Министерство образования и науки Российской Федерации
федеральное государственное бюджетное образовательное учреждение высшего образования
"Российский экономический университет имени Г.В.Плеханова"
МОСКОВСКИЙ ПРИБОРОСТРОИТЕЛЬНЫЙ ТЕХНИКУМ

УТВЕРЖДАЮ:
Заместитель директора
по учебной работе
_____ Д. А. Клопов
«31» августа 2017 год

ВАРИАНТЫ ЗАДАНИЙ ПРАКТИЧЕСКИХ РАБОТ

учебной дисциплины ОП 01. Операционные системы

код, специальность
09.02.03 Программирование в компьютерных системах
квалификация: техник - программист

Форма проведения: выполнение практического задания

Составил:
Преподаватель ФГБОУ ВО «РЭУ им. Г.В. Плеханова», Минаев К.А.
Должность, ФИО

РАССМОТРЕНО
На заседании цикловой методической комиссии

«Общепрофессиональных дисциплин (программное обеспечение)»
Протокол № 1-17/18 ЗК от «28» августа 2017г

Председатель ЦМК _____/Волкова Г.Ю. /

ПЕРЕЧЕНЬ
ПРАКТИЧЕСКИХ РАБОТ
(общее время на выполнение – 50 ч.)

Составлен в соответствии с рабочей программой по данной дисциплине.

1. Работа в оболочке командной строки. PowerShell, CMD.
2. Создание сценариев в PowerShell, создание скриптов(*.bat)
3. Работа с пользователями. Программный интерфейс. Файловая система ОС Windows.
4. PowerShell как средство автоматизации, работа с оснастками, командлеты
5. Установка и предварительная настройка ОС, Windows, Unix.
6. Реестр ОС. Работа с реестром в Windows. RegEdit, PowerShell.
7. Файловый менеджер Far Manager. Управление доступом к файловым ресурсам.
8. Основы работы в Unix-системах.
9. Linux: Работа с конфигурационными файлами, настройка системы. Средства администрирования системы.
10. Работа с файлами и каталогами в Linux. Файловые менеджер Midnight Commander. Bash. Gparted
11. Управление пользователями и группами в ОС Unix.
12. Управление процессами ОС Linux
13. Создание пользовательских скирптов ОС Unix
14. Настройка и работа с сетью. Конфигурирование сети ОС Unix.
15. Установка и настройка WEB-сервера ОС Unix, ОС Windows.
16. Резервное копирование и восстановление данных в Windows, Unix.
17. Брандмауэры, основы работы в Unix.
18. Основные правила и требования шифрованию данных в операционных системах. ПО обеспечивающие пользовательское шифрование.
19. Осуществление настройки сетевых протоколов серверов и рабочих станций
20. WindowsServer: Обеспечение работы системы регистрации и авторизации пользователей сети
21. WindowsServer: Осуществление системного администрирования локальных сетей

ИНФОРМАЦИОННОЕ ОБЕСПЕЧЕНИЕ РЕАЛИЗАЦИИ ПРОГРАММЫ

Основная литература:

1. **Операционные системы и среды** : учебник / Рудаков А.В. — М.: КУРС: ИНФРА-М, 2018. — 304 с. — (Среднее профессиональное образование).
http://znanium.com/catalog/product/946815

2. **Информационная безопасность и защита информации**: Учебное пособие / Баранова Е.К., Бабаш А.В., - 4-е изд., перераб. и доп. - М.:ИЦ РИОР, НИЦ ИНФРА-М, 2018. - 336 с.
http://znanium.com/catalog/product/957144

3. **Операционные системы. Основы UNIX** : учеб. пособие / А.Б. Вавренюк, О.К. Курышева, С.В. Кутепов, В.В. Макаров. — М. : ИНФРА-М, 2018. — 160 с.
http://znanium.com/catalog/product/958346

Дополнительная литература:

4. **Комплексная защита информации в корпоративных системах** : учеб. пособие / В.Ф. Шаньгин. — М. : ИД «ФОРУМ» : ИНФРА-М, 2017. — 592 с.
http://znanium.com/catalog/product/546679

5. **Операционные системы, среды и оболочки** : учебное пособие / Т.Л. Партыка, И.И. Попов. — 5-е изд., перераб. и доп. — М. : ФОРУМ : ИНФРА-М, 2017. — 560 с. : ил. — (Профессиональное образование).
http://znanium.com/catalog/product/552493

Министерство образования и науки Российской Федерации
федеральное государственное бюджетное образовательное учреждение высшего образования
"Российский экономический университет имени Г.В. Плеханова"
МОСКОВСКИЙ ПРИБОРОСТРОИТЕЛЬНЫЙ ТЕХНИКУМ

ПРАКТИЧЕСКАЯ РАБОТА № 1
ДИСЦИПЛИНА: ОПЕРАЦИОННЫЕ СИСТЕМЫ

Тема: 1. Работа в оболочке командной строки. PowerShell, CMD.

