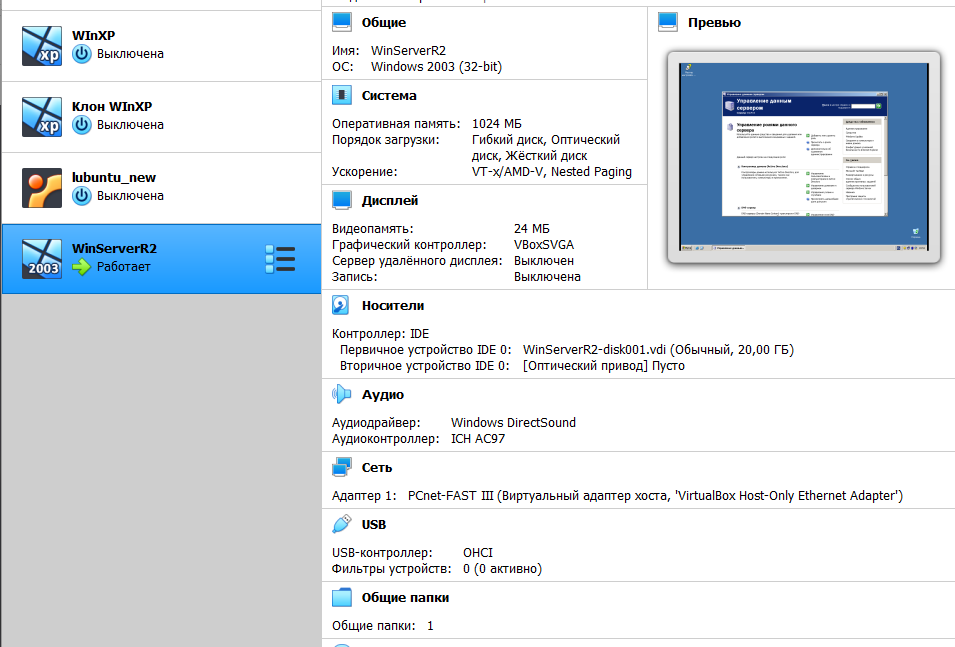
## **Изучение оснастки групповых политик  домена на базе Windows 2003 Server**

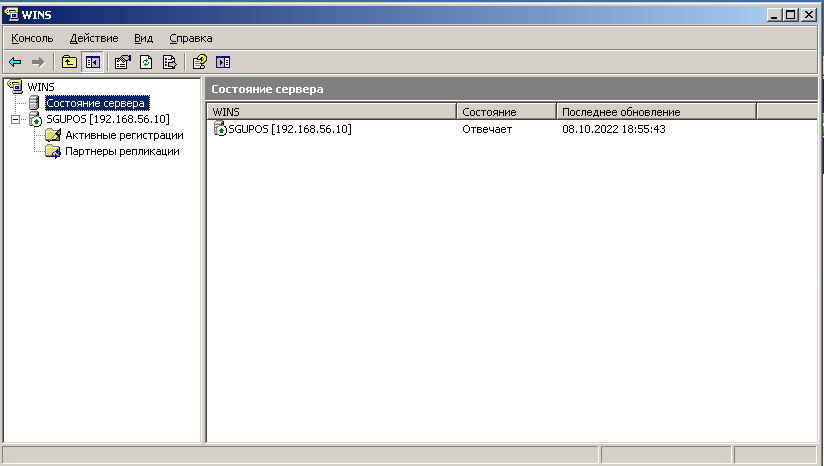
**Работу выполнил студент 431гр. Никитин А.В.**

Подключение в домен.

Первым делом импортировал машину и вошел в систему под пользователем Администратор с использованием пароля «123456»:

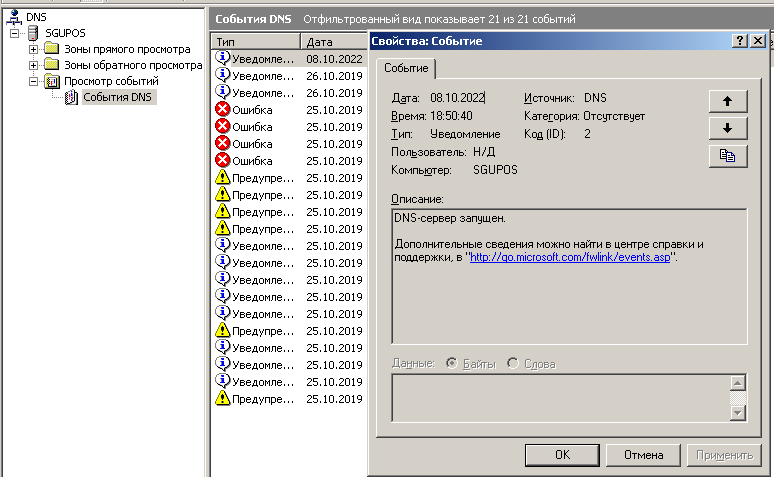


1. Поверить следующие серверы на Windows 2003 Server:

- Wins указан адрес доменного сервера:

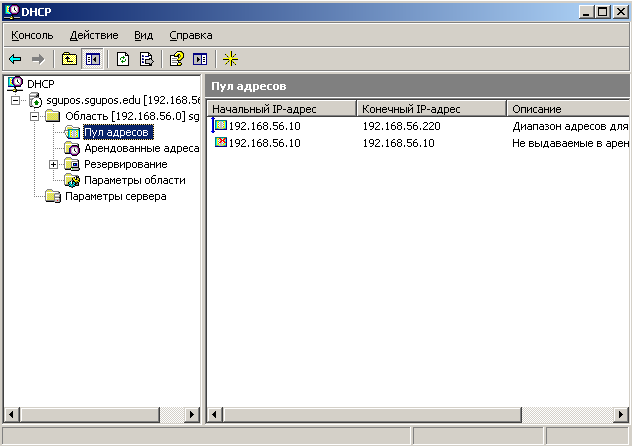
- DNS указан адрес доменного сервера

Указан адрес доменного сервера. Сервер запущен:

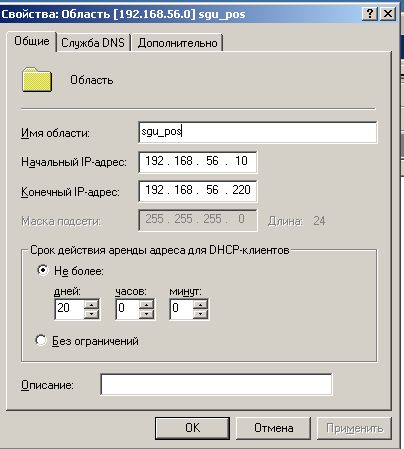


- DHCP указан адрес доменного сервера, создать область раздачи адресов 192.168.56.10 – 192.168.56.220 маска 24 аренда адреса на 20 дней

Выставил нужный диапазон адресов (изначально конечный IP-адрес был 192.168.56.200):

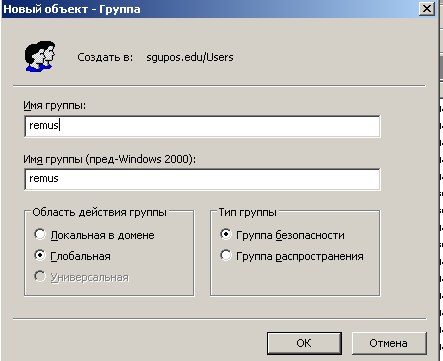


Также выставил максимальный срок аренды в 20 дней:

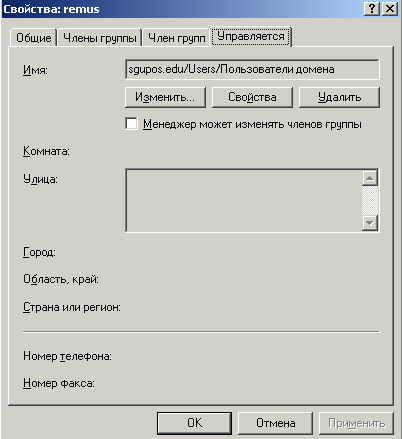


1. В пользователях Active Directiry создать группу remus, подчиненную группе Пользователи

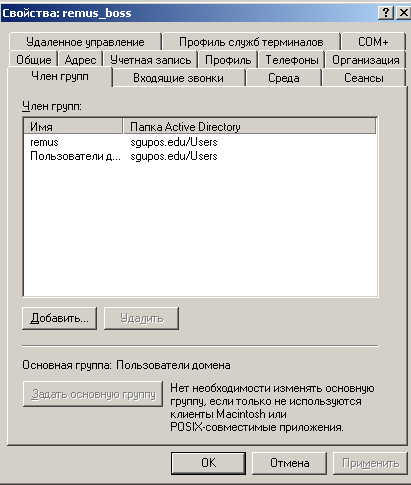
Создал группу:



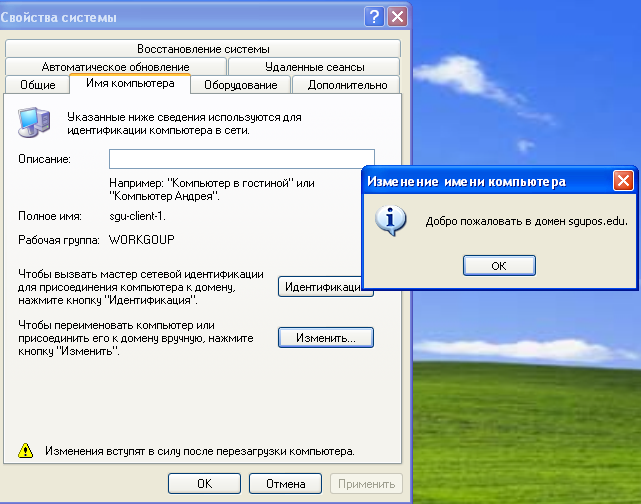
И сделал ее подчиненной группе Пользователи домена:



В пользователях Active Directiry создать пользователя remus\_boss и включить в группу remus

Создал пользователя remus\_boss и включил его в группу remus:

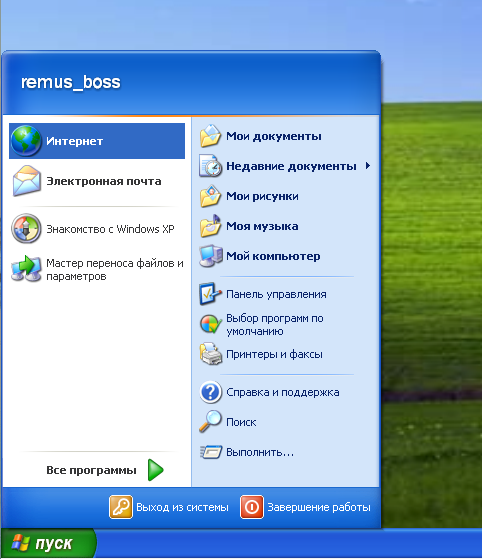
1. В Windows XP изменить идентификацию компьютера указав его членом домена SGUPOS.EDU. При этом для идентификации пользователя использовать встроенную в домен учетную запись Администратор (у которой устанавливали пароль)

 После добавления компьютера в домен, изменилось окно входа в систему:

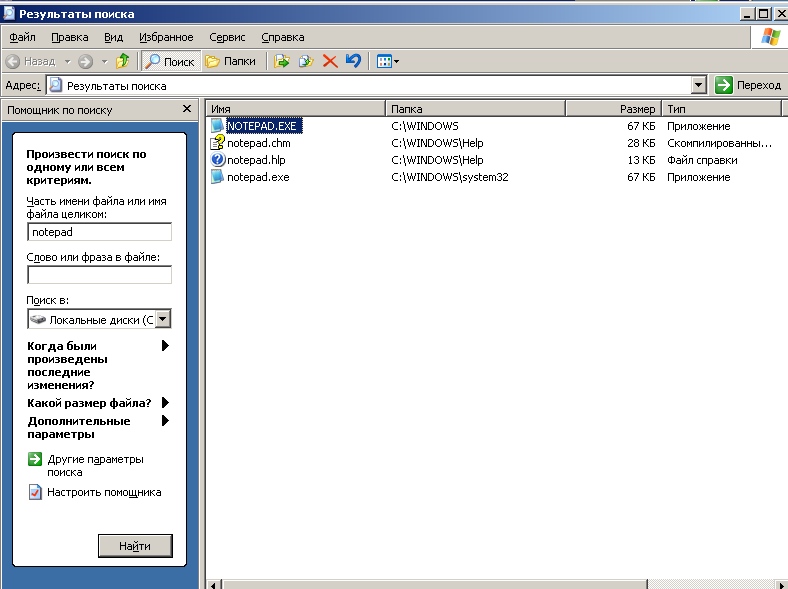


1. В случае успешного включения компьютера в домен – войти в систему под именем remus\_boss

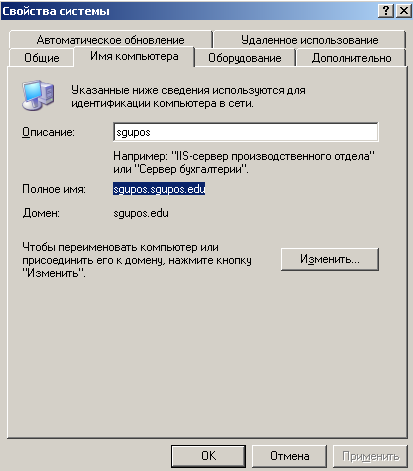
Входим в систему под пользователем remus\_boss:



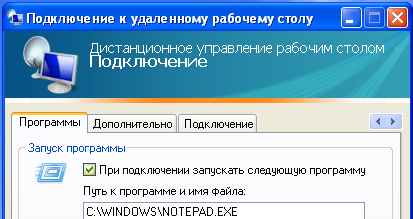
1. Создать файл .rdp для запуска удаленного рабочего стола на сервере с автоматическим запуском одного-единственного приложения Notepad.exe

Notepad.exe расположен по адресу C:\WINDOWS\NOTEPAD.EXE:

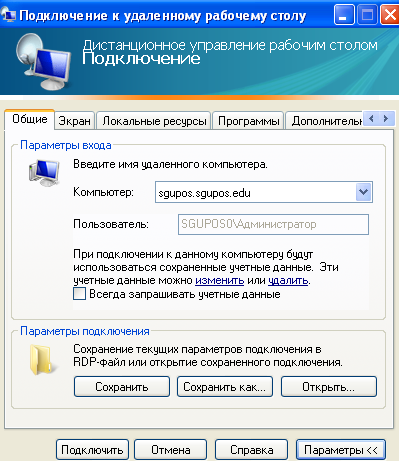
Полное имя компьютера, к которому будем подключаться:

Выполнил команду **mstsc.exe** для создания файла для подключения к удаленному рабочему столу.

