МГАПИ	МОСКОВСКАЯ ГОСУДАРСТВЕННАЯ АКАДЕМИЯ ПРИБОРОСТРОЕНИЯ И ИНФОРМАТИКИ Кафедра “Персональные компьютеры и сети” Брейман А.Д. **Администрирование сетевых систем** Учебное пособие Москва, 2002

УДК 681.326(075)

Администрирование сетевых систем. Учебное пособие. /Брейман А.Д. – М.:МГАПИ, 2002. – ___с.:ил.

Рекомендовано Ученым Советом МГАПИ в качестве учебного пособия для специальности 22.01 “Вычислительные машины, комплексы, системы и сети”.

Настоящее пособие предназначено для подготовки студентов, изучающих принципы построения компьютерных сетей и технологии, использующиеся в локальных сетях. Рассмотрены принципы администрирования компьютерных сетей и телекоммуникационных систем.

Для специальности 22.01 настоящее пособие может быть использовано при изучении курса “Администрирование сетевых систем”.

Автор: Брейман А.Д.

Рецензенты: проф., к.т.н. Рощин А.В.
доц., к.т.н. Журавлев В.А.

Работа рассмотрена и одобрена на заседании кафедры ИТ-4 “Персональные компьютеры и сети” “ ” _____ 2002 г., протокол № __.

Зав. кафедрой ИТ-4,
профессор, д.т.н. Михайлов Б.М.

© Брейман А.Д., 2002
© МГАПИ, 2002

СОДЕРЖАНИЕ

ВВЕДЕНИЕ.....6
1. ВВЕДЕНИЕ В СИСТЕМНОЕ И СЕТЕВОЕ АДМИНИСТРИРОВАНИЕ . 6
1.1. Функции и обязанности сетевого администратора 6
1.2. Обеспечение доступности и прозрачности сети**Ошибка! Закладка не определена.**
1.3. Общие принципы обеспечения безопасности сетей 6
1.4. Безопасность в Интернете 6
1.5. Основные сетевые операционные системы 6
2. АДМИНИСТРИРОВАНИЕ СЕТЕЙ НА ОСНОВЕ MICROSOFT WINDOWS NT/2000/XP 6
2.1. Домены и рабочие группы 7
2.2. Пользователи и группы пользователей домена 7
2.3. Многодоменные сети 8
2.4. Служба Active Directory в Windows 2000/XP 9
2.5. Служба DNS в Windows NT/2000/XP 9
2.6. Файловые системы Windows NT/2000/XP 9
2.7. Механизмы отказоустойчивости дисковой подсистемы 9
3. УПРАВЛЕНИЕ ПОЛЬЗОВАТЕЛЯМИ В MICROSOFT WINDOWS NT/2000/XP 9
3.1. Состав бюджета пользователя 9
3.2. Политика управления пользователями 10
3.3. Типы прав пользователей 10
3.4. Встроенные группы пользователей и их права 10
3.5. Назначение разрешений на доступ к файлам и каталогам 11
3.6. Сценарии логического подключения 13
4. СРЕДСТВА МЕЖСЕТЕВОГО ВЗАИМОДЕЙСТВИЯ 13
4.1. Стек протоколов TCP/IP в Windows NT/2000/XP 13
4.2. Службы DHCP и WINS 13
4.3. Использование Windows NT/2000/XP для подключения локальной сети к Интернету 13
5. ПЕЧАТЬ, УДАЛЕННЫЙ ДОСТУП, АУДИТ, РЕЗЕРВИРОВАНИЕ ДАННЫХ 13
5.1. Средства печати Windows NT/2000/XP 13
5.2. Администрирование удаленного доступа 14
5.3. Настройка клиентов и сервера удаленного доступа (RAS) 14
5.4. Средства аудита Windows NT/2000/XP 14
5.5. Резервирование данных: устройства и программные средства 14
6. ИСПОЛЬЗОВАНИЕ LINUX-СЕРВЕРОВ В WINDOWS-СЕТЯХ 14
6.1. Использование Linux в качестве сетевой операционной системы для сетей с рабочими станциями под управлением Micosoft Windows 14
6.2. Установка и настройка файлового сервера Samba 14
6.3. Установка и настройка шлюза, маршрутизатора и брандмауэра 14
7. АДМИНИСТРИРОВАНИЕ ЭЛЕКТРОННОЙ ПОЧТЫ 14

