Лекция 5. Windows 2000

Windows 2000 (NT 5.0, или на слэнге w2k) - операционная система фирмы Microsoft, основанная на технологии Windows NT 4.0. Была создана группой разработчиков под руководством Дэйва Катлера, который еще в 1988 году пришёл в Microsoft (ранее работал в DEC) специально для работы над NT 4.0
Существуют следующие варианты Win2000:

1. Windows 2000 Professional - вариант для рабочей станции = Windows NT Workstation.
2. Windows 2000 Server или Windows 2000 Advanced Server - варианты для сервера = Windows NT Server. Наилучший выбор - Advanced Server: более полный пакет программ, поддерживает до 8 процессоров.
3. Windows 2000 Data Center – вариант для мощных корпоративных серверов (поддержка до 64 процессоров, в небольших сетях будет только зря использовать ресурсы).

5.1. Отличительные особенности Win2000

Windows 2000 – это мощная и удобная операционная система, которая имеет свои достоинства и недостатки. Сопоставление Windows 2000 и Unix/Linux систем, с точки зрения выбора операционной системы для сервера локальной сети, приведены ниже.

Таблица 5.1.

Сопоставление Windows 2000 и Unix/Linux систем

Windows 2000	Unix/Linux
Удобный и привычный для пользователей Windows графический интерфейс. Большинство настроек выполняется при помощи удобных графических форм (флажки, переключатели и т.п.).	В последнее время большинство *nix систем получило графический интерфейс, однако пока еще большое значение (и одновременно преимущество) имеет управление сервером из командной строки, и использование простых текстовых редакторов для ручного редактирования файлов конфигурации.
Большинство задач по конфигурированию и управлению сервером выполняется при помощи удобных мастеров. Для настройки системы необязательно иметь детальное представление о принципах ее работы. Сложно допустить фатальную ошибку.	Большинство действий по конфигурации системы выполняются вручную. Невозможно правильно настроить систему, не разобравшись перед этим во всех деталях того, что Вы собираетесь делать. Пользователь с низким уровнем подготовки может легко допустить ошибку, критическую для сетевой безопасности или стабильной работы системы.
Справочная система рассчитана на пользователя с низким и средним уровнем подготовки.	Справочная система рассчитана на пользователя со средним и высоким уровнем подготовки.
Хорошая локализация. Настройка русского, или других национальных языков, не представляет проблем.	Хотя даже между различными дистрибутивами Linux в этом вопросе имеются различия, однако в целом локализация реализована плохо. Настройка русского языка представляет собой не тривиальную проблему. Отсутствует единая схема настройки. Приходится настраивать русский язык в нескольких местах и даже по отдельности в разных программных пакетах.
Чрезвычайно требовательна к ресурсам оборудования (объем памяти, процессор, дисковое пространство и т.д.).	Мало требовательна к ресурсам оборудования. Если на том же компьютере, где установлена Windows 2000, установить Linux, то система будет работать в несколько раз быстрее.
Хотя Windows 2000 защищена существенно больше, чем Windows 95/98/ME, однако и она имеет существенные проблемы с сетевой безопасностью. В целом уязвима вся операционная система, хотя наиболее часто атакам подвергается Internet Information Services (IIS), предоставляющий доступ к сервисам HTTP, FTP, SMTP и др.	Гораздо меньше, чем Windows 2000 уязвима к сетевым атакам. Большинство из атак хорошо изучены и отработаны механизмы противодействия им. Если не пользоваться новым не стабильным и не протестированным программным обеспечением, а также грамотно конфигурировать сервер, то Вы будете достаточно надежно защищены от сетевых атак.
За использование лицензионной копии операционной системы необходимо платить достаточно большую сумму. Исходные тексты операционной системы не доступны и не могут быть изменены под нужды пользователя.	Операционная система и программное обеспечение для нее распространяется бесплатно и доступна в исходных текстах. Наличие исходных текстов и сама архитектура системы позволяет сконфигурировать ОС "под себя" оставив только то, что действительно необходимо (это значительно повышает и без того высокое быстродействие ОС). Открытые исходные тексты позволяют любому желающему тестировать и исправлять ошибки ОС. В результате, стабильность и надежность работы Unix/Linux значительно превосходят Windows 2000. Наличие исходных текстов ОС и программ позволяет проверить их на наличие "черных ходов" и других нарушений сетевой безопасности, не доверяя честному слову разработчиков.

Исходя из изложенного выше можно сделать вывод: область применения Windows 2000 – это локальные сети небольших предприятий, где персонал администрирования сети имеет низкую или среднюю квалификацию, либо не хочет тратить значительное время на настройку и обслуживание ОС, при условии, что обеспечение сетевой безопасности не является ключевым моментом политики предприятия, и возможные последствия от инцидентов с безопасностью не существенны. Если же сетевая безопасность важна и имеется высококвалифицированный персонал администрирования сети, то лучше использовать Unix/Linux системы. В частности, шлюз в Internet настоятельно рекомендуется реализовывать на базе Unix/Linux.

Из сказанного вовсе не следует, что Linux однозначно лучше Windows 2000. Просто каждая операционная система имеет свою область применения и свой набор возможностей, из которых необходимо выбрать то, что Вам необходимо. Ниже более детально будут рассмотрены некоторые возможности ОС Windows 2000 Server. Рассмотрению возможностей ОС Linux будет посвящена отдельная лекция.

5.2. Файловая система NTFS

NTFS выросла из файловой системы HPFS, разрабатываемой совместно IBM и Microsoft для проекта OS/2. Отличительными характерными чертами NTFS являются:

1. Надежность: вызвать сбой в NTFS чрезвычайно сложно (для опыта запускалась много различных приложений, оптимизаторы диска, и в самые неподходящие моменты жалась кнопка reset - повторение этого эксперимента добрый десяток раз никакого впечатления на систему не произвело). NTFS содержит две копии аналога FAT, которые называются MFT (Master File Table). Если оригинал MFT повреждён (например, при появлении bad-сектора), то система использует копию MFT. В отличие от FAT MSDOS, технология MFT больше напоминает обработку транзакций в базах данных: при любом сбое во время записи файла на диск, MFT будет восстановлена в состояние "до записи файла". Таким образом, вы теряете не весь файл, а только те изменения, которые находились в момент сбоя в памяти или в кэше контроллера, и не успели записаться на диск.
2. Защищенность: NTFS рассматривает файлы, как объекты. Каждый файловый объект обладает методами (например, open, close, read и write) и свойствами (имя, дата создания, дата последнего обновления, архивный статус, дескриптор безопасности). Дескриптор безопасности позволяет настроить права доступа к объекту и аудит объекта (Проводник/Выделить файл (каталог)/Контекстное меню/Свойства/Безопасность). Для различных пользователей (групп пользователей) возможно определить следующие права доступа: полный доступ, запись, чтение, обзор содержимого папки, создание подпапок и файлов, удаление подпапок и файлов, выполнение файлов, чтение и запись атрибутов и разрешений файла (папки), смена владельца и др. Там же, для каждого из пользователей (групп пользователей) можно создать политику аудита, которая будет регистрировать в специальном журнале (Пуск/Панель управления/Администрирование/Просмотр событий/Журнал безопасности) успех или неудачу при попытке получить доступ к файлу (каталогу). Попытки доступа классифицируются в соответствии с приведенным выше перечнем прав доступа. Регистрация успешных попыток позволяет следить за разрешенной деятельностью пользователей, регистрация неудачных попыток позволяет выявить попытки нарушения прав доступа. Для обеспечения большей надежности можно также использовать шифрованную файловую систему (Encrypted File System, EFS). Эта возможность встроена в Windows 2000 (Проводник/Выделить файл (каталог)/Контекстное меню/Свойства/Общие/Атрибуты/Другие/Шифровать содержимое для защиты данных). EFS использует шифрование открытого ключа (асимметричный алгоритм шифрования), что позволяет администратору создать агента восстановления зашифрованных данных – человека, который сможет расшифровать файлы других пользователей (например, при увольнении работника, по решению суда, при утере работником ключа шифрования из-за сбоев на диске).
3. Работа с большими дисками размером до 16,777,216 терабайт. Сжатие данных встроено на уровне файловой системы и позволяет сжимать не только целиком диск, но также отдельные каталоги и файлы "прозрачно" для пользователя (Проводник/Выделить файл (каталог)/Контекстное меню/Свойства/Общие/Атрибуты/Другие/Сжимать содержимое). Более высокая скорость работы с диском, благодаря структуре файловой системы и Microsoft Index Server, который значительно ускоряет поиск файлов, за счёт индексации содержимого дисков. Возможность поиска файла, по имени его владельца. Например, вам нужно удалить все файлы созданные уволенным сотрудником, а их на диске – тысячи.
4. Возможность "квотирования", т.е. ограничения максимального размера, выделяемого пользователю на диске, причем файлы пользователя могут находиться в самых разных каталогах, но их суммарный объем не может превышать установленного администратором (Проводник/Выделить диск/Свойства/Квота).
5. Монтирование сетевых и локальных дисков в любой каталог файловой системы (аналогично монтированию в Unix/Linux). Возможность изменить букву диска, или полностью удалить букву диска и оставить доступ к диску только через каталог на другом диске – таким образом можно организовать доступ к большому количеству дисков через единую структуру каталогов (Пуск/Настройка/Панель управления/Администрирование/Управление компьютером/Запоминающие устройства/Управление дисками/Выбрать диск/Контекстное меню/Изменение буквы диска и пути диска). Данная возможность доступна не только для дисков NTFS, но и для дисков с другими файловыми системами.