Специальность: 09.02.03 «Программирование в компьютерных системах»
Квалификация: техник-программист

Цель работы: знакомство с основными возможностями оболочки командной строки Windows PowerShell, CMD.

Время выполнения работы: 2 академических часа.

Теоретический материал

Теоретический материал описан в документе описание лабораторных и практических работ по предмету «Операционные системы».

Цели и задачи создания новой оболочки

Новая оболочка Windows PowerShell была задумана разработчиками Microsoft как более мощная среда для написания сценариев и работы из командной строки.

Разработчики PowerShell преследовали несколько целей, главная из которых – создание среды составления сценариев, которая наилучшим образом подходила бы для современных версий ОС Windows и была бы более функциональной, расширяемой и простой в использовании, чем какой-либо аналогичный продукт для любой другой ОС. В первую очередь эта среда должна была подходить для решения задач, стоящих перед системными администраторами, а также удовлетворять требованиям разработчиков программного обеспечения, предоставляя им средства для быстрой реализации интерфейсов управления к создаваемым приложениям.

Для достижения этих целей были решены следующие задачи: Обеспечение прямого доступа из командной строки к объектам COM, WMI и .NET. В новой оболочке присутствуют команды, позволяющие в интерактивном режиме работать с COM-объектами, а также с экземплярами классов, определенных в информационных схемах WMI и .NET.

Организация работы с произвольными источниками данных в командной строке по принципу файловой системы. Например, навигация по системному реестру или хранилищу цифровых сертификатов выполняется из командной строки с помощью аналога команды CD интерпретатора Cmd.exe.

Разработка интуитивно понятной унифицированной структуры встроенных команд, основанной на их функциональном назначении. В новой оболочке имена всех внутренних команд (в PowerShell они называются командлетами) соответствуют шаблону "глагол-существительное", например, Get-Process (получить информацию о процессе), Stop-Service (остановить службу), Clear-Host (очистить экран консоли) и т.д. Для одинаковых параметров внутренних команд используются стандартные имена, структура параметров во всех командах идентична, все команды обрабатываются одним синтаксическим анализатором. В результате облегчается запоминание и изучение команд. обеспечение возможности расширения встроенного набора команд.

Внутренние команды PowerShell могут дополняться командами, создаваемыми пользователем. При этом они полностью интегрируются в оболочку, информация о них может быть получена из стандартной справочной системы PowerShell.

Организация поддержки знакомых команд из других оболочек. В PowerShell на уровне псевдонимов собственных внутренних команд поддерживаются наиболее часто используемые стандартные команды из оболочки Cmd.exe и Unix-оболочек. Например, если пользователь, привыкший работать с Unix-оболочкой, выполнит ls, то он получит ожидаемый результат: список файлов в текущем каталоге (то же самое относится к команде dir).

Разработка полноценной встроенной справочной системы для внутренних команд. Для большинства внутренних команд в справочной системе дано подробное описание и примеры использования. В любом случае встроенная справка по любой внутренней команде будет содержать краткое описание всех ее параметров.

Реализация автоматического завершения при вводе с клавиатуры имен команд, их параметров, а также имен файлов и папок. Данная возможность значительно упрощает и ускоряет ввод команд с клавиатуры.

Главной особенностью среды PowerShell, отличающей ее от всех других оболочек командной строки, является то, что единицей обработки и передачи информации здесь является объект, а не строка текста.

Запуск оболочки. Выполнение команд

Для запуска оболочки следует нажать на кнопку Пуск (Start), открыть меню Все программы (All Programs), выбрать элемент Стандартные, Windows PowerShell и Windows PowerShell ISE. Другой вариант запуска оболочки – пункт выполнить… (Run) в меню Пуск (Start), ввести имя файла powershell_ise и нажать кнопку OK.

Типы команд PowerShell

В оболочке PowerShell поддерживаются команды четырех типов: командлеты, функции, сценарии и внешние исполняемые файлы.

Первый тип – так называемые командлеты (cmdlet). Этот термин используется пока только внутри PowerShell. Командлет – аналог внутренней команды интерпретатора командной строки - представляет собой класс .NET, порожденный от базового класса Cmdlet; разрабатываются командлеты с помощью пакета PowerShell Software Developers Kit (SDK). Единый базовый класс Cmdlet гарантирует совместимый синтаксис всех командлетов, а также автоматизирует анализ параметров командной строки и описание синтаксиса командлетов для встроенной справки. Командлеты рассматриваются в данной работе. С командами других типов можно ознакомиться, используя [1].

Данный тип команд компилируется в динамическую библиотеку (DLL) и подгружается к процессу PowerShell во время запуска оболочки (то есть сами по себе командлеты не могут быть запущены как приложения, но в них содержатся исполняемые объекты). Командлеты – это аналог внутренних команд традиционных оболочек.