7.1. Системы электронной почты в Windows и Unix 14
7.2. Установка и настройка Microsoft Exchange Server 14
7.3. Установка и настройка Sendmail 14
8. АДМИНИСТРИРОВАНИЕ WWW-СЕРВЕРА 14
8.1. WWW-серверы в Windows и Unix 14
8.2. Установка и настройка Microsoft Internet Information Server 14
8.3. Установка и настройка Apache 14
СПИСОК ЛИТЕРАТУРЫ 75

ВВЕДЕНИЕ

Считается, что через несколько лет системное администрирование станет в большой степени чисто административной (в бытовом понимании этого термина) работой. Компьютеры и сети будут работать и обслуживать себя сами. Работа системного администратора будет состоять в принятии решений о том, какое программное обеспечение нужно установить и кому оно будет доступно, регистрации пользователей и поддержании общей политики управления.

Однако в настоящее время системное администрирование – это не столько административная, сколько инженерно-техническая работа, касающаяся аппаратного и программного обеспечения, поддержки пользователей, ремонта и профилактики. Системный администратор должен разбираться как в технической стороне дела, так и в административных функциях, а также в психологии пользователей.

Сложность компьютерных (в особенности – сетевых) систем постоянно растет. Даже единственный персональный компьютер под управлением Windows NT/2000/XP, подключенный к сети, имеет уровень сложности, сравнимый с уровнем сложности мейнфреймов IBM или VAX десятилетней давности. Необходимо говорить уже не просто о компьютерах, но о (вычислительных) системах. Отметим несколько групп систем, представляющих интерес для данного курса: многозадачные системы, многопользовательские системы, сетевые системы.

В данном курсе мы будем иметь дело с сетевыми системами, для которых особенно важно следующее соображение. Как только компьютер подключен к сети, он перестает быть вашим “персональным” компьютером. То, что вы на нем делаете, влияет на других людей и их компьютеры, а то, что они делают – влияет на вас. Ваш компьютер становится принципиально подверженным различным атакам со стороны внешнего мира.

Это значит, что появляется этическая (в некоторых случаях – не только этическая) ответственность перед остальными участниками сети: ваш компьютер должен работать корректно, а вы должны вести себя правильно.

1. ВВЕДЕНИЕ В СИСТЕМНОЕ И СЕТЕВОЕ АДМИНИСТРИРОВАНИЕ

1.1. Вычислительные системы и сети

1.2. Функции и обязанности сетевого администратора

Системное администрирование включает в себя планирование, установку и поддержание работоспособности компьютерных систем (с целью обеспечения работы предприятия).

Функции сетевого администратора

Обеспечение доступности сети
Обеспечение прозрачности сети
Обеспечение документированности сети

Две группы задач: поддержка пользователей (управление учетными записями, защита данных пользователей, упрощение работы) и поддержка систем (безопасность, настроенность, своевременность).

Обязанности сетевого администратора

”Тушение пожаров”
Обучение пользователей
Управление учетными записями пользователей и групп
Конфигурирование и обслуживание настольных систем
Резервное копирование и восстановление, анализ производительности, обеспечение защиты
Обслуживание аппаратных и программных средств серверов и сети
Планирование действий в аварийных ситуациях
Планирование расширения сети

Основные свойства сетевой системы с точки зрения пользователя – это надежность и доступность. Параллельное подключение сетевых серверов увеличивает эффективность обслуживания и уменьшает вероятность отказа в обслуживании.

1.3. Общие принципы обеспечения безопасности сетей

1.4. Безопасность в Интернете

1.5. Основные сетевые операционные системы

2. АДМИНИСТРИРОВАНИЕ СЕТЕЙ НА ОСНОВЕ MICROSOFT WINDOWS NT/2000/XP

2.1. Домены и рабочие группы

Компьютеры, входящие в сети, логически объединяют в группы или иерархии.