5.3. Распределенная файловая система DFS

Распределенная файловая система (DFS) дает возможность предоставить пользователям файлы, физически находящиеся на разных серверах, так, как если бы они находились в одном месте. Например, если бухгалтерская документация находится на разных серверах, можно использовать DFS, чтобы для пользователей все выглядело так, как будто вся документация располагается на одном сервере. Или, например, в рамках DFS, можно переместить файл с одного сервера на другой без необходимости информировать пользователей о том, что "файл переехал" – для них файл останется там же, где и был. Кроме того, задачи по обслуживанию сервера (обновлению программ и т.п.), могут выполняться без отключения пользователей. Настройка файловой системы DFS осуществляется через меню Пуск/Настройка/Панель управления/Администрирование/Распределенная файловая система DFS.

5.4. Динамические диски в Windows 2000

Win2000 позволяет преобразовать винчестер (физический диск) в динамический диск (Пуск/Настройка/ Панель управления/ Администрирование/Управление компьютером/Запоминающие устройства/Управление дисками/ Выбрать ***физический*** диск (например, диск 0)/Контекстное меню/Обновление до динамического диска). Внимание! Эта операция полностью передает физический диск в распоряжение Windows 2000 и ***удаляет*** с него логические разделы других операционных систем. Динамический диск не может содержать разделы или логические диски. Данные с динамического диска могут быть считаны только при помощи Windows 2000. Создание динамических дисков позволяет:

1. Создавать составные (spanned) динамические диски, т.е. несколько винчестеров, ведущих себя так, как если бы это был один большой винчестер. Данные пишутся последовательно, т.е. сначала заполняется один винчестер, затем второй и т.д.
2. Создавать чередующиеся (stripped) динамические диски, т.е. несколько винчестеров, ведущих себя как один большой винчестер, причем данные пишутся на диски параллельно, что ускоряет дисковые операции. Чисто условно можно представить себе так: 1-3-5 кластер файла пишется на первый диск, а 2-4-6 кластер – на второй диск.
3. Создавать зеркальные (mirrored) диски. Данные записываемые на один из дисков автоматически дублируются на другом. Это обеспечивает большую надёжность сохранности данных.
4. Создавать RAID диски. RAID – состоит из трёх, или более дисков. Данные пишутся параллельно на два или более дисков (см. п.2), а на третий диск записывается код коррекции ошибок (ECC) , с помощью которого можно восстановить содержимое испорченного блока на одном из дисков данных, по информации уцелевшего блоков второго диска данных. Или, чисто условно, зная содержимое кластеров 1-3-5 на первом диске и коды коррекции ошибок ECC1-ECC2-ECC3 с третьего диска, можно восстановить содержимое кластеров 2-4-6 второго диска. Эта технология экономнее, чем создание зеркальных дисков (дублируются не все кластеры 1-2-3-4-5-6, а только их половина ECC1-ECC2-ECC3), однако работает медленнее.

5.5. Служба каталогов Active Directory в Windows 2000 (ранее NTDS в Win NT 4.0), сценарии входа и профили пользователя.

Active Directory - это новое средство централизованного управления пользователями и сетевыми ресурсами, облегчающее администрирование больших сетей. Вся сеть представляется в виде иерархической структуры каталогов (контейнеров). Преимуществом является то, что все пользователи (группы пользователей, компьютеры, принтеры и т.д.) регистрируются не на каждом компьютере сети по отдельности, а централизованно – в службе каталогов Active Directory. После этого пользователь может подойти к любому компьютеру в офисе, ввести свой пароль, и перед ним будет его рабочий стол, его документы, его настройки. При использовании Active Directory у администратора отпадает необходимость вручную конфигурировать каждый компьютер, если, к примеру, необходимо поменять права доступа к какому-либо объекту сети или установить новый сетевой принтер. Такие изменения можно производить сразу для всей сети.

При использовании Active Directory вся информация о сети (а точнее о домене сети) хранится на специальном сервере – контролере домена. Контролеров домена (серверов) в одном домене может быть несколько, что повышает отказоустойчивость системы. При подключении к сети, пользователь общается именно с контролером домена, передавая ему свое имя и пароль (подробнее система безопасности Windows 2000 будет рассмотрена ниже). Создание службы Active Directory означает ее установку на контролер домена. Контролер домена должен работать под управлением минимум Windows 2000 Server. Рабочие станции под Windows 2000 Professional могут работать в среде Active Directory, но не могут создавать её. Создание Active Directory осуществляется при помощи команды меню "Пуск/Настройка/Панель управления/Администрирование/Настройка сервера/Active Directory". После создания Active Directory управление учетными записями пользователей доступно через команду меню "Пуск/Настройка/Панель управления/Администрирование/Active Directory – пользователи и компьютеры" (подробнее см. в разделе "Система безопасности Windows 2000"). При помощи этого меню можно создавать/удалять пользователей, менять их пароль, членство в различных группах и т.д.

Как уже упоминалось выше, при использовании Active Directory, пользователь может подойти к любому компьютеру в сети, ввести свое имя и пароль и Windows 2000 сам установит все настройки рабочего стола пользователя, подключит сетевые диски с документами пользователя и т.д. Достигается это за счет использования сценариев входа и профилей пользователя.

Профиль пользователя определяет настройки рабочей среды, включая настройки рабочего стола и меню пользователя, настройки дисплея, сеть, соединения с принтером, содержимое реестра и другие установки. Существуют следующие типы профилей пользователя:

- локальный профиль — создается при первом входе пользователя на конкретный компьютер и хранится на локальном жестком диске конкретного компьютера. Любые изменения локального профиля (настройка меню и т.п.) будут применены к данному компьютеру.
- перемещаемый профиль — создается системным администратором и хранится на сервере. При входе пользователя на любой компьютер в сети, он может использовать этот профиль и получить все стандартные настройки своего рабочего места, вне зависимости от того, с какого компьютера он вошел в сеть. Любые изменения перемещаемого профиля будут обновлены на сервере.
- обязательный профиль — является перемещаемым профилем, который не может быть изменен пользователем. Пользователь по-прежнему может настраивать свой рабочий стол и т.д., однако после выхода из системы эти изменения будут утеряны и следующий раз снова загрузится старый экземпляр профиля пользователя. Только системные администраторы могут вносить изменения в обязательный профиль.

Локальный профиль пользователя создается при первом сеансе работы пользователя за данным компьютером и хранится в папке "Documents and Settings\Имя пользователя". Перемещаемый профиль создается администратором. Создание перемещаемого профиля:

1) Создать на сервере папку (например, D:\Перемещаемые_профили) и через "Контекстное меню/Доступ" присвоить ей сетевое имя (например, Профили) и открыть к ней полный общий доступ для группы "пользователи домена" (кнопка "Разрешения").
2) Скопировать в эту папку локальный профиль пользователя с какого-либо компьютера в сети при помощи "Проводника", или меню "Пуск/Настройка/Панель управления/ Система/Двойной щелчок/ Профили пользователей/Выделить нужный профиль/Кнопка копировать/ Копировать профиль на" – указать сервер и каталог, куда будет скопирован профиль. Установить на скопированный каталог и подкаталоги разрешения "Полный доступ" только для данного пользователя и группы "администраторы" (Выделить каталог/Контекстное меню/Свойства/Безопасность).
3) В меню "Пуск/Настройка/Панель управления/Администрирование/Active Directory – пользователи и компьютеры/Выделить пользователя/Двойной щелчок/Профиль/Путь к профилю" указать путь к перемещаемому профилю. Необходимо указывать полный сетевой путь к файлам профиля (например, \\имя_сервера\Профили\имя_пользователя).

Обязательный профиль создается аналогично перемещаемому профилю за исключением того, что создается отдельный общий сетевой ресурс (например, Обязательные_профили), с доступом только "Чтение", а каталог с обязательным профилем должен носить расширение ".man" (например, \\имя_сервера\Обязательные_профили\имя_пользователя.man) и иметь для пользователя разрешения только "чтение и выполнение, список содержимого папки". Для администраторов сохраняются разрешения "полный доступ".

Примечание 1: Создать обязательный профиль можно и переименовав скрытый файл ntuser.dat, находящийся в основном каталоге профиля, в файл ntuser.man и установить на него разрешения "только чтение". Файл NTuser.dat отображает параметры реестра операционной системы Windows 2000.
Примечание 2: Операционная система Windows 2000 не поддерживает использование зашифрованных файлов совместно с перемещаемыми профилями. Файлы профиля не должны быть зашифрованы при помощи EFS.

Профили позволяют настроить параметры среды пользователя, однако не позволяют выполнить определенные ***действия*** (например, подключить сетевой диск). Для этих целей используют сценарии входа пользователя. Сценарий входа – это небольшая программа, которая запускается автоматически при входе пользователя на компьютер. Как правило, сценарий входа в систему представляет собой пакетный файл с расширением ".bat", однако допускается использование и любой исполняемой программы (расширение ".exe"), а также программ на языках JavaScript (расширение ".js") и программ на VBScript (расширение ".vbs"). Программы с расширениями js и vbs могут запускаться благодаря серверу сценариев Windows "Cscript.exe" (или "Wscript.exe").

В сценарии могут использоваться переменные среды. Ниже показаны примеры таких переменных, для использования в bat-файлах (в exe- js- и vbs- программах эти переменные также могут использоваться, однако синтаксис обращения к ним будет отличаться).

Таблица 5.2.

Некоторые переменные среды

Переменная*	Описание
%USERNAME%	Имя пользователя.
%USERPROFILE%	Профиль пользователя.
%HOMEPATH%	Полный путь к основному каталогу пользователя.
%USERDOMAIN%	Имя домена, содержащего учетную запись пользователя.
%HOMEDRIVE%	Имя диска на локальном компьютере пользователя, связанного с основным каталогом пользователя.
%OS%	Операционная система, используемая пользователем.
%SYSTEMROOT%	Корневой каталог Windows.
%COMSPEC%	Имя командного процессора.
%PATH%	Путь поиска выполняемых файлов.
%PATHEXT%	Расширения для поиска выполняемых файлов (com, exe).
%TEMP%	Каталог временных файлов.
%PROCESSOR_ARCHITECTURE%	Тип процессора рабочей станции пользователя (например 80386).
%PROCESSOR_LEVEL%	Уровень процессора рабочей станции пользователя. Например, для Pentium III это значение равно 6.
%PROCESSOR_IDENTIFIER%	Идентификатор процессора. Например x86 Family 6 Model 7 Stepping 3, GenuineIntel.

