ФЕДЕРАЛЬНОЕ АГЕНТСТВО ПО ОБРАЗОВАНИЮ
Государственное образовательное учреждение
высшего профессионального образования
«Пензенский государственный университет»

Лабораторный практикум по курсу «Сети ЭВМ и телекоммуникации»
Часть 2 «АДМИНИСТРИРОВАНИЕ И МОДЕЛИРОВАНИЕ СЕТЕЙ»

Учебно-методическое пособие

Издательство
Пензенского государственного
университета
Пенза 2012

УДК 683.3
Б93

Р е ц е н з е н т :
Заведующий кафедрой информатики и вычислительных систем Пензенского государственного педагогического университета имени В. Г. Белинского
В. И. Горбаченко

Калиниченко, Е.

Лабораторный практикум по курсу «Сети ЭВМ и телекоммуникации». Часть 2 «Администрирование и моделирование сетей»: учеб.-метод. пособие /Е.И. Калиниченко, Н.Н. Коннов – Пенза: Изд-во Пенз. гос. ун-та, 2012. – 67с.: ил.30, табл.8, библ. 5 назв.

Настоящее учебное издание является второй частью руководства к лабораторному практикуму по курсу «Сети ЭВМ и телекоммуникации», посвященному изучению методов передачи данных в современных сетях ЭВМ. Пособие позволяет получить основные навыки администрирования локальной сети на основе домена под управлением *Microsoft Windows Server 2003/2008*, освоить методику моделирования сетей различного типа с помощью пакета *Netcracker Professional*.

Пособие подготовлено на кафедре «Вычислительная техника» и предназначено для студентов, обучающихся по направления 23.0100 - «Информатика и вычислительная техника».

УДК 683.3

Введение

Эта часть лабораторного практикума позволяет получить основные навыки администрирования локальной сети на основе домена под управлением Microsoft Windows Server 2000/2003/2008, а также освоить методику моделирования и документирования сетей различного типа с помощью пакета *Netcracker Professional* v.4.0.

Обучение происходит в ходе решения конкретных практических задач администратора домена. Каждая лабораторная работа содержит цели работы, задания, указания к выполнению, требования к отчету и контрольные вопросы. Практикум строится следующим образом: сначала описывается процесс решения задачи, затем студентам предлагается выполнить ряд самостоятельных заданий. По выполненным заданиям требуется составление отчета, который сдается преподавателю на проверку. Для успешного освоения лабораторного практикума необходимо одновременное изучение теоретического курса.

Выполнение лабораторных работ по администрированию локальной сети представляет собой создание домена следующего уровня в домене, используемом в учебном заведении, и установки между ними одностороннего доверительного отношения от домена нижнего уровня к верхнему. На контроллере домена, предназначенного для обучения, устанавливается сервер терминалов и сервер лицензирования терминалов. Подключаться к контроллеру домена и выполнять администрирование домена с любой рабочей станции можно с использованием подключения к удаленному рабочему столу.

Лабораторная работа № 1

УСТАНОВКА И УПРАВЛЕНИЕ DNS-СЕРВЕРОМ

1.1 Цель работы

Целью работы является приобретение навыков установки и тестирования службы DNS, конфигурирования зоны DNS и применения файла *HOSTS*.

1.2. Теоретический материал

1.2.1 Общая характеристика службы DNS

Служба DNS (*Domain Name System* — система доменных имён) компьютерная распределённая система для получения информации о доменах. DNS предназначена для преобразования символьных доменных имен в IP-адреса и обратно. Установка этой службы необходима перед установкой службы *Active Directory*.

Распределённая база данных DNS поддерживается с помощью иерархии DNS-серверов, взаимодействующих по определённому протоколу.

1.2.2 Установка сервера DNS на машину с Windows Server 2003/2008

Выполните предварительную конфигурацию компьютера, на котором будет установлен сервер DNS, а именно, проверьте, что серверу Windows Server 2003/2008 kit-edu назначен статический IP-адрес (например, 192.168.1.1).

Для установки сервера DNS воспользуйтесь одним из двух способов.

Первый способ:

- Откройте ***Control Panel*** (**Панель управления**), затем ***Add/Remove Programs*** (**Установка/удаление программ**).
- На вкладке ***Add/Remove Windows Components*** (**Установка/удаление компонентов *Windows*)** найдите ***Networking Services*** (**Сетевые службы**) и нажмите ***Details*** (**Подробно**).
- Выберите компонент ***Domain Name System*** (DNS) и подтвердите свой выбор.
- Дождитесь завершения установки сервера.

Второй способ:

- Откройте ***Control*** Panel **-** ***Administrative Tools*** (**Панель управления - Администрирование**).
- Запустите ***Manage Your*** Server (**Управление сервером**).
- Выберите ***Add or remove a role*** (**Добавить или удалить роль**) и выберите ***DNS Server***.
- Дождитесь завершения установки сервера.

Для дальнейшей настройки DNS-сервера используется оснастка главного системного меню ***Administrative Tools*** (***Администрирование)*** – ***DNS***.

1.2.3 Создание зоны прямого просмотра

Для создания зоны прямого просмотра ***myzone*** необходимо выполнить следующие действия:

- Откройте оснастку DNS.
- Разверните узел DNS, далее разверните узел **<Имя компьютера>**.
- Для создания нового домена щелкните правой кнопкой по ***Forward*** **Lookup Zones** (**Зоны прямого просмотра**) и выберите пункт ***New zone*** (**Новая зона**).
- В окне ***Zone Type*** (**Тип зоны**) укажите ***Primary Zone*** (**Основная зона**) и нажмите ***Next*** (**Далее**).
- В окне ***Zone Name*** (**Имя зоны**) укажите имя зоны – ***myzone*** (**Корневая зона**) и нажмите ***Next***.
- В окне ***Zone File*** (**Файл зоны**) убедитесь, что выбран переключатель ***Create A New File With This File Name*** (**Создать новый файл с этим именем**) и имя создаваемого файла – ***myzone.dns***.
- Просмотрите сводку выбранных параметров и щелкните кнопку ***Finish*** (**Готово**).
- Убедитесь, что в ***Forward Lookup Zones*** появился новый узел **myzone** и сгенерированы записи ***Start of Authority*** (***SOA***) (**Начальная запись зоны**), ***Name Server*** (***NS***) (**Сервер имен**) и ***Host*** (***A***) (**Хост**).
- Чтобы добавить новый узл в созданную зону, щелкните правой кнопкой по узлу ***myzone*** и выберите ***New Host*** (**Новый хост**). В поле ***Name*** (**Имя**) введите имя узла – ***kit-edu***. Поле ***IP Address*** установите равным IP-адресу компьютера. Нажмите ***Add Host*** (**Добавить хост**).

1.2.4 Тестирование службы DNS.

Для тестирования службы DNS на данном этапе настройки DNS сервера необходимо выполнить следующие действия:

- Запустите машину с Windows XP и выполните в ней команду ***ping kit-edu.myzone.***
- Убедитесь, что такой узел был найден и отображается его IP-адрес. Если ***ping*** не проходит, нужно исправить настройки.
- Для преобразования IP-адреса в доменное имя выполните утилиту ***nslookup*** с параметром, равным IP-адресу машины. Объясните, почему появилась ошибка на данном этапе настройки DNS сервера.

1.2.5 Создание зоны обратного просмотра

Для создания зоны обратного просмотра (для преобразования IP-адреса в доменное имя) необходимо выполнить следующие действия:

- В узле ***Reverse Lookup Zones*** (**Зоны обратного просмотра**) щелкните правой кнопкой мыши и выберите ***New zone*** (**Мастер создания новой зоны**).
- В окне ***Zone Type*** (**Тип зоны**) укажите ***Primary Zone*** (**Основная зона**) и нажмите ***Next***.
- Убедитесь, что выбран переключатель ***Network ID*** (**Номер сети**). В поле под ним введите адрес вашей сети (например, 192.168.1). Поле ***Reverse Lookup Zone Name*** (**Имя зоны обратного просмотра**) внизу окна должно выглядеть так: ***1.168.192.in-addr.arpa***.
- Завершите работу мастера, оставив все настройки по умолчанию.
- Щелкните правой кнопкой мыши по новому узлу в ***Reverse Lookup Zones*** (например, ***192.168.1.x Subnet***) и выберите ***New Pointer*** **(Новый указатель).** Последнее число установите равным последнему числу в IP-адресе. В поле ***Host name*** (**Имя хоста**) запишите полное имя узла, например ***kit-edu.myzone.***

1.2.6 Создание псевдонима для узла

Для Создания псевдонима для узла kit-edu.myzone необходимо выполнить следующие действия:

- Щелкните правой кнопкой мыши по узлу ***myzone*** и выберите **New *Alias*** (**Новый псевдоним**).
- В поле ***Alias name*** (**Имя псевдонима**) укажите псевдоним узла (например, ***MyServer***). В поле ***Fully qualified domain name*** (**Полное доменное имя**) впишите полное имя ***kit-edu.myzone***

1.2.7 Тестирование службы DNS.

Для тестирования службы DNS необходимо выполнить следующие действия:

- Запустите из командной строки утилиту ***nslookup*** с параметром, равным IP-адресом машины, на которой установлен сервер.
- В дереве консоли откройте свойства узла через команду контекстного меню ***Properties*** (**Свойства**).
- Перейдите на вкладку ***Monitoring*** (**Наблюдение**).
- В группе ***Select A Test Type*** (**Выберите тип теста**) пометьте флажки ***A*** **Simple Query Against This DNS Server** (**Простой запрос к этому DNS-серверу**) и ***Recursive Query To Other DNS Servers*** (**Рекурсивный запрос к другим DNS-серверам**). Щелкните кнопку ***Test Now*** (**Тестировать**).

- В списке ***Test Results*** (**Результаты теста**) против обеих записей вы увидите ***PASS*** (**тест пройден**). Если вы работаете на автономном сервере, напротив ***Recursive Query*** (**Рекурсивный запрос**) вы увидите ***FAIL*** (**ошибка**).

1.2.8 Конфигурирование клиента для использования службы DNS.

Для конфигурирования клиента службы DNS необходимо выполнить следующие действия:

- На машине с ОС *Windows XP* откройте диалоговое окно свойств TCP/IP (сетевые настройки). Настройте систему для автоматического получения адреса DNS (это обеспечивает сервер DHCP) или вручную укажите IP-адреса предпочтительного и дополнительного серверов DNS.

- Для настройки дополнительных параметров DNS щелкните кнопку ***Advanced (Дополнительно).*** Чтобы задать параметры DNS, в диалоговом окне ***Advanced TCP/IP Settings (Дополнительные параметры TCP/IP***) перейдите на вкладку DNS. Здесь можно сконфигурировать и параметры, обеспечивающие разрешение имен узлов, для которых не было указано полное доменное имя, и настроить параметры регистрации DNS.

1.2.9 Разрешение имен с использованием файла *HOSTS*

Для задания разрешения имен с использованием файла ***HOSTS*** в случае отказа службы DNS и для возможности использования коротких имен при доступе к удаленным узлам. необходимо выполнить следующие действия:

- На сервере найдите системный файл ***HOSTS*** и откройте его в текстовом редакторе.

- Используя утилиту ***ping*** с ключом ***/a,*** определите IP-адрес узла ***www.microsoft.com.***

- Внесите запись в файл ***HOSTS***, указав полученный IP-адрес и имя - ***www.microsoft.com.*** Сохраните изменения.

- Проверьте через браузер доступность узла www.microsoft.com.

- Внесите в файл IP-адрес своего сервера и имя в формате **computer.domain**. Сохраните изменения.

- Остановите службу DNS через утилиту Services.

- Проверьте, доступно ли это имя в формате ***computer.domain*** через утилиту ***ping.***

1.3. Задание на лабораторную работу

Выполните последовательно операции по созданию, конфигурированию и тестированию службы DNS, описанные в п.1.2.

Включите в отчет скриншоты каждого шага выполнения установки и проверки работоспособности DNS-сервера.

1.4 Вопросы для самопроверки

1) Для чего предназначены прямые и обратные запросы поиска?

2) Опишите назначение компонентов DNS: зона, сервер имен, доменное пространство имен.

3) Назовите основные типы зон и их назначение.

4) Назовите основные правила именования доменов.

5) Какова максимально допустимая длина имени домена?

6) С какой целью используют несколько серверов имен?

7) Можно ли одному IP-адресу нужно присвоить несколько имен? Перечислите все способы.

8) Для чего используется файл ***HOSTS***?

Лабораторная работа № 2.

СОЗДАНИЕ ДОМЕНА *WINDOWS SERVER 2003/2008*

2.1 Цель работы

Целью работы является приобретение навыков создания домена *Windows Server 2003/2008* и установки службы каталога Active Directory, а так же изучение структуру службы каталога *Active Directory*.

2.2. Теоретический материал

2.2.1 Общая характеристика службы каталогов

Сети Microsoft Windows поддерживают две модели служб каталогов: рабочую группу (*workgroup*) и домен (*domain*). При использовании *Windows Server 2003/2008* в сети, модель домена наиболее предпочтительна. Модель домена характеризуется единым каталогом ресурсов предприятия — *Active Directory*, которому доверяют все системы безопасности, принадлежащие домену. Поэтому такие системы способны работать с субъектами безопасности (учетными записями пользователей, групп и компьютеров) в каталоге, чтобы обеспечить защиту ресурсов.

Active Directory позволяет администраторам использовать групповые политики для обеспечения единообразия настройки пользовательской рабочей среды, развёртывать ПО на множестве компьютеров, устанавливать обновления ОС, прикладного и серверного ПО на всех компьютерах в сети. Active Directory хранит данные и настройки среды в централизованной базе данных.

Служба *Active Directory*, таким образом, играет роль идентификационного хранилища и сообщает «кто есть кто» в этом домене. *Active Directory* — не просто база данных, а это:

- коллекция файлов, включая журналы транзакций и системный том (*Sysvol*), содержащий сценарии входа в систему и сведения о групповой политике;
- службы, поддерживающие и использующие БД, включая протокол LDAP (*Lightweight Directory Access Protocol* - облегчённый протокол доступа к каталогам), протокол безопасности *Kerberos*, процессы репликации и службу FRS (*File Replication Service*).

БД и ее службы устанавливаются на один или несколько контроллеров домена. Контроллер домена назначается ***Мастером установки*** *Active Directory*, который можно запустить с помощью Мастера настройки сервера или командой DCPROMO из командной строки.

После того как сервер становится контроллером домена, на нем хранится копия (реплика) *Active Directory*, и изменения БД на любом

контроллере реплицируются на все остальные контроллеры домена субъектами безопасности (учетными записями пользователей, групп и компьютеров) в каталоге, чтобы обеспечить защиту ресурсов.

2.2.2 Установка службу каталога *Active Directory*

Для установки службы каталога *Active Directory* необходимо выполнить следующие действия:

- Запустите мастер установки *Active Directory* ***Start – Run – dcpromo***.
- Следуя шагам мастера установки, выберите следующие параметры установки:

1. в окне ***Domain Controller Type*** (***Тип контроллера домена***) – переключатель ***Domain controller for a new domain*** (**Контроллер домена в новом домене**);

2. в окне ***Create*** New ***Domain*** (**Создать новый домен**) – переключатель ***Domain in a new forest*** (**Домен в новом лесу**);

3. в окне ***Install or Configure DNS*** (**Установка или настройка DNS**) – переключатель ***No, just install and configure DNS on this computer*** (**Нет, DNS уже установлена и настроена на этом компьютере**), если служба DNS уже установлена на сервере, или ***Yes, I will configure the DNS client*** (**Да, я буду конфигурировать клиента DNS**);

4. в окне ***New Domain Name*** (**Новое доменное имя**) наберите **mydomain** в строке ***Full DNS Name For New Domain*** (**Полное DNS-имя нового домена**);

5. в окне NetBIOS Domain Name (Доменное имя NetBIOS) должна появиться запись MYDOMAIN;

6. убедиться, что для размещения базы данных и протокола выбран путь C:\WINDOWS\NTDS, а для размещения каталога SYSVOL указан путь C:\WINDOWS\SYSVOL;

7. в окне ***Permissions*** (**Разрешения**) выберите ***Permissions compatible only with Windows 2000 or Windows Server 2003/2008 operating systems*** (**Разрешения, совместимые только с операционными системами Windows 2000 или Windows Server 2003/2008**);

8. в окне ***Directory Services Restore Mode Administrator Password*** (**Пароль администратора для режима восстановления**) введите пароль, который хотите присвоить этой учетной записи сервера Administrator в случае, если компьютер загрузится в режиме **Directory Services Restore** (**Режим восстановления**);

9. в окне ***Summary (Сводка)*** изучите список выбранных вами параметров установки и дождитесь завершения процесса установки Active Directory.

- В окне ***Completing The Active Directory Installation Wizard*** (**Завершение работы мастера установки Active Directory**), щелкните

кнопку **Finish** (**Готово**), а затем кнопку ***Restart Now*** (**Перезагрузить компьютер сейчас**).

2.2.3 Просмотр созданного домена

Просмотр созданного домена может быть выполнен двумя способами.

Первый способ:

- Откройте ***My Network Places*** - ***Entire Network*** - ***Microsoft Windows Network*** (**Мое сетевое окружение - Вся сеть - сеть Microsoft Windows)**.

- Убедитесь, что появилась запись о домене ***mydomain***, в котором содержится один компьютер – ***kit-edu***.

Второй способ:

- В меню ***Start*** - ***Programs*** - ***Administrative Tools (*****Пуск - Программы - Администрирование)** выберите ***Active Directory Users And Computers (*****Пользователи и компьютеры Active Directory)**. Откроется одноименная оснастка.

- В дереве оснастки дважды щелкните на ***mydomain*** (или на имени вашего домена), чтобы увидеть содержимое узла ***mydomain.***

- В разделе ***Domain Controllers*** (**Контроллеры домена**) дерева оснастки просмотрите название контроллера домена и его полное имя DNS (например, если имя изолированного сервера было ***kit-edu***, то после установки домена должно стать ***kit-edu.mydomain).***

- В разделе ***Users*** (**Пользователи**) просмотрите список встроенных учетных записей пользователей и групп пользователей домена.

- Активизируйте встроенную учетную запись ***Guest*** (**Гость**) и попробуйте войти в систему. Попытка должна быть неудачной, т. к. на контроллеры домена разрешен вход только администраторам домена.

- Закройте консоль ***Active Directory Users And Computers***.

2.2.4. Проверка работы службы DNS с помощью оснастки DNS.

Для проверки работы службы DNS с помощью оснастки DNS необходимо выполнить следующие действия:

- Откройте консоль ***DNS*** командой ***Start*** - ***Programs*** - ***Administrative Tools*** - ***DNS (*****Пуск - Программы - Администрирование - DNS)**.

- В дереве консоли DNS щелкните правой кнопкой по имени вашего сервера и выберите команду Properties (Свойства). Откроется окно свойств **kit-edu** (если у сервера другое имя, то в заголовке окна будет значиться оно).

- Перейдите на вкладку ***Monitoring*** (**Наблюдение**).

- В списке ***Select A Test Type*** (**Выберите тип теста**) пометьте флажки **A Simple Query Against This DNS Server** (**Простой запрос к этому DNS-серверу**) и ***A Recursive Query To Other DNS Servers*** (**Рекурсивный запрос к**

другим DNS-серверам) и щелкните ***Test Now*** (**Протестировать**). В окне свойств ***Server*** в списке результатов тестирования должна появиться надпись **PASS** (**Пройден успешно**) или ***FAIL*** (**Не пройден**) - в столбцах ***Simple Query*** (**Простой запрос**) и ***Recursive Query*** (**Рекурсивный запрос**). Объясните полученные результаты.

2.2.5 Удаление службы *Active Directory*

Для удаления службы *Active Directory* с сервера необходимо запустить Мастер установки и удаления *Active Directory* ***Start - Run*** **-dcpromo.**

2.2.6 Восстановление службы *Active Directory*

Для восстановление службы *Active Directory* с сервера необходимо запустить Мастер установки и удаления *Active Directory* ***Start - Run*** **-dcpromo.**

2.3 Задание на лабораторную работу

Выполните последовательно все операции по созданию, конфигурированию и тестированию службы *Active Directory*, описанные в п. 2.2.

Включите в отчет скриншоты, отражающие все этапы установки и проверки работоспособности службы *Active Directory*.

2.4 **Вопросы для самопроверки**

1) Опишите различия между рабочей группой и доменом.

2) Каково основное различие между ОС *Windows XP* и *Windows Server 2000/2003/2008*?

3) Возможно, ли создать домен в сети, где все компьютеры сети работают под управлением ОС *Windows XP?*

4) Дайте определение контроллера домена.

5) Перечислите известные Вам встроенные учетные записи пользователей и групп пользователей домена и опишите их назначение.

6) Что означает термин «изолированный» сервер?

7) Опишите различия между рабочей группой и доменом.

Лабораторная работа № 3

УЧЕТНЫЕ ЗАПИСИ ПОЛЬЗОВАТЕЛЕЙ И УПРАВЛЕНИЕ ПРОФИЛЯМИ ПОЛЬЗОВАТЕЛЕЙ

3.1 Цель работы

Целью работы является приобретение навыков создания объектов пользователей и управления ими, управления профилями пользователей.

