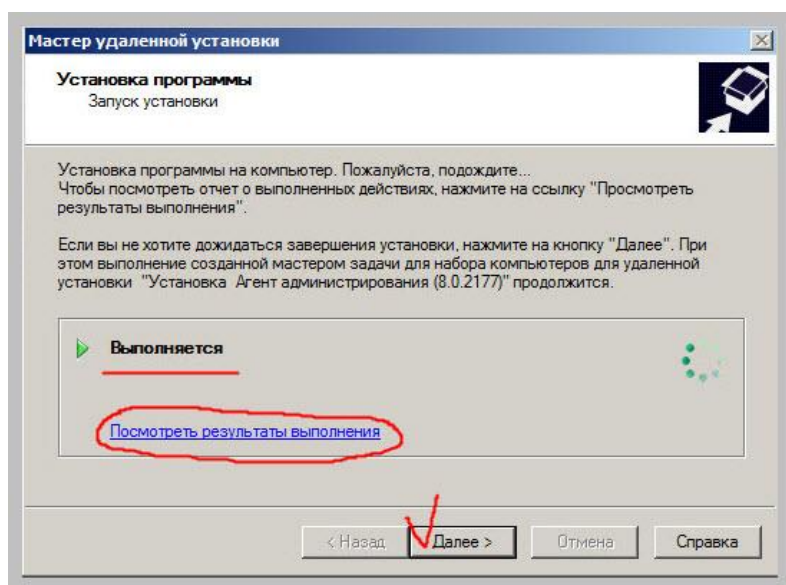
У нас, к примеру, в организации с 350-ю компьютерами есть только одна группа. Возможно это – не правильно? Не знаю. Можете создать их несколько на свое усмотрение. Главное, запомните следующее: пока компьютер не причислен (перемещен) к какой-либо группе, групповые политики и задачи сервера Kaspersky Administration Kit на него не распространяются! Поэтому, в обязательном порядке, если видите компьютеры со статусом «нераспределенный» - вручную перемещайте его в какую-то группу. Именно по этой причине при установке Агента администрирования предусмотрена такая возможность.

Нажимаем «Далее» и переходим к следующему окну сомнительной ценности и информативности ☺



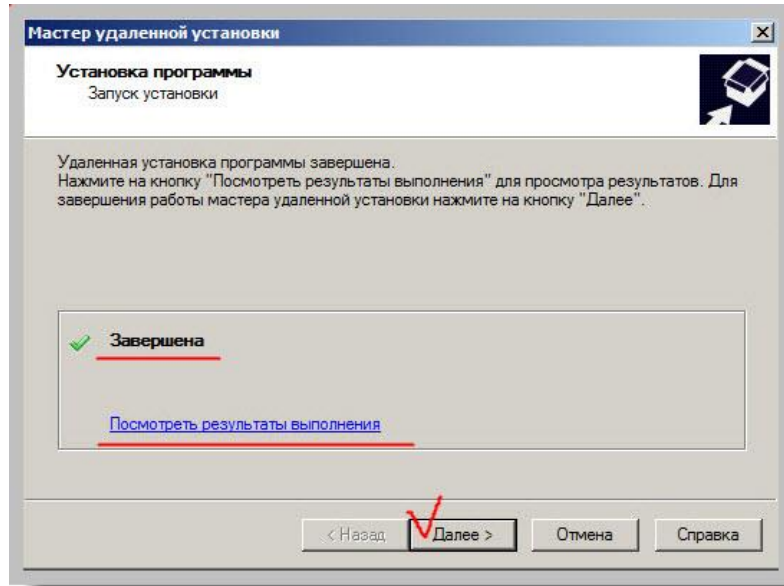
«Далее»

Вот тут уже – интереснее! Мы можем наблюдать за ходом процесса установки нашего приложения на удаленный компьютер!

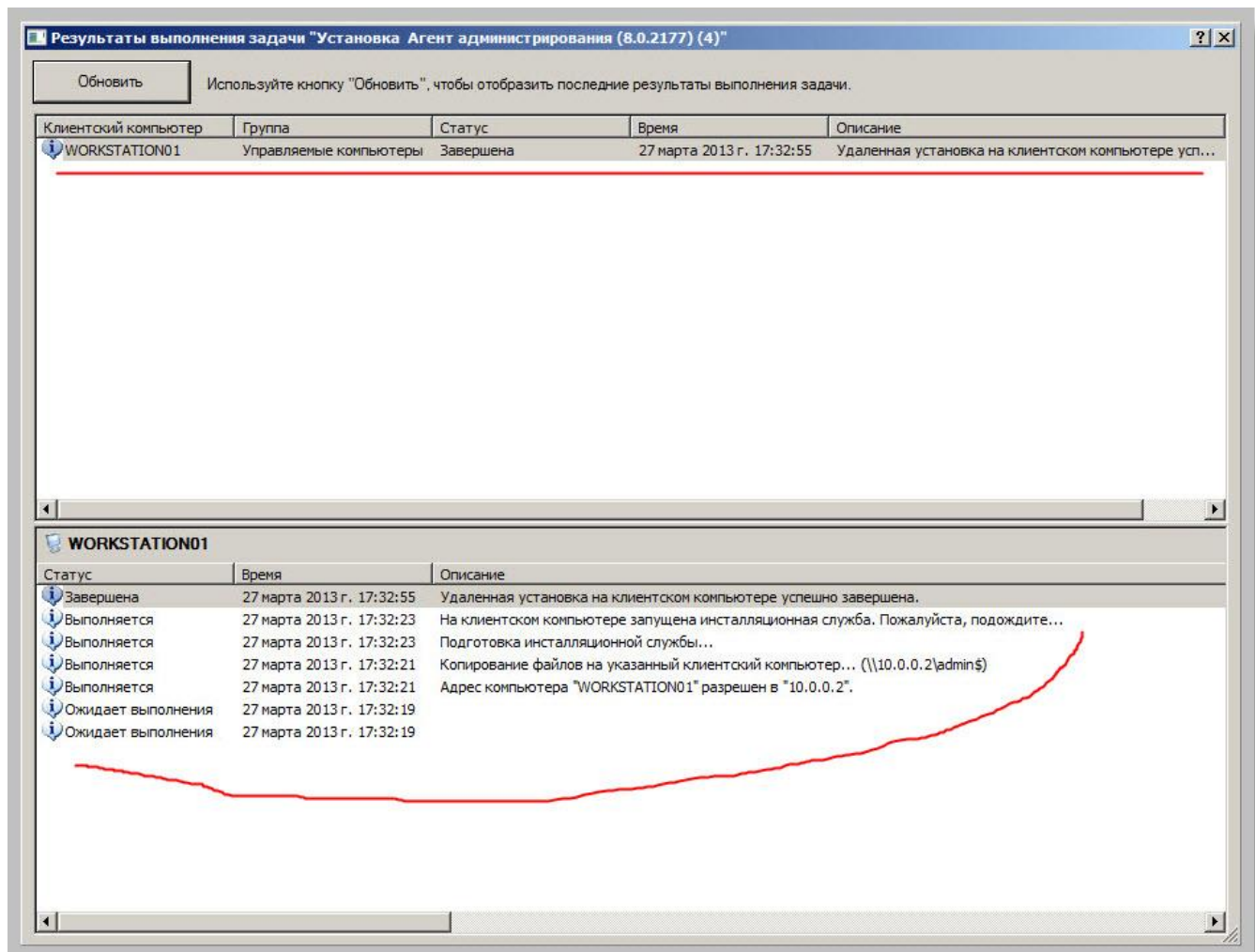


Несмотря на то, что написано на скриншоте, настоятельно рекомендую Вам дождаться чем все закончится? ☺ При желании, можно также посмотреть детальный отчет, нажав на ссылку: [Посмотреть результаты выполнения](#).

После завершения процесса мы увидим его итог. В данном случае установка прошла успешно!

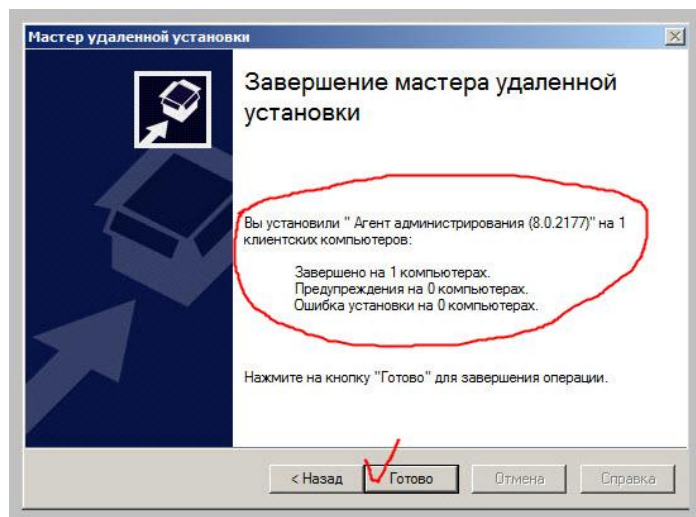


Посмотрим расширенный отчет:

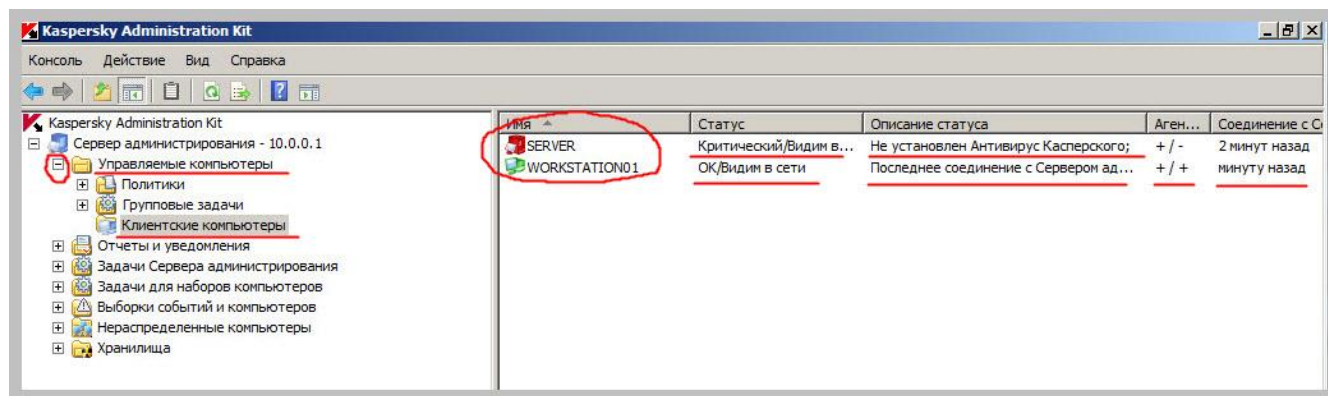


Как видите, все – максимально наглядно и удобно! Вообще, это – фишка Admin Kit-а Касперского: отчеты. Различные графики, выборки и таблицы статистики здесь – просто шикарные (по сравнению с решениями от других разработчиков).

После окончания инсталляции нам также вкратце сообщат о ее результатах и предложат нажать единственную кнопку «Готово».



Теперь давайте сделаем следующее: откроем на сервере раздел «Управляемые компьютеры» и в нем выберем пункт «Клиентские компьютеры» (здесь в правой части окна показаны все управляемые ПК нашей сети).



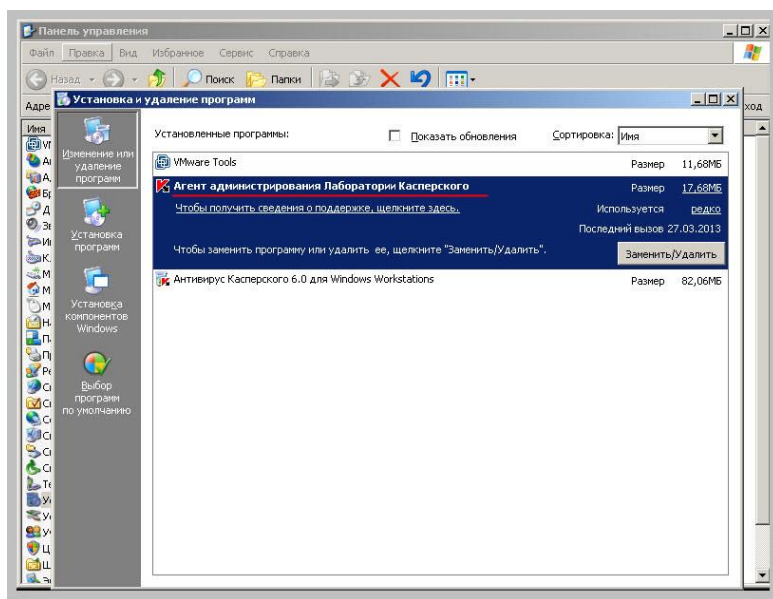
Как видите, там на данный момент присутствуют два ПК. Один из них наш сервер с Windows 2008, а второй – Windows XP. Обратите внимание на цвет, которым они обозначены. Красный «говорит» нам о том, что на рабочей станции есть какие-то проблемы и требуется наше вмешательство. Зеленый – все в порядке.