* Формат %имя_переменной% используется только в bat-файлах.

Пример сценария (файл scenario.bat):

```
@echo off
echo Доброе пожаловать %USERNAME% в домен %USERDOMAIN%
echo .
pause
```

Для создания сценария входа необходимо поместить файл сценария в каталог Scripts (обычно "C:\WINNT\SYSVOL\sysvol\имя_домена\scripts" (сетевое имя NETLOGON) или "C:\Winnt\System32\Repl\Import\Scripts", а затем в меню "Пуск/Настройка/Панель управления/Администрирование/Active Directory - пользователи и компьютеры/ Выделить пользователя/Двойной щелчок/Профиль/Сценарий входа" указать название файла сценария (например, scenario.bat). Если перед именем файла сценария указан относительный путь к файлу (например Admins\scenario.bat), то поиск файла проводится в указанном подкаталоге локального каталога сценариев.

5.6. Службы DNS, WINS, DHCP

Служба DNS отвечает за преобразование URL-адресов (типа www.microsoft.com) в IP-адреса. Сервер DNS интегрирован в Windows 2000, что позволяет использовать в локальной сети тот же формат имен компьютеров, принтеров и др. ресурсов, что и в Интернет. В результате исчезает разница между локальной сетью и Интернет. Например, набрав URL-адрес принтера, пользователь может обратиться к сетевому принтеру локальной сети также, как бы он обратился к любому ресурсу в Интернет. Настройка сервера DNS осуществляется посредством меню Пуск/Настройка/Панель управления/Администрирование/DNS.

Служба WINS использует централизованную базу данных для установления соответствия между NetBIOS-именами и IP-адресами в сети (напомним, что "Сетевое окружение" в ОС Windows использует именно протокол NetBIOS). Настройка сервера осуществляется через меню Пуск/Настройка/ Панель управления/Администрирование/WINS.

Служба DHCP (Dynamic Host Configuration Protocol) используется для динамической настройки IP-адресов компьютеров сети. Каждый компьютер, работающий в сети на основе протокола TCP/IP, должен иметь уникальный IP-адрес. Если быть более точным, то IP-адрес получает не сам компьютер, а сетевые интерфейсы, которые установлены на компьютере. IP-адрес может быть статическим или динамическим. Статический IP-адрес назначается вручную, в меню Пуск/Настройка/Панель управления/Сеть и удаленный доступ к сети/Выбрать название сетевого подключения (сетевой интерфейс)/Контекстное меню/Свойства/ Общие/ Протокол Интернета TCP/IP /Свойства/ Использовать следующий IP-адрес. На этой же вкладке назначаются IP-адреса серверов DNS и WINS, маршрутизаторов. Однако в больших сетях, где состав сети часто изменяется, бывает неудобно назначать каждому компьютеру IP-адрес вручную. Во-первых, это отнимает время, а во-вторых, легко запутаться в большим количеством выданных IP-адресов. Также часто бывает, что в распоряжении предприятия (например, провайдера Интернет) имеется недостаточное количество IP-адресов, чтобы выделить каждому пользователю собственный IP-адрес, но (в связи с тем, что не все пользователи работают в сети одновременно) можно решить эту проблему, димнамически выделяя IP-адреса только тем пользователям, которые подключаются к сети в данный момент. Для динамического назначения IP-адресов используется служба DHCP. При подключении к сети компьютера пользователя, он посылает запрос на

DHCP-север (для этого на компьютере пользователя необходимо указать Мое сетевое окружение/Свойства/ Протокол TCP/IP /Свойства /Получить IP-адрес автоматически). DHCP-сервер ищет в своей базе свободный в данный момент IP-адрес, и передает его клиенту вместе с другими настройками сети (IP-адреса серверов DNS и WINS, маршрутизаторов и др.). Настройка DHCP-сервера происходит при помощи меню Пуск/Настройка/Панель управления/Администрирование/DHCP. При настройке указывают следующие сведения:

- Допустимые диапазоны IP-адресов для динамического назначения пользователям (пул адресов). Адреса, зарезервированные для ручного назначения. При помощи DHCP можно также постоянно назначать конкретному компьютеру (с определенным именем и MAC-адресом сетевой карты) один и тот же IP-адрес.
- Допустимые настройки сети (IP-адреса DNS и WINS серверов, маршрутизаторов).
- Продолжительность аренды, предоставляемой сервером. Аренда определяет промежуток времени, в течение которого назначенный IP-адрес может использоваться.

5.7. Маршрутизация и удаленный доступ

Меню Пуск/Настройка/Панель управления/Администрирование/Маршрутизация и удаленный доступ позволяет создать маршрутизатор локальной сети и сервер удаленного доступа к сети (RAS, Remote Access Server). Функции и принципы работы маршрутизатора, а также основные протоколы маршрутизации были рассмотрены ранее в лекциях. Сервер удаленного доступа позволяет организовать подключение удаленных пользователей к серверу (и, при желании, ко всей остальной сети) при помощи модема. Создание маршрутизатора и сервера удаленного доступа можно осуществить при помощи удобных мастеров (Выделить сервер / Контекстное меню/Настроить и включить маршрутизацию и удаленный доступ) или выбрать ручную настройку. Ниже приведен список некоторых задач и методы их решения.

Таблица 5.3.

Настройка маршрутизации и удаленного доступа

Задача	Решение
Просмотр или создание новых сетевых интерфейсов.	Выделить сервер / Интерфейсы маршрутизации.
Задание статических маршрутов вручную.	Выделить сервер/IP-маршрутизация/Статические маршруты/Контекстное меню/Новый статический маршрут
Задание протоколов маршрутизации.	Выделить сервер/IP-маршрутизация/Общие/Контекстное меню/Новый протокол маршрутизации. Можно воспользоваться протоколами RIPv2 и OSPF.
Задание приоритета использования маршрутной информации, поступающей из разных источников.	Если до одного и того же компьютера/сети в таблице маршрутизации существует несколько маршрутов, то они используются в следующем порядке: 1) статические маршруты, 2) маршруты, полученные по протоколу OSPF, 3) маршруты, полученные по протоколу RIP. Можно изменить приоритеты обработки маршрутной информации: Выделить сервер /IP-маршрутизация/Общие/Контекстное меню/ Свойства/Уровни предпочтений.
Отображение существующих маршрутов.	Выделить сервер/IP-маршрутизация/Статические маршруты/ Контекстное меню/ Отобразить таблицу IP-маршрутизации
Запрещение продвижения пакетов между сетевыми интерфейсами	Выделить сервер/Контекстное меню/Свойства/Вкладка "IP"/ Разрешить IP-маршрутизацию - снять флажок. Если компьютер используется как маршрутизатор локальной сети, то иногда запрещают продвижение пакетов между сетевыми интерфейсами, а доступ из одного сегмента сети в другой осуществляют при помощи прокси-сервисов, прослушивающих соответствующие порты (подробнее о прокси-серверах и их преимуществах, с точки зрения обеспечения безопасности, см. ранее в лекциях). Если компьютер используют в качестве сервера удаленного доступа, то запрет IP-маршрутизации позволит удаленным пользователям подключаться только к серверу, но не даст доступа к остальной сети.
Задание трансляции сетевых адресов (NAT)	Трансляция сетевых адресов NAT уже подробно рассматривалась ранее в лекциях и позволяет большому количеству компьютеров работать с Internet или другой сетью при помощи одного или нескольких IP-адресов. Использование NAT также позволяет скрывать структуру своей сети от внешней сети, т.к. для внешней сети вся внутренняя сеть будет представлена всего одним IP-адресом. Настройка NAT осуществляется через меню IP-маршрутизация/Общие/Контекстное меню/Новый протокол маршрутизации/NAT-преобразование сетевых адресов. После создания протокола NAT: IP-маршрутизация/NAT/Контекстное меню/Новый интерфейс/ Выбрать интерфейс, соответствующей внутренней сети и в диалоговом окне указать "Частный интерфейс, подключен к частной сети". Аналогично выбрать второй интерфейс, соответствующий внешней сети (например, Internet), и в диалоговом окне указать/Общий интерфейс, подключен к интернет, а также установить флажок "Преобразовать TCP/UDP заголовки" и на вкладке "Пул адресов" указать IP-адрес, которым ваша внутренняя сеть будет представлена во внешней сети. Можно указать