Следующий тип команд – функции. Функция – это блок кода на языке PowerShell, имеющий название и находящийся в памяти до завершения текущего сеанса командной оболочки. Функции, как и командлеты, поддерживают именованные параметры. Анализ синтаксиса функции производится один раз при ее объявлении.

Сценарий – это блок кода на языке PowerShell, хранящийся во внешнем файле с расширением ps1. Анализ синтаксиса сценария производится при каждом его запуске.

Последний тип команд – внешние исполняемые файлы, которые выполняются обычным образом операционной системой.

Командная строка Windows использует интерпретатор команд **cmd.exe**, который позволяет загружать приложения и направляет поток данных между ними, проще говоря переводит команды пользователя, в понятный системе вид.

Консоль командной строки интегрирована во все версии ОС Windows. На первый взгляд командный интерфейс пугает пользователя избалованных графическим интерфейсом того-же Windows, но как правило командный интерфейс, намного быстрее и имеет массу дополнительных возможностей, которые не могут быть осуществлены в графическом интерфейсе.

Методы запуска:

- Пуск / Все программы / Стандартные / Командная строка.
- Пуск / Выполнить / в строку вводим cmd.exe
- Запуск из системной папки: C:\WINDOWS\system32\cmd.exe

Команды CMD.

Ниже я представлена таблица с перечнем команд командной строки, а после таблички мы более подробно разберем основные Команды *CMD.*

Команда	Описание
ASSOC	Вывод либо изменение сопоставлений по расширениям имен файлов.
AT	Выполнение команд и запуск программ по расписанию.

Команда	Описание
ATTRIB	Отображение и изменение атрибутов файлов.
BREAK	Включение/выключение режима обработки комбинации клавиш CTRL+C.
CACLS	Отображение/редактирование списков управления доступом (ACL) к файлам.
CALL	Вызов одного пакетного файла из другого.
CD	Вывод имени либо смена текущей папки.
CHCP	Вывод либо установка активной кодовой страницы.
CHDIR	Вывод имени либо смена текущей папки.
CHKDSK	Проверка диска и вывод статистики.
CHKNTFS	Отображение или изменение выполнения проверки диска во время загрузки.
CLS	Очистка экрана.
CMD	Запуск еще одного интерпретатора командных строк Windows.
COLOR	Установка цвета текста и фона, используемых по умолчанию.
COMP	Сравнение содержимого двух файлов или двух наборов файлов.
COMPACT	Отображение/изменение сжатия файлов в разделах NTFS.
CONVERT	Преобразование дисковых томов FAT в NTFS. Нельзя выполнить преобразование текущего активного диска.
COPY	Копирование одного или нескольких файлов в другое место.
DATE	Вывод либо установка текущей даты.
DEL	Удаление одного или нескольких файлов.
DIR	Вывод списка файлов и подпапок из указанной папки.
DISKCOMP	Сравнение содержимого двух гибких дисков.
DISKCOPY	Копирование содержимого одного гибкого диска на другой.
DOSKEY	Редактирование и повторный вызов командных строк; создание макросов.
ECHO	Вывод сообщений и переключение режима отображения команд на экране.
ENDLOCAL	Конец локальных изменений среды для пакетного файла.
ERASE	Удаление одного или нескольких файлов.
EXIT	Завершение работы программы CMD.EXE (интерпретатора командных строк).
FC	Сравнение двух файлов или двух наборов файлов и вывод различий между ними.
FIND	Поиск текстовой строки в одном или нескольких файлах.
FINDSTR	Поиск строк в файлах.

Команда	Описание
FOR	Запуск указанной команды для каждого из файлов в наборе.
FORMAT	Форматирование диска для работы с Windows.
FTYPE	Вывод либо изменение типов файлов, используемых при сопоставлении по расширениям имен файлов.
GOTO	Передача управления в отмеченную строку пакетного файла.
GRAFTABL	Позволяет Windows отображать расширенный набор символов в графическом режиме.
HELP	Выводит справочную информацию о командах Windows.
IF	Оператор условного выполнения команд в пакетном файле.
LABEL	Создание, изменение и удаление меток тома для дисков.
MD	Создание папки.
MKDIR	Создание папки.
MODE	Конфигурирование системных устройств.
MORE	Последовательный вывод данных по частям размером в один экран.
MOVE	Перемещение одного или нескольких файлов из одной папки в другую.
PATH	Вывод либо установка пути поиска исполняемых файлов.
PAUSE	Приостановка выполнения пакетного файла и вывод сообщения.
POPD	Восстановление предыдущего значения текущей активной папки, сохраненного с помощью команды PUSHD.
PRINT	Вывод на печать содержимого текстовых файлов.
PROMPT	Изменение приглашения в командной строке Windows.
PUSHD	Сохранение значения текущей активной папки и переход к другой папке.
RD	Удаление папки.
RECOVER	Восстановление читаемой информации с плохого или поврежденного диска.
REM	Помещение комментариев в пакетные файлы и файл CONFIG.SYS.
REN	Переименование файлов и папок.
RENAME	Переименование файлов и папок.
REPLACE	Замещение файлов.
RMDIR	Удаление папки.
SET	Вывод, установка и удаление переменных среды Windows.
SETLOCAL	Начало локальных изменений среды для пакетного файла.
SHIFT	Изменение содержимого (сдвиг) подставляемых параметров для пакетного файла.