Обратите внимание также на столбцы «Статус», «Описание статуса», «Агент», «Соединение с сервером администрирования». По любому из них можно быстро сориентироваться относительно тех проблем и трудностей, которые имеются с конкретным антивирусным продуктом на удаленном ПК.

Вы, наверное, обратили внимание на то обстоятельство, что наш Server выделен красным цветом, а в описании его статуса написано «Критический»? Читаем поле «Описание статуса». Там написано: не установлен антивирус Касперского. Как такое может быть? Мы же – все устанавливали! Стоп, без паники! ☺ Если вдуматься, то – не все! Дело в том, что сам по себе, **Kaspersky Administration Kit** не является антивирусом. Он осуществляет только серверные функции контроля, управления и отчетности по антивирусной защите в сети.

Поэтому на самую операционную систему Winows Server 2008 тоже нужно ставить антивирус! НО, не простой, а... блин, чуть не написал – «золотой»! ☺ А - для серверных операционных систем. Потом – покажу какой именно скачивать.

Такс, теперь давайте сделаем вот что: посмотрим на нашем клиенте список установленных программ. Мы ведь – Фомы неверующие и должны сами во всем убедиться! ☺ Заходим на Windows XP в панель управления – установка и удаление программ и видим вот такую картину:



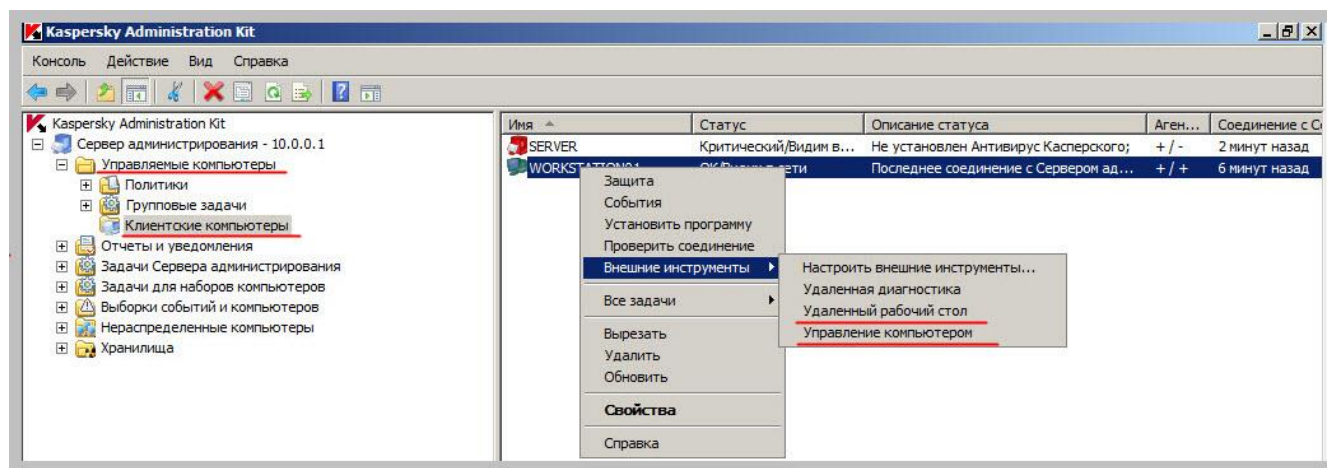
Удаленная установка Агента администрирования прошла успешно!

Вот теперь – внимание! Точно таким же образом можно устанавливать на удаленные компьютеры вообще все что угодно! Мы, к примеру, в нашей локальной сети таким образом устанавливали на компьютеры пользователей третий сервиспак Windows XP, Internet Explorer 8 и браузер Opera (там, где не ставился восьмой IE).

С этим – разобрались! Теперь я покажу Вам еще несколько мощных инструментов из арсенала Kaspersky Administration Kit.

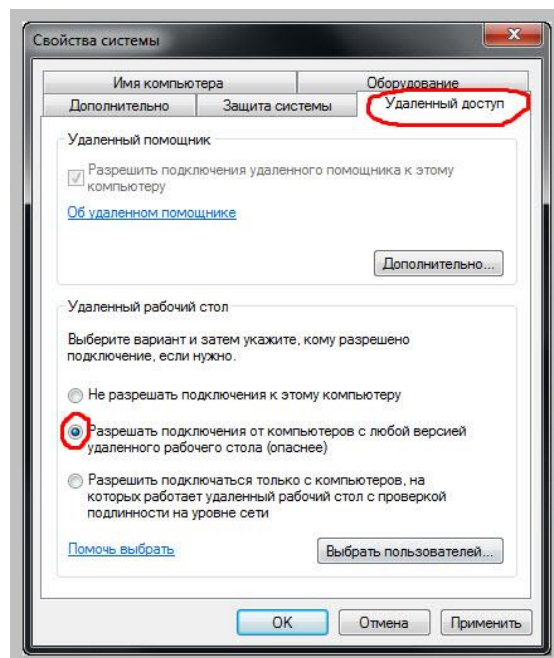
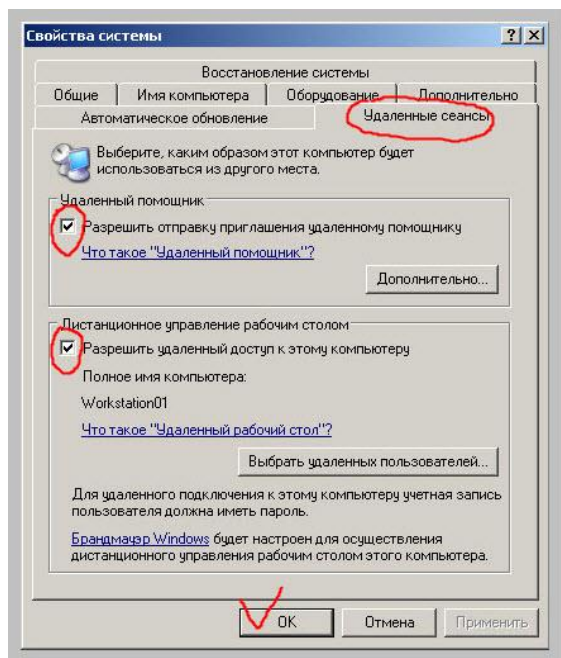
Откроем нашу консоль администрирования, развернем пункт «Управляемые компьютеры», перейдем к «Клиентские компьютеры», в правой части окна нажмем

правой кнопкой мыши по компьютеру Workstation01 и обратим внимание на пункты «Удаленный рабочий стол» и «Управление компьютером».

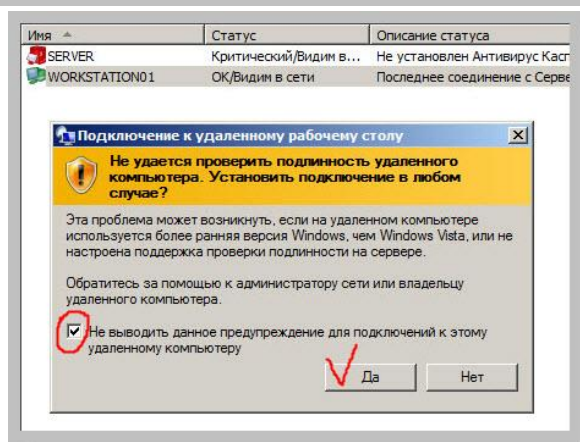


Сейчас мы рассмотрим работу первого из них, а чуть позже – второго. Остальной инструментарий Admin Kit-а Вы уже изучите сами, а то у нас статья и так большая получилась. Моя задача, на данном этапе, – дать Вам в руки рабочий инструмент и показать (на наглядных примерах) выгоды от его использования.

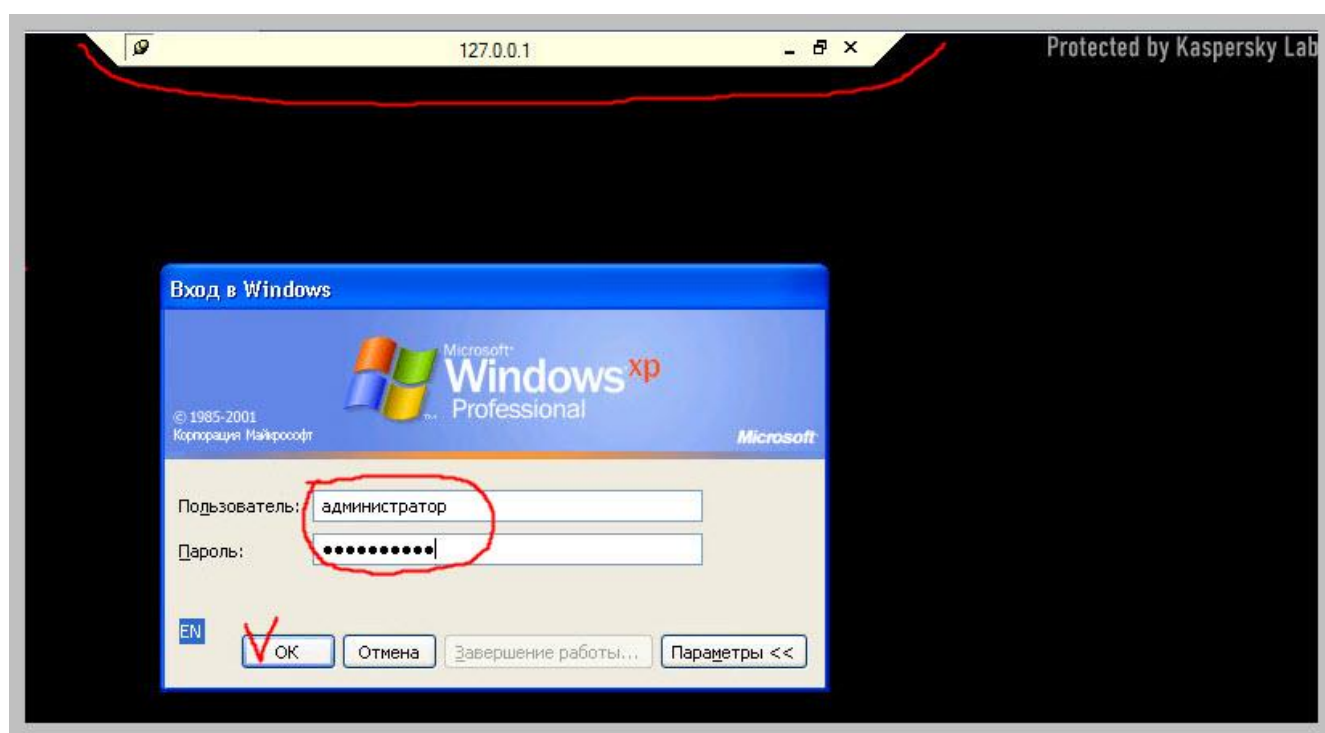
Для того, что бы у нас появилась возможность управлять удаленным рабочим столом на компьютере пользователя нам нужно задействовать на его ПК эту функцию. Ниже представлены два скриншота и обозначены те переключатели и галочки, которые должны быть установлены в операционных системах Windows XP и Windows 7.



Если на клиенте все настроено правильно, то при удаленном подключении к «Workstation01» мы увидим вот такое окно:



В этом предупреждении ничего страшного нет (можем поставить соответствующую галочку и оно больше не будет нам надоедать). Нажимаем кнопку «Да» и вот он – момент истины! 😊

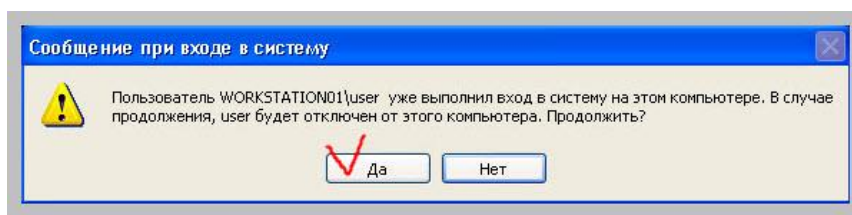


Как видите, мы подключились к удаленному компьютеру в режиме терминальной сессии по RDP протоколу (Remote Desktop Protocol - протокол удалённого рабочего стола). Это – протокол (набор правил сетевого взаимодействия), специально разработанный для обеспечения возможности подключения к рабочим столам других компьютеров (с целью оказания помощи пользователям удаленно или же – для работы в режиме терминального клиента на сервере терминалов).