Продолжение табл. 5.3

Задача	Решение
	несколько адресов, или при помощи кнопки "Резервирование" указать, что конкретный IP-адрес внутренней сети , всегда будет заменяться в пакетах на конкретный IP-адрес внешней сети.
Создание IP-туннеля	При создании IP-туннеля между двумя компьютерами устанавливается логическое (а не физическое) соединение точка-точка. Если между компьютерами А и В существует IP-туннель, и пакет был направлен в этот туннель, то он помещается в дополнительный IP-пакет, в котором в качестве адреса назначения будет указан компьютер В. После поступления такого IP-пакета на компьютер В, из него извлекается первоначальный пакет и передается далее по сети, к которой подключен компьютер В. Обычно IP-туннель (интерфейс IP-в-IP) используется для перенаправления многоадресного IP-трафика из одной части сети в другую, через участок сети, в котором не поддерживается многоадресный IP-трафик. Создать IP-туннель можно следующим образом: "Интерфейсы маршрутизации/ Контекстное меню/Создать IP-туннель", а затем "IP-маршрутизация /Общие/ Контекстное меню/Новый интерфейс/ Выделить созданный ранее IP-туннель/ОК/в диалоговом окне задать локальный (компьютер А) и удаленный (компьютер В) IP-адрес. В том же диалоговом окне, на вкладке "Общие", можно установить фильтры на входящие и исходящие пакеты туннеля (фильтрация по IP-адресам, типам протоколов, портам).
Создание интерфейса вызова по требованию	Поясним на примере. Если известно, что доступ к сети 15.0.0.0 можно получить при помощи модема (адаптера ISDN, другого устройства), позвонив по тел. 555-00-15, а доступ к сети 17.0.0.0 можно получить при помощи модема, позвонив по тел. 555-00-17, то для автоматизации этого процесса можно создать два интерфейса вызова по требованию и добавить в таблицы маршрутизации записи, отправляющие пакеты до соответствующих сетей на эти интерфейсы. Тогда если на маршрутизатор попадет пакет до сети 15.0.0.0, то модем автоматически наберет номер 555-00-15, установит соединение с удаленным компьютером (маршрутизатором) и передаст пакет. В случае если появится пакет до сети 17.0.0.0, то соединение будет установлено по номеру 555-00-17. Настройка интерфейса вызова по требованию происходит следующим образом: Интерфейсы маршрутизации/ Контекстное меню/ Создать новый интерфейс вызова по требованию/Указать тел. и др. параметры. Затем: IP-маршрутизация/Статические маршруты/Контекстное меню/Новый статический маршрут/Выбрать созданный интерфейс вызова по требованию и указать IP-адрес и маску сети (компьютера) назначения. Может также понадобиться указать: "Выделить сервер/Контекстное меню/Свойства/Вкладка "Общие"/ Использовать компьютер как маршрутизатор локальной сети и вызова по требованию".
Настройка компьютера в качестве сервера удаленного доступа (RAS)	Выделить сервер/Контекстное меню/Свойства/Вкладка "Общие"/Использовать компьютер как сервер удаленного доступа – установить флажок. В том же диалоговом окне осуществляются и другие настройки: Вкладка "Безопасность" – указывается выбор между службами проверки подлинности и учета пользователей (служба Windows или служба Radius). Кнопка "Методы проверки подлинности" позволяет включить запрос пароля по схеме CHAP или PAP (подробнее см. ранее в лекциях, протокол PPP) или разрешить удаленное подключение без проверки пароля и имени пользователя. Вкладка "IP" – назначение IP-адресов для подключающихся пользователей: используя протокол DHCP или из статического пула адресов, задаваемого вручную на этой же вкладке (адреса DHCP, DNS и WINS серверов выбираются автоматически, см. выпадающий список "Адаптер"). В дополнение к этому, в политике безопасности удаленного доступа (см. ниже) указывается: назначает ли сервер IP-адрес клиенту, или клиент может сам запросить IP-адрес. Вкладка "PPP" – позволяет задавать объединение нескольких физических подключений (например, несколько модемов) в один логический канал, а также управлять пропускной способностью канала, создавая дополнительные подключения при необходимости. Помимо описанных выше процедур, необходимо также создать соответствующих пользователей (Пуск/Настройка/Панель управления/Администрирование/Active Directory – пользователи и компьютеры/Выделить подразделение/Создать/Пользователь), задать им пароли и разрешить для них "Входящие звонки" (Active Directory – пользователи и компьютеры/Выделить пользователя/Двойной щелчок/Входящие звонки).

Продолжение табл. 5.3

Задача	Решение
Настройка политики удаленного доступа	Создание политики – Выбрать сервер/Политика удаленного доступа/Контекстное меню/ Создать политику удаленного доступа. В уже созданной политике используя кнопку "Добавить", можно задать следующие условия, по которым пользователям будет разрешено/отказано в удаленном доступе: - номер телефона исходящего звонка, который набрал пользователь. - номер телефона входящего звонка. - используемые протоколы и тип службы, которые запрашивает пользователь. - IP-адрес пользователя. - время звонка пользователя. - группа пользователей, к которой принадлежит звонивший и др. Используя кнопку "Изменить профиль" можно настроить профиль подключаемого пользователя: - назначается ли сервером IP-адрес клиенту, или клиент может сам запросить IP-адрес. - задать фильтр пакетов (межсетевой экран, firewall) для данного подключения, ограничивающий прохождение пакетов от клиентов и к клиенту, в зависимости от типа протокола и номера портов. - ограничить максимальную продолжительность и время звонков. - определить методы проверки подлинности и шифрования и др.
Настройка ведения журналов событий удаленного доступа и маршрутизации	Для настройки регистрации всех событий, связанных с удаленным доступом и маршрутизацией следует выбрать меню "Выделить сервер/Контекстное меню/Свойства/Журнал событий" – позволяет указать условия записи событий сервера, связанных с маршрутизацией и удаленным доступом (записывать только ошибки/ошибки и предупреждения/все события/отключить запись). Для настройки ведения журнала удаленного доступа необходимо воспользоваться меню "Выбрать сервер/Ведение журнала удаленного доступа" – позволяет настроить размеры, местоположение, формат файла журнала удаленного доступа и уровень детализации ведения журнала.

5.8. Диспетчер служб Интернета IIS (Internet Information Services).

Internet Information Services (Пуск/Настройка/Панель управления/Администрирование/Диспетчер служб Интернета) позволяет настраивать и администрировать web-, ftp-, smtp- и nntp- (группы новостей) сервисы на машине. Из-за постоянных проблем с безопасностью рекомендуется не использовать IIS и даже не устанавливать его на компьютер (например, в качестве web-сервера лучше использовать Apache).

Создать Web-сервер можно следующим образом: Выделить сервер/Контекстное меню/Создать/Узел Web/Отвечать на вопросы мастера: указать имя узла, IP-адрес (содержимое Web-узла или отдельные каталоги могут находиться как на данном сервере, так и на других компьютерах в сети), порт, каталог, разрешения (чтение, запуск сценариев, выполнение CGI-приложений, запись, обзор). Аналогично создается узел ftp, виртуальный почтовый сервер SMTP и виртуальный сервер новостей SMTP.

Настройка сервисов осуществляется следующим образом: "Выделить Web-узел (ftp, smtp, nntp)/ Контекстное меню/Свойства/". Можно устанавливать домашний каталог сервиса и определить разрешения для него (чтение, запись, обзор каталога, доступ к тексту сценария, запись в журнал, индексация каталога), запретить доступ к web(ftp)-узлу с определенных IP- или URL-адресов, устанавливать времени отключения не отвечающего пользователя, предельное число подключенных пользователей, вести журнал подключений, разрешать или запрещать анонимное подключение, просматривать текущие подключения к серверу, настроить вид html-страниц, возвращаемых пользователю при возникновении ошибок, название html-страницы, отображаемой по умолчанию и т.д. В меню "Выделить сервер/Свойства" можно ограничить полосу пропускания для всех web- и ftp-узлов данного компьютера, ограничив нагрузку на сеть, например величиной 1024 Кбит/с.

Особенностью IIS является поддержка активных серверных страниц (Active Server Pages, ASP). ASP позволяет динамически формировать HTML-страницы. ASP-файл представляет из себя документ HTML, в текст которого включены команды сценария ASP. Перед выдачей ASP-файла клиенту web-сервер обрабатывает команды ASP-сценария и динамически формирует HTML-страницу. Языком написания ASP-сценариев является VBScript (хотя могут использоваться языки JavaScript и Perl). Команды ASP-сценария встраиваются в HTML-страницу при помощи тэгов <Script> </Script> или <% %>. Отличием ASP-сценариев от обычных сценариев на языке VBScript/JavaScript является то, что если обычные сценарии выполняются на стороне клиента, то команды ASP-сценария выполняются на стороне сервера и пользователь получает "готовый" HTML-документ без всяких тэгов <Script> </Script> (только если сам ASP-сценарий не сформировал новые тэги <Script>). То, что ASP-сценарий выполняется на стороне сервера значительно расширяет его возможности. Так, например, в HTML-страницу могут быть динамически вставлены сведенья

из базы данных, хранящейся тут же на сервере. Раньше (и до сих пор, на всех Unix/Linux системах) для динамического формирования HTML-страниц использовались CGI-программы – программы на языках C, Perl и др., удовлетворяющих Общему Шлюзовому Интерфейсу (Common Gateway Interface, CGI). ASP-сценарии призваны заменить CGI-программы и упростить создание динамических HTML-страниц. Однако из-за низкой популярности IIS и Windows 2000, в качестве сервера Internet, ASP-скрипты пока не получили столь же широкое распространение, как CGI-программы.

Примечание: если на компьютере установлен IIS 5.0, то достаточно полную справку по IIS и ASP можно получить, набрав в браузере Internet Explorer адрес http://localhost/iisHelp/iis/misc/default.asp. (как следует из адреса, подключение к Internet для этого не требуется :).

5.9. Служба Telnet.

Служба Telnet позволяет организовать подключение пользователей к серверу по протоколу Telnet. Telnet – это фактически протокол эмуляции терминала: каждый символ, введенный пользователем на своем компьютере, будет считаться символом, введенным на сервере. При подключении к серверу Telnet запускается оболочка – специальная программа, которой и будут передаваться нажатия клавиш пользователя. По умолчанию это программа вида C:\WINNT\System32\cmd.exe – командная строка. Используя командную строку, можно отдавать серверу стандартные команды, типа dir, cd, copy и т.д. В качестве оболочки можно использовать не только командную строку, но и любую другую программу, в том числе, написанную самостоятельно. Общим здесь остается только одно: все нажатия клавиш пользователя будут переданы оболочке.

Настройка службы Telnet осуществляется Пуск/Настройка/Панель управления/Администрирование/Управление сервером Telnet. Управление осуществляется посредством текстового меню, которое позволяет вывести список текущих пользователей, прервать сеанс пользователя, запустить/остановить службу Telnet и изменить ее конфигурацию (см. табл. 5.4).

Таблица 5.4.

Параметры сервера Telnet.

