МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ
РОССИЙСКОЙ ФЕДЕРАЦИИ

Белгородский государственный технологический университет
им. В.Г. Шухова

Е. А. Федотов, А. В. Глухоедов

Сети электронно-вычислительных машин и средства коммуникаций

Утверждено ученым советом университета в качестве лабораторного практикума для студентов специальности 220501 – Управление качеством

Белгород
2013

УДК 004.45 (07)
ББК 32.973.26-018.2 я7
Ф34

Рецензенты:

Кандидат технических наук, доцент Белгородского государственного технологического университета им. В.Г. Шухова *В.Г. Синюк*

Кандидат технических наук, доцент Белгородского государственного национального исследовательского университета *В.М. Михелев*

Федотов, Е. А.
Ф34 Сети электронно-вычислительных машин и средства коммуникаций: лабораторный практикум / Е. А. Федотов, А. В. Глухоедов. – Белгород: Изд-во БГТУ, 2013. – 165 с.

В лабораторный практикум включены требования и рекомендации к выполнению лабораторных работ по дисциплине «Сети электронно-вычислительных машин и средства коммуникаций», а также задания для выполнения данных работ.

Лабораторный практикум предназначен для студентов 3-го курса специальности 220501 – Управление качеством.

Данное издание публикуется в авторской редакции.

УДК 004.45 (07)
ББК 32.973.26-018.2 я7

Оглавление

Лабораторная работа №1.....4

Знакомство с Windows XP Professional.....4

Лабораторная работа №2.....28

Знакомство с рабочими группами и доменами.....28

Лабораторная работа №3.....40

Утилиты диагностики компьютерных сетей.....40

Лабораторная работа №4.....46

Установка и настройка сетевых протоколов.....46

Лабораторная работа №5 69

IP адреса. Октеты. Маски подсетей.....69

Лабораторная работа № 6 90

Создание и управление учетными записями пользователей.....90

Лабораторная работа №7.....111

Обеспечение безопасности ресурсов с помощью разрешений NTFS.....111

Лабораторная работа №8.....139

Администрирование общих папок.....139

Библиографический список.....167

Лабораторная работа №1

Знакомство с Windows XP Professional

Цель работы: Получение навыков установки и настройки виртуальных машин. Использование виртуальных машин для инсталляции и запуска операционной системы Windows.

Порядок выполнения работы

1. Изучить теоретический материал.
2. Выполнить практические задания.
3. Сделать выводы на основании проделанной работы

Установка виртуальной машины на примере MS Virtual PC

Microsoft Virtual PC представляет собой программный пакет виртуализации для операционных систем семейства Windows, который позволяет эмулировать на одном компьютере работу сразу нескольких виртуальных машин. Каждая из таких машин может находиться под управлением своей собственной операционной системы (Windows любой версии, Netware, Linux, Solaris и т.д.), выполнять уникальную задачу, иметь собственную конфигурацию и т.д.

Продукт Virtual PC был создан компанией Connectix в 1997 году для операционной системы Mac OS на платформе PowerPC Macintosh. В 2001 году была выпущена версия 4.0 для ОС Windows. Connectix поставляла Virtual PC с различными гостевыми ОС, включая Linux и OS/2. В феврале 2003 года права на продукты Virtual PC и Virtual Server были куплены компанией Майкрософт. В июле 2006 года Майкрософт выпустила Windows-версию пакета для бесплатного использования.

Продукт Virtual PC предназначен для запуска одной или нескольких гостевых операционных систем на настольных системах, прост в использовании и ориентирован на неискушенных в компьютерных технологиях пользователей.

В новой версии продукта Virtual PC появились следующие основные возможности:

1. Оптимизация платформы под Windows Vista. На платформе Virtual PC 2004 также можно было установить Windows Vista, однако в новой версии продукта эта система работает гораздо быстрее и стабильней.

2. Увеличение быстродействия за счет использования улучшений, введенных в серверной платформе виртуализации Microsoft Virtual Server 2005 R2.

3. Поддержка 64-битных хостовых операционных систем Windows.

4. Поддержка звуковых устройств в гостевых системах Windows Vista.

Скачать последнюю версию программы Microsoft Virtual PC можно бесплатно на официальной станице продукта компании Microsoft. После запуска программы MS Virtual PC появляется New Virtual Machine Wizard - мастер создания новой виртуальной машины (рис. 1.1.). Чтобы приступить к созданию виртуальной машины, нажимаем «Next».

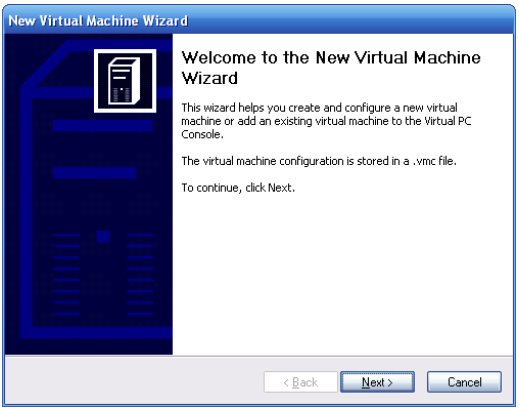


Рис. 1.1. Начальный этап создания виртуальной машины

В появившемся окне следует выбрать один из трех вариантов:

1. «Create a virtual machine» - создание новой виртуальной машины;

2. «Use default settings to create a virtual machine» - создание новой виртуальной машины с настройками по умолчанию;

3. «Add an existing virtual machine» - добавление существующей виртуальной машины (рис. 1.2.).

Для перехода к следующему шагу – «Next».

На следующем шаге следует указать место расположения и имя файла с настройками виртуальной машины (рис. 1.3.).

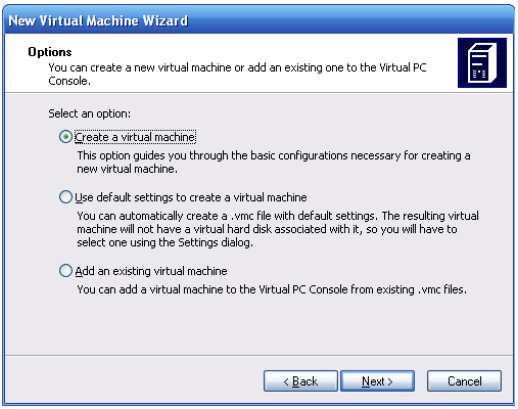


Рис. 1.2. Выбор варианта создания виртуальной машины

На диске, на котором будет храниться файл, должно быть достаточно места для установки гостевой ОС. Рекомендуется хранить файл с настройками виртуальной машины и виртуальный диск в одной директории.

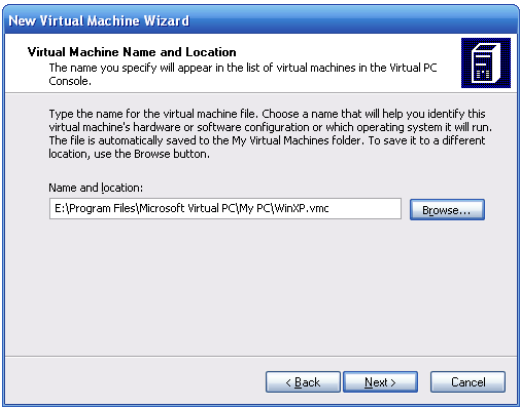


Рис. 1.3. Назначение места расположения и имени файла с конфигурацией виртуальной машины

Выбор типа гостевой операционной системы считается важным этапом, поскольку производительность системы напрямую зависит от типа гостевой ОС. Необходимо выбрать пункт «Other», если устанавливаемой ОС нет в списке «Operating system» (рис. 1.4.).

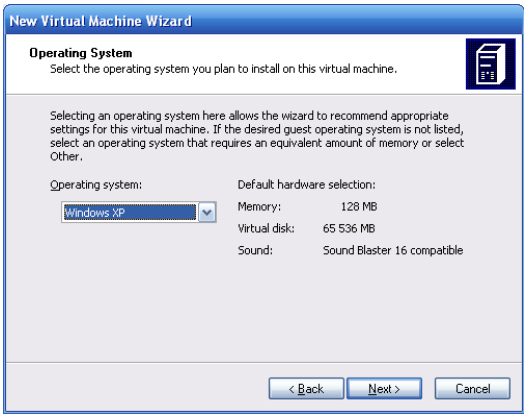


Рис. 1.4. Выбор типа гостевой операционной системы

Также можно выбрать объём оперативной памяти, который будет выделен гостевой системе. Доступны два варианта (рис. 1.5.):

1. «Using the recommended RAM» - память будет выделена по умолчанию.

2. «Adjusting the RAM» - необходимо вручную установить объём выделенной оперативной памяти с учетом минимальных требований устанавливаемой системы к объему RAM и а также объема физической памяти виртуальной машины.

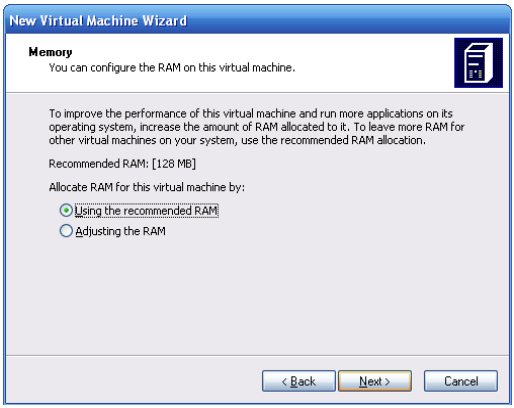


Рис. 1.5. Выбор объёма оперативной памяти

Далее необходимо выбрать, использовать ли уже имеющийся виртуальный жесткий диск («An existing virtual hard disk») или создать новый («A new virtual hard disk») (рис. 1.6.).

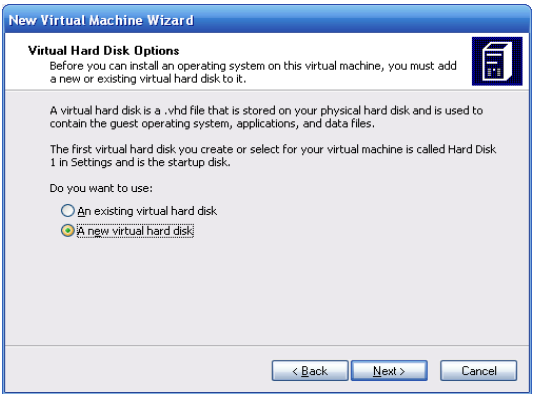


Рис. 1.6. Опции виртуального жёсткого диска

Следующий этап состоит в задании размера виртуального жесткого диска (рис. 1.7.). По умолчанию предлагается создать диск объемом 65536 Мб. Этой величиной определяется максимальный объем диска виртуальной машины, а сам файл будет расти по мере заполнения диска в виртуальной машине.

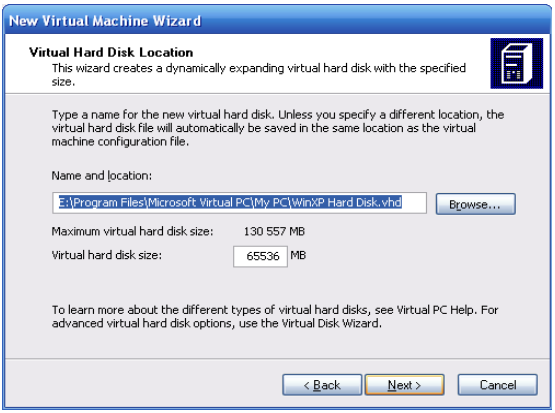


Рис. 1.7. Выбор размера виртуального жесткого диска

На завершающем этапе проверяем атрибуты виртуальной машины и, нажимаем «Finish» (рис. 1.8.). Виртуальная машина создана.

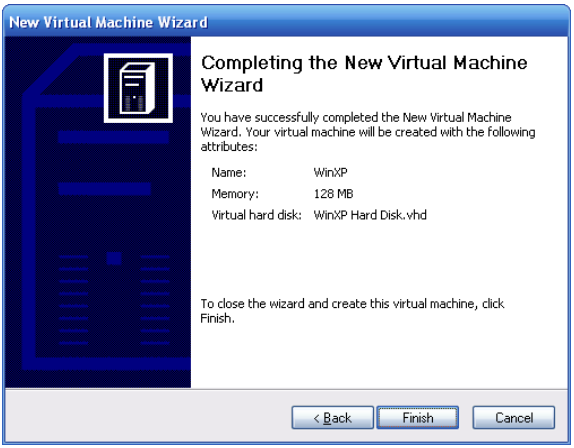


Рис. 1.8. Завершающий этап создания виртуальной машины

После нажатия кнопки «Finish» новая виртуальная машина появится в окне Virtual PC Console (рис. 1.9.):

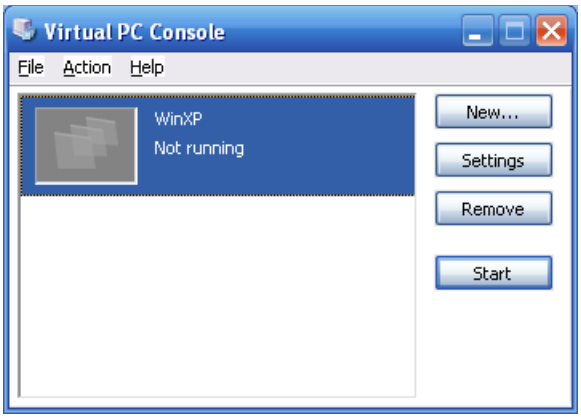


Рис. 1.9. Окно MS Virtual PC

Установка операционной системы в виртуальной машине

В главном окне программы, «Virtual PC Console», нажимаем кнопку «Start». Начнется загрузка виртуальной машины.

Далее необходимо определиться с расположением дистрибутива гостевой операционной системы. Возможные варианты. Если

дистрибутив находится на загрузочном CD или DVD диске, вставьте его в привод, так как с него по умолчанию пытается загрузиться виртуальная машина, после этого нажмите «Enter». Если дистрибутив операционной системы в виде загрузочного образа ISO, откройте меню CD консоли виртуальной машины, выберите пункт «Capture ISO Image» и укажите путь к образу. После этого начнется загрузка операционной системы (рис. 1.10).

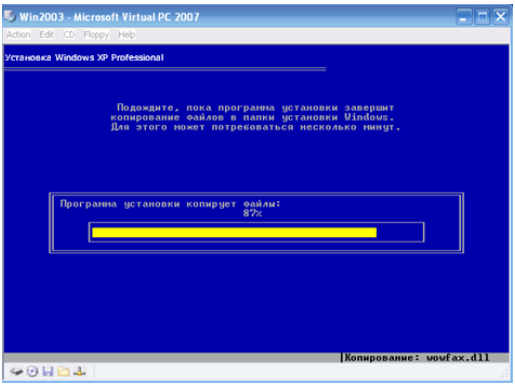


Рис. 1.10 Установка Windows XP Professional

Установка гостевой ОС производится аналогично установке на физическую машину. Виртуальная машина как бы «поглощает» указатель мыши, позволяя работать только внутри гостевой системы. Для выхода из режима захвата указателя мыши - правый Alt.

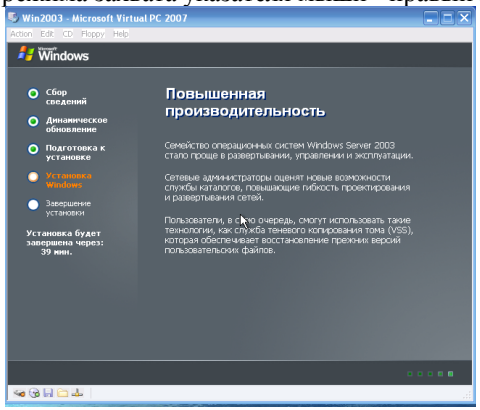


Рис. 1.11 Процесс установки ОС

Затем, как обычно, ожидайте окончания установки операционной системы (рис. 1.11).

Обзор новых возможностей и средств

В Windows XP существует возможность автоматического обновления (Automatic Update, AU). AU позволяет пользователям с правами администратора загружать из Интернета и устанавливать на компьютер обновления системы, такие, как исправления системы безопасности и исправления компонентов. В связи с тем, что подобная процедура иногда требует перезагрузки системы, перед началом установки вы получите соответствующее сообщение, кроме того, вам предоставляется возможность отложить загрузку обновлений. Загрузка выполняется в фоновом режиме, что позволит вам не отрываться от работы [8, 12].

AU использует алгоритмы Windows Update для сканирования системы на предмет необходимости обновления на конкретной машине. Для загрузки обновлений в AU применяется инновационная технология регулирования пропускной способности. При этом используется лишь свободная полоса пропускания, что не мешает и не тормозит другие сетевые процессы, например, работу браузера. В каждый момент времени только один пользователь с доступом администратора может пользоваться клиентом автоматического обновления.

Windows XP Professional дает пользователям возможность сохранить информацию, например фотографии и программное обеспечение, на CD, не прибегая к сторонним программам записи. Так как приводы CD-R и CD-RW из-за относительной дешевизны теперь устанавливают на большинстве компьютеров, эта функция системы расширяет набор стандартных средств Windows для удобства пользователей. Пользователи могут выбрать папку с цифровыми фотографиями, перетащить ее на значок CD-R и создать CD. Более того, теперь стало гораздо проще сохранять файлы, пользуясь CD, а не дискетой небольшого объема.

Кроме того, растут возможности производителей комплектующих (OEM) и независимых поставщиков программного обеспечения. Так,

производители комплектующих (OEM) могут создавать фирменные приложения для создания загрузочных CD вместо загрузочных дискет, а независимые поставщики программного обеспечения — встраивать функции записи CD в Windows - версии и своих программ.

Для копирования файлов или папок на CD следует выполнить следующие действия:

1. Вставьте пустой диск CD-R(W) в привод CD-R(W).
2. Щелкните Пуск, правой кнопкой мыши щелкните Мой компьютер, затем щелкните пункт меню Проводник и выберите файлы и папки, которые вы хотите записать на CD.
3. В группе Задачи для файлов и папок щелкните пункт Копировать файл, Скопировать папку или Скопировать выделенные объекты.
4. В диалоговом окне Копирование элементов щелкните значок привода CD-R(W) (рис. 1.12), а затем — Копирование.

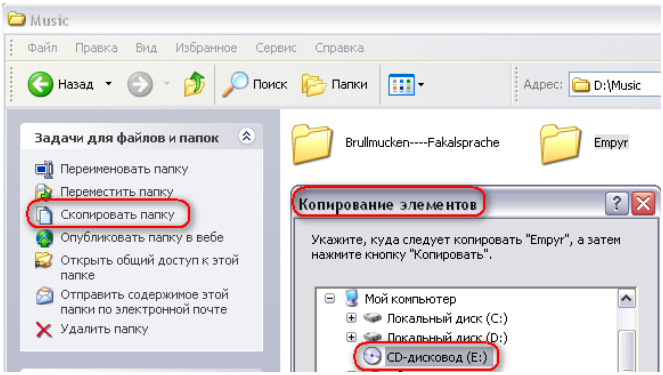


Рис. 1.12 Копирование выбранных элементов на диск

5. В окне **Мой компьютер** щелкните значок привода CD-R(W) и затем — пункт **Записать файлы на компакт-диск** в разделе

Объем стандартных CD — 650 Мбайт. CD высокой плотности вмещают не менее 700 Мбайт информации. Вам необходимо позаботиться о достаточном пространстве на жестком диске для временного хранения файлов, которые вы хотите скопировать на CD. В противном случае записать ничего не удастся.

Windows XP Professional поддерживает ClearType — новую технологию отображения текста на экране. ClearType программно утраивает максимальную горизонтальную разрешающую способность для визуализации текста, что обеспечивает более четкое отображение текста на экране LCD-мониторов с цифровым интерфейсом.

Для использования ClearType необходимо выполнить следующие действия:

1. Щелкните **Пуск** и затем — **Панель управления**.
2. Щелкните категорию Оформление и темы, затем — Экран.
3. В диалоговом окне **Свойства: Экран** выберите вкладку **Оформление**.
4. На вкладке **Оформление** щелкните кнопку **Эффекты**.
5. Установите флажок **Применять следующий метод сглаживания экранных шрифтов**, затем выберите ClearType из раскрывающегося списка (рис. 1.13).

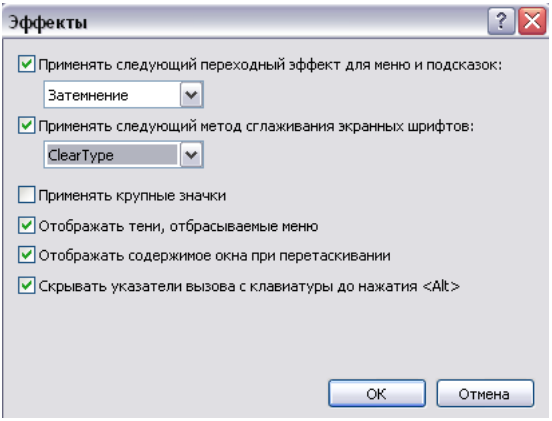


Рис. 1.13 Диалоговое окно **Эффекты**

1. Щелкните **ОК**, чтобы закрыть диалоговое окно **Эффекты**.
2. Щелкните **ОК,** чтобы закрыть диалоговое окно **Свойства: Экран**.

Функция архивации папок дает возможность создавать ZIP-папки и просматривать их содержимое. Эта функция позволяет архивировать

файлы большого размера, а значит, размещать больше файлов на гибком или жестком диске.

Для создания ZIP-папки необходимо выполнить следующие действия:

1. Щелкните **Пуск**, щелкните правой кнопкой мыши **Мой компьютер**, затем щелкните пункт меню **Проводник**. В левой части окна выберите диск, например, диск С.
2. В меню **Файл** щелкните **Создать**, а затем — **Сжатая ZIP-папка**.
3. При перетаскивании файлов и папок в ZIP-папку они архивируются. Нельзя сохранять файлы в ZIP-папке из приложений.

Мастер очистки рабочего стола помогает сохранять ваш рабочий стол в порядке, периодически проверяя его на предмет неиспользуемых ярлыков и удаляя их без повреждения установленных программ. По умолчанию Мастер очистки рабочего стола выполняет поиск неиспользуемых ярлыков раз в два месяца и предлагает переместить их в папку **Неиспользуемые ярлыки** (Unused Desktop Shortcuts), расположенную на рабочем столе. Для запуска **Мастера очистки рабочего стола** необходимо выполнить следующие действия:

1. Щелкните **Пуск**, затем — **Панель управления**.
2. Щелкните **Оформление и темы**, затем - **Экран**.
3. Выберите вкладку **Рабочий стол**, затем щелкните **Настройка рабочего стола**. Windows XP Professional выведет диалоговое окно **Элементы рабочего стола** (рис. 1.14).
4. Для запуска Мастера очистки рабочего стола щелкните кнопку **Очистить рабочий стол** в разделе **Очистка рабочего стола**.

Меню **Пуск** модифицировано так, чтобы упростить доступ к наиболее важным и часто используемым задачам. Кроме ссылок для доступа к Интернету и электронной почте новое меню **Пуск** содержит программы, которые вы используете чаще всего. Windows XP Professional непрерывно обновляет этот список в зависимости от используемых вами программ. При этом добавляются часто

используемые программы и удаляются из списка те, с которыми вы не работаете.

Windows XP Professional удаляет лишь ярлыки программ, а не сами программы. В меню **Пуск** также включены важные пользовательские папки, такие, как **Мои документы**, **Мои рисунки** и **Моя музыка**.

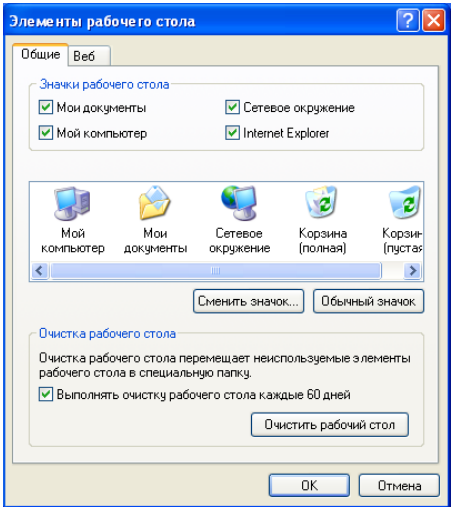


Рис. 1.14 Диалоговое окно **Элементы рабочего стола**

Для настройки меню **Пуск** необходимо выполнить следующие действия:

1. Щелкните правой кнопкой мыши кнопку **Пуск**, затем щелкните пункт меню **Свойства**.
2. Щелкните вкладку **Меню Пуск**.

Вкладка **Меню Пуск** позволяет переключаться между стилем меню Windows XP Professional и классическим стилем ранних версий Windows.

3. Щелкните кнопку **Настроить** .

Диалоговое окно **Настройка меню Пуск** имеет две вкладки: **Общие** и **Дополнительно**. Вкладка **Общие** позволяет изменять размер значков программ, настраивать количество отображаемых в меню

Пуск часто используемых программ, а также выбирать выводимые в меню **Пуск** почтовые клиенты и Интернет-утилиты.

Вкладка **Дополнительно** (рис. 1.15), позволяет настроить параметры меню **Пуск**, элементы меню и отображение последних документов.

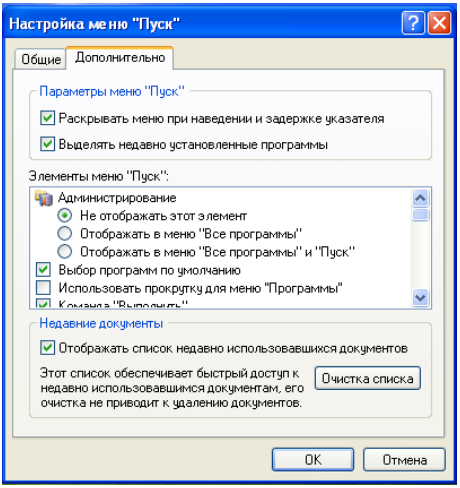


Рис. 1.15 Вкладка **Дополнительно** диалогового окна **Настройка меню Пуск**

В Windows XP Professional предусмотрена поддержка факсимильных сообщений, что позволяет отправлять факсы с компьютера при наличии факс-модема, факсимильной платы или нелокальной сети. Вы можете выводить информацию на факс из любого приложения, отсылать титульные страницы, отслеживать и контролировать факсимильные сообщения. Применение новых мастеров упрощает настройку этой функции.

Администраторам предоставлена возможность использовать для управления факсимильными инструментами программный интерфейс (API) модели компонентных объектов (COM) и для установки факсимильной службы в своей инфраструктуре консоль управления Microsoft (MMC).

Разработчики могут применять COM для программной отправки факсов, а также использовать факсимильные API для создания приложений автоматической отправки факсов.

Для управления факсами или отправки факсов необходимо выполнить следующее:

1. Щелкните **Пуск**, установите указатель на **Все программы**, затем — на **Стандартные**.
2. Установите указатель на Связь, а затем на Факсы.

Функция быстрой смены пользователей позволяет нескольким пользователям одновременно работать с компьютером, не закрывая запущенные приложения. Например, если вы работаете с документом Microsoft Word и на некоторое время отлучаетесь, функция быстрого переключения пользователей позволяет другому человеку, открыв другую учетную запись на этом же компьютере, найти, допустим, остаток на счете клиента, не закрывая открытый вами документ Word. Причем, ни вам, ни этому человеку не придется завершать свой сеанс.

Локализация — это настройка региональных стандартов в соответствии с языковыми предпочтениями пользователя (например, Канадский французский язык и Британский английский язык). В отличие от Windows 2000 Professional, здесь добавлена поддержка следующих языков: галицкий, гуджаратский, каннада, киргизский (кириллица), монгольский (кириллица), панджаби, сирийский (восточно-арамейский диалект) и телугу. Расширения для поддержки этих языков также включены в категорию **Язык и региональные стандарты**.

Автоматическая настройка нескольких сетевых подключений обеспечивает простой доступ к сетевым устройствам и Интернету. Это также дает возможность пользователям портативных компьютеров, не прилагая особых усилий, подключаться как к офисным, так и к домашним сетям без ручного изменения параметров протокола TCP/IP.

Вы можете применять эту функцию, чтобы определить альтернативную конфигурацию TCP/IP, используемую когда не

найден сервер DHCP. Дополнительная конфигурация имеет смысл, если компьютер используется в нескольких сетях, в одной из которых нет сервера DHCP и автоматического назначения IP-адресов.

Microsoft Internet Explorer 6.0 обеспечивает визуальное обновление и расширенную поддержку для объектной модели документа (DOM) 1-го уровня и каскадных таблиц стилей (CSS) 1-го уровня. Особенности Internet Explorer 6.0 перечислены далее:

• улучшена работа с мультимедиа, добавлено меню быстрого вызова для записи изображений, а также поддержка папок **Мое видео** и **Моя музыка** как папок по умолчанию для соответствующих файлов;

• встроенная поддержка файлов Macromedia Flash и Macromedia Shockwave Player;

• имеется автоматическое изменение размеров изображения под текущее окно браузера. Эта функция работает только при непосредственном доступе к изображению; она не редактирует размеры внедренных изображений на HTML-странице.

Также модифицирована работа с сетями, в частности в интересах безопасности, работа с файлами “cookie”, изменены служба Passport и диалоговые окна аутентификации в целях более интегрированного управления паролями и разрешениями.

Возможность передачи мгновенных сообщений позволяет пользователям быстро связываться друг с другом через Интернет. В Internet Explorer 6.0 встроена возможность отображения MSN Messenger, Outlook Express и списка контактов Outlook на боковой панели. Windows Messenger в Windows XP Professional обеспечивает работу с мультимедиа, аудио и видеоданными из Интернета в реальном времени. Для этого нужен паспорт .NET, для получения которого требуется ваша учетная запись Microsoft Hotmail или программа MSN Messenger и соединение по телефонной линии. Если вы хотите работать с аудио и видео в реальном времени, то потребуется микрофон и Web-камера.

Для передачи мгновенных сообщений необходимо выполнить следующие действия:

1. Щелкните **Пуск**, установите указатель на **Все программы**, затем щелкните пункт **Windows Messenger.**
2. Дважды щелкните имя человека, с которым хотите поговорить, в списке доступных лиц.

Microsoft разработала брандмауэр подключения к Интернету (Internet Connection Firewall, ICF) для использования дома и в небольших фирмах. Он обеспечивает защиту компьютеров, непосредственно подключенных к Интернету. Его можно использовать при работе в локальной сети (LAN) или доступе в Интернет по коммутируемой линии, виртуальной частной сети (VPN) и соединениях по протоколу PPP через Ethernet (PPPoE). Он также предотвращает просмотр портов и ресурсов (сетевой доступ к файлам и принтерам) с удаленных ресурсов.

Windows XP Professional имеет две терминальные службы: удаленный рабочий стол и подключение к удаленному рабочему столу. Удаленный рабочий стол обеспечивает доступ к рабочему столу с помощью любого клиента терминальных служб. Он также обеспечивает доступ:

• ко всем установленным приложениям, выполняемым процессам и всем обычным для рабочей станции или сервера видам соединений;

• к сеансам на платформах Windows 2000 Server для администрирования компьютера или вычислений на стороне сервера.

Кроме того, удаленный рабочий стол поддерживает доступ через **Удаленный терминал**, что позволяет перенести изображение с первичного монитора на клиент терминального сервера.

Подключение к удаленному рабочему столу — инструмент конечного пользователя для установления соединения с компьютерами, на которых работают терминальные службы. Служащие компаний, которые работают дома, используя бизнес-приложение с хостингом на терминальном сервере, могут воспользоваться **Службой удаленного доступа** (RAS) для установки телефонного соединения и подключения к удаленному рабочему столу, чтобы использовать эту программу. Подключение к удаленному

рабочему столу предоставляет много возможностей, позволяя оптимизировать сеть любой пропускной способности.

Для подключения к удаленному рабочему столу необходимо выполнить следующие действия:

1. Щелкните **Пуск**, установите указатель на **Все программы.**
2. Установите указатель на **Стандартные**, **Связь**, щелкните **Подключение к удаленному рабочему столу**, затем щелкните кнопку **Параметры** .

Windows XP Professional выведет диалоговое окно **Подключение к удаленному рабочему столу** (рис. 1.16).

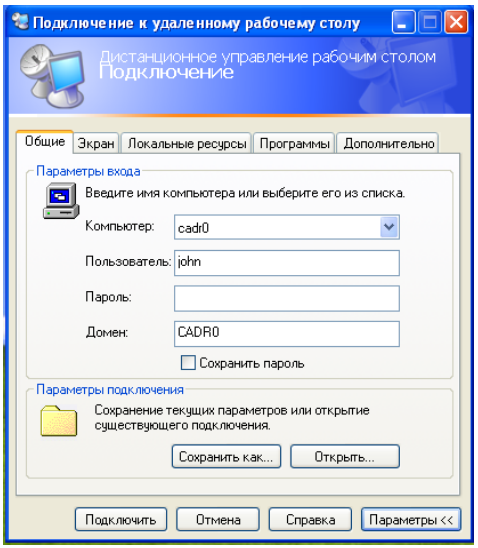


Рис. 1.16 Диалоговое окно Подключение к удаленному рабочему столу

Windows XP Professional теперь имеет две службы поддержки — службу технической поддержки Microsoft и телеконференции Windows, которые позволяют пользователям решать проблемы, возникающие при работе с компьютером.

Вы обращаетесь в Microsoft, и специалисты службы поддержки помогают вам разрешить возникшие трудности. Например, если возникли сложности при установке драйверов для новых аппаратных

средств на вашем компьютере, то стоит через **Центр справки и поддержки** обратиться за помощью в Microsoft.