Что мы видим на фото выше? Небольшая панель сверху экрана – отличительная визуальная особенность того, что мы находимся в режиме терминальной сессии. Далее – окно логина и пароля для входа в удаленный компьютер с Windows XP. Нам нужно указать пользователя, который имеет право доступа на данный компьютер. Можете сразу

указать пароль администратора, чтобы иметь полномочия производить какие-либо важные изменения в настройках системы.

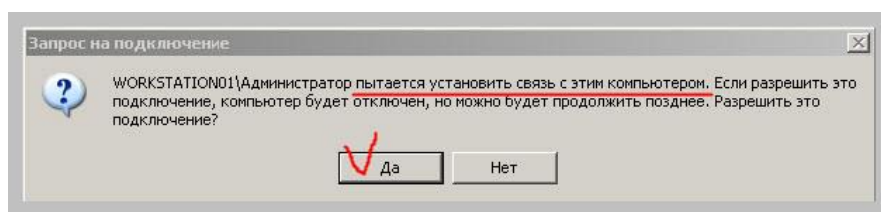
Нажимаем «ОК» и видим вот такое окно:



Все правильно! Мы ведь выполнили вход на виртуальную машину под управлением Windows XP локально? Лично я – выполнил! ☺ И именно под учетной записью «User», как и написано на скриншоте выше.

Теперь – внимание! Смотрим что в этот же момент времени происходит на компьютере «Workstation01», к которому мы подключаемся? Благо никуда бегать не нужно, просто переключимся в окно другой виртуальной машины, как было рассказано в одном из предыдущих уроков.

На ПК «Workstation01» в тот же момент времени мы видим вот такую картину:

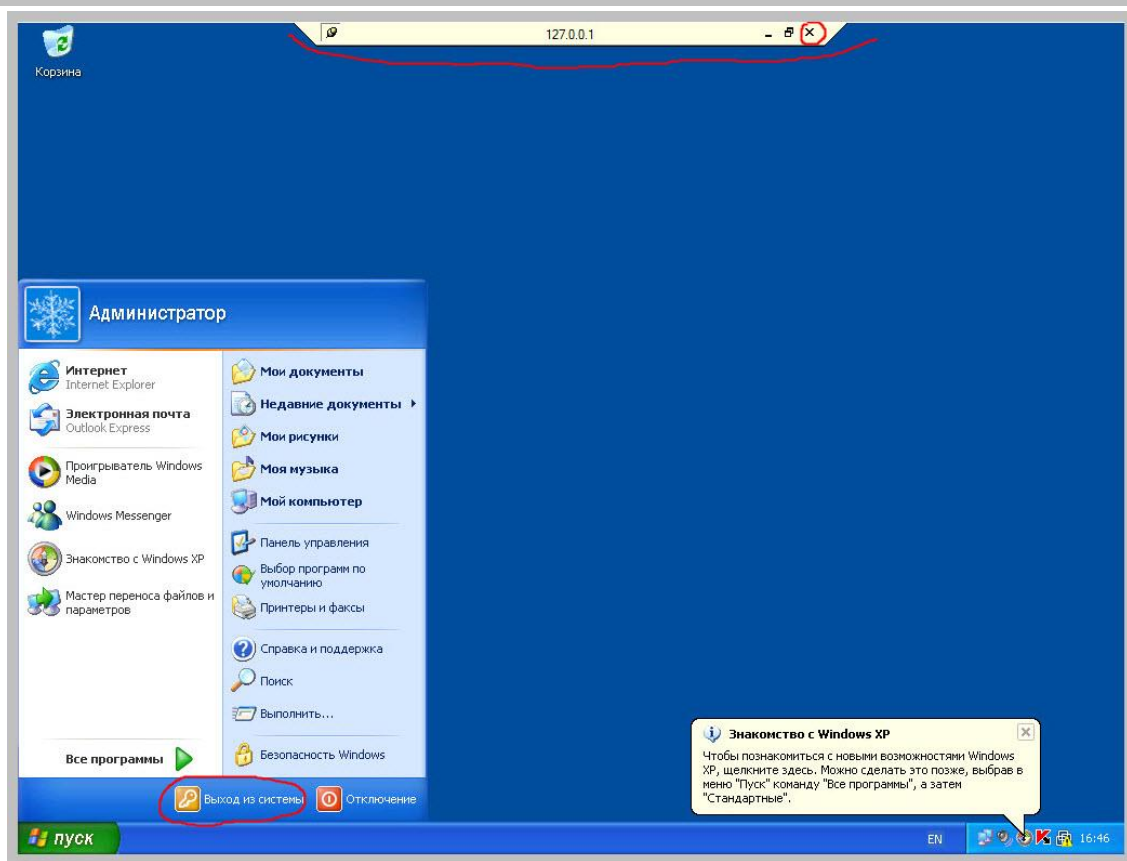


Как видим, пользователю будет показано предупреждение о том, что к его компьютеру удаленно подключился Администратор и предложено на выбор два варианта: разрешить или отклонить данное подключение.

Попробовал бы кто-то из пользователей у нас на работе «отклонить», - без Интернета дня три сидел бы – не меньше! ☺

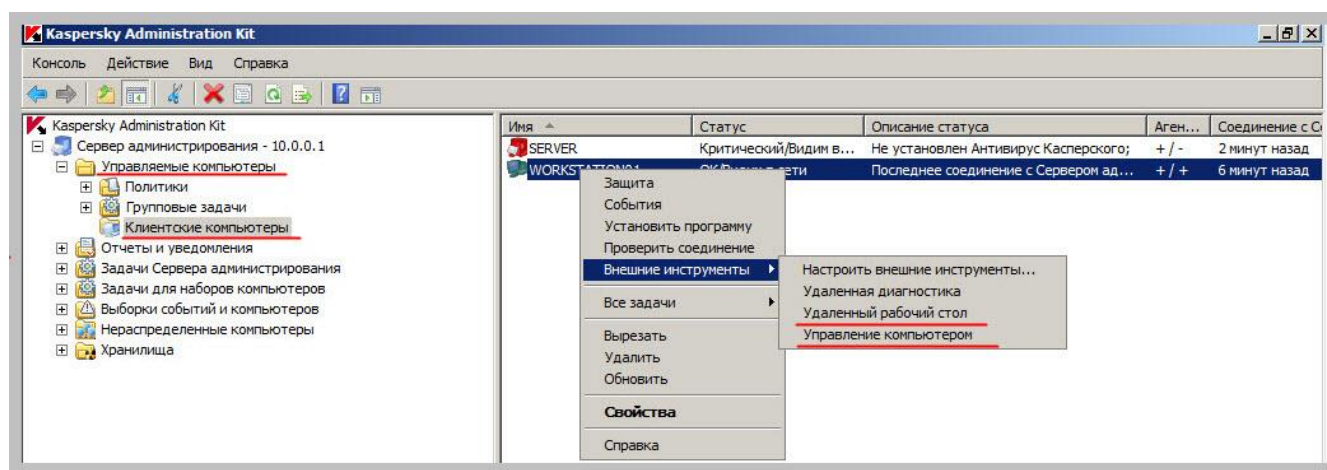
После нажатия пользователем удаленного компьютера на кнопку «Да» мы, со своей консоли администратора на сервере, попадем на удаленный компьютер.

У нас будет – свой (чистый) рабочий стол, но полный доступ к машине.

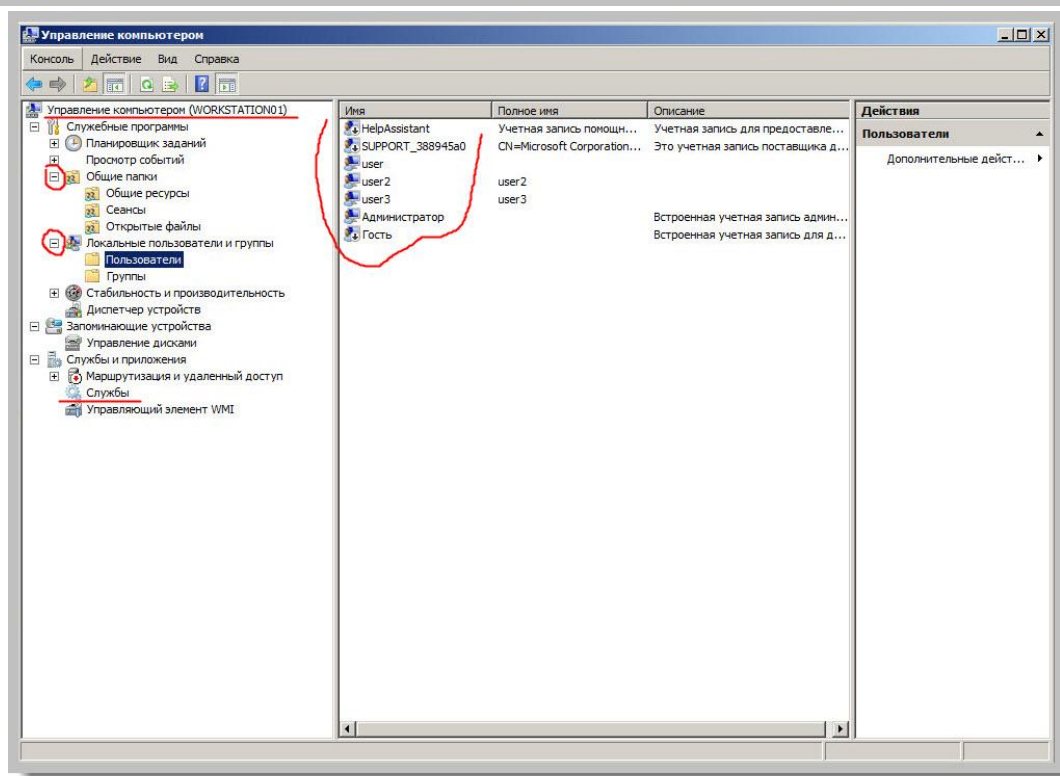


Выйти (отключиться) из удаленного сеанса мы можем либо нажав на надпись «Выход из системы» либо – на крестик на панели вверху экрана.

А сейчас, как и обещал, я покажу Вам еще один инструмент удаленного администрирования, который предоставляет нам Касперский Admin Kit. Это – удаленное «Управление компьютером».



После подключения мы получим в свое распоряжение вот такое окно:



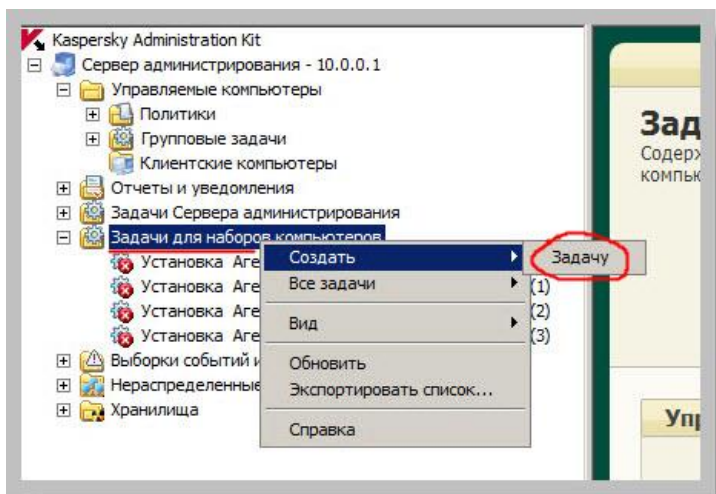
Видите вверху в левой части окна надпись: «Управление компьютером Workstation01»? Это значит, что мы в данный момент работаем именно с удаленной машиной. В левой части окна мы можем наблюдать древовидную структуру, состоящую из перечня служб и функций, которыми мы можем удаленно манипулировать на компьютере пользователя. В правой части окна отображаются настройки и реквизиты каждой конкретной службы.

Как видите, в данный момент, мы вошли в элемент управления локальными пользователями и группами на компьютере Workstation01. Справа в окне мы видим всех пользователей, учетные записи которых присутствуют на удаленном ПК. Мы также можем редактировать их на свое усмотрение: поменять им пароль, заблокировать учетную запись или же – создать новую, удалить или переименовать ее и т.д.