Домены и рабочие группы

Рабочие группы объединяют компьютеры для более удобной работы с сетевыми сервисами. Каждый сервер в рабочей группе должен вести собственную независимую БД пользователей.

Домены логически группируют серверы и рабочие станции; в каждом домене ведется одна БД учетных записей, действительная для всех серверов домена. Эта БД хранится на главном контроллере домена (PDC), на остальных серверах ведется копия центральной БД реплицируемая (5 мин) с PDC. Запрос на вход в систему может проверить любой сервер. Для доступа пользователя к любому из серверов домена нужна только одна учетная запись и единственная процедура подключения. Доверительные отношения между доменами позволяют получать доступ к нескольким доменам, не дублируя учетные записи.

Домен – это понятие, определяющее централизованно управляемый набор ресурсов общего пользования (файл-серверов и серверов приложений, принтеров, модемов и других устройств). Доступ к ресурсам, входящим в домен, предоставляется только пользователям, подключившимся (log on) к домену, и, кроме того, обладающим необходимыми допусками (permission). Ресурсы обычно объединяют в домены по географическому или функциональному признаку (“Киевский филиал”, “Отдел продаж”).

2.2. Пользователи и группы пользователей домена

Учетные записи пользователей

Учетная запись содержит идентификатор безопасности (SID), пользовательские права и права доступа. При подключении (logon), диспетчер безопасности (SAM) сверяет регистрационную информацию с данными из БД с тем, чтобы аутентифицировать вход в систему. После того, как доступ предоставлен, распорядитель локальной безопасности (LSA) создает для этого пользователя маркер безопасности (security access token).

Учетная запись глобального пользователя (global user account): обычная учетная запись; таковы все записи на NT Workstation, и на NT Server – не контроллерах. Аутентифицируются PDC или BDC в домене, или через доверительные отношения.

Учетная запись локального пользователя (local user account): пользователь доступный только через удаленный вход в систему, аутентифицируется на локальном компьютере, обрабатывающем подключение. Невозможно аутентифицировать через доверительные отношения.

При инсталяции WindowsNT создаются три учетные записи:

Administrator (может все; если забыт пароль - можно воспользоваться диском Emergency Repair или переисталлировать систему)

Guest (ограниченный доступ, например может только посылать документы на принтер)

Группы пользователей

Удобно организовать пользователей с одинаковыми административными требованиями в группы пользователей, что упрощает администрирование, группе можно присвоить общий скрипт, права доступа к файлам, разрешения и профиль пользователя. Группы могут быть локальными и глобальными.

Глобальная группа – это набор пользовательских учетных записей из одного домена. Такая группа может содержать только учетные записи пользователей из того домена, в котором она сама создана (не может содержать другие группы и чужих пользователей). Другие домены могут назначать чужим глобальным группам (из доменов, оторым они доверяют) допуски к своим ресурсам.

Локальная группа – это набор пользовательских учетных записей и/или учетных записей глобальных групп, которой могут быть назначены допуски к ресурсам только в том домене, где

она создана. Локальные группы удобно использовать, когда нужно предоставить допуски к ресурсам пользователям из других доменов.

Аутентификация пользователей

1. Обнаружение (Discovery)
2. Установление безопасного канала (Secure channel setup)
3. Сквозная (pass-through) аутентификация (при необходимости)

При недоступности всех контроллеров при интерактивном входе в систему может использоваться кэшированная информация (default – 10 users)

2.3. Многодоменные сети

Доверительные взаимоотношения между доменами

Связь между двумя доменами, позволяющая пользователям, имеющих учетную запись в одном домене (доверяемом), получать доступ к ресурсам другого (доверяющего) без заведения дополнительной учетной записи. Домен, с которым устанавливаются доверительные отношения (доверяемый) позволяет использовать свои учетные записи в домене, который устанавливает доверительные отношения (доверяющем). При установлении доверительных отношений, в SAM доверяемого домена создается невидимая учетная запись междоменных доверительных отношений (с флагом USER_INTERDOMAIN_TRUST_ACCOUNT и случайным паролем)

Доверительные отношения – односторонние (несимметричные), не транзитивные.