Чтобы воспользоваться возможностями **Центра справки и поддержки**, необходимо выполнить следующие действия:

1. Щелкните **Пуск** (Start).
2. Щелкните **Справка и поддержка** (Help And Support).

Windows XP Professional откроет окно **Центр справки и поддержки** (Help And Support Center) (рис. 1.17).

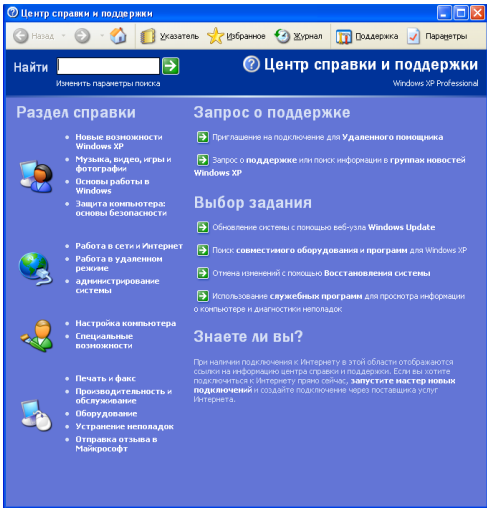


Рис. 1.17 Окно Центр справки и поддержки

Посредством групп новостей Windows можно получить необходимую информацию для разрешения возникших трудностей при работе с компьютером бесплатно в интерактивных условиях. Если вы не хотите обращаться в службу технической поддержки Microsoft и к поставщикам комплектующих, вы всегда можете воспользоваться досками объявлений — для этого не придется устанавливать продолжительное соединение, а также комнатами для дискуссий в реальном времени.

Эти способы позволяют получить ответ на вопрос очень быстро. Эти возможности предоставлены для продвижения услуг Windows и

MSN Community, а чтобы пользователи могли организовать или расширить службу поддержки в своих собственных сообществах.

Чтобы получить доступ к группам новостей Windows, необходимо выполнить следующее:

1. Щелкните **Пуск**, затем — **Справка и поддержка**.
2. В окне **Центр справки и поддержки**, в разделе **Запрос о поддержке**, щелкните **Запрос о поддержке или поиск информации в труппах новостей Windows XP**.

Функция проверки совместимости оборудования и программ позволяет получать свежую и подробную информацию о совместимости оборудования и программ, что помогает пользователям обновить оборудование, определиться в вопросе приобретения нового оборудования и устранить неполадки. Например, вы купили приложение, требующее наличия аппаратного ускорителя трехмерной графики, но не знаете, какие платы совместимы с вашим компьютером. Чтобы найти совместимое устройство, вы можете воспользоваться **Центром справки и поддержки**. В запросе следует указать изготовителя, тип изделия, программное обеспечение или аппаратные средства. Служба совместимости Microsoft для ответа на запрос аккумулирует опыт пользователей, данные независимых поставщиков комплектующих (IHV) и ПО (ISV).

Чтобы воспользоваться функцией проверки совместимости оборудования и программ, выполните следующие действия:

1. **Щелкните Пуск**, затем — **Справка и поддержка**.
2. В окне **Центр справки и поддержки**, в разделе **Выбор задания**, щелкните **Поиск совместимого оборудования и программ для Windows XP**.

В справочной системе Windows для форматирования и отображения информации используется HTML. Если у вас есть подключение к Интернету, то можно искать каждое слово или фразу во всех справочных файлах Windows. Поскольку справочная система Windows открыта, многие поисковые машины могут использовать **Центр справки и поддержки** посредством набора стандартных интерфейсов. Пользователи получают возможность искать данные в

нескольких удаленных сетевых источниках. Например, искать информацию на вашем компьютере, в базе знаний Microsoft или в базе данных поставщика оборудования.

Чтобы воспользоваться полнотекстовым поиском, выполните следующие действия:

1. Щелкните **Пуск**, затем — **Справка и поддержка**.
2. В окне **Центр справки и поддержки**, в поле **Найти**, введите текст, который вы хотите найти.
3. Для настройки параметров поиска щелкните **Изменить параметры поиска** (рис. 1.18).

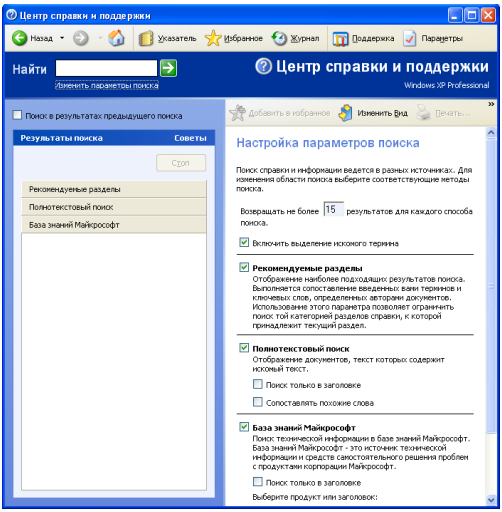


Рис. 1.18 Ссылка **Настройка параметров поиска** в окне Центр справки и поддержки

В разделе **Сведения о компьютере** понятно и доступно представлена информация о программном обеспечении и оборудовании, установленном на вашем или удаленном компьютере, к которому вы имеете административный доступ.

Для просмотра сведений о компьютере необходимо выполнить следующие действия:

1. Щелкните **Пуск**, затем — **Справка и поддержка**.

2. В окне **Центр справки и поддержки**, в разделе **Выбор задания**, щелкните **Использование служебных программ для просмотра информации о компьютере и диагностики неполадок**.
3. В разделе **Сервис** щелкните **Сведения о компьютере.**

Вы можете просмотреть информацию о системе в любой из пяти категорий, все они описаны в следующих разделах.

Категория **Сведения об этом компьютере — Общие** содержит сведения об изготовителе компьютера, модели, базовой системе ввода-вывода (BIOS), о типе и тактовой частоте процессора, операционной системе, объеме оперативной памяти и доступного дискового пространства.

Категория **Сведения об этом компьютере — Состояние** содержит диагностическую информацию о таких компонентах системы, как:

- устаревшие приложения и драйверы устройств;
- системное программное обеспечение;
- аппаратные средства: видеоадаптер, сетевой адаптер, звуковая карта и USB-контроллер;
- жесткие диски;
- оперативная память.

Категория **Сведения об этом компьютере — Оборудование** содержит сведения об установленных аппаратных средствах, включая жесткий диск, монитор, видеоадаптер, модем, звуковую карту, USB-контроялер, сетевые адаптеры, привод CD-ROM, дисководы для гибких дисков, память и принтеры.

Категория **Программное обеспечение** содержит список программных продуктов Microsoft, установленных на вашем компьютере, и их регистрационные номера (PID), включая автоматически загружаемые программы из меню Автозагрузка. Здесь

также хранятся сведения об ошибках, которые произошли в приложениях во время работы компьютера.

Категория **Расширенные сведения о системе** позволяет выбрать следующие варианты:

• просмотр подробных сведений о системе (Msinfo32.exe).

Эта ссылка позволяет просмотреть детальную информацию об аппаратных ресурсах, компонентах (мультимедиа, ввод/вывод, сети, портах и памяти), программной среде и параметрах настройки браузера.

• просмотр выполняющихся служб.

• просмотр журнала регистрации ошибок.

• просмотр сведений о другом компьютере.

Если у вас есть административные права для доступа к удаленному компьютеру, то вы можете просмотреть сведения об этом удаленном компьютере.

Если вы щелкнете пункт **Просмотр сведений о другом компьютере**, то появится диалоговая Web-форма в которой нужно ввести имя этого удаленного компьютера. Введите имя удаленного компьютера, затем щелкните кнопку **Открыть**, чтобы просмотреть сведения об удаленном компьютере.

Вы можете открыть два сеанса приложения **Центр справки и поддержки** одновременно. Параллельные сеансы позволяют отправить сведения о проблемах в службу поддержки Microsoft и одновременно просматривать сведения о системе или справочную информацию.

Приложение **Центр справки и поддержки** позволяет распечатать целый раздел справки, используя одну команду вывода на печать, то есть, распечатать все доступные разделы на указанном узле.

Если некоторые разделы недоступны из-за проблем подключения к сети Windows XP Professional напечатает только доступную информацию. Отыскав нужную информацию, щелкните кнопку Печать.

Удаленный помощник позволяет дистанционно просматривать выводимую на экран информацию и управлять компьютером для выполнения различных задач поддержки. Он также позволяет передавать файлы и голосовые сообщения. Если вам не удается самостоятельно решить какую-либо проблему при работе с компьютером, попросите помощи у специалиста или другого пользователя (удаленного помощника) через Интернет. Удаленный помощник примет вашу просьбу обсудить эту проблему и просмотрит ваш рабочий стол. Также он может передать любые файлы, необходимые для устранения проблемы. Если с вашего разрешения он получит полный контроль над вашим компьютером, то сумеет выполнить любые сложные задачи, необходимые для решения проблемы.

Задание к работе

1. Установить виртуальную машину MS Virtual PC.

2. Установить операционную систему семейства Windows в виртуальной машине.

3. Ознакомиться со следующими возможностями и средствами ОС.

3.1. Автоматическое обновление.

3.2. Копирование файлов и папок на диски не прибегая к стороннему ПО.

3.3. Поддержка ClearType.

3.4. Архивация папок.

3.5. Мастер очистки рабочего стола.

3.6. Меню Пуск.

3.7. Поддержка факсимильных сообщений.

3.8. Локализация и региональные стандарты.

3.9. Автоматическая настройка нескольких сетевых подключений.

3.10. Microsoft Internet Explorer 6.0.

3.11. Мгновенные сообщения.

3.12. Брандмауэр подключения к Интернету (ICF).

3.13. Терминальные службы: удаленный рабочий стол и подключение к удаленному рабочему столу.

3.14. Устранение неполадок с помощью Центра справки и поддержки службы поддержки. Служба технической поддержки Microsoft. Группы новостей Windows Совместимость оборудования и программ. Полнотекстовый поиск. Сведения о компьютере. Несколько экземпляров приложения. Удаленный помощник

Содержание отчета

1. Название работы
2. Цель работы
3. Краткие теоретические сведения.
4. Скриншоты выполненных заданий. Необходимо сопровождать все проделанные действия скриншотами и описаниями к ним.
5. Выводы.

Контрольные вопросы

1. В чем отличие ручной и автоматической установки объёма оперативной памяти при создании виртуальной машины с помощью программы MS Virtual PC?
2. Перечислите возможные варианты расположения дистрибутива гостевой операционной системы.
3. Что позволяет функция записи CD?
4. Что такое поддержка Clear Type?
5. Что позволяет функция сжатия папок?
6. Что удаляет мастер очистки рабочего стола для поддержания его в порядке? Как часто происходит запуск мастера по умолчанию?
7. Поддерживается ли в Windows XP Professional отправка факсимильных сообщений? Если да, то каким образом.
8. Какие возможности предоставляет функция быстрой смены пользователей?
9. Какая версия программы Internet Explorer входит в состав Windows XP Professional?
10. Какие данные можно передавать с помощью мгновенных сообщений через Интернет?
11. Каковы функции Брандмауэра?

12. Каким образом Windows XP Professional поможет вам определить необходимые модернизации оборудования?
13. Как средствами Центра справки и поддержки определить версию BIOS на вашем компьютере?
14. Как определить модель и драйвер каждого сетевого адаптера в рабочей группе, имея административный доступ ко всем компьютерам, входящим в нее?
15. С помощью какой службы можно обратиться в Microsoft и при участии специалистов из службы поддержки разрешить возникшие трудности?
16. Какие возможности пользователю предоставляют Группы новостей Windows?
17. Что обеспечивает функция проверки совместимости оборудования и программ?
18. Какая информация представлена в разделе Сведения о компьютере?

Лабораторная работа №2

Знакомство с рабочими группами и доменами

Цель работы: определить основные характеристики рабочих групп и доменов, понять принцип их работы. Научиться пользоваться экраном приветствия, описать особенности диалогового окна Безопасность Windows.

Порядок выполнения работы

1. Изучить теоретический материал.
2. Выполнить практические задания.
3. Сделать выводы на основании проделанной работы

Рабочие группы и домены

Windows поддерживает два сетевых окружения, в которых пользователи могут совместно использовать общие ресурсы независимо от размера сети: рабочие группы и домены [1, 7, 12].

Рабочая группа (workgroup) — логическое объединение компьютеров в сети, которые совместно используют такие общие ресурсы, как файлы и принтеры. Рабочую группу также называют *одноранговой сетью* (peer-to-peer network), потому что все компьютеры в ней могут использовать общие ресурсы на равных условиях, т. е. без выделенного сервера.

Организация рабочей группы нецелесообразна в сетях, содержащих более 10 компьютеров.

Каждый компьютер в рабочей группе обслуживает *базу данных политики безопасности локального компьютера*. Эта база данных представляет собой перечень учетных записей пользователей и информации о правах доступа к ресурсам на компьютере, где она постоянно находится. Использование базы данных политики безопасности локального компьютера децентрализует администрирование учетных записей пользователей и политики доступа к ресурсам в рабочей группе. На рис. 2.1 показана база данных политики безопасности локального компьютера.

В рабочую группу могут входить компьютеры на таких платформах Microsoft, как Windows NT и Windows 2003 Server, если, он не настроен как контроллер домена. В рабочей группе компьютер на платформах Windows NT или Windows 2003 Server называют *изолированным сервером*.

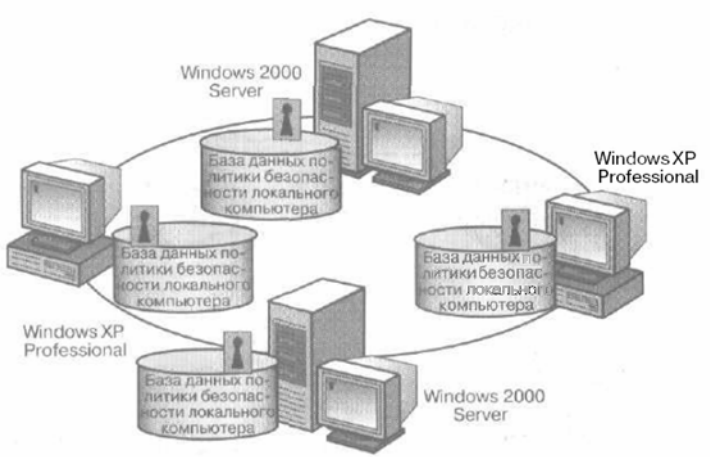


Рис. 2.1 Пример рабочей группы Windows XP Professional

Поскольку рабочие группы децентрализуют администрирование и политику доступа к ресурсам, верны следующие утверждения:

• пользователь должен иметь свою учетную запись на каждом компьютере, к которому он хочет получить доступ;

• любое изменение учетных записей пользователя, например замена его пароля или создание новой учетной записи, необходимо выполнить на каждом компьютере рабочей группы. Если администратор забудет зарегистрировать новую учетную запись на одном из компьютеров вашей рабочей группы, то новый пользователь не сможет получить доступ к этому компьютеру и его ресурсам.

Рабочая группа имеет следующие преимущества:

• она не требует включения в сеть контроллера домена для хранения централизованной информации о политиках безопасности;

• она проста в проектировании и эксплуатации. В отличие от домена, не требует крупномасштабного планирования и администрирования;

• это удобная сетевая среда для небольшого числа компьютеров, расположенных не слишком далеко друг от друга.

Домен (domain) — логическое объединение компьютеров в сети, которые совместно используют центральную базу данных каталога (рис. 2.2). *База данных каталога* содержит учетные записи пользователя и информацию о политиках безопасности для домена. Эту базу данных называют каталогом, и она представляет собой часть базы данных службы Active Directory — службы каталогов Windows 2003.

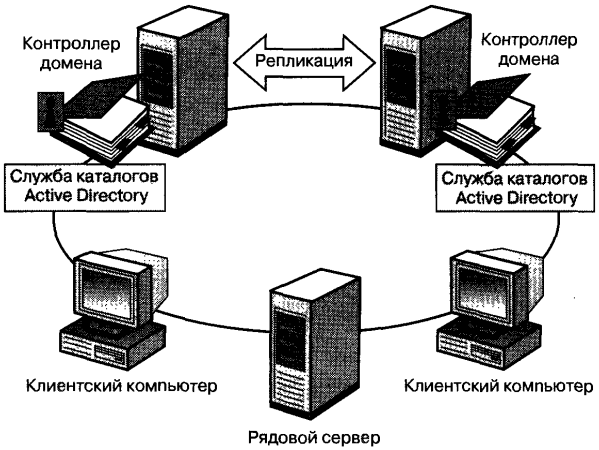


Рис. 2.2 Домен Windows 2003

В домене каталог размещен на компьютерах - контроллерах домена. **Контроллер домена** - это сервер, который координирует все параметры безопасности при взаимодействии пользователя и домена и централизует администрирование и управление политиками безопасности.

Можно назначить контроллером домена только компьютер на одной из платформ Microsoft серии Windows 2003 Server. Если все компьютеры в сети работают на платформе Windows XP Professional, то единственным доступным видом сети будет рабочая группа.

Домен не имеет отношения к местоположению в сети или определенному типу сетевой конфигурации. Компьютеры в домене могут располагаться рядом в небольшой локальной сети или находиться в различных уголках мира. Они могут связываться друг с другом по любому физическому соединению, включая телефонные

линии, линии ISDN, оптоволоконные линии, линии Ethernet, кольцевые сети с маркерным доступом, подключение с ретрансляцией кадров, спутниковую связь и выделенные линии.

Домен имеет следующие преимущества:

• централизованное администрирование, т.к. вся информация о пользователях хранится в одном месте;

• однократная регистрация пользователя для получения доступа ко всем сетевым ресурсам (файлам, принтерам и программам) при наличии требуемых прав доступа. Т.е. можно зарегистрироваться на одном компьютере сети и использовать ресурсы другого компьютера при условии, что имеются соответствующие разрешения на доступ;

• практически неограниченная масштабируемость, что позволяет создавать очень большие сети.

Типы компьютеров, которые включает типичный домен Windows 2003, перечислены ниже.

Контроллеры домена на платформе Windows 2003 Server. Каждый контроллер домена хранит и обслуживает копию каталога. В домене нужно создать единственную учетную запись пользователя, которую Windows 2003 записывает в каталог. Когда пользователь входит в систему на компьютере домена, контроллер домена аутентифицирует пользователя, проверяя в каталоге его учетную запись, пароль и ограничения на вход в систему. Если в домене есть несколько контроллеров домена, то они периодически обмениваются данными своих копий каталога (репликация).

Рядовые серверы на платформе Windows 2003 Server. Рядовой сервер (member server) — это сервер, не имеющий статуса контроллера в конкретном домене. Рядовой сервер не ведет каталог и не способен аутентифицировать пользователей. Рядовые серверы обеспечивают совместный доступ к сетевым ресурсам, например к общим папкам или принтерам.

Клиентские компьютеры на платформе операционной системы Microsoft. Клиентские компьютеры — это персональные компьютеры пользователей, которые предоставляют пользователям доступ к ресурсам домена.

Начало и завершение сеанса пользователя в Windows

Windows XP Professional предлагает два варианта локального входа в систему: экран приветствия и классическое диалоговое окно **Вход в Windows**.

По умолчанию для локального входа в систему в Windows XP Professional используется экран приветствия. Для начала сеанса нужно щелкнуть значок учетной записи, которая будет использовать. Если учетная запись требует пароля, появится предложение ввести его. Если учетная запись не защищена паролем, то пользователь беспрепятственно войдет в систему. Также можно использовать комбинацию CTRL+ALT+DELETE в экране приветствия, чтобы перейти к диалоговому окну **Вход в Windows**. Это окно дает возможность воспользоваться учетной записью администратора, которая не выводится на экран приветствия, если имеются другие учетные записи. Чтобы вывести окно для ввода имени и пароля, необходимо нажать CTRL+ALT+DELETE дважды.

Возможны два варианта локального входа в систему:

- на компьютере, который является членом рабочей группы;
- на компьютере, который входит в домен, но не является контроллером домена.

Поскольку контроллеры домена не обслуживают базы данных политик безопасности локальных компьютеров, местные учетные записи не доступны на контроллерах домена. Поэтому пользователю не удастся войти в систему на контроллере домена.

Категория **Учетные записи пользователей** в панели управления включает раздел **Изменение входа пользователей в систему**, который позволяет настроить параметры Windows XP Professional так, чтобы вернуться к диалоговому окну **Вход в Windows**.

При использовании диалогового окна **Вход в Windows** для входа в Windows XP Professional необходимо указать правильное имя пользователя; если имя пользователя защищено паролем, то следует также ввести пароль. Windows XP Professional аутентифицирует пользователя в процессе регистрации. Только пользователи с соответствующими правами доступа могут получить доступ к ресурсам и информации компьютера или сети. Windows XP Professional аутентифицирует пользователей при входе в систему на их

рабочем компьютере, а один из контроллеров домена на платформах семейства Windows 2003 аутентифицирует пользователей при входе в домен.

При классическом входе в Windows XP Professional посредством диалогового окна **Вход в Windows** появляется кнопка **Параметры**. Ниже описаны параметры диалогового окна **Вход в Windows** компьютера, входящего в домен.

Пользователь - уникальное имя пользователя для входа в систему, которое назначается администратором. Чтобы войти в домен под этим именем, пользователь должен иметь учетную запись, которая хранится в каталоге.

Пароль - пароль, присваиваемый учетной записи пользователя. Для аутентификации пользователю необходимо ввести пароль. Пароли учитывают регистр. В целях безопасности пароль отображается на экране в виде звездочек (*). Во избежание несанкционированного доступа к ресурсам и данным, рекомендуется держать пароли в местах с ограниченным доступом посторонних лиц.

Вход в систему - позволяет пользователю выбирать местный вход в систему или регистрацию в домене.

Вход в систему через телефонное соединение - позволяет соединиться с сервером домена по модему. Удаленный доступ к сети позволяет пользователю войти в сеть и работать удаленно.

Завершение работы - закрывает все файлы, сохраняет все параметры операционной системы и готовит компьютер к отключению.

Параметры - переключение между режимами **Вход в систему** и **Вход в систему через телефонное соединение**. Переключатели появляются, только если компьютер входит в домен.

Если ваш компьютер не входит в домен, то поле **Вход в систему** не отображается.

Процесс аутентификации в Windows

Доступ к системе на платформе Windows XP Professional или к любому ресурсу на этой системе осуществляется посредством окна

приветствия или диалогового окна **Вход в Windows.** В любом случае необходимо ввести имя пользователя и пароль. Процесс аутентификации в Windows XP Professional зависит от того, входит ли пользователь в домен или работает локально.

Процесс аутентификации:

1. Пользователь входит в систему, предоставив такие данные, как имя пользователя и пароль, и Windows XP Professional передает эту информацию подсистеме безопасности локального компьютера.
2. Windows XP Professional сравнивает эту информацию с информацией о пользователях в базе данных политик безопасности локального компьютера; эта база хранится в подсистеме безопасности локального компьютера.
3. Если данные совпадают и учетная запись пользователя верна, Windows XP Professional создает маркер доступа для такого пользователя.

Маркер доступа — это удостоверение личности пользователя для локального компьютера. В нем содержатся параметры настройки политик безопасности пользователя, которые позволяют ему получить доступ к соответствующим ресурсам и выполнять определенные системные задачи на этом компьютере.

Помимо процесса входа в систему, когда пользователь соединяется с системой, компьютер аутентифицирует пользователя и предоставляет маркер доступа. Этот процесс аутентификации невидим для пользователя.

Если пользователь входит в домен, Windows XP Professional связывается с доступным контроллером в домене. Контроллер сравнивает данные входа в систему с информацией о пользователях, которая хранится в каталоге домена. Если данные совпадают и учетная запись пользователя верна, контроллер домена создает маркер доступа для этого пользователя. Параметры безопасности маркера доступа предоставляют пользователю доступ к соответствующим ресурсам в домене.

Завершение сеанса в Windows XP Professional

Чтобы завершать сеанс пользователя и выйти из Windows XP Professional, щелкните **Пуск**, затем — **Выход из системы**. В меню **Пуск** (рис. 2.3) также предусмотрена возможность выключения компьютера.

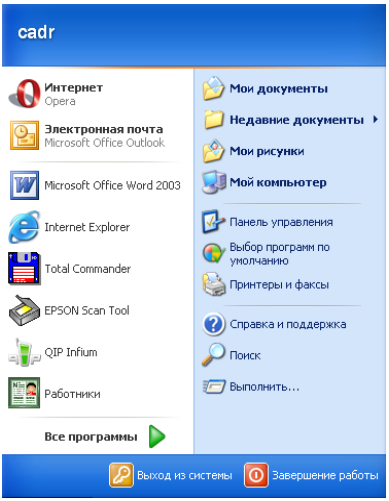


Рис. 2.3 Завершение сеанса в Windows XP Professional

Диалоговое окно Безопасность Windows

В диалоговом окне **Безопасность Windows** отображается информация об активированной учетной записи пользователя, а также имя домена или компьютера, где открыт сеанс пользователя. Эта информация важна для пользователей с несколькими учетными записями, например тех, кто имеет обычную учетную запись пользователя и учетную запись пользователя с административными правами. Если компьютер работает в домене или заблокирован экран приветствия, то можно вызвать диалоговое окно **Безопасность Windows**, нажав CTRL+ALT+DELETE. В противном случае откроется диспетчер задач. Ниже приведены параметры диалогового окна **Безопасность Windows**.

Блокировка - позволяет пользователям заблокировать компьютер, не завершая сеанс и не закрывая запущенные приложения. Пользователи могут заблокировать компьютер, если хотят отлучиться на некоторое время. Затем пользователь может отменить блокировку,

нажав CTRL+ALT+DELETE и введя правильный пароль. Администратор также имеет право разблокировать компьютер. В этом случае сеанс текущего пользователя завершается.

Выход из системы - позволяет завершить сеанс текущего пользователя и закрыть все запущенные программы, не завершая работу Windows XP Professional.

Завершение работы - позволяет закрыть все файлы, сохранить все параметры ОС, и подготовить компьютер к отключению.

Смена пароля - позволяет изменить пароль учетной записи пользователя. Чтобы задать новый пароль, необходимо знать текущий пароль. Это единственный возможный способ изменить собственный пароль. Администраторы также имеют право изменять пароли других учетных записей.

Диспетчер задач - предоставляет сведения об использовании памяти и центрального процессора, о выполняемых компьютером программах и процессах, а также позволяет просмотреть динамику использования ресурсов памяти и центрального процессора каждой запущенной программой, компонентом программы или системным процессом. Пользователи также могут применять диспетчер задач для переключения между приложениями и закрытия зависшей программы.

Отмена - закрывает диалоговое окно **Безопасность.**

Задание к работе

1. Ознакомиться с рабочими группами и доменами. Изучить их преимущества и недостатки.
2. Изучить начало и завершение сеанса пользователя в Windows XP Professional.
3. Изучить процесс аутентификации в Windows XP Professional.
4. Ознакомиться с диалоговым окном **Безопасность Windows.**

Содержание отчета

1. Название работы
2. Цель работы
3. Краткие теоретические сведения.

4. Скриншоты выполненных заданий. Необходимо сопровождать все проделанные действия скриншотами и описаниями к ним.
5. Выводы.

Контрольные вопросы

1. Какие из следующих утверждений о рабочей группе Windows XP Professional верны? (Выберите все правильные ответы).
   - Рабочая группа также называется одноранговой сетью.
   - Рабочая группа – логическое объединение сетевых компьютеров, которые совместно используют центральную базу данных каталога.
   - Применение рабочей группы нецелесообразно в сетях, объединяющих более 100 компьютеров.
   - В рабочую группу могут входить компьютеры на платформе Microsoft Windows Server 2003, не настроенные для работы в качестве контроллера домена.
2. Что такое контроллер домена?
3. Как называется база данных каталога, содержащая учетные записи пользователя и информацию о политиках безопасности домена, и частью какой службы Windows 2003 она является?
4. Какие действия может выполнить пользователь после входа в систему и от чего это зависит?
5. В чем главное различие аутентификации для входа в систему и входа в домен?
6. Как настроить Windows XP Professional, чтобы система использовала диалоговое окно **Вход в Windows** вместо экрана приветствия?
7. На каком из следующих компьютеров возможен локальный вход в систему? (Выберите все правильные ответы).
   - На компьютере с Windows XP Professional, который находится в рабочей группе.
   - На компьютере с Windows XP Professional, который расположен в домене.

- На компьютере с Windows 2003 Server, который является контроллером домена.
- На компьютере с Windows 2003 Server, который является рядовым сервером в домене.

8. Какое из следующих утверждений о диалоговом окне **Безопасность Windows** верное? (Выберите все правильные ответы).

- Вызывается нажатием CTRL+ALT+DELETE.
- Оно сообщает, как долго текущий пользователь находится в системе.
- Позволяет завершить сеанс на компьютере или в домене.
- Позволяет пользователю с административными правами изменять пароли других пользователей.

9. В каком случае пользователь может войти в доменную зону?
10. Что такое маркер доступа в среде рабочей группы?

Лабораторная работа №3

Утилиты диагностики компьютерных сетей

Цель работы: Изучить основные сетевые утилиты.

В состав стека протоколов TCP/IP входят следующие диагностические утилиты, предназначенные для проверки конфигурации тестирования сетевого соединения.

arp - выводит для просмотра и изменения таблицу трансляции адресов, используемую протоколом разрешения адресов ARP (Address Resolution Protocol - определяет локальный адрес по IP-адресу).

hostname - выводит имя локального хоста. Используется без параметров.

ipconfig - выводит значения для текущей конфигурации стека TCP/IP: IP-адрес, маску подсети, адрес шлюза по умолчанию, адреса WINS (Windows Internet Naming Service) и DNS (Domain Name System).

nbstat - выводит статистику и текущую информацию по NetBIOS, установленному поверх TCP/IP. Используется для проверки состояния текущих соединений NetBIOS.

netstat - выводит статистику и текущую информацию по соединению TCP/IP.

nslookup - осуществляет проверку записей и доменных псевдонимов хостов, доменных сервисов хостов, а также информации операционной системы, путем запросов к серверам DNS.

ping - осуществляет проверку правильности конфигурирования TCP/IP и проверку связи с удаленным хостом.

route - модифицирует таблицы маршрутизации IP. Отображает содержимое таблицы, добавляет и удаляет маршруты IP.

tracert - осуществляет проверку маршрута к удаленному компьютеру путем отправки эхо-пакетов протокола ICMP (Internet Control Message Protocol). Выводит маршрут прохождения пакетов на удаленный компьютер.

При устранении неисправностей и проблем в сети TCP/IP следует сначала проверить правильность конфигурации TCP/IP. Для этого используется утилита ipconfig.

Эта команда полезна на компьютерах, работающих с DHCP (Dynamic Host Configuration Protocol), так как дает пользователям возможность определить, какая конфигурация сети TCP/IP и какие величины были установлены с помощью DHCP.

Далее следует применить утилиту ping (Packet Internet Grouper), которая используется для проверки конфигурирования TCP/IP и диагностики ошибок соединения. Она определяет доступность и функционирование конкретного хоста. Использование ping - лучший способ проверки того, что между локальным компьютером и сетевым хостом существует маршрут. Хостом называется любое сетевое устройство (компьютер, маршрутизатор), обменивающееся информацией с другими сетевыми устройствами по TCP/IP.

Команда ping проверяет соединение с удаленным хостом путем посылки к этому хосту эхо-пакетов ICMP и прослушивания эхо-ответов. Ping ожидает каждый посланный пакет и печатает количество переданных и принятых пакетов. Каждый принятый пакет проверяется в соответствии с переданным сообщением. Если связь между хостами плохая, из сообщений ping станет ясно, сколько пакетов потеряно.

По умолчанию передается 4 эхо-пакета длиной 32 байта (периодическая последовательность символов алфавита в верхнем регистре). Ping позволяет изменить размер и количество пакетов, указать, следует ли записывать маршрут, который она использует, какую величину времени жизни (ttl) устанавливать, можно ли фрагментировать пакет и т.д.. При получении ответа в поле time указывается, за какое время (в миллисекундах) посланный пакет доходит до удаленного хоста и возвращается назад. Так как значение по умолчанию для ожидания отклика равно 1 секунде, то все значения данного поля будут меньше 1000 миллисекунд. Если вы получаете сообщение ``Request time out'' (Превышен интервал ожидания), то, возможно, если увеличить время ожидания отклика, пакет дойдет до удаленного хоста. Это можно сделать с помощью ключа -w.

Ping можно использовать для тестирования как имени хоста (DNS или NetBIOS), так и его IP-адреса. Если ping с IP-адресом выполнилась успешно, а с именем - неудачно, это значит, что проблема заключается в распознавании соответствия адреса и имени, а не в сетевом

соединении.

Tracert - это утилита трассировки маршрута. Она использует поле TTL (time-to-live, время жизни) пакета IP и сообщения об ошибках ICMP для определения маршрута от одного хоста до другого.

Утилита tracert может быть более содержательной и удобной, чем ping, особенно в тех случаях, когда удаленный хост недостижим. С помощью нее можно определить район проблем со связью (у Internet-провайдера, в опорной сети, в сети удаленного хоста) по тому, насколько далеко будет отслежен маршрут. Если возникли проблемы, то утилита выводит на экран звездочки (*), либо сообщения типа ``Destination net unreachable'', ``Destination host unreachable'', ``Request time out'', ``Time Exeeded''.