Команда	Описание
SORT	Сортировка ввода.
START	Запуск программы или команды в отдельном окне.
SUBST	Сопоставляет заданному пути имя диска.
TIME	Вывод и установка системного времени.
TITLE	Назначение заголовка окна для текущего сеанса интерпретатора командных строк CMD.EXE.
TREE	Графическое отображение структуры папок заданного диска или заданной папки.
TYPE	Вывод на экран содержимого текстовых файлов.
VER	Вывод сведений о версии Windows.
VERIFY	Установка режима проверки правильности записи файлов на диск.
VOL	Вывод метки и серийного номера тома для диска.
XCOPY	Копирование файлов и дерева папок.

Создание и использование массивов

Для создания и инициализации массива достаточно присвоить значения его элементам. Значения, добавляемые в массив, разделяются запятыми и отделяются от имени массива символом присваивания. Например, следующая команда создаст массив $a из трех элементов:

```
PS C:\> $a=1,5,7
PS C:\>$a
1
5
7
```

Можно создать и инициализировать массив, используя оператор диапазона (..). Например, команда

```
PS C:\> $b=10..15
```

создает и инициализирует массив $b, содержащий 6 значений 10, 11, 12, 13, 14 и 15.

Для создания массива может использоваться операция ввода значений его элементов из текстового файла:

```
PS C:\> $f = Get-Content c:\data\numb.txt –Total Count 25
PS C:\>$f.length
25
```

В приведенном примере результат выполнения командлета Get-Content присваивается массиву $f. Необязательный параметр –TotalCount ограничивает количество прочитанных элементов величиной 25. Свойство объекта массив – length – имеет значение, равное количеству элементов массива, в примере оно равно 25 (предполагается, что в текстовом файле munb.txt по крайней мере 25 строк).

Обращение к элементам массива

Длина массива (количество элементов) хранится в свойстве Length. Для обращения к определенному элементу массива нужно указать его индекс в квадратных скобках после имени переменной. Нумерация элементов массива всегда начинается с нуля. В качестве индекса можно указывать и отрицательные значения, отсчет будет вестись с конца массива – индекс -1 соответствует последнему элементу массива.

Контрольные вопросы

1. Какая команда отвечает за сравнение содержимого двух гибких дисков.
2. Какая команда отвечает за копирование одного или нескольких файлов в другое место.
3. В чем отличия комады DISKCOMP от команды DISKCOPY

Оформление отчета:

1. Цель работы.
2. Постановка задачи.
3. Подробное описание технологии выполнения каждого пункта задания, подкрепленное изображением.
4. Вывод.

Министерство образования и науки Российской Федерации
федеральное государственное бюджетное образовательное учреждение высшего образования
"Российский экономический университет имени Г.В. Плеханова"
МОСКОВСКИЙ ПРИБОРОСТРОИТЕЛЬНЫЙ ТЕХНИКУМ

ПРАКТИЧЕСКАЯ РАБОТА № 2
ДИСЦИПЛИНА: ОПЕРАЦИОННЫЕ СИСТЕМЫ

Тема: 2. Создание сценариев в PowerShell, создание скриптов(*.bat) .

Специальность: 09.02.03 «Программирование в компьютерных системах»
Квалификация: техник-программист

Цель работы: Освоение механизмов управления средствами командных файлов, скриптов и сценариев в ОС. Использование командных файлов и скриптов в командных файлах для автоматической работы.

Время выполнения работы: 2 академических часа.

Задание к лабораторной работе:

а) Написать bat-файл формирующий список всех файлов, расположенных на устройстве c: в текущем каталоге выдать на экран и в файл all.txt (в каталог c:\temp или в каталог группы).

б) Среди файлов, расположенных в каталоге c:\Winnt найти самый длинный файл.

в) Написать bat-файл, выдающий содержимое файлов с расширением txt из текущего каталога на устройстве c: на экран.

г) Написать bat-файл, имена файлов в каталоге Winnt на устройстве c:, в расширении которых вторая буква - x, записать в файл withx.txt

д). Написать bat-файл, который имена файлов, содержащих в расширении символ x, записывает в файл x.txt

е). Из файлов в корневом каталоге на устройстве c: выбрать файл с самым поздним временем создания.

ж) Все буквы r в именах файлов заменить на буквы p.

з) Написать bat-файл, рисующий бесконечный треугольник:

аа
аааа
аааааа
аааааааа
ааааааааа
аааааааааа
ааааааааааааа
...