Модели доменов

Одиночный домен - <10000 (NT3.5) или 26000 (NT4) пользователей, взаимное доверие между подразделениями; вариант: множество одиночных доменов

Главный домен - <10000 (NT3.5) или 26000 (NT4) пользователей,: один домен является доверяемым для всех остальных, сам не доверяет никому, несет все пользовательские учетные записи; остальные домены могут доверять друг другу по необходимости

Множественные главные домены: крупные организации; несколько главных доменов, каждый из которых доверяет всем остальным главным доменам, все главные домены являются доверяемыми для всех остальных, а сами не доверяет ни одному из субдоменов; хорошо масштабируема

Множественные доверительные отношения; каждый домен доверяет всем остальным; хорошо масштабируема

2.4. Служба Active Directory в Windows 2000/XP

2.5. Служба DNS в Windows NT/2000/XP

2.6. Файловые системы Windows NT/2000/XP

2.7. Механизмы отказоустойчивости дисковой подсистемы

3. УПРАВЛЕНИЕ ПОЛЬЗОВАТЕЛЯМИ В MICROSOFT WINDOWS NT/2000/XP

3.1. Состав бюджета пользователя

Учетная запись пользователя

Имеет уникальный идентификатор безопасности (SID), присваиваемый при создании; если удалить учетную запись, а потом создать новую с тем же именем, все допуски будут потеряны.

Username (вводится при logon'е), Password, Full name, Logon hours, Logon on workstations, Expiration date, Home directory, Logon script, Profile (environment), Account Type

Окружение пользователя (Environment)

Доступные ресурсы + конфигурация пиктограмм desktop'а + фоновые рисунки + параметры автоматических соединений по сети + startup – программы; управляется профилем, входным сценарием (скриптом), личным каталогом

Содержание профиля (profile)

Сохраняются при выходе настройки, которые мог сделать сам пользователь:

(Program/Desktop manager): собственные группы программ и shortcut'ы

(File manager / Explorer): сетевые соединения

(DOS session) шрифты, цвета, параметры видеобуфера, положение окон

(Print manager) связь с принтерами сети и все настройки

(Control Panel) набор цветов, screensaver, настройки мыши и клавиатуры, sound, international, cursor

(Accessories) настройки прикладных программ: Calc, Calendar, Cardfile, Clock, Notepad, PBrush, Terminal

настраиваемые на пользователя прикладные программы

закладки в системе справки

Типы профилей

На NT Workstation автоматически создаются локальные профили (в Registry: HKLM\Software\Microsoft\Windows\Current Version\Profile List)

На NT Server – персональные (.USR) или обязательные (.MAN) профили, привязанные к учетным записям

Личный каталог (home directory)

\Users\Default (\Users\имя_пользователя)

Входные сценарии (script)

\WinNT или \WinNT\SYSTEM32\REPL\IMPORT\SCRIPTS

.BAT, .CMD, .EXE – файл

3.2. Политика управления пользователями

3.3. Типы прав пользователей

Права и допуски

Право (Right) – относится к системе в целом и разрешает пользователю выполнять в системе определенные действия (logon, set server time, backup/restore, etc.); Права предоставляются на уровне домена.

Допуск (Permission) – относится к объекту (каталогу, файлу или принтеру); является правилом, определяющим, кто из пользователей имеет доступ к объекту и каким образом.