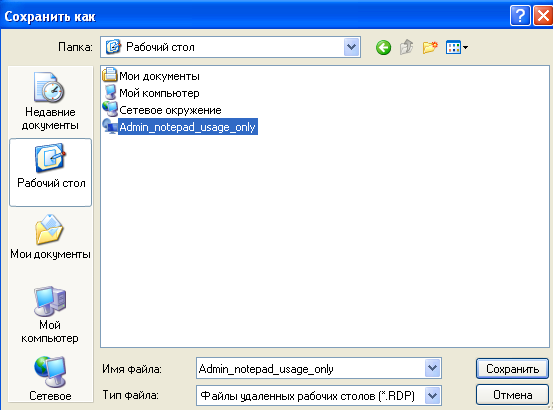
Ввел собранную информацию:



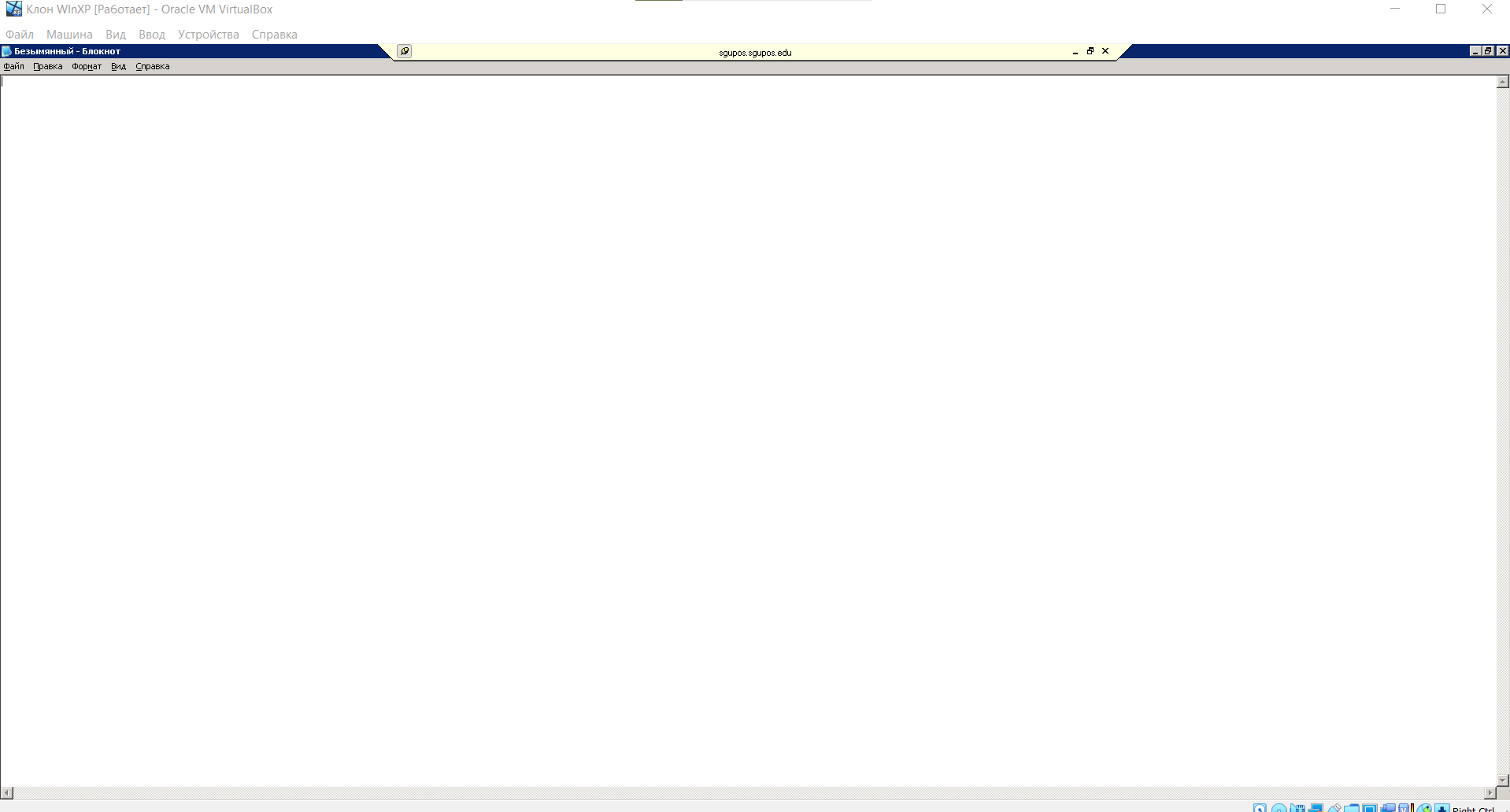
Компьютер, к которому будет выполнено подключение:



Создал файл rdp:



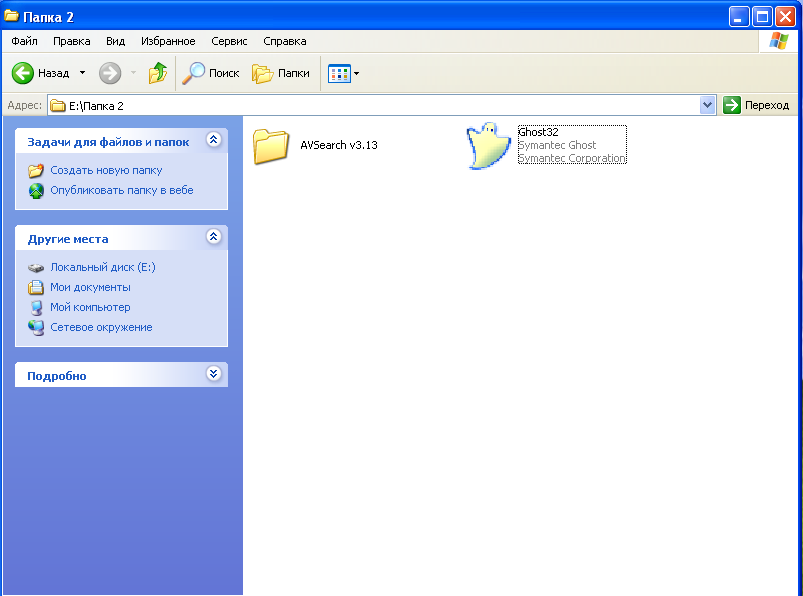
И при его открытии выполнено подключение, а также открыта программа notepad:



1. Настройка групповых политик безопасности

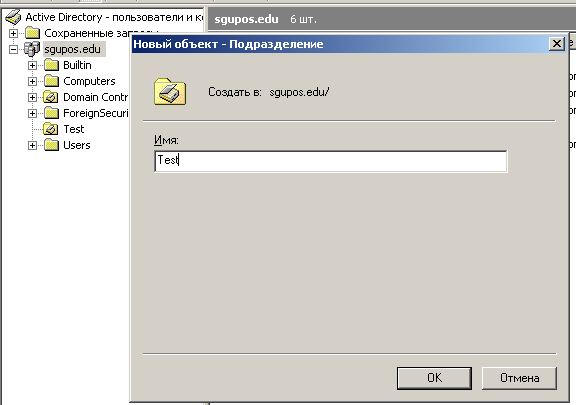
- Предварительно необходимо создать на логическом диске D: компьютера пользователя два каталога, куда поместить две программы, позволяющие выполнять запуск без инсталляции. Для этого можно использовать, например Ghost и AVSearch v3.13 (из PrgEx), скопировав их в одну папку на [D:\](file:///D:/).

Создал на диске 2 каталога (Папка 1 и Папка 2) и добавил в них предложенные программы:

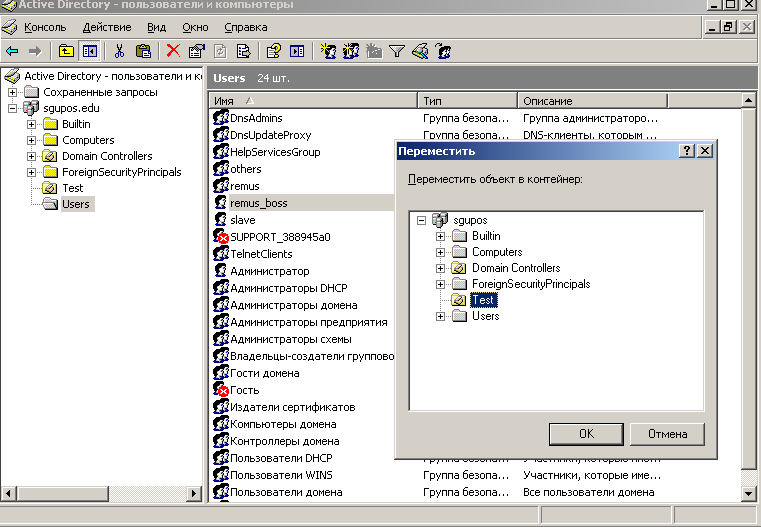


1. Политика ограничения запуска программ для
   1. Создать новую организационную единицу (OU) Подразделение вне группы Users (применяем контекстное меню на  имени домена SGUPOS.EDU). Пусть OU называется Test.

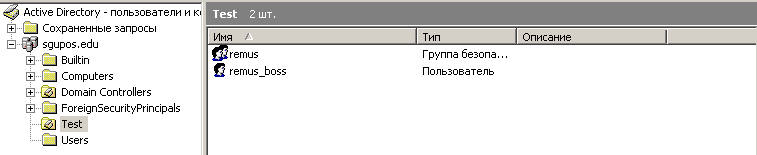
Создал подразделение Test:



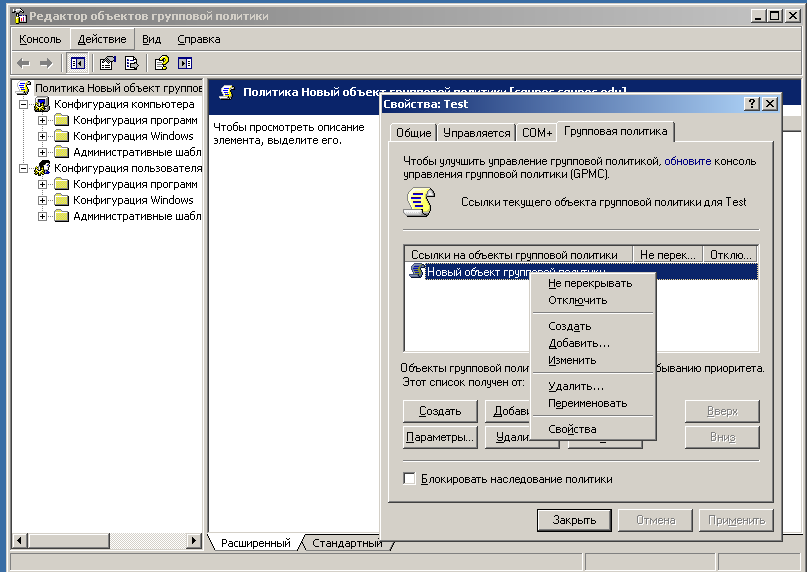
* 1. В эту OU переместить группу remus и пользователя remus\_boss.



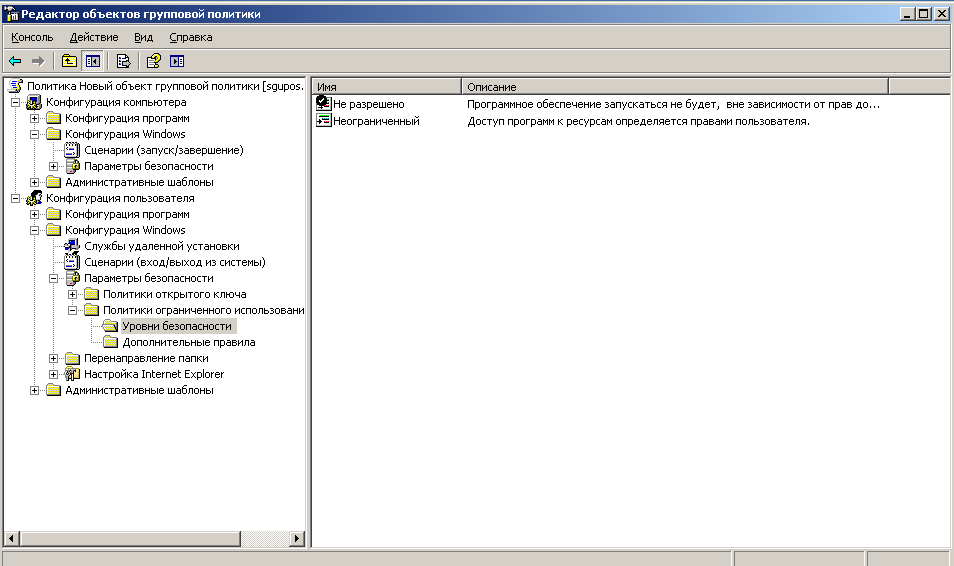
Группа и пользователь оказались в подразделении:



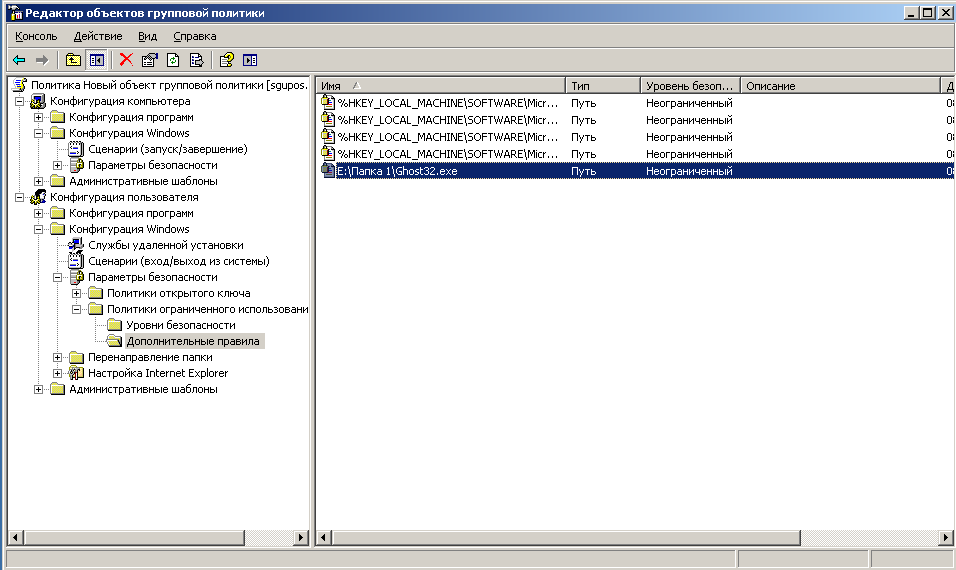
* 1. Обратиться к свойствам OU Test (контекстное меню), выбираем закладку групповая политика и создаем новую групповую политику. Далее его нужно настроить (изменить). Получаем новое окно оснастки mmc для gpedit.msc



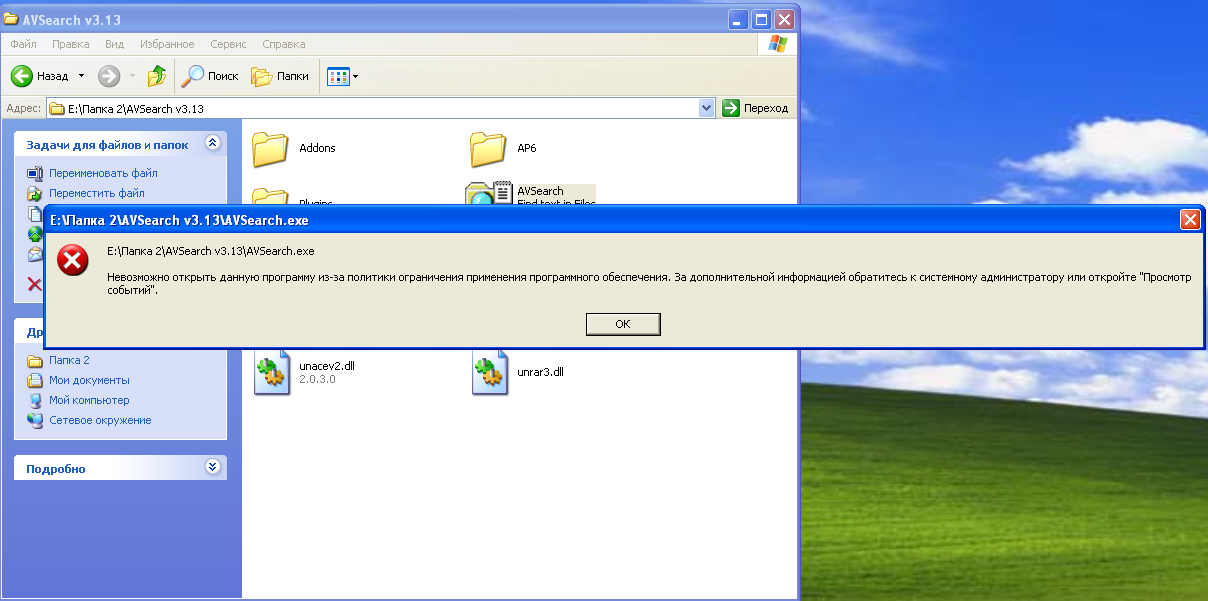
* 1. Создать Политику ограниченного использования программ, запретив все запуски кроме Ghost. Проверить работу на обоих программах и какой-либо стандартной программе. Посмотрите содержимое ключей ветви HKEY\_CURRENT\_USER\Software\Policies\Microsoft\Windows\Safer\CodeIdentifiers\262144\Paths на машине пользователя.

Запретим все запуски программ, установив по умолчанию не разрешение запуска программ:

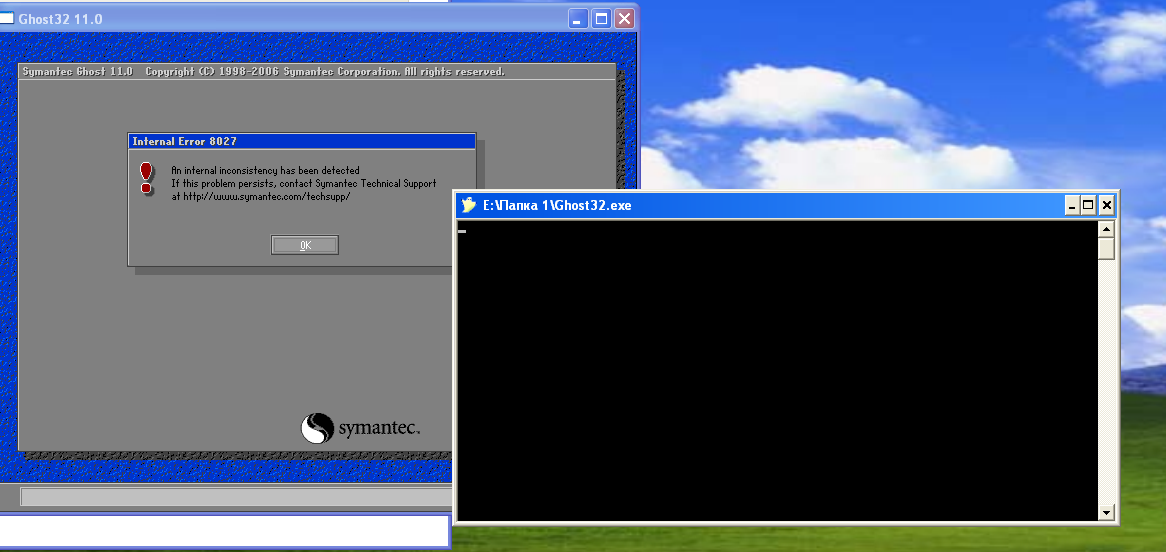
И разрешим использование программы Ghost:



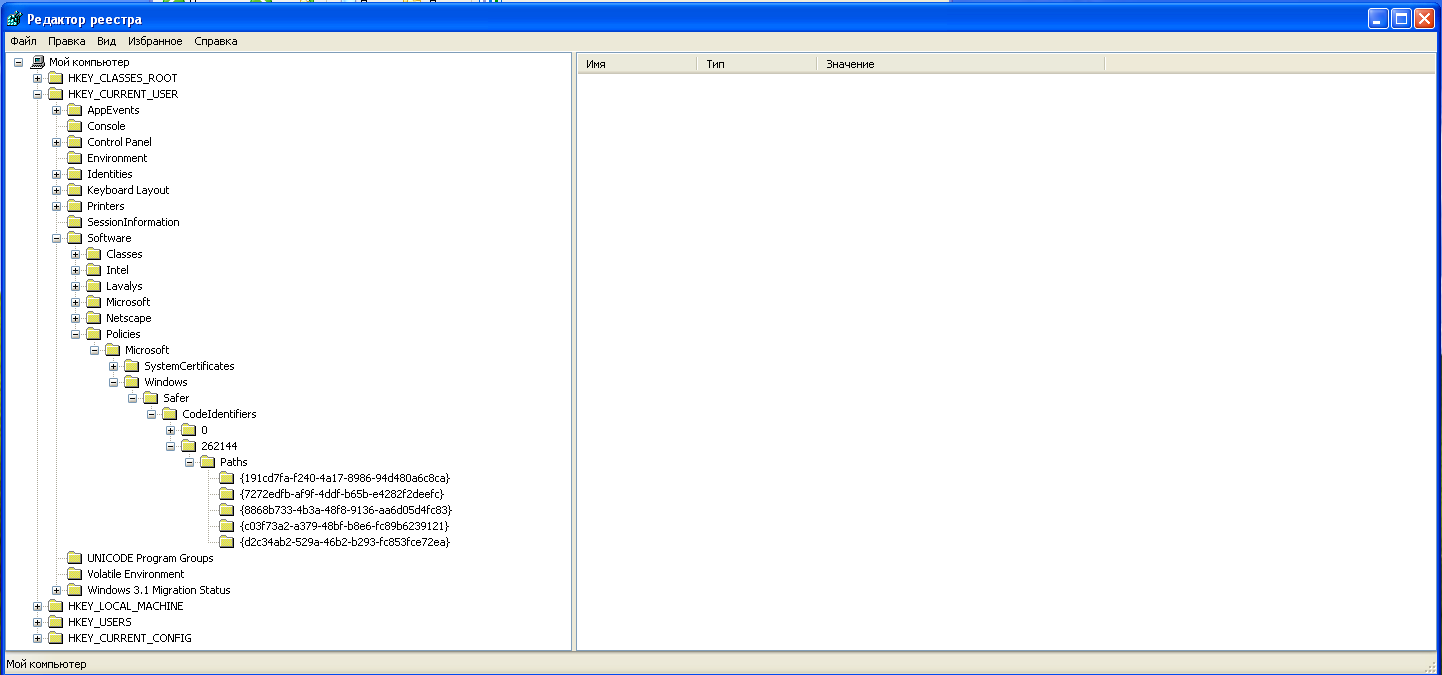
Никакие программы, кроме Ghost даже в Папке 2 запустить не получится:



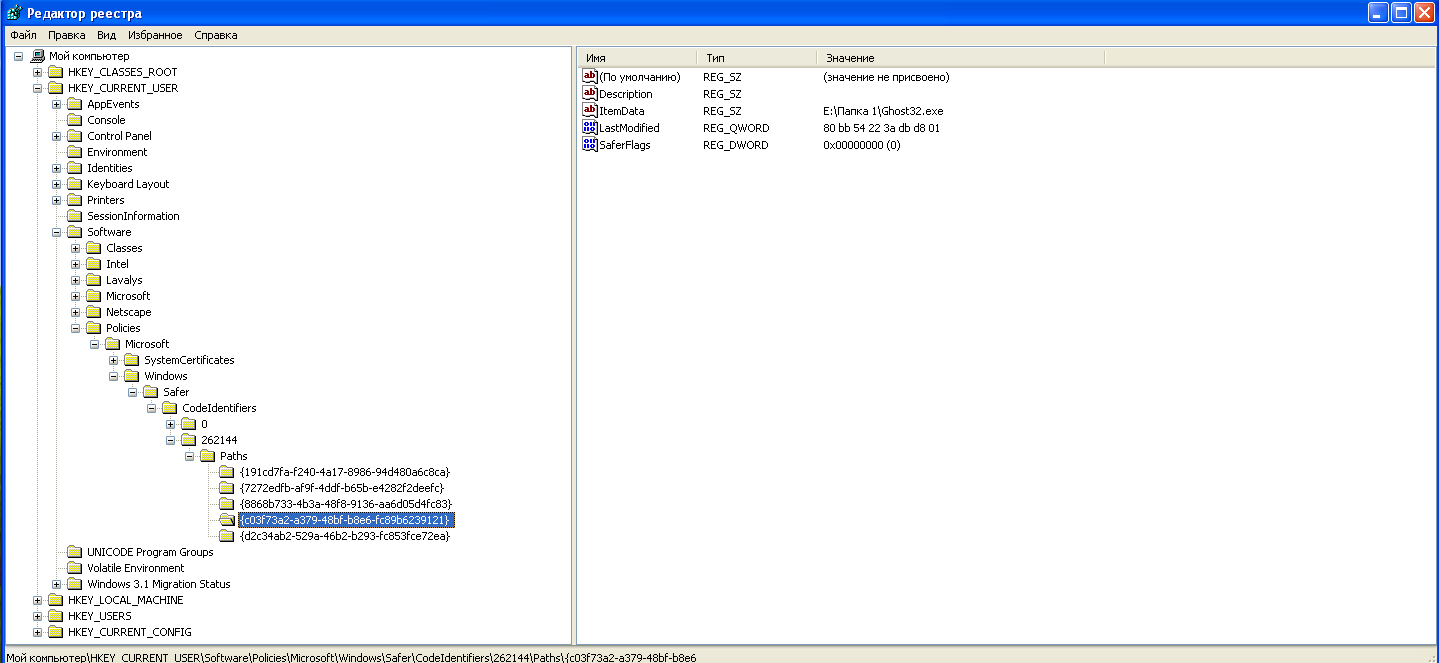
Программа Ghost запустилась и сообщения об ошибке не было:

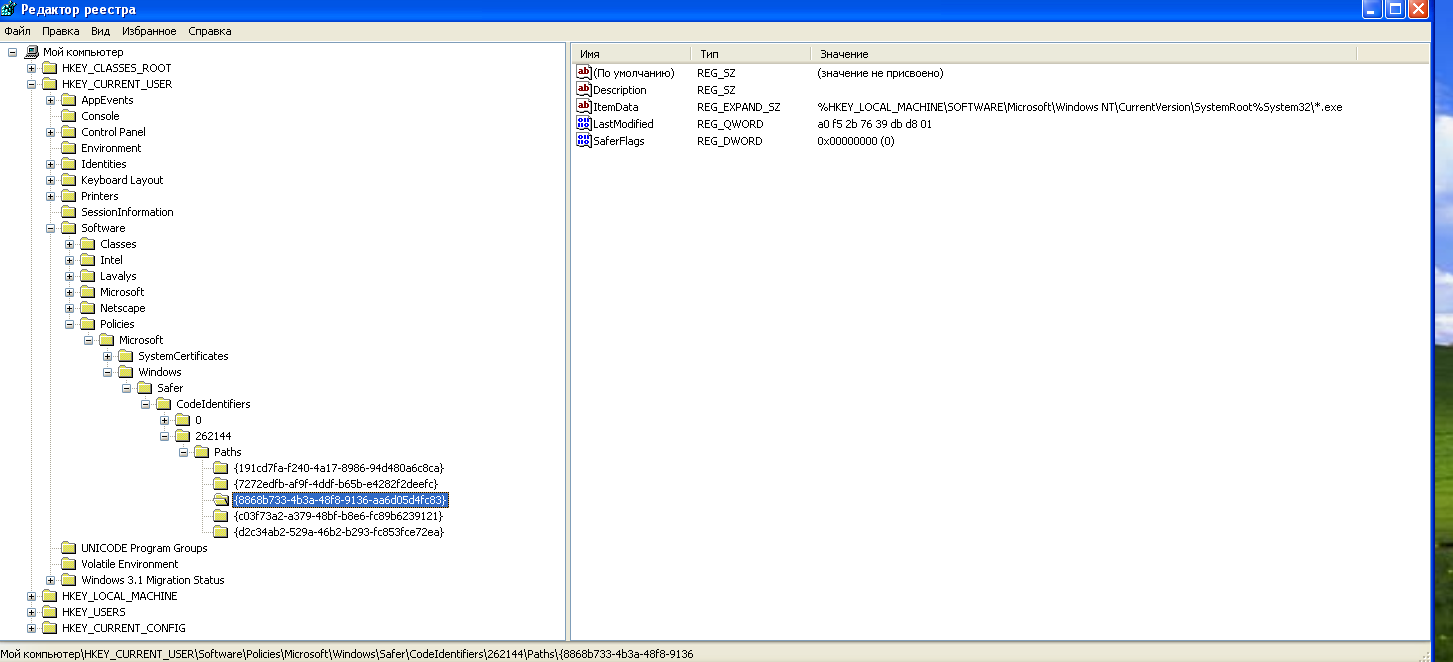


Далее с помощью команды **regedit** зашел в редактор реестра и открыл предложенный путь:

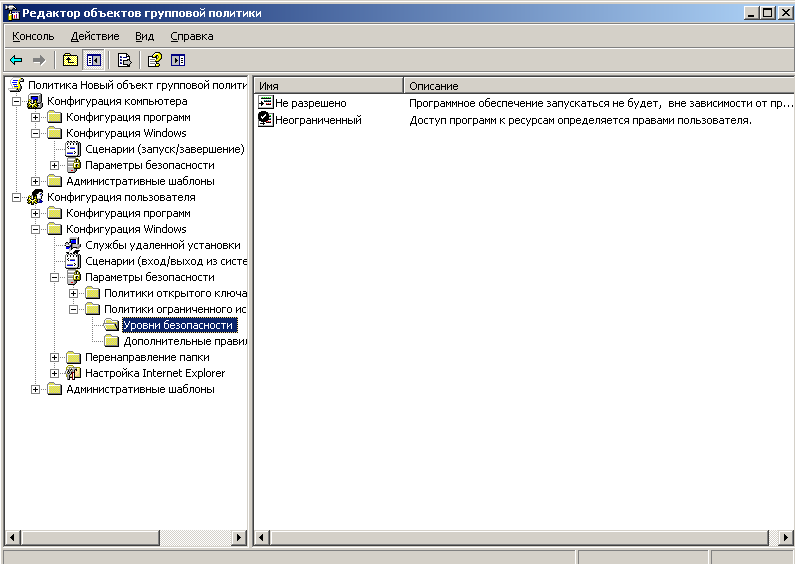


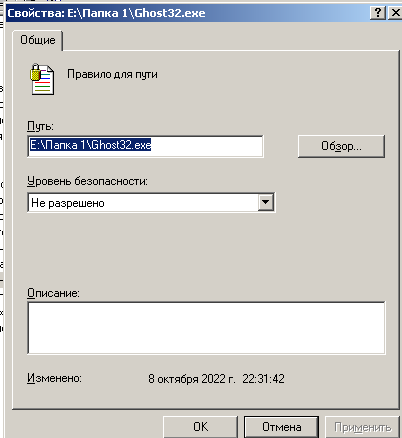
Разрешение на использование программы Ghost из Папки 1:



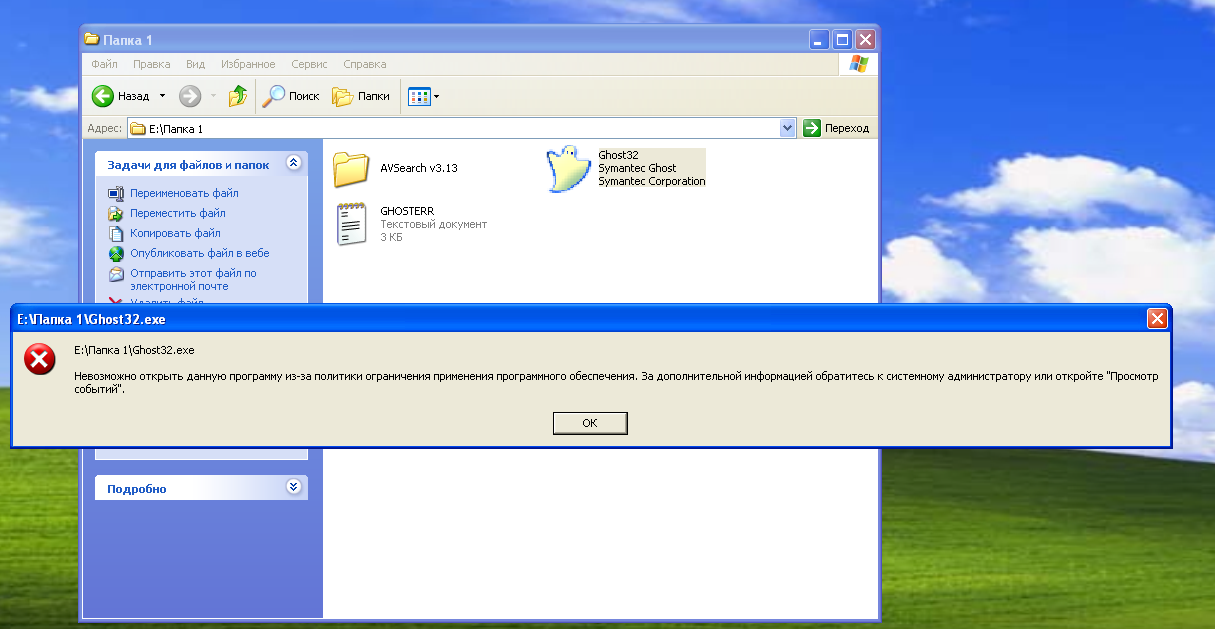
Разрешение на использование всех остальных исполняемых файлов:

* 1. Создать Политику ограниченного использования программ, разрешив все запуски, кроме Ghost. Проверить работу на обоих программах и какой-либо стандартной программе. Как изменилось содержимое ключей ветви HKEY\_CURRENT\_USER\Software\Policies\Microsoft\Windows\Safer\CodeIdentifiers\262144\Paths на машине пользователя?

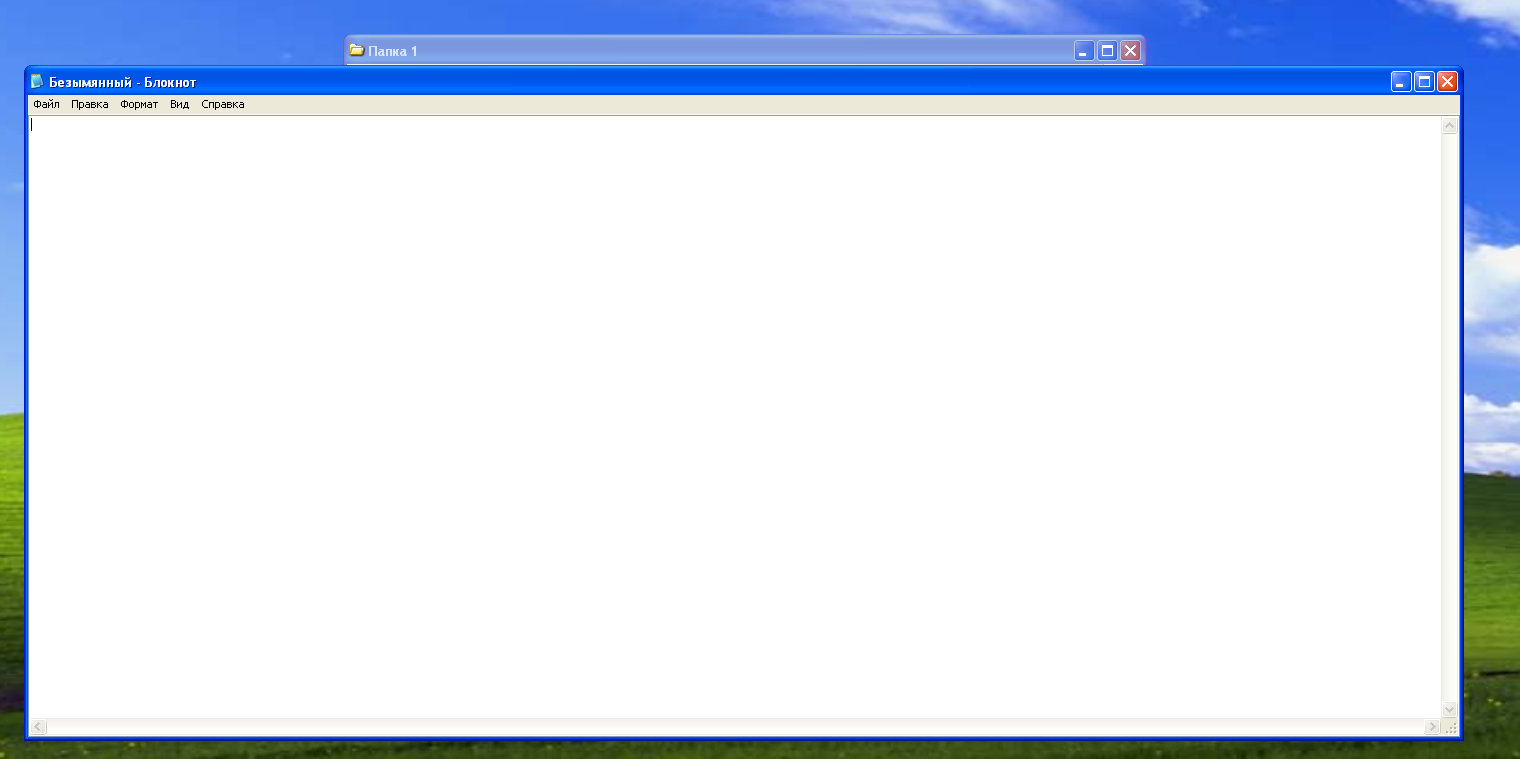
Вернем значение на неограниченный:

А запуск Ghost запретим:

Теперь программу запустить не получилось:

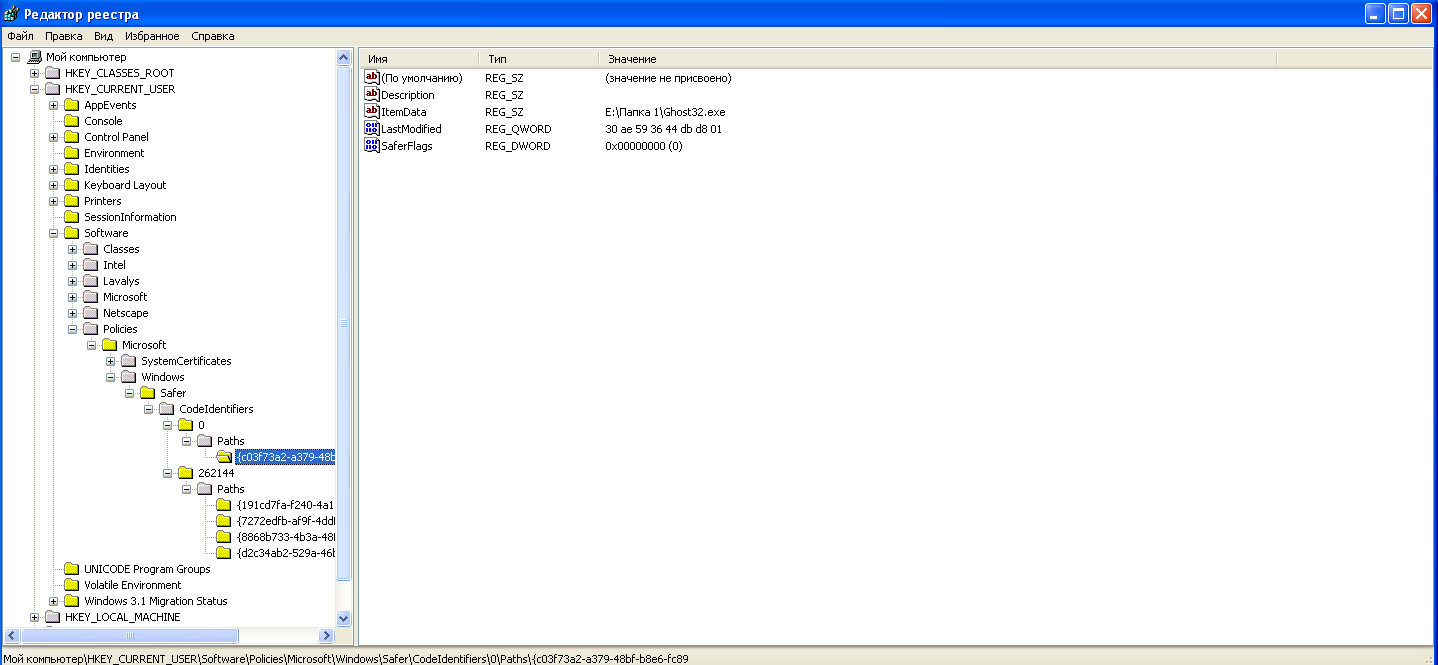


А вот стандартный блокнот открылся:



Теперь просмотрим, как изменились значения в реестре:

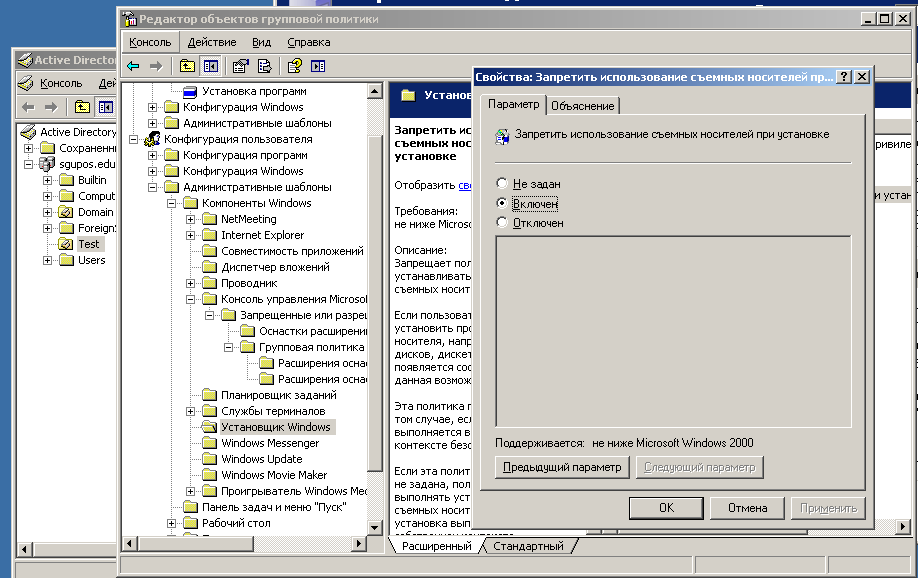
Видно, что запуск Ghost запрещен

Как отразится на уровне безопасности системы решение по ограничению запуска программ методом «запретить все» и разрешить запуск всех программ из некоторого пользовательского каталога?