и) найти и разобрать работу скриптовых прототипов для реализации пунктов заданий а,б,…, з.

Индивидуальные задания.

а) Написать bat-файл, показывающий содержимое своего параметра. Если параметр - каталог, то должно выдаваться содержимое (список файлов) каталога, если файл - содержимое (текст) файла.

б) Значения всех переменных системного окружения OS выдать в файл envir.txt

в) Написать файл, запускающий программу help с одним параметром

Если параметр не задан, или задано больше одного параметра, должно выдаваться сообщение об ошибке.

г) Написать файл triangle.bat, рисующий текстовый треугольник с количеством строк, равным значению первого параметра и из символа, задаваемого вторым параметром. Например: triangle 10 аа рисует следующий треугольник:

аа
аааа
аааааа
аааааааа
ааааааааа
аааааааааа
ааааааааааааа

д) Написать bat-файл, выдающий на экран номер своего запуска. (Т.е. первый раз выдающий "1", второй - "2", и т.д.)

е) найти и разобрать работу скриптовых прототипов для реализации пунктов заданий а,б,…,д.

Примеры выполнения задания:

а) Написать bat-файл формирующий список всех файлов, расположенных на устройстве c: в текущем каталоге выдать на экран и в файл all.txt (в каталог c:\temp или в каталог группы)

```
@echo off
subst x: c:\temp
dir >x:\all.txt
type x:\all.txt
```

б) Среди файлов, расположенных в каталоге c:\Winnt найти самый длинный файл.

```
@echo off
dir /O:-S c:\winnt | more
```

в) Написать bat-файл, выдающий содержимое файлов с расширением txt из текущего каталога на устройстве c: на экран.

```
@echo off
for %%i in (*.txt) do type type *.txt
```

г) Написать bat-файл, имена файлов в каталоге Winnt на устройстве c:, в расширении которых вторая буква - x, записать в файл withx.txt

```
@echo off
dir *.?x* > c:\temp\withx.txt
```

д). Написать bat-файл, который имена файлов, содержащих в расширении символ x, записывает в файл x.txt

```
@echo off
dir *.*x* > x.txt
```

е). Из файлов в корневом каталоге на устройстве c: выбрать файл с самым поздним временем создания.

```
@echo off
dir /O:D c: | more
```

ж) Все буквы r в именах файлов заменить на буквы p.

```
@echo off
break on
SET A=
:start
rename %A%r*.* %A%p*.*
SET A=%A%?
goto start
```

з) Написать bat-файл, рисующий бесконечный треугольник:

```
@echo off
break on
SET A=
:loop
SET A=%A%aa
echo %A%
goto loop
```

Контрольные вопросы.

- Приведите примеры других операционных систем, языков и средств системного программирования, особенности их установки, настройки, применения и удаления?
- Как применить в данной работе системные программные средства, разработанные Вами при выполнении предыдущих лабораторных работ?
- Перечислите все средства ОС и СПО, использованные Вами в работе?
- Можно ли повысить эффективность применения средств, использованных Вами в данной работе?
- Какие альтернативные системные программные средства можно применить для выполнения данного задания?

- Опишите (в общих чертах), как выглядит решение данного задания в виде отдельных команд ОС или системных утилит, командного файла автоматизации, скрипта или пакета скриптов, библиотеки функций, оболочки или других системных средств?
- Предложите свой вопрос по теме лабораторной работы и ответьте на него.
- Что сделает строка командного файла
- for %%i in (“echo aaa>a.txt” dir “type a.txt“) do %%i

Оформление отчета:

1. Цель работы.
2. Постановка задачи.
3. Подробное описание технологии выполнения каждого пункта задания, подкрепленное изображением.
4. Вывод.

Министерство образования и науки Российской Федерации
федеральное государственное бюджетное образовательное учреждение высшего образования
"Российский экономический университет имени Г.В. Плеханова"
МОСКОВСКИЙ ПРИБОРОСТРОИТЕЛЬНЫЙ ТЕХНИКУМ

Практическая работа № 3
Дисциплина: Операционные системы

Тема: Работа с пользователями. Программный интерфейс. Файловая система ОС Windows.

Специальность: 09.02.03 «Программирование в компьютерных системах»
Квалификация: техник-программист

Цель работы: изучение основных принципов управление пользователями в ОС Windows
Время выполнения работы: 2 академических часа.
Теоретические сведения:
Управление пользователями и группами.

В операционной системе Windows XP Professional для проверки подлинности (аутентификации) пользователя используются учетные записи. Они хранятся в специальной базе данных на локальных компьютерах и на сервере (для сети с выделенным сервером). Каждый раз при аутентификации пользователя, происходит сравнение введенных им данных с данными из базы, и при совпадении пользователь получает доступ к компьютеру или в локальную сеть. Windows XP Professional использует три типа учетных записей пользователей:

Локальные учетные записи пользователей для регистрации пользователей локального компьютера. Индивидуальная база учетных записей локальных пользователей хранится на каждом компьютере, и содержит информацию о пользователях данного компьютера.