3.4. Встроенные группы пользователей и их права

Группы, создающиеся автоматически при инсталляции (если не указано другое, то локальные):

Administrators, Users, Backup Operators, Guests – Windows NT WS и Server

Domain Admins (глобальная), Domain Users (глобальная), Account Operators, Print Operators, Server Operators, Replicators – Windows NT Server

Power Users – NT WS или Server – не котроллер

Права пользователей (в скобках – группы, которые обладают данным правом по умолчанию)

Access this computer from network (Admin,Users)
Backup files and directories (выше чем No Access) (Admin,ServOp,BackOp)
Change system time (Admin,ServOp)
Force shutdown from a remote system (Admin,ServOp)
Log on locally (Admin,ServOp,AccOp,PrnOp,BackOp)
Manage auditing and security log (Admin)
Restore files and directories (Admin,ServOp,BackOp)
Shut down the system (Admin,ServOp,AccOp,PrnOp,BackOp)
Take ownership of files and other objects (Admin)

Следующие дополнительные права есть только у группы Administrators:
Load and unload device drivers
Log on as a service
Bypass traverse checking
Add workstations to domain
Create a page file
Debug programs
Profile single process
Profile system performance

3.5. Назначение разрешений на доступ к файлам и каталогам

Из дисковых файловых систем, поддерживаемых Windows NT, только NTFS предоставляет полный набор средств обеспечения безопасности. Доступ к дискам с файловой системой FAT может быть ограничен только на уровне папок общего доступа (share-level security).

Папки общего доступа (shared folders) автоматически предоставляют доступ к своим подпапкам и файлам, то есть не дают возможности тонкой настройки допусков. Второй их недостаток – проверка допуска к таким папкам производится только при доступе по сети, а пользователь, подключившийся локально (с клавиатуры сервера), независимо от того,

имеет полный допуск ко всем таким папкам, Папку общего доступа можно скрыть (ее имя не будет видно при просмотре списка папок), добавив к ее имени символ доллара ‘$’.

Допуски к папкам общего доступа:

No Access (None) – нет доступа

Read – пользователь может видеть имена файлов и подпапок, переходить в подпапки, открывать файлы в режиме “только чтение” и запускать программы. Пользователь не может изменять содержимое файлов и удалять их.

Change – пользователь может выполнять действия, разрешенные допуском Read, и, кроме того, создавать, изменять и удалять файлы и подпапки.

Full Control (All) – пользователь может выполнять действия, разрешенные допуском Change, и, кроме того, управлять допусками NTFS к этой папке, ее файлам и подпапкам, а также приобретать права владельца папки.

NT Server автоматически создает несколько административных папок общего доступа:

ADMIN$ – папка, в которой находятся файлы операционной системы (скорее всего, C:\WinNT)

[буква диска]$ – корневые папки всех разделов всех жестких дисков сервера.

Файловая система NTFS хранит для каждого своего объекта (папки или файла) набор дополнительных атрибутов, в том числе, атрибутов, управляющих доступом к данному объекту – допусков NTFS (NTFS permissions). Если для объекта заданы допуски для нескольких групп, то пользователь, принадлежащий к этим группам обладает некоторым допуском, если такой допуск есть у любой из этих групп. Допуски NTFS, установленные для папок общего доступа не могут повысить уровень доступа, а только понизить или оставить прежним.

Файловые допуски NTFS:

No Access (None) – нет доступа к файлу

Read (RX) – можно просматривать имя файла, открывать его в режиме “только чтение”. Если этот файл – программа, то ее можно выполнять.

Change (RWXD) – пользователь может выполнять действия, разрешенные допуском Read, и, кроме того, создавать, изменять и удалять файлы и подпапки.

Full Control (All) – пользователь может выполнять действия, разрешенные допуском Change, и, кроме того, управлять допусками NTFS к этой папке, ее файлам и подпапкам, а также приобретать права владельца папки.

Special Access – можно задать любую комбинацию элементарных допусков (Read, Write, eXecute, Delete, change Permissions, take Ownership).

Допуски к папкам NTFS (в первых скобках – эффект для самой папки, во вторых скобках – эффект для файлов, содержащихся в ней):

No Access (None) (None) – нет доступа к папке и ее содержимому

List (RX) () – можно просматривать список файлов и подпапок, а также переходить в подпапки.

Read (RX) (RX) – можно выполнять действия, разрешенные допуском List, и, кроме того, открывать файлы в режиме “только чтение”, а также запускать программы.

Add (WX) () – можно создавать новые файлы и подпапки, но нельзя открывать файлы – даже только что созданные.