Если запретить запуск всех программ запретить из некоторого каталога, то в зависимости от того, как был выдан запрет, данные программы могут не запускаться как в конкретном каталоге так и во всех остальных. Незапуск программы по каталогу реализуется путем прописывания ограничение на использовании программы с помощью пути к ней. А если требуется, чтобы данная программа не запускалась вообще во всех каталогах, то требуется использование захэшированного пути к программе.

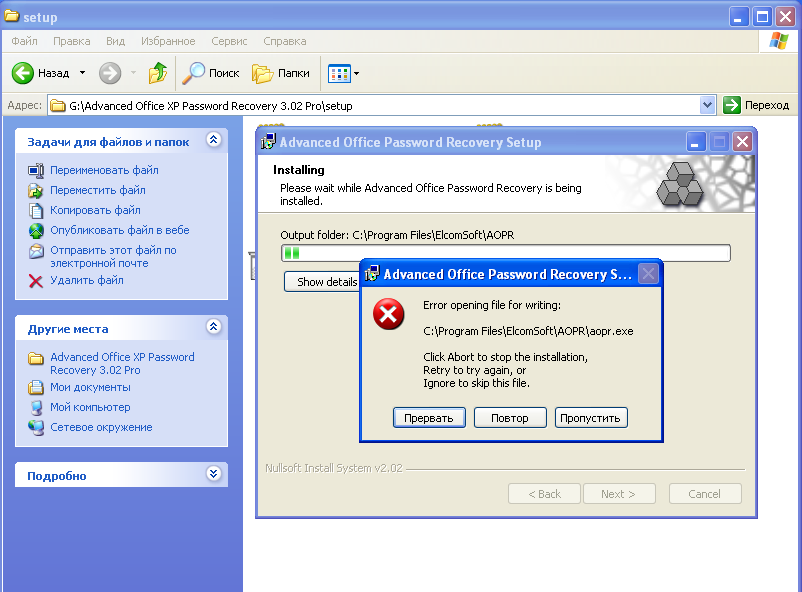
Если использовать “запретить все”, то никакие программы за исключением выбранных в политике не будут запускаться.

1. Политика ограничения использования сменных носителей
   1. Запретить установку программ для группы remus со съемных носителей. Проверить, используя flash-носитель и инсталляционный пакет Advanced Office XP Password Recovery 3.02 Pro (из PrgEx). Использовать для этого Группу Административных шаблонов.

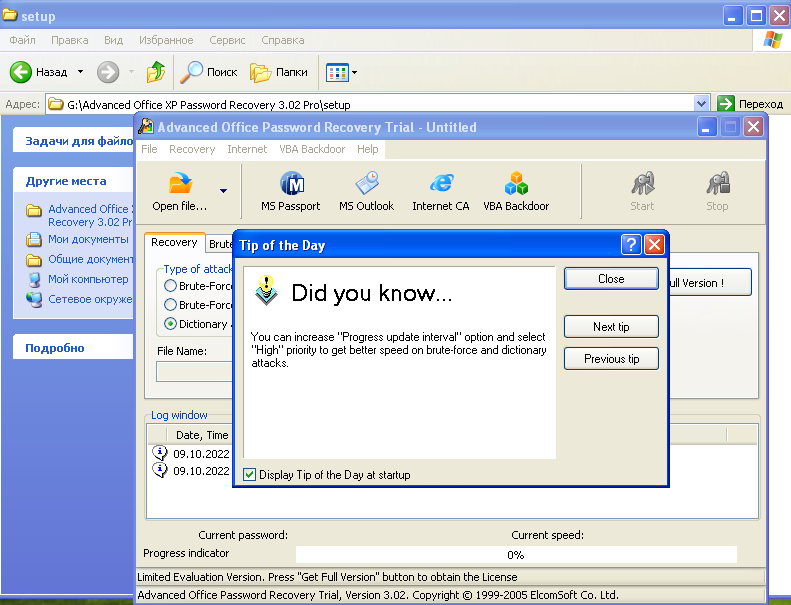


Теперь проверим, работает ли запрет.

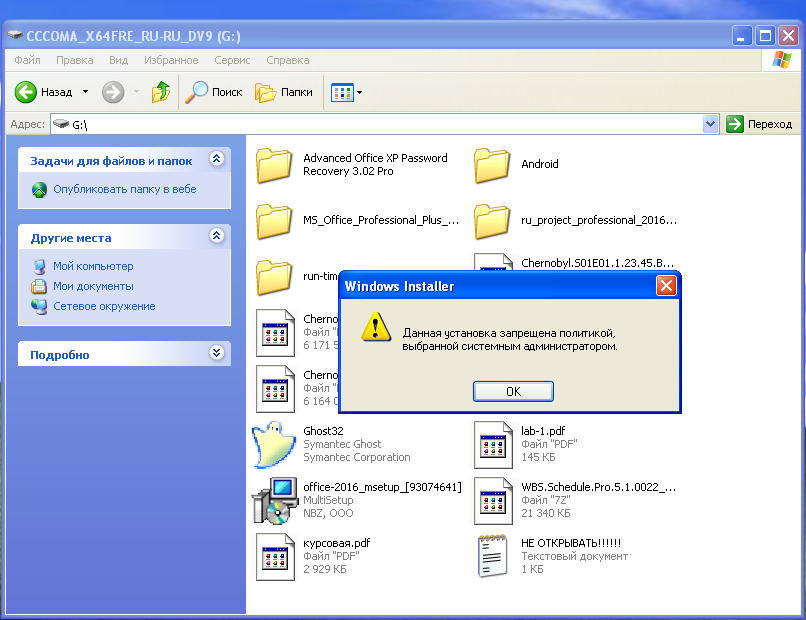
Установка программы не получается:



Попробовал установить программу на исходной неклонированной машине, которая не подключена к домену (удачно):

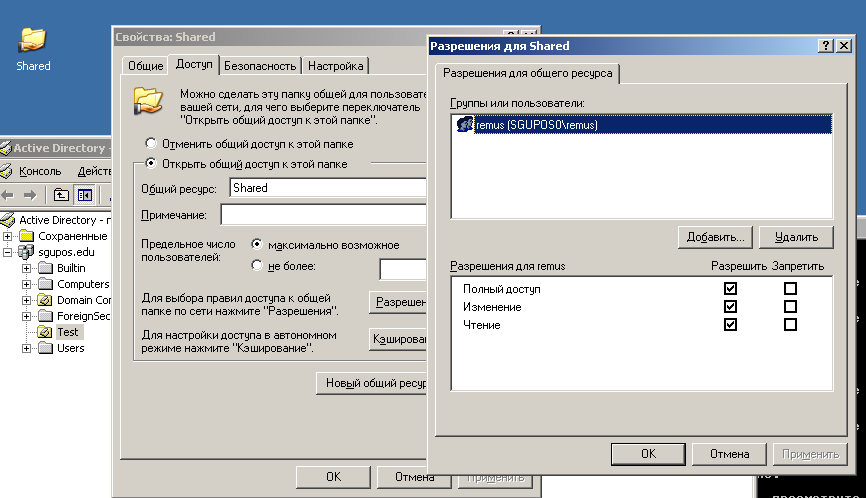


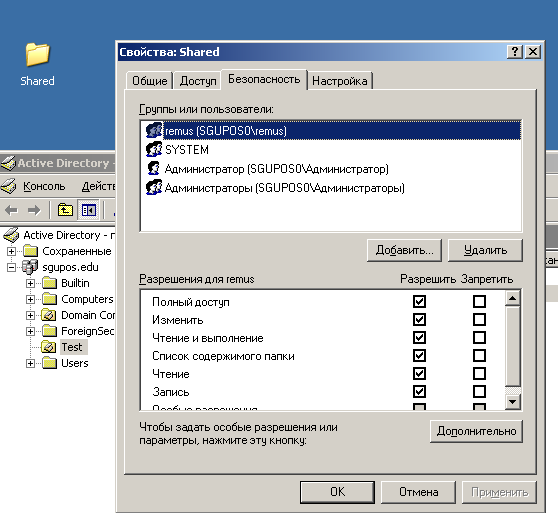
С msi файлом возникает следующая ошибка:



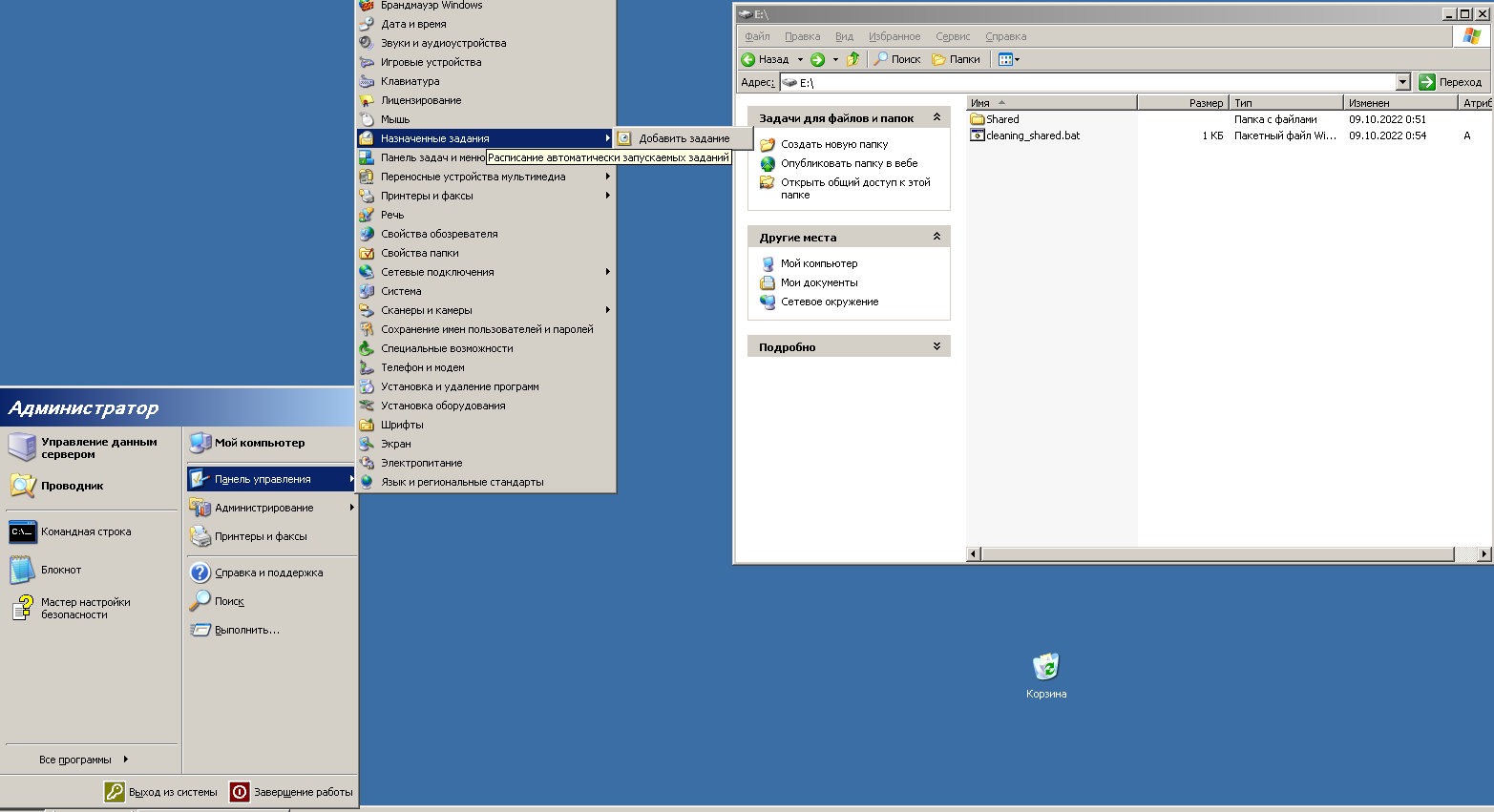
1. Создать общую папку на сервере. Разрешить доступ к ней всем пользователям группы remus. Задать с использованием планировщика заданий процедуру очистки этой папки в 00:00 каждых суток. Проверить работу данного механизма защиты информации.