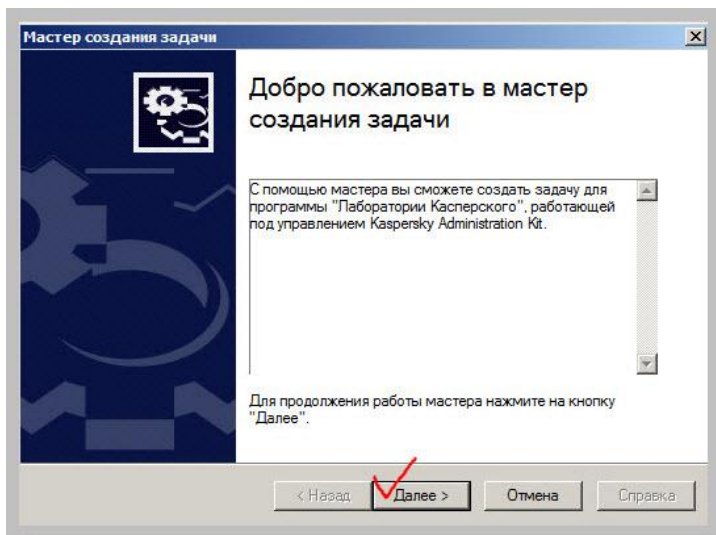
Компонент «Общие ресурсы» позволяет управлять общим доступом к файлам и папкам на удаленном компьютере, а – «Службы» - запускать и останавливать системные службы и процессы на нем. В «Управлении дисками» мы получим доступ к разделам жесткого диска сетевого компьютера. Более детально изучите оснастку сами.

Что бы нам такого полезного сделать дальше? ☺ А давайте - вот что: создадим групповую задачу поиска вирусов на всех рабочих станциях! В нашей организации, к примеру, она запускается один раз в месяц одновременно на всех управляемых компьютерах. После этого мне на почту приходит куча писем с отчетами. Помните, одно из таких писем мы рассматривали в первой части статьи?

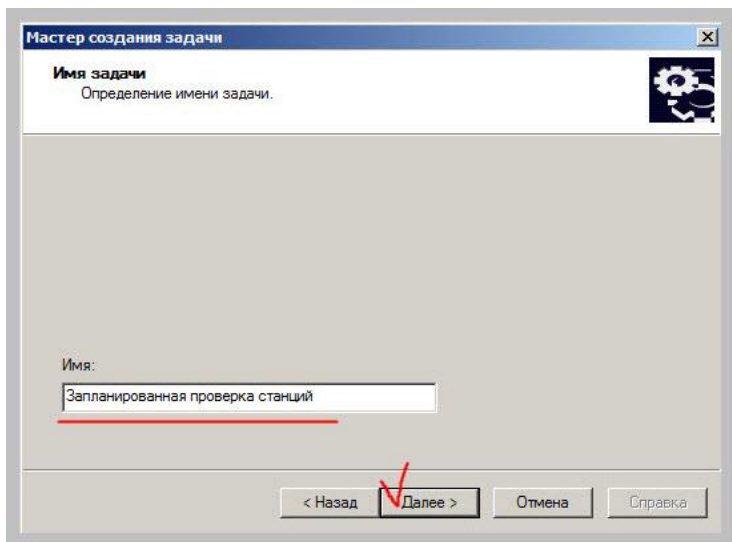
Итак, для создания групповой задачи открываем раздел «Задачи для наборов компьютеров», нажимаем правой кнопкой мыши и из выпавшего меню выбираем «Создать», потом – «Задачу».



Запустится мастер создания задачи, который будет нам помогать (по факту - вести за руку) ☺

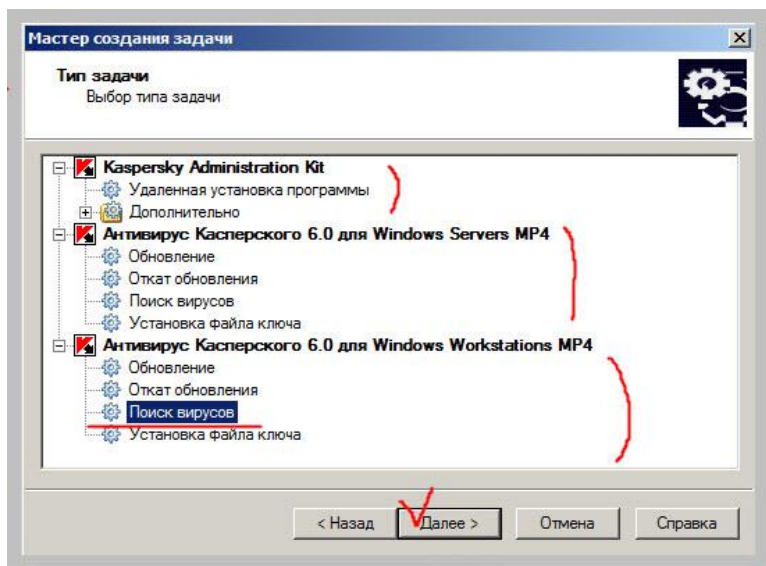


Нажимаем «Далее».



В текстовом поле «Имя» пишем название нашей задачи. Старайтесь давать осмысленные названия, так как потом нам с ними же и работать. Нажимаем «Далее».

На следующем шаге нам предложат указать какую именно и для какого класса программных решений задачу мы будем создавать?

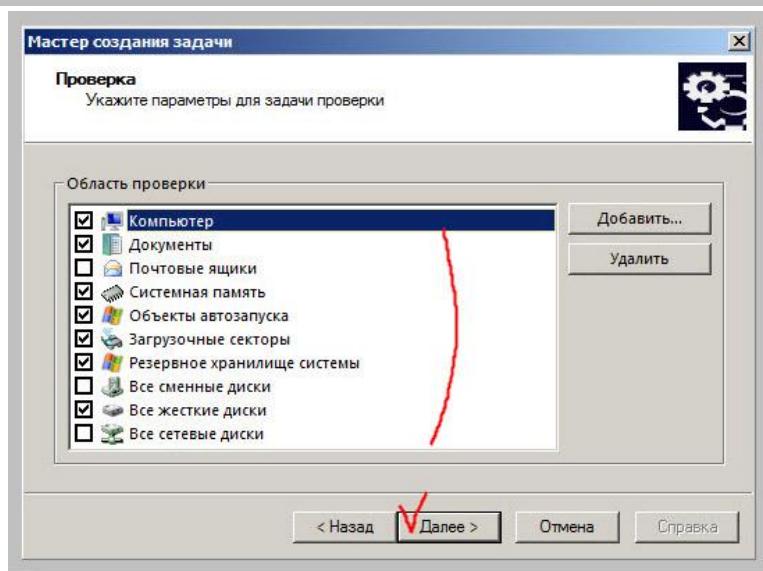


Верхняя секция отвечает за создаваемые задачи для самого Kaspersky Administration Kit, средняя – за задачи для антивирусов, установленных на серверных операционных системах, а третья – для клиентских.

Поскольку мы создаем задачу для всего парка компьютеров пользователей, то обращаемся именно к третьей секции и выбираем там из задач-заготовок: «Поиск вирусов».

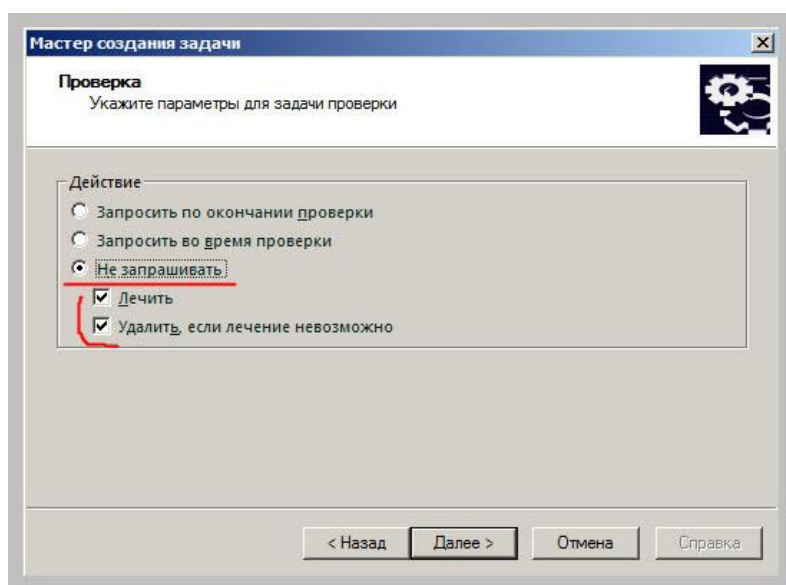
Примечание: при необходимости, Вы можете создавать свои собственные задачи с нуля, называть их, как Вам удобно, а затем – запускать на выполнение на всех подчиненных компьютерах!

В окне, представленном на фото ниже, нам нужно будет указать, какие именно объекты и зоны должны будут проверяться на удаленных компьютерах?



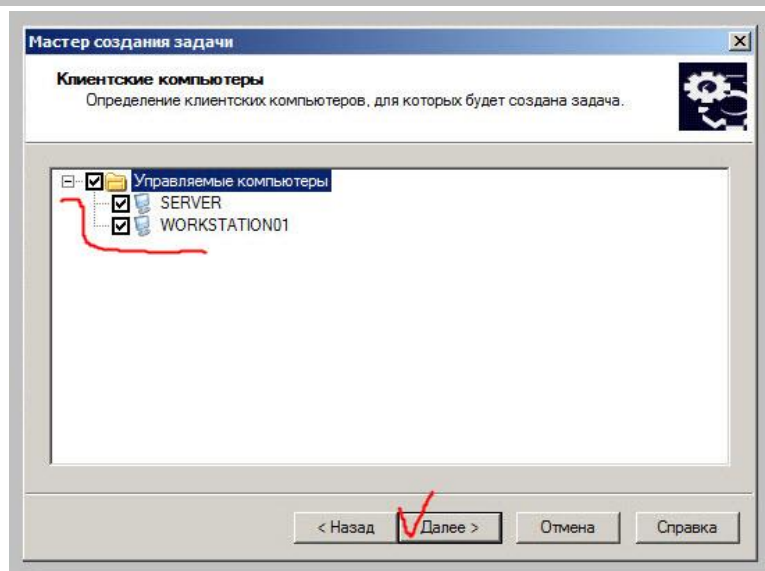
При необходимости, можете воспользоваться кнопкой «Добавить». Нажимаем «Далее».

После этого необходимо будет указать антивирусу, что ему делать в случае обнаружения угрозы (вируса)?



Я настоятельно рекомендую выбрать именно третий вариант: «Не запрашивать» и поставить две галочки, как на скриншоте выше. Такая настройка позволит максимально эффективно бороться с вирусами, а не выводить каждый раз при обнаружении угрозы пользователю всплывающее окно с вариантом выбора действия: «лечить/пропустить». Разве что – Вы на 100% доверяете и уверены в своих пользователях! Или, все таки, - сомневаетесь? ☺

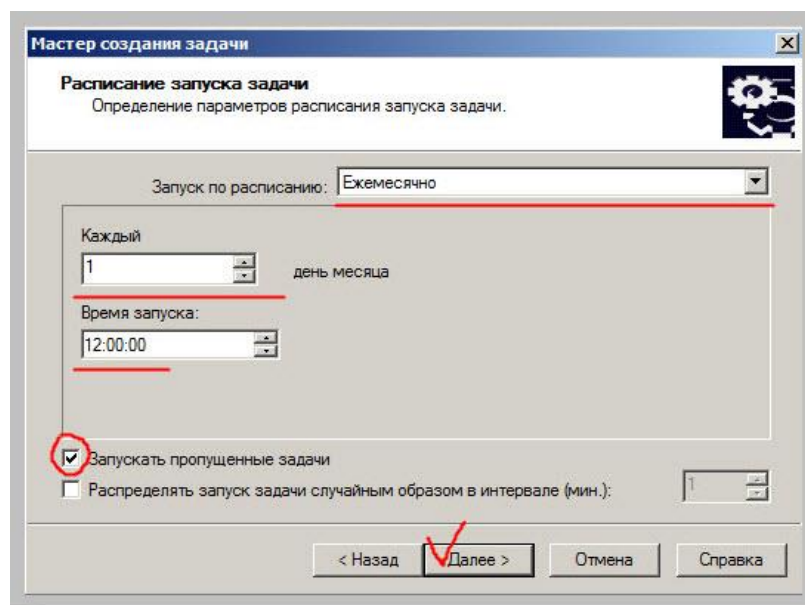
На следующем шаге мастера необходимо будет указать, для каких именно компьютеров в Вашей сети будет создана задача?



Я думаю – для всех. Хотя, решайте сами.