*Встроенные учетные записи пользователей создаются автоматически при установке Windows XP Professional. В состав встроенных учетных записей входят две основные записи - Администратор и Гость. Встроенные учетные записи хранятся в той же базе, что и локальные учетные записи.

*Учетные записи пользователей домена хранятся на выделенном сервере и содержат личные данные о пользователях локальной сети.

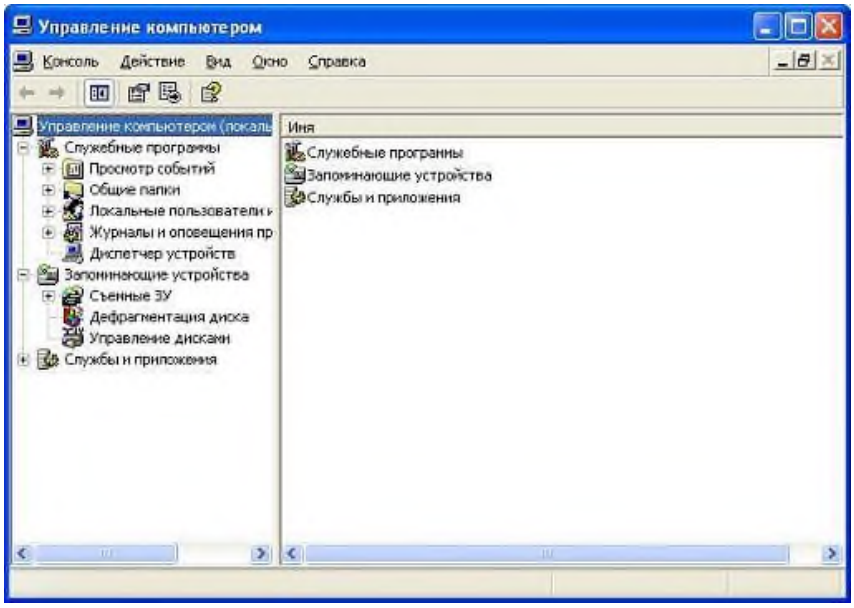
Если пользователь, работая за компьютером, имеет доступ к локальной сети, он должен иметь две учетные записи, одну для доступа к компьютеру (локальная), другую для доступа к сети (пользователь домена). Эти записи могут отличаться (например, могут быть разные пароли), но для удобства работы лучше этого не делать.

Независимо от того, подключен ваш компьютер к локальной сети или нет, он содержит локальную базу данных безопасности. Это позволяет создавать на рабочих станциях локальные учетные записи пользователей и локальные группы, а также управлять ими. Локальные пользователи — это люди, которые будут пользоваться вашим компьютером, либо работая непосредственно за ним, либо подключаясь по сети. Для каждого из них можно создать отдельную учетную запись, которая будет содержать индивидуальные сведения о пользователе и настройках операционной системы Windows XP Professional.

Кроме того, администратор данного компьютера, может установить отдельно для каждого пользователя свою политику безопасности и предоставить индивидуальные права доступа к ресурсам компьютера.

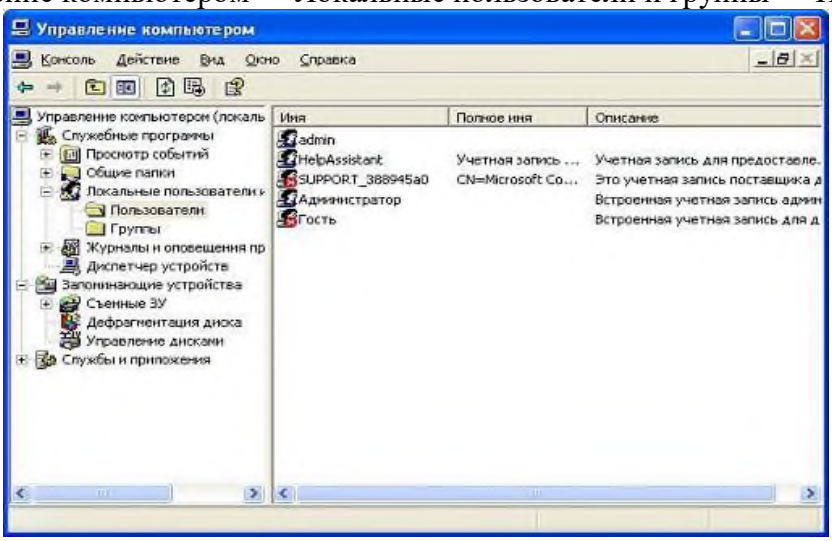
Для удобства управления локальными пользователями, их можно объединять в группы и управлять группами, не устанавливая одни и те же настройки для каждого пользователя в отдельности.