№	Название	Описание и допустимые значения	Стандартно
1	AllowTrusted Domain	0: Разрешен доступ только для локальных пользователей. 1: Разрешен доступ пользователям из доменов с доверительными отношениями.	1
2	AltKey Mapping	0: Ctrl-A воспринимается как Ctrl-A (работает только для VT100). 1: Ctrl-A воспринимается как Alt (работает только для VT100).	1
3	Default Domain	Домен по умолчанию. Можно указать любой домен с доверительными отношениями. Локальный домен обозначается символом "." (точка).	
4	DefaultShell	Задает оболочку. По умолчанию: %systemroot%\System32\Cmd.exe /q /k	
5	LogonScript	Задает путь к расположению сценария входа на сервер Telnet. Администратор может настроить сценарий входа на выполнение определенных функций для каждого пользователя. По умолчанию: %systemroot%\System32\login.cmd	
6	MaxFailed Logins	Задает максимальное число неудачных попыток входа в систему перед завершением подключения.	3
7	NTLM	0: Стандартная проверка подлинности пользователя. Имя пользователя и пароль передаются в открытом виде. По соображениям безопасности не рекомендуется использовать параметры 0 и 1, однако в таком случае может возникнуть проблема совместимости с клиентами Telnet других операционных систем. В таком случае лучше вообще отказаться от использования Telnet. 1: Сначала предпринимается попытка выполнить проверку подлинности NTLM. При сбое используется стандартная проверка (имя пользователя и пароль). 2: Используется только проверка подлинности NTLM. Работает только между компьютерам, работающими под управлением Windows NT или Windows 2000. Подробнее о NTLM см. в разделе "Система безопасности Windows 2000".	2
8	TelnetPort	Задает порт, на котором работает служба Telnet.	23

5.10. Диспетчер службы терминалов

Несколько пользователей сети, с удаленных компьютеров, могут одновременно подключиться к программам Windows, работающим на сервере, используя службу терминалов. При помощи оснастки "Пуск/Настройка/Панель управления/Администрирование/Создатель клиента службы терминалов" администратор создает установочные дискетты (2 для Windows 9x, 4 для Windows 3.11) и обходит с ними соответсвующие компьютеры, устанавливая и настраивая клиента. После установки клиента, пользователи могут работать на своих компьютерах так, как будто бы они сидели за клавиатурой сервера: все нажатия клавиш и движения мыши передаются на сервер, программы выполняются на сервере, используя его ресурсы, а пользователям передается соответствующее изображение экрана монитора, которое и отображается на компьютере пользователя. Такая схема позволяет съэкономить средства: компьютеры пользователей могут не модернизироваться

– все равно они будут использоваться только как терминал (монитор и клавиатура), а все программы будут реально выполняться на сервере. Это позволяет добиться большой "скорости работы" даже на 486-х компьютерах с 32 Мб памяти, при условии, что вы не съэкономили на оперативной памяти сервера. Для стандартных "офисных" программ необходимо минимум 100Мб для самой Windows 2000 плюс по 20Мб на каждого клиента. При использовании графических и "ресурсоемких" приложений, объем памяти необходимо скорректировать в большую сторону.

Диспетчер службы терминалов ("Пуск/Настройка/ Панель управления/Администрирование/ Диспетчер службы терминалов") обеспечивает настройку терминала Windows 2000 Server, позволяет вывести список пользователей подключившихся через терминалы, подключить или отключить пользователя, отправить ему сообщение.

Единственное неудобство при работе с терминальным сервером – это лицензирование. Перед использованием терминального сервера необходимо активизировать "Лицензирование службы терминалов" и проинсталировать купленные лицензии (в виде дискеты или серийного номера). При подключении клиента, сервер терминальных лицензий проверяет, есть ли у клиента лицензия на подключение (Windows 2000 Professional всегда имеет встроенную лицензию). Если лицензии нет то сервер проверяет, есть ли у него в банке свободные еще не розданные лицензии. Если свободная лицензия есть то она автоматически выдается этому клиенту, причем лицензия выдается на конкретную машину и уже не может быть самостоятельно возвращена в банк или передана другой машине, а при переустановке Windows лицензия теряется. Если лицензии кончились то клиенту выдается временная лицензия на 90 дней, после чего терминальный клиент перестает работать. Это неудобно, однако легко обходится либо установкой на сервере фиксированной даты (используется редко и как временная мера), либо удалением каждые 89 дней у клиентов всего содержимого реестра по адресу: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\MSLicensing , после чего клиент получает новую лицензию на 90 дней. Последний способ является нарушением авторских прав корпорации Microsoft и не может использоваться в коммерческих целях.

5.11. Управление компьютером.

Меню "Пуск/Настройка/Панель управления/Администрирование/Управление компьютером" позволяет управлять локальным компьютером или другим компьютером в сети ("Управление компьютером/Контекстное меню/Подключиться к другому компьютеру"), при условии, что на нем установлена Windows 2000/NT и удаленное управление разрешено. При помощи команды "Управление компьютером/Контекстное меню/ Свойства/Дополнительно/Загрузка и восстановление" можно установить операционную систему загружаемую по умолчанию (если на компьютере установлена не только Windows 2000) и время, которое отображается меню выбора операционной системы. Другие команды меню кратко обобщены ниже.

Таблица 5.5.

Меню "Управление компьютером"

Раздел / подраздел	Пояснения
Раздел "Служебные программы"	
Просмотр событий	Позволяет просмотреть журналы событий системы (эта команда также доступна через меню Пуск/Настройка/Панель управления/Администрирование/Просмотр событий). Журналы событий подробнее будут рассмотрены в разделе "Система безопасности Windows 2000".
Сведения о системе	Позволяет просмотреть детальные сведения о системе, включая характеристики оборудования и установленного программного обеспечения.
Оповещения и журналы производительности	Позволяет настраивать средства наблюдения за производительностью системы.
Общие папки	Позволяет просмотреть общие ресурсы (диски/каталоги), доступные для сетевых пользователей, просмотреть/отключить текущие сеансы (подключившихся пользователей), просмотреть/принудительно закрыть все открытые по сети файлы.
Диспетчер устройств	Позволяет просматривать/отключать/включать/настраивать устройства компьютера (сетевые карты, модемы, мониторы, контролеры жестких дисков и т.д.). Именно здесь можно сменить драйверы устройств или устранить конфликты в распределении ресурсов системы между устройствами
Локальные пользователи и группы	Позволяет создавать пользователей/группы пользователей на локальном компьютере. Если на компьютере установлена служба каталогов Active Directory, то эта команда недоступна, а управление осуществляется через меню Active Directory – пользователи и компьютеры.
Раздел "Запоминающие устройства"	Позволяет управлять жесткими дисками (подробнее см. NTFS) и съемными носителями.

Продолжение табл. 5.5.

Раздел / подраздел	Пояснения
Раздел "Службы и приложения / Службы"	Позволяет отобразить запущенные на компьютере службы, просмотреть зависимости между службами, а также настроить режим их запуска (автоматически, вручную, отключено), определить учетную запись пользователя, от имени которой работает служба, определить поведение службы при первом, втором и последующих сбоях (ничего не делать, перезапустить службу, запустить определенную программу, перезагрузить компьютер). Доступ к настройке служб осуществляется через меню "Управление компьютером/Службы и приложения/Выделить службу/Свойства". Меню "Службы" также доступно через "Пуск/Настройка/Панель управления/ Администрирование/Службы".

5.12. Система безопасности Windows 2000

5.12.1. Пользователи и группы пользователей, права доступа, аудит.

Используя понятие "пользователь" и "группа пользователей" Windows 2000 позволяет реализовать достаточно мощную систему разграничения прав доступа. В Windows 95/98 запрос имени и пароля пользователя использовался только при работе в сети. При локальном входе на компьютер (без подключения к сети) пароль не требовался и любой человек мог изменить/ удалить любой файл, запустить/остановить любую программу, заразить компьютер вирусом и т.д. В Windows 2000 такое невозможно: при входе в систему пользователь в обязательном порядке указывает свое имя и пароль. Если имя и пароль верны, то пользователь входит в систему и получает строго ограниченный набор прав. Он может выполнять только те действия, которые разрешил ему администратор. При этом можно настроить аудит – регистрацию обращений пользователей к тем или иным объектам (файлы, принтеры и т.д.).

Создание пользователя осуществляется при помощи меню "Пуск/Настройка/Панель управления/ Администрирование/Active Directory – пользователи и компьютеры" (если Active Directory не установлена, то управление осуществляется через "Пуск/Настройка/Панель управления/Администрирование/Управление компьютером/Служебные программы/Локальные пользователи и группы"). Для создания пользователя необходимо выделить то подразделение, где он будет создан (или папку Users) и дать команду "Контекстное меню/Создать/Пользователь". Группа пользователей создается при помощи команды " Контекстное меню/ Создать/Группа". Группы используются для более удобного управления правами доступа – нет необходимости вручную определять права доступа для каждого члена группы. Права определяются в целом на группу, а члены группы получают эти права автоматически. Например, если какие-либо файлы доступны группе "Служба сбыта", то достаточно поместить сотрудника в эту группу, и файлы станут автоматически доступны и ему. Один и тот же сотрудник может быть членом в нескольких группах. Для того, чтобы изменить членство в группах необходимо воспользоваться командой "Выделить пользователя/Двойной щелчок/Член групп/Добавить". В этом же диалоговом окне, на вкладке "Учетная запись", можно запретить смену пароля пользователем, указать срок действия пароля, ограничить время входа пользователя и др. Вкладка "Среда" позволяет запустить определенную программу при входе пользователя в систему. Вкладка "Входящие звонки" позволяет разрешить/запретить входящие звонки от имени этого пользователя, определить номер, по которому перезвонит сервер удаленного доступа, при попытке пользователя подключиться к нему. Другие вкладки позволяют разрешить удаленное управление сеансом пользователя, указать адрес пользователя, номер телефона и пейджера, определить перемещаемый профиль пользователя, сценарии входа пользователя в систему и др.