Утилита tracert работает следующим образом: посылается по 3 пробных эхо-пакета на каждый хост, через который проходит маршрут до удаленного хоста. На экран при этом выводится время ожидания ответа на каждый пакет (Его можно изменить с помощью параметра -w). Пакеты посылаются с различными величинами времени жизни. Каждый маршрутизатор, встречающийся по пути, перед перенаправлением пакета уменьшает величину TTL на единицу. Таким образом, время жизни является счетчиком точек промежуточной доставки (хопов). Когда время жизни пакета достигнет нуля, предполагается, что маршрутизатор пошлет в компьютер-источник сообщение ICMP ``Time Exeeded'' (Время истекло). Маршрут определяется путем посылки первого эхо-пакета с TTL=1. Затем TTL увеличивается на 1 в каждом последующем пакете до тех пор, пока пакет не достигнет удаленного хоста, либо будет достигнута максимально возможная величина TTL (по умолчанию 30, задается с помощью параметра -h).

Маршрут определяется путем изучения сообщений ICMP, которые присылаются обратно промежуточными маршрутизаторами.

Некоторые маршрутизаторы просто молча уничтожают пакеты с истекшим TTL и не будут видны утилите tracert.

Основная задача протокола ARP - трансляция IP-адресов в соответствующие локальные адреса. Для этого ARP-протокол

использует информацию из ARP-таблицы (ARP-кэша). Если необходимая запись в таблице не найдена, то протокол ARP отправляет широковещательный запрос ко всем компьютерам локальной подсети, пытаясь найти владельца данного IP-адреса. В кэше могут содержаться два типа записей: статические и динамические. Статические записи вводятся вручную и хранятся в кэше постоянно. Динамические записи помещаются в кэш в результате выполнения широковещательных запросов. Для них существует понятие времени жизни. Если в течение определенного времени (по умолчанию 2 мин.) запись не была востребована, то она удаляется из кэша.

Утилита netstat позволяет получить статическую информацию по некоторым из протоколов стека (TCP, UDP, IP, ICMP), а также выводит сведения о текущих сетевых соединениях. Особенно она полезна на брандмауэрах, с ее помощью можно обнаружить нарушения безопасности периметра сети.

Задание к работе

1. Получение справочной информации по командам.

Выведите на экран справочную информацию по утилитам arp, ipconfig, nbstat, netstat, nslookup,route, ping, tracert, hostname. Для этого в командной строке введите имя утилиты без параметров или с /?. Изучите и запишите ключи, используемые при запуске утилит.

2. Получение имени хоста. Выведите на экран имя локального хоста с помощью команды hostname.

3. Изучение утилиты ipconfig. Проверьте конфигурацию TCP/IP с помощью утилиты ipconfig. Заполните таблицу:

IP-адрес	
Маска подсети	
Основной шлюз	
Используется ли DHCP (адрес DHCP-сервера)	
Описание адаптера	
Физический адрес сетевого адаптера	
Адрес DNS-сервера	

Адрес WINS-сервера	

4. Тестирование связи с помощью утилиты ping. Проверьте правильность установки и конфигурирования TCP/IP на локальном компьютере. Проверьте, правильно ли добавлен в сеть локальный компьютер и не дублируется ли IP-адрес. С помощью команды ping проверьте адреса: *127.0.0.1, 192.168.233.25.*

Для каждого из них отметьте время отклика. Попробуйте увеличить время отклика. Задайте различную длину посылаемых пакетов. Определите доменное имя компьютера.

5. Определение пути IP-пакета. С помощью команды tracert проверьте для перечисленных ниже адресов, через какие промежуточные узлы идет сигнал. Отметьте их: 172.22.222.1, mail.ru, bstu.ru.

6. Просмотр ARP-кэша. С помощью утилиты arp просмотрите ARP-таблицу локального компьютера.

7. Получение информации о текущих сетевых соединениях и протоколах стека TCP/IP. С помощью утилиты netstat выведите перечень сетевых соединений и статистическую информацию для протоколов UDP, TCP, ICMP, IP.

8. Net view. Выводит список доменов, компьютеров или общих ресурсов на данном компьютере. Вызванная без параметров, команда net view выводит список компьютеров в текущем домене. Исследовать ресурсы домена bstu с помощью команды **net view**. Получить списки общих ресурсов компьютеров вашей аудитории.

Контрольные вопросы:

1. Какие утилиты можно использовать для проверки правильности конфигурирования TCP/IP?
2. Каким образом команда ping проверяет соединение с удаленным хостом?
3. Что такое хост?
4. Что такое петля обратной связи?
5. Сколько промежуточных маршрутизаторов сможет пройти IP-

пакет, если его время жизни равно 30?

6. Как работает утилита tracert?

Лабораторная работа №4
Установка и настройка сетевых протоколов

Цель работы: изучить набор протоколов TCP/IP. Научиться настраивать TCP/IP и устранять неисправности.

Порядок выполнения работы

1. Изучить теоретический материал.
2. Выполнить практические задания.
3. Сделать выводы на основании проделанной работы.

Набор протоколов TCP/IP

Протокол (protocol) — это набор правил и соглашений для передачи информации по сети. Microsoft Windows XP Professional использует протокол **TCP/IP** (Transmission Control Protocol/ Internet Protocol) для авторизации, работы файловых служб и служб печати, репликации информации между контроллерами домена и для других сетевых функций [1, 7, 12].

TCP/IP обеспечивает связь различных операционных систем и разных аппаратных архитектур через сеть. Реализация Microsoft TCP/IP позволяет организовать сеть масштаба предприятия и обеспечить связь между компьютерами, работающими под управлением Windows XP Professional.

Набор протоколов TCP/IP — это промышленный стандарт, который позволяет организовать сеть масштаба предприятия и связывать компьютеры, работающие под управлением Windows XP Professional.

Применение протокола TCP/IP в Windows XP Professional дает следующие преимущества:

• сетевой протокол с маршрутизацией поддерживается почти всеми операционными системами. Кроме того, почти все большие сети основаны на TCP/IP;

• эта технология позволяет соединить разнородные системы. Можно использовать много стандартных утилит связи для доступа и передачи данных между разнородными системами. В Windows XP Professional входят некоторые из этих стандартных утилит;

• это надежная, расширяемая интегрированная среда на основе модели “клиент — сервер”, работающая на различных платформах. TCP/IP поддерживает интерфейс Microsoft Windows Sockets (Winsock), который идеально подходит для разработки приложений “клиент сервер” на стеках Winsock;

• простое получение доступа к ресурсам Интернета.

Набор протоколов TCP/IP предоставляет ряд стандартов для связи компьютеров и сетей. Набор протоколов TCP/IP основан на концептуальной модели, состоящей из четырех уровней:

1. уровень сетевого интерфейса,
2. уровень Интернета,
3. транспортный уровень
4. уровень приложения.

В основании модели расположен уровень сетевого интерфейса, на котором передаются и принимаются сами пакеты.

Протоколы на уровне Интернета формируют пакеты в дейтаграммы Интернета и выполняют все необходимые алгоритмы маршрутизации. Здесь работают четыре протокола — Internet Protocol (IP), Address Resolution Protocol (ARP), Internet Control Message Protocol (ICMP) и Internet Group Management Protocol (IGMP).

Протокол IP обеспечивает доставку пакетов для всех других протоколов в наборе. Он не гарантирует доставку пакетов или правильную последовательность пакетов. Он не исправляет ошибки, такие, как:

- потерянные пакеты,
- пакеты, доставленные в неверной последовательности,
- дублированные пакеты
- задержанные пакеты.

Подтверждение передачи пакетов и повторная передача потерянных пакетов возлагается на протокол более высокого уровня,

такой, как TCP. IP в основном отвечает за правильную адресацию и маршрутизацию пакетов между узлами.

Протокол ARP обеспечивает отображение адресов IP в адрес подуровня управления доступом к среде для сопоставления физического адреса MAC получателя. Разрешение адресов IP требуется, так как пакеты IP передаются на основе широковещательной сетевой технологии с совместным доступом, такой, как Ethernet. С помощью широковещательного запроса IP передается специальный пакет запроса ARP, содержащий IP-адрес системы получателя. Система, которая имеет этот IP-адрес, отвечает, отправляя свой физический адрес источнику запроса. Подуровень MAC соединяется непосредственно с сетевой картой и отвечает за безошибочную доставку данных между двумя компьютерами в сети.

Протокол ICMP обеспечивает специальное соединение между узлами, позволяя им совместно использовать информацию об ошибках сети и о ее состоянии. Протоколам более высокого уровня эта информация позволяет исправлять проблемы передачи данных. Сетевые администраторы используют эту информацию для обнаружения сетевых неисправностей. Утилита ping использует ICMP-пакеты для определения наличия устройства с заданным IP-адресом в сети. В единственном случае ICMP обеспечивает специальное соединение между узлами — когда IP не способен доставить пакет в узел получателя, ICMP посылает в узел отправителя сообщение Destination Unreachable (получатель не распознан).

Протокол IGMP обеспечивает многоадресную передачу, которая представляет собой ограниченную форму широковещания, для соединения и управления информацией между всеми устройствами в группе многоадресной передачи IP. Группа многоадресной передачи IP — это несколько узлов, которые прослушивают трафик IP, предназначенный для специального адреса многоадресной передачи IP. Трафик многоадресной передачи IP посылается на один MAC-адрес, но обрабатывается несколькими узлами. IGMP информирует соседние маршрутизаторы многоадресной передачи о членстве узла группы в конкретной сети. Windows XP Professional поддерживает возможность многоадресной передачи, которая позволяет разработчикам создавать программы многоадресной передачи.

С помощью протоколов транспортного уровня реализуются сеансы связи между компьютерами. Предпочтительный метод доставки данных определяет транспортный протокол. Протоколов транспортного уровня — два: **Протокол управления передачей** (Transmission Control Protocol, TCP) и **Протокол дейтаграмм пользователя** (User Datagram Protocol, UDP)**.**

Протокол TCP предоставляет ориентированный на соединения надежный способ коммуникации для приложений, которые обычно передают большие объемы данных сразу или требуют подтверждения после получения данных. TCP основан на соединениях, поэтому соединение должно быть установлено, прежде чем узлы смогут обмениваться данными. TCP обеспечивает надежные соединения, назначая последовательно номера каждому сегменту данных. Они передаются так, чтобы узел получателя смог послать подтверждение (ACK), что данные получены. Если ACK не получено, то данные передаются повторно, TCP гарантирует доставку пакетов, правильную последовательность данных и формирует контрольную сумму, которая подтверждает корректность заголовка пакета и его данных.

Протокол UDP обеспечивает связь не устанавливая соединение. Он не гарантирует доставку или правильную последовательность передачи пакетов. Приложения, которые обычно используют UDP, передают маленькие объемы данных за один раз. Надежная доставка возлагается на само приложение.

Наверху модели — уровень приложений, на котором приложения получают доступ в сеть. Для этого уровня разработано множество стандартных утилит и служб TCP/IP — File Transfer Protocol (FTP), Telnet, Simple Network Management Protocol (SNMP), система доменных имен (Domain Name System, DNS) и т. д.

TCP/IP предоставляет два интерфейса для сетевых приложений, предназначенных для работы с набором протоколов TCP/IP: Winsock и интерфейс NetBIOS no TCP/IP (NetBT).

Winsock представляет собой стандартный интерфейс между приложениями на основе сокетов и протоколов TCP/IP. Приложение задает протокол, IP-адрес узла получателя и порт приложения получателя. Интерфейс Winsock предоставляет службы, которые позволяют приложению связываться с заданным портом и IP-адресом на узле, инициализировать и разрешать соединение, посылать и получать данные, а также закрывать соединение.

NetBT представляет собой стандартный интерфейс для сервисов NetBIOS, включая сервис имен, дейтаграмм и сессий. Кроме того, обеспечивает стандартный интерфейс между приложениями на основе NetBIOS и протоколами TCP/IP.

Настройка TCP/IP и устранение неисправностей

Каждый узел TCP/IP идентифицирован своим логическим IP-адресом, который идентифицирует положение компьютера в сети. Реализация Microsoft TCP/IP позволяет узлу TCP/IP использовать статический IP-адрес или получить IP-адрес автоматически с помощью DHCP-сервера (Dynamic Host Configuration Protocol). Для простых сетевых конфигураций, основанных на локальных сетях (LAN), он поддерживает автоматическое назначение IP-адресов. В Windows XP Professional включены утилиты, которые вы можете применять для диагностики TCP/IP и тестирования связи.

Каждый IP-адрес состоит из идентификатора (ID) сети и ID узла. ID сети, также известный как адрес сети, идентифицирует системы, которые расположены в одной и той же физической сети. Все компьютеры в физической сети должны иметь один и тот же ID сети, и ID сети должен быть уникален в межсетевой среде. ID узла, также известный как адрес узла, идентифицирует каждый узел TCP/IP в пределах сети, IP-адреса — логические 32-битные номера, которые разделены на четыре поля по 8 бит, называемые октетами. Microsoft TCP/IP поддерживает классы адресов A, B и C. Классы адресов определяют, какие биты используются для ID сети и какие — для ID узла. В таблице 4.1 описаны классы IP адресов A, B и C.

Таблица 4.1

Классы IP адресов A, B и C

Класс	Описание
A	Первый ID сети — 1.0.0.0, последний — 126.0.0.0. Это позволяет иметь 126 сетей и 16 777 214 узлов в сети. Адреса класс A 127.x.y.z зарезервированы для петлевого тестирования и связи между процессами на локальном компьютере. Для адресов класса A ID сети — первый октет в адресе, а ID узла — последние три октета
B	Первый ID сети - 128.0.0.0, последний - 191.255.0.0. Это позволяет иметь 16 384 сетей и 65 534 узлов в сети. Для адресов класса B ID сети — первые два октета в адресе, а ID узла — последние два октета
C	Первый ID сети - 192.0.0.0, последний- 223.255.255.0. Это позволяет иметь 2 097 152 сети и 254 узла в сети. Для адресов класса C ID сети — первые три октета в адресе, а ID узла — последний октет

Использование статического IP-адреса

По умолчанию компьютеры клиентов, работающие под управлением Windows XP Professional, Windows 2003, получают информацию о настройке TCP/IP автоматически от службы DHCP. Однако даже в том случае, если в сети доступен DHCP-сервер, нужно назначить статический IP-адрес для отдельных компьютеров в сети. Например, компьютеры с запущенной службой DHCP не могут быть клиентами DHCP, поэтому они должны иметь статический IP-адрес.

Если служба DHCP недоступна, можно настроить TCP/IP для использования статического IP-адреса. Для каждой платы сетевого адаптера в компьютере, которая использует TCP/IP, можно установить IP-адрес, маску подсети и шлюз по умолчанию, как показано на рис. 4.1.

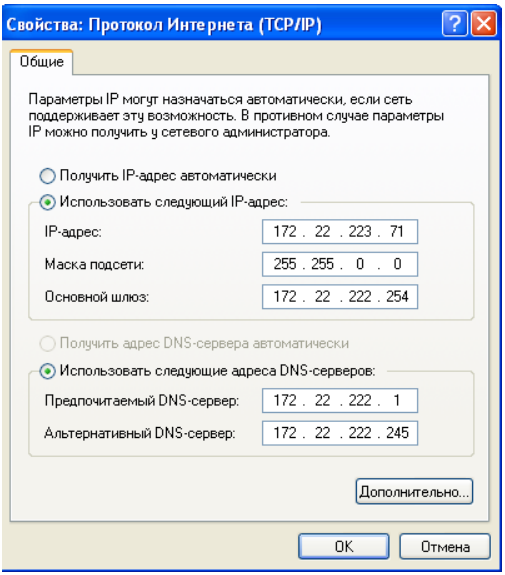


Рис. 4.1. Настройка статического адреса TCP/IP

Ниже перечислены параметры, которые используются при настройке статического адреса TCP/IP.

IP адрес (IP address) - логический 32-битный адрес, который идентифицирует TCP/IP узел. Каждой плате сетевого адаптера в компьютере с запущенным протоколом TCP/IP необходим уникальный IP адрес, например, 192.168.212.5. Каждый адрес имеет две части: ID сети, который идентифицирует все узлы в одной физической сети, и ID узла, который идентифицирует узел в сети. В этом примере ID сети - 192.168.212, и ID узла — 5.

Маска подсети (Subnet mask) - подсети делят большую сеть на множество физических сетей, соединенных маршрутизаторами. Маска подсети закрывает часть IP-адреса так, чтобы TCP/IP мог отличать ID сети от ID узла. Когда узлы TCP/IP пробуют связаться, маска подсети определяет, находится узел получателя на локальной или удаленной сети. Для того чтобы связываться в локальной сети, компьютеры должны иметь одинаковую маску подсети.

Шлюз по умолчанию (Default gateway) - промежуточное устройство в локальной сети, на котором хранятся сетевые

идентификаторы других сетей предприятия или Интернета. Для того чтобы связаться с узлом в другой сети, нужно установить IP-адрес для шлюза по умолчанию. TCP/IP посылает пакеты в удаленную сеть через шлюз по умолчанию (если никакой другой маршрут не настроен), который затем пересылает пакеты другим шлюзам, пока пакет не достиг шлюза, связанного с указанным адресатом.

Для настройки TCP/IP с использованием статического IP адреса необходимо выполнить следующие действия:

1. Щелкните Пуск и затем — Панель управления.
2. В окне Панель управления щелкните Сеть и подключения к Интернету.
3. В окне Сеть и подключения к Интернету (Network And Internet Connections) щелкните значок Сетевые подключения (Network Connections), щелкните правой кнопкой мыши Локальные подключения (Local Area Connection) и затем щелкните пункт меню Свойства (Properties).
4. В диалоговом окне Свойства: локальная сеть щелкните Протокол Интернета (TCP/IP), удостоверьтесь, что флажок слева установлен, и затем щелкните Свойства.
5. В диалоговом окне Свойства: Протокол Интернета (TCP/IP), на вкладке Общие, щелкните переключатель Использовать следующий IP адрес, введите параметры настройки TCP/IP и затем щелкните ОК.
6. Щелкните ОК, чтобы закрыть диалоговое окно Свойства: локальная сеть, и затем закройте окно Сетевые подключения.

Автоматическое получение IP-адреса

Если сервер с запущенной службой DHCP доступен в сети, он автоматически предоставляет информацию о параметрах TCP/IP клиенту DHCP. Затем можно настроить любой клиентский компьютер с системой Windows XP Professional для получения информации о параметрах TCP/IP автоматически от службы DHCP. Это упростит администрирование и гарантирует правильность настройки.

В Windows XP Professional не включена служба DHCP. Только продукты семейства Windows 2003 Server предоставляют службу DHCP.

В состав Windows XP Professional также входит функция автоматического назначения частных IP-адресов, которая предоставляет клиентам DHCP ограниченные функциональные сетевые возможности, если DHCP-сервер недоступен во время запуска.

Можно использовать службу DHCP, чтобы автоматически передавать клиентам информацию о параметрах TCP/IP. Однако следует настроить компьютер в качестве клиента DHCP до того, как он сможет взаимодействовать со службой DHCP.

Для настройки клиента DHCP нужно выполнить следующие действия:

1. Щелкните Пуск, затем — Панель управления.
2. В окне Панель управления щелкните Сеть и подключения к Интернету.
3. В окне Сеть и подключения к Интернету щелкните значок Сетевые подключения дважды щелкните Локальные подключения и затем щелкните пункт меню Свойства.
4. В диалоговом окне Свойства: локальная сеть щелкните Протокол Интернета (TCP/IP), удостоверьтесь, что флажок слева установлен, и затем щелкните кнопку Свойства.
5. В диалоговом окне Свойства: Протокол Интернета (TCP/IP), на вкладке Общие, щелкните переключатель Получить IP-адрес автоматически.
6. Щелкните OK, чтобы закрыть диалоговое окно Свойства: локальная сеть и затем закройте окно Сетевые подключения.

Использование автоматического назначения частных IP-адресов

В Windows XP Professional реализация TCP/IP поддерживает автоматическое назначение IP-адресов для простых локальных сетевых конфигураций. Этот механизм адресации — расширение динамического назначения IP-адресов для сетевых адаптеров,

позволяющее выполнять настройку IP-адресов без назначения статического IP-адреса или установки службы DHCP. Автоматическое назначение частных IP адресов доступно по умолчанию в Windows XP Professional, что позволяет пользователям, работающим дома, и тем, кто занимается мелким бизнесом, создать работающую одиночную подсеть на основе TCP/IP без необходимости настраивать TCP/IP-протокол вручную или устанавливать DHCP-сервер.

Автоматического назначения частных IP-адресов работает следующим образом:

1. TCP/IP в Windows XP Professional пытается найти DHCP-сервер в присоединенной сети для динамического назначения IP-адреса.
2. Если во время загрузки DHCP-сервер отсутствует (например, если он выключен на обслуживание или ремонт), клиент не может получить IP-адрес.
3. Функция автоматического назначения частных IP-адресов генерирует IP-адреса (APIPA) в форме 169.254.x.y (где x.y — уникальный идентификатор клиента) и маску подсети 255.255.0.0.

Internet Assigned Numbers Authority (IANA) резервирует адреса от 169.254.0.0 до 169.254.255.255 для автоматического назначения частных IP-адресов. В результате автоматическое назначение частных IP-адресов предоставляет адрес, который гарантировано не будет конфликтовать с адресами таблицы маршрутизации.

После генерации адреса компьютер рассылает широковещательным способом этот адрес и затем присваивает его себе, если другие компьютеры не отвечают. Компьютер использует этот адрес, пока не обнаружит DHCP-сервер и не получит от него информацию о параметрах. Таким образом, два компьютера, подключенные к сетевому концентратору, могут перезапускаться без настройки IP-адресов и использовать TCP/IP для доступа в локальную сеть.

Если компьютер настроен как клиент DHCP, предварительно получил разрешение от DHCP-сервера и срок действия разрешения не истек во время начальной загрузки, последовательность событий

немного другая. Клиент пытается возобновить разрешение у DHCP-сервера. Если ему не удается связаться с DHCP-сервером в течение попытки обновления, он пытается послать запрос шлюзу по умолчанию, указанному в разрешении.

Если шлюз по умолчанию отвечает на запрос, клиент DHCP предполагает, что он все еще находится в той же самой сети, где получил текущее разрешение, поэтому он продолжает использовать разрешение. По умолчанию клиент пытается возобновить разрешение, когда истекло 50% назначенного времени действия разрешения. Если шлюз по умолчанию не отвечает на запрос, клиент предполагает, что он был перемещен в другую сеть, в которой в настоящий момент нет службы DHCP, и далее он автоматически настраивает параметры, как описано выше. Настроившись, он пытается найти DHCP-сервер каждые 5 минут.

Функция автоматического назначения частных IP-адресов может назначать TCP/IP-адрес для клиентов DHCP автоматически. Однако при этом не генерируется вся информация, которая обычно предоставляется DHCP, например адрес шлюза по умолчанию. Следовательно, компьютеры с включенным автоматическим назначением частных IP-адресов могут связываться только с компьютерами в той же самой подсети (которые имеют адреса вида *169.254.x.y).*

По умолчанию функция автоматического назначения частного IP-адреса разрешена. Однако можно ее отключить, выполнив альтернативную настройку, которая используется, если DHCP-сервер не удается найти.

Определение альтернативной конфигурации для TCP/IP

Автоматическая настройка для нескольких сетевых соединений обеспечивает простой доступ к сетевым устройствам и Интернету. Она также позволяет работать на переносном компьютере в сетях офиса и дома, не перенастраивая параметры TCP/IP вручную.

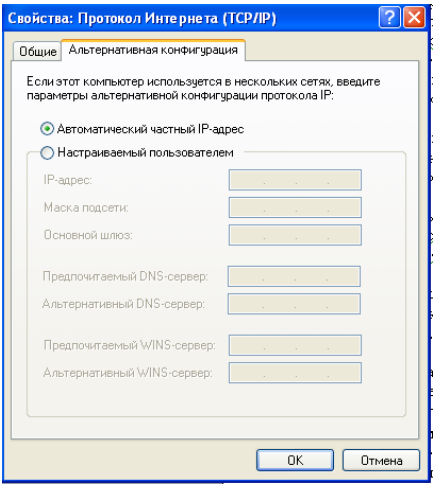


Рис. 4.2. Определение альтернативной настройки TCP/IP

Задается альтернативную конфигурацию для TCP/IP, используемую, если DHCP-сервер не найден. Альтернативная конфигурация полезна, когда компьютер используется в нескольких сетях, одна из которых не имеет DHCP-сервера, и не используется средство автоматического назначения частных IP-адресов.

Чтобы установить автоматическую настройку для нескольких сетевых соединений необходимо выполнить следующее:

1. Щелкните Пуск, затем щелкните Панель управления .
2. В окне Панель управления щелкните Сеть и подключения к Интернету.
3. В окне Сеть и подключения к Интернету щелкните значок Сетевые подключения, а затем — Локальные подключения.
4. Щелкните Изменить параметры этого подключения. Windows XP Professional покажет диалоговое окно Свойства: локальная сеть.
5. Щелкните Протокол Интернета (TCP/IP) (Internet Protocol TCP/IP) и затем — Свойства (). Windows XP Professional покажет диалоговое окно Свойства: Протокол Интернета (TCP/IP) с активной вкладкой Общие.
6. Щелкните вкладку Альтернативная конфигурация .
7. Задайте альтернативную конфигурацию TCP/IP (рис. 4.2).

Применение утилит TCP/IP

В Windows XP Professional включены утилиты, показанные на рис. 4.3, которые можно использовать для диагностики TCP/IP и проверки связи.

Рис. 4.3. Утилиты TCP/IP, включенные в состав Windows XP Professional

В Windows XP Professional имеется несколько утилит, предназначенных для диагностики TCP/IP:

ping - проверка настройки и проверка подключений;

arp - отображение локального соответствия IP-адресов в физические адреса;

ipconfig - отображение текущей настройки TCP/IP;

nbtstat - Отображение статистики и подключений, использующих NetBT;

netstat - отображение статистики протокола TCP/IP и подключений TCP/IP;

route - отображение или изменение локальной таблицы маршрутизации;

hostname - возвращает имя узла локального компьютера для идентификации при помощи утилит Remote Copy Protocol (RCP), Remote Shell (RSH) и Remote Execution (REXEC);

tracert - проверка маршрута к удаленной системе;

pathping - Проверяет, какие маршрутизаторы на пути к удаленному узлу работают правильно, выявляя потерю пакетов при выполнении множества транзитов.

Задание к работе

1. Изучить предлагаемый теоретический материал.
2. Настроить TCP/IP с использованием статического IP адреса. Для адресации использовать частный IP адрес класса C.
3. Настроить клиент DHCP для автоматического получения IP-адреса.
4. Изучить функцию автоматического назначения частных IP-адресов. Отключить автоматическое назначение частных IP-адресов.
5. Проверить средствами командной строки параметры протокола TCP/IP. Результаты записать в таблицу.
6. Настроить TCP/IP для использования статического IP-адреса из диапазона 198.168.233.2 - 198.168.233.254.
1. Щелкните Пуск и затем — Панель управления.
2. В окне Панель управления щелкните Сеть и подключения к Интернету.
3. В окне Сеть и подключения к Интернету щелкните значок Сетевые подключения и затем — Локальные подключения.
4. В разделе Сетевые задачи щелкните Измененить параметры этого подключения. Появится диалоговое окно Свойства: локальная сеть с информацией об используемом сетевом адаптере и сетевых компонентах, которые используются в этом подключении.
5. Щелкните Протокол Интернета (TCP/IP) и удостоверьтесь, что флажок слева от пункта установлен.
6. Щелкните кнопку Свойства. Появится диалоговое окно Свойства: Протокол Интернета (TCP/IP).
7. Щелкните переключатель Использовать следующий IP-адрес.
8. В текстовом поле IP-адрес наберите 198.168.233.__, а в текстовом поле Маска подсети наберите 255.255.255.0.
9. Щелкните ОК, чтобы возвратится в диалоговое окно Свойства:локальная сеть.
10. Щелкните ОК, чтобы закрыть диалоговое окно Свойства: локальная сеть и возвратиться к окну Сетевые подключения.

11. Сверните окно Сетевые подключения.

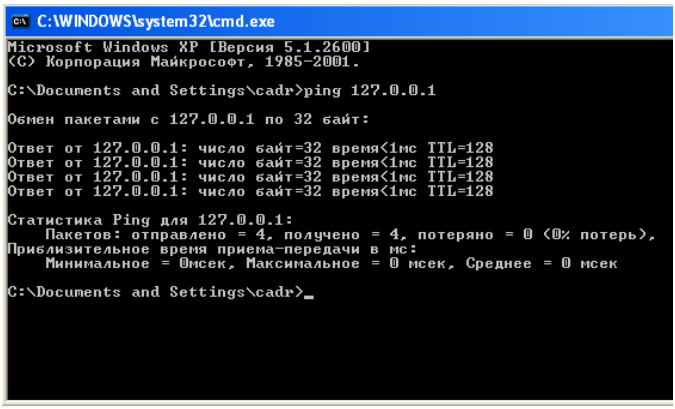
7. Проверить правильность настройки TCP/IP. Для тестирования использовать команды ipconfig и ping.

1. Восстановите окно командной строки.
2. В командной строке наберите ipconfig /all | more и затем нажмите Enter.
3. Утилита настройки IP Windows XP Professional покажет параметры физических и логических адаптеров вашего компьютера.
4. Нажимайте Пробел для прокрутки информации о параметрах и поиска информации о подключении локальной области.
5. Запишите текущие параметры TCP/IP для вашего подключения локальной области в таблицу:

Параметры	Значения
IP-адрес	
Маска подсети	
Шлюз по умолчанию	
Компьютер для проверки связи	

6. Нажимайте Пробел по необходимости для прокрутки информации о параметрах и возвращения в командную строку.
7. Чтобы удостовериться, что IP-адрес работает и настроен для вашего адаптера, наберите ping 127.0.0.1 и затем нажмите Enter.

Если адрес работает и настроен, вы получите следующий результат:



8. Наберите ping ip_address(где ip_address — IP-адрес того компьютера, который используетсz для тестирования связи) и затем нажмите Enter. Сверните командную строку.

8. Настроить TCP/IP для автоматического получения IP-адреса. Проверить правильность настройки TCP/IP.

1. Восстановите окно Сетевые подключения, щелкните правой кнопкой мыши Локальные подключения и затем щелкните Свойства. Появится диалоговое окно Свойства: локальная сеть.
2. Щелкните Протокол Интернета (TCP/IP), проверьте, что флажок слева установлен.
3. Щелкните кнопку Свойства. Появится диалоговое окно Свойства:; Протокол Интернета (TCP/IP).
4. Щелкните переключатель Получить IP-адрес автоматически.
5. Щелкните OK, чтобы закрыть диалоговое окно Свойства: Протокол Интернета (TCP/IP).
6. Щелкните OK, чтобы закрыть диалоговое окно Свойства: локальная сеть.
7. Сверните окно Сетевые подключения.

9. Получить IP-адрес с использованием автоматического назначения частных IP-адресов. Проверить правильность настройки TCP/IP.

Если у вас есть сервер с запущенной службой DHCP, вы должны отключить его, чтобы DHCP-сервер стал недоступен для предоставления IP-адреса вашему компьютеру. Без DHCP-сервера, который предоставляет IP-адрес, функция автоматического назначения частных IP-адресов Windows XP Professional предоставит уникальные IP-адреса для вашего компьютера.

1. В командной строке наберите ipconfig /release и затем нажмите Enter.
2. В командной строке наберите ipconfig /renew и затем нажмите Enter. Подождите, пока Windows XP Professional найдет DHCP-сервер в сети.

3. Щелкните ОК, чтобы закрыть диалоговое окно.

10. Тестирование параметров TCP/IP.

1. В командной строке наберите ipconfig | more и затем нажмите Enter.

2. Нажимайте клавишу Пробел по необходимости, запишите текущие параметры TCP/IP для вашего подключения локальной области в таблицу.

3. Это тот же самый IP-адрес, который назначен вашему компьютеру в предыдущем упражнении? Почему тот же или почему не тот?

4. Нажимайте Пробел, по необходимости, для завершения просмотра информации о параметрах.

5. Чтобы удостовериться, что TCP/IP работает и связан с вашим адаптером, наберите ping 127.0.0.1 и затем нажмите Enter. Внутренний петлевой тест показывает четыре ответа, если TCP/IP связан с адаптером.

6. Наберите ping ip_address (где ip_address — IP-адрес компьютера, который вы используете для тестирования связи) и затем нажмите Enter. Если у вас нет компьютера для тестирования связи, пропустите этот пункт.

7. Получить IP-адрес с помощью DHCP. Проверить правильность настройки TCP/IP. Для проверки параметров компьютера используют комбинацию двух утилит — ipconftg и ping:

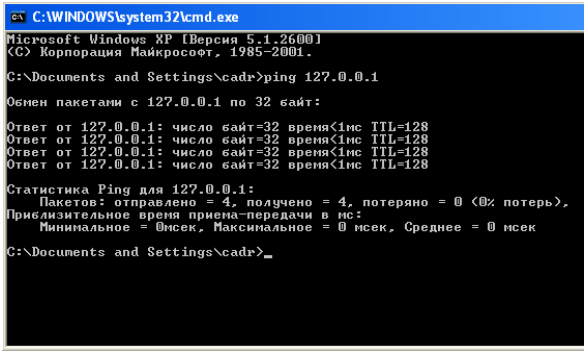
1. Щелкните Пуск и затем — Выполнить.
2. В диалоговом окне Выполнить наберите cmd и затем щелкните ОК, чтобы открыть командную строку.
3. В командной строке наберите ipconflg /all | more и затем нажмите Enter.
4. Утилита настройки IP Windows XP Professional покажет параметры TCP/IP для физических и логических адаптеров, установленных на вашем компьютере.
5. Нажимайте Пробел для прокрутки выводимой на экран информации до показа заголовка Local Area

Connection. Используя показанную информацию, заполните таблицу 4.2.