3.2. Теоретический материал

3.2.1 Общая характеристика объектов службы *Active Directory*

Active Directory имеет иерархическую структуру, состоящую из объектов. Объекты разделяются на три основные категории: ресурсы (например, принтеры), службы (например, электронная почта) и люди (учётные записи пользователей и групп пользователей). *Active Directory* предоставляет информацию об объектах, позволяет организовывать объекты, управлять доступом к ним, а также устанавливает правила безопасности.

Каждый объект представляет отдельную сущность — пользователя, компьютер, принтер, приложение или общую сетевую папку, и его атрибуты. Объекты могут также быть контейнерами для других объектов. Объект уникально идентифицируется своим именем и имеет набор атрибутов — характеристик и данных, которые объект может содержать; последние, в свою очередь, зависят от типа объекта. Контейнер аналогичен объекту в том смысле, что он также имеет атрибуты и принадлежит пространству имён, но, в отличие от объекта, контейнер не обозначает ничего конкретного: он может содержать группу объектов или другие контейнеры.

Объект пользователя создается с использованием оснастки *Active Directory* — пользователи и компьютеры. Хотя он может быть создан в корне домена или в любом из контейнеров, созданных по умолчанию при установке операционной системы, при выполнении лабораторной работы нужно создать свое организационное подразделение (ОП) (в англоязычной версии – *container* (контейнер)) по следующему правилу: <№ группы>_<№ бригады>. Например, 05ВП2_бр3.

Чтобы создать объект пользователя вы должны быть членом групп Администраторы предприятия (*Enterprise Admins*), Администраторы домена (*Domain Admins*) или Операторы учета (*Account Operators*), либо вам должны быть делегированы (переданы через администратора) одно или несколько из этих административных полномочий.

3.2.2 Создание объектов пользователей и управление ими

Для создания объектов пользователей необходимо выполнить следующие действия:

- Выберите свой контейнер (ОП), затем в меню **Действие (Action)** щелкните **Создать (New)\Пользователь (User)**. Откроется диалоговое окно

Новый объект — Пользователь (New Object—User), показанное на рисунке 3.1. На первой странице этого окна необходимо ввести сведения об имени пользователя (смотри табл. 3.1).

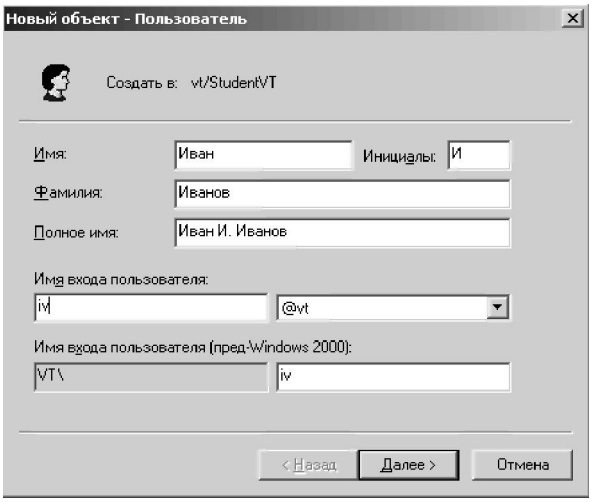

Рисунок 3.1. Диалоговое окно **Новый объект — Пользовате**ль

Таблица 4.1 Свойства пользователя окна **Новый объект-Пользователь**

Свойство	Описание
Имя (*First Name*)	Имя пользователя. Необязательное
Инициалы (*Initials*)	Инициалы (отчество) пользователя. Необязательное
Фамилия (*Last Name)*	Фамилия пользователя. Необязательное
Полное имя (*Full Name)*	Полное имя пользователя. Если вы указали имя или фамилию пользователя, значение этого свойства будет подставлено автоматически. После, в случае необходимости, можно изменить предложенное значение. Это обязательное поле. На основе введенного здесь имени генерируется несколько свойств объекта пользователя, в частности CN (обычное имя), DN (различающееся имя), name (имя) и *displayName* (отображаемое имя). Поскольку значение CN должно быть в контейнере уникальным, введенное здесь имя должно быть уникальным среди остальных объектов в ОП (или другом контейнере), где вы создаете объект пользователя
Имя входа пользователя (*User Logon Name*)	Главное имя пользователя (*user principal name*, UPN) состоит из имени пользователя для входа и суффикса UPN, которым по умолчанию является DNS_имя домена, в котором вы создаете объект. Это свойство обязательно, а UPN_имя в целом (в формате <имя_для_входа>@ DNS суффикс) должно быть уникальным в лесу *Active Directory*. Например, UPN_имя может быть таким: ivan@edu.vt. UPN можно использовать для входа в систему *Windows 2000/XP* или *Windows Server 2000/2003/2008*
Имя входа пользователя (пред_Windows 2000) [*User Logon Name* (*Pme_Windows 2000*)]	Это имя используется для входа в систему с клиентов под управлением более ранних версий *Windows,* например *Windows 9x/Me/NT 4* или *Windows NT 3.51*. Это поле является обязательным и должно быть уникальным в домене. Обычно, если нет особого случая, оно совпадает со значением **Имя входа пользователя(*User Logon Name*)**

• Закончив ввод значений, щелкните Далее (Next). На второй странице окна Новый объект — Пользователь (New Object—User) необходимо ввести пароль пользователя и установить управляющие флажки учетной записи (рисунок 3.2).

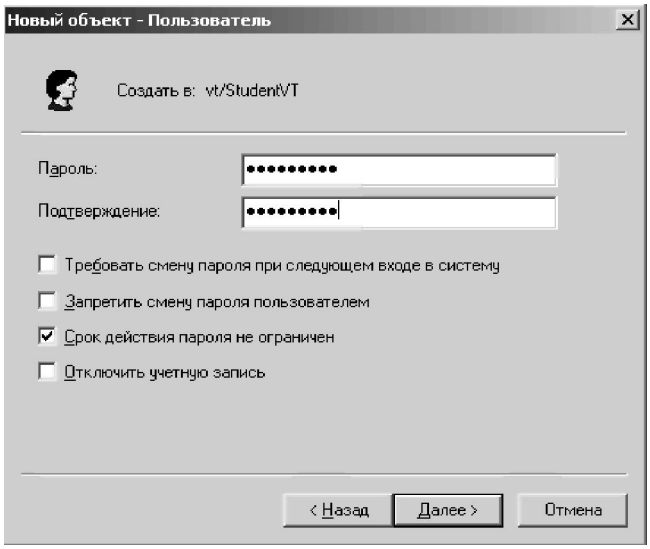

Рисунок 3.2. Вторая страница окна **Новый объект — Пользователь**

• Обратите внимание, что политика учетных записей (которую можно перенастроить в объекте групповой политики ***Default Domain Policy***), устанавливаемая по умолчанию в домене *Windows Server 2000/2003/2008,* требует задания сложного пароля, а именно, с применением символов трех или четырех типов (прописные буквы, строчные буквы, цифры, специальные символы) и длиной не менее семи. В табл. 4.2 перечислены свойства со второй страницы окна **Новый объект — Пользователь (*New Object—User*).**

Таблица 4.2 Вторая страница окна **Новый объект — Пользователь**

Свойство	Описание
Пароль ***(Password)***	Этот пароль будет использоваться для проверки подлинности пользователя. В целях безопасности пароль необходимо задавать всегда. Во время ввода символы будут скрыты
Подтверждение ***(Confirm Password)***	Подтвердите пароль, набрав его еще раз
Требовать смену пароля при следующем входе в систему ***(User Must Change Password At Next Logon)***	Установите этот флажок, если хотите, чтобы пользователь изменил пароль, введенный вами при первом входе в систему. Если выбрали Срок действия пароля не ограничен (Password Never Expires), изменить значение этого параметра нельзя. При выборе этого параметра флажок исключающего его параметра Запретить смену пароля пользователем (***User Cannot Change Password***) будет автоматически снят
Запретить смену пароля пользователем (***User Cannot Change Password)***	Установите этот флажок, если одной учетной записью в домене пользуются несколько человек [допустим, учетной записью Гость (Guest)] или если необходимо контролировать пароли учетной записи этого пользователя. Обычно этот параметр используется для управления паролями учетных записей служб. Его нельзя выбрать, если вы установили флажок Требовать

	смену пароля при следующем входе в систему **(*User Must Change Password At Next Logon)***
Срок действия пароля не ограничен (*Password Never Expires)*	Установите этот флажок, если хотите, чтобы срок действия пароля не истекал. При этом флажок Требовать смену пароля при следующем входе в систему (***User Must Change Password* At *Next Logon)*** будет автоматически снят, так как это взаимоисключающие параметры. Обычно используется для управления паролями учетных записей служб
Отключить учетную запись (*Account is disabled*)	Установите этот флажок для отключения учетной записи пользователя, допустим, при создании объекта для только что созданного пользователя, которому пока не требуется входить в сеть

Внимание! Администратор домена при создании объектов новых пользователей должен соблюдать следующие требования:

- для каждого пользователя создавать уникальный сложный пароль, не отвечающий какому-либо предсказуемому шаблону;
- включать параметр, который заставляет пользователя сменить пароль при следующем входе в систему;
- если пользователь не будет входить в сеть долгое время, отключать его учетную запись;
- когда пользователю в первый раз потребуется доступ к сети, убеждается, что эта учетная запись включена (тогда система попросит пользователя задать новый уникальный пароль, который будет известен только этому пользователю).

3.2.3 Создание нескольких объектов пользователей

В определенных случаях администратору домена требуется быстро создать множество объектов пользователей, например для целого класса новых учащихся в школе или группы новых сотрудников организации. В таких ситуациях необходимо знать, как эффективно упростить, или автоматизировать создание объектов пользователей, чтобы не создавать учетные записи по одной.

Это можно сделать при помощи шаблона, если объекты обладают одинаковыми свойствами. Например, все студенты потока могут принадлежать одной группе безопасности, им всем может быть разрешен вход в систему в одно и то же время, а их домашние папки и перемещаемые профили могут храниться на одном сервере. В таких случаях при создании объекта пользователя полезно предварительно задать для него общие свойства. Для этого можно создать общий объект пользователя, часто называемый шаблоном, и копировать его, создавая новые объекты пользователей. Чтобы сгенерировать шаблон, создайте объект пользователя и настройте его свойства. Поместите пользователя в требуемые группы.

Внимание! Чтобы гарантировать, что эта учетная запись не будет использована для доступа к сетевым ресурсам, обязательно отключите данного пользователя, так как это всего лишь шаблон.

Для создания объекта пользователя укажите нужный шаблон и в меню **Действие** (***Action***) щелкните **Копировать** (***Copy***). При этом потребуется задать некоторые свойства, также как и при создании нового объекта пользователя: имя и фамилию, инициалы, имя входа, пароль и параметры учетной записи. После создания объекта по шаблону можно видеть, что другие свойства были скопированы из шаблона согласно следующему алгоритму для вкладок:

- **Общие** (***General)*** — свойства не копируются;
- **Адрес (*Address*)** — копируются все свойства, кроме Улица (Street);
- **Учетная запись** (***Account***) — копируются все свойства, кроме имени входа, которое вам будет предложено ввести при копировании шаблона;
- Профиль (***Profile***) — копируются все свойства, а пути к профилю и домашней папке изменяются в соответствии с именем для входа нового пользователя;
- **Телефоны *(Telephones)*** — свойства не копируются;
- ***Организация (Organization***) — копируются все свойства, кроме Должность (Title);
- **Член групп (*Member Of)*** — копируются все свойства;
- **Входящие звонки (*Dial_in),* Среда (*Environment*)**, **Сеансы (*Sessions*)**, **Удаленное управление (*Remote Control*)**, **Профиль служб терминалов (*Terminal Services Profile*)**, **COM+ свойства** не копируются.

Внимание! Пользователь, объект которого был сгенерирован путем копирования шаблона, по умолчанию участвует в тех же группах, что и шаблон, то есть получает разрешения и права, назначенные этим группам. Однако разрешения и права, назначенные самому шаблонному объекту пользователя, не копируются и не переназначаются, поэтому у объектов пользователей, генерируемых по шаблону, их не будет.

3.2.4 Управление профилями пользователей

Администратор домена должен обеспечить пользователям домена, которые не являются специалистами в области информационных технологий настройку рабочей станции для удобной работы с ней. Например, если пользователь войдет в систему и не сможет получить доступ к папке **Избранное *(Favorites)*** в *Internet Explorer*, или не увидит знакомых ярлыков, сетевых дисков и документов на рабочем столе, производительность его труда резко снизится (а может работа станет невозможной), а в службу поддержки домена поступит звонок с требованием исправить положение. Все эти примеры относятся к компонентам "профиля пользователя". Профили

можно настраивать, повышая их доступность, безопасность и надежность. Профиль может быть локальным, перемещаемым, групповым и обязательным.

Профиль пользователя (*user profile)* — это набор папок и файлов данных, содержащих элементы среды рабочего стола конкретного пользователя. Профиль состоит из:

- ярлыков в меню **Пуск (*Start)*,** на рабочем столе и на панели быстрого запуска;
- документов на рабочем столе и, если не настроена переадресация, в папке **Мои документы** ***(My Documents)****;*
- избранных страниц и файлов «*cookie»* в *Internet Explorer*;
- сертификатов (если они внедрены в сети);
- специальных файлов приложений, например пользовательского словаря, шаблонов и списка автотекста в *Microsoft Office*;
- содержимого папки **Сетевое окружение** (***My Network Places***);
- параметров отображения рабочего стола, например его вида, фона и заставки.

Эти важные элементы у каждого пользователя свои. Желательно, чтобы они не изменялись между входами в систему, были доступны, если пользователю потребуется войти в систему на другой рабочей станции, и их можно было восстановить в случае, если система даст сбой и ее потребуется переустановить.

3.2.4.1 Локальные профили пользователей

По умолчанию профили пользователей хранятся локально в папке *%Systemdrive%\Documents and Settings\%Username%* и работают следующим образом *(%Systemdrive%* - это системная переменная, значение которой указывает диск на который установлена ОС; *%Username%* - это системная переменная, значение которой указывает **Имя входа пользователя (*User Logon Name))***.

Когда пользователь входит в систему впервые, система создает для него профиль путем копирования профиля **Пользователь по умолчанию *(Default User*)**. Имя для нового профиля формируется на основе имени для входа, указанного при первом входе в систему. Все изменения рабочего стола пользователя и программной среды хранятся в локальном профиле пользователя. Для каждого пользователя существуют отдельные профили, поэтому все параметры индивидуальны.

Настройка профиля пользователя может быть расширена за счет профиля **Все пользователи (*All Users*)**, который может включать ярлыки на рабочем столе или в меню **Пуск (*Start*)**, адреса компьютеров в сети и даже данные приложений. При входе пользователя в систему на рабочей станции

элементы профиля **Все пользователи** ***(All Users)*** соединяются с профилем пользователя. По умолчанию только члены группы **Администраторы (*Administrators)*** могут модифицировать профиль **Все пользователи (*All Users)***.

Профиль является локальным в том смысле, что если пользователь впервые входит в систему на другой станции для него генерируется новый локальный профиль из ***Default User*** этой станции. Поэтому пользователю придется заново производить его настройку.

3.2.4.2 Перемещаемые профили пользователей

Если пользователь в разное время может работать на нескольких компьютерах, то для него надо использовать перемещаемый профиль пользователя ***(roaming user profile, RUP),*** чтобы обеспечить сохранность и неизменность его документов и параметров вне зависимости от того, в какую систему он входит. RUP хранит профили на сетевом ресурсе, а значит, их можно архивировать, проверять на наличие вирусов и централизованно управлять ими. Даже если пользователи не перемещаются по рабочим станциям, RUP обеспечивает сохранность информации окружения среды пользователя. Если система на рабочей станции пользователя дала сбой и ее необходимо переустановить, RUP гарантирует, что новая пользовательская среда будет идентичная предыдущей.

Чтобы создать и настроить RUP, создайте общую папку на сетевом ресурсе. В идеальном случае это должен быть файловый сервер, на котором часто проводится архивирование.

Внимание! Настройте общий доступ так, чтобы всем ((Everyone) – это встроенная группа) был разрешен полный контроль над папкой (Full Control). Это разрешение надо сделать дополнительно, так как стандартное разрешение общего доступа в Windows Server 2000/2003/2008 позволяет только чтение папки, но этого недостаточно для настройки перемещаемого профиля.

На вкладке **Профиль** ***(Profile)*** диалогового окна **Свойства** ***(Properties)*** пользователя нужно ввести Путь к профилю (Profile Path) в следующем формате: \\<имя_компьютера>\<имя_общего_ресурса >\% *Username%.*

Вместо переменной *% Username%* будет автоматически подставлено имя входа пользователя.

При следующем входе пользователя система найдет местоположение перемещаемого профиля. Когда пользователь выходит из системы, его профиль выгружается на сервер профилей. Теперь пользователь может входить в любую рабочую станцию в домене, и его документы и настройки, являющиеся частью RUP, всегда будут загружены на неё.

Внимание! *Windows Server 2003/2008* представляет новую политику: Разрешать использование только локальных профилей (*Only Allow Local User*

Profiles). Эта политика, связанная с ОП, содержащим учетные записи компьютеров, не позволяет использовать на данных компьютерах перемещаемые профили. Вместо этого пользователи работают с локальными профилями.

Когда пользователь с RUP впервые регистрируется на рабочей станции, её ОС не копирует профиль (*Default User*), а загружает RUP из сетевого ресурса. Когда пользователь выходит из системы или входит в систему, на которой работал ранее, копируются только измененные файлы.

3.2.4.3 Синхронизация перемещаемого профиля

В отличие от предыдущих версий, *Windows Server 2003/2008* не загружают и не выгружают весь профиль пользователя при входе и выходе, а синхронизируют его. Между локальной системой и сетевой папкой для хранения RUP перемещаются только измененные файлы. Это означает, что вход и выход из системы с использованием RUP выполняется существенно быстрее, чем в предыдущих версиях *Windows*. Организации, которые не внедряли RUP из-за опасения, что такие профили будут отрицательно влиять на процесс входа в систему и сетевой трафик, должны еще раз оценить ситуацию с учетом этого момента.

3.3 Задание на лабораторную работу

3.3.1. Для изучения операций по созданию объектов пользователей и управление ими выполните следующие действия:

- зайти от имени администратора домена;
- создать организационное подразделение бригады в edu.vt;
- создать внутри него пользователей по каждому члену бригады со сменой пароля при первом входе;
- проверить вход каждого пользователя;
- заблокировать учетную запись и проверить вход;
- разблокировать учетную запись, и запретить смену пароля;
- войти от имени созданноно пользователя и попытаться сменить пароль.

3.3.2. Для изучения операций по созданию нескольких объектов пользователей ими выполните следующие действия:

- создать шаблон, заполнив все свойства объекта;
- заблокировать эту учетную запись;
- создать объект нового пользователя по шаблону;
- просмотреть его свойства в сравнении со свойствами шаблона.

3.3.3. Для изучения операций по управлению профилями пользователей ими выполните следующие действия:

- создать пользователя с локальным профилем, настроить его (ярлыки на рабочий стол, сетевой диск);
- обменяться местами с соседней бригадой и зайти от имени этого пользователя, убедиться, что профиль загружен по умолчанию;
- создать пользователя с перемещаемым профилем, настроить его (ярлыки на рабочий стол, сетевой диск);
- обменяться местами с соседней бригадой и зайти от имени этого пользователя, убедиться, что профиль загружен тот же самый профиль.

Отчет должен включать скриншоты каждого шага выполнения заданий.

3.4 Вопросы для самопроверки

1) Опишите различия между рабочей группой и доменом.
2) Можно ли установить Active Directory без установки DNS?
3) Можно ли создать домен без установки Active Directory?
4) Чем отличаются домен, дерево и лес в Active Directory?
5) Как устанавливается и удаляется Active Directory?

Лабораторная работа №4.

ГРУППОВЫЕ ПОЛИТИКИ

4.1 Цель работы

Целью работы является изучение способов задания и видов параметров групповых политик, приобретение навыков формирования групповых политик для разных объектов.

4.2. Теоретический материал

4.2.1 Общая характеристика групповых политик

Групповая политика — это набор правил, в соответствии с которыми производится настройка рабочей среды *Windows*. Групповые политики создаются в домене, реплицируются в его рамках и позволяют реализовать гибкое управление членами доменами – пользователями и компьютерами. Объект групповой политики состоит из двух физически раздельных составляющих: контейнера групповой политики GPC (*Group Policy Container*) и шаблона групповой политики GPT (*Group Policy Template*,). Эти два компонента содержат в себе всю информацию о параметрах рабочей среды, которая включается в состав объекта групповой политики. Продуманное применение объектов GPO к объектам каталога Active Directory позволяет создавать эффективную и легко управляемую компьютерную рабочую среду на базе ОС *Windows.* Политики применяются сверху вниз по иерархии каталога Active Directory.

4.2.2 Задание в домене политику при установке пароля пользователя

Рассмотрим пример задания в домене политику, в соответствии с которой на уровне всего домена при установке пароля пользователя требовалось бы следующее:

- длина пароля – не менее 8 символов;
- пользователь не может установить ни один из трех предыдущих паролей;
- пароль должен отвечать требованиям сложности;
- максимальный возраст пароля – 60 дней.