Добавление пользователя в группу можно осуществить и другим способом: "Выделить группу/ Двойной щелчок/Члены группы/Добавить" (на этой же вкладке удобно просматривать список пользователей, входящих в данную группу). Можно сделать саму группу членом другой группы: "Выделить группу/ Двойной щелчок/Член групп/Добавить". Для быстрого добавления большого количества пользователей в группу можно воспользоваться командой "Выделить пользователей или подразделения/Контекстное меню/Добавить участников в группу".

Смена пароля пользователя может быть осуществлена, как самим пользователем ("CTRL-ALT-DELETE / Смена пароля"), так и администратором ("Выделить пользователя/Контекстное меню/Смена пароля"). Для того, чтобы временно отключить учетную запись (имя – пароль) пользователя, необходимо воспользоваться командой "Выделить пользователя/Контекстное меню/Отключить учетную запись". Для того, чтобы переместить пользователя в новое подразделение, необходимо воспользоваться командой "Выделить пользователя/Контекстное меню/Переместить". Подразделение – это аналог отдела предприятия, способ объединения пользователей и групп пользователей, со сходными требованиями к политике безопасности (например, подразделение "Бухгалтерия"). Для того, чтобы создать подразделение необходимо воспользоваться командой "Выделить имя домена/Контекстное меню/Создать/Подразделение". В рамках подразделения можно создавать пользователей и группы пользователей. Можно создавать подразделения, вложенные в другие подразделения. Для подразделения можно задать групповую политику безопасности "Выделить подразделение/Контекстное меню/Свойства/Групповая политика/Создать" (подробнее групповая и другие политики безопасности будут рассмотрены в разделе "Политики безопасности Windows 2000").

Каждое имя пользователя/группы связывается с уникальным идентификатором пользователя/группы (например, S-1-2-34-56789012345-67890123456-7890123456-7890). Разграничение доступа и система аудита в Windows 2000 использует уникальные идентификаторы для назначения прав доступа и контроля доступа к разным объектам (файлы, принтеры и т.д.). При этом администраторы работают по прежнему с понятными именами пользователей, а уникальные идентификаторы используются только внутри самой Windows 2000. Невозможно в рамках одной лекции полностью описать всю систему разграничения доступа Windows 2000, поэтому приведем лишь несколько примеров разграничения доступа на основании имен пользователей/групп пользователей:

1) Для ограничения доступа к файлу/каталогу достаточно воспользоваться командой "Выделить файл (каталог)/Контекстное меню/Свойства/Безопасность" – указать пользователей/группы пользователей, имеющих доступ к данному файлу(каталогу), указать права этих пользователей. Нажав кнопки "Дополнительно" и "Показать/Изменить" на этой же вкладке, можно перейти к расширенному управлению правами доступа. В этом же диалоговом окне, на вкладке "Аудит", можно задать аудит (контроль) действий пользователя по доступу к этому файлу/каталогу. Можно настроить запись в специальный журнал (Пуск/Панель управления/ Администрирование/Просмотр событий/Журнал безопасности) успех или неудачу при попытке получить доступ к файлу (каталогу). Регистрация успешных попыток позволяет следить за разрешенной деятельностью пользователей, регистрация неудачных попыток – выявить попытки нарушения прав доступа.

2) Для ограничения доступа к различным разделам реестра, необходимо воспользоваться программой regedt32 (Пуск/Выполнить/regedt32).

3) Политики безопасности (см. ниже) могут запретить пользователю локальный вход на конкретный компьютер или/и доступ к конкретному компьютеру по сети. Соответствующие параметры политик называются "Локальный вход в систему" и "Отказ в доступе к компьютеру из сети" и доступны через меню "Пуск/Настройка/Панель управления/Администрирование/ Локальная политика безопасности/Параметры безопасности/Локальные политики/Назначение прав пользователя" (см. также политику безопасности домена, контролера домена, групповые политики – подробнее далее в лекциях).

5.12.2. Домены в Windows 2000, доверительные отношения между доменами, аутентификация пользователя (протоколы Kerberos и NTLM).

В Windows 2000 вся сеть подразделяется на домены. Домен - это семейство компьютеров, объединенных по некоторому признаку (например, домен "Бухгалтерия", домен "Маркетинг). Домен создается при установке Active Directory на сервер - контролер домена ("Пуск/Настройка/Панель управления/Администрирование/Настройка сервера/Active Directory"). В каждом домене свой набор рабочих групп и список пользователей. Домены имеют древовидную структуру, могут иметь подчиненные домены и подразделения.

В каждом домене назначается свой администратор. Администратор домена имеет право устанавливать права доступа только в своем домене. Таким образом, административные права не сконцентрированы в одних руках одного пользователя (как, например, root в Unix/Linux системах), а распределены между администраторами доменов, каждый из которых отвечает только за свою область. В рамках своего домена, администратор, путем установки дополнительных разрешений, может делегировать отдельным пользователям часть прав по администрированию домена, снимая с себя лишнюю работу. Например отдельному пользователю/группе пользователей можно делегировать следующие права по управлению подразделением "бухгалтерия": чтение всей информации о пользователе, создание, удаление и изменение информации в учетных записях пользователей (групп пользователей), изменение членства пользователя в группах, смена паролей пользователей, применение к подразделению той или иной групповой политики. Для этого достаточно отдать команду "Пуск/Панель управления/Администрирование/Active Directory – пользователи и компьютеры/ Выделить подразделение/Контекстное меню/Делегирование управления". Аналогично выполняется делегирование управление и для других объектов Active Directory: домена, стандартных пользователей (папка "Users"), компьютеров (папка "Computers") и контролеров домена ("Domain controlers").

Между доменами могут устанавливаться доверительные отношения ("Пуск/Панель управления/Администрирование/Active Directory – домены и доверие/Выделить домен/ Контекстное меню/ Свойства/Доверия"). Доверительные отношения означают, что если пользователь прошел регистрацию в домене "Бухгалтерия" (правильно ввел имя и пароль), и между доменом "Бухгалтерия" и доменом "Маркетинг" есть доверительные отношения, то пользователь может получить доступ к компьютерам домена "Маркетинг", не проходя там повторную регистрацию. Необходимо отметить, что пользователь домена "Бухгалтерия" даже не имеет в домене "Маркетинг" учетной записи (имя-пароль) и тем не менее может получить доступ к компьютерам "Маркетинга", естественно, в пределах прав, которые администратор домена "Маркетинг" установит для "людей из бухгалтерии". Доверительные отношения между доменами могут быть двусторонними (если А доверяет В, то и В доверяет А) или односторонними (если А доверяет В, то это не означает, что В доверяет А). Двусторонние доверительные отношения являются транзитивными, т.е. если А доверяет В и В доверяет С, то и А доверяет С. Однако в любом случае, взаимодействие доменов в доверительных отношениях происходят только по криптографически защищенным протоколам Kerberos или NTLM, во избежание подмены злоумышленником одной из сторон доверительного взаимодействия.

Протоколы Kerberos и NTLM используются для аутентификации (подтверждении личности) пользователя. Протокол NTLM использовался еще в Windows NT 4.0, а протокол Kerberos появился в Windows 2000. Ниже кратко приведены сведения по этим протоколам:

- **протокол Kerberos V5** – специальный протокол, который подтверждает подлинность как пользователя, так и сетевых служб. Механизм таков: пользователь входит в сеть, введя свой пароль (система challenge-response) или используя смарт-карту. При правильности введенных данных Kerberos выдает пользователю "билет пользователя" (TGT) на все время нахождения в сети. Имея "билет пользователя", пользователь в любое время может обратиться к Kerberos, для получения "билета службы" (TGS - например, билет для почтовой службы или билет для доверенного домена "Маркетинг"), который во-первых подтверждает для службы подлинность пользователя (содержит зашифрованные данные о пользователе), а во-вторых подтверждает для пользователя подлинность службы, т.к. только подлинная служба (криптографически стойко подключенная к центру распространения ключей шифрования Kerberos) сможет правильно обработать зашифрованный "билет службы" и правильно ответить пользователю. Для самого пользователя весь этот процесс протекает абсолютно прозрачно: он только вводит свое имя и пароль при подключении к сети.
- **аутентификация NTLM** – используется для совместимости с предыдущей версией Windows NT 4.0. Система challenge-response: пользователь передает серверу свое имя, сервер возвращает пользователю случайное число, при помощи которого пользователь шифрует свой пароль (однонаправленная хэш-функция MD5) и возвращает его серверу, который имея в своей базе подлинный пароль пользователя, выполняет над ним туже операцию хэширования и сравнивает результат с пришедшим от пользователя. При совпадении – пользователь регистрируется. Такая методика позволяет избежать передачи пароля по сети в открытом виде. Причем каждый раз передается разное значение, перехват которого ничего не даст. Получить пароль по перехваченному хэш-значению, даже зная хэш-функцию – трудноразрешимая задача.

5.12.3. Политики безопасности Windows 2000

Windows 2000 позволяет использовать достаточно большое количество политик безопасности для централизованного управления доступом. Политика безопасности – это набор стандартных правил, применяемых к группе пользователей (подразделению, домену, компьютеру) и описывающая единые требования к безопасности. Ниже приведен краткий обзор политик безопасности Windows 2000.

Таблица 5.6.