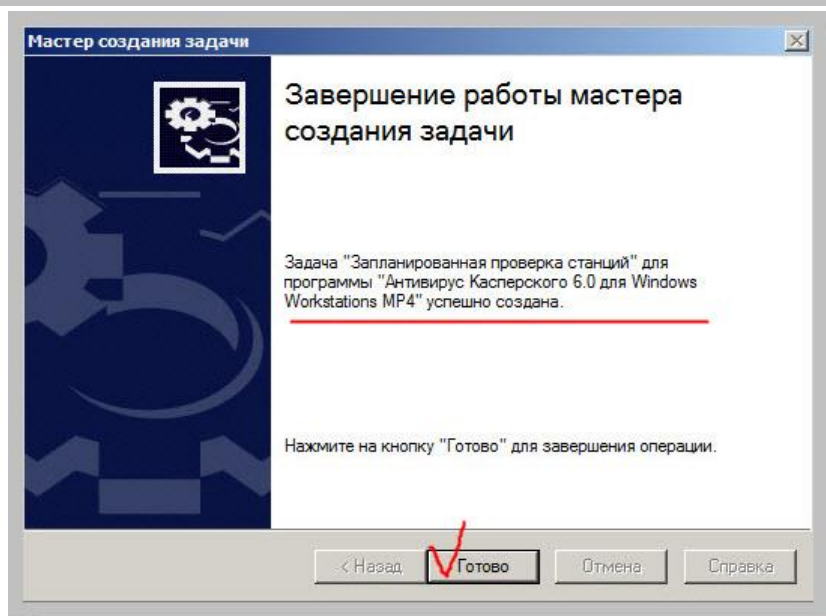
Нажимаем «Далее».

Важная настройка – установка времени запуска задачи:



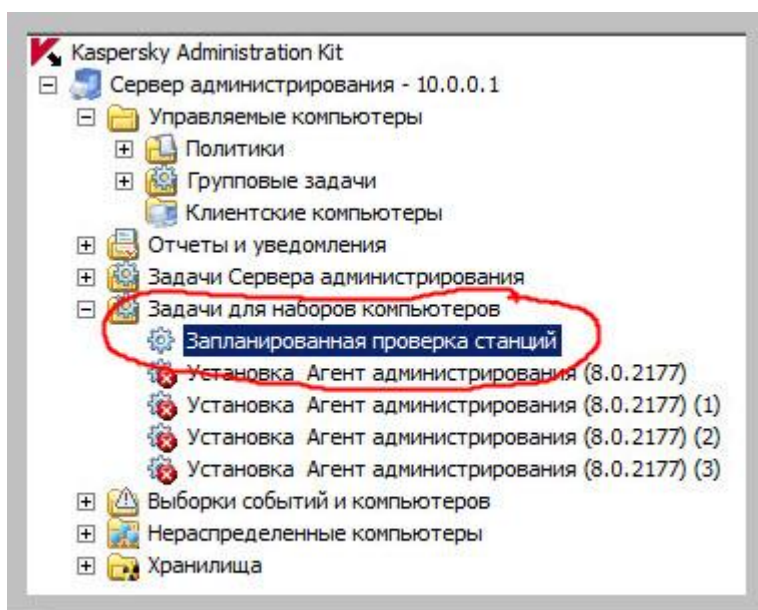
Как видите, я определил ее запуск один раз в месяц, каждый первый день месяца (первого числа) в 12:00. Поскольку полная проверка на вирусы достаточно серьезно нагружает клиентские компьютеры, старайтесь выбирать обеденное время, когда большинство работников не заняты своими служебными обязанностями. Также можете отметить галочку «Запускать пропущенные задачи» - пригодится!

После всех этих приготовлений нам, наконец-то, будет представлен небольшой отчет об успешном создании запланированной задачи и предложено нажать кнопку «Готово»:



Незамедлительно воспользуемся.

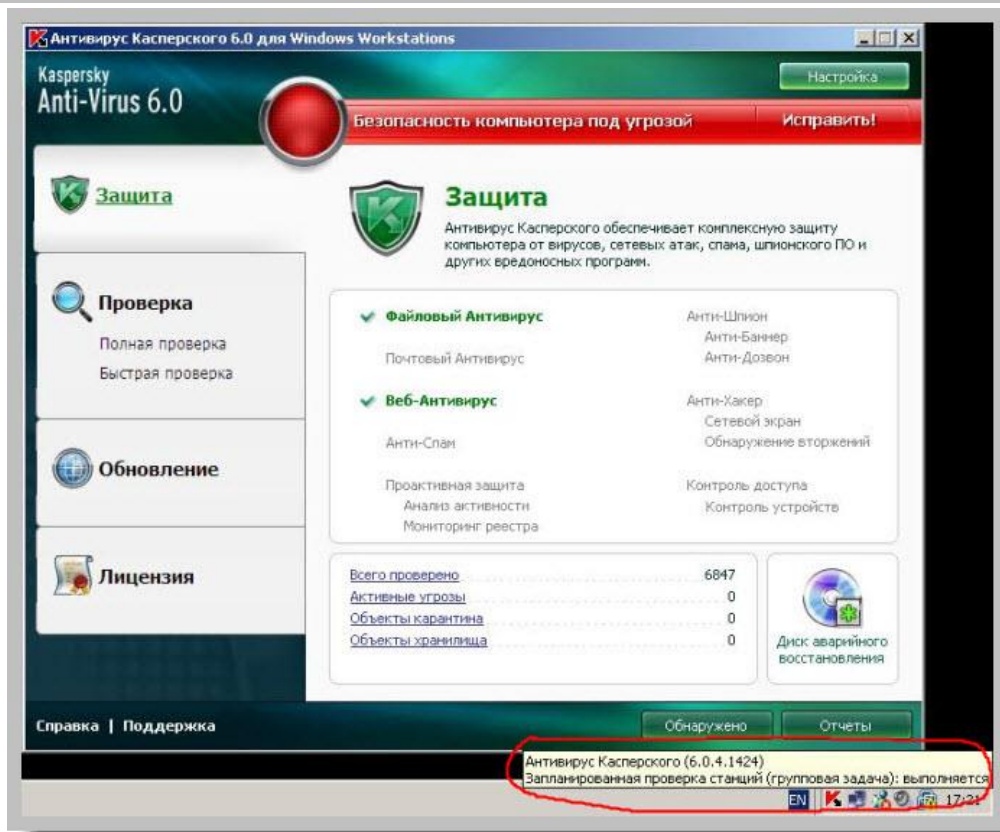
Теперь внимательно посмотрим на нашу консоль и увидим, что задача появилась в определенном для нее разделе:



Она — готова к выполнению (не обозначена красным крестиком) и ждет своего времени. Но поскольку мы с Вами не собираемся сидеть здесь до первого числа и ждать пока она запустится по расписанию, то сами форсируем этот процесс!

Нажимаем на ней правой кнопкой мыши и выбираем пункт «Запустить».

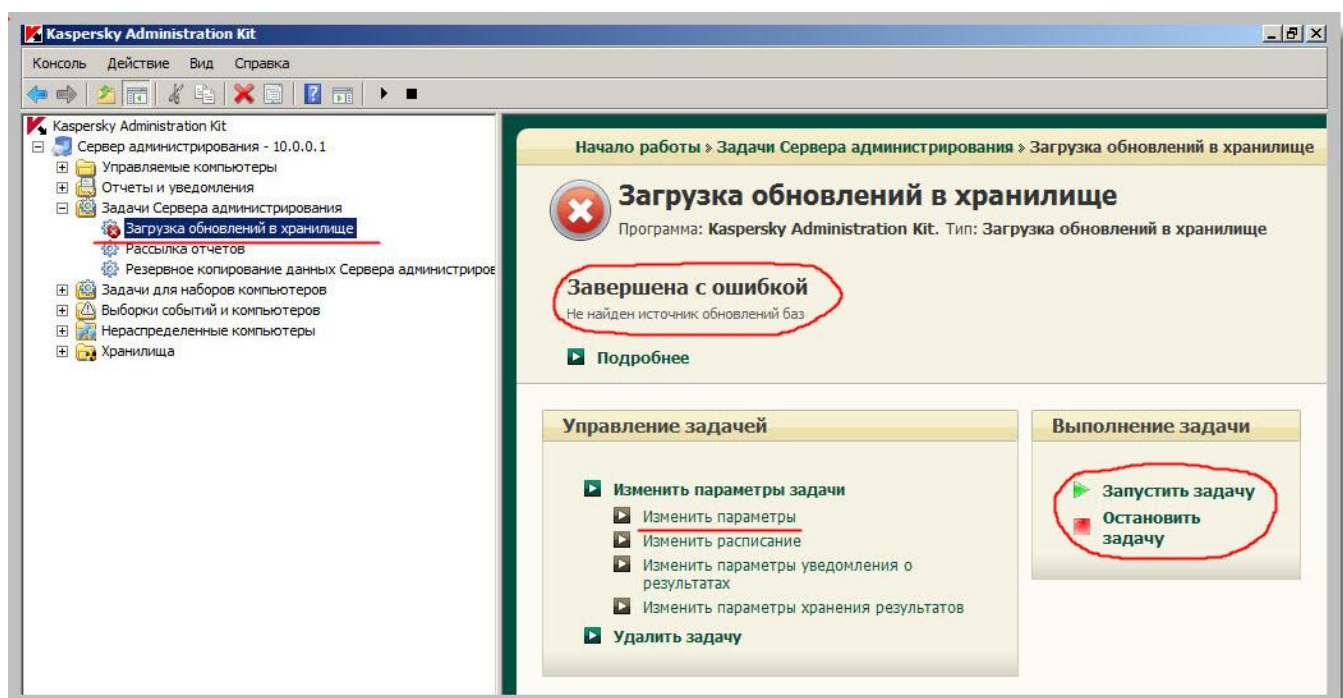
Теперь «идем» на клиентский компьютер, наводим мышку на значек антивируса Касперского в системном трее и видим вот такую надпись:



Отлично! Проверка рабочих станций – запустилась!

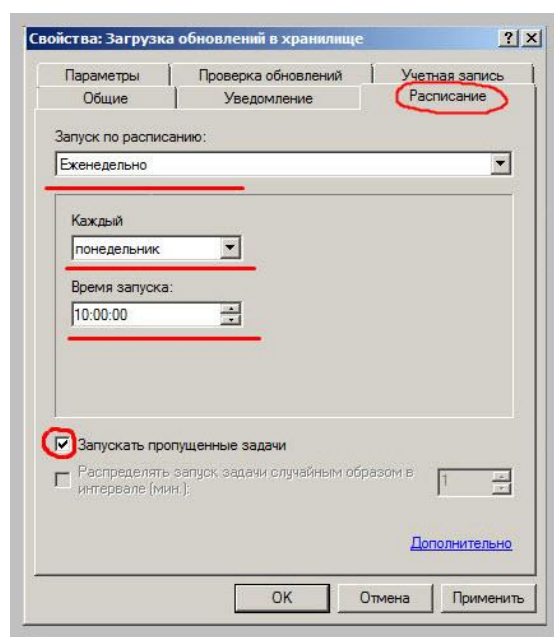
Теперь я хочу показать Вам еще одну очень важную вещь, которую нам нужно будет настроить. Это – бесперебойное получение обновлений самим сервером администрирования. Ведь все остальные компьютеры будут автоматически обновляться с него и это – очень важный момент!

В консоли раскрываем пункт «Задачи Сервера администрирования» и нажимаем на пункт «Загрузка обновлений в хранилище»



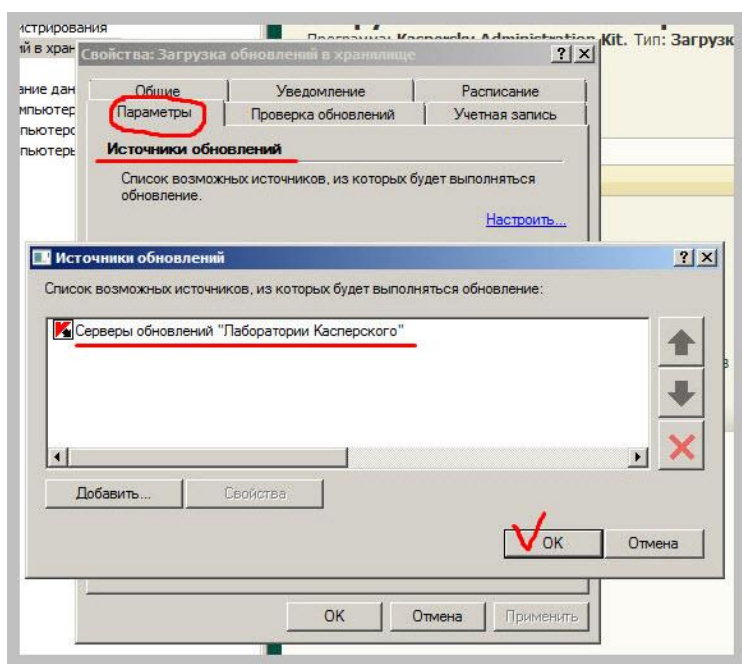
В правой части окна видим настройки этого пункта. Видим, что у нас есть возможность в любой момент вручную запустить задачу, нажав на одноименный пункт справа и – остановить ее выполнение.

Сейчас же нам необходимо произвести первоначальную настройку получения обновлений антивирусных баз Admin Kit-ом с официальных серверов обновлений лаборатории Касперского. Нажимаем на кнопку «Изменить параметры» и в открывшемся окне переходим на вкладку «Расписание».