Таблица 4.2

Параметры подключения локальной области	Значение
Имя компьютера	
Основной DNS-суффикс	
Описание DNS-суффикса для подключения	
Физический адрес	
DHCP включен	
Автоконфигурация включена	
IP-адрес автоконфигурации	
Маска подсети	
Шлюз по умолчанию	

6. Нажимайте Пробел по необходимости для прокрутки выводимой информации о параметрах и возврата в командную строку.
7. Чтобы удостовериться, что IP-адрес работает и настроен для вашего адаптера, наберите ping 127.0.0.1 и затем нажмите Enter. Такой ответ свидетельствует об успешном обмене пакетами:



8. Сверните командную строку.

11. Тестирование параметров TCP/IP.

1. Восстановите командную строку, наберите *ipconfig /release* и затем нажмите Enter.

2. В командной строке наберите ipconfig /renew и затем нажмите Enter.
3. В командной строке наберите ipconfig | more и затем нажмите Enter.
4. Нажимайте Пробел по необходимости для прокрутки выводимой информации и запишите текущие параметры TCP/IP для вашего подключения локальной области в таблицу:

Параметры	Значения
IP-адрес	
Маска подсети	
Шлюз по умолчанию	

Чтобы удостовериться, что TCP/IP работает и связан с вашим адаптером, наберите *ping 127.0.0.1* и затем нажмите Enter.

5. Внутренний петлевой тест покажет четыре ответа, если TCP/IP связан с адаптером.

12. Получение IP-адреса с помощью DHCP.

Для выполнения этого упражнения понадобится доступная служба DHCP, запущенная на компьютере, который действует как DHCP-сервер. Ваш компьютер получит информацию об IP-адресе от DHCP-сервера.

1. В командной строке наберите *ipconflg /release* и затем нажмите Enter.
2. В командной строке наберите *ipconfig /renew* и затем нажмите Enter.
3. После короткого ожидания в окне появится сообщение, что новый IP-адрес назначен.
4. Щелкните ОК, чтобы закрыть окно сообщения.
5. В командной строке наберите ipconflg /all | more и затем нажмите Enter.
6. Убедитесь, что DHCP-сервер назначил IP-адрес вашему компьютеру.
7. Закройте командную строку.

Содержание отчета

1. Название работы
2. Цель работы
3. Краткие теоретические сведения.
4. Скриншоты выполненных заданий. Необходимо сопровождать все проделанные действия скриншотами и описаниями к ним.
5. Выводы.

Контрольные вопросы

1. Из каких четырех уровней состоит набор протоколов TCP/IP? Каковы функции протоколов на каждом уровне?
2. Какое из следующих утверждений верно описывает протокол IP? (Выберите все правильные ответы).
3. IP гарантирует доставку пакета и правильную последовательность пакетов.
4. IP предоставляет надежную связь, основанную на соединениях, приложениям, которые обычно передают большие объемы данных за один раз.
5. Основная обязанность IP – адресация и маршрутизация пакетов.
6. IP обеспечивает доставку пакета без установления соединения для всех других протоколов в комплекте.
7. Какое из следующих утверждений верно описывает протокол TCP? (Выберите все правильные ответы).
8. TCP обеспечивает связь без установления соединения, но не гарантирует доставку пакетов.
9. TCP предоставляет приложениям надежную связь, основанную на соединениях, которые обычно передают большие объемы данных за один раз.
10. TCP предоставляет службы, которые позволяют приложению связываться с конкретным портом и IP-адресом на узле.
11. TCP предоставляет и назначает последовательные номера каждому передаваемому сегменту данных.
12. В какой их четырех уровней набора протоколов TCP/IP входит протокол IGMP и для чего он используется?
13. Что такое многоадресная передача?
14. Перечислите протоколы транспортного уровня.
15. Какое из следующих утверждений верно описывает протокол ARP? (Выберите все правильные ответы.)
16. ARP – протокол в составе уровня Интернет.
17. ARP – протокол в составе транспортного уровня.

18. ARP обеспечивает отображение адреса IP в подуровень MAC-адреса для сопоставления контрольного физического адреса MAC получателя.

19. Основная обязанность ARP – адресация и маршрутизация пакетов между узлами.

20. Какие стандартные утилиты для обеспечения связи включает Windows XP Professional?Для каких целей они служат?

21. В каком случаем на компьютер следует назначить статический IP-адрес?

22. Какое из следующих утверждений верно описывает IP-адреса? (Выберите все правильные ответы.)

23. Логические 64-битные адреса, которые идентифицируют TCP/IP-узел.

24. Каждая плата сетевого адаптера в компьютере с запущенным TCP/IP требует уникального IP-адреса.

25. 192.169.0.108 – пример IP-адреса класса C.

26. ID узла в IP-адресе - всегда последние два октета в адресе.

27. Каково назначение маски подсети?

28. Какое из следующих утверждений об автоматическом получении IP-адреса верно? (Выберите все правильные ответы.)

29. В Windows XP Professional включена служба DHCP.

30. В Windows XP Professional включена функция автоматического назначения частных IP-адресов, которая предоставляет клиентам DHCP ограниченные сетевые возможности, если DHCP-сервер недоступен во время запуска.

31. Internet Assigned Numbers Authority (IANA) резервирует адреса от 169.254.0.0 до 169.254.255.255 для автоматического назначения частных IP-адресов.

32. Вы должны всегда запрещать автоматическое назначение частных IP-адресов в маленьких рабочих группах.

33. На вашем компьютере с Windows XP Professional выполнена ручная настройка TCP/IP. Вы можете соединиться с любым узлом в вашей собственной подсети, но вам не удается соединяться или обмениваться пакетами с любым узлом в удаленной подсети. Какова причина проблемы и как ее устранить?

34. Вы выполнили обмен пакетами с другим компьютером, локальный адрес которого возвращен как 169.254.x.y. О чем это говорит?

Лабораторная работа №5
IP адреса. Октеты. Маски подсетей.

Цель работы: изучить структуру IP адреса. Научиться преобразовывать адреса из двоичного и десятичного представлений. Научиться разбивать IP-сети на подсети и создавать надсети.

Порядок выполнения работы

1. Изучить теоретический материал.
2. Выполнить практические задания.
3. Сделать выводы на основании проделанной работы.

Краткие теоретические сведения

Для обмена данными в частной TCP/IP-сети или через Интернет, каждый сетевой узел должен обладать уникальным 32-битным IP-адресом. IP-адреса делятся на общие и частные. Первые уникальны в глобальном масштабе и используются для адресации в Интернете. Вторые ограничены диапазонами, которые обычно используются в частной сети, но не видны из Интернета [1,3,12].

Общие IP-адреса

Для обеспечения уникальности адресов сетей в сети Интернет организация IANA (Internet Assigned Numbers Authority) разделила незанятую часть пространства IP-адресов и делегировала полномочия по их распределению региональным реестрам, среди которых Asia-Pacific Network Information Center (APNIC), American Registry for Internet Numbers (ARIN) и Reseaux IP Europeens (RIPE NCC). Региональные регистраторы выделяют блоки адресов небольшому количеству крупных поставщиков интернет-услуг (ISP), которые затем выдают более мелкие блоки своим клиентам и менее крупным провайдерам. Как правило, интернет-провайдер выдает по одному общему IP-адресу на каждый напрямую подключенный к провайдеру компьютер. Этот IP-адрес может назначаться динамически в момент подключения компьютера к ISP или статически закрепляться за выделенной линией или модемным подключением.

Частные IP-адреса

Часть IP-адресов никогда не используется в Интернете. Они называются частными и используются для организации адресации в сетях, которые “не видны” в общей сети. Например, пользователю, объединяющему компьютеры в домашнюю TCP/IP-сеть, не надо назначать общие IP-адреса каждому узлу — он использует частные адреса (табл. 5.1.).

Таблица 5.1.

Диапазоны частных IP адресов

Начальный адрес	Конечный адрес
10.0.0.0	10.255.255.254
172.16.0.0	172.31.255.254
192.168.0.0	192.168.255.254

Узлы с частными IP-адресами могут подключаться к Интернету через прокси-сервер или компьютер с Windows Server 2003, сконфигурированный в качестве NAT-сервера (Network Address Translation). Windows Server 2003 также поддерживает сервис общего доступа к Интернету (Internet Connection Sharing, ICS), предоставляющий клиентам частной сети упрощенные сервисы NAT.

Методы IP-адресации

IP-адреса могут назначаться вручную, динамически (DHCP-сервером) или автоматически.

Назначение IP-адресов вручную используется нечасто, но иногда без него не обойтись. Например, ручное конфигурирование потребуется в сети, состоящей из нескольких сегментов, при отсутствии DHCP-сервера, или если IP-адрес DHCP-сервера также назначается вручную. Наконец, важным сетевым серверам, например DNS- или WINS-серверу или контроллеру домена, обычно назначают статические IP-адреса. Статические IP- адреса можно выделить по механизму резервирования DHCP-адресов, но большинство администраторов предпочитает не перепоручать это дело DHCP-серверу и назначают их вручную. Во всех остальных случаях ручное конфигурирование рекомендуется, только если невозможно

использовать DHCP. Администрирование назначенных вручную IP-адресов отнимает много времени и чревато ошибками, особенно в средних и крупных сетях.

DHCP-сервер автоматически выделяет DHCP-клиентам IP-адреса из заданных администратором диапазонов. DHCP-сервер можно настроить на конфигурирование других параметров TCP/IP, например адресов DNS- и WINS-серверов, основных шлюзов и т. п.

APIPA (Automatic Private IP Addressing) служит для автоматического назначения адресов и применяется в простых односегментных сетях без DHCP-сервера.

Также существует альтернативная конфигурация, которая позволяет назначить IP-адрес компьютерам, которым недоступен DHCP-сервер. Однако в отсутствие такого сервера компьютер с альтернативной конфигурацией не сможет использовать APIPA, даже если этот протокол будет доступен в сети. Эта функция полезна, когда компьютер работает в нескольких сетях, в одной из которых нет DHCP-сервера. Например, портативный компьютер, используемый для работы в офисе и дома. В обеих сетях используется один и тот же адаптер и локальное подключение, настроенное на автоматическое получение IP-адреса. При подключении к корпоративной сети параметры TCP/IP настраиваются DHCP-сервером. Дома DHCP-сервера нет, поэтому используется определенная альтернативная конфигурация: IP-адрес, маска подсети и основной шлюз для домашней сети.

Структура IP-адреса

IP-адреса привычно представляется в форме четырех чисел, разделенных точкой, например 192.168.233.22. Однако это лишь одна из форм IP-адреса, которая называется десятично-точечной нотацией и используется для удобства запоминания адреса. В компьютере применяется двоичная нотация, в которой все числа представлены только цифрами 1 и 0. Это “родная” форма IP-адреса. Логика IP-адресации становится понятной при рассмотрении двоичной версии IP-адреса. Для конфигурирования, управления и устранения неполадок IP-адресации нужно уметь работать с IP-адресами в двоичной форме, а также переводить их из двоичного в десятичное представление и обратно.

Преобразование двоичного и десятичного представлений

В десятично-точечной нотации каждое 32-битное число IP-адреса представляется в виде четырех десятичных групп, значение каждой из которых лежит в диапазоне 0—255, например 192.168.0.225. Эти числа представляют четыре 8-битных значения, составляющих 32-битный адрес. В любой нотации каждая из четырех групп называется октет. Но только двоичная форма позволяет наглядно увидеть значение каждого бита. Например, IP-адрес 192.168.0.225 в двоичной форме выглядит так: 11000000 10101000 00000000 11100001. В IP-адресах октеты и биты считаются слева направо. Первый октет соответствует первому слева, а биты с 1 по 8 соответствуют первым восьми битам, начиная с самого левого. Второй октет - это следующие восемь битов (9 - 16), затем идет третий октет (биты 17 - 24), а замыкает последовательность четвертый октет (биты 25 - 32). В десятично-точечной нотации октеты отделяются точками, а в двоичной - пробелами.

В таблице 5.2 показано десятичное представление битов в двоичном октете. Обратите внимание: если смотреть слева направо, то первый бит дает значение 128, а каждый последующий бит - половину значения предыдущего. И, наоборот, в направлении справа налево, начиная с восьмого бита (значение 1), цена каждого последующего бита в два раза больше, чем предыдущего.

Таблица 5. 2.

Возможные значения в бинарном октете

Октет	1-й бит	2-й бит	3-й бит	4-й бит	5-й бит	6-й бит	7-й бит	8-й бит
Десятичное представление	128	64	32	16	8	4	2	1
Пример	1	0	1	0	1	1	0	0

Вклад бита в общую сумму ненулевой, только если он содержит 1. Например, если первый бит — 1, то ему соответствует десятичное значений 128. Если же его значение — 0, то и десятичное значение равно нулю. Октету со всеми битами; равными 1, соответствует

десятичное значение 255. Если все биты содержат 0, десятичное значение октета равно 0.

Пример перевода из двоичной нотации в десятичную

Пусть первый октет IP-адреса в двоичном представлении выглядит так:

10101100 .

Первый, третий, пятый и шестой биты содержат 1, а остальные - 0. Для упрощения решения нарисуем таблицу перевода, в которой отобразим возможные веса битов октета:

128	64	32	16	8	4	2	1
1	0	1	0	1	1	0	0

сложим десятичные эквиваленты каждого бита и найдем десятичную сумму октета: 1-й бит (128) + 3-й бит (32) + 5-й бит (8) + 6-й бит (4) = сумма октета (172) Поскольку сумма составляет 172, первый октет нашего IP-адреса в десятичной форме равен 172. Применив этот же метод, можно преобразовать полный IP-адрес вида 10101100 00010001 00000111 00011011 в десятично-точечное представление: 172.17.7.27.

Пример перевода из десятичной нотации в двоичную

Перевод октета из десятичной формы в двоичную осуществляется записью 1 или 0 в соответствующий бит октета слева направо, пока не будет получено искомое десятичное число. Если запись 1 в очередной бит приводит к тому, что полученная сумма превосходит десятичное число, просто запишите в этот бит 0 и перейдите к следующему. Допустим, надо перевести IP-адрес 172.31.230.218 в двоичный вид. Первым делом запишите последовательность возможных весов битов в таблицу.

Начнем с первого числа — 128. Поскольку 128 меньше 172, запишем 1 в первый бит, а наша промежуточная сумма будет 128. Затем посмотрим вес второго бита — 64. Так как 128 + 64 больше 172, второй бит установим в 0. Затем перейдем к третьему биту, вес которого — 32. 128 и 32 в сумме дают меньше 172, поэтому запишем в

этот бит 1. Промежуточная сумма становится 128 + 0 + 32=160. Перейдем к четвертому биту, его вес — 16. 160 и 16 в сумме дают больше 172, поэтому пишем 0. Вес пятого бита — 8. Сумма 160 + 8 меньше 172, пишем в пятый бит 1, а промежуточная сумма становится 128 + 0 + 32 + 0 + 8 = 168. И наконец вес шестого бита — 4, сумма 168 и 4 равна 172, т. е. искомому числу. Поэтому пишем 1 в шестой бит, а оставшиеся седьмой и восьмой биты заполняем нулями.

Таким образом, первый октет в двоичной форме выглядит так: 10101100

Выполнив аналогичные операции с остальными октетами получим двоичное представление адреса 172.31.230.218: 10101100 00011111 11100110 11011010

Идентификаторы сети и узла

Маршрутизаторы, переправляющие пакеты данных между TCP/IP-сетями не обязаны знать, какому именно узлу предназначен тот или иной IP-пакет. Вместо этого маршрутизатор считывает из IP-пакета только адрес сети, в которой находится узел — приемник пакета, а затем на основе своей таблицы маршрутизации определяет, каким образом доставить пакет в сеть, в которой расположен адресат. Точное местоположение узла определяется только после доставки пакета в нужный сегмент сети.

Такой механизм маршрутизации возможен благодаря делению IP-адреса на два компонента:

• идентификатор сети (network ID) — первая часть IP-адреса, представляющая конкретную сеть в более крупной TCP/IP-сети (например, в Интернете);

• идентификатор узла (host ID) — вторая часть IP-адреса, определяющая узел TCP/IP (рабочую станцию, сервер, маршрутизатор или любое другое TCP/IP-устройство). Например, разбиение IP-адреса (131.107.16.200) на идентификаторы сети (это первые два октета — 131.107) и узла (последние два октета — 16.200).

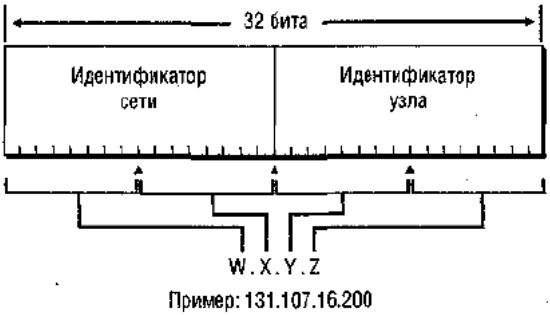


Рис. 5.1. Идентификаторы сети и узла

Маска подсети

Еще один необходимый для нормальной работы TCP/IP параметр — маска подсети (subnet mask), которая служит для определения, в какой сети находится приемник пакета — локальной или внешней. Маска подсети — это 32-битный адрес, представляющий собой последовательность битов со значением 1, который используется для выделения, или маскировки, идентификатора сети адреса назначения пакета и отделения идентификаторов сети и узла. Каждому узлу сети TCP/IP нужна маска подсети (если сеть не разбита.на подсети, т. е. состоит из одной подсети) или маска по умолчанию (в случае разбиения сети на подсети).

Например, такое 32-битное число представляет маску подсети по умолчанию для узлов с адресами класса B (например 172.20.16.200):

11111111 11111111 00000000 00000000 (255.255.0.0)

Когда TCP/IP-узел с адресом 172.20.16.200 отправляет пакет по адресу 172.21.17.201, он сначала выполняет побитовую операцию И по отношению к локальным адресу и маске подсети. Поскольку эта логическая операция в результате дает 0 во всех битах кроме тех, в который в обоих операндах стояли 1, то 172.20.16.200 И 255.255.0.0 = 172.20.0.0

Затем узел повторяет эту операцию, но вместо адреса отправителя подставляет адрес получателя. В результате получается 172.21.0.0. Затем TCP/IP сравнивает результаты этих операций. Если они

совпадают, получатель расположен в этой же подсети. Иначе приемник и получатель расположены в разных подсетях.

Длина префикса сети в маске подсети

Биты идентификатора сети всегда идут последовательно и начинаются с самого левого, поэтому самый простой способ показать маску подсети — это указать количество битов идентификатора сети в виде префикса сети. Таким образом, маска подсети выражается в виде IP-адрес/префикс сети. Например, IP-адрес 131.107.16.200 и маску подсети 255.255.0.0 можно записать в виде 131.107.16.200/16. Число 16 после слеша обозначает количество единичных битов в маске подсети. Точно так же, /24 обозначает маску подсети 255.255.255.0 для адреса класса C, например 206.73.118.23/24.

Нотация с префиксом сети также известна как бесклассовая междоменная маршрутизация (Classless Interdomain Routing, CIDR).

Таблица 5.3.

Маска подсети

Класс адреса	Маска подсети по умолчанию в двоичном виде	Префикс сети и десятичный эквивалент
Класс A	11111111 00000000 00000000 00000000	/8; 255.0.0.0
Класс B	11111111 11111111 00000000 00000000	/16; 255.255.0.0
Класс C	11111111 11111111 11111111 00000000	/24; 255.255.255.0

Основной шлюз

Связь между TCP/IP-узлами разных сетей, как правило, выполняется через маршрутизаторы. Маршрутизатор — это устройство с несколькими интерфейсами, подключенными к разным сетям, а маршрутизация — процесс приема IP-пакетов на одном интерфейсе и пересылка их на другой интерфейс в направлении адресата. С точки зрения узла сети TCP/IP, основной шлюз — это IP-адрес маршрутизатора, сконфигурированного на пересылку IP-трафика в другие сети. Пытаясь передать информацию другому узлу IP-сети, компьютер определяет тип узла (локальный или удаленный) по маске подсети. Если узел-получатель расположен в локальном сегменте сети,

пакет направляется в локальную сеть по методу широковещания. В противном случае компьютер пересылает пакет в основной шлюз, определенный в параметрах TCP/IP. Обязанность дальнейшей пересылки пакета в нужную сеть возлагается на маршрутизатор, адрес которого указан в качестве основного шлюза.

Разбиение IP-сетей на подсети и создание надсетей

Маски подсети позволяют настраивать адресное пространство в соответствии с требованиями к сети. Разбиение на подсети позволяет организовать иерархическую структуру сетей, а надсети и CIDR позволяют объединить разные сети в едином адресном пространстве.

Маски подсети помогают определить, как IP-адрес разбивается на идентификаторы сети и узла. В адресах классов A, B и C применяются стандартные маски подсети, занимающие соответственно первые 8, 16 и 24 бита 32-битового адреса. Подсетью называется логическая сеть, определяемая маской подсети.

Стандартные маски годятся для сетей, которые не предполагается разбивать. Например, в сети из 100 компьютеров, соединенных с помощью карт гигабитного Ethernet, кабелей и коммутаторов, все узлы могут обмениваться информацией по локальной сети. Сеть не нуждается в маршрутизаторах для защиты от чрезмерного широковещания или для связи с узлами, расположенными в отдельных физических сегментах. В таком простом случае вполне достаточно идентификатора сети класса C.

Механизм разбиения на подсети

Разбиение на подсети (subnetting) представляет собой логическое разделение адресного пространства сети путем установки в 1 дополнительных битов маски подсети. Такое расширение позволяет создавать множество подсетей в адресном пространстве сети.

Например, если маска подсети по умолчанию 255.255.0.0 используется для узлов сети класса B 131.107.0.0, IP-адреса 131.107.1.11 и 131.107.2.11 находятся в одной подсети и поддерживают взаимодействие посредством широковещания. Но если расширить маску подсети до 255.255.255.0, то эти адреса окажутся в разных подсетях и для обмена данными соответствующим узлам придется пересылать пакеты на основной шлюз, который перенаправит дейтаграммы в нужную подсеть. Внешние по отношению к сети узлы по-прежнему используют маску подсети по умолчанию для взаимодействия с узлами внутри сети. Обе версии показаны на рис. 5.2. и 5.3.

Показанное на рис. 5.2 исходное адресное пространство класса B, состоящее из единственной подсети, может содержать максимум 65 534 узлов, а новая маска подсети (рис. 5.3) позволяет разделить адресное пространство на 256 подсетей, в каждой из которых можно разместить до 254 узлов.

Разбиение на подсети часто используют для обеспечения соответствия физической и логической топологии сети или для ограничения широковещательного трафика. Другие несомненные преимущества: более высокий уровень защиты (благодаря ограничению неавторизованного трафика маршрутизаторами) и упрощение администрирования (благодаря передаче управления подсетями другим отделам или администраторам).

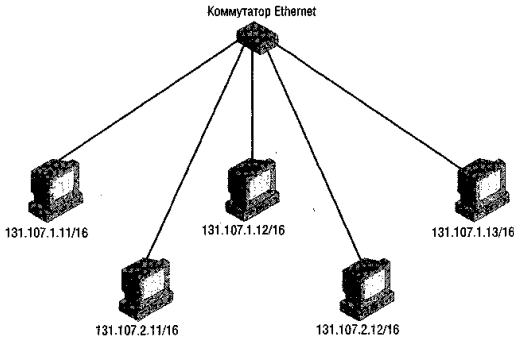


Рис. 5.2. Неразбитое на подсети адресное пространство класса B

Единственный сегмент сети 131.107.0.0/16.

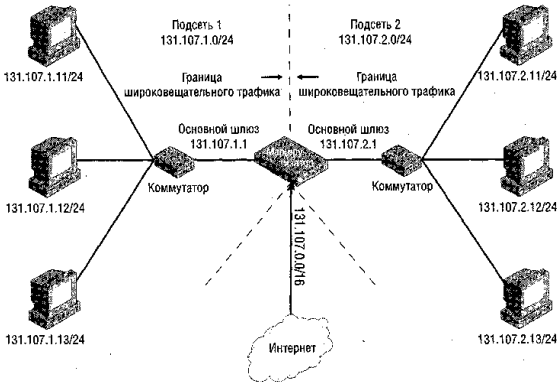


Рис. 5.3. Разбитое на подсети адресное пространство класса B

Ограничение широковещательного трафика

Широковещание — это рассылка сообщений с одного компьютера на все расположенные в локальном сегменте устройства. Широковещание существенно нагружает ресурсы, поскольку занимает полосу пропускания и требует участия всех сетевых адаптеров и процессоров логического сегмента сети.

Маршрутизаторы блокируют широковещание и защищают сети от излишнего трафика. Поскольку маршрутизаторы также определяют логические ограничения подсетей, разбиение на подсети позволяет косвенно ограничивать широковещательный трафик в сети.

Определение максимального количества узлов в сети

Зная сетевой адрес, определить максимальное количество узлов в сети просто: надо возвести 2 в степень, равную количеству битов в идентификаторе узла, и вычесть 2. Например, в сетевом адресе 192.168.0.0/24 под идентификатор узла отведено 8 бит, поэтому возможное максимальное число узлов 2s — 2 = 254.

208.147.66.192/26

ID подсети (в двоичном виде):11

Исключение идентификаторов узла, состоящих из одних нулей или одних единиц.

Значение 2x показывает общее количество комбинаций значений битов двоичного числа x, включая комбинации из одних нулей и одних единиц. Например, 23 дает 8, т. е. количество различных комбинаций из 3 битов (дес. означает десятичную систему счисления):

000 = 0 (дес.)
001 = 1 (дес.)
010 = 2 (дес.)
011 = 3 (дес.)
100 = 4 (дес.)
101 = 5 (дес.)
110 = .6 (дес.)
111 = 7 (дес.)

Однако узлам нельзя назначать адреса, состоящие из одних только нулей или единиц, поскольку они зарезервированы для других целей. Идентификатор узла, состоящий из одних нулей, на самом деле определяет сеть без указания конкретного узла. Идентификатор узла из одних единиц зарезервирован в протоколе IP для широковещания (передачи сообщения всем узлам сети). При подсчете максимального количества узлов в сети эти варианты надо исключить из рассмотрения (т. е. вычесть из него 2).

Определение емкости подсети

При увеличении количества битов в маске подсети для создания подсетей в адресном пространстве идентификатор узла укорачивается, и создается новое адресное пространство для идентификатора подсети.

Чтобы определить количество доступных в адресном пространстве подсетей, просто возведите 2 в степень y, где y — количество бит в идентификаторе подсети. Например, если в адресном пространстве 172.16.0.0/16 выделить 8 бит на адрес подсети (т. е. привести к виду 172.16.0.0/24), количество доступных подсетей станет 2s, или 256. Из него не надо вычитать 2, поскольку большинство современных маршрутизаторов принимают идентификаторы подсетей только из единиц или нулей.

Планируя адресное пространство и маски подсети, следует учитывать, что отведенных на идентификатор подсети бит достаточно

для размещения всех подсетей, а также обеспечен резерв для расширения сети в будущем. Любую физическую сеть нужно рассматривать как подсеть.

Калькулятор позволяет быстро определить необходимое число бит для идентификатора подсети. Вычтите 1 из требуемого количества подсетей в десятичном формате, переведите результат в двоичный вид и посчитайте количество бит в нем. Например, если нужна 31 подсеть, введите 30 и установите переключатель Bin. Полученное число НПО говорит, что под идентификатор подсети нужно зарезервировать 5 бит.

Количество узлов в подсети

Количество идентификаторов узлов в подсети определяется так же, как и узлов в сети — оно равно 2x — 2, где x — количество бит в идентификаторе узла. Например, в адресе 172.16.0.0/24 резервируется 8 бит под идентификатор узла, поэтому число узлов в подсети равно 28 — 2, т. е. 254. Для вычисления количества узлов во всей сети умножают полученный результат на количество подсетей.

В нашем примере адресное пространство 172.16.0.0/24 дает 254 сетей * 256 узлов = 65 024.

Конфигурируя адресное пространство и маски подсети в соответствии с требованиями сети следует учитывать, что на идентификатор узла отведено достаточно бит с учетом возможного увеличения количества узлов в подсети в будущем.

Калькулятор позволяет быстро определить необходимое количество бит для идентификатора узла. Прибавьте 1 к требуемому количеству узлов в подсети в десятичном формате, переведите результат в двоичный вид и посчитайте количество бит в нем. Например, если нужно 33 узла в подсети, введите 34 и установите переключатель Bin. Результат 100010 говорит о том, что нужно зарезервировать 6 бит под идентификатор подсети.

В предыдущем примере мы расширили маску подсети для адресного пространства 172.16.0.0/16 до 255.255.255.0, увеличив ее на целый октет. На практике маску расширяют более мелкими порциями, вплоть до отдельных битов.

Определение диапазонов адресов подсети

Десятично-точечная форма маски подсети позволяет определить диапазоны IP-адресов в каждой подсети простым вычитанием из 256 числа в соответствующем октете маски.

Например, в сети класса C с адресом 207.209.68.0 с маской подсети 255.255.255.192 вычитание 192 из 256 даст 64. Таким образом, новый диапазон начинается после каждого 64 адреса: 207.209.68.0-207.209.68.63, 207.209.68.64-207.209.68.127 и т.д. В сети класса B 131.107.0.0 с маской подсети 255.255.240.0 вычитание 240 из 256 дает 16. Следовательно, диапазоны адресов подсетей группируются по 16 в третьем октете, а четвертый октет принимает значения из диапазона 0—255: 131.107.0.0—131.107.15.255, 131.107.16.0— 131.107.31.255 и т. д.

Узлам нельзя назначать идентификаторы из одних нулей или единиц, так что исключаются первый и последний адрес каждого диапазона.

Сложение маршрутов путем создания надсетей

Чтобы предотвратить истощение доступных идентификаторов сетей старших классов, организации, ответственные за адресацию в Интернете, предложили схему, называемую созданием надсетей (supernetting), согласно которой несколько сетей (маршрутов) можно объединить (или сложить) в единую более крупную сеть. Надсети позволяют эффективнее управлять выделением участков адресного пространства.

Допустим, организации нужно объединить в сеть 2000 узлов. Это слишком много для одной сети класса C, которая поддерживает не более 254 узлов. Сеть класса B поддерживает 65 534 узла, но таких сетей возможно всего 16 383 и количество свободных стремительно сокращается. Интернет-провайдеру нет смысла (да и возможности) выделять сети класса B клиентам, которые будет использовать только 3% диапазона адресов.

Надсети позволяют интернет-провайдеру выделить клиенту блок адресов класса C, который будет рассматриваться как единая сеть, представляющая собой нечто среднее между классами C и B. В нашем

примере блок из 8 идентификаторов сети класса С даст возможность организации объединить в сеть до 2032 узлов.

Надсети отличаются от подсетей тем, что заимствуют биты идентификатора сети и маскируют их как идентификатор узла. Допустим, интернет-провайдер выделил блок из 8 адресов сети: 207.46.168.0—207.46.175.0. Если определить на маршрутизаторах провайдера и всех узлов сети маску подсети /21 (вместо /24 по умолчанию), все сети будут казаться единственной сетью из-за того, что их идентификаторы (урезанные до 21 бита) будут выглядеть одинаково (рис. 5.4).

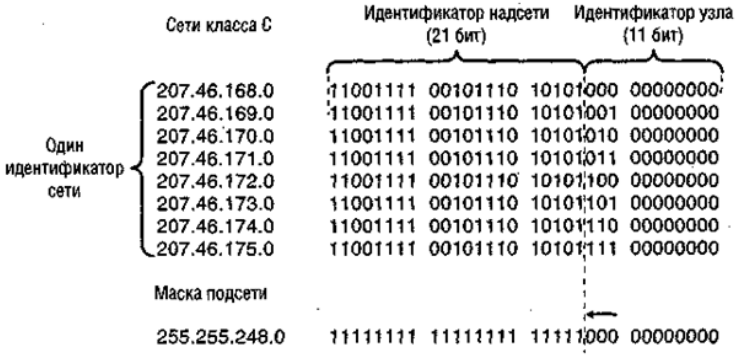


Рис. 5.4 Надсеть на основе блока адресов класса С

Использование бесклассовой междоменной маршрутизации

CIDR - это эффективный метод поддержки надсетей с помощью таблиц маршрутизации. Не будь CIDR, в таблицах маршрутизации следовало бы размещать отдельные записи для каждой сети в надсети, а так вся надсеть представляется одной записью.

Выделенные региональными регистраторами Интернета или интернет-провайдерами блоки адресов надсети часто называют CIDR-блоками, а термин CIDR часто используется для обозначения самих надсетей.

CIDR не совместим с устаревшим протоколом RIP (Routing Information Protocol) версии 1, который применялся в старых маршрутизаторах, и требует, чтобы маршрутизатор использовал

бесклассовый протокол маршрутизации, такой как RIP версии 2 или OSPF (Open Shortest Path First).

Использование CIDR для выделения адресов дает новую жизнь идентификаторам сети. CIDR-блок из предыдущего примера (131.107.0.0, 255.255.248.0) можно рассматривать двояко:

• как блок 8 адресов сетей класса C;

• как адресное пространство, в котором зафиксирован 21 бит, а 11 битов доступны для изменения.