Add & Read (RWX) (RX) – можно выполнять все действия, разрешенные допусками Read и Add.

Change (RWXD) (RWXD) – можно выполнять все действия, разрешенные допуском Add & Read и, кроме того, изменять содержимое файлов, а также удалять файлы и подпапки.

Full Control (All) All) – можно выполнять действия, разрешенные допуском Change, и, кроме того, управлять допусками NTFS к этой папке, ее файлам и подпапкам, а также приобретать права владельца папки.

Special Directory Access – можно задать любую комбинацию элементарных допусков (Read, Write, eXecute, Delete, change Permissions, take Ownership). Допуск eXecute для папки означает возможность перехода в нее.

Special File Access – можно задать любую комбинацию элементарных допусков (Read, Write, eXecute, Delete, change Permissions, take Ownership).

Допуски к папкам NTFS имеют преимущество над файловыми допусками NTFS: если для пользователя установлен допуск к папке NTFS 'Full Control', а к некоторому файлу в этой папке – 'Read', то в результате пользователь может производить любые операции с этим файлом.

3.6. Сценарии логического подключения

4. СРЕДСТВА МЕЖСЕТЕВОГО ВЗАИМОДЕЙСТВИЯ

4.1. Стек протоколов TCP/IP в Windows NT/2000/XP

4.2. Службы DHCP и WINS

4.3. Использование Windows NT/2000/XP для подключения локальной сети к Интернету

5. ПЕЧАТЬ, УДАЛЕННЫЙ ДОСТУП, АУДИТ, РЕЗЕРВИРОВАНИЕ ДАННЫХ

5.1. Средства печати Windows NT/2000/XP

Принтеры общего доступа

NT позволяет предоставить общий доступ как к принтерам, непосредственно подключенным к серверу, так и к принтерам с непосредственным подключением к сети (например, оборудованным сетевым интерфейсом HP JetDirect) и принтерам, подключенным к другим компьютерам (в том числе, к серверам Novell Netware).

Типы доступа к принтеру:

No Access – нет доступа

Print – можно печатать документы, но нельзя управлять очередью печати (например, нельзя отменить свое же задание на печать).

Manage Documents – можно печатать документы и управлять принтером.

Full Control – можно печатать документы, управлять принтером и изменять его настройки (этот тип доступа обычно назначается только группам Administrators, Print Operators и Server Operators).

5.2. Администрирование удаленного доступа

5.3. Настройка клиентов и сервера удаленного доступа (RAS)

5.4. Средства аудита Windows NT/2000/XP

5.5. Резервирование данных: устройства и программные средства

6. ИСПОЛЬЗОВАНИЕ LINUX-СЕРВЕРОВ В WINDOWS-СЕТЯХ

6.1. Использование Linux в качестве сетевой операционной системы для сетей с рабочими станциями под управлением Micosoft Windows