Для задания политики выполнить следующие действия:

- Для запуска консоли управления MMC выполните команду ***Start*** – ***Run – mmc.***
- Для управления объектами групповой политики на уровне домена в консоли MMC добавьте оснастку ***Group Policy Object Editor*** командой ***File*** **(Консоль)** – ***Add*** **(Добавить)** – ***Remove Snap-in*…** **(Добавить или удалить оснастку*)*** – **Add… (Добавить*)*** и выберите из списка соответствующую оснастку.

- Для определения объекта действия политики нажмите ***Browse…*** **(Обзор…)**

- Изучите окно и перечислите объекты групповых политик.

- Выберите ***Default Domain Policy.*** Нажмите ***Finish (*****Готово*****)***. В левом окне консоли должна появиться оснастка ***Default Domain Policy <имя контроллера домена> Policy.***

- Разверните оснастку и выберите ***Computer Configuration (*****Конфигурация компьютера*****) – *Windows Settings (*****Конфигурация *Windows*)*** **– *Security Settings (*****Параметры безопасности*****) – *Account Policies (*****Политики учетных записей*****) – *Password Policy*** **(Политика паролей*).***

- Изучите политики паролей и установите настройки в соответствии с требованием задания.

- Создайте нового пользователя и проверьте правильность настроек.

4.2.3 Задание в домене политику блокировки учетных записей

Рассмотрим пример задания политику на уровне всего домена, выполняющую блокировки учетных записей на 5 минут в том случае, если подряд было сделано не менее трех ошибок входа в систему.

Для задания политики выполнить следующие действия:

- Соответствующая политика находится в следующем разделе: ***Computer Configuration*** **(Конфигурация компьютера*) - *Windows Settings*** **(Конфигурация Windows) - *Security Settings*** **(Параметры безопасности*) - *Account Policies*** **(Политики учетных записей) - *Account Lockout Policy*** **(Политика блокировки учетной записи).**

- Проверьте правильность настроек политики путем нескольких попыток ввести неверный пароль пользователя на рабочей станции.

- Зайдите на контроллер домена и разблокируйте учетную запись пользователя.

4.2.4 Создание организационного подразделения

Для создания организационного подразделения ***StudentSecurity*** необходимо выполнить следующие действия:

- Выполните команду ***Start*** - ***Programs*** - ***Administrative Tools*** - ***Active Directory Users and Computers (*****Пуск - Программы - Администрирование - Пользователи и компьютеры Active Directory)**.

- Раскройте папку ***mydomen*** в левой панели окна.

- В меню ***Action*** выберите команду ***New*** - ***Organization Unit (*****Создать - Организационное подразделение).**

- В окне ***New Object*** - ***Organization Unit (*****Новый объект - Подразделение*)** в поле ***Nam*****е** наберите ***StudentSecurity***.

- Поместите в организационное подразделение учетную запись студента.
- Правой кнопкой щелкните по новому объекту, выберите ***Properties*** **(Свойства) -** ***Security*** **(Безопасность)**.
- Просмотрите список групп, обладающих правом доступа к подразделению ***StudentSecurity***.

4.2.5 Задание политики на уровне организационного подразделения

Рассмотрим пример задания политики на уровне **организационного подразделения *StudentSecurity,*** запрещающей менять картинку рабочего стола и загружающую общую для всех картинку. Для задания политики выполнить следующие действия:

- Откройте окно **StudentSecurity**.
- Выполните команду ***User Configuration*** **(Конфигурация пользователя) -** ***Administrative Templates*** **(Административные шаблоны) -*Desktop*** **(Рабочий стол) -** ***ActiveDesktop***, выберите параметр, запрещающий изменение картинки и задайте общую картинку рабочего стола для всего подразделения.
- Убедитесь в правильности настройки.

4.3 Задание на лабораторную работу

Выполните последовательно все операции по созданию и тестированию групповых политик, описанные в п. 4.2.

Включите в отчет скриншоты, отражающие каждый шаг выполнения задания.

4.4 Вопросы для самопроверки

1) Дайте определение групповой политики.
2) К каким объектам можно применить групповые политики?
3) Где расположен объект локальной групповой политики?
4) Приведите примеры нелокальных объектов групповой политики.
5) В чем разница между конфигурационными и пользовательскими параметрами?
6) Перечислите требования к сложному паролю.

Лабораторная работа №5.

УЧЕТНЫЕ ЗАПИСИ КОМПЬЮТЕРОВ

5.1 Цель работы

Целью работы является навыков присоединять компьютеры к домену и задавать и изменять права доступак ним, изучение способов публикации ресурсов и запуска приложения от имени другого пользователя.

5.2. Теоретический материал

5.2.1 Общая характеристика учетные записи компьютеров

Каждый компьютер, работающий под управлением *Windows NT, Windows 2000, Windows XP* или сервер под управлением *Windows Server 2003/2003*, который присоединяется к домену, имеет учетную запись компьютера, которая, Так же, как и учетная запись пользователей, предоставляетт возможность проверки подлинности и аудита доступа компьютера к сети и к ресурсам домена. Учетная запись компьютера должна быть уникальной.

Учетные записи компьютеров и пользователей добавляются, отключаются, восстанавливаются и удаляются с помощью оснастки *Active Directory* — пользователи и компьютеры. Учетная запись компьютера может быть создана при подключении компьютера к домену.

Когда функциональный уровень домена установлен в режиме *Windows Server 2003*, появляется новый атрибут ***lastLogonTimestamp***. Он используется для отслеживания времени последнего входа для учетных записей пользователей или компьютеров. Этот атрибут реплицируется в домене и дает возможность получать необходимую информацию при просмотре журналов пользователя или компьютера.

5.2.2 Включение рабочей станцию в домен

Для того, что бы включить рабочую станцию в домен, необходимо:

- задать следующие сетевые параметры рабочей станции: имя рабочей станции - ***user1***; IP-адрес назначить из той же сети, что и контроллер домена (если не работает сервер DHCP);
- проверить возможность установления связи между контроллером домена и рабочей станцией.
- включить рабочую станцию в домен.

Выполнить следующую последовательность действий:

- Для присоединения компьютера к домену на рабочей станции следует открыть окно **System Properties** (**Свойства системы**), выполнив одну из команд **Settings** (**Настройка**) - **Control Panel** (**Панель управления**) -**System** (**Система**) или вызвать из контекстного меню окно свойств папки **My Computer** (**Мой компьютер**).

- Перейдите на вкладку **Computer Name** (**Имя компьютера**).
- Выберите **Network ID** (**Идентификация**). Откроется мастер сетевой идентификации **Network Identification Wizard**. Нажмите **Next** (**Далее**).
- На вкладке **Connecting to the Network** (**Подключение к сети**) выберите **This computer is part of a business network, and I use it to connect to other computers at work** (**Компьютер входит в корпоративную сеть, и во время работы я использую его для соединения с другими компьютерами**). На этой вкладке существует второй вариант. Какой? В каких случаях он применяется?
- Выберите тип сети - ***My company uses a network with domain*** (**Моя организация использует сеть с доменами**).
- В окне ***Network Information*** (**Сетевая информация**) изучите, какие сетевые параметры понадобятся.
- В окне ***User Account and Domain Information*** (**Сведения об учетной записи и домене**) оставьте все без изменения. Нажмите **Next**.
- В окне ***Computer Domain*** (**Домен компьютера**) запишите имя домена и узла - ***Computer name*** (**Имя компьютера**) - ***user1***, а ***Computer domain*** (**Домен компьютера**) -**mydomen**. Нажмите **Next**.
- Появится окно, в котором нужно ввести имя и пароль учетной записи, которая имеет разрешение на добавление пользователей в домен. Например, в нашем случае это будут:
- ***User name*** - **Administrator**
- ***Password*** - пустой (или текущий пароль администратора)
- ***Domain - mydomen***
- В окне ***User Account*** будет предложено добавить новых пользователей. Выберите переключатель ***Do not add user at this time*** (**Не добавлять пользователей в это время**).
- Нажмите ***Finish*** (**Готово**) и перезагрузите компьютер.

5.2.3 Удаление рабочей станции из домена

Для того, чтобы удалить **рабочую станцию из домена** небходимо выполнить следующую последовательность действий:

- На рабочей станции войдите под учетной записью администратора.
- Вызовите окно свойств папки **My Computer** (**Мой компьютер**).
- На вкладке ***Computer Name*** (**Имя компьютера**) нажмите ***Network ID*** (**Идентификация**).
- На вкладке ***Connecting to the Network*** (**Подключение к сети**) выберите ***This computer is for home use and not a part of business network***

(**Компьютер предназначен для домашнего использования и не входит в корпоративную сеть**).

5.3 Задание на лабораторную работу

Выполните последовательно все операции по созданию изменению и учетных записей компьютеров, описанные в п. 5.2.

Включите в отчет скриншоты, отражающие каждый шаг выполнения задания.

5.4 Вопросы для самопроверки

1) Как определить, является ли компьютер членом домена или рабочей группы?

2) Какие разрешения существуют для общих папок?

3) Как отменить наследование свойств объекта от родительской папки?

4) Может ли пользователь запретить доступ администратору к своей папке, а может ли администратор в этом случае вернуть права?

5) Опишите права субъектов доступа - Владелец и Администратор.

Лабораторная работа № 6

УЧЕТНЫЕ ЗАПИСИ ГРУПП

6.1 Цель работы

Целью работы является приобретение навыков создания групп, изменение состава группы и нахождение доменных групп, к которым относится пользователь.

3.2. Теоретический материал

3.2.1 Общая характеристика учетных записей групп

Пользователи, компьютеры и группы - ключевые объекты в службе каталогов *Active Directory*, так как они позволяют всем, кто использует компьютер в сети, идентифицировать себя в качестве участника безопасности. Без такой идентификации персонал не сможет получить доступ к компьютерам, программам и данным, необходимым для повседневной работы. Хотя для минимальной идентификации достаточно знать имя пользователя и компьютера, управление участниками безопасности для каждого отдельного пользователя серьезно усложнит работу администратора домена, если не организовать пользователей в группы. На определенном этапе назначать разрешения каждому из большого множества пользователей станет просто невозможно. При использовании групп - назначение разрешений и управление для пользователей сильно упрощается.

В *Windows Server 2003/2008* существует два типа групп, каждая из которых может иметь три области действия. Понимание их структуры в рамках соответствующей области действия гарантирует оптимальное распределение административных ресурсов при управлении правами доступа к ресурсам. Возможности конструкции группы также зависят от того, в каком режиме работает их родительский домен или лес *Windows Server 2003/2008:* основном, промежуточном или смешанном. В *Windows Server 2003/2008* несколько групп уже созданы предварительно, или встроены. Вы можете создать дополнительно столько групп, сколько пожелаете.

Область действия группы (*group scope*) определяет, каким образом участникам группы назначаются разрешения. В *Windows Server 2003/2008* и группы безопасности, и группы распространения классифицируют по трем областям действия: локальная доменная, глобальная и универсальная.

Локальные группы (*local groups*) компьютера используются в основном для обратной совместимости с *Windows NT 4*. На компьютерах с *Windows XP* существуют локальные пользователи и группы, но контроллеры доменов не используют локальные группы. Локальные группы могут содержать участников из любого домена в пределах леса, из доверенных доменов в других лесах и более низкого уровня. Локальная группа действует в пределах конкретного компьютера и может предоставлять разрешения для ресурсов только на этом компьютере.

Локальные группы домена (*domain local groups*) главным образом используются для назначения глобальным группам разрешений на доступ к локальным ресурсам домена. Характерные черты локальных групп домена таковы:

- существуют во всех режимах работы доменов и лесов — смешанном, промежуточном и основном;
- доступны в пределах всего домена только в доменах основного режима Windows 2000 или доменах Windows Server 2003/2008.

Локальная группа домена функционирует подобно локальной группе на контроллере домена, пока домен работает в смешанном режиме. Локальные группы могут содержать участников из любого домена в пределах леса, из доверенных доменов в других лесах и более низкого уровня. Действуют в пределах домена в основном режиме *Windows 2000* и режиме *Windows Server 2003/2008* и могут использоваться для предоставления прав на ресурсы на любом компьютере с *Windows Server 2003/2008* в том домене, где определена группа.

Глобальные группы (*global groups*) чаще используются для предоставления категоризированного членства в локальных группах доменов для отдельных участников безопасности и для прямого назначения разрешений (в частности, в доменах смешанного или промежуточного режимов). Часто глобальные группы применяются для объединения пользователей или компьютеров в одном домене и совместного исполнения одной работы, роли или функции. Характеристики глобальных групп таковы:

- существуют во всех режимах работы доменов и лесов — смешанном, промежуточном и основном,
- могут содержать только членов из своего домена,
- могут сами являться членами локальной группы компьютера или домена,
- могут получать разрешения в любом домене, включая доверенные домены в других лесах и домены пред-Windows 2003/2008,
- могут содержать другие глобальные группы, но только в домене, работающем в основном режиме Windows 2000 или в режиме Windows Server 2003/2008.

Универсальные группы (*universal groups*) в основном применяют для предоставления доступа к ресурсам во всех доверенных доменах. Однако такие группы могут использоваться только как участники безопасности (то есть как группы безопасности) в доменах, работающих в основном режиме Windows 2000 или в режиме *Windows Server 2003/2008.* Универсальные группы могут содержать участников из любого домена в лесу. В домене основного режима *Windows 2000* или режима *Windows Server 2003/2008*

универсальным группам могут предоставляться разрешения в любом домене, включая доверенные домены в других лесах.

Универсальные группы помогают представить и объединить группы, которые распределены по разным доменам и выполняют типичные функции в рамках вашей организации. Рекомендуется делать универсальными широко используемые и редко изменяемые группы.

Консоль ***Active Directory* — пользователи и компьютер**ы (***Active Directory Users And Computers***) является основным средством для создания групп, указания области действия, типа и состава членов группы.

6.2.2 Создание и изменение группы

Для создания и изменения групп необходимо выполнить выполнить следующую последовательность действий:

- В консоли **Active Directory — пользователи и компьютеры** раскройте свой контейнер и создайте в нем глобальную группу распространения **Агенты**.

- Щелкните правой кнопкой группу **Агенты** и выберите **Свойства (*Properties*)**. Проверьте, можете ли вы изменить область действия и тип этой группы. Если вы не можете изменить тип и область действия группы, значит ваш домен работает в смешанном режиме *Windows 2000* или в промежуточном режиме *Windows Server 2003/2008.* Чтобы изменить тип или область действия группы, необходимо перевести домен в основной режим *Windows 2000* или в режим *Windows Server 2003/2008*.

6.2.3 Управление учетными записями групп

Для управления учетными записями групп необходимо выполнить следующую последовательность действий:

- Для создания группы безопасности в окне консоли **Active Directory — пользователи и компьютеры (*Active Directory Users And Computers)*** щелкните правой кнопкой в правой панели контейнера, где вы хотите создать группу, и выберите **Создать (*New*)\Группа (*Group*).** Затем определите тип и область действия создаваемой группы.

В домене смешанного или промежуточного режима группа безопасности может быть только глобальной или локальной группой домена. В таком домене нельзя создать группу безопасности с универсальной областью действия (рисунок 6.1). Впрочем, локальную группу домена, глобальную или универсальную группу в доменах смешанного или промежуточного режима можно создать в виде группы распространения. Группы безопасности в таком домене могут иметь локальную доменную или глобальную область действия.

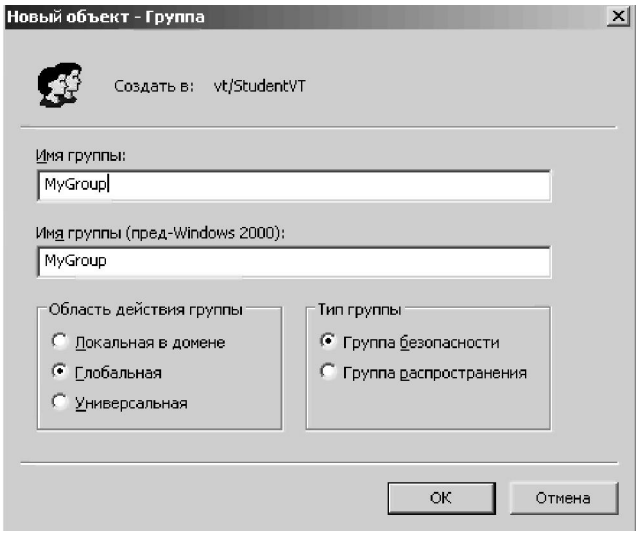

Рисунок 6.1. Создание группы безопасности в доменах смешанного или промежуточного режима

- **Изменение состава группы.** Добавление или удаление членов группы также выполняется из консоли **Active Directory — пользователи и компьютеры (*Active Directory Users And Computers*)**. Щелкните правой кнопкой любую группу и выберите **Свойства (*Properties*)**. На рисунке 6.2 показано окно свойств для глобальной группы безопасности ***MyGroup***.

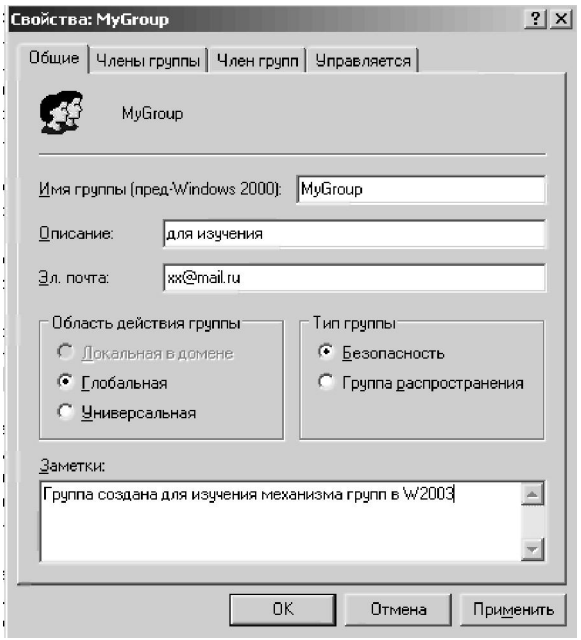

Рис. 4.4. Окно свойств группы безопасности MyGroup

В таблице 6.1 описаны вкладки этого окна свойств для настройки членства.

Таблица 6.1. Настройка членства

Вкладка	Назначение
Члены группы (*Members*)	Добавление, удаление и отображение списка участников безопасности — членов этого контейнера
Член групп (*Member)*	Добавление, удаление и отображение перечня контейнеров, членом которых является данный контейнер

Примечание. Домен должен работать в режиме *Windows Server 2003/2008*. Если это не так, измените режим домена в консоли **Active Directory — пользователи и компьютеры:**

- Создайте три глобальные группы в своем ОП: **Группа1, Группа 2 и Группа.**
- Добавьте три учетные записи пользователей: ***User1, User2 и User3.***
- Добавьте ***User1, User2 и User3*** в группу **Группа1**.
- Добавьте **Группа1** в группу **Группа2.** Проверьте возможность преобразования групп в универсальные.

6.3 Задание на лабораторную работу

Выполните последовательно все операции по созданию и изменению групп, описанные в п. 6.2.

Включите в отчет скриншоты, отражающие каждый шаг выполнения задания.

6.4 Вопросы для самопроверки

1) Какой тип доменной группы больше всего похож на локальную группу на рядовом сервере? В чем их сходство?

2) Какие участники безопасности могут быть членами глобальной группы в домене, работающем в режиме Windows Server 2003/2008?

3) На какой вкладке в окне свойств группы можно добавить в нее пользователей?

4) Вы хотите, чтобы группа ***IT Administrators***, члены которой администрируют участников группы ***MyGroup***, была вложена в ***MyGroup*** и имела доступ к тем же ресурсам, что и ***MyGroup***. На какой вкладке в окне свойств группы ***IT Administrators*** можно выполнить такую настройку?

Лабораторная работа №7.

ФАЙЛЫ И ПАПКИ

7.1 Цель работы

Целью работы является приобретение навыков работы с редактором таблицы управления доступом **(ACL) и** управления общими папками, изучение возможности оснастки **Общие папки**.

7.2. Теоретический материал

7.2.1 Общая характеристика управления свойствами Папок и файлов

Если с помощью проводника, выбрать какой либо файл или папку, нажать правую кнопку мыши и выбрать в контекстном меню Свойства, то можно получить доступ к двум вкладкам: **Безопасность и Доступ.**

Вкладка **Безопасность** определяет права доступа к файлу или папке интерактивных пользователей, т.е. пользователей, которые регистрируются (работают) на компьютере, в котором на устройстве хранения с файловой системой NTFS эти файлы или папки расположены.

Вкладка **Доступ** определяет права доступа к файлу или папке пользователей, которые подсоединяются к компьютеру, хранящему эти файлы или папки на устройстве хранения с файловой системой NTFS по сети.

Вначале рассмотрим настройку разрешений NTFS с использованием вкладки **Безопасность**.