Во втором случае идентификаторы сети освобождаются от классовой наследственности и становятся частью бесклассового пространства IP-адресов. Каждый идентификатор сети независимо от длины представляет адресное пространство, в котом биты идентификатора сети зафиксированы, а биты узла можно менять. Биты узла можно использовать в качестве идентификаторов узлов или в других целях (допустим, для организации подсетей) и таким образом наилучшим образом удовлетворить потребности организации в поддержке сетей.

Маски подсети переменной длины

Традиционно все узлы и маршрутизаторы организации используют одну маску подсети. В этом случае сеть может разбиваться на подсети, в которых максимальное количество идентификаторов узлов одинаковое.

Однако поддержка масок подсети переменной длины (variable-length subnet mask, VLSM) позволяет маршрутизаторам обслуживать разные маски. Чаще всего VLSM применяют для разбиения на подсети самих подсетей. Допустим, большой организации принадлежит большое адресное пространство 131.107.0.0/16. Внешние маршрутизаторы для определения идентификатора сети используют первые 16 бит адреса и в соответствии с этим осуществляют маршрутизацию. При получении данных из Интернета маршрутизаторы организации используют маску подсети /22 для перенаправления трафика в любой из 64 региональных отделений организации. А маршрутизаторы региональных офисов в свою очередь

используют маску подсети /25 для маршрутизации трафика в 8 отделов в рамках отделения.

Как и CIDR, работа масок подсетей переменной длины основана на бесклассовых протоколах маршрутизации, таких как RIP версии 2 и OSPF. VRLM несовместим с более старыми протоколами маршрутизации (например с RIP версии 1).

Использование VLSM для поддержки подсетей разного размера

VLSM также позволяет разбивать сеть на подсети разных размеров на одном уровне иерархии и более эффективно использовать адресное пространство.

Например, если одна подсеть должна объединять 100 компьютеров, вторая — 50, а третья — 20, то не удастся обойтись традиционной маской по умолчанию для единственного идентификатора сети класса С. Как видно из таблицы 5.4, никакая из масок подсети по умолчанию не обеспечивает одновременно достаточное число подсетей и узлов в подсети.

В таких ситуациях проблему решает VLSM. При этом не надо обращаться к интернет-провайдеру за новым диапазоном адресов.

При разбиении на подсети различного размера нужно использовать специальный шаблон с завершающими нулями; сеть класса С поддерживает до семи подсетей. Завершающие нули нужны для предотвращения пересечения адресных пространств подсетей.

Таблица 5.4.

Параметры маски подсети класса С (статическое)

Сетевой адрес	Число подсетей	Число узлов в подсети
208.147.66.0/24	1	254
208.147.66.0/25	2	126
208.147.66.0/26	4	62
208.147.66.0/27	8	30

Если идентификатор подсети с маской переменной длины соответствует шаблону из таблицы 5.5, подсети не пересекутся, и адреса будут интерпретироваться однозначно.

Таблица 5.5

Идентификаторы подсети на основе VLSM

Номер сети	Идентификатор подсети	Маска подсети	Количество узлов	Пример адреса подсети
1	0	255.255.255.128	126	192.168.233.0/25
2	10	255.255.255.192	62	192.168.233.128/25
3	110	255.255.255.224	30	192.168.233.192/27
4	1110	255.255.255.240	14	192.168.233.224/28
5	11110	255.255.255.248	6	192.168.233.240/29
6	111110	255.255.255.252	2	192.168.233.248/30
7	1111110	255.255.255.252	2	192.168.233.252/30

Увеличение количества доступных узлов средствами VLSM

В табл. 5.5 последняя подсеть имеет такое же количество узлов, как и шестая, отличаются только идентификаторы подсети, да и то всего одним битом (в идентификаторе 7-й сети в отличие от остальных отсутствует завершающий нуль). Можно не использовать все семь подсетей — достаточно определить состоящий из одних единиц идентификатор подсети на любом уровне, который заменит все перечисленные в следующих строках таблицы подсети. Например, определить идентификатор подсети 1111, который заменит подсети 5—7 (таблица 5). Благодаря этому вы получите еще одну подсеть с 14 узлами вместо 3 подсетей, вместе содержащих только 10 узлов. Это позволит максимизировать количество узлов, которые вмещает сеть, состоящая из 5 подсетей.

Если сеть класса C разбита на 3, 5, 6 или 7 подсетей, VLSM позволяет максимизировать количество доступных узлов.

Задания к лабораторной работе

1. Перевод числа из десятичного представления в двоичное вручную и наоборот.

Число в десятичном представлении:	Число в двоичном представлении
159	
65	
	1001010
	01110011

2. Какое из перечисленных далее двоичных значений соответствует адресу 207.209.68.100?

a. 11001111 11010001 01000100 01100100.

b. 11000111110100010100100 01100100.

c. 11001111101000101000100 01101100.

d. 11001111 11010001 11001101 01100100.

3. Какое из перечисленных далее десятично-точечных значений соответствует двоичному адресу 11001100 00001010 11001000 00000100?

a. 204.18.200.3.

b. 204.34.202.4.

c. 204.10.200.44.

d. 204.10.200.4.

2. Преобразование маски подсети из десятично-точечной формы в форму с префиксом сети и обратно.

Преобразуйте нестандартную маску подсети из десятично-точечной формы в форму с префиксом сети и наоборот.

1. 255.255.255.192.

2. 255.255.252.0.

3. /27.

4. /21.

3. Интернет-провайдер выделил адрес сети 206.73.118.0/24. Заполните таблицы, указав количество бит, необходимое для идентификаторов подсети или узла, число бит, оставшееся на

идентификатор узла или подсети, маску подсети в виде префикса сети и маску подсети в десятично-точечном виде. При заполнении отталкивайтесь от требований, указанных над таблицей.

Требование	Количество бит, необходимое для идентификатора подсети	Оставшееся на идентификатор узла количество бит	Маска подсети (в виде префикса сети)	Маска подсети (в десятично-точечном виде)
6 подсетей	3	5	/27	255.255.255.224
9 подсетей				
3 подсети				
20 узлов на подсеть				

4. Определите класс сети и маску подсети по умолчанию для каждого приведенного в таблице идентификатора сети. Затем вычислите действительную маску подсети, назначенную адресу, доступное количество подсетей и количество узлов в каждой подсети.

Идентификатор сети	класс сети	маска по умолчанию	заданная маска подсети	доступное количество подсетей	доступное кол-во узлов в подсети
192.168.212.0/28					
151.142.0.0/21					
8.0.0.0/12					
205.168.75.0/26					

6. С помощью логической функции “И” определить, принадлежат ли два адреса одной и той же логической подсети.

Адрес №1	Адрес №2	Результат
192.168.212.45/26	192.168.233.46/25	
172.22.222.45/17	172.22.212.48/18	

Контрольные вопросы

1. Перечислите диапазоны частных адресов для каждого класса.

2. Какие методы IP-адресации вы знаете? В каком случае применяется ручная IP-адресация?
3. Какова структура IP-адреса?
4. Для каких целей используются договоренности об особых адресах?
5. Что такое маска подсети и для чего она используется?
6. Что такое основной шлюз?
7. Что такое надсети? Опишите механизм разбиения на надсети.
8. Что такое широковещание?
9. Как определить максимальное число узлов в сети?
10. Каким образом определяется число узлов в подсети и ее диапазоны?
11. Что такое нотация CIRD?
12. Каковы особенности использования масок подсети переменной длины?
13. Для чего используется VLSM?
14. Возможно ли увеличение числа доступных узлов средствами VLSM?

Лабораторная работа № 6

Создание и управление учетными записями пользователей

Цель работы: Приобретение навыков планирования, создания и обслуживания учетных записей пользователей в Microsoft Windows.

В Windows XP Professional используются три типа учетных записей пользователей: локальные учетные записи пользователей, учетные записи пользователей домена и встроенные учетные записи пользователей [2, 7, 12].

Локальная учетная запись пользователя позволяет начать сеанс на компьютере и воспользоваться его ресурсами.

Учетная запись пользователя домена позволяет войти в домен и воспользоваться сетевыми ресурсами.

Встроенная учетная запись пользователя позволяет выполнить административные задачи и воспользоваться локальными или сетевыми ресурсами.

Локальные учетные записи пользователей

Локальные учетные записи пользователей позволяют начать сеанс на компьютере, на котором они были созданы, и воспользоваться ресурсами только этого компьютера. Когда администратор создает локальную учетную запись пользователя, Windows XP Professional создает учетную запись в базе данных политик безопасности лишь для этого компьютера. Ее называют *базой данных политик безопасности локального компьютера.* Windows XP Professional использует базу данных политик безопасности локального компьютера для аутентификации локальной учетной записи пользователя, что позволяет пользователю войти в систему на этом компьютере. Windows XP Professional не копирует локальную информацию об учетных записях пользователя на какой-либо другой компьютер.

Рекомендуется использовать локальные учетные записи пользователей только на компьютерах в рабочих группах. Если создается локальная учетная запись пользователя в рабочей группе из пяти компьютеров на платформе Windows XP Professional, например

User1 на Computer1, то, используя учетную запись Userl, можно войти в систему только на Computer1. Если нужен доступ под именем User1 ко всем пяти компьютерам этой рабочей группы, то следует создать локальную учетную запись Userl на всех пяти компьютерах. Кроме того, когда необходимо будет изменить пароль для Userl, то это придется сделать на всех пяти компьютерах, потому что каждый компьютер имеет свою собственную базу данных локальных политик безопасности.

Домен не распознает локальные учетные записи пользователей, поэтому не следует создавать локальные учетные записи пользователей в системах на платформе Windows XP Professional, которые являются частью домена. В противном случае не удастся воспользоваться ресурсами домена, а администратор домена не сможет управлять локальными учетными записями или предоставить разрешения на доступ к ресурсам домена.

Учетные записи пользователей домена

Учетные записи пользователей домена позволяют войти в домен и воспользоваться сетевыми ресурсами. При входе в систему пользователь предоставляет имя пользователя и пароль. Microsoft Windows 2003 Server использует эту информацию для аутентификации пользователя и предоставления маркера доступа, который содержит данные пользователя и параметры безопасности. Маркер доступа идентифицирует пользователя для компьютеров в домене, в котором он хочет воспользоваться сетевыми ресурсами. Маркер доступа действителен до конца сеанса пользователя.

Чтобы получить учетную запись пользователя домена, необходимо быть членом домена. Домен можно создать при использовании, по меньшей мере, одной системы на какой-либо платформе семейства Windows 2003 Server, имеющей статус контроллера домена со службой каталогов Active Directory,

Учетная запись администратора

Встроенная учетная запись администратора используется для полного управления компьютером. Она позволяет выполнять

административные задачи, такие как, создание и изменение учетных записей пользователей и групп, управление политиками безопасности, создание ресурсов печати и предоставление пользовательским учетным записям разрешения и права на доступ к ресурсам.

Если требуется войти в систему под именем администратора с использованием экрана приветствия, то надо дважды нажать Ctrl+Alt+Delete. Windows XP Professional выведет окно входа в систему, позволяющее войти в систему под именем администратора. Учетная запись администратора на экране приветствия не появляется в случае, если вы находитесь в среде рабочей группы, экран приветствия не отключен, и вы создали какую-либо учетную запись во время установки.

Будучи администратором, можно создать учетную запись пользователя для выполнения неадминистративных задач и работать под учетной записью администратора только при выполнении административных задач.

Учетную запись администратора удалить нельзя. Рекомендуется переименовывать встроенную учетную запись администратора для обеспечения наибольшей безопасности. Следует использовать имя, отличающееся от Administrator, что затруднит несанкционированный доступ в систему.

Учетная запись администратора активирована по умолчанию, однако ее можно отключить, воспользовавшись оснасткой **Политика групп**.

Гостевая учетная запись

Встроенную учетную запись гостя следует использовать для предоставления прав на вход в систему и доступ к ресурсам случайным пользователям. Например, сотруднику, которому нужен доступ к ресурсам на короткое время.

Гостевой доступ следует использовать только в сетях с низким уровнем безопасности. Всегда назначайте пароль для этой учетной записи. Учетную запись гостя можно переименовать, но не удалить.

Планирование новых учетных записей пользователей

Для упрощения процесса создания учетных записей пользователей планируют и организуют информацию об учетных записях пользователей, используя:

• соглашения о назначении имен;

• требования к паролю.

Соглашение о назначении имен (naming convention) — это установленный корпоративный стандарт для идентификации пользователей в домене. Последовательная политика назначения имен помогает администраторам и пользователям держать в памяти имена учетных записей. Это также упрощает администраторам систематизирование учетных записей при добавлении их в группы или администрировании. Ниже перечислены некоторые правила назначения имен в вашей организации.

1. Локальные имена учетных записей пользователей должны быть уникальны в системах, где создаются. Имена учетных записей пользователей домена должны быть уникальны в каталоге домена.

2. Следует использовать не более 20 символов. Имена учетных записей могут содержать до 20 символов верхнего или нижнего регистра. В поле разрешается ввести более 20 символов, но Windows XP Professional использует только первые 20.

3. Имена учетных записей нечувствительны к регистру. Для создания уникальных учетных записей пользователей можно использовать комбинацию специальных и алфавитно-цифровых символов. Имена учетных записей нечувствительны к регистру, однако Windows XP Professional сохраняет регистр в целях визуального восприятия.

4. Не следует использовать недопустимые символы " / \ [ ]: ; ! = , + * ? < >.

5. Следует определится, как называть двух пользователей со схожими именами. Например, можно создать имя, состоящее из имени, второго инициала и других букв фамилии. Одного из двух пользователей по имени John Evans можно назвать johne. А другого

johnev. Также можно задать для каждого номер, например johne1 и johne2.

6. Определите категорию служащего. Некоторые организации предпочитают отразить статус временных служащих в их учетных записях. Например, перед именем добавить T и дефис (T-johne) или использовать скобки в конце имени — johne (Temp).

7. В целях безопасности следует переименовать встроенные учетные записи администратора и гостя.

В целях безопасности каждая учетная запись пользователя должна иметь пароль.

Во избежание несанкционированного доступа всегда следует назначать пароль для учетной записи администратора.

Следует определить, кто имеет право изменять пароли: администратор или пользователи. Можно назначить уникальные пароли учетным записям пользователей самостоятельно и запретить пользователям их изменять или позволить пользователям задать свои собственные пароли во время первого сеанса. В большинстве случаев пользователям следует предоставить возможность изменить пароль.

Следует использовать пароли, которые трудно угадать. Избегайте паролей содержащих, например, имена членов семьи.

Пароли могут содержать до 128 символов; минимальная рекомендуемая длина — 8 символов.

Следует использовать символы как верхнего, так и нижнего регистра (в отличие от имен пользователей, пароли чувствительны к регистру), цифры и прочие допустимые символы.

Создание, изменение и удаление учетных записей пользователей

В Windows XP Professional изменять и удалять учетные записи пользователей разрешается двумя способами: с помощью категории панели управления Учетные записи пользователей и оснастки Управление компьютером (рис. 6.1).

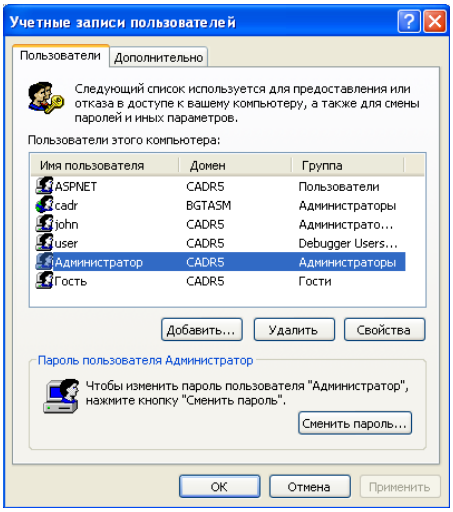


Рис. 6.1 Категория Учетные записи пользователей

Пользователь из группы администраторов может выполнять следующие задачи:

• изменить учетную запись (включая удаление учетной записи);

• создать новую учетную запись пользователя;

• изменить способ входа в систему.

Изменение учетной записи

Для изменения учетной записи необходимы административные реквизиты. В разделе **Изменение учетной записи** можно изменить любую учетную запись пользователя на компьютере. При входе в систему под учетной записью пользователя, состав группы **Выберите задание** видоизменяется — в ней находятся лишь некоторые из команд, доступных администратору.

Изменение имени. Изменяет имя учетной записи пользователя. Увидеть эту команду можно только с правами администратора, потому что только администратору разрешено выполнять эту задачу.

Создание пароля. Создает пароль для учетной записи. Увидеть эту команду можно, только если учетная запись пользователя не имеет

пароля. Только администратору разрешено создавать пароли для других учетных записей пользователей.

Изменение пароля. Изменяет пароль учетной записи. Увидеть эту команду вместо опции **Создание пароля** можно, только если для учетной записи пользователя уже назначен пароль. Лишь администратор имеет право изменять пароли других учетных записей пользователей.

Удаление пароля. Удаляет пароль учетной записи на компьютере. Увидеть эту команду можно, только если для учетной записи пользователя уже назначен пароль. Только администратор имеет право удалять пароли других учетных записей пользователей.

Изменение изображения. Изменяет изображение, которое появляется на экране приветствия. Только администратор имеет право изменять изображение других учетных записей пользователей.

Изменение типа учетной записи. Изменяет тип указанной учетной записи. Только администратор имеет право изменять тип учетной записи пользователя.

Использовать паспорт .NET. Запускает Мастер паспорта .NET. Паспорт позволяет проводить интерактивные сеансы связи с семьей и друзьями, создавать собственные личные Web-страницы и регистрироваться в любых службах и на сайтах с поддержкой .NET. Можно создать паспорт .NET только для собственной учетной записи.

Удаление учетной записи. Удаляет указанную учетную запись пользователя. Это может сделать только администратор.

При удалении учетной записи пользователя Windows XP Professional выводит окно **Хотите сохранить файлы, принадлежавшие имя_учетной_записи**. Если щелкнуть **Сохранить файлы**, Windows XP Professional сохранит содержимое рабочего стола и папки **Мои документы** этой учетной записи на рабочий стол в новую папку с именем имя_учетной_записи. Сообщения электронной почты, избранное из Интернета и другие параметры настройки при этом теряются.

Создание учетной записи пользователя

Создавать новые учетные записи пользователей могут только администраторы. Эта команда доступна в группе **Выберите задание**,

только если при входе в систему под именем члена группы администраторов.

Чтобы создать новую учетную запись пользователя, выполните следующие действия:

1. Щелкните **Пуск**, **Панель управления** и **Учетные записи пользователей**.

2. В окне **Учетные записи пользователей** щелкните **Создать новую учетную запись**. Появляется окно **Задайте имя новой учетной записи**.

3. В поле **Введите имя для новой учетной записи** введите имя пользователя (до 20 символов) и щелкните **Далее**. Появляется окно **Выбор типа учетной записи**. В Windows XP Professional можно создать два типа учетных записей: «администратор компьютера» и «ограниченная учетная запись».

4. Выберите нужный тип учетной записи и щелкните **Создать учетную запись**.

Изменение способа начала и завершения сеанса пользователя

Только администраторы имеют право изменять параметры начала и завершения сеанса пользователя на компьютере. Эта возможность доступна только при входе в систему под именем члена группы администраторов.

Два флажка изменяют параметры начала и завершения сеансов всех пользователей компьютера:

2. **Использовать экран приветствия.** Если флажок установлен, достаточно щелкнуть свою учетную запись пользователя на экране приветствия, чтобы войти в систему. Если снять флажок, придется ввести свое имя пользователя и пароль в окне входа в систему.

3. **Использовать быстрое переключение пользователей.** Если флажок установлен, то можно быстро переключиться на другую учетную запись пользователя, не завершая сеанс и не закрывая все запущенные программы. По окончании работы можно вернуться к первой учетной записи.

Раздел **Выбор изменяемой учетной записи** категории **Учетные записи пользователей** доступен только при входе в систему под именем члена группы администраторов. В нем можно выбрать учетную запись пользователя, которую вы хотите изменить. Изменения, разрешенные в учетной записи, зависят от типа вашей учетной записи и ее параметров.

Оснастка Управление компьютером

Одно из инструментальных средств управления Windows XP Professional — консоль управления Microsoft (MMC). Консоль MMC обеспечивает стандартизированный метод создания, сохранения и открытия административных инструментальных средств. Консоль MMC не имеет самостоятельных функций администрирования, но включает так называемые *оснастки* (snap-in), предназначенные для выполнения ряда административных задач:

1. **Администрирование и устранение неполадок в локальном масштабе.** Можно выполнять большинство административных задач и решать многие проблемы при помощи консоли MMC.

2. **Администрирование и устранение неполадок дистанционно.** Можно использовать большинство оснасток для удаленного администрирования и устранения неполадок. Windows XP Professional выводит диалоговое окно, если есть возможность использовать оснастку дистанционно.

3. **Централизованное администрирование**. Консоли позволяют выполнять большинство административных задач с одного компьютера. Каждая консоль имеет одну или более оснасток, в том числе и сторонние оснастки, что позволяет создать одну консоль со всеми инструментальными средствами для выполнения административных задач.

Добавляя оснастки в пустую консоль, вы настраиваете ее под свои нужды. На рис. 6.2 показана одна из оснасток, которую можно добавить, — **Управление компьютером**. Оснастка **Управление компьютером** — это инструментальное средство Windows XP Professional для создания, удаления, изменения и отключения локальных учетных записей и изменения паролей.

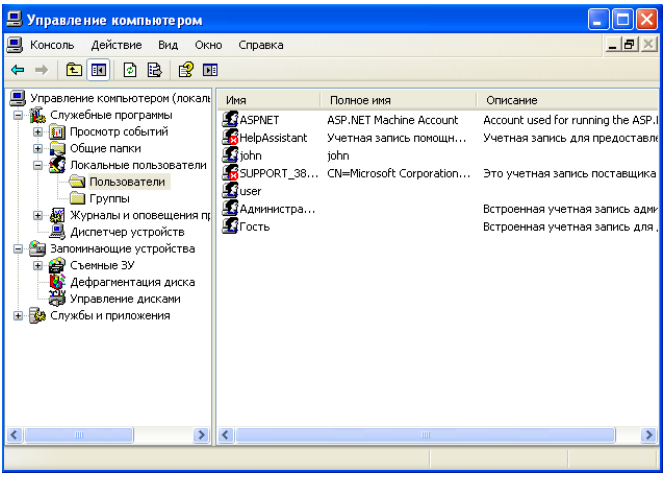


Рис. 6.2 Оснастка Управление компьютером

Настройка консоли MMC

Можно добавить оснастку **Управление компьютером** для локального компьютера, на котором работаете, или, если локальный компьютер подключен к сети, добавить оснастку **Управление компьютером** и указать удаленный компьютер. Чтобы добавить оснастку **Управление компьютером** для удаленного компьютера, в диалоговом окне **Управление компьютером** выберите переключатель **Другим компьютером** и щелкните **Обзор**. В диалоговом окне **Выбор компьютера**, в текстовом поле **Введите имена выбираемых объектов**, введите имя удаленного компьютера, которым вы хотите управлять с помощью оснастки **Управление компьютером** и щелкните **ОК**. В этом окне есть флажок, который позволяет изменить выбранный компьютер при запуске из командной строки.

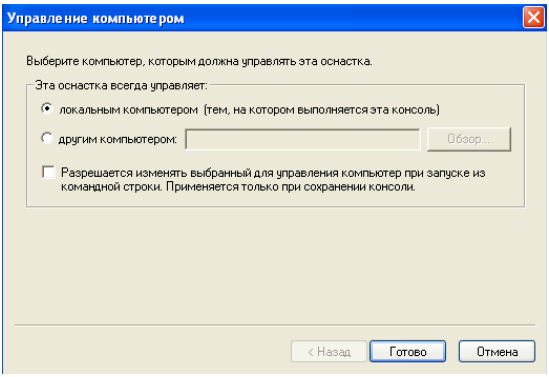


Рис. 6.4 Диалоговое окно **Управление компьютером**

Создание локальной учетной записи пользователя с помощью оснастки Управление компьютером

Чтобы создать локальную учетную запись пользователя с помощью оснастки **Управление компьютером**, выполните следующие действия:

1. Разверните консоль MMC с оснасткой **Управление компьютером** на весь экран.

2. В левой области окна **Управление компьютером** разверните дерево **Управление компьютером (локальным)**, щелкнув знак «плюс» (+) возле значка этой оснастки. На верхнем уровне дерева находятся три папки: **Служебные программы**, **Запоминающие устройства и Службы и приложения**.

3. В левой области окна дважды щелкните **Служебные программы**, а затем **— Локальные пользователи и группы.**

4. В правой области окна щелкните правой кнопкой мыши **Пользователи**, а затем щелкните пункт меню **Новый пользователь**.

5. Заполните соответствующие текстовые поля в диалоговом окне **Новый пользователь** (рис. 6.5), щелкните **Создать** и **Закрыть**.

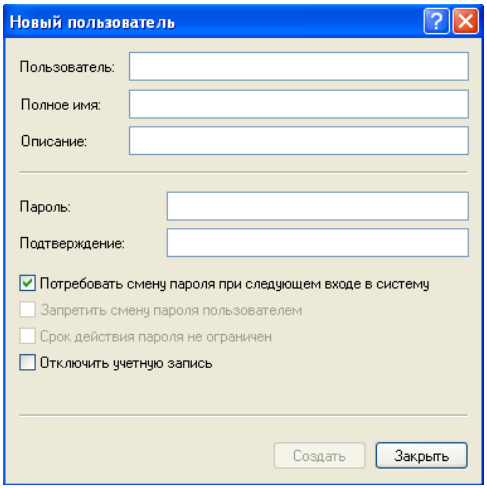


Рис. 6.5 Диалоговое окно **Новый пользователь**

Ниже описаны параметры локальной учетной записи пользователя.

Имя пользователя. Введят имя пользователя. Это поле заполнять обязательно.

Полное имя. Полное имя пользователя. Можно указать имя и фамилию пользователя, а также второе имя (отчество) или инициалы. Это поле заполнять не обязательно.

Описание. Описание учетной записи пользователя или пользователя. Это поле заполнять не обязательно.

Пароль. Для аутентификации пользователя введят пароль учетной записи. В интересах безопасности рекомендуется всегда назначать пароль. В качестве дополнительной меры защиты пароль отображается в виде звездочек.

Подтверждение. Подтвердите пароль, повторно введя его в этом поле. Поле заполнять обязательно, если вы назначаете пароль.

Потребовать смену пароля при следующем входе в систему. Установите этот флажок, если требуется, чтобы пользователь мог изменить свой пароль при первом входе в систему. Это гарантирует, что только пользователь будет знать пароль, Флажок установлен по умолчанию.

Запретить смену пароля пользователем. Установите этот флажок, если более одного человека входят под одной и той же учетной записью пользователя или если требуется, чтобы только администратор мог управлять паролями. Если вы установили флажок **Потребовать смену пароля при следующем входе в систему**, этот флажок недоступен.

Срок действия пароля неограничен. Установите флажок, если вы не хотите, чтобы пароль когда-либо был изменен, например пароль учетной записи пользователя домена, которую использует программа или служба Windows XP Professional. Установка флажка **Потребовать смену пароля при следующем входе в систему** отменяет действие этого параметра, поэтому, если вы установили флажок **Потребовать смену пароля при следующем входе в систему**, этот флажок недоступен.

Отключить учетную запись. Установите этот флажок, чтобы отключить учетную запись нового сотрудника, который еще не начал работать в организации

Всегда требуйте, чтобы новые пользователи изменяли свои пароли при первом входе в систему. В этом случае их пароли будут знать только они.

В интересах безопасности сети при создании уникальных начальных паролей для всех новых учетных записей пользователей используйте комбинацию символов и цифр.

Задания к лабораторной работе

1. Ознакомиться с предлагаемым теоретическим материалом.

2. Создайте новую учетную запись пользователя в формате Имя_Студента. (Например Ivan_Ivanov).

1. Войдите в систему под своим именем или именем члена группы администраторов.
2. Щелкните **Пуск**, **Панель управления** и **Учетные записи пользователей**.
3. В окне **Учетные записи пользователей**, в разделе **Выберите задание**, щелкните **Создание учетной записи**.

4. В текстовом поле **Введите имя для новой учетной записи** введите Имя_Студента и щелкните **Далее**. Windows XP Professional выводит диалоговое окно **Выбор типа учетной записи**.

5. Щелкните переключатель **Ограниченная запись**. Если у вас ограниченный тип учетной записи, то можно изменить или удалить свой пароль, изменить изображение своей учетной записи, тему и другие параметры рабочего стола. Вы также можете просмотреть созданные вами файлы и файлы в совместно используемых папках.

6. Щелкните кнопку **Создать учетную запись**. Windows XP Professional выводит окно **Учетные записи пользователей**; в списке учетных записей появляется Имя_Студента.

7. Создайте вторую учетную запись Имя_Студента2. Не закрывайте окно **Учетные записи пользователей**.

3. Назначьте пароль для локальной учетной записи созданного пользователя с помощью категории **Учетные записи пользователей.**

1. В окне **Учетные записи пользователей** щелкните Имя_Студента.
2. Щелкните **Создать пароль**.
3. Введите **password** в полях **Введите пароль** и **Введите пароль для подтверждения** .
4. Введите **обычно используемый пароль** в поле **Введите слово или фразу, служащие подсказкой о пароле**.
5. Щелкните кнопку **Создать пароль**, Появляется окно **Что вы хотите изменить в учетной записи пользователя** Имя_Студента**?**. Обратите внимание, что список изменений, которые вы можете теперь сделать, включает два новых варианта: **Изменение пароля** и **Удаление пароля**, а команды **Создать пароль** теперь нет.
6. Щелкните значок **Домой**, чтобы вернуться к окну **Учетные записи пользователей**.
7. Назначьте для учетной записи Имя_Студента2 пароль.
8. Закройте окно **Учетные записи пользователей** и панель управления.

4. Измените параметры начала и завершения сеанса пользователя, выполнив следующие действия:

1. Щелкните **Пуск**, **Панель управления** и **Учетные записи пользователей**. Появляется окно **Выберите задание**.
2. Щелкните нужное изменение и следуйте указаниям на экране.

Чтобы изменить учетную запись, если вы вошли под именем администратора, выполните следующие действия:

1. Щелкните **Пуск**, **Панель управления** и Учетные **записи пользователей**.
2. В окне **Учетные записи пользователей** щелкните **Изменение учетной записи**. Появляется окно **Выберите изменяемую учетную запись**.
3. Щелкните учетную запись, которую хотите изменить. Появляется окно **Что вы хотите изменить в учетной записи пользователя имя_пользователя**.
4. Щелкните нужное изменение и следуйте указаниям на экране.

5. Создайте локальную учетную запись пользователя с помощью оснастки Управление компьютером.

1. В левой области окна **Управление компьютером** разверните дерево **Управление компьютером (локальным)**, щелкнув знак «плюс» (+) возле значка этой оснастки. Там содержатся три папки: **Служебные программы**, **Запоминающие устройства** и **Службы и приложения**.
2. В левой области окна дважды щелкните **Служебные программы**, а затем **Локальные пользователи и группы**.
3. В правой области окна щелкните правой кнопкой мыши папку **Пользователи**, а затем щелкните пункт меню **Новый пользователь**. Появляется диалоговое окно **Новый пользователь**.
4. В текстовом поле **Имя пользователя** введите Имя_Студента3.
5. В текстовом поле **Полное имя** введите Имя Студента3**.** Не назначайте пароль для этой учетной записи пользователя.
6. Убедитесь, что установлен флажок **Потребовать смену пароля при следующем входе в систему**.

7. Чтобы создать учетную запись нового пользователя, щелкните **Создать**, затем щелкните кнопку **Закрыть**.

8. Щелкните **Пуск**, **Панель управления**, затем **Учетные записи пользователей**. Появляется окно **Учетные записи пользователей.** Обратите внимание, что Имя_Студента3 - защищенная паролем учетная запись. Паролем для Имя_Студента3 является пустая строка.

9. Закройте окно **Учетные записи пользователей** и панель управления.

10. В правой области окна **Управление компьютером** щелкните правой кнопкой мыши папку **Пользователи**, а затем — пункт меню **Новый пользователь**.

11. В текстовом поле **Имя пользовате** введите Имя_Студента4

12. В текстовом поле **Полное имя** введите Имя Студента4

13. В текстовых полях **Пароль** и **Подтвердите пароль** введите User4.

14. Убедитесь, что установлен флажок **Потребовать смену пароля при следующем входе в систему**, и щелкните кнопку **Создать**.

15. Закройте диалоговое окно **Новый пользователь**.

16. Чтобы закрыть консоль MMC с оснасткой **Computer Management**, в консоли **Управление компьютером**, в меню **Консоль**, щелкните пункт **Выход**. Появляется диалоговое окно MMC, в котором можно сохранить параметры консоли с оснасткой **Управление компьютером**. Если вы шелкнете **Да**, в следующий раз при открытии консоли **Управление компьютером** ее параметры останутся прежними. Если вы щелкнете **Нет**, Windows XP Professional параметры не сохранит.

17. Щелкните **Да**, чтобы сохранить параметры консоли.

6. Создайте консоль MMC.

1. Щелкните **Пуск**, а затем **Выполнить**.

2. В текстовом поле **Открыть** введите mmc и щелкните **ОК.** Запускается MMC и выводится пустая консоль.

3. Разверните окно **Консоль 1**.