Виды политик безопасности

Политики	Область действия	Пункт меню
Политика безопасности контролера домена.	Определяет политику безопасности компьютера, являющегося контролером домена.	Пуск/Настройка/Панель управления /Администрирование/ Политика безопасности контролера домена
Политика безопасности домена.	Определяет общие установки политики безопасности всех компьютеров, входящих в домен.	Пуск/Настройка/Панель управления /Администрирование/Политика безопасности домена
Локальная политика безопасности.	Позволяет переопределить общие установки политики безопасности домена для конкретного локального компьютера.	Пуск/Настройка/Панель управления /Администрирование/Локальная политика безопасности
Групповая политика безопасности подразделения.	Позволяет определить установки политики безопасности для подразделения. Подразделение – это способ объединения пользователей и групп пользователей, со сходными требованиями к политике безопасности. Например, подразделение "Бухгалтерия".	Шаг 1. Создать подразделение предприятия. Пуск/Настройка/Панель управления /Администрирование/ActiveDirectory пользователи и компьютеры / Контекстное меню / Создать / Подразделение Шаг 2. Задать групповую политику для подразделения. Выбрать нужное подразделение / Контекстное меню / Свойства/ Групповая политика / Создать *для ссылки на уже ранее описанную групповую политику выбрать команду "Добавить".
Групповая политика безопасности домена.	Позволяет определить большое количество установок политики безопасности для домена. Фактически "Политика безопасности домена" является подразделом "Конфигурация компьютера/Конфигурация Windows/Параметры безопасности" данной групповой политики.	Пуск/Настройка/Панель управления /Администрирование/ActiveDirectory пользователи и компьютеры / Выделить нужный домен/Контекстное меню/Свойства/ Групповая политика/Создать.

Политика удаленного доступа	Позволяет ограничить доступ удаленных пользователей к серверу, через модем (подробнее см. ранее, в разделе "Маршрутизация и удаленный доступ).	Пуск/Настройка/Панель управления /Администрирование/Маршрутизация и удаленный доступ к сети/ Выбрать сервер/Политика удаленного доступа.

Таблица 5.7.

Политика безопасности контролера домена, политика безопасности домена, локальная политика безопасности – раздел параметры безопасности

Название раздела	Примеры параметров, пояснения
Политики учетных записей	
1.Политика паролей	Максимальный (минимальный) срок действия пароля, минимальная длина пароля, требовать неповторяемость паролей (система помнит N последних паролей и запрещает использовать их).
2. Политика блокировки учетной записи	Блокировка учетной записи (на N минут в случае неверного ввода пароля), пороговое значение блокировки (максимально допустимое число раз неверного ввода пароля), сброс счетчика блокировки (счетчика неверно введенных паролей) через N минут.
3. Политика Kerberos	Максимальный срок жизни билета пользователя (билета службы). Билеты криптографически надежно удостоверяют подлинность пользователей и служб в домене. Подробнее о системе аутентификации Kerberos см. далее в лекциях.
Локальные политики	
1. Политика аудита	Параметры раздела включают (выключают) запись в журнал безопасности системы неуспешные (успешные) попытки входа в систему, доступа к объектам, доступа к службе каталогов, управления учетными записями пользователей, аудит изменения политики безопасности, аудит системных событий и отслеживания процессов.
2. Назначение прав пользователя	Определить пользователей (группы пользователей), которым разрешен (запрещен): доступ к компьютерам домена (данному компьютеру) из сети, локальный вход в систему непосредственно на этом компьютере, завершение работы компьютера, изменение системного времени, архивирование и восстановление файлов и каталогов, увеличение дисковых квот пользователям, управление аудитом и журналом безопасности, делегирование части административных функций другим пользователям, получение прав владельца объекта, добавление новых компьютеров к домену и др.
3. Параметры безопасности	Позволяет потребовать использование безопасного канала передачи данных в сети (шифрование и цифровая подпись), задать сообщение для пользователей при их входе в систему, отключить обязательное нажатие CTRL+ALT+DEL перед входом в систему (не рекомендуется по соображениям безопасности), запретить пользователям установку драйверов принтеров, определить поведение системы при установке неподписанных программ и драйверов, потребовать обязательную очистку файла виртуальной памяти при выключении системы, задать уровень проверки подлинности пользователей (для совместимости с NT 4.0), переименовать стандартную учетную запись гостя и администратора и др.
Журнал событий	
1. Настройка протоколирования*	Максимальный размер журнала безопасности или количество дней, в течении которых хранятся события в журнале. Ограничить доступ гостей к журналу.
Прочие	
1. Группы с ограниченным доступом*	Если занести группу пользователей в этот раздел, а затем двойным щелчком по группе открыть диалоговое окно и добавить пользователей в раздел “Члены этой группы”, то при перезагрузке системы и применении политики безопасности, только пользователи явно указанные посредством раздела "Группы с ограниченным доступом" будут сохранены в данной группе, остальные пользователи будут автоматически удалены из группы. Этот способ фактически дублирует обычные методы занесения пользователей в те или иные группы, однако здесь ключевым моментом является то, что этот способ интегрирован в политику безопасности и позволяет централизованно и наглядно проконтролировать членство в наиболее важных группах, со значительным объемом прав на систему (например, Администраторы).

Продолжение табл. 5.7.

Название раздела	Примеры параметров, пояснения
2. Системные службы*	Позволяет задавать ограничения на режим запуска (вручную/автоматически/ запрещено) системных служб, которые отвечают за определенные сервисы, например сервис Telnet. Определяет разрешения для определенных групп пользователей (пуск, остановка, запуск, удаление сервиса, смена/чтение разрешений, смена владельца, определение зависящих сервисов, опрос сервиса и т.д.), настроить аудит (для всех пользователей или отдельных групп пользователей можно задать какие действия – см. разрешения – будут записываться в журнал безопасности в случае их успеха/неуспеха).
3. Реестр*	Позволяет ограничить доступ к отдельным разделам реестра различным пользователям и группам пользователей. Также позволяет организовать аудит успешных/неуспешных действий по доступу к реестру для всех пользователей или отдельных пользователей и их групп.
4. Файловая система*	Позволяет ограничить доступ различных пользователей и групп пользователей к отдельным папкам и файлам. Также позволяет настроить аудит по результатам успешного/неуспешного доступа различных групп пользователей к отдельным папкам и файлам. Эти же операции можно выполнить и из "Проводника" (выбрать папку/файл, контекстное меню/свойства/Безопасность), однако данная настройка политики безопасности позволяет вести легко контролируемый единый список всех важных папок/файлов, а также позволяет запретить изменение разрешений и тогда только пользователи, имеющие право изменять политику безопасности, смогут изменить разрешения для этой папки.
5. Политики открытого ключа	Политика открытого ключа строится на основании асимметричных алгоритмов шифрования. Если в симметричных алгоритмах данные шифруются и дешифруются при помощи одного и того же ключа, то в асимметричных алгоритмах ключи создаются парами: закрытый ключ – открытый ключ. Данные, зашифрованные при помощи одного из этих ключей, не могут быть дешифрованы этим же ключом – для дешифровки необходим второй ключ. Такая схема позволяет организовать безопасное распространение ключей при котором нет необходимости скрывать открытый ключ: закрытый ключ остается у владельца, открытый – передается всем желающим. Любой человек может направить зашифрованное сообщение адресату, используя его открытый ключ. При этом другие пользователи, также имеющие открытый ключ адресата, не смогут прочитать сообщение, т.к. у них нет закрытого ключа. Более того, такая схема позволяет организовать цифровую подпись документов и программ: по тексту документа вычисляется необратимая хэш-функция (функция вида Y=f(X), в которой по значению Y нельзя получить значение X) и генерируется дайджест сообщения – обычно 128-битное число, результат вычисления хэш-функции. Если в тексте документа изменить хотя бы один бит, то его дайджест не совпадет с дайджестом, приложенным к документу. Чтобы приложенный к документу дайджест нельзя было подменить, он шифруется при помощи закрытого ключа отправителя. Любой человек, имеющий открытый ключ отправителя, может проверить корректность дайджеста, но только отправитель, имеющий закрытый ключ, может сформировать корректный дайджест. В Windows 2000 асимметричные алгоритмы реализованы посредством механизма сертификатов. Сертификаты — это своего рода электронные удостоверения пользователя (компьютера, службы), подписанные цифровой подписью центра сертификации, в которых указывается данные о пользователе (компьютере, службе), открытый ключ пользователя, дата начала и окончания действия сертификата. Сертификаты используются для проверки подлинности сервера/ клиента, защиты от изменений содержимого электронной почты или кода программ, установки криптографически защищенных штампов времени в документах, шифровании и восстановлении файлов шифрованной файловой системы EFS, шифровании IP-трафика и т.д. Управление центром сертификации осуществляется при помощи меню "Пуск/Настройка/Панель управления/ Администрирование/Центр сертификации". Настройка "Политики открытого ключа" позволяет указать доверенные центры сертификации и список доверенных сертификатов, указать параметры автоматического запроса сертификатов. Она также позволяет создать агента восстановления шифрованной файловой системы EFS - пользователя, который может расшифровывать зашифрованные файлы других пользователей.

Продолжение табл. 5.7.

Название раздела	Примеры параметров, пояснения
6. Политики безопасности IP	Позволяет задать параметры безопасности для IP-соединений: разрешить соединение, запретить соединение или потребовать определенный метод проверки личности пользователя (например, Kerberos), или алгоритм шифрования и проверки целостности данных и адресов IP-пакетов. Требования устанавливаются в зависимости от типа подключения (по локальной сети или через удаленный доступ), IP- или DNS-адресов, типа протокола, и портов компьютеров, участвующих в соединении. Фактически, настройка "Политики безопасности IP" реализуют простой, но достаточно гибкий межсетевой экран (firewall).

* - отсутствует в локальной политике безопасности.

Таблица 5.8.