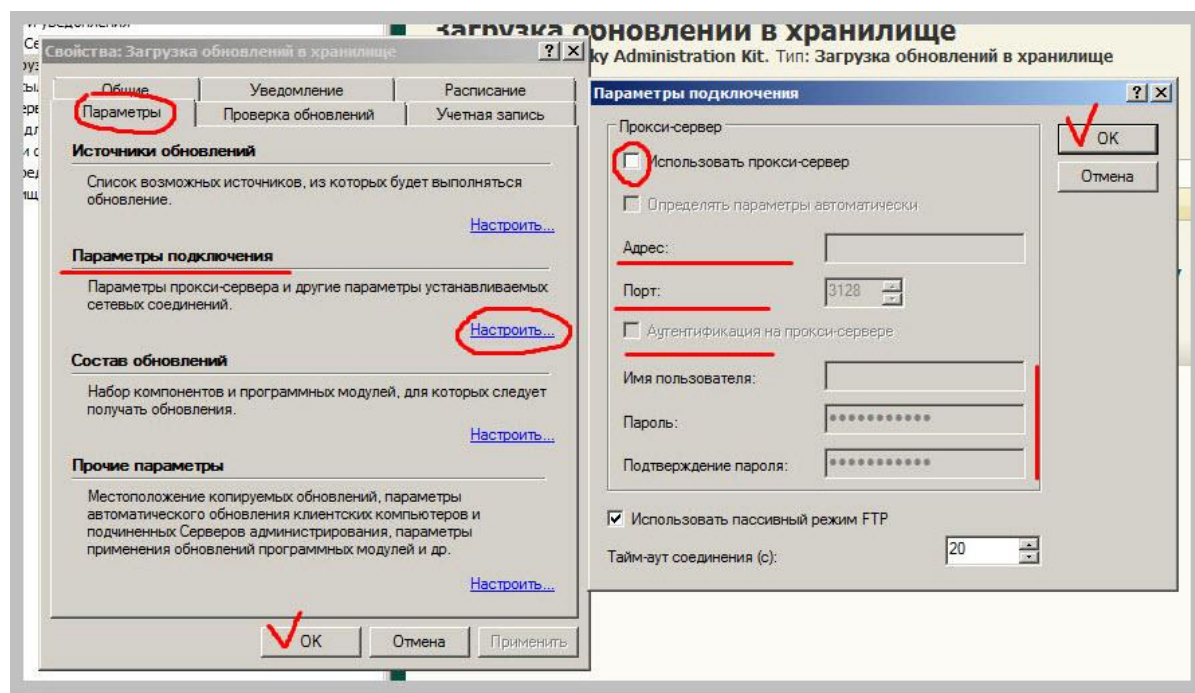
Устанавливаем частоту загрузки обновлений (я считаю, что один раз в неделю – вполне оптимально), выбираем день недели и время запуска задачи.

Затем переходим на вкладку «Параметры» и проверяем, чтобы источником обновлений у нас были выставлены Серверы обновлений Лаборатории Касперского.



При необходимости – корректируем этот момент.

На той же вкладке «Параметры» в секции «Параметры подключения» нажимаем на ссылку «Настроить». Откроется еще одно окно:

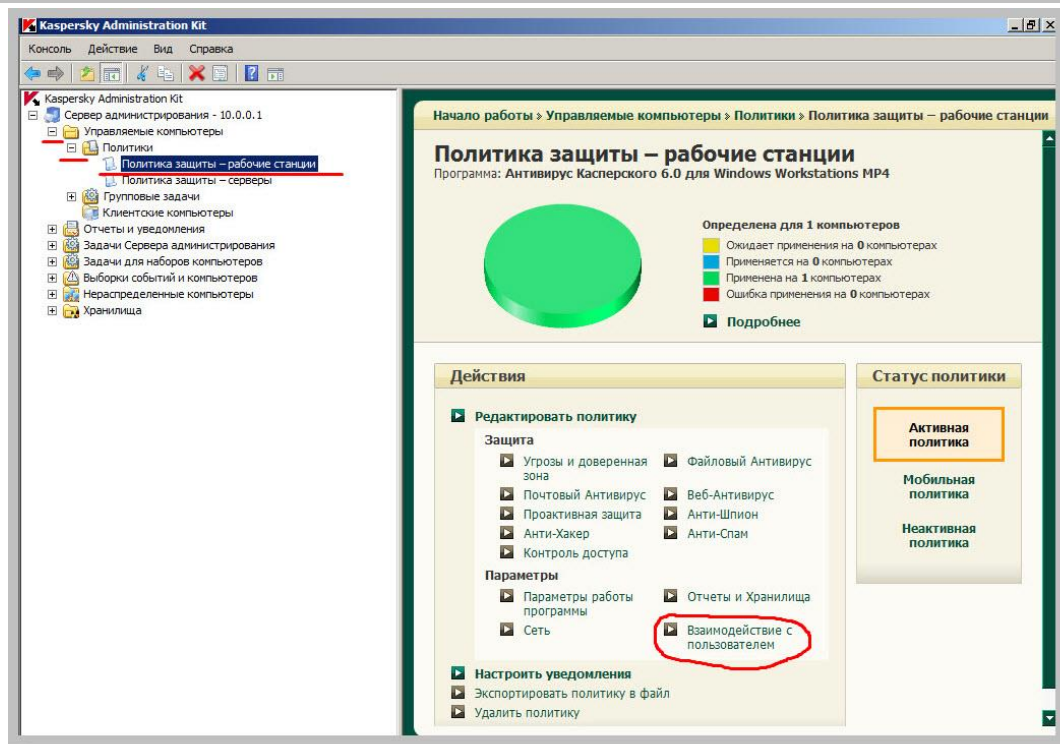


В нем мы можем указать настройки нашего прокси-сервера (если таковой мы используем у себя в организации). Если не знаете, что это такое – просто не задействуйте соответствующую галочку. Если же сами настраивали свой прокси, то и объяснять здесь Вам ничего не нужно 😊

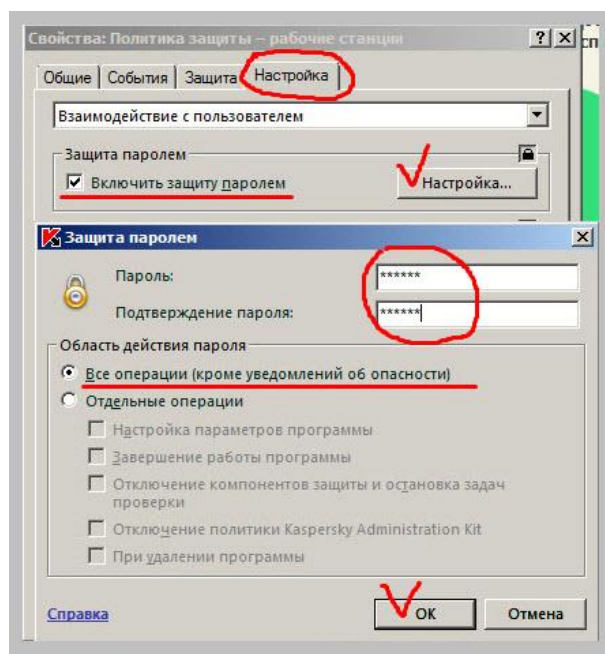
Вот теперь, можно считать, что первоначальная настройка и развертывание антивирусной защиты в нашей сети выполнены! Можете поздравить себя с этим, потому что это действительно очень важно – осуществлять централизованный контроль и управление антивирусной защитой и реагировать на потенциальные угрозы почти в режиме реального времени!

В завершении, покажу Вам еще одну «полезность», которую я рекомендую использовать при настройке сервера администрирования. Помните, в первой части статьи (при установке антивируса на рабочей станции пользователя), мы рассматривали такую возможность, как защита настроек программы паролем? Тогда мы пропустили этот пункт и я обещал рассказать Вам, как это можно сделать централизованно при помощи сервера администрирования. Настало время разобраться с этим!

Заходим в «Управляемые компьютеры» - «Политики» - «Политика защиты – рабочие станции» в правой части окна отобразятся настройки данной политики:



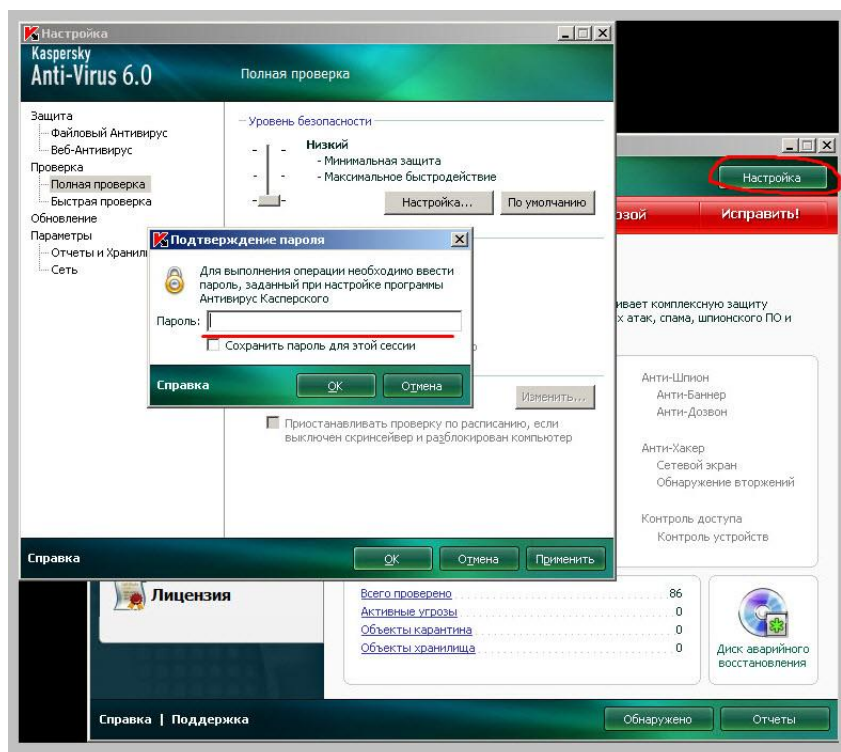
Здесь нам нужно будет нажать на ссылку «Взаимодействие с пользователями». Появится окно, в котором мы переходим на вкладку «Настройка», ставим галочку напротив пункта «Включить защиту паролем» и нажимаем на кнопку «Настройка»:



После этого появится еще одно небольшое окно, где нам надо будет указать пароль, который будет защищать настройки антивируса от изменения неопытным пользователем. **Не забудьте пароль сами!** 😊

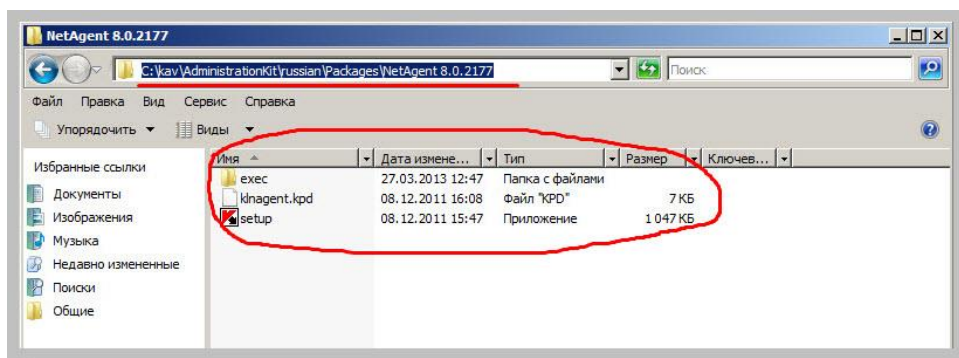
Нажимаем во всех открытых окнах «ОК» и «идем» на клиентский компьютер с XP, проверить задействовались ли данная политика ограничения?

Двойным кликом на значке антивируса в трее вызываем главное окно программы и нажимаем на кнопку «Настройка»



Как видите, появилось окно с приглашением ввода пароля доступа к настройкам. Все – работает!