4. Разверните окно **Корень консоли.**

5. В меню **Консоль** щелкните пункт **Добавить или удалить оснастку**..

6. Щелкните кнопку **Добавить**. Консоль ММС выводит диалоговое окно **Добавить изолированную оснастку**.

7. В списке **Доступные изолированные оснастки** щелкните **Управление компьютером**, а затем — кнопку **Добавить**. Консоль ММС выводит диалоговое окно **Управление компьютером**, в котором можно указать компьютер для управления. Вариант **Локальный компьютер** выбран по умолчанию.

8. Щелкните **Готово**. ММС создаст консоль с оснасткой **Управление компьютером** для управления локальным компьютером.

9. В диалоговом окне **Добавить изолированную оснастку** щелкните кнопку **Закрыть**.

10. В диалоговом окне **Добавить/удалить оснастку** щелкните **ОК**; чтобы добавить оснастку **Управление компьютером** в свою консоль ММС. В дереве консоли появилась оснастка **Управление компьютером (локальным)**.

11. В меню **Консоль** щелкните пункт **Сохранить как**. ММС выводит диалоговое окно **Сохранить как**.

12. В текстовом поле **Имя файла** введите **управление локальным компьютером,** а затем щелкните **Сохранить**. В заголовке окна появятся слова **Управление локальным компьютером.** Вы только что создали консоль ММС с оснасткой **Управление компьютером** и назвали ее **Управление локальным компьютером.**

7. Проверка новой локальной учетной записи пользователя.

1. Щелкните **Пуск** и **Выход из системы.** Windows XP Professional выводит диалоговое окно **Выход из Windows**, где, если вы не хотите закрывать программы, щелкните **Смена пользователя** и переключитесь на другого пользователя. В противном случае можете щелкнуть **Выход** или **Отмена**.

2. В диалоговом окне **Выход из Windows** щелкните **Выход**.

3. На экране приветствия щелкните значок Имя_Студента3.

4. Щелкните **ОК**. Появится диалоговое окно **Измените пароль**.

5. Оставьте текстовое поле **Старый пароль** без изменения, а в полях **Новый пароль** и **Подтвердите новый пароль** введите

Имя_Студента3 и щелкните **ОК**. Windows XP Professional выводит диалоговое окно **Измените пароль**.

6. Щелкните **ОК**, чтобы закрыть диалоговое окно **Измените пароль**. Учетная запись пользователя User3, которую вы создали с помощью оснастки **Управление компьютером** позволила вам войти в систему. Поскольку вы оставили установленный по умолчанию флажок **Потребовать смену пароля при следующем входе в систему** без изменений при создании учетной записи, вас попросили сменить пароль, когда вы первый раз вошли под именем Имя_Студента 3. Вы убедились, что учетная запись Имя_Студента 3была создана с пустой строкой в качестве пароля, когда вы оставили без изменений поле **Старый пароль** и успешно изменили пароль на Имя_Студента 3.

7. Завершите сеанс работы.

8. Удаление локальной учетной записи пользователя.

1. Войдите в систему под своим именем или именем члена группы администраторов.

2. В панели управления щелкните **Учетные записи пользователей**.

3. Щелкните Имя_Студента3. Windows XP Professional выводит окно **Что вы хотите изменить в учетной записи пользователя** Имя_Студента3**?**.

4. Щелкните **Удаление учетной записи**. Windows XP Professional выводит окно **Хотите сохранить файлы, принадлежавшие** Имя_Студента3**?** Windows XP Professional может автоматически сохранить содержимое рабочего стола и папки **Мои документы** учетной записи Имя_Студента3 на рабочий стол в новую папку с именем Имя_Студента3. Но сообщения электронной почты, избранное из Интернета и другие параметры настройки при этом теряются.

5. Щелкните **Удалить эти файлы**. Windows XP Professional выводит окно **Вы действительно хотите удалить учетную запись** Имя_Студента 3**?**

6. Щелкните **Удалить учетную запись**. Windows XP Professional выводит окно **Учетные записи пользователей**. Обратите внимание,

что учетная запись Имя_Студента3 на странице **Выберите изменяемую учетную запись** теперь отсутствует.

7. Закройте категорию **Учетные записи пользователей** и **Панель управления**.

8. Завершите сеанс работы.

Контрольные вопросы

1. На каком компьютере с помощью локальных учетных записей пользователей можно войти в систему и получить доступ к ресурсам?

2. Где создаются учетные записи пользователей для компьютеров на платформе Windows XP Professional, которые являются частью домена?

3. Какие из следующих утверждений об учетных записях пользователей домена верны?

- Учетные записи пользователей домена позволяют войти в домен и получить доступ к ресурсам сети, если у пользователей есть необходимые права.
- Если хотя бы одна система на какой-либо из платформ семейства Windows 2003 Server имеет статус контроллера домена, то нужно использовать только учетные записи пользователей домена.
- Контроллер домена копирует информацию о новой учетной записи пользователя на все компьютеры домена.
- В базе данных локальных политик безопасности контроллера домена, в котором вы создали учетную запись, создается новая учетная запись пользователя.

4. Какие из следующих утверждений о встроенных учетных записях верны?

- Вы можете удалить учетную запись гостя.
- Вы не можете удалить учетную запись администратора.
- Вы не можете переименовать учетную запись администратора.
- Вы можете переименовать учетную запись администратора.

5. Как отключить учетную запись гостя?

6. Каково максимальное количество символов, которое Windows XP Professional признает в имени локальной учетной записи пользователя?

7. Когда допустимо дублирование локальных учетных записей в сети на платформе Windows XP Professional?

8. Какие из перечисленных символов разрешается использовать в имени локальной учетной записи в системе на платформе Windows XP Professional?

- 0 () 9
- - + = >
- От A до Z; от a до z
- [] _ |

9. Если пользователи создают свои собственные пароли, каких рекомендаций они должны придерживаться? (Выберите все правильные ответы.)

- Используйте максимальное возможное в пароле количество символов.
- Используйте пароль, который трудно угадать.
- Используйте хотя бы одну прописную букву, один символ нижнего регистра, одну цифру и один допустимый не алфавитно-цифровой символ.
- Чтобы не забыть пароль, используйте что-то вас характеризующее.

10. Какие из следующих утверждений о категории **Учетные записи пользователей** Windows XP Professional верны?

- позволяет дистанционно создавать, изменять и удалять учетные записи пользователей на всех компьютерах в сети на платформе Windows XP Professional.
- позволяет просматривать и изменять все учетные записи на компьютере.
- задачи, которые можно выполнить с помощью категории Учетные записи пользователей, зависят от типа учетной записи, с которой вы вошли в локальную систему.
- позволяет пользователям могут изменить, создать или удалить свой пароль.

11. Какие из следующих задач выполняют с помощью обоих типов учетных записей?

- Изменение изображения значка своей учетной записи.
- Изменение типа своей учетной записи.
- Создание, изменение и удаление своего пароля.
- Изменение имени своей учетной записи.

12. Какие из следующих утверждений о входе в систему или завершении сеанса под управлением Windows XP Professional верны?

- При использовании экрана приветствия для входа в локальную систему можно быстро переключиться на другую учетную запись пользователя, не завершая сеанс и не закрывая запущенные программы.
- Категория Учетные записи пользователей позволяет отключить локальную запись пользователя, что дает этому пользователю войти в систему.
- При использовании экрана приветствия для входа в локальную систему можно воспользоваться только одной из учетных записей, отображенных на экране приветствия.
- Категория Учетные записи пользователей позволяет заменить экран приветствия классическим окном входа в систему, в этом случае пользователям необходимо ввести свое имя и пароль.

13. Какой флажок при создании учетной записи пользователя средствами оснастки **Управление компьютером** нужно установить, чтобы запретить новому служащему пользоваться своей учетной записью до начала работы в компании?

Лабораторная работа №7

Обеспечение безопасности ресурсов с помощью разрешений NTFS

Цель работы: Приобретение навыков обеспечения безопасности ресурсов в Microsoft Windows.

Разрешения NTFS позволяют явно указать, какие пользователи и группы имеют доступ к файлам и папкам и какие операции с содержимым этих файлов или папок им разрешено выполнять. Разрешения NTFS применимы только к томам, отформатированным с использованием файловой системы NTFS. Они не предусмотрены для томов, использующих файловые системы FAT или FAT32. Система безопасности NTFS эффективна независимо от того, обращается ли пользователь к файлу или папке, размещенных на локальном компьютере или в сети [2, 12].

Разрешения, устанавливаемые для папок, отличаются от разрешений, устанавливаемых для файлов. Администраторы, владельцы файлов или папок и пользователи с разрешением **Полный доступ** имеют право назначать разрешения NTFS пользователям и группам для управления доступом к этим файлам и папкам.

Разрешения для папок в NTFS

Разрешения для папок можно установить для управления доступом пользователей к папкам и файлам в этих папках. Ниже перечислены стандартные разрешения для папок в NTFS, которые можно установить, и обеспечиваемые ими типы доступа.

Чтение - разрешено просматривать файлы и папки, а также список владельцев разрешения и атрибуты папки такие, как **Только чтение**, **Скрытый**, **Архивный** и **Системный**.

Запись - разрешено создавать новые файлы и папки внутри папки, изменять атрибуты папки и просматривать владельцев и разрешения для папки.

Список содержимого папки - разрешено просматривать имена файлов и папок.

Чтение и выполнение - разрешено перемешаться по структуре папок в поисках других файлов или папок, даже если пользователь не

обладает разрешением на доступ к просматриваемым папкам. А также выполнять все действия, право на которые дают разрешения **Чтение** и **Список содержимого папки**.

Изменить - разрешено удалять папки и выполнять все действия, право на которые дают разрешения **Запись** и **Чтение и выполнение**

Полный доступ - разрешено изменять разрешения, менять владельца, удалять папки и файлы и выполнять действия, право на которые дают все остальные разрешения NTFS для папок

Можно запретить разрешение для пользователя или группы.

Для полного запрещения доступа пользователя или группы к папке, откажите в разрешении **Полный доступ**.

Разрешения для файлов в NTFS

Разрешения на доступ к файлам устанавливают для управления доступом пользователей к файлам. Ниже перечислены стандартные разрешения для файлов в NTFS, которые можно установить и обеспечиваемые ими типы доступа.

Чтение - разрешено просматривать файлы, владельцев, разрешения и атрибуты.

Запись - разрешено перезаписывать файл, изменять атрибуты файлов и просматривать владельцев и разрешения.

Чтение и выполнение - разрешено запускать приложения и выполнять все действия, право на которые дает разрешение **Чтение.**

Изменить - разрешено изменять и удалять файл, а также выполнять все действия, право на которые дают разрешения **Запись** и **Чтение и выполнение**.

Полный доступ - разрешено изменять разрешения, менять владельца и выполнять действия, право на которые дают все остальные разрешения NTFS для файловж.

Список управления доступом

В NTFS хранится *список управления доступом* (access control list, ACL**)** для каждого файла и папки на томе NTFS. В этом списке перечислены пользователи и группы, для которых установлены разрешения для файла или папки, а также сами назначенные

разрешения. Чтобы пользователь получил доступ к ресурсу, в ACL должна быть запись, называемая *элемент списка управления доступом* (access control entry, ACE), для этого пользователя или группы, к которой он принадлежит. Эта запись назначит запрашиваемый тип доступа [например, **Чтение**] пользователю. Если в ACL нет соответствующей ACE, то пользователь не получит доступ к ресурсу.

Множественные разрешения NTFS

Можно установить несколько разрешений пользователю и всем группам, членом которых он является. Для этого нужно иметь представление о правилах и приоритетах, по которым в NTFS назначаются и объединяются множественные разрешения и о наследовании разрешений NTFS.

Эффективные разрешения

Эффективные разрешения пользователя для ресурса — это совокупность разрешений NTFS, которые администратор назначает отдельному пользователю и всем группам, к которым он принадлежит. Если у пользователя есть разрешение **Чтение** для папки, и он входит в группу, у которой есть разрешение **Запись** для той же папки, значит, у этого пользователя есть оба разрешения.

Приоритет разрешений для файлов над разрешениями для папок

В NTFS разрешения для файлов имеют больший приоритет, чем разрешения для папок. Если у пользователя есть разрешение на доступ к файлу и право **Обход перекрестной проверки**, то он сможет воспользоваться доступом к этому файлу, даже если у него нет доступа к папке, в которой содержится файл. Он можете получить доступ к тем файлам, для которых у него есть разрешения, воспользовавшись UNC-именем файла или локальным путем для открытия файла из соответствующего приложения. Это возможно, даже если папка, в которой находится файл, невидима и у пользователя нет соответствующего разрешения для данной папки. Другими словами, если у пользователя нет разрешения на доступ к

папке, содержащей нужный ему файл, для доступа к файлу ему необходимо обладать правом **Обход перекрестной проверки** и знать полный путь к файлу.

Приоритет запрещения над разрешениями

Можно запретить доступ к файлу пользователю или группе, хотя этот метод контроля ресурсов и не является предпочтительным. Запрет имеет больший приоритет, чем разрешение на всех уровнях, на которые он распространяется. Даже если у группы в которую входит пользователь имеется разрешение на доступ к файлу или папке, запрет на доступ для пользователя блокирует все имеющиеся разрешения.

Наследование разрешений в NTFS

По умолчанию разрешения, назначаемые родительской папке, наследуются и распространяются на подпапки и файлы, содержащиеся в родительской папке. Однако можно предотвратить наследование разрешений.

Все разрешения, устанавливаемые для родительской папки, также действуют и на подпапки и файлы, содержащиеся в родительской папке. При установке разрешения NTFS на доступ к папке, одновременно устанавливают разрешения как для всех существующих подпапок и файлов, так и для создаваемых в родительской папке новых файлов и подпапок.

Можно предотвратить наследование разрешений, назначенных для родительской папки, подпапками и файлами, содержащимися в ней. Это значит, что подпапки и файлы не унаследуют разрешения, установленные для родительской папки. Папка, для которой предотвратили наследование, становится новой родительской папкой. Подпапки и файлы, содержащиеся в этой новой родительской папке, унаследуют разрешения, установленные для нее.

Установка разрешений NTFS и особых разрешений

Следует руководствоваться определенными принципами при установке разрешений NTFS. Устанавливайте разрешения согласно потребностям групп и пользователей, что включает в себя разрешение

или предотвращение наследования разрешений родительской папки подпапками и файлами, содержащимися в родительской папке.

Планирование разрешений NTFS

Разрешениями легко управлять, если уделить немного времени на планирование разрешений NTFS и соблюдать при планировании несколько следующих принципов.

1. Для упрощения процесса администрирования сгруппируйте файлы по папкам следующих типов: папки с приложениями, папки с данными, личные папки. Централизуйте общедоступные и личные папки на отдельном томе, не содержащем файлов операционной системы и других приложений. Действуя таким образом, вы получите следующие преимущества:

- сможете устанавливать разрешения только папкам, а не отдельным файлам;
- упростите процесс резервного копирования, так как не придется делать резервные копии файлов приложений, а все общедоступные и личные папки находятся в одном месте.

2. Устанавливайте для пользователей только необходимый уровень доступа. Если необходимо чтение файла, установите пользователю разрешение Чтение для этого файла. Это уменьшит вероятность случайного изменения файла или удаления важных документов и файлов приложений пользователем.

3. Создавайте группы согласно необходимому членам группы типу доступа, затем установите соответствующие разрешения для группы. Назначайте разрешения отдельным пользователям только в тех случаях, когда это необходимо.

4. При установке разрешений для работы с данными или файлами приложений установите разрешение Чтение и выполнение для групп Пользователи и Администраторы. Это предотвратит случайное удаление файлов приложений или их повреждение вирусами или пользователями.

5. При установке разрешений для папок с общими данными назначьте разрешения Чтение и выполнение и Запись группе Пользователи и разрешение Полный доступ для группы Создатель-

владелец. По умолчанию пользователь, создавший документ, также является его владельцем. Владелец файла может дать другому пользователю разрешение на владение файлом. Пользователь, который принимает такие права, в этом случае становится владельцем файла. Если вы установите разрешение Чтение и выполнение и Запись группе Пользователи и разрешение Полный доступ группе Создатель-владелец, то пользователи получат возможность читать и изменять документы, созданные другими пользователями, а также читать, изменять и удалять файлы и папки, создаваемые ими.

6. Запрещайте разрешения, только если необходимо запретить отдельный тип доступа определенному пользователю или группе.

7. Поощряйте пользователей в установке разрешений для файлов и папок, которые они создают, и научите их это делать самостоятельно.

Установка разрешений NTFS

По умолчанию при форматировании тома с использованием файловой системы NTFS разрешение **Полный доступ** устанавливается для группы **Все**. В Windows XP Professional учетная запись **Анонимный вход** не включена в группу **Все**. При обновлении операционной системы Windows 2000 Professional до Windows XP Professional ресурсы с разрешениями установленными для группы **Все** недоступны для группы **Анонимный вход**.

Администраторы, пользователи с разрешение **Полный доступ** и владельцы файлов и папок могут устанавливать разрешения для отдельных пользователей и групп. Для установки или изменения разрешения NTFS для файла или папки на вкладке **Безопасность** диалогового окна свойств файла или папки настройте параметры, показанные на рис. 7.1 и описанные ниже.

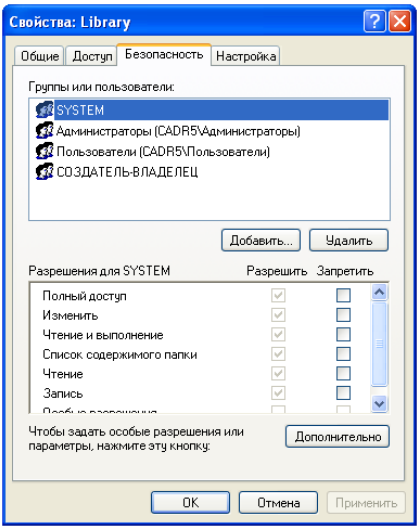


Рис. 7.1 Вкладка Безопасность диалогового окна свойств папки

Группы или пользователи - позволяет выделить пользователя или группу, для которой вы хотите изменить разрешения или, которые вы собираетесь удалить из списка.

Разрешения для имя группы или пользователя - устанавливает и запрещает разрешения. Отметьте флажок **Разрешить** для назначения разрешения. Отметьте флажок **Запретить** для запрета разрешения.

Добавить - открывает диалоговое окно **Выбор: пользователи или группы**, в котором можно выбрать пользователей или группы для добавления их к списку **Группы или пользователи**.

Удалить - удаляет выделенного пользователя или группу и соответствующие разрешения для файла или папки.

Дополнительно - открывает диалоговое окно **Дополнительные параметры безопасности** для выделенной папки. В открывшемся окне вы можете назначать или запрещать особые разрешения (рис. 7.2).

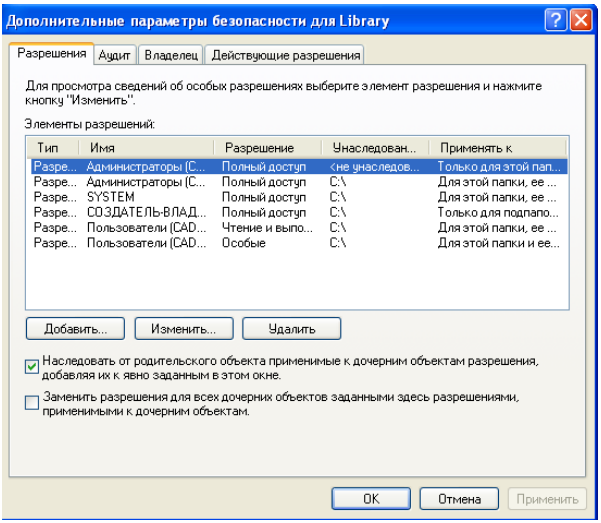


Рис. 7.2 Вкладка **Разрешения** диалогового окна **Дополнительные параметры безопасности** свойств папки

Добавление пользователей или групп

Щелкните кнопку **Добавить** для открытия диалогового окна **Выбор: пользователи или группы** (рис. 7.3). Используйте это диалоговое окно для добавления пользователей или групп, для которых вы собираетесь назначать разрешения на доступ к папке или файлу. Параметры, доступные в диалоговом окне **Выбор: пользователи или группы**, описаны ниже.

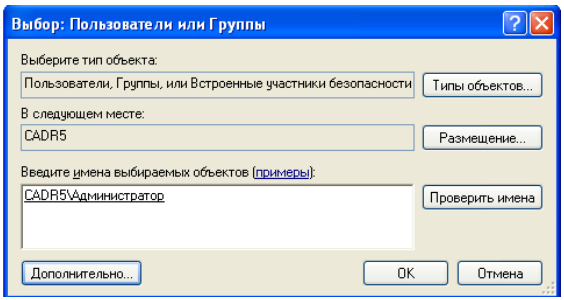


Рис. 7.3 Вкладка Выбор: пользователи или группы

Выберите тип объектов - позволяет выбрать тип объекта, например встроенные участники безопасности (пользователи, группы и учетные записи отдельных компьютеров), пользователи или группы

В следующем месте - указывает текущую область поиска, например, в домене или на локальном компьютере

Размещение - позволяет выбрать область поиска, например, в домене или на локальном компьютере

Введите имена выбираемых объектов - позволяет ввести список тех встроенных участников безопасности, пользователей и групп, которых вы хотите добавить

Проверить имена - проверяет выделенный список встроенных участников безопасности, пользователей и групп, которых вы хотите добавить

Дополнительно - позволяет получить доступ к дополнительным возможностям поиска, включая возможность поиска удаленных учетных записей пользователей, учетных записей с неустаревшими паролями и учетных записей, по которым не подключались определенное количество дней

Назначение или запрещение особых разрешений

Щелкните кнопку **Дополнительно**, чтобы открыть диалоговое **окно Дополнительные параметры безопасности**, где перечислены группы и пользователи и установленные для них разрешения для этого объекта. В поле **Элементы разрешений** также указано, от какого объекта разрешения унаследованы и к каким объектам применимы. Вы можете воспользоваться диалоговым окном **Дополнительные параметры безопасности** для изменения разрешений, установленных для пользователя или группы. Для изменения разрешений, установленных для пользователя или группы, выделите пользователя и щелкните кнопку **Изменить**. Откроется диалоговое окно **Элемент разрешения для** (рис. 7.4). Затем выделите или отмените определенные разрешения, которые вы хотите изменить, как описано далее.

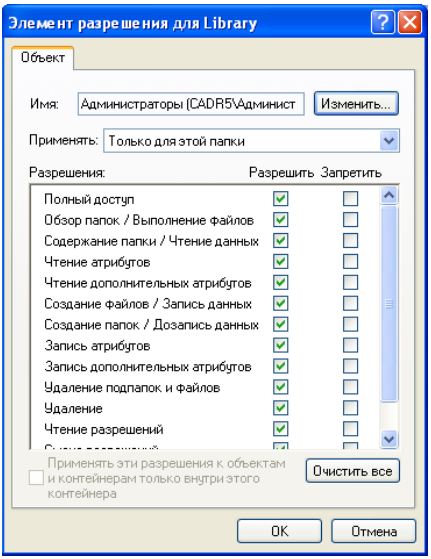


Рис. 7.4 Диалоговое окно **Элемент разрешения для**

Полный доступ - устанавливает все разрешения для пользователя или группы.

Обзор папок/Выполнение файлов - разрешает или запрещает перемещение по структуре папок в поисках других файлов или папок, даже если пользователь не обладает разрешением на доступ к просматриваемым папкам. Разрешение на обзор папок не применяется в том случае, если группа или пользователь обладает правом **Обход перекрестной проверки**, устанавливаемым в оснастке **Групповая политика**. По умолчанию группа **Все** наделена правом **Обход перекрестной проверки**, поэтому, если вы хотите воспользоваться разрешением **Обзор папок**, вам придется изменить групповую политику. Разрешение **Обзор папок** применимо только к папкам. **Выполнение файлов** разрешает или запрещает запуск исполняемых файлов (файлов приложений). Разрешение **Выполнение файлов** применимо только к файлам.

Содержание папки/Чтение данных - разрешает или запрещает просмотр имен файлов и подпапок, содержащихся в папке. Это

разрешение применимо только к папкам Разрешение **Чтение данных** позволяет или запрещает просмотр содержимого файлов. Разрешение **Чтение данных** применимо только к файлам.

Чтение атрибутов - разрешает или запрещает просмотр атрибутов файла или папки. Атрибуты определяются файловой системой NTFS

Чтение дополнительных атрибутов - разрешает или запрещает просмотр дополнительных атрибутов файла или папки. Дополнительные атрибуты определяются программами.

Создание файлов/Запись данных - разрешает или запрещает создание файлов в папке, Это разрешение применимо только к папкам **Запись данных** разрешает или запрещает внесение изменений в файл и запись поверх имеющегося содержимого. Это разрешение применимо только к файлам.

Создание папок/Дозапись данных - разрешает или запрещает создание папок внутри папки. Это разрешение применимо только к папкам. **Дозапись данных** разрешает или запрещает добавление данных в конец файла, но не разрешает изменение, удаление или замену имеющихся данных. Это разрешение применимо только к файлам.

Запись атрибутов - разрешает или запрещает смену атрибутов файла или папки. Атрибуты определяются файловой системой NTFS

Запись дополнительных атрибутов - разрешает или запрещает смену дополнительных атрибутов файла или папки. Дополнительные атрибуты определяются программами.

Удаление подпапок и файлов - разрешает или запрещает удаление подпапок и файлов даже при отсутствии разрешения **Удаление** для данной подпапки или файла.

Удаление - разрешает или запрещает удаление файла или папки. Если для файла или папки отсутствует разрешение **Удаление**, объект все же можно удалить при наличии разрешения **Удаление подпапок и файлов** для родительской папки.

Чтение разрешений - разрешает или запрещает чтение разрешений на доступ к файлу или папке.

Смена разрешений - разрешает или запрещает смену разрешений на доступ к файлу или папке. Вы можете предоставить администраторам и пользователям возможность смены разрешений

для файла или папки без установки разрешения **Полный доступ** для данной папки или файла. Таким образом, администратор или пользователь не сможет удалить, изменить или записать данные в файл или папку, но смогут установить разрешения для файла или папки.

Смена владельца - разрешает или запрещает вступать во владение файлом или папкой. Владелец файла или папки всегда может изменять разрешения на доступ к ним независимо от любых разрешений, защищающих этот файл или папку Разрешается передавать право владельца файлов и папок от одного пользователя к другому. Вы можете предоставить кому-либо право.

Синхронизация - разрешает или запрещает ожидание различными потоками файлов или папок и синхронизацию их с другими потоками, которые могут занимать их. Это разрешение применимо только к программам, выполняемым в многопоточном режиме с несколькими процессами.

Смена владельца

Разрешается передавать право владельца файлов и папок от одного пользователя к другому. Можно предоставить кому-либо право смены владельца или, как администратор, самим сменить владельца файла или папки. Для смены владельца файла или папки действуют определенные правила.

1. Текущий владелец или любой пользователь с разрешением **Полный доступ** может установить стандартное разрешение **Полный доступ** или особое разрешение доступа **Смена владельца** для другого пользователя или группы, позволяя пользователю или любому члену группы стать владельцем.

2. Администратор имеет право сменить владельца папки или файла независимо от назначенных разрешений. Если администратор становится владельцем, группа **Администраторы** также становится владельцем, и любой из членов группы **Администраторы** может изменять разрешения для файла или папки и назначать разрешение **Смена владельца** другому пользователю или группе.

Например, если сотрудник уволился из организации, то администратор может изменить владельца для файлов данного

сотрудника и назначить разрешение **Смена владельца** другому сотруднику, который и станет владельцем этих файлов.

Нельзя назначить владельцем файла или папки любого пользователя. Владелец файла, администратор или любой пользователь с разрешением **Полный доступ** имеет право назначить разрешение **Смена владельца** отдельному пользователю или группе, тем самым, позволяя им стать владельцем. Для того чтобы стать владельцем файла или папки, пользователь или член группы с разрешением **Смена владельца** должен явно стать владельцем файла или папки.

Чтобы сменить владельца файла или папки, пользователь или член группы с разрешением **Смена владельца** должен явно назначить нового владельца. Для этого необходимо выполнить следующие действия:

1. На вкладке **Безопасность** диалогового окна свойств файла или папки щелкните кнопку **Дополнительно**.

2. В открывшемся диалоговом окне Допо**лнительные параметры безопасности,** на вкладке **Владелец**, в списке **Изменить владельца на**, выберите нужное имя.

3. Установите флажок **Заменить владельца субконтейнеров и объектов** для того, чтобы стать владельцем всех подпапок и файлов, содержащихся в папке. Затем щелкните **ОК**.

Предотвращение наследования разрешений

По умолчанию подпапки и файлы наследуют разрешения, установленные для родительской папки. Признаком этого служит установленный флажок **Наследовать от родительского объекта применимые к дочерним объектам разрешения, добавляя их к явно заданным в этом окне** в диалоговом окне **Дополнительные параметры безопасности**. Для предотвращения наследования разрешений от родительской папки снимите этот флажок. При этом вам придется выбрать один из вариантов, описанных далее.

Копировать - копирует разрешения, которые были ранее переданы от родительского объекта к дочерним объектам, затем

запрещает последующее наследование разрешений от родительской папки.

Удалить - удаляет разрешения, которые были ранее переданы от родительского объекта к дочерним объектам, и сохраняет только те разрешения, которые явно установлены здесь**.**

Отмена - закрывает диалоговое окно.

Устранение проблем с разрешениями

При установке разрешений NTFS для файлов и папок могут возникать различные проблемы. При копировании или перемещении файлов и папок разрешения, установленные для них, могут изменяться. Существуют особые правила изменения разрешений. Понимание их поможет вам разрешать возникающие проблемы. Устранение этих проблем является важным фактором для поддержания доступности ресурсов для соответствующих пользователей и защиты от неавторизированных пользователей.

Копирование файлов и папок

При копировании файлов ил и папок из одной папки в другую или с одного тома на другой, разрешения изменяются. При копировании файла внутри тома NTFS или с одного тома NTFS на другой обратите внимание на следующее:

- Windows XP Professional обращается к скопированному файлу, как к новому. В качестве нового файла он принимает разрешения папки, куда он был скопирован;
- для копирования файлов и папок необходимо обладать разрешением **Запись** для папки, куда вы копируете данные;
- вы становитесь создателем и владельцем скопированных файлов и папок.

При копировании на тома FAT файлов или папок те утрачивают разрешения NTFS, так как тома FAT не поддерживают разрешения NTFS.

Перемещение файлов и папок

При перемещении файла или папки разрешения могут изменяться в зависимости от того, куда вы перемещаете файл или папку.

Перемещение внутри тома NTFS

При перемещении файла или папки внутри тома NTFS обратите внимание на следующее:

- файл или папка сохраняют первоначальные разрешения;
- для перемещения файлов или папок необходимо разрешение **Запись** для папки, куда вы перемещаете файлы или папку;
- необходимо обладать разрешением **Изменить** для перемещаемого файла или папки. Для перемещения файла или папки необходимо разрешение **Изменить**, потому что в Windows XP Professional файл или папка удаляются из первоначального места после копирования в новое.

Перемещение с одного тома NTFS на другой

При перемещении файла или папки с одного тома NTFS на другой обратите внимание на следующее:

- файл или папка наследуют разрешения папки, куда они перемещаются;
- для перемещения файлов или папок необходимо разрешение **Запись** для папки, куда вы перемешаете файлы или папку;
- необходимо разрешение **Изменить** для перемещаемого файла или папки. Для перемещения файла или папки необходимо разрешение **Изменить**, потому что в Windows XP Professional файл или папка удаляются из первоначального места после копирования в новое;
- вы становитесь создателем и владельцем перемещенных файлов или папок.

При перемещении на тома FAT файлов или папок те утрачивают разрешения NTFS, гак как тома FAT не поддерживают разрешения NTFS.

Устранение проблем с разрешениями

Ниже описаны наиболее часто встречающиеся проблемы с разрешениями и описаны возможные способы их разрешения.

Пользователь не может получить доступ к файлу или папке. Если файл или папка копируются или перемещаются на другой том NTFS, разрешения могут измениться. Проверьте разрешения, установленные непосредственно пользователю и группам, к которым пользователь принадлежит. Пользователь может не обладать разрешениями или получить отказ в доступе как отдельный пользователь либо как член группы.

Вы добавили пользователя к группе, чтобы предоставить ему доступ к файлу или папке, но пользователь все равно не получил доступа. Чтобы изменения вступили в силу, пользователю необходимо либо завершить сеанс работы, а затем войти в систему снова, либо отключить все сетевые соединения с компьютером, где хранится файл или папка, и затем подключиться заново.

Пользователь с разрешением Полный доступ для папки удалил файл в папке, хотя у него не было разрешения на удаление непосредственно этого файла. Вы хотите предотвратить возможное дальнейшее удаление файлов. Чтобы удалить разрешения особого доступа, снимите флажок **Удаление подпапок и файлов** для этой папки. Таким образом, вы предотвратите возможное удаление файлов из этой папки пользователями с разрешением **Полный доступ** для данной папки.

Windows XP Professional поддерживает приложения стандарта Portable Operating System Interface for UNIX (POSIX), разработанные для работы в UNIX. В системах UNIX разрешение **Полный доступ** позволяет удалять файлы в папке. В Windows XP Professional в разрешение **Полный доступ** включено особое разрешение **Удаление подпапок и файлов**, также позволяющее удалять файлы в этой папке независимо от ваших разрешений для этих файлов.

Предотвращение проблем с разрешениями

Избежать проблем при установке разрешений NTFS можно учитывая следующие рекомендации.