Групповая политика безопасности (подразделения/домена)

Название раздела	Примеры параметров, пояснения
1. Конфигурация компьютера	
1.1.Конфигурация программ/ Установка программ	Позволяет автоматически установить необходимые программы всем пользователям в подразделении/домене. При этом на каждом конкретном компьютере программа только появляется в меню "Пуск" и реестре, а фактически устанавливается только в тот момент, когда пользователь в первый раз запускает программу.
1.2. Конфигурация Windows	
Сценарии (запуск, завершение)	Позволяет задать сценарии (exe-, bat-, vba-, js-файлы), выполняющиеся на компьютерах пользователей подразделения/домена (должна быть установлена Windows 2000) при запуске/выключении компьютера.
Параметры безопасности	Фактически представляет собой еще один способ обратиться к меню "Политика безопасности домена" (см. выше).
1.3. Административные шаблоны/Компоненты Windows	
NetMeeting	Позволяет запретить/разрешить пользователям подразделения/домена удаленное управление рабочим столом при помощи NetMeeting. Подробнее см. раздел "Конфигурация пользователя/Конфигурация Windows".
Internet Explorer	Позволяет установить общие для всех пользователей подразделения/домена настройки зон безопасности Internet Explorer и настройку разрешений зон безопасности (настройка зон безопасности и разрешений для этих зон выполняется в разделе "Конфигурация пользователя/Конфигурация Windows/Поддержка Internet Explorer). Пользователям будет запрещено самостоятельно изменять эти настройки. Можно также определить обязательные настройки использования прокси-сервера. Подробнее см. раздел "Конфигурация пользователя/Конфигурация Windows".
Планировщик заданий	Планировщик заданий отвечает за запуск по расписанию определенных программ. Можно запретить пользователям подразделения/домена просматривать/создавать /удалять задачи, останавливать запущенные задачи до их полного завершения и т.д.
Установщик Windows	Позволяет определить обязательные параметры установщика Windows (установка программ) или вообще запретить его использование пользователями подразделения/домена. В этом случае программное обеспечение смогут устанавливать только администраторы.
1.4. Административные шаблоны/Система	
для пользователей подразделения/домена позволяет определить список программ, запускающихся автоматически, при входе в систему, или вообще отключить автозапуск. Можно отключить автоматическое шифрование для файлов, перемещаемых в зашифрованные папки и др.	
Вход в систему	Для пользователей подразделения/домена можно задать синхронный запуск сценариев входа в систему (рабочий стол не будет создан, пока не будут выполнены все сценарии) и асинхронный/синхронный режим выполнения сценариев (все сценарии выполняются параллельно/последовательно). Можно также определить максимальное время выполнение сценариев и режим отображения команд сценария, принудительно завершать сеанс пользователя при ошибке в перемещаемом профиле.
Дисковые квоты	Позволяет настроить обязательные параметры использования дисковых квот для пользователей подразделения/домена. Пользователи, не имеющие право изменять политику безопасности, не смогут самостоятельно изменить эти параметры.
DNS-клиент	Позволяет принудительно определить основной DNS-суффикс для пользователей подразделения/домена.

Продолжение табл. 5.8.

Название раздела	Примеры параметров, пояснения
Групповая политика	Задает параметры использования групповой политики: интервал и режим обновления политики (применения новых параметров политики), асинхронное применение политики (ускоряет загрузку, однако возможно формирование рабочего стола еще до полного применения всех параметров политики) и др.
Защита файлов в Windows	Защита файлов Windows проверяет системные файлы Windows на наличие в них изменений. По умолчанию файлы сканируются только при установке программ. Использование этой политики позволяет задать сканирование системных файлов во время каждой загрузки системы.
1.5. Административные шаблоны/Сеть	
Автономные файлы	Windows 2000 позволяет кэшировать сетевые файлы на локальном компьютере для того, чтобы они были доступны даже при отключении сети. Данная политика разрешает/запрещает использование автономных файлов, а также настраивает параметры их использования.
Сеть и удаленный доступ к сети	Windows 2000 позволяет организовать для локальной сети общий доступ к удаленной сети (например, Internet) через одно модемное подключение. Данная политика позволяет запретить администраторам, не имеющим право изменять данную политику, настраивать общий доступ. Подробнее см. раздел "Конфигурация пользователя/ Административные шаблоны/Сеть/Сеть и удаленный доступ к сети".
1.6. Административные шаблоны/ Принтеры	Позволяет настроить режим публикации (объявления) и обзора (просмотра) сетевых принтеров и др. параметры.
2. Конфигурация пользователя	
2.1.Конфигурация программ/ Установка программ	Аналогично разделу 1.1. (см. выше). Параметры, указанные в разделе "Конфигурация пользователя", частично совпадают с параметрами, указанными в разделе "Конфигурация компьютера". В таком случае параметры раздела "Конфигурация компьютера" имеют более высокий приоритет. Однако стоит проверять разделы политик с совпадающими названиями, т.к. чаще всего содержимое этих разделов не дублирует, а дополняет друг-друга.
2.2. Конфигурация Windows	
Поддержка Internet Explorer	Позволяет задать для пользователей подразделения/домена внешний вид Internet Explorer (заголовки окна, фон и кнопки панели инструментов, содержимое меню "Избранное", адрес домашней страницы), параметры подключения к Internet (например, прокси-сервер), настройки зон безопасности и разрешений для этих зон и др. параметры.
Сценарии входа/ выхода из системы	Позволяет задать для пользователей подразделения/домена сценарии, выполняющиеся при входе/выходе пользователя из системы. Эти сценарии являются общими для всех пользователей подразделения/домена.
Параметры безопасности	Подраздел Политики открытого ключа/Доверительные отношения позволяет создать список доверия сертификатов для пользователей подразделения/ домена.
Службы удаленной установки	Позволяет настроить параметры установки для пользователей Подразделения/Домена: возможность выполнять выборочную установку, возможность автоматической установки, перезапуска установки и др. параметры.
Перенаправление папки	Позволяет задать для пользователей подразделения/домена расположение папок "Мои документы", "Главное меню", "Рабочий стол". Для различных пользователей/групп пользователей можно указать различное расположение, или указать общее расположение для всех пользователей.
2.3. Административные шаблоны / Компоненты Windows	
Net Meeting	Позволяет настроить обязательные для всех пользователей подразделения/домена параметры Net Meeting: запретить общий доступ к приложениям, командной строке, окнам проводника, рабочему столу, удаленное управление при помощи Net Meeting, скрыть страницы настройки, ограничить пропускную способность сети или вообще запретить передачу аудио- и видеоданных, запретить прием/передачу файлов, ограничить размер передаваемых файлов.
Internet Explorer	Позволяет полностью контролировать внешний вид Web-браузера Internet Explorer (содержимое меню, кнопки, вкладки, запретить изменение настроек языков, цветов, прокси-сервера и др.), ограничить максимальный размер получаемых файлов, ограничить использование Windows Media, ShockWave Flash и др. программ, связанных с Internet.

Продолжение табл. 5.8.

Название раздела	Примеры параметров, пояснения
Проводник	Позволяет для пользователей подразделения/домена полностью контролировать внешний вид Проводника: содержимое меню, кнопки, запретить контекстное меню, скрыть значки "Мои документы", значки "Вся сеть", скрыть вкладку "Оборудование", скрыть некоторые диски локального компьютера, скрыть кнопку "Поиск", скрыть команды подключения/ отключения сетевых дисков, команды и др.
Консоль управления Microsoft	Позволяет для пользователей подразделения/домена ограничить возможность запуска большинства меню конфигурирования Windows, в том числе из папки "Администрирование".
Планировщик заданий	Аналогично такому же разделу в "Конфигурации компьютера".
Установщик Windows	Аналогично такому же разделу в "Конфигурации компьютера".
2.4. Административные шаблоны / Панель задач и меню пуск	Позволяет для пользователей подразделения/домена настроить вид меню "Пуск" и панели задач: убрать из меню подменю "Документы", команды "Найти", "Выполнить", "Завершение работы", "Завершение сеанса", "Сеть и удаленный доступ к сети", запретить перетаскивание и контекстное меню в меню "Пуск" и на "Панели задач", запретить изменение параметров панели задач и меню "Пуск".
2.5. Административные шаблоны / Рабочий стол	Позволяет для пользователей подразделения/домена настроить вид рабочего стола: скрыть значки "Сетевое окружение", "Мои документы", запретить пользователям изменять положение папки "Мои документы", запретить изменение места положения панелей, скрыть все значки рабочего стола.
2.6. Административные шаблоны / Панель управления	
Установка и удаление программ	Позволяет для пользователей подразделения/домена запретить установку и удаление программ, скрыть некоторые пункты меню "Установка и удаление программ", запретить установку программ с CD-диска, дискет или по сети.
Экран	Позволяет для пользователей подразделения/домена запретить настройку экрана или отключить некоторые вкладки в меню настройки. Позволяет явно указать имя файла хранителя экрана для предотвращения проникновения в систему вредоносных программ через хранитель экрана (для этого необходимо не только указать имя файла-заставки, но и правильно выставить права доступа к этому файлу, чтобы пользователь не смог заместить его своим файлом, с таким же именем).
Принтеры	Позволяет запретить/разрешить установку или удаление принтеров, обзор принтеров по сети и др.
Язык и стандарты	Позволяет указать обязательный язык для меню и диалогов в Windows.
2.7. Административные шаблоны/Сеть	
Автономные файлы	Аналогично такому же разделу в "Конфигурации компьютера".
Сеть и удаленный доступ к сети	Для пользователей подразделения/домена позволяет ограничить доступ к настройке подключений по сети и удаленного доступа. Например, запретить дополнительную настройку TCP/IP (указание IP-адресов шлюзов, DNS и WINS серверов).
2.8. Административные шаблоны/Система	
для пользователей подразделения/домена позволяет скрыть средства редактирования реестра, запретить использование командной строки, выполнять только зарегистрированные приложения Windows, не запускать определенные программы (указывается список), отключить автозапуск или вообще задать особый интерфейс пользователя. По умолчанию запускается программа Explorer.exe, соответствующая стандартному интерфейсу Windows, но можно указать и собственную программу.	
Вход/выход из системы	Для пользователей подразделения/домена позволяет запускать указанные программы при входе в систему, запретить запуска диспетчера задач, блокировку компьютера, запретить изменение пароля, завершение сеанса и др.
Групповая политика	Задает параметры обновления групповой политики.