Еще я хотел бы показать Вам следующую вещь:

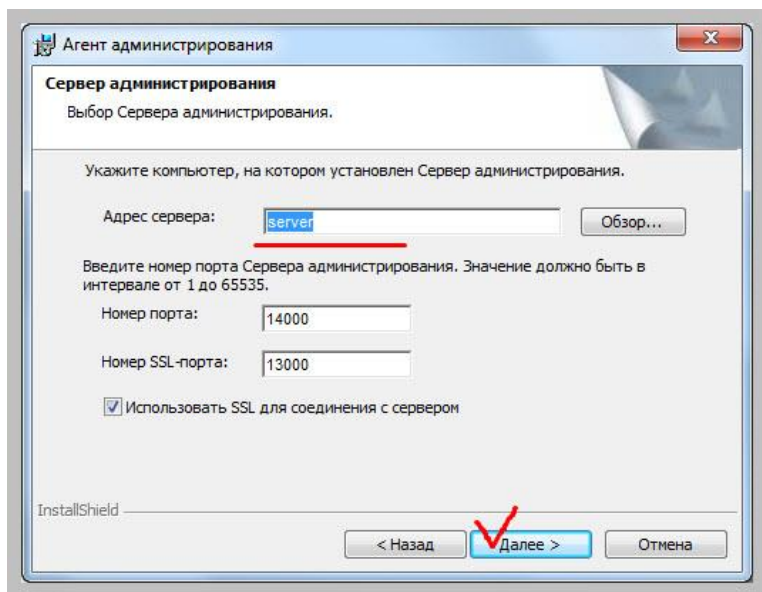


Помните, мы удаленно устанавливали Агент администрирования на компьютер пользователя? Мы делали это, зайдя в раздел «Хранилище». А на скриншоте выше показан путь к этому самому «хранилищу», где и находятся файлы установки Агента администрирования. Их можно скопировать оттуда и устанавливать пользователю отдельно с флешки (я иногда так и делаю).

Сам процесс установки «вручную» описывать подробно не буду. Там главное – все время нажимать кнопку «Далее» ☺ Если на ранних этапах настройки сервера никакие из портов не были переназначены вручную, - все должно пройти гладко.

Единственное, что придется указать вручную, так это имя (или IP адрес) сервера администрирования, чтобы Net Agent «знал», на каком компьютере установлен его сервер.

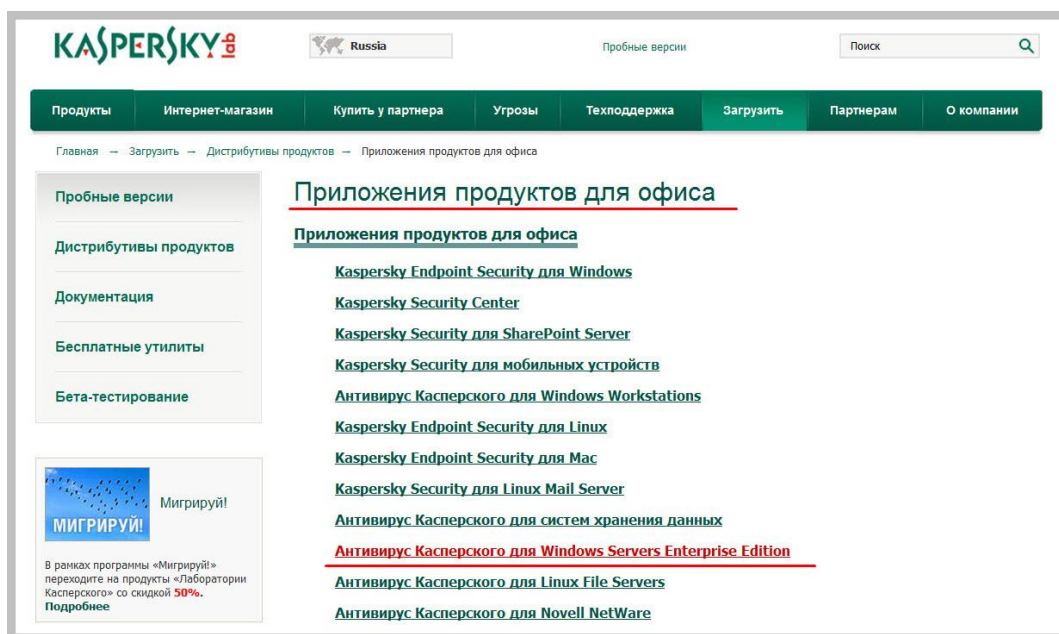
Вот эта настройка:



Повторюсь, остальное ничего не изменяйте, все – по умолчанию.

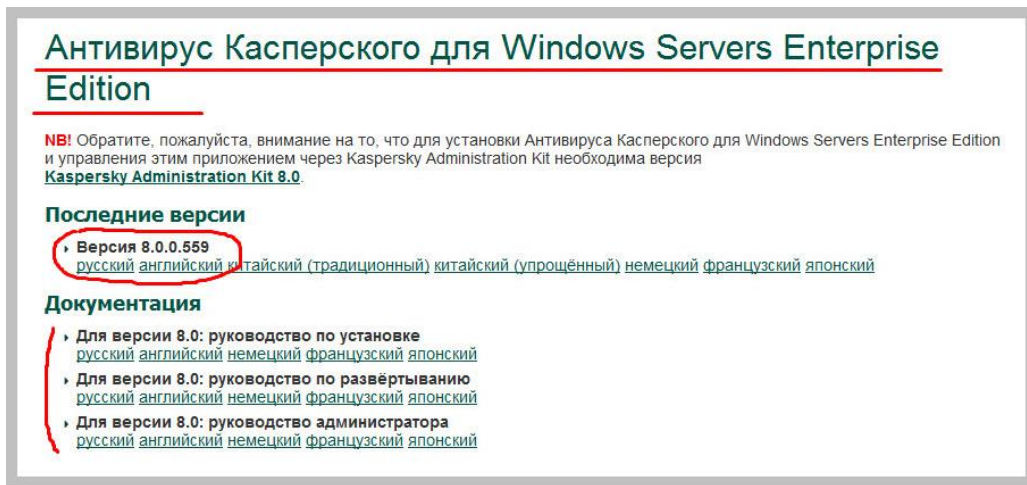
Теперь давайте покажу Вам, откуда скачать антивирус Касперского для серверов (тот который мы устанавливали на Workstation01 на Windows 2003 или 2008 Server не установится).

Итак, на официальном сайте лаборатории заходим в раздел «Приложения продуктов для офиса» и там ищем «Антивирус Касперского для Windows Servers Enterprise Edition»



Вот именно он нам и нужен!

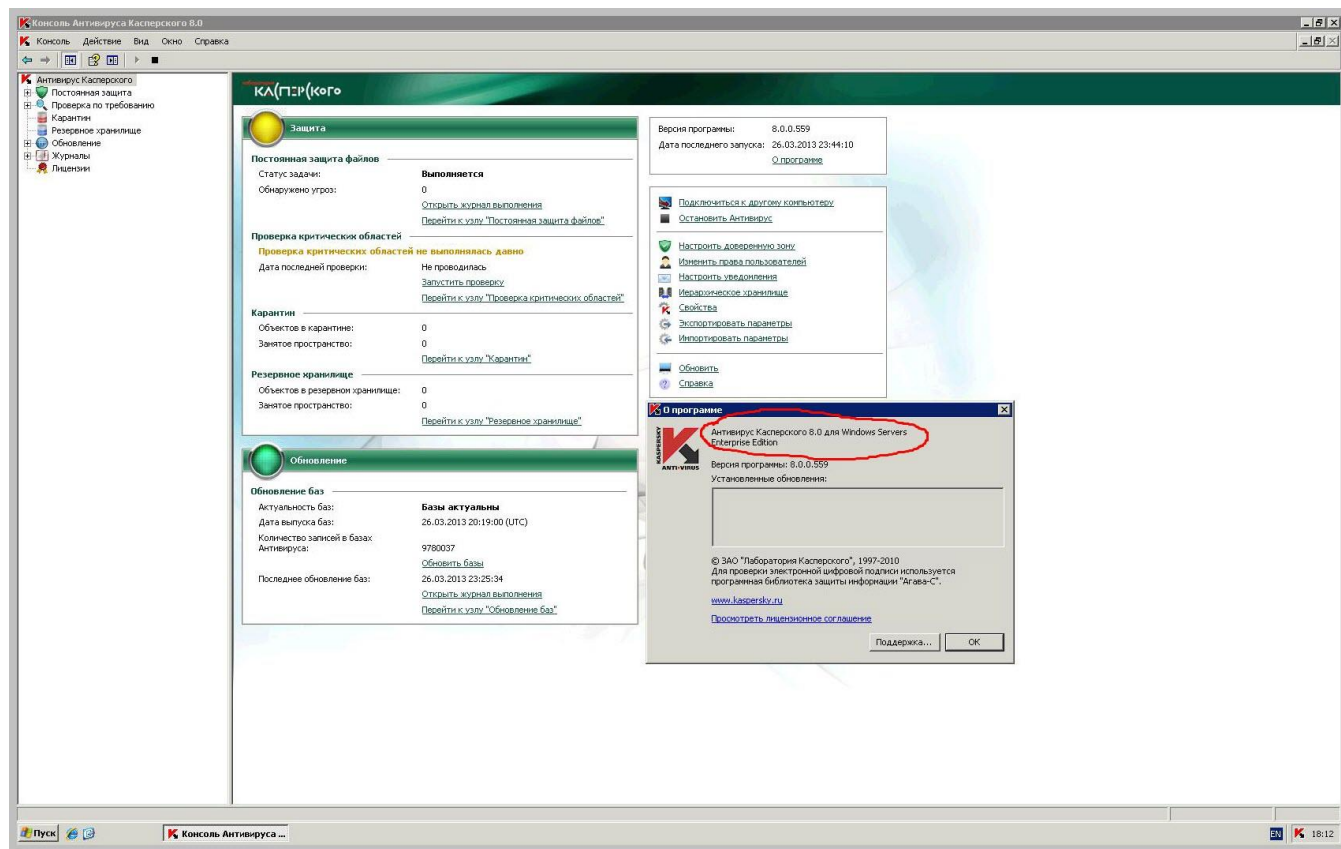
Нажимаем на ссылку и переходим на страницу загрузки приложения:



Как видите, здесь есть ссылка как на загрузку разных языковых версий, так и на различную документацию и руководства (тоже на русском).

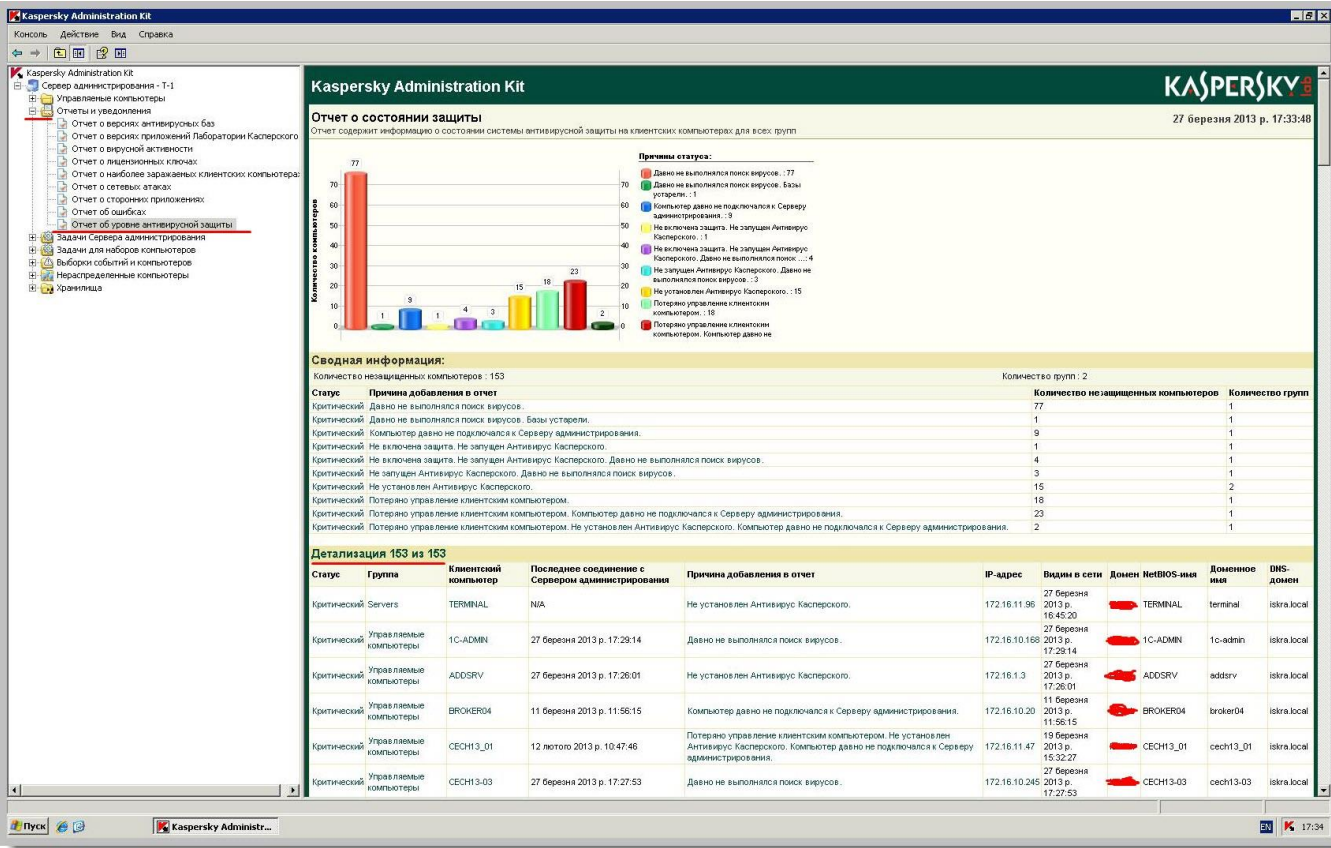
Загружаем его себе на компьютер и устанавливаем на наш сервер.