7.2.2 Настройка разрешений NTFS

Для управления настройкой разрешений NTFS необходимо выполнить следующую последовательность действий:

- Создайте папку D:\Docs.
- Откройте папку D:\Docs, и создайте папку с именем ***Project101***.
- Откройте редактор ACL, щелкнув папку Project101 правой кнопкой, выберите **Свойства** ***(Properties***) и перейдите на вкладку **Безопасность** ***(Security).*** Просмотрите кто имеет права на эту папку и различие в этих правах.
- Настройте доступ согласно таблице 7.1. Для этого продумайте и настройте наследование и разрешения для групп.
- Когда нужные разрешения будут настроены, щелкните **Применить (*Apply*)**, а затем **Дополнительно (*Advanced*)**. Сравните открывшееся окно **Дополнительные параметры безопасности (*Advanced Security Settings)*** с примером на рисунке 7.1.

Таблица 7.1 Настройка доступа

Участник безопасности	*Доступ*
***Администраторы*(Administrators)**	*Полный доступ* (*Full Control*)
Пользователи из группы *Project101 Team*	Чтение данных, создание файлов и папок, полный доступ к собственным файлам и папкам
Группа *Managers*	Чтение и изменение любых файлов, запрет на удаление чужих файлов. Полный доступ к собственным файлам и папкам
System	Службы, запущенные под учетной записью System, должны иметь полный доступ

Для настройки этих разрешений необходимо запретить наследование. Иначе все пользователи, а не только члены группы ***Project101 Team,*** смогут читать файлы в папке ***Project101***. От родительской папки, C:\Docs, группа ***Users*** **(Пользователи**) наследует разрешение **Чтение и выполнение *(Read & Execute).*** Единственный способ запретить такой доступ - снять флажок **Разрешить наследование разрешений от родительского объекта к этому объекту (*Allow Inheritable Permissions From The Parent To Propagate To This Object).*** Заметьте: требования не указывают запретить чтение группе ***Users*** **(Пользователи),** но там и не говорится, что этой группе доступ на чтение необходим. В таких случаях рекомендуется предоставлять минимально требуемый доступ.

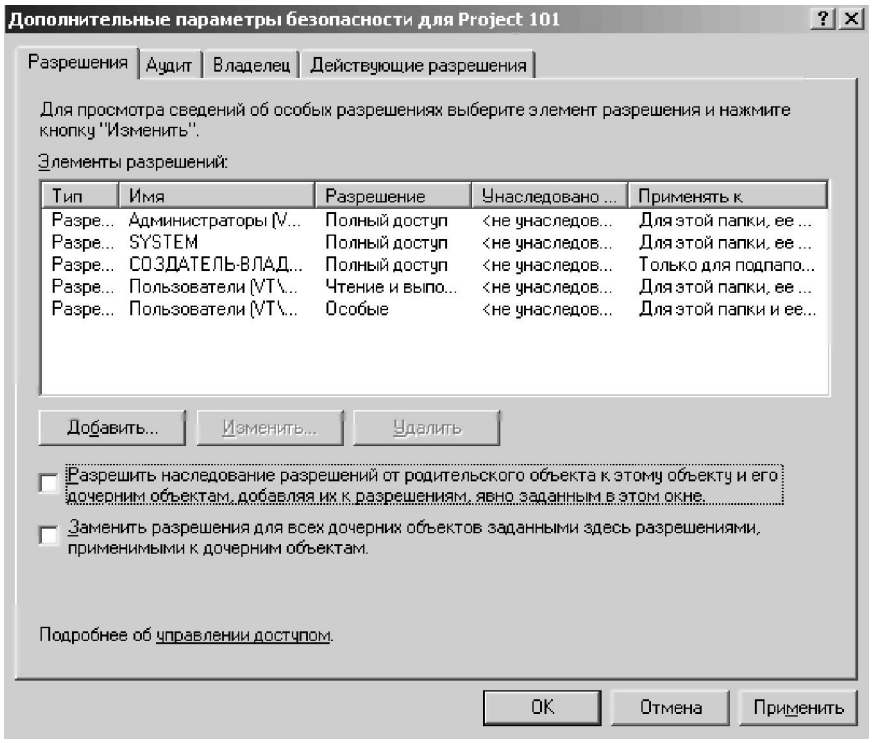

Рисунок 7.1. Вкладка **Дополнительные параметры безопасности**

После отмены наследования диалоговое окно Дополнительные параметры безопасности должно выглядеть, как показано на рисунке 7.1.

Флажок, отвечающий за наследование, был снят, и все разрешения отображаются с пометкой не унаследовано (***not inherited).*** Учетным записям:

Администраторы, System и Создатель-владелец предоставлен полный доступ.

Помните, что, когда учетной записи **Создатель-владелец** предоставлен полный доступ, пользователь, создавший файл или папку, получает полный доступ к этому ресурсу. Указано, что группа ***Project101*** обладает особым элементом разрешения. Учетной записи ***Managers*** предоставлены разрешения **Чтение, Запись и Выполнение**. Этот шаблон содержит разрешения на создание файлов и папок. Как и группе ***Project101***, членам группы ***Managers*** при создании новых ресурсов предоставляются разрешения учетной записи Создатель-владелец. Этот набор разрешений не позволяет группе ***Managers*** удалять файлы других пользователей. Помните, что разрешение **Удаление** содержится в шаблоне **Изменение**, который вы не указали.

7.2.3 Использование запретов

Более тонкую настройку прав доступа можно выполнить, используя **разрешения** и **запреты**, через вкладку **Действующие разрешения** как показано на рисунке 7.2.

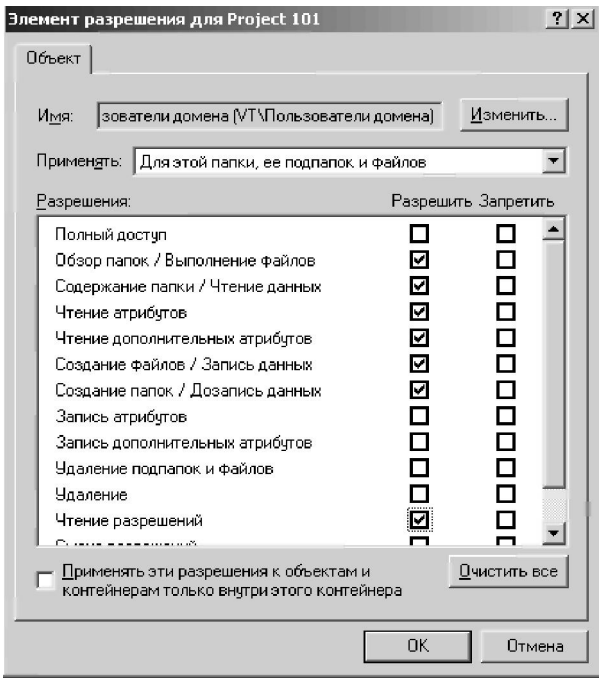

Рисунок 7.2. Особые разрешения, назначенные группе Пользователи домена

7.2.3 Право владения

При создании пользователем папки или файла он автоматически становится её владельцем с правами, назначенными ОС по умолчанию. В последующем может возникнуть необходимость сменить владельца, например, бывший владелец уволился и т.п. Это делается следующим образом:

- Войдите в систему как обычный пользователь (используя одну из учетных записей созданных вами).
- Откройте общую папку, подключившись **к \\kit-edu\Docs.**
- Откройте папку ***Project101*** и создайте текстовый файл с именем ***Report***.
- Из окна свойств файла ***Repor***t откройте окно **Дополнительные параметры безопасности (*Advanced Security Settings*)**.
- Убедитесь, что все разрешения наследуются от родительской папки. Папка ***Project101*** дает полный доступ учетной записи **Создатель-владелец (*Creator Owne*r)**. Файл Report предоставляет полный доступ пользователю. Когда он создал этот файл, ее идентификатору SID были назначены разрешения, которыми владела особая группа **Создатель-владелец**. Кроме того, разрешения **Создание файлов (*Create Files)* и Создание папок (*Create Folders),*** предоставленные группе ***Project101 Team***, относятся к папкам, а потому отсутствуют в ACL файла ***Report***.
- Войдите в систему как **Администратор (*Administrator*)**.
- Из окна свойств файла Report откройте окно **Дополнительные параметры безопасности (*Advanced Security Settings*)**.
- Перейдите на вкладку **Владелец (*Owner*)**.
- Посмотрите, кто текущий владелец.
- Выберите свою учетную запись и щелкните **Применить (*Apply).*** Теперь вы стали владельцем данного объекта.
- Пользователь с **привилегией Администратор (*Administrator*)** может передать права владения другому пользователю. Щелкните **Иные пользователи или группы (*Other Users Or Group*)** и выберите другую учетную запись. Когда она появится в списке **Изменить владельца на (*Change Owner To*)**. щелкните **Применить (*Apply*)**.
- Убедитесь, что этот **пользователь** теперь владеет файлом Report.

Теперь рассмотрим **настройку** разрешений NTFS с использованием вкладки **Доступ** (рис.4.7).

Администратор должен осуществлять поддержку сетевых файлов и папок. Создание общих папок для обеспечения удаленного доступа является одной из важных задач сетевого администратора. **Общие папки, это такие папки**, к которым можно получить доступ **с любого компьютера в сети**, при условии наличия соответствующего разрешения. Открытие общего доступа к папке указывает **Службе доступа к файлам и принтерам сетей *Microsoft (File And Printer Sharing For Microsoft Networks)*** разрешить клиентам, на компьютерах которых запущена служба **Клиент для сетей *Microsoft (Client For Microsoft Networks)***, подключаться к этой папке и ее подпапкам.

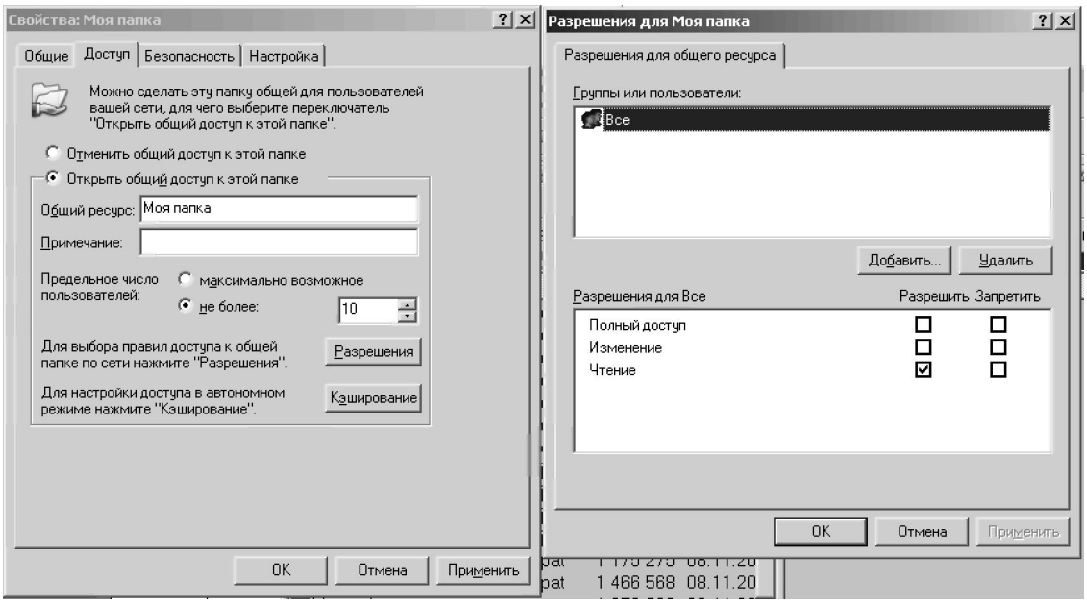

Рисунок 7.3. Вкладка **Доступ** диалогового окна свойств общей папки **Моя папка**

Чтобы создать общую папку с помощью **Проводника** Windows нужно щелкнуть папку правой кнопкой, выбрать **Доступ (*Sharing*)** и установить переключатель **Открыть общий доступ к этой папке (*Share This Folder*)**. Однако вкладка **Доступ (*Sharing*)** окна свойств папки в **Проводнике** Windows доступна, только когда вы входите в систему локально или с помощью служб терминалов, а создать общую папку на удаленном компьютере нельзя. Поэтому рассмотрим создание, свойства, конфигурацию и управление общими папками с помощью оснастки **Общие папки (*Shared Folders*)**, которую можно использовать как локально, так и удаленно.

Открыв оснастку **Общие папки** (***Shared Folders***) в настраиваемой консоли MMC или в консолях **Управление компьютером (*Computer Management)*** или **Управление файловым сервером (*File Server Management)*,** можно сразу заметить, что в *Windows Server 2003/2008* уже настроено несколько стандартных административных общих ресурсов: системный каталог (обычно C:\Windows) и корень каждого жесткого диска. Имя ресурса для таких общих папок заканчивается знаком доллара ($). Знаком доллара в конце сетевого имени обозначают скрытые общие папки. Они не видны в обозревателе, но к ним можно подключиться по UNC-имени вида *\\имя_сервера\имя_общего_ресурса$*. К административным общим ресурсам могут подключаться только администраторы.

Для открытия общего доступа к папке, подключитесь к нужному компьютеру из оснастки Общие папки: щелкните корневой узел **Общие папки *(Shared Folders)*** правой кнопкой и выберите **Подключиться к другому компьютеру (*Connect To Another Computer*).** Выбрав компьютер, щелкните узел **Общие папки (*Shares*),** а затем в контекстном меню или в меню **Действие (*Action*)** выберите **Новый общий ресурс (*New* Share).**

Мастер создания общих ресурсов содержит следующие страницы и настройки:

- Страница ***Folder Path*** **(Путь к папке).** Укажите путь к общей папке на локальном жестком диске, например, если папка находится на диске D: сервера, путь к ней будет иметь вид D:\имя_папки.

- Страница ***Name, Description, and Settings*** **(Имя, описание и параметры).** Введите имя общего ресурса. Если к сети подключены устаревшие клиенты (например, компьютеры под управлением DOS), старайтесь придерживаться правил именования NNNNNNNN.RRR, чтобы обеспечить им доступ к общим папкам. Имя ресурса вместе с именем сервера образуют UNC-имя вида **\\имя_сервера\имя_общего_ресурса**. Добавьте знак доллара в конце сетевого имени, чтобы сделать общий ресурс скрытым. В отличие от встроенных скрытых административных общих ресурсов, к скрытым общим папкам, созданным вручную, может подключиться любой пользователь, причем его права ограничиваются только разрешениями общего ресурса.

- Страница **Разрешения (*Permissions*).** Выберите подходящие разрешения общего ресурса.

Узел Общие **папки (*Shares*)** в оснастке **Общие папки (*Shared* Folders)** содержит список всех общих ресурсов компьютера и для каждого из них предоставляет контекстное меню, которое позволяет прекратить доступ, открыть общий ресурс в **Проводнике** или настроить его свойства. Все свойства, которые предлагает заполнить мастер **Мастер создания общих ресурсов (*Share* A Folder Wizard)**, можно изменить в окне свойств общего ресурса (рисунок . 7.4).

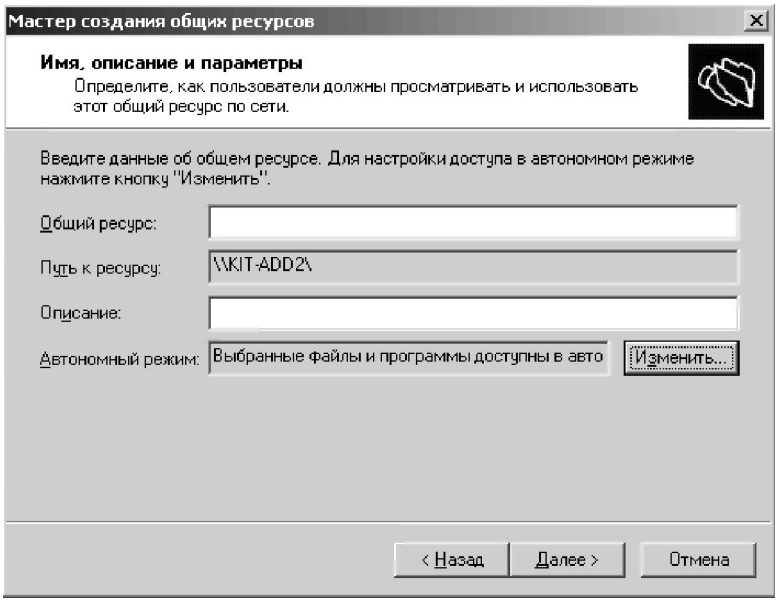

Рисунок 7.4. Мастер создания общих ресурсов ***(Share A Folder Wizard)***

При создании общей папки (ресурса) в поле **Общий ресурс** указывается его имя, которое может не совпадать с именем папки, а в поле **Описание** можно указать назначение ресурса. Обратите внимание, что имя общего ресурса и путь к нему предназначены в операционной системе только для чтения. Чтобы переименовать общий ресурс, нужно сначала закрыть доступ, а затем создать общий ресурс с новым именем.

Кнопка **Разрешения** (***Share Permissions***) служит для настройки разрешений доступа к общему ресурсу. Доступные разрешения общего ресурса перечислены в табл. 7.2. Хотя они не настолько подробны, как разрешения NTFS, но позволяют настроить основные типы доступа к общей папке: **Чтение** (***Read***)**, Изменение (*Change*)** и **Полный доступ (*Full Control*)**.

Табл. 7.3. Разрешения для общего ресурса

Разрешение	Описание
Чтение (Read)	Пользователи могут просматривать имена папок, а также имена, содержимое и атрибуты файлов, запускать программы и обращаться к другим папкам внутри общей папки
Изменение (*Change*)	Пользователи могут создавать палки, добавлять файлы и редактировать их содержимое, изменять атрибуты файлов, удалять файлы и папки и выполнять действия, допустимые разрешением *Чтение* (*Read*)
Полный доступ (*Full Control*)	Пользователи могут изменять разрешения файлов, становится владельцами файлов и выполнять все действия, допустимые разрешением *Изменение* (*Change*)

Разрешения общего ресурса можно предоставлять или отменять. Действующим набором разрешений общего ресурса называют сумму разрешений, предоставленных пользователю и всем группам, членом которых он является. Например, если пользователь входит в группу с разрешением **Чтение *(Read)*** и в группу с разрешением **Изменение (*Change*)**, действующим разрешением считается Изменение. Тем не менее, запрет всегда приоритетнее разрешения. Например, если пользователь входит в группу с разрешением **Чтение *(Read)*** и в группу, которой запрещено разрешение **Полный доступ (*Full Control*),** он не сможет прочитать файлы и папки внутри общего ресурса.

Разрешения общего ресурса определяют максимальные действующие разрешения для всех файлов и папок внутри общей папки. Назначая разрешения NTFS для отдельных файлов и папок, доступ можно ужесточить, но не расширить. Другими словами, доступ пользователя к файлу или папке определяется наиболее жестким набором из разрешений общего ресурса и разрешений NTFS. Если разрешения NTFS дают группе полный доступ к папке, а разрешения общего ресурса остаются стандартными — группе **Все (**Everyone) предоставлено разрешение **Чтение *(Read)*** или даже **Изменение (*Change)* —**

разрешения NTFS ограничиваются разрешением общего ресурса. Этот механизм означает, что разрешения общего ресурса усложняют управление доступом к ресурсам. Это одна из причин, по которой в организациях обычно назначают общим ресурсам открытые разрешения: группе **Все (Everyone)** дается разрешение **Полный доступ *(Full Control*),** а для защиты папок и файлов используют только разрешения NTFS.

Разрешения общего ресурса имеют ряд существенных ограничений:

- **Область действия.** Разрешения общего ресурса применяют только для ограничения удаленного доступа через службу ***Клиент для сетей Microsoft* (*Client for Microsoft Networks*)**; они не распространяются ни на локальный доступ, ни на доступ через службы терминалов, ни на любые другие типы удаленного доступа, например по протоколам HTTP, FTP, Telnet и т. п.

- **Репликация.** Разрешения общего ресурса игнорируются **Службой репликации файлов (*File Replication Service, FRS*)**.

- **Устойчивость.** Разрешения общего ресурса не сохраняются при архивировании или восстановлении тома данных.

- **Хрупкость.** Разрешения общего ресурса теряются при перемещении или переименовании папки.

- **Недостаточно детальный контроль.** Разрешения общего ресурса не поддерживают тонкую настройку; они предлагают один шаблон разрешений, который применяется ко всем файлам и папкам внутри общей папки. Нельзя расширить или ограничить доступ к файлам и папкам внутри общей папки без применения разрешений NTFS.

- **Аудит.** Нельзя настроить аудит на основе разрешений общего ресурса.

7.3 Задание на лабораторную работу

Выполните последовательно все операции по управлению файлами и папками, описанные в п. 7.2.

Включите в отчет скриншоты, отражающие каждый шаг выполнения задания.

7.4 Вопросы для самопроверки

1) Какие минимальные разрешения NTFS требуются, чтобы пользователи могли открывать файлы и запускать программы из общей папки?

2)Пользователь ***Ivan*** жалуется, что не может получить доступ к плану отдела. Вы открываете вкладку **Безопасность (*Security*)** в окне свойств плана и видите, что все разрешения доступа к документу наследуются от родительской папки плана. Для группы, куда включен ***Ivan,*** разрешение **Чтение (*Read*)** отменено. Какое действие позволило бы пользователю ***Ivan*** получить доступ к плану?