Создал общую папку Shared и добавил к ней группу remus:

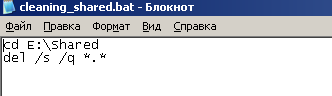




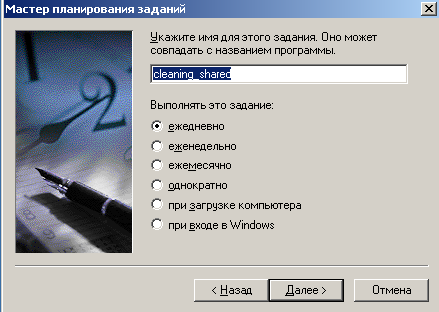
Открыл планировщик заданий:



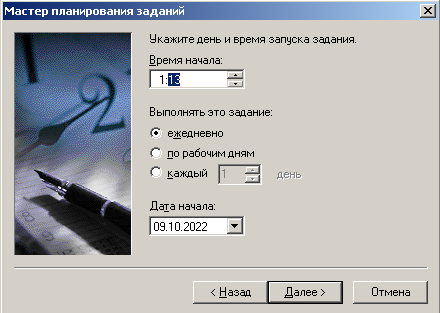
Скрипт, благодаря запуску которого будет очищаться папка Shared, расположенная на диске [E](file:///E:/):



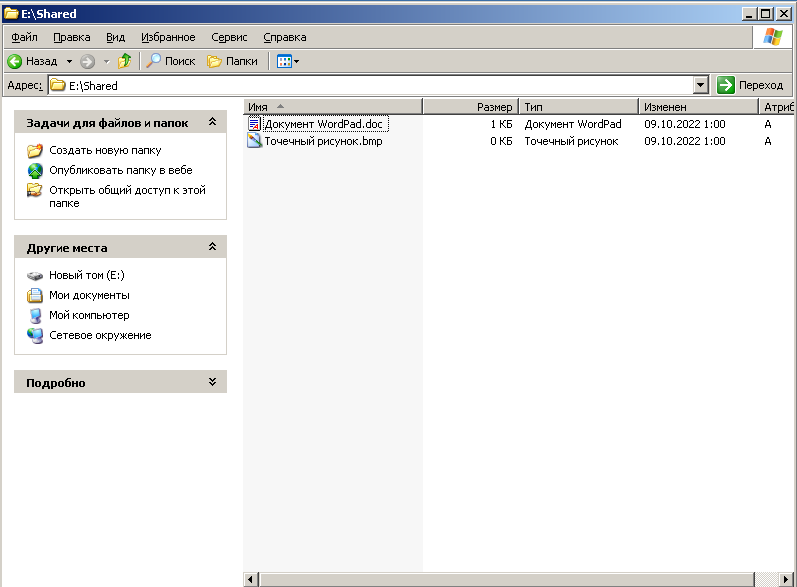
Выбрал написанный скрипт в качестве задания:



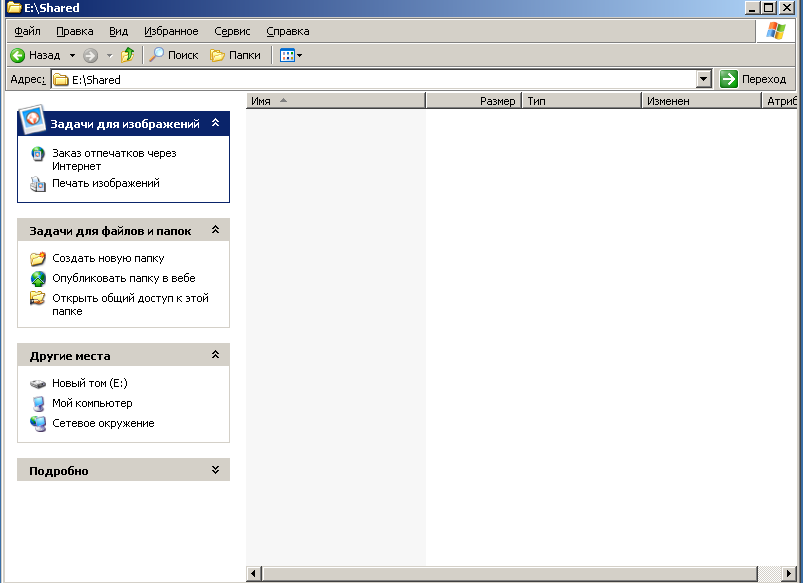
Составил расписание:



Папка до очистки:

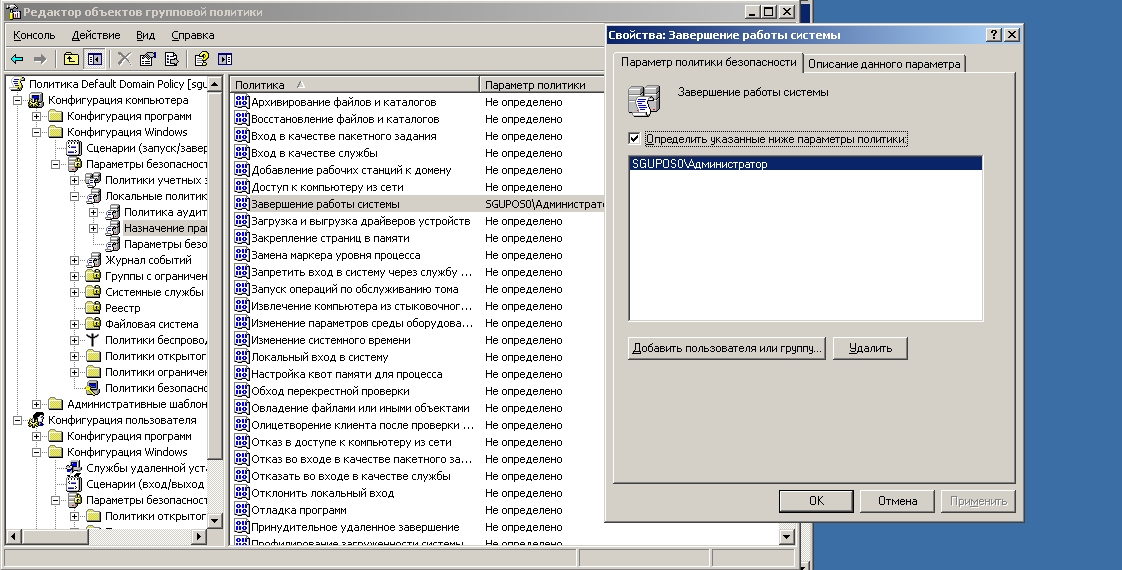


Папка после выполнения задания стала пустой:



1. Запретить всем пользователям кроме Администратора выключение компьютера (см. политики безопасности домена)

Назначил Администратору право завершения работы системы в политике Default Domain Policy:



## **Централизованное развёртывание программ**

Можно использовать групповую политику для распространения программы с помощью следующих методов:

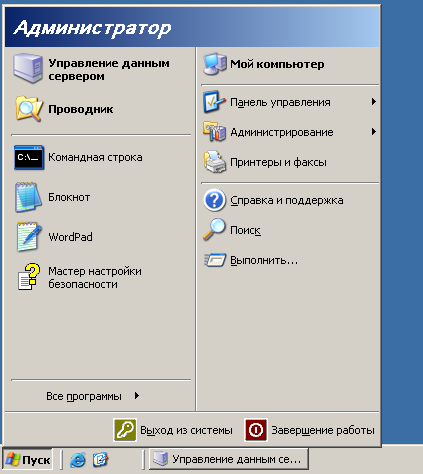
* Назначение программного обеспечения  
  Распространение программы можно назначить пользователям или компьютерам. Если программа назначения пользователю, устанавливается при входе пользователя в систему. При первом запуске программы установка завершается. Если назначить программу на компьютер, установки при загрузке компьютера, и он доступен всем пользователям, входящим в систему на компьютере. При первом запуске программы установка завершается.
* Публикации программного обеспечения  
  Можно опубликовать программу распространения для пользователей. При входе пользователя в систему, опубликованной программе отображается в диалоговом окне **Установка и удаление программ** и могут устанавливаться оттуда.

### **Создание точки распространения**

Для публикации или назначения компьютерной программы, необходимо создать на сервере публикации точки распространения.

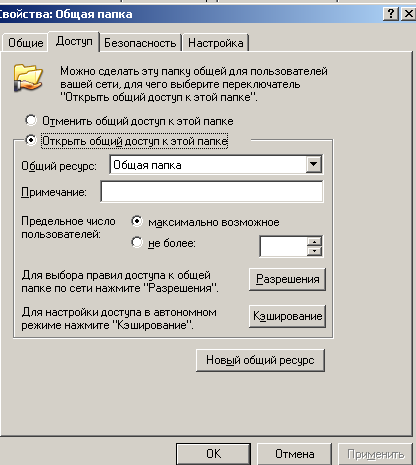
1. Войдите на сервер с правами администратора.

Вошел на сервер с правами администратора:

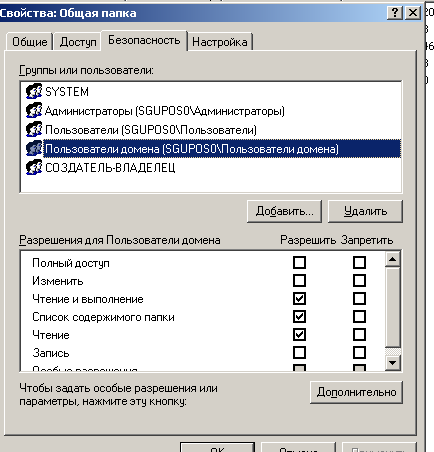


1. Создайте общую сетевую папку, где будет размещен пакет установщика Microsoft Windows (MSI-файл), который необходимо распространять.

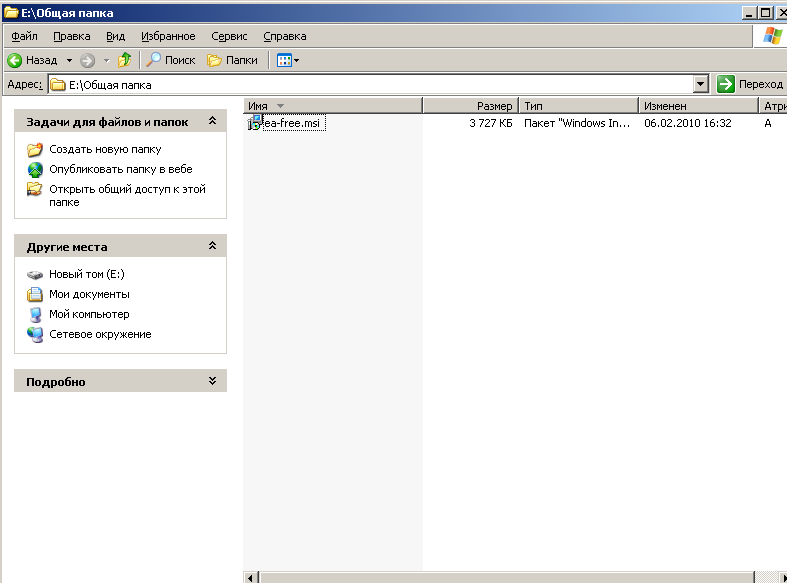
Создал общую сетевую папку:



1. Установить разрешения для общего ресурса, чтобы разрешить доступ к установочному пакету.

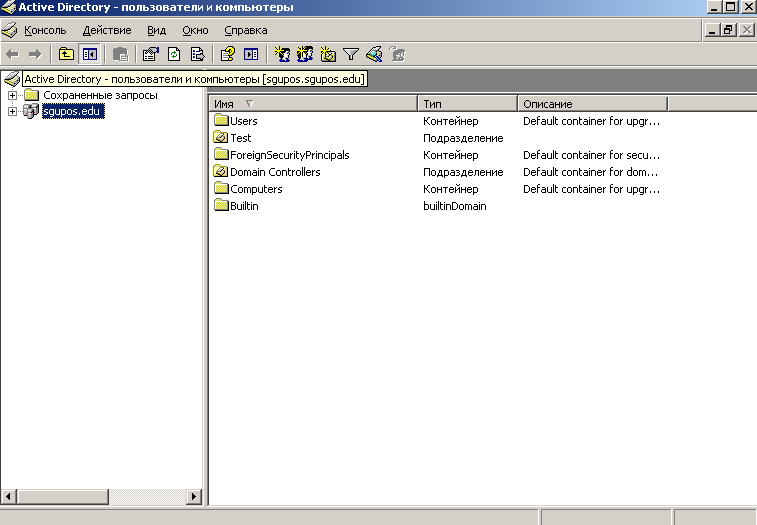
Затем установил разрешения для пользователей домена:

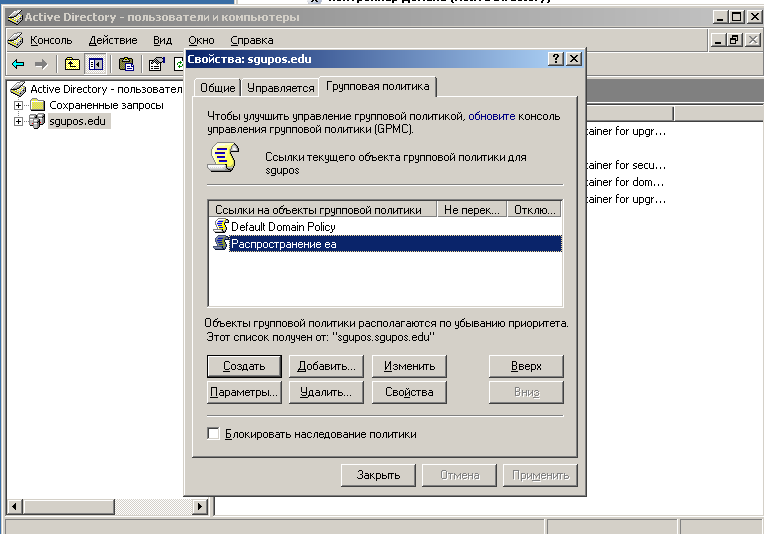
1. Скопируйте или установите пакет в точку распространения. Например для распространения Microsoft Office XP, запустите административную установку (setup.exe /a) для копирования файлов в точку распространения.