Вот как, к примеру, выглядит главное окно серверного антивируса, запущенное на одном из наших рабочих серверов:



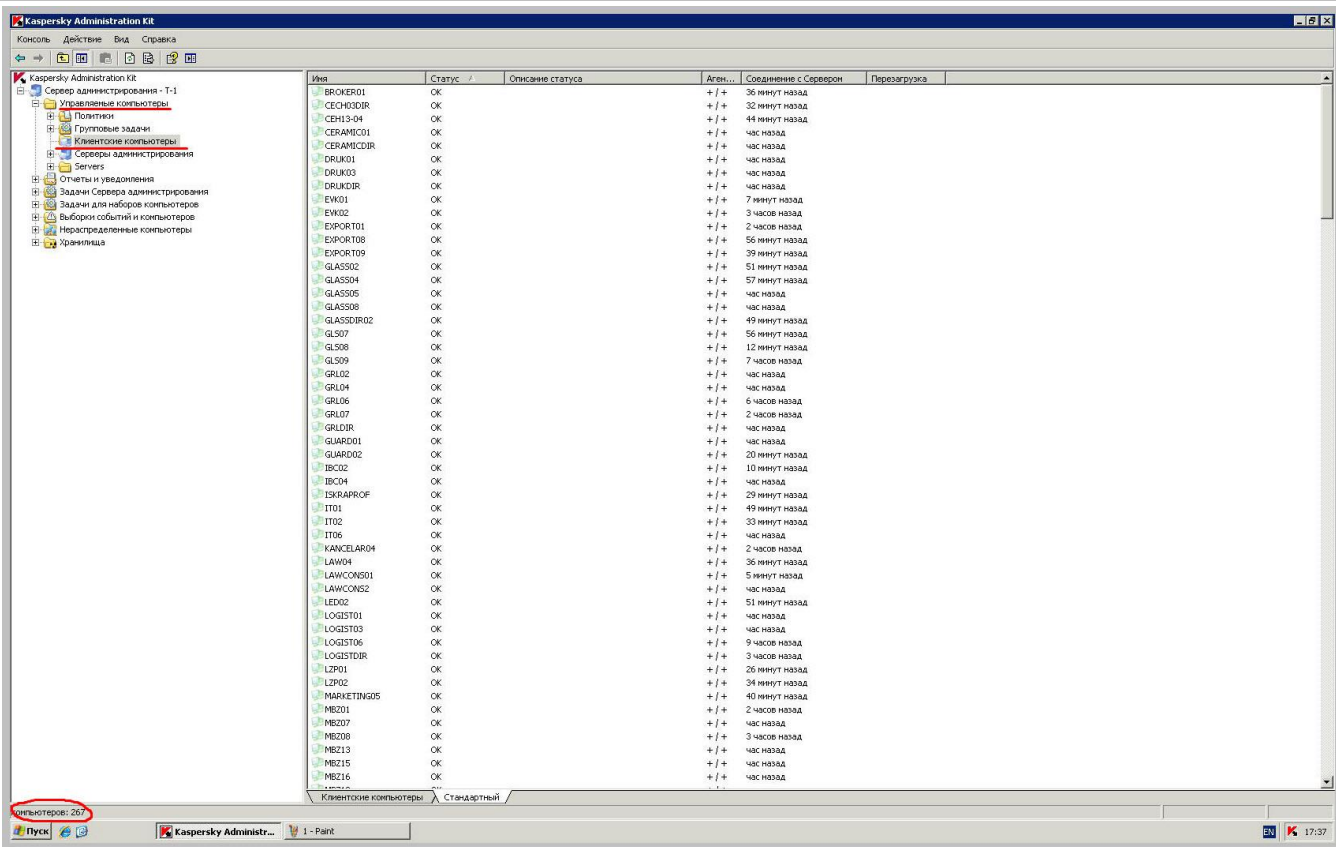
Ну и уж совсем напоследок, — еще несколько скриншотов из рабочей версии Kaspersky Administration Kit, который контролирует локальную сеть в нашей организации.

Вот – скриншот, который показывает одну из многочисленных статистических выборок, сформированных по моему требованию:



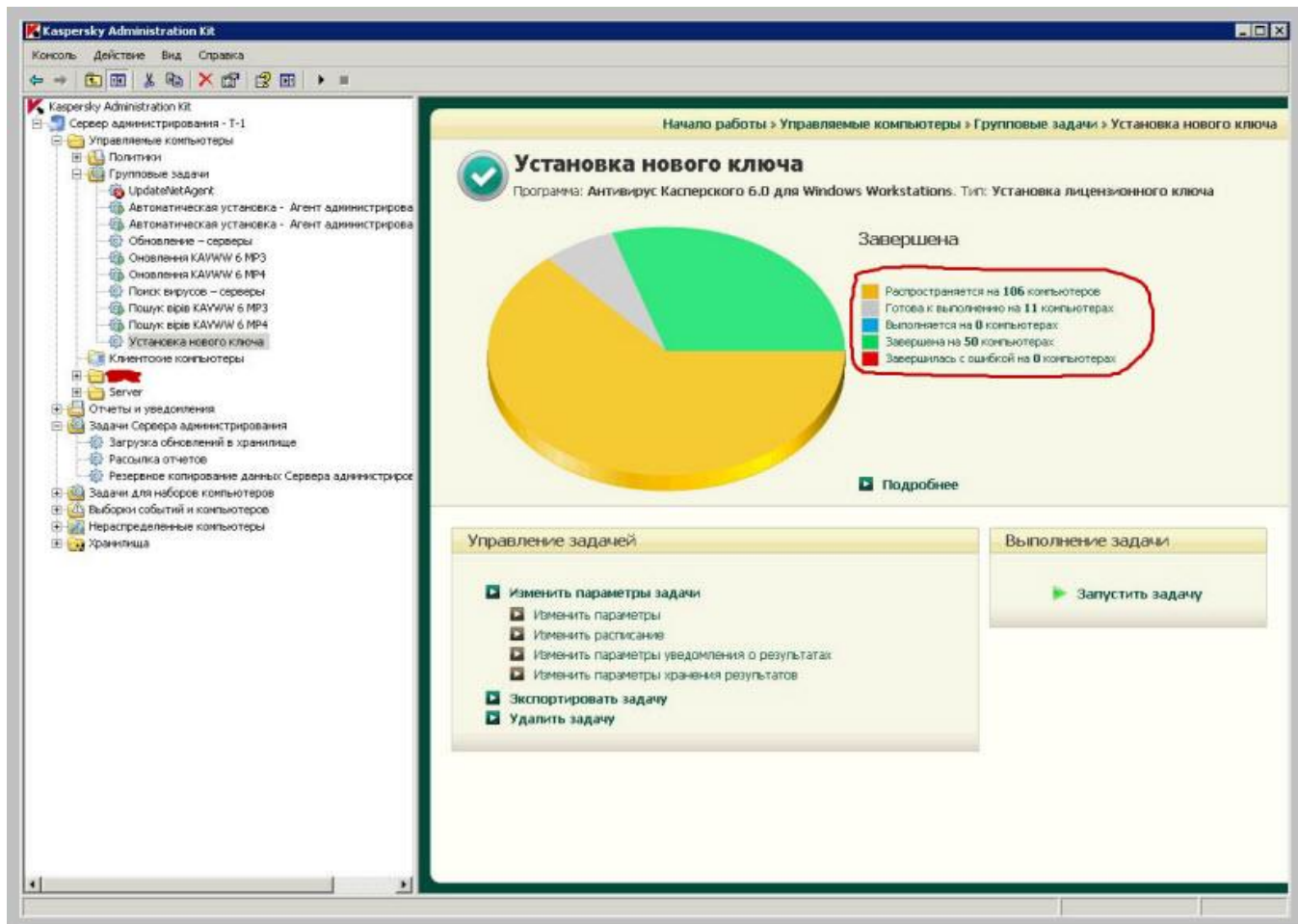
Обратите внимание, как все красочно и наглядно представлено! Просто так – глаза и душа радуются ☺

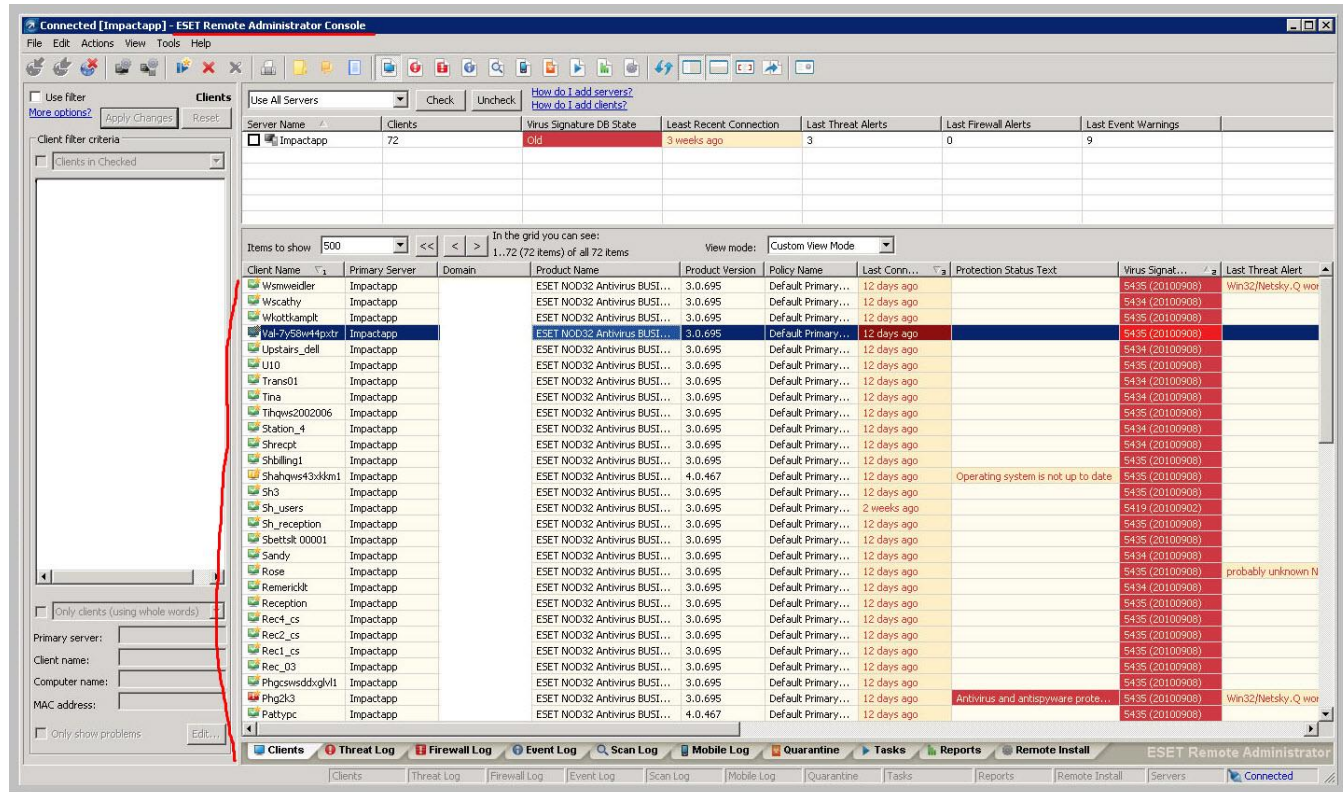
А вот – одна из выборок наших рабочих компьютеров. Обратите внимание на количество ПК, указанное в левом нижнем углу.



Это – не все компьютеры нашей рабочей сети, но – большая их часть.

А на скриншоте ниже я, с помощью созданной перед этим групповой задачи, устанавливаю на компьютеры сети новый ключ лицензии, вместо заканчивающегося.





Здесь с лицензированием – проще (для человека славянской национальности 😊), но как-то мне не удобно было работать с интерфейсом данного программного решения.

Также есть похожие решения от «Symantec» и «Dr.Web», но их я пока не тестировал.

Вот и все, собственно, что я хотел рассказать Вам сегодня о корпоративных антивирусах и особенностях их работы. В принципе, если хотите, можете задействовать подобное решение даже в том случае, если Ваша сеть – не очень большая (всего 10 или более компьютеров). Зато Вы все спланируете правильно изначально и не придется потом ничего переделывать. А на сегодня – все! 😊

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

До встречи в следующих уроках !