Лабораторная работа №8.

АУДИТ ДОСТУПА К ФАЙЛОВОЙ СИСТЕМЕ

8.1 Цель работы

Целью работы является приобретение навыков аудита доступа к файлу или папке и анализа событий, зарегистрированные в журнале безопасности

8.2. Теоретический материал

8.2.1 Общая характеристика аудита доступа к файловой системе

Аудит доступа к файловой системе используется для оценки использования ресурсов и определения потенциально слабых мест в системе защиты. Windows Server 2003/2008 поддерживает подробный аудит на основе учетных записей пользователей или групп и определенных действий этих записей. Для настройки аудита необходимо указать его параметры, включить политику и изучить события в журнале безопасности.

8.2.2 Настройка параметров аудита

Чтобы указать действия, которые нужно наблюдать, следует настроить параметры аудита в диалоговом окне **Дополнительные параметры безопасности (*Advanced Security Settings*)** файла или папки. Вкладка **Аудит (*Auditing*)** (рисунок 8.1) похожа на вкладку **Разрешения (*Permissions*)**. Только вместо элементов разрешений вы добавляете элементы аудита.

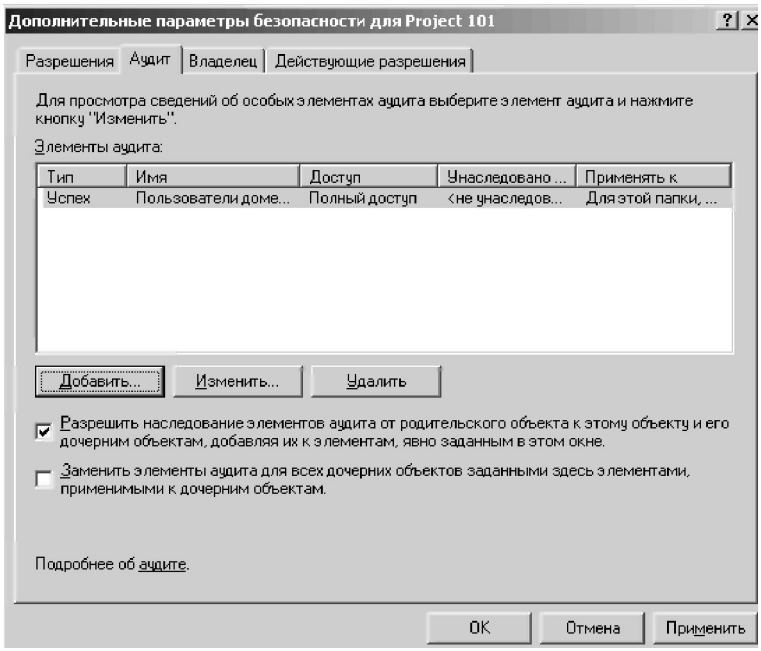

Рисунок 8.1. Вкладка Аудит диалогового окна Дополнительные параметры безопасности

Щелкните кнопку **Добавить (*Add*)**, чтобы выбрать пользователя, группу или компьютер для аудита. Затем в диалоговом окне **Элемент аудита (*Auditing Entry*)** укажите разрешения, которые нужно отслеживать. Аудиту подлежат успешные и неудачные попытки доступа учетной записи к ресурсу с использованием каждого из назначенных объекту разрешений.

Аудит успешных попыток доступа можно использовать для:

- регистрации попыток доступа к ресурсам для составления отчетов и выписки счетов;
- мониторинга попыток доступа, которые бы указали, что пользователи выполняют непредусмотренные действия, то есть разрешения настроены недостаточно жестко;
- выявления попыток доступа, которые нехарактерны для данной учетной записи; это может быть признаком того, что учетная запись взломана.

Аудит неудачных попыток позволяет:

- обнаружить попытки доступа к секретному ресурсу;
- определить неудачные попытки обращения к файлу или папке, доступ к которой действительно требуется пользователю; это означает, что предоставленных разрешений недостаточно для решения бизнес-задач.

Параметры аудита, как и разрешения, удовлетворяют правилам наследования. Наследуемые параметры аудита распространяются на объекты, разрешающие наследование.

Примечание. Журналы аудита довольно быстро растут, поэтому золотое правило аудита - следить за минимальным количеством событий, которых достаточно для решения задачи. Если настроить аудит успешных и неудачных попыток доступа к часто используемой папке для группы **Все (Everyone)** и контролировать все виды доступа, будут созданы огромные журналы аудита, которые могут снизить производительность сервера и крайне затруднить поиск нужных событий.

Включение аудита осуществляется через политику. Настройка элементов аудита в дескрипторе безопасности файла или папки сама по себе не включает аудит. После включения аудита подсистема безопасности начинает принимать во внимание параметры аудита и регистрировать соответствующие попытки доступа.

Политику аудита можно включить на изолированном сервере в консоли **Локальная политика безопасности (*Local Security Policy*)**, и на контроллере домена в консоли **Политика безопасности контроллера *домена (Domain Controller Security Policy)***. Раскройте узел **Локальные политики (Local Policies),** затем **Политика аудита (*Audit Policy*)** и дважды щелкните политику **Аудит доступа к объектам (*Audit Object Access*).** Выберите **Определить следующие параметры политики (*Define These Policy Settings*)** и укажите, какие попытки доступа (успешные, неудачные или и те, и другие) должны подлежать аудиту.

Примечание Помните, что попытки доступа, которые отслеживаются и регистрируются, — это комбинация элементов аудита для отдельных файлов или папок и параметров политики аудита. Если элементы аудита разрешают регистрацию неудачных попыток доступа, а политика аудита — успешных, журналы аудита останутся пустыми.

Аудит можно включить на одном или нескольких компьютерах, используя объекты групповой политики (ОГП) *Active Directory*. Узел **Политика аудита (*Audit Policy*)** расположен в дереве **Конфигурация компьютера (*Computer Configuration*)\Конфигурация *Windows* (*Windows Settings*)\Параметры безопасности (*Security Settings*)\Локальные политики (*Local Policies*)\Политика аудита (*Audit Policy*).** Как и остальные групповые политики, политика аудита влияет на все компьютеры, расположенные в области ее действия. Если вы подключите политику к ОП Servers и включите аудит, все объекты компьютеров в ОП Servers будут подвергаться аудиту доступа к ресурсам согласно элементам аудита файлов и папок, заданным на этих системах.

Когда элементы аудита файлов и папок настроены, и аудит доступа к объектам включен через локальную или групповую политику, система начинает регистрировать попытки доступа согласно элементам аудита. Вы можете анализировать журнал безопасности с помощью оснастки **Просмотр событий (*Event Viewer*)**, показанной на рисунке 8.2.

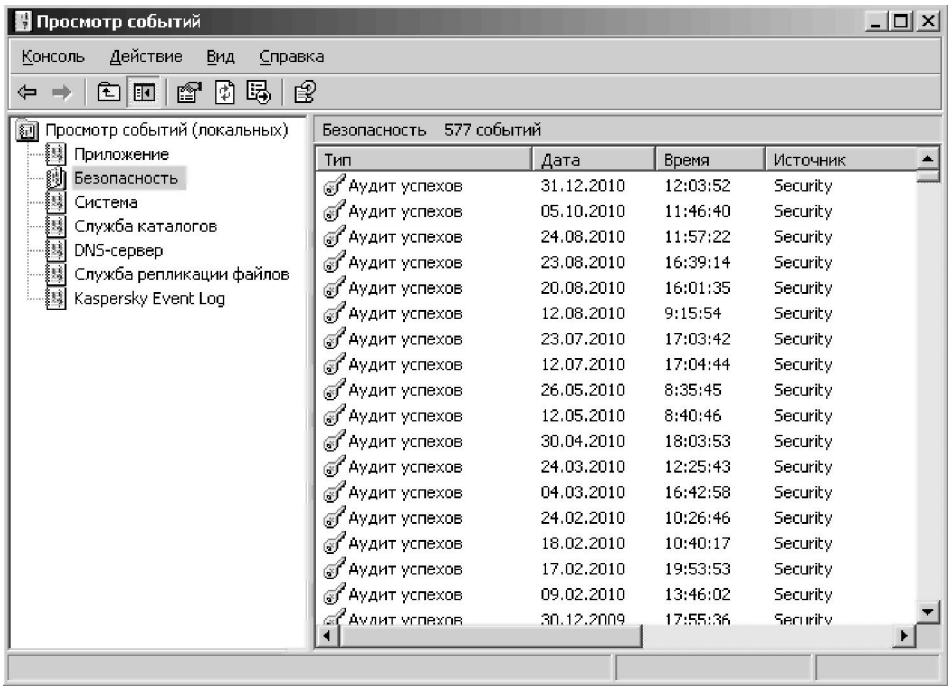

Рисунок 8.2 Результаты аудита в журнале безопасности

Как видно, размер журнала безопасности зависит от типа событий, подлежащих аудиту. Можно отсортировать собранные данные, чтобы быстрее найти события доступа к объекту. Для этого щелкните заголовок

столбца **Категория (*Category*)** и выберите **Доступ к объектам (Object Access).**

Впрочем, сортировка малоэффективна, когда нужно детально разобраться в зарегистрированных событиях. Лучше отфильтровать журнал событий. Для этого в меню **Вид (*View*)** выберите **Фильтр (*Filter*)** или щелкните узел журнала безопасности и в контекстном меню или в меню ***Action* (Действие)** выберите **Свойства (*Properties*),** после чего перейдите на вкладку **Фильтр (*Filter*).** Эта вкладка позволяет указать условия поиска, включая тип события, категорию, источник, временной диапазон, пользователя и компьютер. Пример фильтрации доступа к объектам по дате показан на рисунке 8.3.

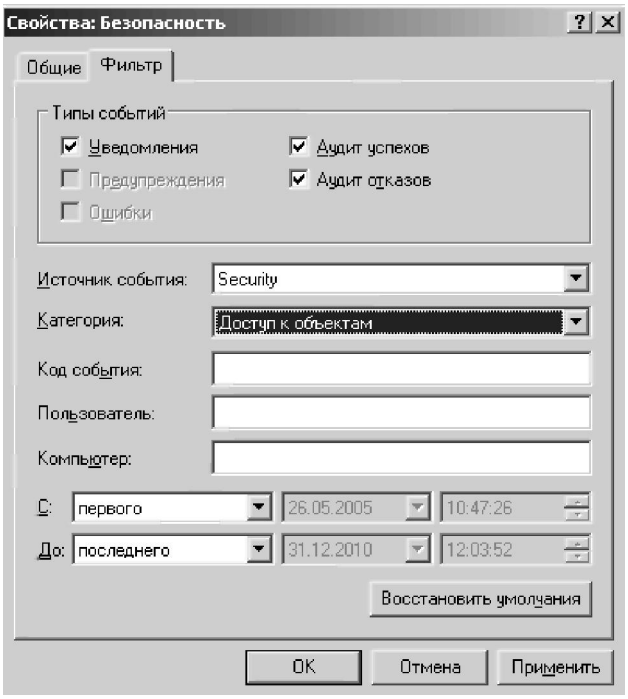

Рисунок 8.3. Вкладка **Фильтр**

Наконец, можно экспортировать журнал безопасности. Для этого в контекстном **меню** журнала нужно выбрать **Сохранить файл журнала как (*Save Log File As*).** Файлы собственных журналов Windows имеют разрешение .evt. Этот файл можно открыть на другом компьютере с помощью оснастки ***Просмотр событий (Event Viewer*)**. Либо можно сохранить журнал в текстовом файле формате с разделителями — запятыми или символами табуляции, который читает большинство средств анализа, включая Microsoft Excel. В Excel можно также применять фильтры для поиска более специфичной информации, например, чтобы найти определенный текст в поле **Описание (*Description*)** для события.

При выполнении лабораторной работы настройте параметры аудита, включите политики аудита для доступа к объектам и используете фильтр для

поиска определенных событий в журнале безопасности. Задача - отследить удаление файлов из важной папки, чтобы убедится, что это делают только соответствующие пользователи.

8.3 Задание на лабораторную работу

8.3.1. Настройте параметры аудита, для чего:

- Войдите в систему как **Администратор (*Administrator*)** рабочей станции.
- Откройте окно **Дополнительные параметры безопасности (*Advanced Security Settings*)** для папки ***C:\Docs\Project101***.
- Перейдите на вкладку **Аудит (*Auditing*)**.
- Добавьте элемент аудита, позволяющий отслеживать действия группы ***Project101 Team***. Укажите, что нужно отслеживать успешные и неудачные попытки применения разрешения **Удаление (*Delete*)**.

8.3.2. Включите политику аудита на контроллере домена, используя консоль **Политика безопасности контроллера домена (*Domain Controller Security Policy*)**, а на изолированном сервере, исполуя консоль **Локальная политика безопасности (*Local Security Policy*)**. Для включения аудита также можно задействовать ОГП:

- Откройте консоль **Политика безопасности контроллера домена (*Domain Controller Security Policy)*** из группы программ **Администрирование (*Administrative Tools).***
- Раскройте узел **Локальные политики (Local Policies)** и щелкните **Политика аудита (*Audit Policy*).**
- Дважды щелкните политику **Аудит доступа к объектам (*Audit Qbject Access).***
- Щелкните **Определить следующие параметры политики (*Define These Policy Settings).***
- Включите аудит успешных и неудачных попыток доступа.
- Щелкните **ОК** и закройте консоль.
- Чтобы обновить политику и гарантировать, что все параметры были применены, в командной строке исполните **обновить политику** (***gpupdate***).

8.3.3 Сгенерируйте событий, подлежащие аудиту, для чего:

- Войдите в систему с правами обычного пользователя.
- Подключитесь к папке ***\\kit-edu\Docs\Project101***.
- Удалите текстовый файл ***Report***.

8.3.4. Для анализа журнала безопасности выполнить следующие действия:

- Войдите в систему как **Администратор (*Administrator*)**.

- Откройте консоль **Просмотр событий (*Event Viewer*)** из группы **Администрирование (*Administrative Tools*).**
- Щелкните узел **Безопасность (*Security log*).**
- Какие типы событий вы видите в журнале безопасности? Только события доступа к объекту? Другие типы событий? Помните, что политики позволяют отслеживать множество действий, связанных с безопасностью, в том числе доступ к службе каталогов, управление учетными записями, вход в систему и т. п.
- Чтобы сузить область поиска, в меню **Вид (*View*)** выберите **Фильтр (*Filter*).**
- Настройте как можно более узкий фильтр. Что вы знаете о событии, которое хотите найти? Вы знаете, что оно может быть успешным или неудачным, принадлежит **к** категории **Доступ к объектам (*Object Access*)** и что оно произошло сегодня.
- Щелкните **Применить (*Apply*).**
- Можно ли как-нибудь упростить поиск события, которое свидетельствует об удалении файла Report соответствующим пользователем? Откройте событие и просмотрите его содержимое. Описание содержит имя пользователя, имя файла и действие. Консоль **Просмотр событий (*Event Viewer*)** не позволяет задать фильтр по содержанию описания, но это можно сделать, экспортировав файл в другое средство анализа журналов или в *Microsoft Excel.*
- (***Необязательная*** операция.) Если у вас есть *Microsoft Excel*, щелкните узел журнала безопасности правой кнопкой и выберите **Сохранить файл журнала как (Save Log File As).** Введите имя файла и выберите для него тип с разделителем — запятой. Откройте полученный файл в Excel.

Включите в отчет скриншоты, отражающие каждый шаг выполнения заданий.

8.4 Вопросы для самопроверки

1)Как включить политику аудита на контроллере домена?

2) Что нужно сделать, чтобы сгенерировать журнал событий доступа к файлу или папке?

3) Что является допустимым условием фильтра для поиска событий доступа к файлу или папке в журнале безопасности?

4) Что такое аудит успешных и неудачных попыток доступа?

Лабораторная работа № 8

МОДЕЛИРОВАНИЯ СЕТЕЙ С ПОМОЩЬЮ ПАКЕТА *NETCRACKER PROFESSIONAL*

8.1 Цель работы

Целью работы является изучение методов моделирования компьютерных сетей с использованием пакета *NetCracker Professional 4.0*.

8.2. Теоретический материал

8.2.1 Общая характеристика пакета *NetCracker Professional*

Одним из популярных инструментов для моделирования сетей является пакет *NetCracker Professional 4.0*, который представляет собой CASE-средство автоматизированного проектирования, моделирования и анализа компьютерных сетей различных классов. Пакет позволяет, исследуя поведение сети в стандартных и критических ситуациях, обосновать выбор типа сети, сред передачи, сетевых компонент оборудования и программно-математического обеспечения, найти узкие места сетевой инфраструктуры.

Программные средства пакета позволяют выполнить сбор соответствующих данных о существующей сети без останова ее работы, создать проект этой сети и выполнить необходимые эксперименты для определения предельных характеристик, возможности расширения, изменения топологии и модификации сетевого оборудования с целью дальнейшего ее совершенствования и развития.

В составе пакета *NetCracker* имеется мощная база данных сетевых устройств (рабочих станций, серверов, сред передачи, сетевых адаптеров, повторителей, мостов, коммутаторов, маршрутизаторов и др.) ведущих производителей для различных сетевых технологий. Каждое устройство описывается набором свойств, которые определяют такие данные как задержка, скорость передачи, фильтрации и перенаправления пакетов, используемые протоколы, тип портов, их доступность, описание интерфейсной карты и т.д. Пользователю предоставляет так же возможность добавления в базу данных и конфигурирования нового оборудования. Аппаратное и программное обеспечение в совокупности позволяет описывать разнообразные сетевые архитектуры: клиент-сервер, VLAN (виртуальная локальная сеть), беспроводные сети и др.

С помощью пакета можно разрабатывать многоуровневые проекты с заданной проектировщиком степенью детализации; при этом имеется достаточно удобный интерфейс и средства быстрого просмотра всех уровней проекта.

Для реализаций функций имитационного моделирования в составе пакета *NetCracker* предусмотрены средства:

- задания характеристик трафиков (размер пакетов, время ожидания между их передачами, закон изменения этих величин) различных протоколов: SMTP, POP3, FTP, HTTP, CAD/CAM client-server и др.;
- визуального контроля заданных параметров;
- накопления статистической информации и формирования отчетной документации о проведенных экспериментах с возможностью экспорта в HTML-файл.

NetCracker обладает такой полезной возможностью, как имитация разрыва и восстановления связей между сетевыми устройствами, что позволяет администратору моделировать сети работу не только в нормальном режиме, но и при выходе из строя ее отдельных элементов.

В качестве дополнительных функций в пакете реализованы возможности.

- сканирования и распознавания реальной сети и её устройств с параметрами настройки, а так же автоматического создания нового проекта на основе полученных данных;
- импортирования проектов, созданных с помощью программы Microsoft Visio, и экспортирования созданного проекта в графический файл;
- автоматического подсчёта стоимости всего оборудования в проекте и протяжённости линий связи.

Системные требования к пакет *NetCracker*:

- процессор *Pentium II* и выше;
- свободная память на жестком диске 60 MB, оперативная память не менее 256 MB, видео памяти не менее 4 MB;
- операционная система *MS Windows NT 4.x* и выше.

8.2.2. Запуск и графический интерфейс пакета

Главное окно *NetCracker,* открывающееся после запуска программы, состоит из заголовка, главного меню, панелей инструментов и анимации, из трех фреймов: браузер (***Browser)*** слева, рабочей зоны проекта (***Workspace***) справа и панели изображений (***Image)*** снизу (рисунок 8.1).

Панель браузера содержит несколько закладок. Закладка ***Project Hierarchy*** предназначена для отображения структуры документов создаваемого проекта сети. Закладка ***Devices*** предназначена для отображения базы данных устройств. Список устройств имеет несколько видов отображения:

- ***Types*** (Типы) – устройства в списке группируются по типам, а затем в каждой группе могут выделяться подтипы устройств по функциональным признакам, после этого устройства разделяются по изготовителям;
- ***Vendors*** (Изготовители) – устройства в списке группируются по изготовителям, затем в каждой группе выделяются подгруппы, соответствующие типу устройств;

- ***User*** (Пользовательские) – устройства, определяемые пользователем, в свою очередь также могут группироваться по типам или изготовителям.

Закладка ***Compatible Devices*** предназначена для отображения списка совместимых устройств.

В нижней части окна программы обычно располагается панель изображения устройств, которая может быть отображена с помощью команды ***View→Bars→Image Pane***. Данная панель предназначена для отображения устройств из выбранной группы (здания, университетские городки, рабочие группы локальной сети и т.п.).