6.2. Установка и настройка файлового сервера Samba

6.3. Установка и настройка шлюза, маршрутизатора и брандмауэра

7. АДМИНИСТРИРОВАНИЕ ЭЛЕКТРОННОЙ ПОЧТЫ

7.1. Системы электронной почты в Windows и Unix

7.2. Установка и настройка Microsoft Exchange Server

7.3. Установка и настройка Sendmail

8. АДМИНИСТРИРОВАНИЕ WWW-СЕРВЕРА

8.1. WWW-серверы в Windows и Unix

8.2. Установка и настройка Microsoft Internet Information Server

8.3. Установка и настройка Apache

СПИСОК ЛИТЕРАТУРЫ

1. **Компьютерные сети. Принципы, технологии, протоколы.** / В.Г.Олифер, Н.А.Олифер. — СПб: Издательство “Питер”, 1999. — 672 с.: ил.
2. **Высокопроизводительные сети. Энциклопедия пользователя**: Пер. с англ./Марк А. Спортак и др. — К.: Издательство “ДиаСофт”, 1998. – 432с.
3. Кульгин М. **Технологии корпоративных сетей. Энциклопедия** — СПб: Издательство “Питер”, 2000. — 704 с.: ил.
4. Гук М. **Аппаратные средства локальных сетей. Энциклопедия** – СПб.: Издательство “Питер”, 2000. –576с.:ил.
5. **Компьютерные сети+.** Учебный курс (MSCE 70-058)/Пер. с англ. — М.: “Русская редакция”, 2000. — 552с.
6. **Сети Windows NT 4.0**: Пер. с англ. /Джон Д. Рули и др. — К.: Издательская группа BHV, 1997. — 800с.
7. Мельников Д.А. **Информационные процессы в компьютерных сетях. Протоколы, стандарты, интерфейсы, модели…** – М: КУДИЦ-ОБРАЗ, 1999. – 256с., ил.
8. Якубайтис Э.А. **Информационные сети и системы.** Справочная книга. — М.: Финансы и статистика, 1996. — 368с.: ил.
9. Ратынский М.В. **Основы сотовой связи** / Под ред. Д.Б. Зимина. – 2-е изд., перераб. и доп. – М.:Радио и связь, 2000. – 248с.:ил.
10. Семенов А.Б., Стрижаков С.К., Сунчелей И.Р. **Структурированные кабельные системы,** 3-е изд. – М.: “Компьютер-Пресс”, 2001. – 608с.

1. Вишневский А. **Сетевые технологии Windows 2000 для профессионалов** – СПб.:Питер, 2000. – 592с.
2. Джонс А. **Руководство системного администратора Windows: для профессионалов** – СПб.:Питер, 2000. – 368с.
3. **Сети Windows NT 4.0**: Пер. с англ. /Джон Д. Рули и др. — К.: Издательская группа BHV, 1997. — 800с.
4. **Ресурсы MS Windows NT Server 4.0**: пер. с англ. – СПб.: BHV – Санкт-Петербург, 1998. – 408с.
5. **Сетевые средства MS Windows NT Server 4.0**: пер. с англ. – СПб.: BHV – Санкт-Петербург, 1998. – 496 с.

б) дополнительная литература

1. Хиллей В. **Секреты Windows NT Server 4.0**: пер. с англ. – К.:"Диалектика", 1997. – 528 с., ил.
2. Microsoft Corp. **Администрирование сети на основе Microsoft Windows 2000.** Учебный курс MCSE №70-216 /Пер. с англ. – М.: “Русская редакция”, 2000. – 512с.
3. Карлинг М. и др. **Системное администрирование Linux** – М.: Вильямс, 2000. – 320с.

4. Сэри П. **Сервер Red Hat Linux для MS Windows. Методология эффективного построения и управления локальными сетями**: пер. с англ. – М.: ДиаСофт, 2000. – 400с.
5. Устинов Г.Н. **Основы информационной безопасности систем и сетей передачи данных** – М.:СИНТЕГ, 2000. – 248с.

ИНТЕРНЕТ

1. Русские документы: сетевые технологии http://www.rusdoc.ru/net.shtml
2. Сетевые протоколы http://www.protocols.ru
3. Аналитический обзор базовых стандартов СКС http://www.ecolan.ru/st_review.htm
4. Техническая библиотека компании BiLiM Systems http://www.bilim.com
5. Сервер информационных технологий: сетевые технологии http://www.citforum.ru/nets/
6. Книги по сетям http://document.newmail.ru/la.htm
7. Термины и основные понятия телекоммуникаций http://www.online.ru/it/helpdesk/race/index.htm
8. Архив: проектирование сетей http://www.osp.interline.ru/archive/35.htm
9. Практика проектирования сетей http://kgg.moldline.net/

http://www.rusdoc.ru/nt.shtml
http://www.citforum.ru/nets/spsmp/index.shtml
http://www.citforum.ru/operating_systems/windows.shtml
http://www.bookcase.ru/os/oswint1.html
http://www.rusdoc.ru/unix.shtml
http://www.bugtraq.ru
http://www.opennet.ru

Учебное издание

Брейман Александр Давидович

Администрирование сетевых систем.
Учебное пособие.