1. Назначайте максимально ограниченные разрешения NTFS, они должны позволять выполнение только требуемых действий.

2. Устанавливайте разрешения на уровне папок, а не файлов. Сгруппируйте файлы в отдельной папке, к которой вы хотите ограничить доступ пользователей. Затем установите ограниченный доступ ля этой папки.

3. Для всех исполняемых файлов установите:

– для группы **Администраторы** разрешения **Чтение и выполнение** и **Изменение**;

– для группы **Пользователи** разрешение **Чтение и выполнение**. Повреждение файлов приложения, как правило, является результатом случайных действий и вирусов. Назначив разрешения **Чтение и выполнение** и **Изменение** группе Администраторы и разрешение **Чтение и выполнение** группе **Пользователи**, вы сможете предотвратить повреждение или удаление исполняемых файлов вирусами или пользователями. Для обновления файлов члены группы **Администраторы** могут установить для себя разрешение **Полный доступ** на время внесения изменений, а затем снова установить разрешения **Чтение и выполнение и Изменение**.

4. Установите для папок с общими данными для группы **Создатель-Владелец** разрешение **Полный доступ**, чтобы предоставить пользователям возможность удалять и изменять создаваемые ими файлы. Таким образом, пользователь, создавший документ или папку, получит полный доступ только к тем файлам или папкам, которые он или она создали в папке с общими данными.

5. Установите для папок с общими данными для группы Создатель-владелец разрешение **Полный доступ** и разрешения Чтение и **Запись** для группы **Все**. Таким образом, пользователи получат полный доступ к создаваемым документам или папкам, но члены группы **Все** смогут только читать файлы, хранящиеся в папке, и добавлять файлы к папке.

6. Используйте длинные, детальные имена, если доступ к ресурсам предполагаете осуществлять только на данном компьютере. Если к папке со временем будет предоставлен общий доступ, применяйте имена файлов и папок, доступные для всех клиентских компьютеров.

7. Старайтесь назначать, а не запрещать разрешения. Если вы хотите, чтобы определенный пользователь или группа не имели

доступа к папке или файлу, не устанавливайте соответствующего разрешения. Запрещение разрешений должно быть исключением, а не правилом.

Задания к лабораторной работе

1. Ознакомиться с предлагаемым теоретическим материалом.

2. Начните сеанс работы, используя учетную запись члена группы **Администраторы**, и создайте учетные записи пользователей по данным следующей таблицы.

Учетная запись пользователя	**Тип**
Имя_Студента1	Ограниченная учетная запись
Имя_Студента2	Ограниченная учетная запись
Имя_Студента3	Ограниченная учетная запись
Имя_Студента4	Ограниченная учетная запись

3. Создайте следующие папки:

- Public;
- Public\Library.

4. Определите устанавливаемых по умолчанию разрешений NTFS для папки.

1. Начните сеанс, используя учетную запись пользователя, который является членом группы **Администраторы**.
2. Щелкните правой кнопкой мыши значок **Мой компьютер**, затем щелкните пункт меню **Проводник**.
3. Откройте локальный диск C, затем щелкните правой кнопкой мыши значок папки Public и выберите пункт меню **Свойства**. В Windows XP Professional откроется диалоговое окно свойств папки Public с активной вкладкой **Общие**.
4. Перейдите на вкладку **Безопасность** для просмотра разрешений, установленных для папки Public.

Если на экране не видна вкладка **Безопасность**, вам следует уточнить два вопроса. Раздел вашего диска отформатирован как NTFS или как FAT? Только на разделах NTFS используются разрешения

NTFS, и, таким образом, только на разделах NTFS видна вкладка **Безопасность**. Используете ли вы **простой общий доступ к файлам** или нет? Щелкните кнопку **Отмена**, чтобы закрыть диалоговое окно свойств папки Public. В пункте меню **Сервис** выберите пуню **Свойства папки**. В диалоговом окне **Свойства папки** перейдите на вкладку **Вид**. В списке **Дополнительные параметры** снимите флажок **Использовать простой общий доступ к файлам (рекомендуется)** и щелкните **ОК**. Повторите пункты 3 и 4 и продолжите.

Если для какого-либо пользователя или группы установлены особые разрешения, выделите пользователя или группу и щелкните кнопку **Дополнительно** для просмотра списка особых разрешений.

В Windows XP Professional в диалоговом окне свойств папки Public видна вкладка **Безопасность**.

5. Щелкните **ОК**, чтобы закрыть диалоговое окно свойств папки Public.
6. Закройте окно **Проводник** и завершите сеанс.

4. Проверьте разрешения, установленных для папки Public.

1. Войдите в систему, используя учетную запись Имя_Студентal, затем запустите **Проводник**.
2. Перейдите в папку Public.
3. В папке Public создайте текстовый документ, назовите его Имя_Студентal. Введите какой-нибудь текст.

Выделите значок папки Public в древовидной структуре папок. В пункте меню **Файл** выберите **Создать**, затем щелкните **Текстовый документ** для создания нового документа.

4. Попытайтесь выполнить следующие операции с созданным файлом:

- откройте файл;
- измените файл;
- удалите файл.

Какие действия вы смогли успешно совершить и почему?

5. В папке Public снова создайте текстовый документ Имя_Студентal.
6. Завершите сеанс работы с Windows XP Professional.

7. Войдите в систему, используя учетную запись Имя_Студента2.
8. Попытайтесь выполнить следующие операции с текстовым документом Имя_Студента1:

- откройте файл;
- измените файл;
- удалите файл.

5. Установите разрешения NTFS соблюдая следующие правила:

- все пользователи должны иметь возможность читать документы и файлы в папке Public;
- все пользователи должны иметь возможность создавать документы в папке Public;
- все пользователи должны иметь возможность изменять содержание, свойства и разрешения для создаваемых ими документов в папке Public;
- пользователь Имя_Студента2 несет ответственность за подержание папки Public и должен иметь возможность изменять и удалять все файлы в папке Public.

Основываясь на полученной в упражнении 1 информации, определите, как следует изменить разрешения для соответствия этим четырем критериям? Почему?

В настоящее время ваша регистрационная запись — Имя_Студента2. Можете ли вы изменить разрешения, установленные для пользователя Имя_Студента2, пока вы подключены как Имя_Студента2? Почему?

6. Проверьте разрешения NTFS для папки.

1. Войдите в систему, используя учетную запись Имя_Студента2.
2. Запустите Проводник.
3. Откройте диск С:, затем откройте папку Public.
4. Попытайтесь совершить следующие действия с текстовым документом Имя_Студента1:

- измените файл;
- удалите файл.

Какие действия вы смогли совершить и почему?

7. Проверить разрешения для папки Library.

1. Войдите в систему, используя учетную запись Имя_Студента1, затем запустите Проводник.
2. В Проводнике откройте папку Public\Library.
3. Создайте текстовый документ Имя_Студента1в папке Library.
4. Завершите сеанс Windows XP Professional.

7. Проверить разрешения для папки Library с использованием подключения с учетной записью Имя_Студента2.

1. Зарегистрируйтесь в системе, используя учетную запись Имя_Студента2, затем запустите Проводник.
2. Откройте папку Public\Library.
3. Попытайтесь совершить следующие действия с текстовым документом Имя_Студента1

- открыть файл;
- изменить файл;
- удалить файл.

Какие действия вы смогли совершить и почему?

4. Завершите работу с Windows XP Professional.

8. Определить разрешения для файла.

1. Подключитесь, используя учетную запись пользователя, который является членом группы **Администраторы**.

2. В папке Public создайте текстовый документ и назовите его OWNER.

3. Щелкните правой кнопкой мыши значок документа OWNER, затем выберите пункт меню Свойства, В Microsoft Windows XP Professional откроется диалоговое окно Свойства: Owner с активной вкладкой Общие.

4. Перейдите на вкладку Безопасность для просмотра разрешений, установленных для файла OWNER. Щелкните кнопку Дополнительно. Откроется диалоговое окно Дополнительные параметры безопасности для Owner с активной вкладкой Разрешения. Перейдите на вкладку Владелец. Кто является текущим владельцем файла OWNER?

9. Установить разрешения, позволяющие пользователю сменить владельца.

1. В диалоговом окне **Дополнительные параметры безопасности для Owner** перейдите на вкладку **Разрешения**.

2. Щелкните кнопку **Добавить** Откроется диалоговое окно **Выбор: пользователи или группы**.

3. Убедитесь, что в текстовой поле Размещение, которое расположено вверху диалогового окна, выбрано имя вашего компьютера.

4. В текстовом поле Введите имена выбираемых объектов введите Имя_Студента1, затем щелкните кнопку **Проверить имена**.

В списке **Введите имена выбираемых объектов** должна появиться запись “имя компьютера”\ Имя_Студента1. Это означает, что учетная запись пользователя Userl найдена на компьютере с именем “имя компьютера” и является действительной учетной записью.

5. Щелкните **ОК**.
6. В Windows XP Professional станет активным диалоговое окно Элемент разрешения для Owner. Обратите внимание на то, что все элементы разрешений для пользователя Имя_Студента1не отмечены.
7. В колонке Разрешения установите флажок Разрешить для разрешения Сменить владельца.
8. Щелкните ОК.

В Windows XP Professional станет активным диалоговое окно **Дополнительные параметры безопасности для Owner**с открытой вкладкой **Разрешения**.

9. Щелкните ОК для того, чтобы вернуться к диалоговому окну свойств файла OWNER.
10. Щелкните ОК для сохранения изменений и закройте диалоговое окно свойств файла OWNER.
11. Закройте Проводник и выйдите из системы.

10. Сменить владельца файла.

1. Зарегистрируйтесь в системе, используя учетную запись Имя_Студента1, затем запустите Windows Explorer.

2. Разверните папку Public.
3. Щелкните правой кнопкой мыши значок файла OWNER и выберите пункт меню Свойства.
4. В Windows XP Professional откроется диалоговое окно свойств файла OWNER с активной вкладкой Общие.
5. Перейдите на вкладку Безопасность для просмотра разрешений для файла.
6. Щелкните Дополнительно для открытия диалогового окна Дополнительные параметры безопасности для Owner и перейдите на вкладку Владелец.
7. В колонке Изменить владельца на выберите Имя_Студента1, затем щелкните кнопку Применить.
8. Кто теперь является владельцем файла OWNER?
9. Щелкните ОК, чтобы закрыть диалоговое окно Дополнительные параметры безопасности для Owner.
10. Щелкните ОК, чтобы закрыть диалоговое окно свойств файла OWNER.

11. Проверить разрешения для файла в качестве владельца.

1. Установите разрешение **Полный доступ** пользователю Имя_Студента1 к текстовому документу OWNER и щелкните кнопку Применить.
2. Щелкните кнопку Дополнительно и снимите флажок Наследовать от родительского объекта применимые к дочерним объектам разрешения, добавляя их к явно заданным в этом окне.
3. В диалоговом окне Безопасность щелкните кнопку Удалить.
4. Щелкните ОК, чтобы закрыть диалоговое окно Дополнительные параметры безопасности для Owner.
5. Щелкните ОК, чтобы закрыть диалоговое окно свойств файла OWNER.
6. Удалите текстовый документ OWNER.

12. Создать папку при подключении с учетной записью пользователя.

1. Пока вы зарегистрированы в системе пол учетной записью User1, в **Проводнике**, в корневой папке диска С, создайте папку с именем Temp1.
2. Закройте все приложения и закончите работу с Windows XP Professional.

13. Создание папки при подключении с учетной записью члена группы Администраторы.

1. Подключитесь с учетной записью Администратор или как пользователь, который является членом группы **Администраторы**, и запустите **Проводник**.
2. В корневой палке диска С: создайте папки Temp2 и Temp3.
3. Установите разрешения для папок Temp2 и Temp3. Снимите флажок **Наследовать от родительского объекта применимые к доченим объектам разрешения, добавляя их к явно заданным в этом окне**. В открывшемся диалоговом окне щелкните **Удалить** для удаления всех разрешений, кроме указанных явно.

Папка	Установите следующие разрешения
Temp2	Администраторы: Полный доступ Пользователи: Чтение и выполнение
Temp3	Администраторы: Полный доступ Операторы архива: Чтение и выполнение Пользователи : Полный доступ

14. Копирование папки в другую папку на одном и том же томе NTFS в Windows XP Professional

1. Пока вы находитесь в системе под учетной записью члена группы **Администраторы**, в **Проводнике**, скопируйте папку C:\Temp2 в папку C:\Templ. Для этого выделите значок папки C:\Temp2 и, удерживая нажатой клавишу CTRL, перетащите мышью C:\Temp2 в C:\Templ. Так как была произведена операция копирования, должны существовать обе папки: C:\Temp2 и C:\Templ\Temp2.
2. Выделите C:\Templ\Temp2, затем сравните разрешения и права владельца с папкой C:\Temp2.

15. Перемещение папки на одном и том же томе.

1. Зарегистрируйтесь в системе как пользователь User1.
2. В Проводнике выделите значок папки C:\Temp3, затем переместите ее в папку C:\Templ.
3. Что произошло с разрешения и владельцем для папки C:\Templ\ Temp3? Почему?
4. Закройте все окна и завершите сеанс работы.

16. Создание файла и запрет доступа к нему.

1. Войдите в систему, используя учетную запись члена группы Администраторы.
2. В папке C:\Temp1\Temp3 создайте текстовый документ с именем NOACCESS.
3. Запретите для группы Пользователи разрешение Полный доступ для текстового документа NOACCESS. В Windows XP Professional отобразится диалоговое окно Безопасность со следующим сообщением: «Вы запретили доступ для NOACCESS.txt. Никто не сможет получить доступ к NOACCESS.txt, и только владелец сможет изменить разрешения. Продолжить выполнение операции?»
4. Щелкните Да, чтобы изменения вступили в силу и чтобы закрыть диалоговое окно Безопасность.
5. Щелкните ОК, чтобы закрыть диалоговое окно свойств файла
6. NOACCESS.

17. Просмотр результата запрета разрешения Полный доступ к папке.

1. В Проводнике дважды щелкните значок текстового документа NOACCESS в папке Temp3 для того, чтобы открыть его.
2. Щелкните Пуск, затем — Выполнить.
3. В Windows XP Professional откроется диалоговое окно Выполнить.
4. Введите в текстовом поле Открыть cmd и щелкните ОК.
5. Перейдите в папку C:\Templ\Temp3.
6. Введите Del NOACCESS.TXT и нажмите клавишу ENTER.

Контрольные вопросы

1. Какое из следующих утверждений правильно описывает разрешения NTFS для папок и файлов?

– Система безопасности NTFS эффективна только в том случае, если пользователь получает доступ к файлу или папку при работе в сети.

– Система безопасности NTFS эффективна, если пользователь получает доступ к файлу или папке на локальном компьютере.

– Разрешения NTFS явно указывают, какие пользователи и группы могут получить доступ к файлам и папкам, и какие действия можно совершать с содержимым этих файлов и папок.

– Разрешения NTFS могут быть использованы для всех файловых систем, совместимых с Windows XP Professional.

2. Какое из следующих разрешений NTFS для папок позволяет удалить папку?

- Чтение.
- Чтение и выполнение.
- Изменение.
- Администрирование.

3. Какое разрешение NTFS для файлов следует установить для файла, если вы позволяете пользователям удалять файл, но не позволяете становиться владельцем файла?

4. Что такое список управления доступом (ACL)? Чем ACL отличается от элемента списка управления доступом (ACE)?

5. Что такое эффективные разрешения пользователя для ресурса?

6. Какие объекты по умолчанию наследуют разрешения, установленные для родительской папки?

7. Какое разрешение устанавливается для группы Все при форматировании тома?

8. Какие разрешения рекомендуется устанавливать при установке разрешений для папок общего доступа для группы Пользователи, а какие для группы Создатель-Владелец?

9. Кто может устанавливать разрешения для отдельных пользователей и групп?

- Члены группы Администраторы.
- Члены группы Опытные пользователи.
- Пользователи, обладающие разрешением Полный доступ.
- Владельцы файлов и папок.

10. Какой из следующих вкладок диалогового окна свойств файла или папки следует воспользоваться для установки или изменения разрешения NTFS для файла или папки?

- Дополнительно.
- Разрешения.
- Безопасность.
- Общие.

11. Каково назначение особого разрешения Обзор папок/Выполнение файлов?

12. Чем отличается разрешение Удаление от разрешения Удаление подпапок и фалов?

13. Какое из следующих утверждений о копировании файла или папки верно?

- При копировании фала из одной папки в другую на одном томе разрешения для файла не изменяются.
- При копировании файла из папки на томе NTFS в другую папку на томе NTFS разрешения для файла не изменяются.
- При копировании файла из одной папки на томе NTFS в другую папку на другом томе NTFS разрешения для файла совпадают с разрешениями для папки, в которую файл копируют.
- При копировании файла из папки на томе NTFS в другую папку на томе FAT разрешения для файла утрачиваются.

14. Какое из следующих утверждений о перемещении файла или папки верно?

- При перемещении файла из одной папки в другую на одном томе разрешения для файла не изменяются.

– При перемещении файла из папки на томе NTFS в другую папку на томе FAT разрешения для файла не изменяются.

– При перемещении файла из одной папки на томе NTFS в другую папку на другом томе NTFS разрешения для файла совпадают с разрешениями для папки, в которую файл перемещают.

– При перемещении файла из одной папки в другую на томе NTFS разрешения для файла не совпадают с разрешениями для папки, в которую файл перемещают.

15. С какими ограничениями следует устанавливать разрешения при установке разрешений NTFS?

16. Если вы хотите, чтобы пользователь или группа не имела доступа к определенной папке или файлу, следует ли запретить разрешения для этой папки или файла?

Лабораторная работа №8

Администрирование общих папок

Цель работы: Получить навыки предоставления доступа к папкам через сеть. Научиться предоставлять общий доступ к файловым ресурсам, обеспечивать их безопасность с помощью разрешений и доступ к ресурсам.

Начальные сведения об общих папках

Общие папки (shared folders) используются для предоставления пользователям в сети доступа к файловым ресурсам. Если к папке установлен общий доступ, пользователи могут обратиться к папке через сеть и получить доступ к содержащимся в ней файлам. Но для получения доступа к файлам, пользователи должны обладать разрешениями для доступа к общим папкам [2, 12].

В общей папке, называемой *личная папка* (home folder), содержатся приложения, данные или личные данные пользователя. Для каждого типа данных требуются различные разрешения для общих папок.

Ниже описаны характеристики разрешений для общих папок:

1. Разрешения для общих папок относятся к папкам, а не к отдельным файлам. Поскольку эти разрешения применяются только к папке в целом, а не к отдельным файлам или подпапкам в общей папке, они обеспечивают более низкий уровень безопасности, чем разрешения NTFS.

2. Разрешения для общих папок не ограничивают доступ пользователям, обращающимся к папке непосредственно на локальном компьютере, где хранится папка. Они действительны только для пользователей, обращающихся к папке через сеть.

3. Разрешения для общих папок являются единственным способом обеспечения безопасности сетевых ресурсов на томе FAT. Разрешения NTFS недоступны на томах FAT.

4. Разрешением для общих папок по умолчанию является **Полный доступ**, которое устанавливается для группы **Все** при предоставлении общего доступа к папке.

В **Проводнике** значок общей папки выглядит как рука, поддерживающая папку (рис. 8.1).

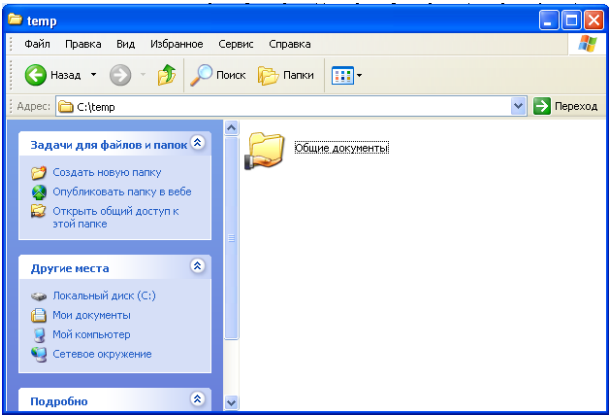


Рис. 8.1. Значок общей папки в Проводнике

Для того чтобы контролировать доступ пользователей к общей папке, необходимо установить разрешения для доступа к общим папкам. В таблице 8.1 перечислены возможности пользователя для каждого разрешения в порядке убывания ограничений.

Таблица 8.1

Разрешения для доступа к общим папкам

Разрешение	Возможности
Чтение	Позволяет просматривать имена файлов и папок, данные в файлах, их атрибуты; выполнять программные файлы и изменять папки внутри общей папки
Изменить	Позволяет создавать папки, добавлять файлы в папки, изменять данные в файлах, добавлять данные в файлы, изменять атрибуты файлов, удалять папки и файлы; а также выполнять все действия, что и разрешение Чтение
Полный доступ	Позволяет корректировать разрешения для файла, изменять владельца файла и выполнять все задачи, что и разрешение Изменить

Можно устанавливать или запрещать разрешения доступа к общим папкам. Как правило, предпочтительнее устанавливать разрешения для групп, а не для отдельных пользователей. Запрещайте разрешения только в том случае, если вы не хотите допустить действия уже установленных разрешений, например, если необходимо запретить разрешение определенному пользователю, принадлежащему к группе, для которой это разрешение назначено. Для полного запрета доступа к общей папке запретите разрешение **Полный доступ.**

Назначение разрешений для общих папок

Разрешения на доступ к общим папкам, предоставленные пользователям и группам, влияют на доступ к общей папке. Запрещение имеет более высокий приоритет, чем установленные разрешения. Ниже описаны эффекты применения разрешений.

Множественные разрешения. Пользователь может быть членом нескольких групп, для каждой из которых установлены различные разрешения, обеспечивающие разные уровни доступа к общей папке. При назначении разрешения на доступ к общим папкам пользователю, являющемуся членом группы, которой было предоставлено другое разрешение, эффективным разрешением будет комбинация разрешений пользователя и группы. Например, если для пользователя установлено разрешение **Чтение** и он является членом группы с разрешением **Изменить**, эффективным разрешением для него будет разрешение **Изменить**, которое включает в себя **Чтение**.

Запрещение разрешений. Запрет разрешений имеет преимущество над любыми разрешениями, установленными для отдельных пользователей и групп. Если запретить разрешение на доступ к общей папке пользователю, он не будет иметь доступа к ней, даже если установить данное разрешение для группы, членом которой он является.

Разрешения NTFS. Для доступа к файлам и папкам на томе FAT достаточно установить разрешения для общих папок. Однако на томе NTFS этого недостаточно. На томе FAT пользователи получают доступ не только к самой папке, для которой у них есть разрешение, но и к ее содержимому. Когда же пользователи получают доступ к общей

папке на томе NTFS, им понадобится разрешение для общих папок, а также соответствующие разрешения NTFS для каждого файла и папки, к которым они обращаются. Действующим разрешением для общих папок на томе NTFS считается наиболее строгое из всех разрешений.

При копировании общей папки оригинал остается общей папкой, а копия — нет. При переименовании или перемещении общая папка перестанет быть общей.

Руководство для установки разрешений для общей папки

Ниже приведены советы по управлению общими папками и назначении разрешений для общих папок.

1. Для каждого ресурса определите, каким группам необходим доступ к нему, уточните требуемый уровень доступа для каждой группы и составьте список групп и разрешений.

2. Для упрощения администрирования назначайте разрешения группам, а не отдельным пользователям.

3. Устанавливайте максимально строгие разрешения, которые, однако, должны давать возможность пользователям совершать требуемые действия. Например, если пользователям необходимо только чтение информации в папке, а удаление и создание файлов не требуется, следует назначить разрешение Чтение.

4. Организуйте ресурсы таким образом, чтобы папки с одинаковым уровнем требований безопасности находились в одной папке. Например, если пользователям нужно разрешение Чтение на доступ к нескольким папкам с приложениями, поместите все эти папки в одну. Затем установите общий доступ только к ней, а не задавайте общий доступ отдельно к каждой папке с приложениями.

5. Применяйте интуитивно понятные сетевые имена, чтобы пользователи смогли легко распознавать и находить их. Назначайте только такие имена, которые нее клиентские операционные системы смогут использовать.

Планирование, предоставление общего доступа и обращение к общим папкам

При планировании общего доступа к папкам можно облегчить администрирование и упростить доступ пользователей, надлежащим

образом организовав ресурсы, к которым будет предоставляться общий доступ, и разместив их по папкам согласно общим требованиям доступа. Также можно определить, к каким ресурсам предоставить общий доступ, организовать ресурсы согласно их назначению и решить, как именно вы будете администрировать эти ресурсы.

В общих папках могут содержаться приложения и данные. Используйте общие папки, содержащие приложения, для централизации администрирования и предоставления единого места, где пользователи смогут хранить и обращаться к часто используемым файлам. Если все файлы, содержащие данные, поместить в одну общую папку, пользователи смогут легко найти их. Если папки с данными и приложениями централизованы, то гораздо легче создавать резервные копии и обновлять программное обеспечение.

Можно предоставлять общий доступ к ресурсам, открывая общий доступ к папкам, содержащим эти ресурсы. Для предоставления общего доступа к папке необходимо быть членом одной из нескольких групп — в зависимости от назначения компьютера, на котором находится эта папка. Предоставляя общий доступ к папке, можно ограничивать число пользователей, которые одновременно получают доступ к ней, а также контролировать доступ к папке и ее содержимому посредством назначения разрешений для определенных пользователей и групп. С того момента как папка стала общей, для получения доступа к ней пользователям необходимо иметь соответствующие разрешения. После предоставления общего доступа к папке, возможно, понадобится изменить ее параметры. Можно запретить общий доступ к ней, изменить сетевое имя и разрешения для доступа к ней для пользователей и групп.

Некоторые общие папки используются для хранения приложений, установленных на сетевом сервере и могут быть востребованы с клиентских компьютеров. Основное преимущество приложений с общим доступом — не нужно устанавливать и поддерживать множество приложений на каждом компьютере. Хотя программные файлы для приложений разрешается хранить на сервере, информация о конфигурации для большинства сетевых приложений часто хранится на каждом клиентском компьютере. Выбор способа предоставления

общего доступа к папкам с приложениями зависит от приложений, вашего сетевого окружения и организации компании.

При предоставлении общего доступа к папкам, содержащим приложения, примите во внимание рекомендации, перечисленные далее.

1. Создайте одну общую папку для приложений и поместите все ваши приложения в эту папку. Таким образом, у вас будет единое место для установки и обновления программного обеспечения.

2. Назначьте группе **Администраторы** разрешение **Полный доступ** к папке, содержащей приложения. Таким образом, члены этой группы смогут управлять программным обеспечением и контролировать разрешения для пользователей.

3. Запретите разрешение **Полный доступ** группе **Все** и установите разрешение **Чтение** группе **Пользователи**.

4. Назначьте разрешение **Изменить** группам, члены которых отвечают за обновление ПО и устранение проблем с приложениями.

5. Создайте общую папку отдельно от папок, содержащих приложения, для любых приложений, для которых нужны другие разрешения. Затем установите соответствующие разрешения на доступ к этой папке.

Пользователи в сети обмениваются общими и рабочими данными с помощью папок с данными. К папкам с рабочими данными обращаются члены команды, которым необходим доступ к файлам с общим доступом, а также группы, которым нужен доступ к часто используемым данным.

Создайте и предоставьте общий доступ к папкам с часто используемыми данными на отдельном томе, не содержащем операционную систему и приложения. Рекомендуется часто создавать резервные копии и поэтому хранить папки с данными следует на отдельном томе. Если требуется переустановка операционной системы, том, содержащий папку с данными, не будет затронут.

При предоставлении общего доступа папке с часто используемыми общими данными, выполните следующие операции:

1. Используйте централизованные папки с данными для облегчения создания резервных копий данных.

2. Установите разрешение **Изменить** группе **Пользователи** на доступ к папке с часто используемыми данными. Таким образом, вы создадите единое доступное место хранения файлов, к которым пользователи смогут обеспечить доступ другим пользователям, предоставив им право читать, создавать и изменять файлы.

При предоставлении общего доступа к папке с рабочими данными, выполните следующие рекомендации:

1. Назначьте разрешение **Полный доступ** группе **Администраторы** на доступ к главной папке с данными для того, чтобы дать возможность администраторам управлять данными.

2. Если необходимо ограничить доступ к папкам с данными, находящимся в главной папке, установите разрешение общего доступа **Изменить** для соответствующих групп.

Требования к предоставлению общего доступа

В Windows XP Professional члены встроенных групп **Администраторы** и **Опытные пользователи** могут предоставлять общий доступ к папкам. Какие группы и на каких компьютерах могут предоставлять общий доступ к папкам, зависит от того, рабочая ли это группа или домен, а также от типа компьютера, на котором находятся эти папки.

В Windows XP Professional группа **Администраторы домена** может предоставлять общий доступ к папкам, расположенным на любом компьютере в домене.

Члены групп **Администраторы** и **Опытные пользователи** рабочей группы Windows имеют право предоставлять общий доступ к папкам, находящимся на автономном сервере Windows 2003 или компьютере, работающем под управлением Windows XP Professional, на котором хранится учетная запись этой группы.

Если папка, к которой планируется предоставить общий доступ, находится на томе NTFS, пользователям необходимо разрешение NTFS **Чтение** на доступ к этой папке, чтобы получить общий доступ к ней.

Административные общие папки

В Windows XP Professional по умолчанию предоставляется общий доступ к некоторым папкам для административных целей. Эти общие папки помечены знаком доллара ($), который скрывает их от пользователей при просмотре файлов компьютера. Корневой каталог каждого тома, системный корневой каталог и местоположение драйверов принтера относятся к скрытым общим папкам, доступ к которым вы можете получить через сеть.

Ниже описаны назначение административных общих папок, создаваемых по умолчанию в Windows XP Professional.

C$, D$, E$, и т. д. - к корневому каталогу каждого тома на жестком диске по умолчанию устанавливается общий доступ с сетевым именем буквы диска, к которой добавлен знак доллара. При обращении к данной папке вы получаете доступ ко всему тому. Административные общие папки используются для удаленного доступа к компьютеру для выполнения административных задач

Admin$ - для системного корневого каталога устанавливается по умолчанию имя C:\Windows, а сетевое имя — Admin$. Администраторы имеют право обращаться к этой общей папке для администрирования Windows XP Professional, не зная действительного имени папки, в которой установлены системные файлы. Только члены группы Администраторы имеют доступ к этой сетевой папке. В Windows XP Professional группе **Администраторы** назначается разрешение **Полный доступ**.

Print$ - при установке первого принтера с общим доступом сетевым именем папки %systemroot%\System32\Spool\Drivers становится Print$. Эта папка обеспечивает доступ к файлам драйвера принтера дли клиентов. Только членам групп **Администраторы** и **Опытные пользователи** предоставлено разрешение **Полный доступ**. Группе **Все** назначается разрешение **Чтение**.

Скрытые общие папки не только создаются системой автоматически. Можно обеспечить общий доступ к дополнительным папкам и добавить символ доллара в коней сетевого имени. Только те пользователи, которые знают точное имя папки, смогут получить доступ при условии наличия соответствующих разрешений.

Предоставление общего доступа к папке

При предоставлении общего доступа к папке, можно дать сетевое имя, создать комментарии для папки и ее содержимого, проконтролировать количество пользователей, имеющих доступ к папке, установить разрешения и установить общий доступ к одной папке несколько раз.

Вот как предоставить общий доступ к папке:

1. Войдите в систему под учетной записью пользователя, который входит в группу, имеющую возможность предоставлять общий доступ к папкам.

2. Щелкните правой кнопкой мыши значок папки, к которой нужно предоставить общий доступ, и выбрать пункт меню **Свойства**.

3. На вкладке **Доступ** диалогового окна свойств папки щелкните переключатель **Открыть общий доступ к этой папке** и настройте параметры, показанные на рис. 8.2 и описанные ниже.

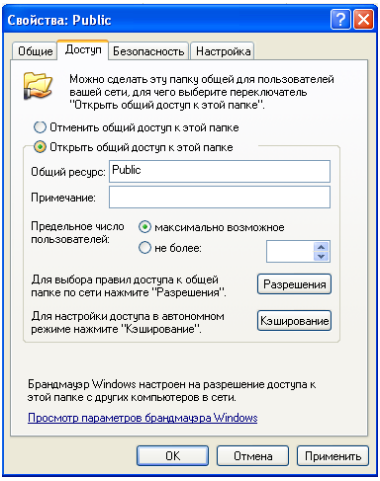


Рис. 8.2 Вкладка **Доступ** диалогового окна свойств папки

Таблица 8.2

Параметры вкладки Доступ

Параметр	Описание
Общий ресурс	Имя общей папки, используемое при удаленном обращении пользователем. Вы должны ввести имя общего ресурса. По умолчанию присваивается имя папки. Вы можете ввести другое имя длиной до 80 символов
Комментарий	Необязательное описание общего ресурса. Комментарий будет появляться вместе с именем общего ресурса при просмотре пользователями на клиентском компьютере общих папок на сервере. Комментарий позволяет распознавать содержимое папки
Предельное число пользователей	Предельное число пользователей, которые могут одновременно обращаться к общей папке. Если вы выберете в качестве предельного Максимально возможное, то имейте в виду, что Windows XP Professional поддерживает 10 соединений максимально. Сервер Windows 2003 поддерживает неограниченное число соединений, но количество приобретенных вами *клиентских лицензий* ограничивает соединения
Разрешения	Разрешения для общих папок действуют, только когда к папке обращаются через сеть. По умолчанию группе Все назначено разрешение Полный доступ для всех новых общих папок
Кэширование	Этот параметр позволяет настроить автономный доступ к данной общей папке
Новый общий ресурс	Этот параметр позволяет настроить несколько общих ресурсов и установить разрешения для этой папки. Параметр доступен, только если папка уже является общей

Установка разрешений для общих папок

После того как был предоставлен общий доступ к папке, следует явно указать, кто из пользователей получит доступ к общей папке. Для этого надо установить разрешения для общих папок определенным группам и пользователям.