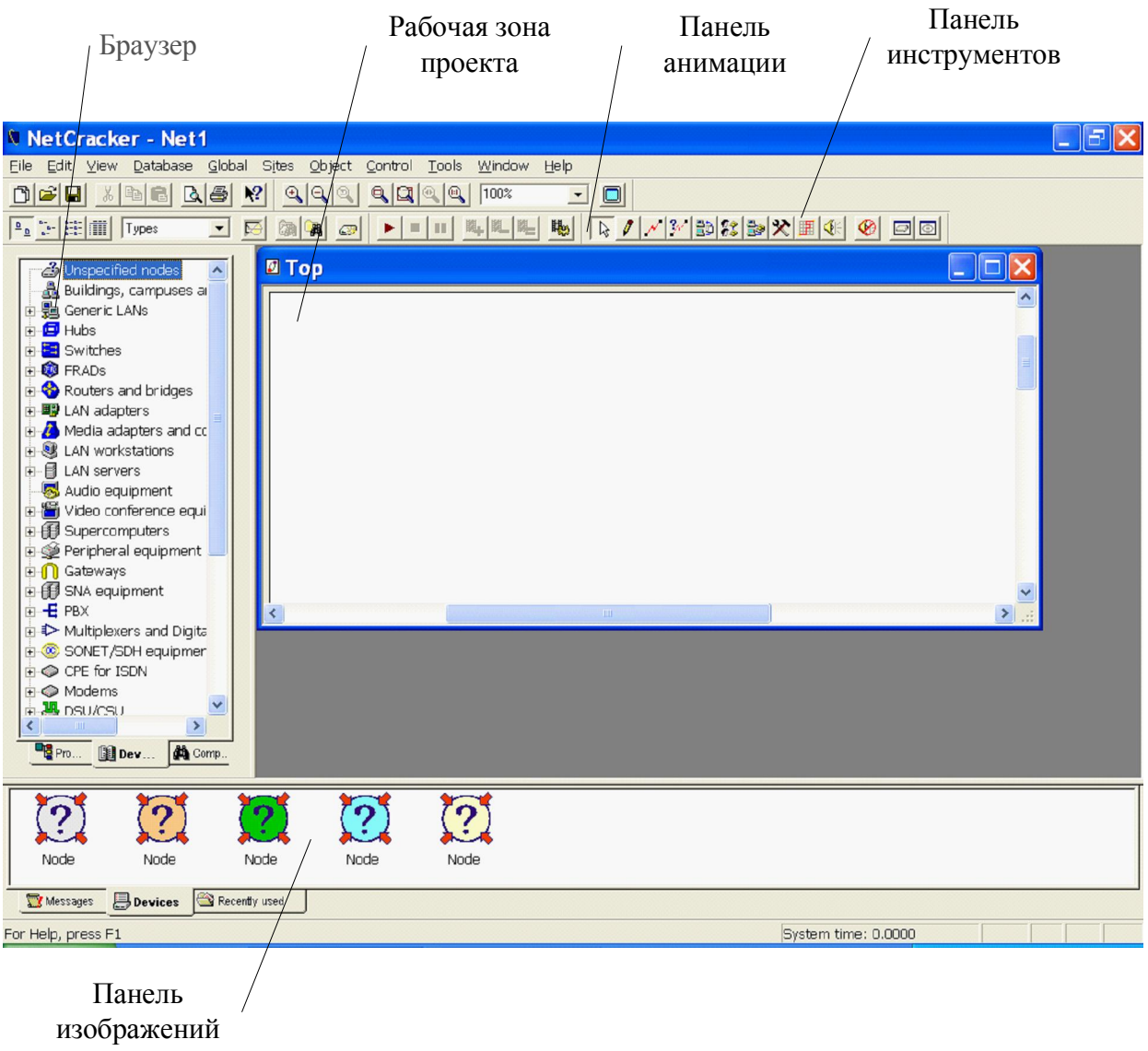

Рисунок 8.1. Главное окно пректа

Рабочая зона представляет собой наборное поле, в котором необходимо размещать используемые компоненты при моделировании структуры сети. Когда запускается *NetCracker*, рабочая зоны содержит пустой сайт ***Net 1***.

8.2.3. Технология создания, исследования и документирования проекта сети

8.2.3.1 Порядок создания, исследования и документирования проекта сети рассмотрим на примере моделирования простой локальной сети, включающей сервер и две рабочие станции, объединенные по технологии *Fast Ethernet* через концентратор (*Hub*). Пусть сервер поддерживает службу FTP, используемую обеими станциями, которые дополнительно обмениваются прямыми сообщениями (*LAN peer-to-peer traffic*).

8.2.3.2 Для создания нового проекта:

- запустите *NetCracker,* если он не запущен;
- создайте пустой проект ***lab1*** (меню ***File→New***);
- максимизируйте окно сайта и увеличьте видимую область до размеров окна.

8.2.3.3. Добавьте к проекту коммутатор, для чего:

- убедитесь, что режим дерева устройств (на панели Database) установлен в ***Types***;
- в дереве устройств выберите категорию ***Hubs*** (концентраторы), раскройте ее, в ней выберите подкатегорию ***Shared media*** (разделяемая среда), в ней – ***Ethernet***, в ней – ***Bay networks*** и выберите устройство ***BayStack 100BASE-T Fast Ethernet Hub with 12 100BASE-TX ports, 1 expansion slot,and 1 100BASE-T slot;***
- перетащите значок выбранного концентратора с панели изображения устройств в рабочую зону (рисунок 8.2);
- увеличьте размер картинки концентратора путем буксирования угловых квадратиков;
- отредактируйте текст подписи под картинкой, щелкнув два раза по тексту, и увеличьте размер шрифта (в контекстном меню выберите пункт ***Properties***).

8.2.3.4. Добавьте к проекту сервер, для чего:

- в дереве устройств выберите категорию ***LAN Servers*** (сетевые верверы), раскройте ее, в ней выберите подкатегорию ***IBM*** и в ней выберите устройство ***RS/6000 Telecommunications Server;***
- перетащите значок выбранного сервера с панели изображения устройств в рабочую зону;
- с помощью контекстного меню (пункты ***Propertie→Ports***) определите состав портов выбранного сервера (рисунок 8.3)

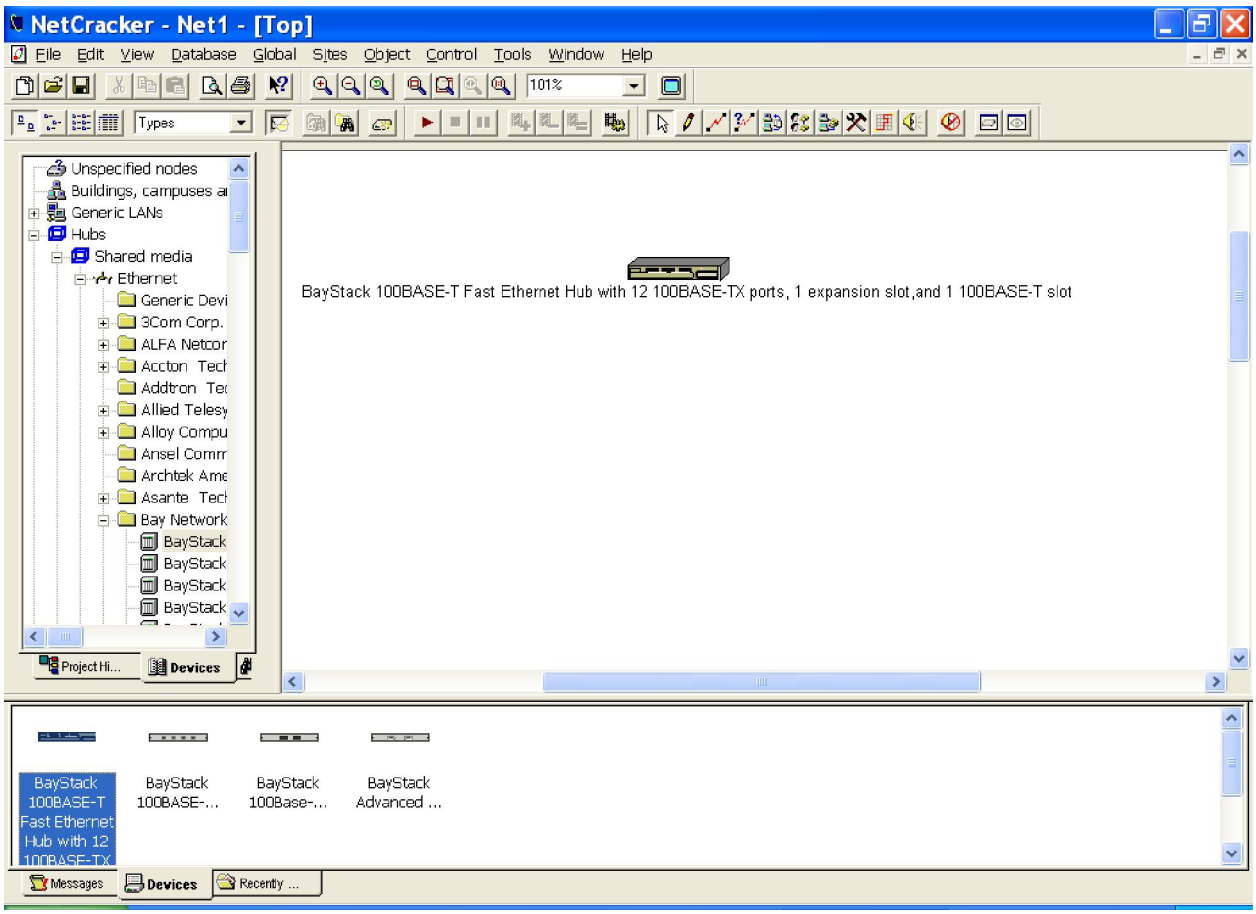

Рисунок 8.2. Включение концентратора в проект

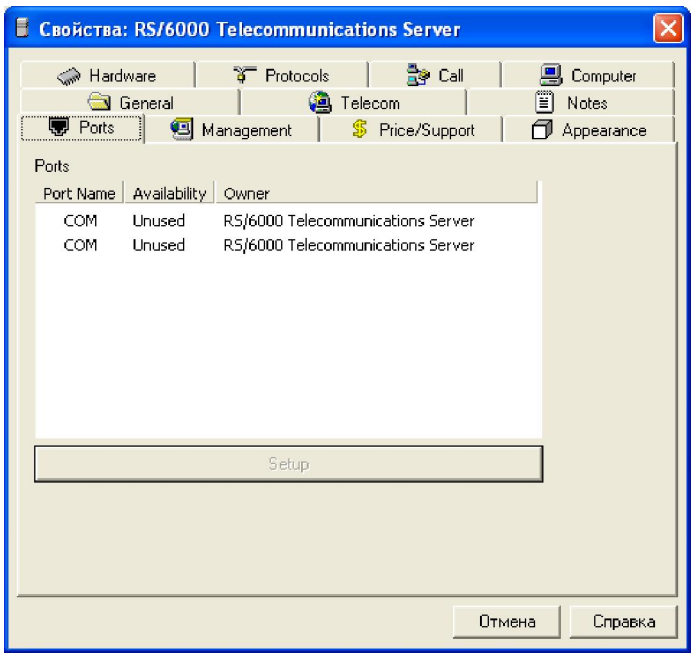

Рисунок 8.3. Контроль встроенных портов сервера

8.2.3.5. Поскольку сервер *RS/6000* не содержит встроенных портов *Fast Ethernet*, то необходимо добавить сетевой адаптер, для чего:

- в дереве устройств откройте категорию ***LAN adapters***, выберете подкатегорию ***Ethernet,*** в ней – ***IBM***,

- найдите на панели картинок сетевой адаптер ***IBM 100/10 EtherJet PCI Adapter with Wake-On-LAN*** перетяните его на картинку сервера в рабочей зоне;
- с помощью контекстного меню (пункты ***Propertie→Configuration***) убедитесь в подключении адаптера (рисунок 8.4).

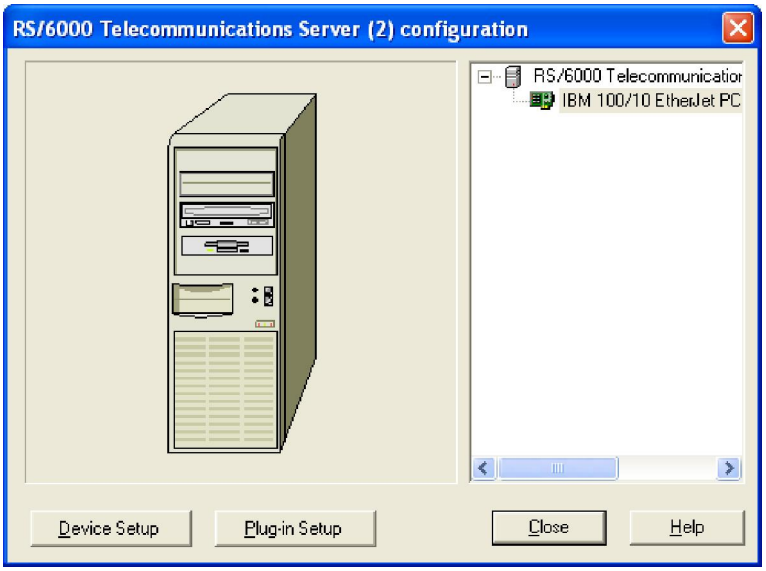

Рисунок 8.4. Контроль подключения адаптера к серверу

8.2.3.6. Добавьте к проекту рабочие станции, для чего:

- в дереве устройств выберите категорию ***LAN Workstation*** (сетевые станции), раскройте ее, в ней выберите подкатегорию ***IBM,*** и в панели изображения выберите устройство ***IntelliStation E Pro 6893 Series-689361U;***
- перетащите значок выбранного сервера с устройства в рабочую зону;
- с помощью контекстного меню (пункты ***Propertie→Ports***) определите состав портов выбранной станции (рисунок 8.5), убедившись в наличии встроенного порта со спецификацией *100BASE-TX,* соответствующей типу *Fast Ethernet,* принятому в концентраторе.
- продублируйте подключенную к проекту станцию (меню ***Edit →Dublicate***).

8.2.3.7. Установите связи компьютеров с концентратором, для чего:

- выберите режим ***Link***, нажав кнопку в меню ***Site*** →*Modes*;
- щелкните по картинке сервера, а затем щелкните по картинке концетратора, после чего откроется окно диалога Помощника по связи ***Link Assistant*** (рисунок 8.6);
- нажмите кнопку ***Link***, заполните параметры литии связи в открывшихся формах, затем нажмите кнопку ***Close***;
- установите связи между рабочими станциями и концентратором, используя вместо меню ***Site*** кнопку  панели инструментов.

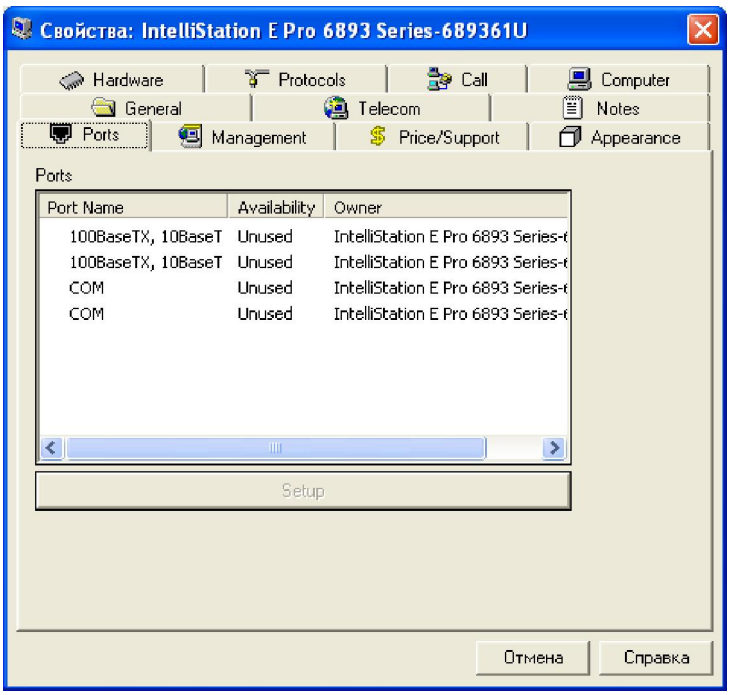

Рисунок 8.5. Контроль встроенных портов станции

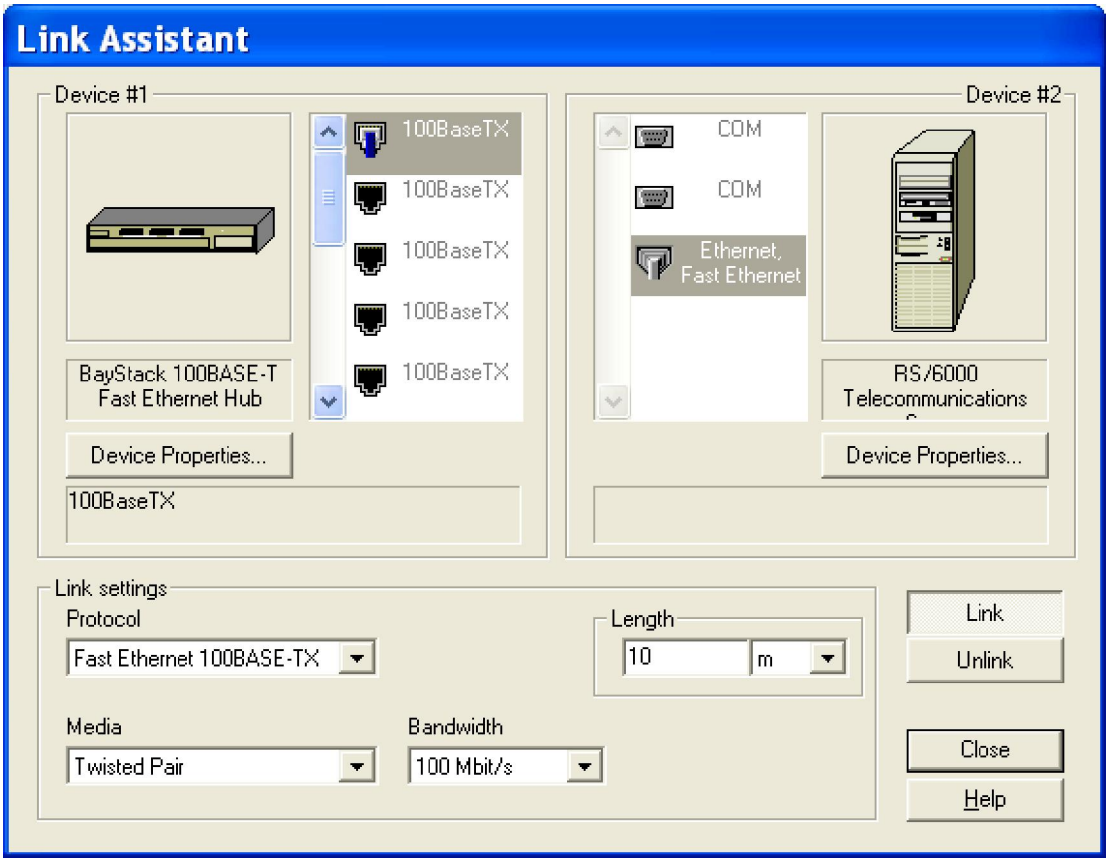

Рисунок 8.6. Окно диалога Помощника по связи

8.2.3.7. Установите серверное программное обеспечение, для чего:

- в дереве устройств выберите категорию ***Network and enterprise software*** (сетевое и прикладное ПО), раскройте ее, в ней выберите подкатегорию ***Server software*** и в панели изображения выберите ПО ***FTP server*** (рисунок 8.7)***;***

- перетяните его на картинку сервера в рабочей зоне;
- с помощью контекстного меню (пункт ***Configuration***) убедитесь в подключении серверного ПО (рисунок 8.8);
- с помощью меню ***FTP server →Propertie*** откройте закладку ***Server*** и установите параметры ответа FTPсервера (рисунок 8.9).