### **Создание объекта групповой политики**

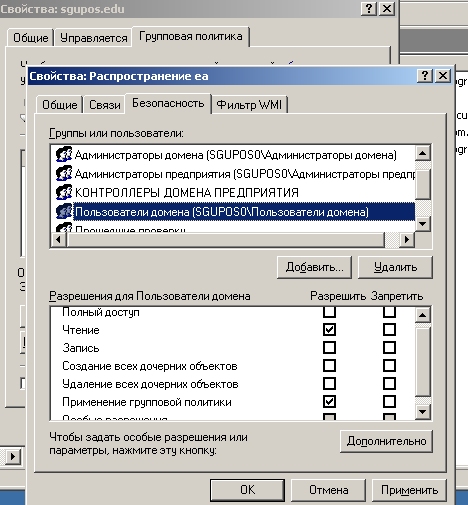
Чтобы создать объект группы политики (GPO) для распространения пакета программного обеспечения, выполните следующие действия:

1. Запустите оснастку "Active Directory — пользователи и компьютеры". Для этого нажмите кнопку **Пуск**, выберите пункт **Администрирование** и выберите команду **Active Directory — поль****зователи и компьютеры**.
2. В дереве консоли щелкните правой кнопкой мыши домен и выберите команду **Свойства**.
3. Откройте вкладку **Групповая политика** и нажмите кнопку **Создать**.
4. Введите имя для этой новой политики (например, Распространение Office XP) и нажмите клавишу ВВОД.



1. Выберите команду **Свойства** и откройте вкладку **Безопасность** .
2. Снимите флажок **Применить групповую политику** для групп безопасности, которые не требуется для применения этой политики.
3. Установите флажок **Применить групповую политику** для группы, которые требуется применить эту политику.
4. Когда закончите, нажмите кнопку **ОК**.

Добавил группу пользователи домена, а также отметил галочкой применение групповой политики, затем нажал кнопку применить, а также убедился, что для других пользователей или групп данная галочка не установлена и политика, следовательно, применяться не будет:

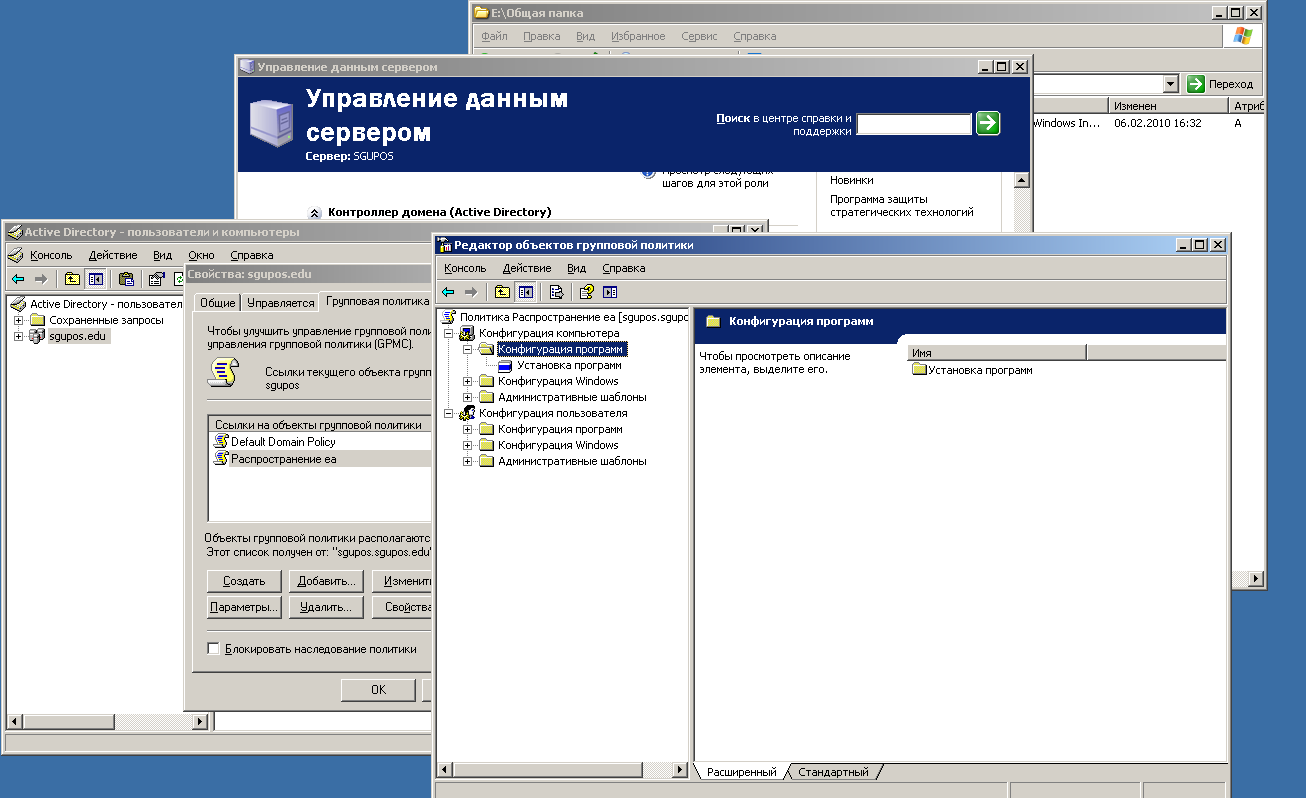


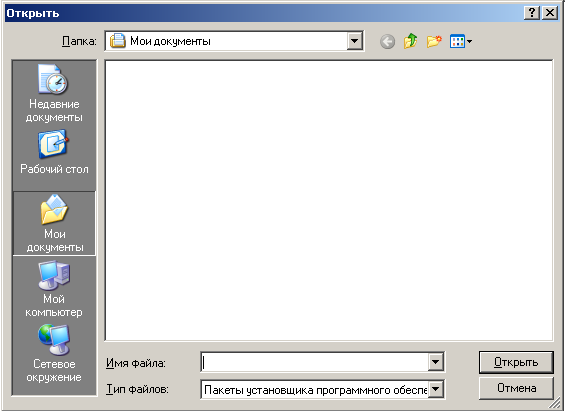
### **Назначение пакета**

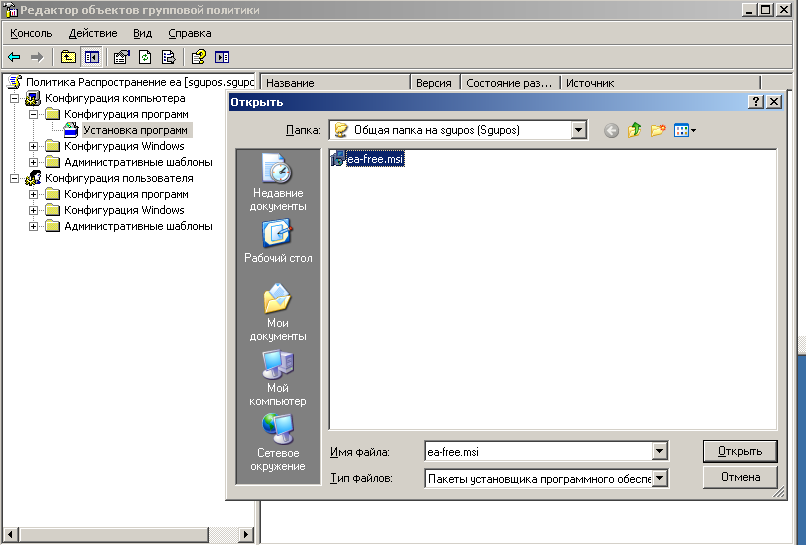
Чтобы назначить программу на компьютерах под управлением Windows Server 2003, Windows 2000 или Windows XP Professional, или для пользователей, вход на один из этих рабочих станций, выполните следующие действия: [щелкните здесь, чтобы показать или скрыть решения](https://support.microsoft.com/" \l "method3)

1. Запустите оснастку "Active Directory — пользователи и компьютеры". Для этого нажмите кнопку **Пуск**, выберите пункт **Администрирование** и выберите команду **Active Directory — пользователи и компьютеры**.
2. В дереве консоли щелкните правой кнопкой мыши домен и выберите команду **Свойства**.
3. Откройте вкладку **Групповая политика** , выберите нужную политику и нажмите кнопку **Изменить**.
4. В разделе **Конфигурация компьютера** разверните **Конфигурация программ**.

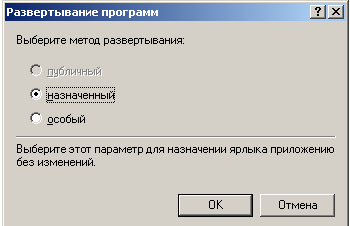
Проделал предложенные выше шаги:

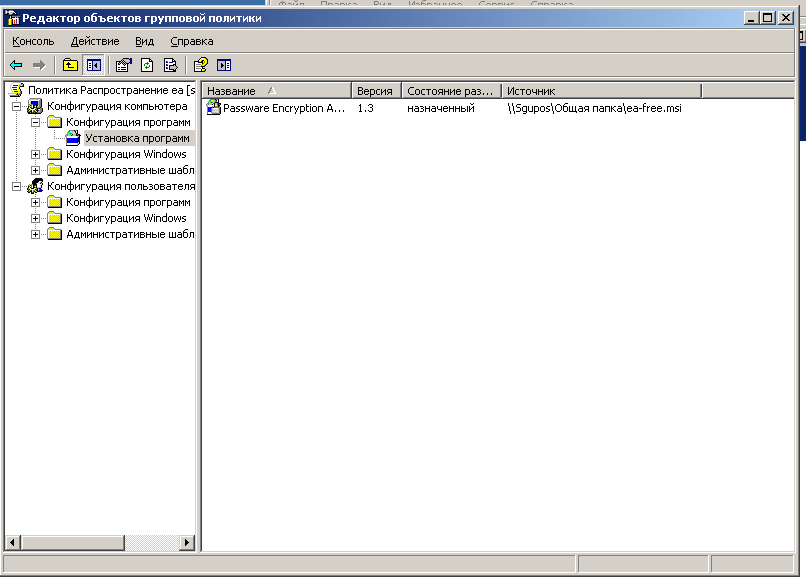


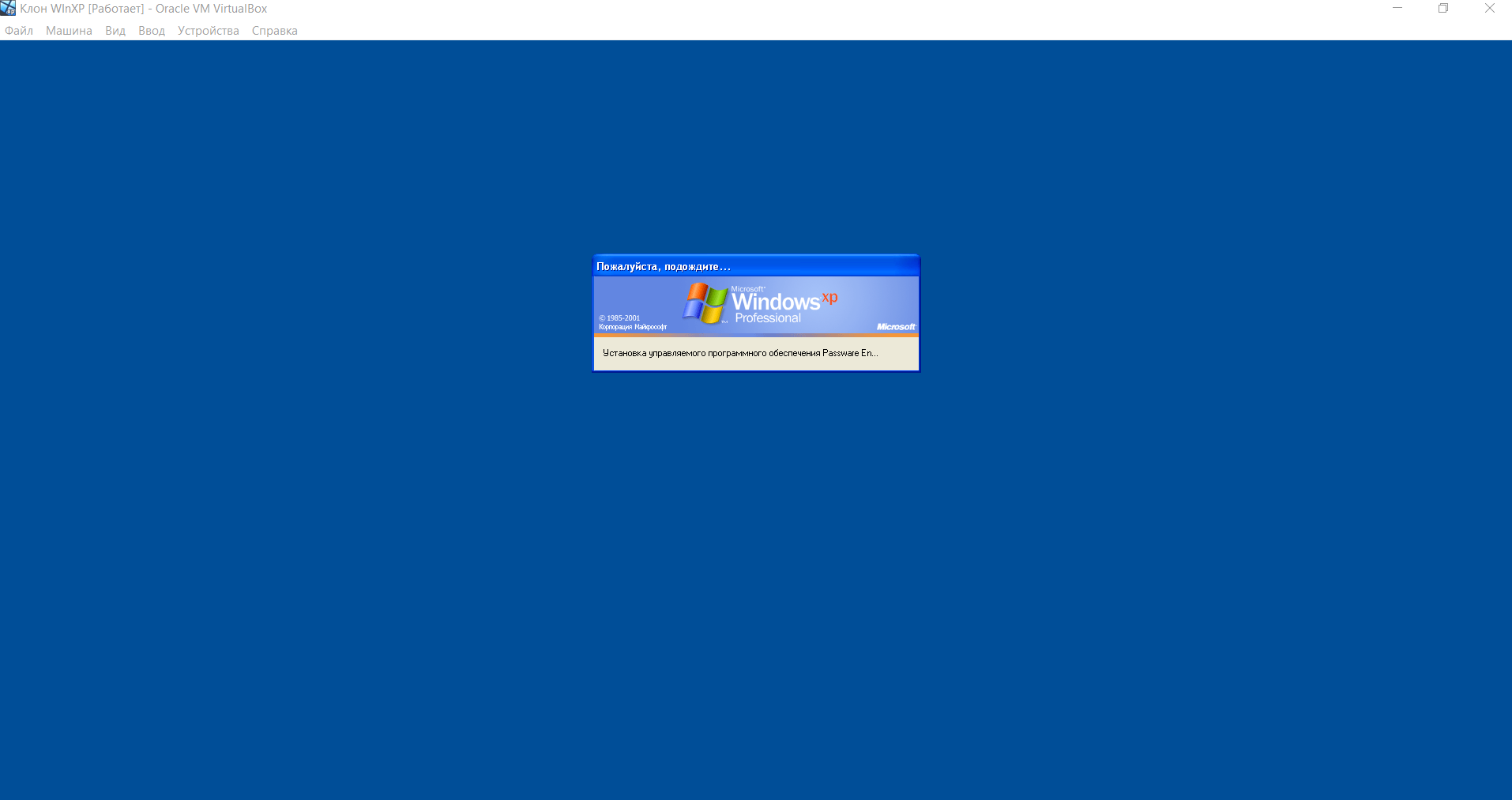
1. Щелкните правой кнопкой мыши **Установка программ**, выберите пункт **Создать** и выберите **пакет**.
2. В поле **Открыть** введите полный путь универсального соглашения об именах (UNC) общий установочный пакет, вы должны. Например \\**файловом сервере**\**совместно**\**имя файла** MSI-файл.  
     
   Важным следует использовать кнопку Обзор для доступа к расположению. Убедитесь, что используется пакет установщика общей UNC-путь.



1. Нажмите кнопку **Открыть**.
2. Выберите **Назначение** и нажмите кнопку **ОК**. Пакет отобразится в правой области окна « **Групповая политика** ».



1. Закройте оснастку « **Групповая политика** », нажмите кнопку **ОК** и закройте оснастку «Active Directory-пользователи и компьютеры».
2. При запуске компьютера клиента, автоматически устанавливается пакет управляемого программного обеспечения.