Управление учетными записями пользователей и группами осуществляется при помощи консоли Управление компьютером. Вы можете вызвать ее, в меню Пуск, выбрав Панель управления -> Администрирование или щелкнув правой кнопки мыши пункт Мой компьютер (в меню Пуск) и в контекстном меню выбрав пункт Управление.



Управление локальными и встроенными учетными записями.

Для управления учетными записями пользователей раскройте ветвь дерева Управление компьютером -> Локальные пользователи и группы -> Пользователи.



В списке справа отображаются локальные и встроенные учетные записи пользователей. Все операции по управлению учетными записями осуществляются с помощью контекстного меню, которое вызывается нажатием правой кнопки мышки, установив указатель на имя учетной записи. Также можно использовать пункт Действие строчного меню. Локальные учетные записи создаются администратором данного компьютера или пользователем, имеющим определенные права.

Встроенные учетные записи необходимы как для работы самой операционной системы, так и для того, чтобы вы могли начать работать с ней. При установке Windows XP Professional, создается ряд стандартных встроенных учетных записей, приведенных в таблице:

Учетная запись	Описание
Администратор	Учетная запись администратора системы. Необходима для выполнения многих административных задач, решаемых на данном компьютере. Запись не может быть удалена!

Гость	Гостевая учетная запись. Обладает минимальными правами и предназначена для регистрации анонимных пользователей. Отключена по умолчанию. Запись не может быть удалена!
HelpAssistant	Учетная запись для предоставления удаленной помощи
SUPPORT_388945a0	Это учетная запись поставщика для службы справки и поддержки

Создание новой учетной записи.

Что бы создать новую учетную запись пользователя, поместите указатель мышки на поле Пользователи и нажмите правую кнопку мышки. В контекстном меню выберите Новый пользователь.

В появившемся окне введите имя учетной записи (поле Пользователь), полное имя пользователя и описание учетной записи. При задании имени учетной записи рекомендуется использовать только латинские символы, цифры и некоторые знаки.

Поля Полное имя и Описание заполнять не обязательно. Достаточно удобно в качестве описания учетной записи указывать должность пользователя или кратко описывать выполняемые им функции.

В именах учетных записей желательно использовать не более 20 символов, хотя разрешается вводить больше. Windows XP Professional использует только первые 20 символов. Имена учетных записей не чувствительны к регистру, например, IvanovAP, ivanovap, IVANOVAP означают одно и тоже имя пользователя.

Не используйте в имени пользователя следующие спецсимволы: / \ < > | [ ] : ; ? * , = + В целях безопасности, переименуйте учетные записи Администратор и Гость, чтобы избежать проникновение злоумышленника через локальную сеть.

Далее вы должны задать пароль для новой учетной записи. Допустимо использование пустого пароля, хотя это не рекомендуется из соображений безопасности, особенно для учетной записи администратора.

По умолчанию локальная политика безопасности не запрещает использование пустых паролей пользователей, однако это поведение может быть изменено как в самой локальной политике безопасности, так и при помощи политики домена. В любом случае пароль должен иметь длину не менее указанной в политике безопасности.

Максимальная длина пароля 128 символов, к тому же пароль не чувствителен к регистру. Рекомендуется использовать пароль длинной не менее 8 символов, содержащий символы верхнего и нижнего регистров, цифры и спецсимволы. На ряду с символами нижнего регистра, использовать хотя бы один символ верхнего регистра, одну цифру и один спецсимвол (например, f*4Wyz9c).

При необходимости можно изменить параметры создаваемой учетной записи. Функция смены пароля при следующем входе в систему реализуется за счет установления срока устаревания пароля. При этом сразу после входа в систему пароль считается устаревшим, и система предлагает его сменить. Этот механизм не может работать при установленном флажке Срок действия пароля не ограничен.

После заполнения всех свойств новой учетной записи щелкните кнопку Создать. Учетная запись будет создана, а консоль управления компьютером предложит вам ввести данные следующего пользователя. Если вы ввели всех пользователей, щелкните кнопку Закрыть.

Изменение параметров учетной записи. Чтобы изменить параметры существующей учетной записи, поместите указатель на нужную учетную запись и щелкните правой кнопки мыши. В контекстном меню выберите пункт Свойства. На вкладке Общие вы можете изменять те же параметры, что и при создании новой учетной записи. Обратите внимание,

что нельзя изменить имя учетной записи — это осуществляется при помощи операции переименования.

Кроме того, появился еще один флажок - Заблокировать учетную запись. Этот флажок не может быть установлен вручную. Он включается системой безопасности Windows XP при многократных попытках ввода неправильного пароля. Поведение системы безопасности в случае подбора пароля устанавливается локальной или доменной политикой безопасности.

Администратор системы может только снять блокировку с учетной записи, уже заблокированной операционной системой.

Вы не можете отключить встроенную учетную запись администратора. Вы можете ограничить срок действия пароля учетной записи администратора, но даже при настроенной политике безопасности этот параметр не будет действовать На вкладке Членство в группах вы можете управлять членством пользователей в локальных группах. На вкладке выводится список групп, членом которых является пользователь.