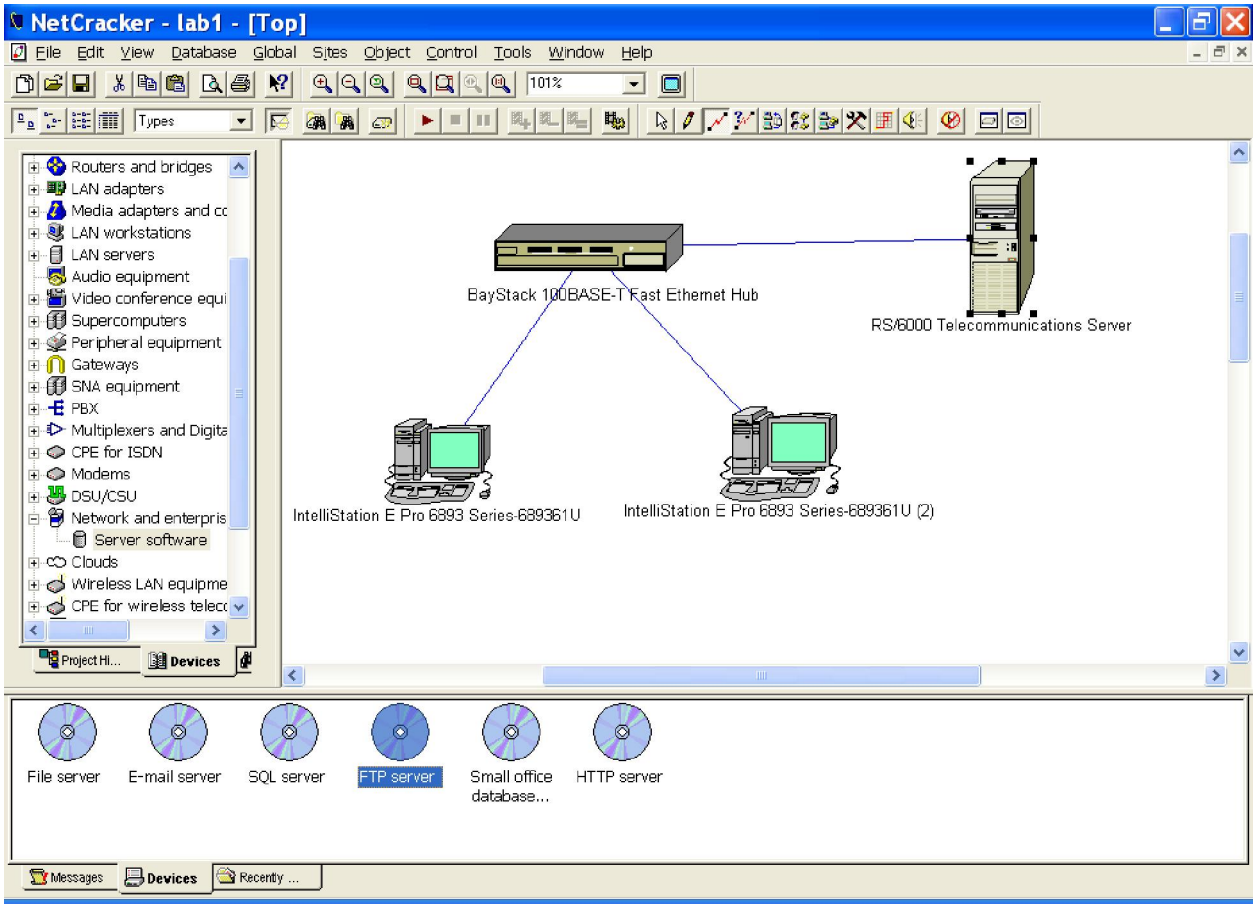

Рисунок 8.7. Окно диалога установки серверного ПО

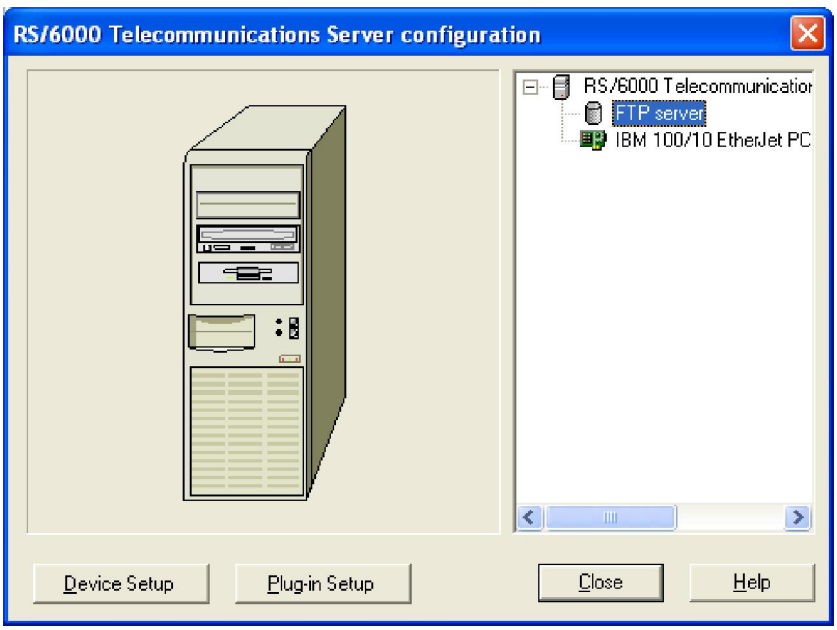

Рисунок 8.8. Окно контроля установки серверного ПО

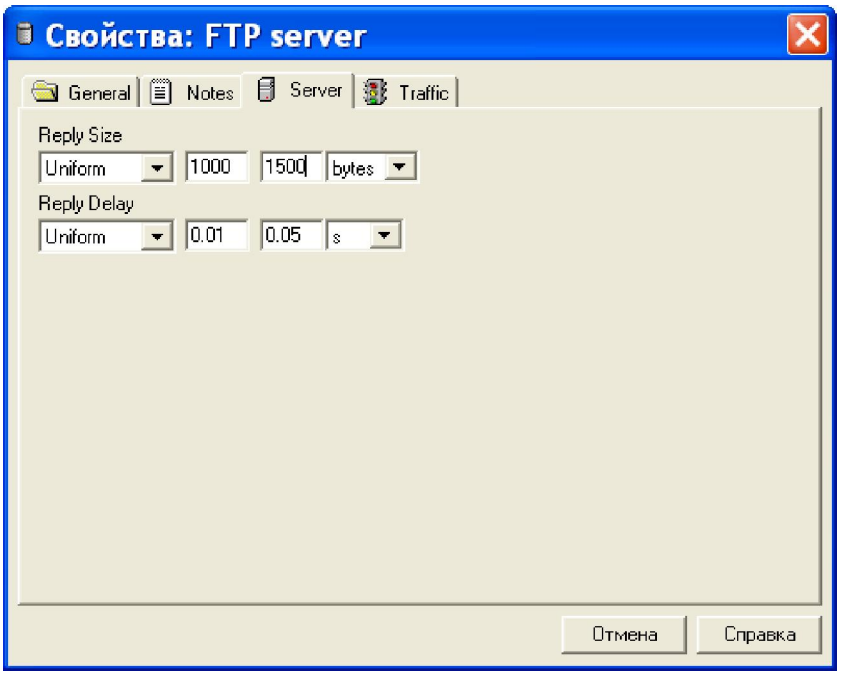

Рисунок 8.9. Окно установки параметров отклика сервера

8.2.3.8. Назначьте потоки данных между компьютерами, для чего:

- нажмите кнопку  ***Set Traffics*** панели инструментов;
- щелкните по картинке рабочей станции 1, а тем по картинке сервера, откроется диалог *Profile* (рисунок 8.10)
- чтобы определить трафик ***FTP*** между рабочей станцией и сервером выберите профиль ***FTP client*** на панели списка выбора *Profiles****;***
- нажмите кнопку ***Advanced*** и в открывшемся окне задайте параметры трафика (рисунок 8.11),
- нажмите кнопку ***Assign,*** чтобы назначить трафик и закрыть диалог.

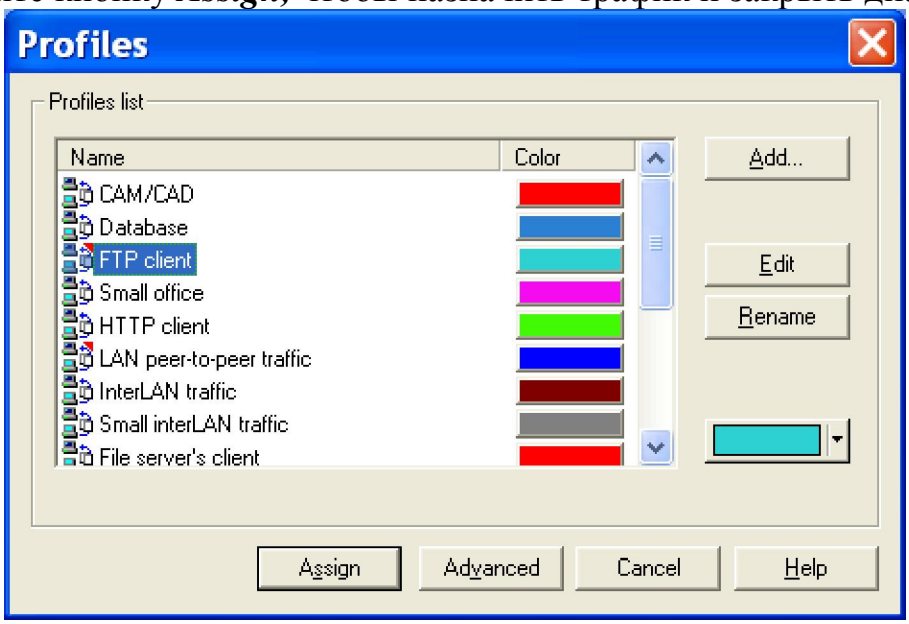

Рисунок 8.10. Окно выбора типа трафика

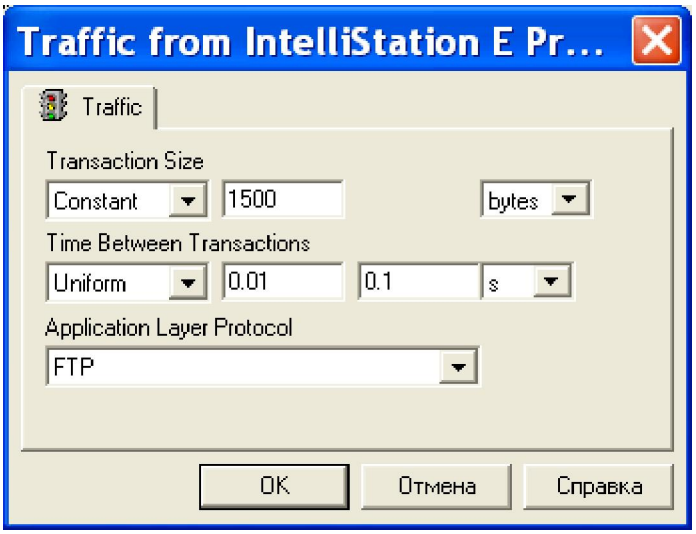

Рисунок 8.11. Окно параметров FTP трафика

Приведенные выше шаги повторите, выбрав рабочую станцию 2, а затем по аналогии задайте трафик *LAN peer-to-peer*, изменив параметры как показано на рисунке 8.12.

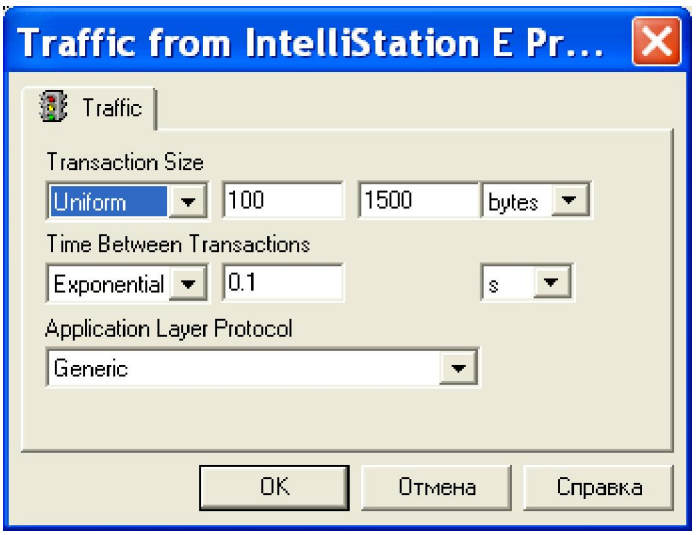

Рисунок 8.12. Окно параметров *LAN peer-to-peer* трафика

Установленные потоки данных между компьютерами можно проконтролировать в окне ***Data Flow*** (Потоки данных), вызываемом из меню ***Global → Data Flow*** (рисунок 8.13).

8.2.3.9.Для того, чтобы отображать итоги моделирования, задайте вид и значение собираемой статистики, для чего:

- выберите концентратор и в контекстном меню выберите пункт ***Statistics…,*** после чего откроется окно задания статистики, собираемой по выделенному устройству;
- задайте собираемую статистику, как показано на рисунке 8.14.

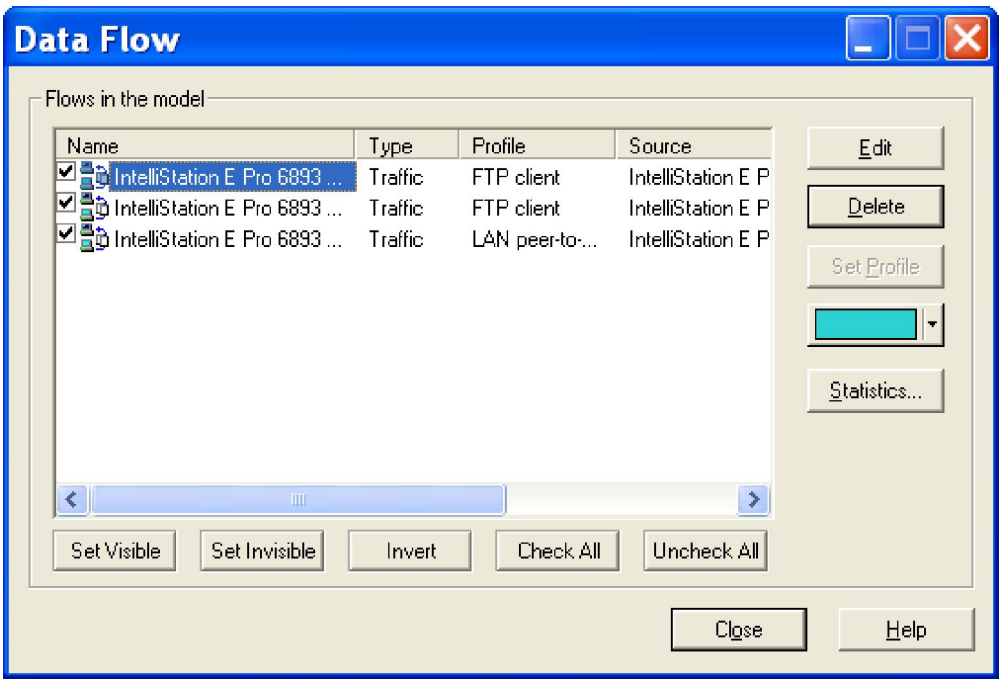

Рисунок 8.13. Окно Потоки данных

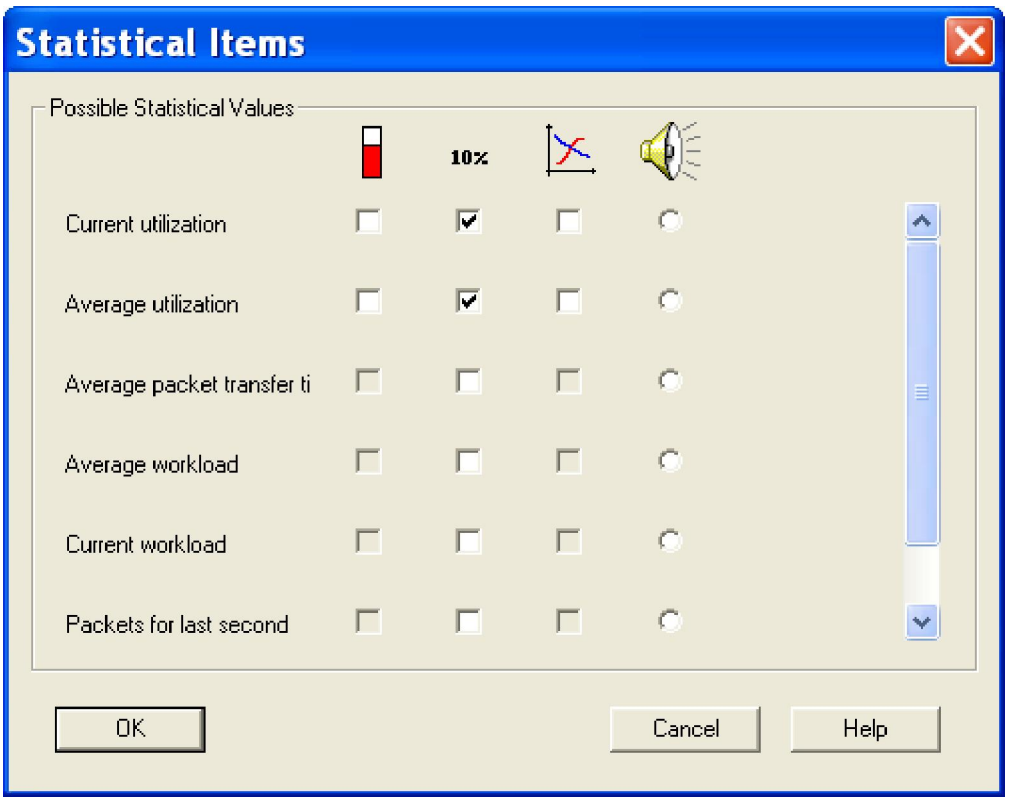

Рисунок 8.14. Диалог статистики

8.2.3.10. Для проверки работоспособности модели запустите анимацию с помощью кнопки  на панели инструментов. На модели можно наблюдать перемещение пакетов (рисунок 8.15). Приостановка (пауза) и прекращение анимации выполняется с помощью кнопок  и  .

Чтобы изменить параметры анимации (частоту следования пакетов, скорость передачи пакетов или их размер) надо вызвать меню настройки анимации, нажав кнопку ***Animation Setup***  , и воспользоваться соответствующими движками (рисунок 8.16).

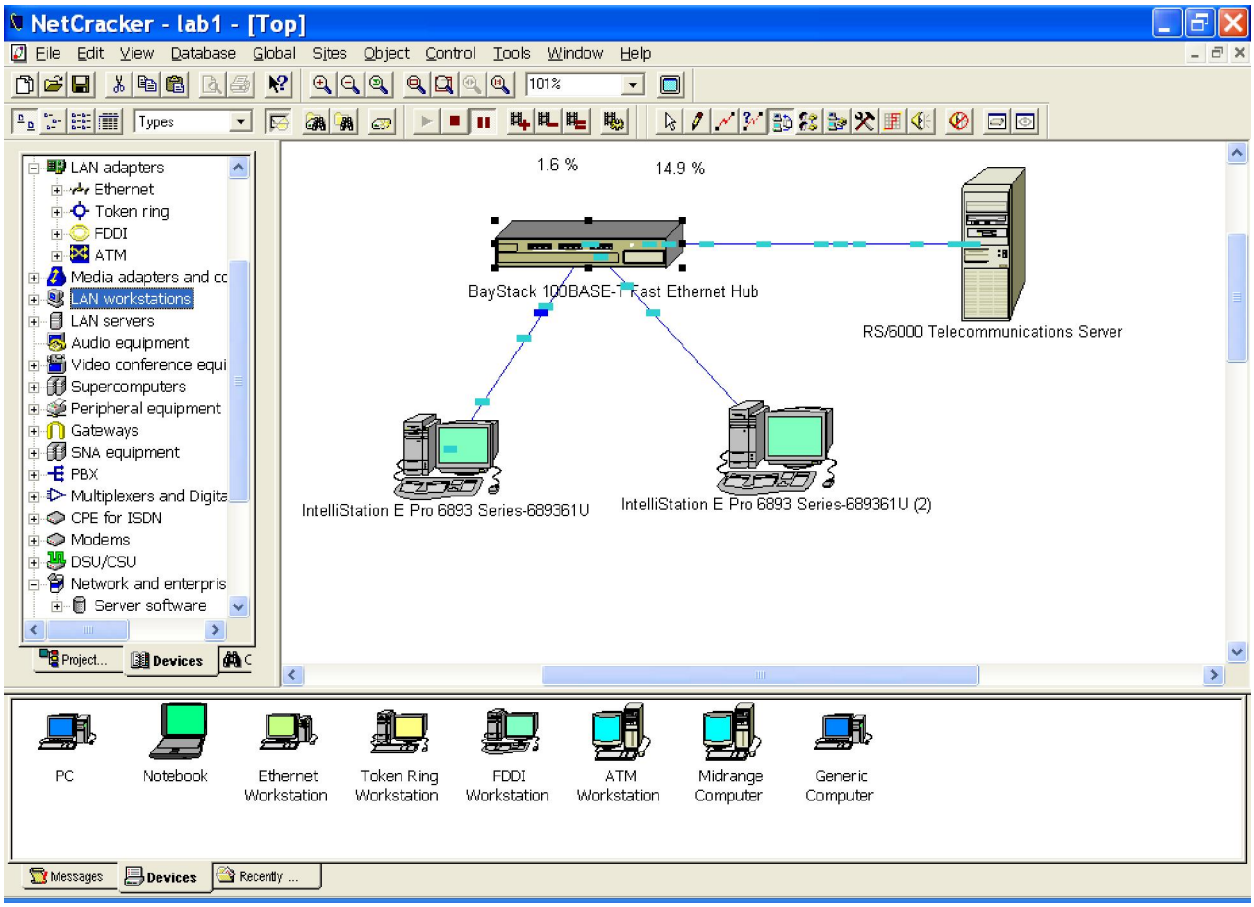

Рисунок 8.15. Анимация

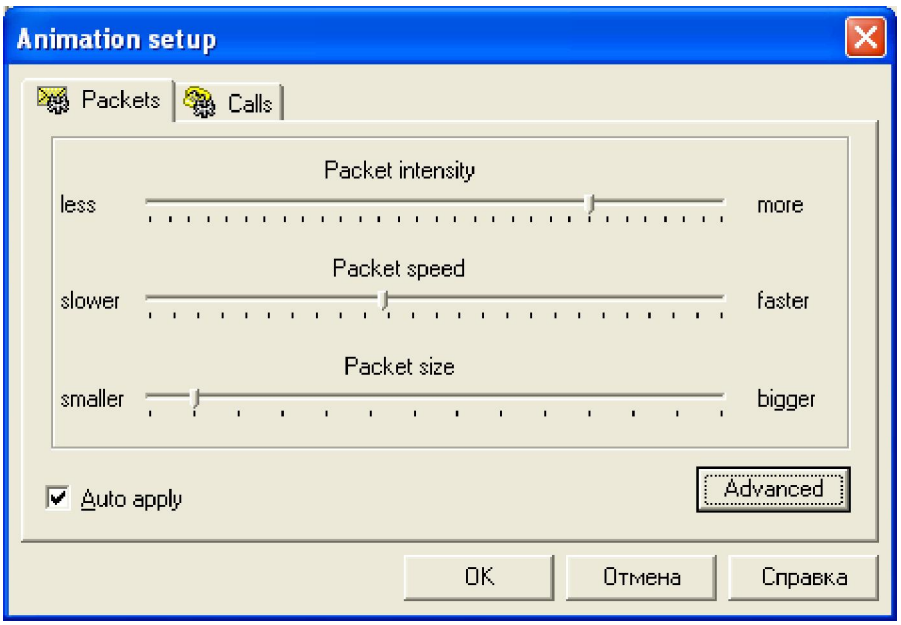

Рисунок 8.16. Меню настройки анимации

Для просмотра параметров отдельных пакетов:

- перейдите в режим паузы анимации;
- выберете стандартный режим, нажав кнопку  ;
- установите маркер на интересующий пакет;
- вызовите контекстное меню и выберите пункт ***Properties,***

В открывшемся окне (рисунок 8.17) отобразятся значения параметров выбранного пакета.