### **Публикация пакета**

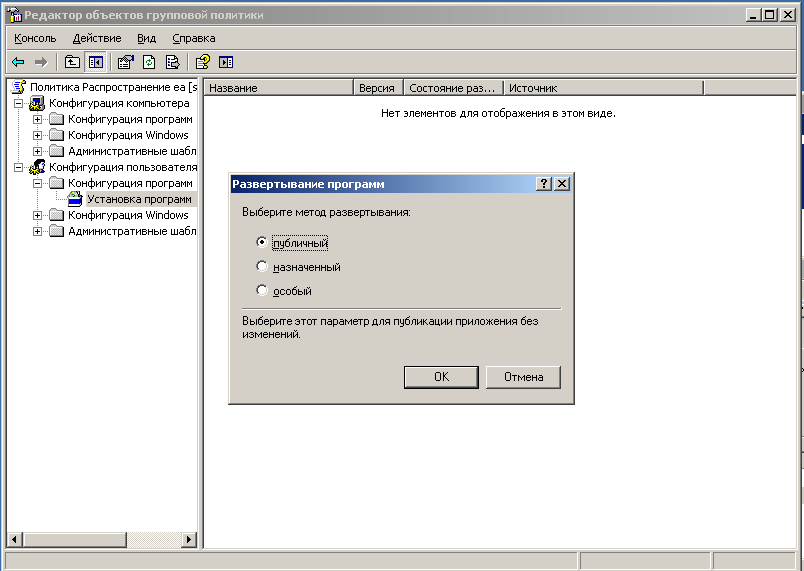
Для публикации пакета для пользователей компьютеров и сделать его доступным для установки из списка **Установка и удаление программ** на панели управления, выполните следующие действия:

1. Запустите оснастку "Active Directory — пользователи и компьютеры". Для этого нажмите кнопку **Пуск**, выберите пункт **Администрирование** и выберите команду **Active Directory — пользователи и компьютеры**.
2. В дереве консоли щелкните правой кнопкой мыши домен и выберите команду **Свойства**.
3. Перейдите на вкладку **Групповой политики** , щелкните нужную политику и нажмите кнопку **Изменить**.
4. **Конфигурация пользователя** последовательно разверните узлы **Конфигурация программ**.
5. Щелкните правой кнопкой мыши **Установка программ**, выберите пункт **Создать**и выберите **пакет**.
6. В поле **Открыть** введите полный UNC-путь нужный общий установочный пакет. Например \\**файловом сервере**\**совместно**\**имя файла** MSI-файл.

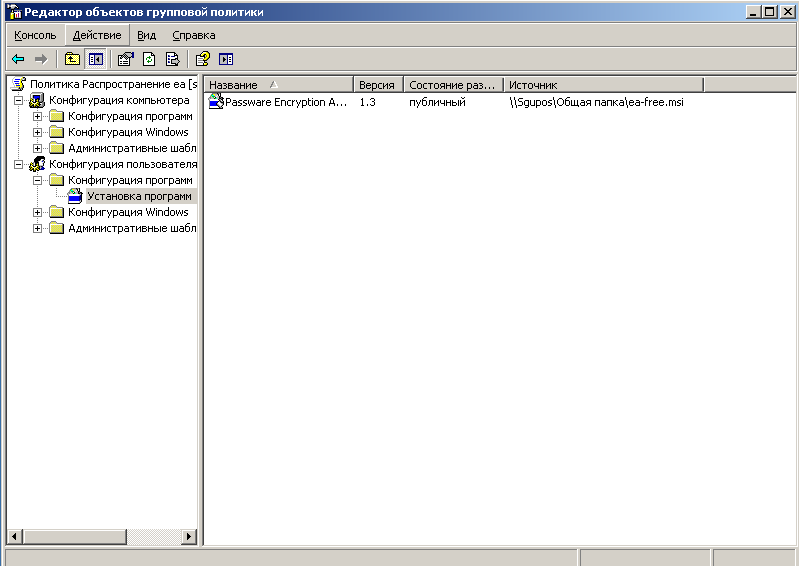
Важным следует использовать кнопку Обзор для доступа к расположению. Убедитесь, что используется пакет установщика общей UNC-путь.

Использовал ранее созданную групповую политику для распространения программы.

1. Нажмите кнопку **Открыть**.
2. Нажмите кнопку **Опубликовать** и нажмите кнопку **ОК**.



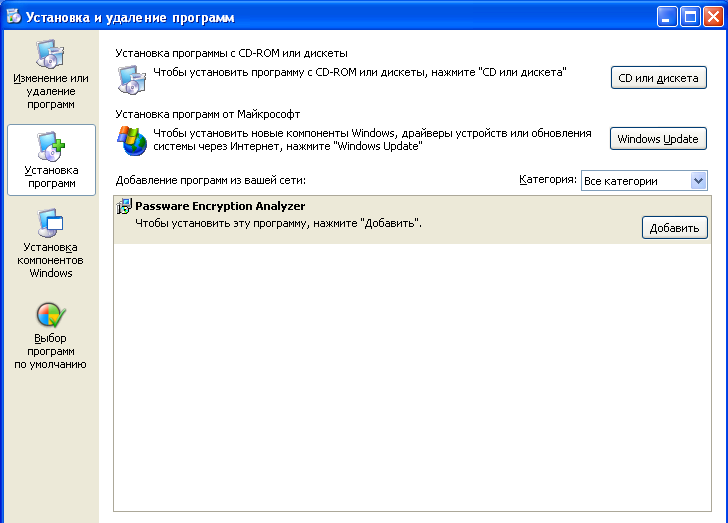
1. Пакет отобразится в правой области окна « **Групповая политика** ».



1. Закройте оснастку «Групповая политика», нажмите кнопку **ОК**и закройте оснастку «Active Directory-пользователи и компьютеры».
2. Проверьте пакет.

Зашел под пользователем remus\_boss в компьютер домена:

И открыл установка и удаление программ на панели управления, теперь программу можно установить:

  
  
В некоторых версиях Windows, описанные действия могут существенно отличаться от того, что написано в данной статье. Если это так, обратитесь к документации продукта для выполнения этих действий.

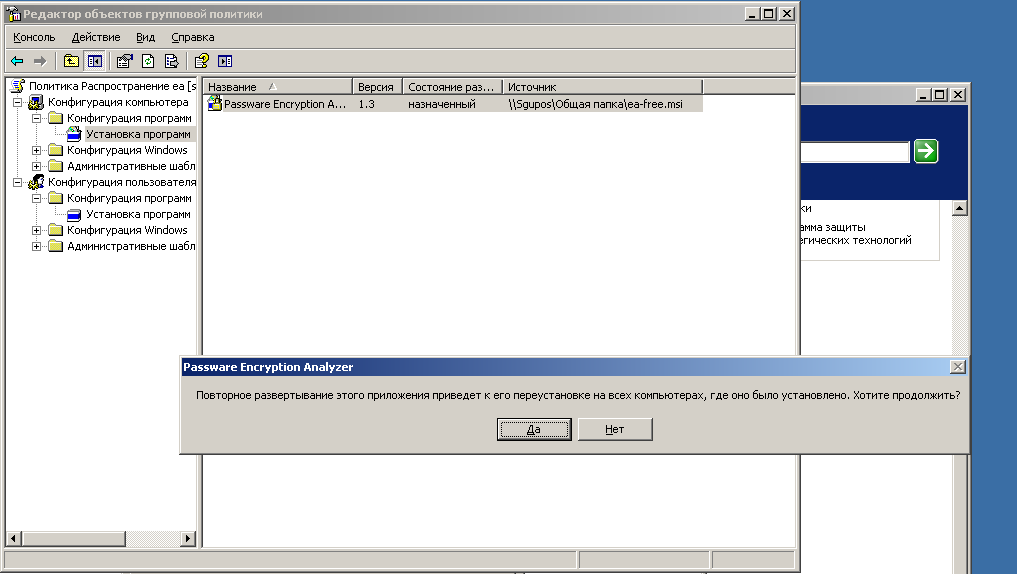
* 1. Войдите в систему на рабочей станции под управлением Windows 2000 Professional или Windows XP Professional с помощью учетной записи, публикации пакета.
  2. В Windows XP нажмите кнопку **Пуск**и выберите **Панель управления**.
  3. Дважды щелкните значок **Установка и удаление программ** и нажмите кнопку **Установка программ**.
  4. Выберите программу, которая опубликована в списке **Установка программ из локальной сети** и нажмите кнопку **Добавить**. Программа установлена.
  5. Нажмите кнопку **ОК**, а затем нажмите кнопку **Закрыть**.

### **Повторное развертывание пакета**

В некоторых случаях может потребоваться повторное развертывание пакета (например, при обновлении или изменении пакета). Чтобы повторно развернуть пакет, выполните следующие действия:

1. Запустите оснастку "Active Directory — пользователи и компьютеры". Для этого нажмите кнопку **Пуск**, выберите пункт **Администрирование** и выберите команду **Active Directory — пользователи и компьютеры**.
2. В дереве консоли щелкните правой кнопкой мыши домен и выберите команду **Свойства**.
3. На вкладке **Групповой политики** щелкните объект групповой политики, который использовался для развертывания пакета и нажмите кнопку **Изменить**.
4. Разверните контейнер **Конфигурация программ** , содержащий элемент установки программного обеспечения, который использовался для развертывания пакета.
5. Выберите контейнер установки программного обеспечения, содержащий пакет.
6. В правой области окна « **Групповая политика** » щелкните правой кнопкой мыши программу, выберите пункт **Все задачи** и нажмите кнопку **развернуть приложение заново**. Появится следующее сообщение:

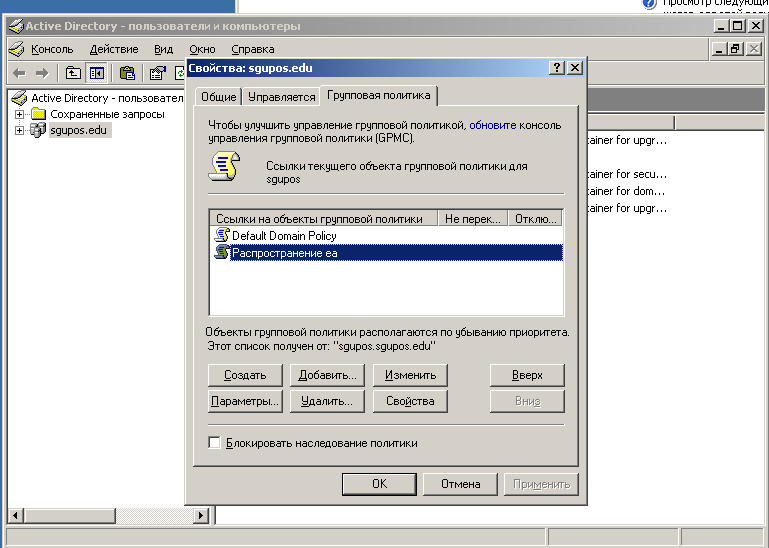
Повторное развертывание этого приложения будет переустановить приложение везде, где он уже установлен. Вы действительно хотите продолжить?



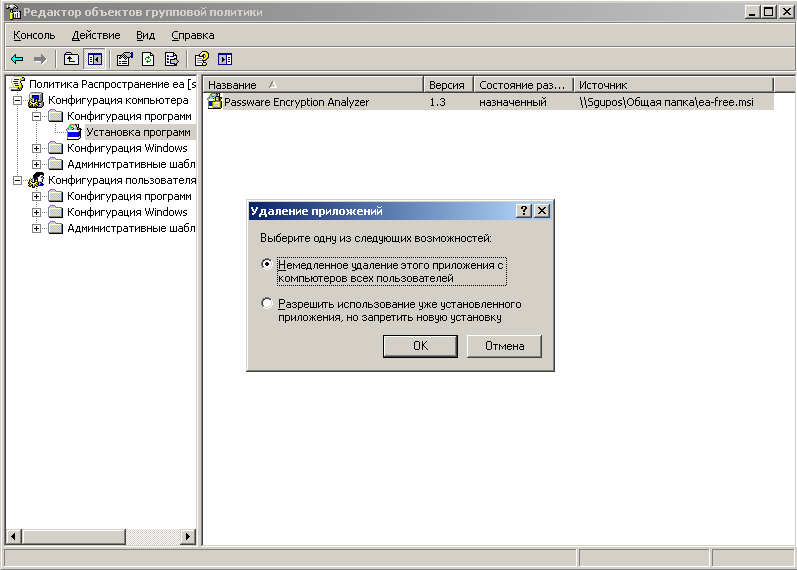
### **Удаление пакета**

Чтобы удалить опубликованный или назначенный пакет, выполните следующие действия:

1. Запустите оснастку "Active Directory — пользователи и компьютеры". Для этого нажмите кнопку **Пуск**, выберите пункт **Администрирование** и выберите команду **Active Directory — пользователи и компьютеры**.
2. В дереве консоли щелкните правой кнопкой мыши домен и выберите команду **Свойства**.
3. На вкладке **Групповой политики** щелкните объект групповой политики, который использовался для развертывания пакета и нажмите кнопку **Изменить**.



1. Разверните контейнер **Конфигурация программ** , содержащий элемент установки программного обеспечения, который использовался для развертывания пакета.
2. Выберите контейнер установки программного обеспечения, содержащий пакет.
3. В правой области окна « **Групповая политика** » щелкните правой кнопкой мыши программу, выберите пункт **Все задачи** и нажмите кнопку **Удалить**.
4. Выполните одно из следующих действий:
   * Выберите **Немедленное удаление этого приложения с компьютеров всех пользователей** и нажмите кнопку **ОК**.
   * Нажмите кнопку **Разрешить пользователям продолжить использование программного обеспечения, но запретить новую установку** и нажмите кнопку **ОК**.
5. Закройте оснастку «Групповая политика», нажмите кнопку **ОК**и затем closet оснастку «Active Directory-пользователи и компьютеры».



### **Разрешение вопросов**

#### ***После их удаления с помощью групповой политики на клиентском компьютере отображаются опубликованные пакеты***

Это может произойти, если пользователь установил программу, но не использовал его. При первом запуске опубликованной программе пользователя установка завершится. Групповая политика затем удаляет программы