1. На вкладке **Доступ** диалогового окна свойств папки щелкните кнопку **Разрешения**.

2. В диалоговом окне **Разрешения** выделите группу **Все**, затем щелкните кнопку **Удалить**.

3. В диалоговом окне **Разрешения** щелкните кнопку **Добавить**.

4. В диалоговом окне **Выбор: пользователи или группы** (рис. 8.3) в текстовом поле **Введите имена выбираемых объектов** введите имя пользователя или группы, для которого вы хотите установить разрешение.

Если требуется ввести более одного имени пользователи или группы за один раз, разделите имена точкой с запятой. Чтобы удостовериться, что имена введены правильно, щелкните кнопку **Проверить имена**.

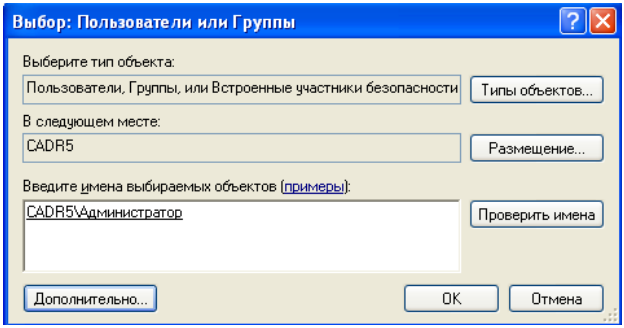


Рис. 8.3 Диалоговое окно **Выбор: пользователи или группы**

1. Щелкните **ОК**.

2. В диалоговом окне **Разрешения** для общей папки выделите имя пользователя или группы и затем в колонке **Разрешения** установите флажок **Разрешить** или флажок **Запретить** для соответствующего разрешения для пользователя или группы.

Кэширование

Для обеспечения автономной работы с общими папками копии файлов сохраняются на зарезервированной части диска вашего компьютера, называемой *кэш* (cache). Поскольку кэш находится на жестком диске, компьютер может обращаться к нему независимо от наличия соединения с сетью. По умолчанию размер кэша равен 10% свободного места на диске. Можно изменить размер кэша, используя вкладку **Автономные файлы** диалогового окна **Свойства папки**. Чтобы узнать размер кэша, достаточно открыть папку **Автономные файлы** и щелкнуть пункт **Свойства** в меню **Файл**.

При назначении общего доступа к папке вы можете разрешить другим пользователям работать с общей папкой автономно, щелкнув в диалоговом окне свойств папки кнопку **Кэширование**. В диалоговом окне **Параметры кэширования** (рис. 8.4) установите флажок **Разрешить кэширование файлов в этой папке** для включения кэширования.

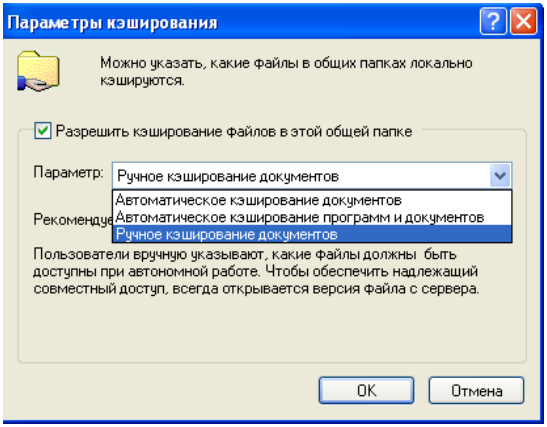


Рис. 8.4 Диалоговое окно **Параметры кэширования**

В диалоговом окне **Параметры кэширования** можно установить три варианта кэширования.

1. Ручное кэширование документа. Пользователи вручную указывают все файлы, которые должны быть доступными при автономной работе. Этот параметр, устанавливаемый по умолчанию, рекомендуется при работе с общей сетевой папкой, содержащей файлы, которые имеют право изменять несколько пользователей. Для обеспечения надлежащего совместного доступа всегда открывается версия файла с сервера.

2. Автоматическое кэширование документов. Каждый файл в общей папке, открываемый пользователем, становится доступным при автономной работе. Файлы, которые не открывались, не доступны при автономной работе. Каждый раз, когда открывается файл, ранняя копия файла автоматически удаляется. Для обеспечения надлежащего совместного доступа всегда открывается версия файла с сервера.

3. Автоматическое кэширование программ и документов. Предоставляется автономный доступ к общим папкам, содержащим файлы, которые пользователи читают, на которые ссылаются, запускают, но не изменяют в процессе работы. Данный параметр кэширования снижает сетевой трафик, так как автономные файлы открываются без доступа к сетевым версиям, и. как правило, автономные файлы обычно запускаются и выполняются быстрее, чем сетевые версии. Использование автоматического кэширования программ и документов рекомендуется для папок, содержащих данные, которые доступны только для чтения и для приложений, запускаемых удаленно.

Создание нескольких имен для общих ресурсов.

Иногда требуется установить различные разрешения для общей папки. Вы можете создавать несколько имен для одной папки и устанавливать различные разрешения для каждого имени. Для предоставления общего доступа к папке с множественными именами щелкните кнопку **Новый общий ресурс** в диалоговом окне свойств папки. В открывшемся диалоговом окне **Новый общий ресурс** (рис. 8.5) можно назначить новое имя, ограничить количество подключений к этому общему ресурсу. Также можете щелкнуть кнопку **Разрешения** для установки разрешений на доступ к данной папке.

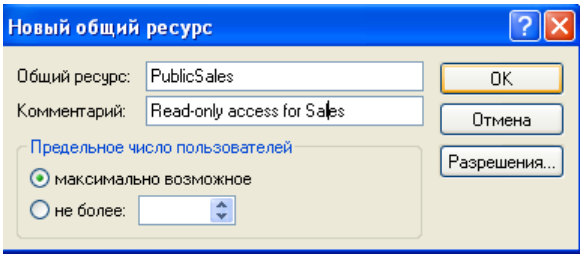


Рис. 8.5 Диалоговое окно **Новый общий ресурс**

Изменение параметров общей папки

Можно изменить параметры общей папки, отменить общий доступ к ней и отредактировать разрешения для нее. Чтобы изменить параметры общей папки в диалоговом окне свойств общей папки перейдите на вкладку **Доступ**.

Изменить параметры общей папки можно следующим образом:

1. Прекратить общее использование папки - щелкните **Отменить общий доступ к этой** папке.

2. Изменить имя общего ресурса - щелкните **Отменить общий доступ к этой папке** для отмены общего доступа к этой папке и далее — кнопку **Применить**. Затем щелкните **Открыть общий доступ к этой папке** и введите новое сетевое имя в текстовом поле **Общий ресурс.**

3. Изменить разрешения для общей папки - щелкните кнопку **Разрешения**. В открывшемся диалоговом окне **Разрешения** щелкните кнопку **Добавить** для добавления пользователя или группы, чтобы явно указать разрешения для них, или щелкните кнопку **Удалить** дли удаления пользователя или группы. В диалоговом окне **Выберите тип объекта: Пользователи, Группы или Встроенные участники безопасности** выделите пользователя или группу, разрешения для которых вы хотите изменить. Затем щелкните флажок **Разрешить** или **Запретить** для соответствующего разрешения

Если отменили общий доступ к папке, в то время как пользователь открыл файл, данные могут быть потеряны. Если щелкнуть переключатель **Отменить общий доступ к этой папке** в то время когда пользователь обращается к общей папке, в Windows XP

Professional откроется диалоговое окно с соответствующим уведомлением.

Обращение к общей папке

Можно получить доступ к общей папке, используя компоненты **Сетевое окружение** и **Мой компьютер**, **Мастер добавления в сетевое окружение** и команду **Выполнить** из меню **Пуск**.

Для соединения с общей папкой с помощью компонента **Сетевое окружение** выполните следующие действия:

1. Щелкните **Пуск.** Когда вы начинаете работу с **Сетевым окружением**, этот пункт добавится в меню **Пуск**. Если пункт **Сетевое окружение** уже отображается в меню **Пуск**, щелкните его и переходите к пункту 4.

2. Щелкните **Панель управления**, а затем **— Сеть и подключения к Интернету**.

3. В окне **Сеть и подключения к Интернету** в разделе **См. также** щелкните **Сетевое окружение**.

4. Дважды щелкните значок общего ресурса, к которому вы хотите получить доступ. Если общий ресурс, к которому вы хотите получить доступ, включен в список, то, дважды щелкнув его левой кнопкой мыши, вы подключитесь к нему. Если общий ресурс не включен в список, перейдите к пункту 5.

5. Если общий ресурс, к которому вы хотите получить доступ, не включен в список, щелкните значок **Добавить новый элемент в сетевое окружение**. Откроется окно **Мастера добавления в сетевое окружение**.

6. Щелкните кнопку **Далее**.

7. На странице **Укажите, где вы хотите создать сетевое размещение** щелкните **Выберите другое сетевое размещение**, затем щелкните **Далее**.

8. На странице **Укажите адрес этого сетевого размещения** вы можете ввести путь к папке в формате **UNC** *(\\имя_компьютера\ имя_общей папки;* см. рис. 8.6), затем щелкните **Далее**.

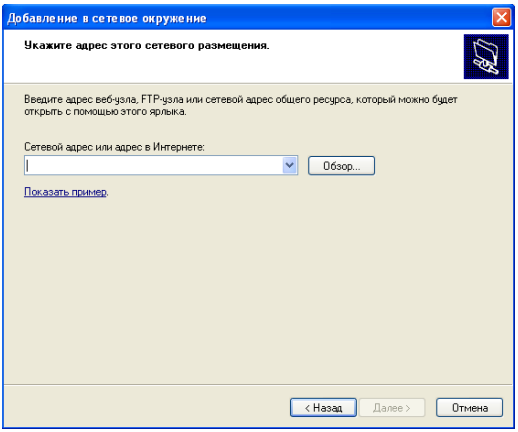


Рис. 8.6 Страница **Укажите адрес этого сетевого размещения**

Для соединения с общей папкой с помощью компонента **Мой компьютер** выполните следующие операции:

1. Щелкните **Пуск**, затем — **Мой компьютер**.

2. В меню **Сервис** щелкните пункт **Подключить сетевой диск**. В Windows XP Professional откроется окно **Подключить сетевой диск** (рис. 8.7), в котором вы сможете установить букву диска для соединения. По умолчанию диск обозначается буквой Z или последней незадействованной буквой алфавита.

3. В текстовом поле **Папка** укажите путь *\\сервер\общий_ресурс* или щелкните кнопку **Обзор** для поиска общего ресурса. По умолчанию установлен флажок **Восстанавливать при входе в систему**.

4. Снимите флажок **Восстанавливать при входе в систему**, если вы не хотите, чтобы в Windows XP Professional в последующих сеансах автоматически создавалось соединение с этим общим ресурсом.

5. Щелкните кнопку **Готово** для установки соединения. Соединение с общей папкой включено в раздел **Сетевые диски** окна **Мой компьютер**.

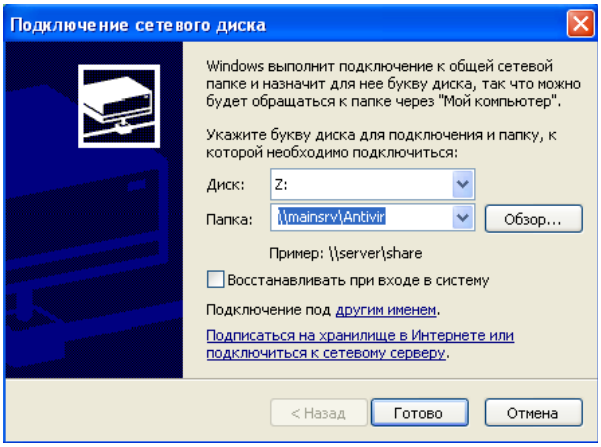


Рис. 8.7 Диалоговое окно **Подключить сетевой диск**

Для соединения с общей папкой с помощью команды **Выполнить** выполните следующие операции:

1. Щелкните **Пуск**, затем — **Выполнить** и введите в открывшемся текстовом поле **Открыть** *\\имя_компьютера*. В Windows XP Professional откроется окно с общими папками указанного компьютера.

2. Дважды щелкните значок общей папки, к которой вы хотите получить доступ.

Объединение разрешений для общей папки и разрешений NTFS

Общий доступ к папкам предоставляется для того, чтобы пользователи в сети смогли обращаться к ресурсам компьютера. При работе с томом FAT разрешения для общих папок являются единственным способом обеспечить безопасность общих папок и их содержимого. На томе NTFS можно назначить разрешения NTFS отдельным пользователям и группам, что облегчит управление доступом к файлам и подпапкам, содержащимся в общей папке. При объединении разрешений для общей папки и разрешений NTFS наиболее строгое разрешение всегда имеет приоритет над другими.

Стратегии объединения разрешений для общей папки и разрешений NTFS

Одна из стратегий предоставления доступа к ресурсам тома NTFS - предоставление общего доступа с установленными по умолчанию разрешениями к общим папкам и последующее управление доступом при помощи установки разрешений NTFS. При предоставлении общего доступа к папке на томе NTFS разрешения для общей папки и разрешения NTFS объединяются, что более полно обеспечивает безопасность ресурсов.

Разрешения для общих папок ограничивают уровень безопасности ресурсов. Наибольшей гибкости при управлении доступом к общим папкам вы добьетесь, используя разрешения NTFS. Они действуют независимо от того, происходит ли обращение к ресурсу, размещенному на локальном компьютере или в сети.

При назначении разрешений на доступ к общей папке на томе NTFS действуют следующие правила:

1. Можно применять разрешения NTFS для файлов и подпапок в общей папке, а также различные разрешения NTFS для каждого файла и каждой подпапки в общей папке.

2. В дополнение к разрешениям на доступ к общим папкам пользователям необходимы разрешения NTFS для доступа к файлам и подпапкам, содержащимся в общей папке. Что касается томов FAT, то в этом случае разрешения для общей папки — единственные, которые обеспечивают безопасность файлов и подпапок в общей папке,

3. При объединении разрешения на доступ к общей папке и разрешений NTFS наиболее строгое разрешение всегда имеет приоритет над остальными.

Задания для выполнения

1. Назначить разрешения для доступа к ресурсам пользователю User101 - как отдельному пользователю и как члену группы (рис. 8.8).

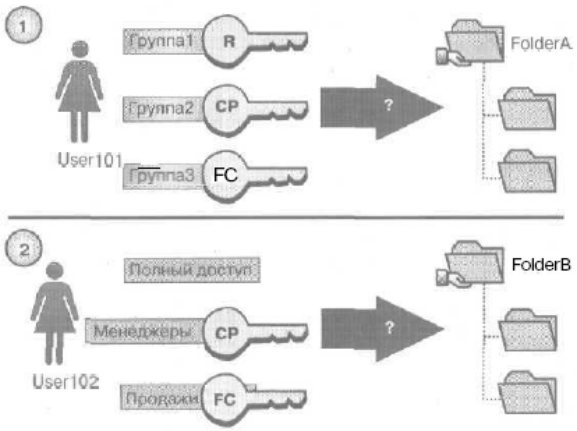


Рис. 8.8 Применяемые разрешения

2. Определить, какие эффективные разрешения установлены для пользователя User101 и для пользователя User102.

1. Пользователь User101 является членом групп Группа1, Группа2 и ГруппаЗ. У группы Группа1 есть разрешение **Чтение**. У Группы2 есть разрешение **Полный доступ** для папки FolderA. ГруппаЗ обладает разрешением **Изменить**, установленным для папки FolderA. Каковы эффективные разрешения пользователя User101 для папки FolderA?

2. Пользователю User102 назначено разрешение **Полный доступ** для общей папки FolderB, как отдельному пользователю. Пользователь User102 является членом группы Менеджеры, для которой было установлено разрешение **Изменить** для папки FolderB, и группы **Продажи**, которой был запрещен доступ к папке FolderB. Каковы эффективные разрешения пользователя User102 на доступ к папке FolderB?

3. На рис. 8.9 показаны примеры общих папок на томах NTFS. В этих общих папках содержатся под папки, для которых также

установлены разрешения NTFS. Определите эффективные разрешения для пользователя для каждого примера.

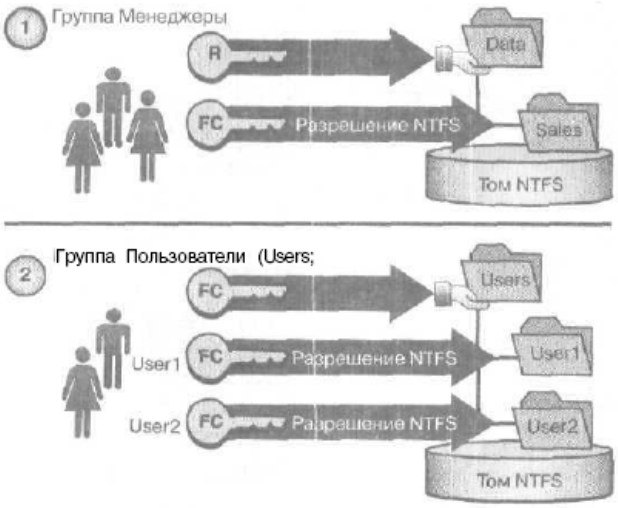


Рис. 8.9 Объединенные разрешения

В первом примере папка Data является общей. Группе **Менеджеры** назначено разрешение **Чтение** на доступ к общей папке Data и разрешение NTFS **Полный доступ** на доступ к подпапке Sales. Какие разрешения группы Менеджеры будут действовать при получении доступа к подпапке Sales путем установки соединения с общей папкой Data?

Во втором примере в папке **Users** содержатся личные папки пользователей. В каждой такой папке содержатся данные, доступные только пользователю, именем которого названа папка. Папка Users сделана общей, и группе **Пользователи** для доступа к ней назначено разрешение общих папок **Полный доступ**. Для пользователей User1 и User2 назначены разрешения NTFS **Полный доступ** для их личных папок и не назначено никаких разрешений NTFS для остальных папок. Пользователи User1 и User2, принадлежат к группе **Пользователи**.

4. Спланировать общий доступ к ресурсам на серверах. Зафиксируйте ваши решения в таблице, помещенной в конце этого упражнения. Рис. 8.10 иллюстрирует структуру папок для серверов.

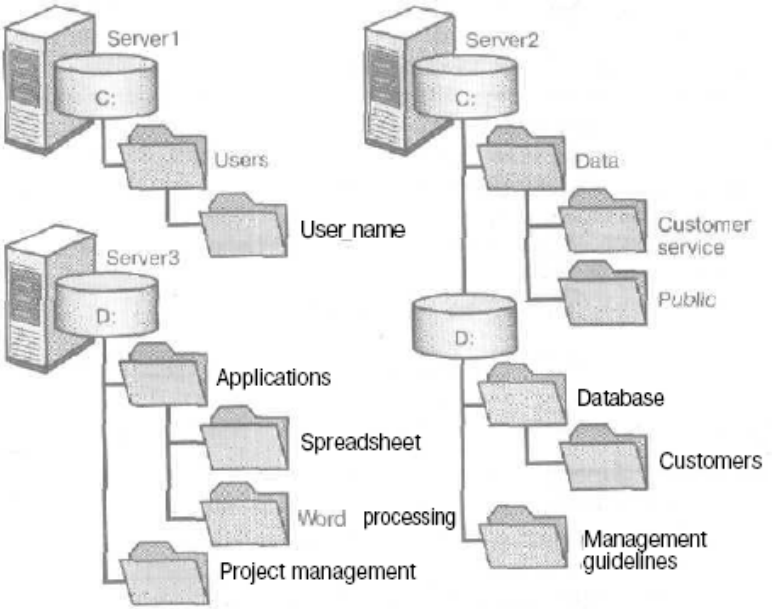


Рис. 8.10 Структура папок для серверов промышленной компании

Нужно предоставить доступ к ресурсам, расположенным на сервере, пользователям сети. Для этого определите, к каким папкам вы собираетесь предоставить общий доступ и какие разрешения вы установите для групп, включая соответствующие встроенные группы. Принимая решения, руководствуйтесь соображениями, перечисленными ниже.

– Членам группы **Менеджеры** (Managers) необходим доступ на чтение и изменение документов в папке Management Guidelines. Никто более не должен иметь доступ к этой папке.

– Администраторы должны получить полный доступ ко всем общим папкам, кроме папки Management Guidelines.

– Сотрудники клиентского отдела нуждаются в собственном дисковом пространстве для хранения рабочих файлов. Все представители клиентского отдела являются членами группы **Клиентский отдел**.

– Всем сотрудникам требуется дисковое пространство для обмена информацией друг с другом.

– Все сотрудники работают с такими программными продуктами, как электронные таблицы, базы данных и текстовые редакторы.

– Только члены группы **Менеджеры** (Managers) должны иметь доступ к программному обеспечению для управления проектами.

– Членам группы CustomerDBFull необходим доступ на чтение и обновление базы данных по клиентам.

– Членам группы CustomerEiBRead требуется только доступ на чтение базы данных о клиентах.

– Каждому пользователю следует выделить отдельное дисковое пространство для хранения личных файлов.

Зафиксируйте свои ответы в таблице.

Имя и расположение папки	Сетевое имя	Группы и разрешения
Пример: Management Guidelines	MgmtGd	Менеджеры: Полный доступ

5. Предоставьте общий доступ к папкам.

1. Подключитесь под учетной записью члена группы **Администраторы**. Запустите **Проводник**, создайте папку C:\MktApps, щелкните правой кнопкой мыши значок папки и выберите пункт меню **Свойства**.

2. В диалоговом окне свойств папки MktApps перейдите на вкладку **Доступ**.

3. Щелкните переключатель **Открыть общий доступ к этой папке**.

4. По умолчанию сетевое имя соответствует имени папки. Если вы хотите установить другое имя, введите его в текстовом поле **Общий ресурс**.

5. В текстовом поле **Комментарий** введите **Общие маркетинговые приложения** и щелкните **ОК.**

6. В **Проводнике** изменится значок папки MktApps: в нем появится рука, указывающая, что теперь это обшая папка.

6. Установите разрешения для общей папки.

1. **Определите текущие разрешения для общей папки MktApps.** В **Проводнике** щелкните правой кнопкой мыши значок папки C:\MktApps и выберите пункт меню **Общий доступ и безопасность**. В Windows XP Professional откроется диалоговое окно свойств папки MktApps с активной вкладкой **Доступ**. Щелкните кнопку **Разрешения**. В Windows XP Professional откроется диалоговое окно **Разрешения для MktApps**. По умолчанию группе **Все** назначено разрешение **Полный доступ**.

2. **Удалите разрешении для группы.** Убедитесь, что группа **Все** выделена. Щелкните кнопку **Удалить.**

3. **Установка разрешений для группы.** Щелкните кнопку **Добавить**. В Windows XP Professional откроется диалоговое окно **Выбор: Группы или Пользователи**. В текстовом поле **Введите имена выбираемых объектов** введите Administrators и щелкните **ОК**. В Windows XP Professional к списку имен с разрешениями добавится группа **Администраторы**. Какой тип разрешений устанавливается по умолчанию в Windows XP Professional для группы **Администраторы**? В диалоговом окне **Разрешения для Администраторы** в колонке **Разрешить** установите флажок **Полный доступ**. Почему в **Проводнике** также было выделено разрешение **Изменить**? Щелкните кнопку **Добавить**. В Windows XP Professional откроется диалоговое окно **Выбор: Группы или Пользователи**. В текстовом поле **Введите имена выбираемых объектов** введите Users и щелкните ОК. В Windows XP Professional группа **Пользователи** будет добавлено к списку имен. По умолчанию для группы **Пользователи** будет установлено разрешения **Чтение**. Щелкните **ОК**, чтобы закрыть диалоговое окно **Разрешения для MktApps**. Щелкните **ОК**, чтобы

закрыть диалоговое окно свойств папки MktApps. Закройте **Проводник**.

7. Отмените общий доступ к папке

1. Зарегистрируйтесь под учетной записью **Администратор** на компьютере PRO1 (или на компьютере, работающем под управлением Windows XP Professional с установленным вами именем), затем запустите **Проводник**.
2. Щелкните правой кнопкой мыши значок папки C:\MktApps и выберите пункт меню **Общий доступ и безопасность**.
3. Щелкните переключатель **Отменить общий доступ к этой папке**, затем щелкните **ОК**. Откроется диалоговое окно **Доступ** с сообщением, что файл все еще открыт, и запросом, хотите ли вы продолжить.
4. Щелкните **Да** для продолжения. В Windows XP Professional более не виден значок в виде руки для папки MktApps, указывающий общую папку. Возможно, вам для этого необходимо обновить экран, нажав F5.
5. Закройте **Проводник**.

8. Установите разрешения NTFS и разрешения для общих папок

1. Откройте **Проводник** и создайте папку C:\MktApps.
2. На вкладке **Безопасность** диалогового окна свойств папки MktApps добавьте группу **Администраторы** и установите разрешение NTFS **Полный доступ**.
3. Добавьте группу **Пользователи** и установите для нее разрешение NTFS **Чтение и выполнение**.
4. Удалите группу **Все**. Прежде чем вы удалите группу **Все**, нужно снять флажок **Наследовать от родительского объекта применимые к дочерним объектам разрешения** в диалоговом окне **Дополнительные параметры безопасности для MktApps**. При запросе удалите элементы разрешений, ранее унаследованные от родительского объекта.
5. Щелкните **ОК**, чтобы закрыть диалоговое окно **Дополнительные параметры безопасности для MktApps**, затем щелкните **ОК**, чтобы закрыть диалоговое окно свойств папки MktApps.

6. Воспользуйтесь **Проводником** для создания папки C:\MktApps\Manuals.

7. В диалоговом окне дополнительных параметров безопасности для папки Manuals снимите флажок **Наследовать от родительского объекта применимые к дочерним объектам разрешения** и при запросе щелкните **Удалить**, чтобы удалить элементы разрешений, ранее унаследованные от родительского объекта.

8. Щелкните кнопку **Добавить** и добавьте группу **Администраторы** с разрешением NTFS **Полный доступ**.

9. Щелкните **ОК**, чтобы закрыть диалоговое окно **Элемент разрешения для Manuals**.

10. Щелкните **ОК**, чтобы закрыть диалоговое окно **Дополнительные параметры безопасности для Manuals**.

11. Добавьте группу **Пользователи** с разрешением NTFS **Чтение и выполнение**.

12. Воспользуйтесь **Проводником** для создания папки C:\MktApps\Public.

13. Снимите флажок **Наследовать от родительского объекта применимые к дочерним объектам разрешения**. При запросе удалите элементы разрешений, ранее унаследованные от родительского объекта.

14. Щелкните кнопку **Добавить** и добавьте группу **Администраторы** с разрешением NTFS **Полный доступ**.

15. Щелкните **OK,** чтобы закрыть диалоговое окно **Элемент разрешения для Public**.

16. Щелкните **ОК**, чтобы закрыть диалоговое окно **Дополнительные параметры безопасности для Public**.

17. Добавьте группу **Пользователи** с разрешением NTFS **Чтение и выполнение**.

9. Откройте общий доступ к папке MktApps и установите разрешения для пользователей, работающих в сети, основываясь на информации в следующей таблице. Удалите все остальные разрешения для общих папок.

Путь и имя общей папки	**Группа или пользователь**	**Разрешения для общей папки**
C:\MktApps, сетевое	Администраторы	Полный доступ

имя MktApps		
C:\MktApps, сетевое имя MktApps	Пользователи	Полный доступ

Контрольные вопросы

1. Вы используете разрешения NTFS для того, чтобы явно указать, какие пользователи и группы имеют доступ к файлам и папкам и какие действия можно совершать с содержимым этих файлов или папок. Для чего нужны общий доступ к папке и разрешения для общих папок?

2. Какие из следующих разрешений являются разрешениями для общих папок? (Выберите все правильные ответы.)

- Чтение.
- Запись.
- Изменить.
- Полный доступ.

3. Какие приоритеты имеют разрешения общих папок друг для друга (запрещенные/установленные)?

4. При копировании общей папки копируемая папка более не является общей, а скопированная не становится общей?

5. Является ли общая папка все еще общей при ее перемещении?

6. Является ли общая папка все еще общей при ее переименовании?

7. Что такое общая папка с приложениями? Каково основное преимущество использования приложений с общим доступом?

8. Какие группы при работе в рабочих группах Windows могут предоставлять общий доступ только к папкам, хранящимся на автономном сервере Windows 2003 или компьютере, работающем под управлением Windows XP Professional, на котором находится учетная запись этой группы?

9. В Windows XP Professional автоматически предоставляется общий доступ к папкам для административных целей. Каким значком отмечаются эти ресурсы, который скрывает их от пользователей при просмотре файлов на компьютере?

10. Какое имя имеет сетевой системный корневой каталог, устанавливаемый по умолчанию как C:\Windows? Администраторы

могут обращаться к этой папке для администрирования Windows XP Professional, не зная действительного имени папки, в которой установлены системные файлы. Только члены группы **Администраторы** имеют доступ к этой сетевой папке. В Windows XP Professional назначается разрешение **Полный доступ** группе **Администраторы**.

11. Какими из вкладок следует воспользоваться для назначения разрешений пользователям и группам общей папки?

- Вкладкой Разрешения диалогового окна свойств общей папки.
- Вкладкой Доступ диалогового окна свойств общей папки.
- Вкладкой Общие диалогового окна свойств общей папки.
- Вкладкой Безопасность диалогового окна свойств общей папки.

12. Какое утверждение о размере КЭШа, необходимого для обеспечения автономного доступа к общим папкам, верно?

- По умолчания размер КЭШа равен 20% свободного места на диске.
- По умолчанию размер КЭШа равен 15% свободного места на диске.
- По умолчанию размер КЭШа равен 10% свободного места на диске.
- По умолчанию размер КЭШа равен 5% свободного места на диске.

13. Наиболее строгое разрешение всегда приоритетнее, если вы используете и разрешения для общих папок и разрешения NTFS?

14. Какое из следующих утверждений об объединении разрешений для общих папок и разрешений NTFS верно? (Выберите все правильные ответы.)

- Вы можете использовать разрешения общих папок для любых папок с общим доступом.
- Разрешение для общих папок **Изменить** более строгое, чем разрешение NTFS **Чтение**.
- Вы можете использовать разрешения NTFS для всех общих папок.

- Разрешение NTFS **Чтение** считается более строгим, чем разрешение **Изменить** для общей папки.

15. Какое из следующих утверждений о разрешениях NTFS и разрешениях для общей папки верно? (Выберите все правильные ответы.)

- Разрешения NTFS применяются только при обращении через сеть.
- Разрешения NTFS применяются независимо от того, происходит ли обращение к ресурсу локально или через сеть.
- Разрешения для общих папок применяются только при обращении через сеть.
- Разрешения для общих папок применяются независимо от того, происходит ли обращение к ресурсу локально или через сеть.

16. Какие разрешения вы можете установить при необходимости для каждой папки, файла или подпапки?

Библиографический список

1. Олифер В.Г., Олифер Н.А.. Компьютерные сети. Принципы, технологии, протоколы: Учебник для вузов 4-е изд. - СПб.: Питер, 2012. - 944 с.: ил.

2. В.Г. Олифер, Н.А.Олифер. Сетевые операционные системы. «Питер», 2005.

3. TCP/IP. Учебный курс: Пер. с англ. /Л.А. Чеппел, Э. Титтел. -СПб: БХВ-Петербург, 2003г. -953с.

4. Основы сетей передачи данных. Курс лекций: учебное пособие /В.Г Олифер, Н.А. Олифер – изд. 2-е, испр. – М: Интернет-Университет Информационных Технологий, 2005г. - 174 с.

5. Бэрри Нанс. Компьютерные сети. М., Восточная Книжная Компания, 1996.

6. Чекмарев А.Н., Вишневский А.В., Кокорева О.И. Microsoft Windows Server 2003. Русская версия / Под общ. ред. А.Н. Чекмарева. - СПб.: БХВ-Петербург, 2008. - 1120 с.: ил.

7. Танненбаум Э., Уэзеролл Д. Компьютерные сети. – СПб.: Питер, 2012. - 960 с.: ил.

8. Компьютерные сети. Учебный курс, 2-е изд. (+CD-ROM). – Microsoft Press, Русская редакция, 1998.

9. Блэк Ю. Сети ЭВМ: Протоколы, стандарты, интерфейсы: пер. с англ.-М.:Мир, 1990.-506 с.: ил.

10. Microsoft TCP/IP. Учебный курс: Официальное пособие Microsoft для самостоятельной подготовки: Пер. с англ. – 2-е изд., испр.-М.:Издательско-торговый дом «Русская редакция», 1999.-344с.

11. Моримото, Р. Microsoft Windows Server 2008 R2. Полное руководство / Р. Маримото, М. Ноэл, О. Драуби и др.; пер. с англ. Я.П. Волкова [и др.]. – М.: ООО «И.Д. Вильямс», 2011. – 1456 с.: ил.

12. Microsoft Windows XP Professinal/ Учебный курс Microsoft / Пер. с англ. - 3-е изд., испр. - М.: «Русская редакция», 2008. - 704 стр.: ил..