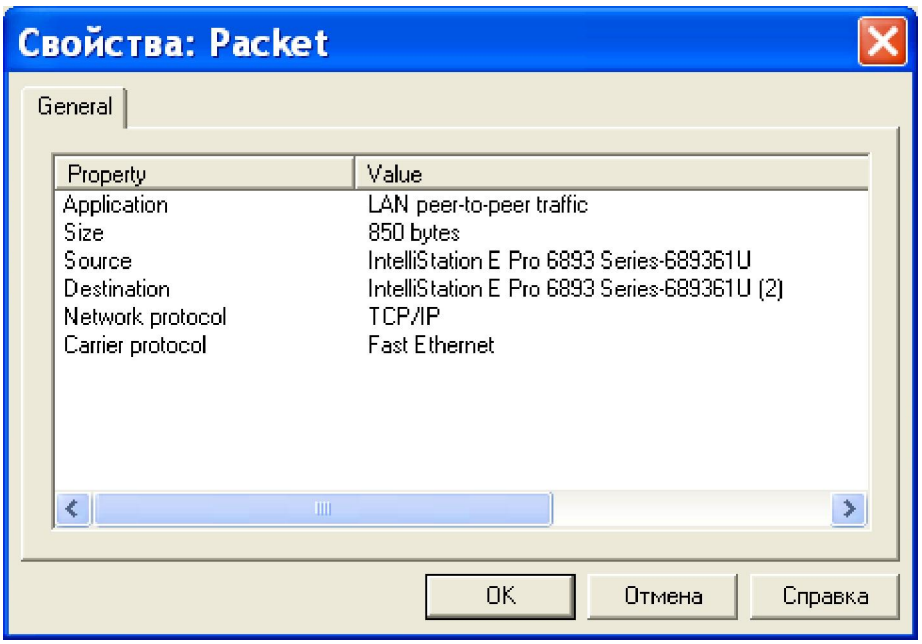

Рисунок 8.17. Окно параметров пакета

8.2.3.11. Для автоматизации присвоения IP адресов устройствам модели рекомендуется использовать приложение ***IP Planner*** пакета *NetCracker*, вызываемое из меню Tools. Для построенной ранее модели распределение адресов может выгладить, как показано на рисунке 8.18.

8.2.3.12. В процессе разработки проекта сети в *NetCracker* можно получить набор отчетов различного содержания о проекте. Например, операция ***Tools menu→Reports→Device Summary*** позволяет получить спецификацию всех единиц оборудования (рисунок 8.19). Таким же образом можно получить отчет о номенклатуре оборудования, входящего в проект сети, ценах каждой единицы оборудования, общей цены проекта, подобные спецификации можно сгенерировать и по отдельным классам оборудования (например, ***Workstations, Servers, Hubs***, и т. д.).

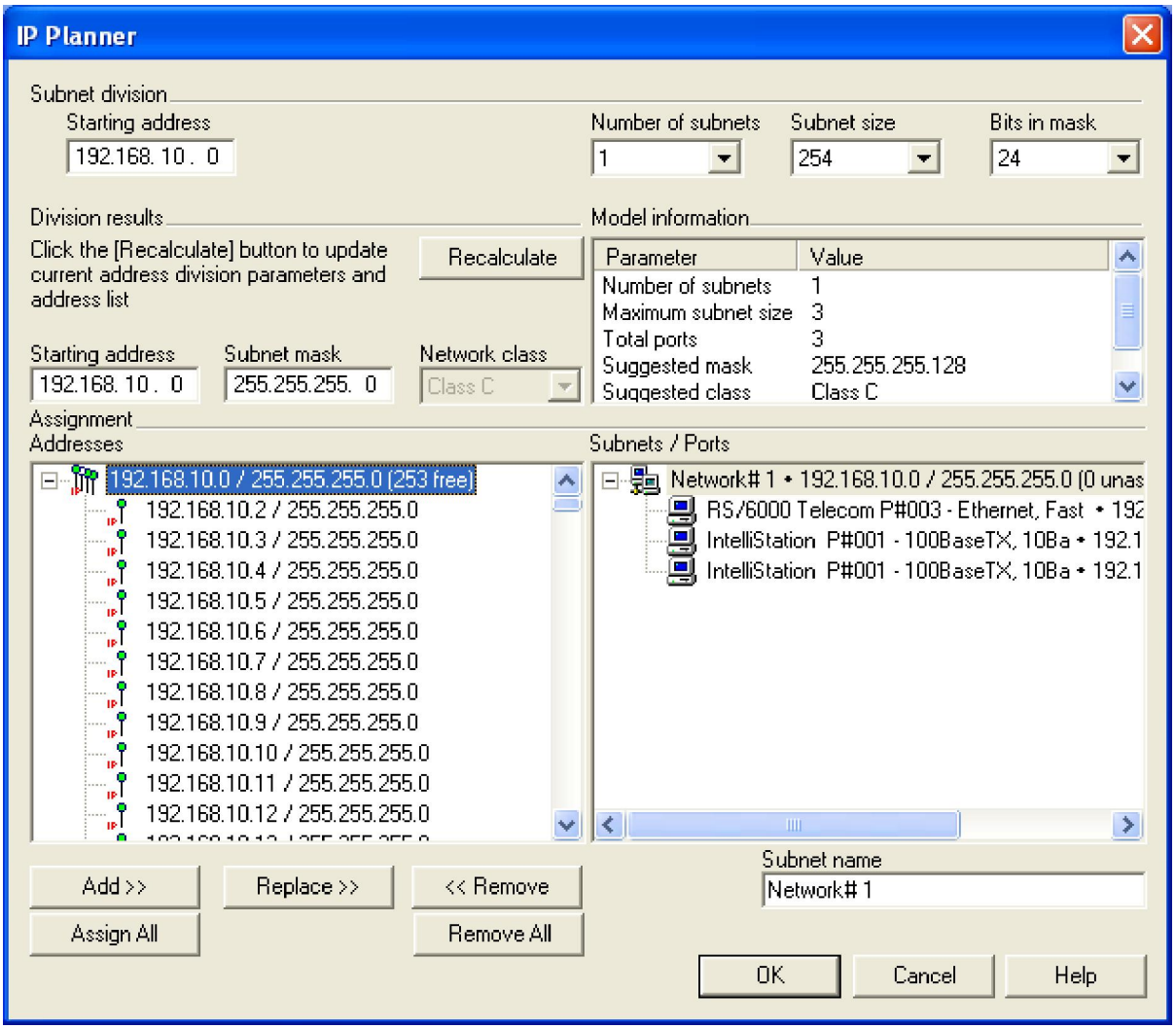

Рисунок 8.18. Окно приложения ***IP Planner***

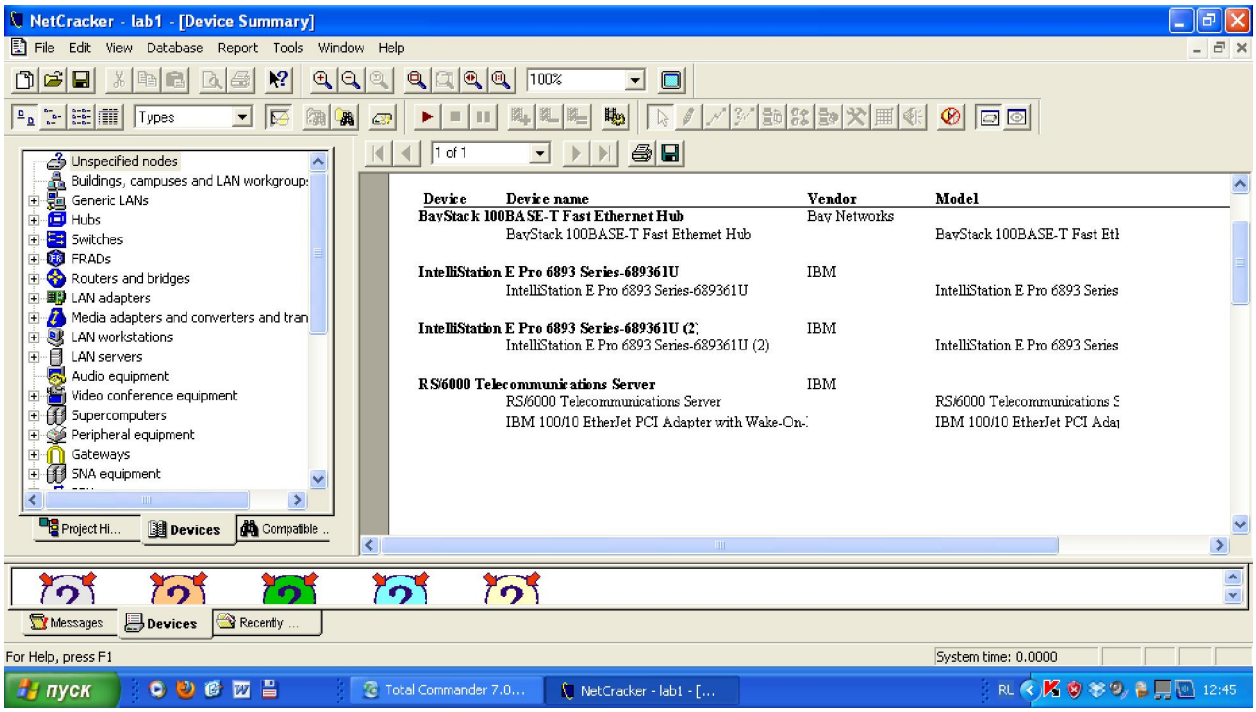

Рисунок 8.19. Спецификация всех единиц оборудования модели

8.2.3.13. При завершении работы необходимо сохранить созданный проект. Для этого выберите пункт ***Save*** в меню ***File***, откроется диалог выбора имени сохраняемого файла (по умолчанию – *Net1.net*).

6.3 Задание на лабораторную работу

8.3.1. Для изучения технологии создания проекта, и операций по созданию объектов и управление ими выполните действия, описанные в п. 8.2.3. Параметры трафика задайте самостоятельно.

8.3.2. Разработать и исследовать модель корпоративной сети, состав которой определяется вариантом задания.

Вариант1. Корпоративная сеть включает 3 сегмента, объединенных маршрутизатором:

- сегмент 1 - станции PC1-PC3, сервер1, сервер3 технология коммутируемый *Ethernet.*
- Сегмент 2 – станции PC4-PC6, сервер2, технология *Token Ring.*
- Сегмент 3 – станции PC7-PC8, технология *10-Base 2*.

Сервер 2 обслуживает клиентов CAD/CAM- приложений, сервер 3 обслуживет HTTP,. сервер 1 обслуживает FTP -клиентов. Станции PC1-PC4, PC7 и PC8 являются FTP –клиентами, станции PC4-PC6 являются клиентами CAD/CAM- приложений, все станции являются клиентами HTTP. Помимо серверов рабочие станции взаимодействуют внутри своих подсетей друг с другом по трафику *Small office peer-to-peer*.

Вариант 2. Корпоративная сеть включает 3 сегмента, объединенных маршрутизатором.

- Сегмент 1 – станции PC1-PC3, сервер1, технология *Token Ring.*
- Сегмент 2 – станции PC4-PC5, сервер2, технология коммутируемый 100-Base –TX.
- Сегмент 3– станции PC6-PC7, сервер3 технология 10-Base –T.

Сервер 2 обслуживает клиентов CAD/CAM- приложений, сервер 3 обслуживает HTTP, FTP –клиентов, сервер 1 обслуживает клиентов базы данных. Станции PC1-PC4 работаю с базой данных. Станции PC4-PC5, PC7 являются клиентами CAD/CAM- приложений. Все станции являются HTTP–клиентами. Помимо серверов рабочие станции взаимодействуют внутри своих подсетей друг с другом по трафику *Small office peer-to-peer*.

Вариант 3. Корпоративная сеть включает 3 сегмента, объединенных сетью *Frame Relay* посредством устройств DSU/CSU и многопротокольных маршрутизаторов:

- Сегмент 1– станции PC1-PC2, сервер1, технология 10-Base-T.
- Сегмент 2– станции PC3-PC5, сервер2, технология коммутируемый10-Base-T.
- Сегмент 3– станции PC6-PC7, сервер3, технология *Token Ring.*

Сервер 1 обслуживает клиентов базы данных. Сервер 2 обслуживает клиентов CAD/CAM- приложений. Сервер 3 обслуживает HTTP, FTP - клиентов. Станции PC1-PC2 работаю с базой данных. Станции PC3-PC7 являются клиентами CAD/CAM- приложений.

Все станции являются HTTP, FTP –клиентами. Помимо серверов рабочие станции взаимодействуют внутри своих подсетей друг с другом по трафику *Small office peer-to-peer.*

Вариант 4. Корпоративная сеть включает 3 сегмента, которые объединены сетью FDDI:

- Сегмент 1– станции PC1-PC4, сервер 3, технология коммутируемый 100-Base –TX;
- Сегмент 2– станции PC5-PC6, сервер 2, технология *Token Ring.*
- Сегмент 3– станции PC7-PC9, сервер 1, технология коммутируемый 10-Base –T.

Сервер 2 обслуживает клиентов CAD/CAM- приложений. Сервер 3 обслуживает HTTP, FTP -клиентов. Сервер 1 обслуживает клиентов базы данных . Станции PC 7-PC9 работаю с базой данных. Станции PC1-PC4 являются клиентами CAD/CAM- приложений. Все станции являются HTTP, FTP –клиентами. Помимо серверов рабочие станции взаимодействуют внутри своих подсетей друг с другом по трафику *Small office peer-to-peer*

Вариант 5 Корпоративная сеть включает 3 сегмента, объединенных коммутатором:

- Сегмент 1– станции PC1-P2, сервер1, сервер2, сервер3, технология коммутируемый 100-Base –TX.
- Сегмент 2– станции PC3-PC4, технология 10-Base –T.
- Сегмент 3– станции PC5-PC7, технология *Token Ring.*
- Сегменты объединены мостами по технологии FDDI.

Сервер 2 обслуживает клиентов CAD/CAM-приложений. Сервер 3 обслуживает HTTP, FTP-клиентов. Сервер 1 обслуживает клиентов базы данных. Станции PC1, PC5-PC7 работаю с базой данных. Станции PC5-PC7 являются клиентами CAD/CAM- приложений. Все станции являются HTTP, FTP –клиентами. Помимо серверов рабочие станции взаимодействуют внутри своих подсетей друг с другом по трафику *Small office peer-to-peer.*

Вариант 6. Корпоративная сеть включает 3 сегмента, объединеных маршрутизатором:

- Сегмент 1– станции PC1-PC4, сервер1, технология FDDI.
- Сегмент 2– станции PC5-PC6, технология *Token Ring*;
- Сегмент 3– станции PC7-PC8, сервер2, сервер 3, технология коммутируемый 10-Base –T.

Сервер 2 обслуживает клиентов CAD/CAM- приложений. Сервер 3 обслуживает HTTP, FTP -клиентов. Сервер 1 обслуживает клиентов базы данных. Станции PC1-PC4 работаю с базой данных. Станции PC5-PC7 являются клиентами CAD/CAM- приложений. Все станции являются HTTP–клиентами. Помимо серверов рабочие станции взаимодействуют внутри своих подсетей друг с другом по трафику *Small office peer-to-peer.*

Вариант 7. Корпоративная сеть включает 3 сегмента, объединенных коммутатором:

- Сегмент 1– станции PC1-PC3, сервер1, сервер 3, технология коммутируемый 100-Base –TX.
- Сегмент 2– станции PC4-PC5, сервер2, технология 10-Base –T;
- Сегмент 3– станция PC6, технология 10-Base –T; сервер удаленного доступа, который через модемы и телефонную сеть общего пользования соединен с рабочими станциями PC7, PC8

Сервер 1 обслуживает клиентов CAD/CAM- приложений. Сервер 2 обслуживает HTTP -клиентов. Сервер 3 обслуживает FTP – клиентов. Станции PC1-PC5 работаю с FTP-сервером. Станции PC1-PC3 являются клиентами CAD/CAM- приложений. Все станции являются HTTP–клиентами. Помимо серверов рабочие станции сегмент 1 и 2 взаимодействуют внутри своих подсетей друг с другом по трафику *Small office peer-to-peer.*

Параметры трафика задаются в таблице 8.1

Таблица 8.1

Сервер	Размер транзакций		Время между транзакциями	
	Распределение	Параметры (байт)	Распределение	Параметры (с)
База данных	Нормальное	1500, 900	Экспонен.	0.11
CAM/CAD	Равномерное	100,1000	Нормальное	0.1, 0.009
HTTP	Экспонен.	400	Экспонен.	0.12
FTP	Нормальное	1000,400	Нормальное	0.5, 0.01
Peer-to-pear	Равномерное	100,1500	Равномерное	0.01, 0.5

Размер ответа серверов на запрос рассчитывается по экспоненциальному закону с математическим ожидание 250 байт. Задержка ответа сервера на запрос распределена равномерно в интервале 0.1 -1 с.

8.3.3. Отчёты должены содержать:

- наименование работы;
- вариант задания;
- скриншоты собранных и функционирующих проектов сети.

8.4. Вопросы для самопроверки

9) Какие задачи проектирования и исследования сетей могут быть решены с использованием пакета *NetCracker*?

10) Для каких целей служат браузеры устройств, рабочая зона, панель изображений?

11) Какие средства *NetCracker* позволяют количественно судить о степени загруженности конкретного канала связи?

12) Каков порядок установки трафика моделируемой сети?

13) Каким образом можно добавить, заменить и удалить устройства сетевого оборудования?

14) Как создается конфигурация Устройства?

15) Как определить свойства устройства (перечислите эти свойства)?

16) Как определить, что устанавливаемый в устройство модуль не может быть включен в устройство?

17) Какие средства необходимо использовать, чтобы связать устройства проекта?

18) Как проверить типы установленных связей проекта?

19) Какие параметры трафика необходимо задать для моделирования потоков данных.

Список литературы

1. Холме, Д. Управление и поддержка Microsoft Windows Server 2003. Учебный курс MCSA/MCSE / Д. Холме, О. Томас — М.: Издательско-торговый дом «Русская Редакция», 2004.

2. Коннов, Н. Анализ сетевых протоколов: лаб. практикум по курсу «Сети ЭВМ и телекоммуникации» / Н. Н. Коннов, В. Б. Механов. – Пенза: Изд-во ПГУ, 2010. – Ч. 1.

3. Власов, Ю. Администрирование сетей на платформе MS Windows Server. Учебный курс / Ю.В. Власов, Т.И. Рицкова - URL: http://www.intuit.ru/department/os/sysadmswin.

4. Котельников, Е.В. Сетевое администрирование на основе Microsoft Windows Server 2003. Лабораторный практикум / Е. В. Котельников, Н. А. Кротова - URL: http://window.edu.ru/window_catalog/files/r57451/kotelnikov-server2003-lab.pdf.

5. Бутаев, М.М. Моделирование сетей ЭВМ: Учебно-методическое пособие / М.М. Бутаев, Н.Н. Коннов – Пенза: Изд-во Пенз. гос. ун-та, 2007.

Содержание

Учебное издание

Калиниченко Евгений Иванович,
Коннов Николай Николаевич

Лабораторный практикум по курсу
«Сети ЭВМ и телекоммуникации»

Часть 2
«АДМИНИСТРИРОВАНИЕ И МОДЕЛИРОВАНИЕ СЕТЕЙ»

Редактор
Корректор
Компьютерная верстка

Подписано в печать . Формат 60x841/16.
Усл. печ. л. . Тираж 50.
Заказ № .

Издательство ПГУ.
440026, Пенза, Красная, 40.