Включение пользователя в ту или иную группу может потребоваться для предоставления ему доступа к определенному ресурсу или расширения его полномочий. По умолчанию все вновь создаваемые пользователи включаются в группу Пользователи.

Для включения пользователя в одну или более групп щелкните кнопку Добавить. В появившемся окне можно выбрать группы из списка или вписать их названия вручную в поле в нижней части окна. Имена нескольких групп разделяются точками с запятой.

Вы можете добавлять локальные учетные записи пользователей только в локальные группы. Добавление локальных учетных записей пользователей в любые группы домена невозможно.

На вкладке Профиль вы можете управлять параметрами профиля пользователя. Профиль хранится на локальном компьютере в папке %homedrive%\Documents and Settings. В папке профиля пользователя сохраняются его личные файлы, персонифицированные файлы приложений, временные файлы пользователя, его рабочий стол и сетевое окружение, данные системного реестра.

локальный - создается на основе стандартного профиля пользователя при первом входе в систему и хранится в указанной выше папке. Применяется в основном для настольных компьютеров;

перемещаемый - создается путем преобразования локального профиля и хранится в папке на сервере. Копируется в локальную папку при входе пользователя в систему и возвращается обратно при выходе из системы. Применяется для перемещаемых пользователей (например, пользователей переносных компьютеров, пользователей, не имеющих постоянного рабочего места, или при переустановке операционной системы на рабочей станции);

обязательный - создается путем преобразования перемещаемого профиля и хранится в папке на сервере, как и перемещаемый; копируется в локальную папку при входе пользователя в систему, но не копируется обратно при выходе.

Указав в поле Путь к профилю сетевой путь к перемещаемому или обязательному профилю, вы укажете Windows копировать профиль из указанной сетевой папки, а не создавать его на основании стандартного профиля пользователя.

В поле Сценарий входа можно указать имя файла сценария, который будет выполнен при входе пользователя в систему. Даже в одноранговой сети вы можете хранить данные всех пользователей на одном компьютере, упрощая резервное копирование данных и доступ к ним с разных компьютеров. Если личные данные пользователя хранятся на другом компьютере в сети, вы можете автоматически подключить соответствующую папку другого компьютера при входе пользователя в систему. Для этого нужно задать букву диска и сетевой путь к подключаемому ресурсу. Если пользователь работает на локальном компьютере, но хранит свои данные не в одной из папок профиля, а, скажем, на другом

диске, вы можете указать путь к соответствующей папке в поле Локальный путь. Если ни один из этих параметров не указан, то домашней папкой считается папка его локального профиля (%homedrive%\Documents and Settings\%username% или %userprofile%).

Переименование учетной записи.

Учетная запись любого пользователя, включая администратора, может быть переименована. Это возможно, т. к. Windows идентифицирует учетные записи не по имени, а по специальному уникальному коду, жестко привязанному к каждой учетной записи. Этот код называется идентификатор безопасности (Secure ID, SID) и используется не только для учетных записей, но и для имен компьютеров.

Переименовать учетную запись вы можете, выбрав соответствующий пункт контекстного меню или нажав клавишу F2. Для переименования укажите новое имя учетной записи пользователя и нажмите Enter.Дополнительного подтверждения при переименовании не требуется.

Изменение пароля учетной записи.

Ни один пользователь системы, даже ее администратор, не может получить пароль пользователя в открытом виде. При необходимости работать с данными пользователя от его имени, администратор может установить пользователю новый пароль и использовать его для входа в систему. Такая необходимость может возникнуть и при смене паролей пользователей, которые не могут сделать этого самостоятельно или просто забыли пароль.

Любой пользователь для смены своего собственного пароля обязан ввести сначала старый, а потом новый пароль. При использовании консоли для управления пользователями администратор может устанавливать новые пароли пользователей, не зная старых.

Для смены пароля выберите пункт Задать пароль контекстного меню. Дважды введите новый пароль и щелкните ОК. Новый пароль начинает действовать немедленно.

После смены пароля пользователя рекомендуется выйти и снова войти в систему. Иначе такая ситуация может привести к невозможности доступа к некоторым ресурсам сети после смены пароля.

При смене пароля пользователя в рабочей группе вы должны изменить пароль на всех компьютерах рабочей группы, которые содержат учетную запись этого пользователя. Это связано с тем, что каждый компьютер рабочей группы имеет свою собственную базу данных безопасности, не синхронизированную с базами данных других компьютеров.

Удаление учетной записи.

Чтобы удалить учетную запись, выберите соответствующий пункт контекстного меню или нажмите клавишу Delete (Del). После подтверждения учетная запись будет удалена.

Очень осторожно относитесь к удалению учетных записей пользователей. При удалении учетной записи также теряется ее идентификатор безопасности (SID), поэтому создание новой учетной записи после удаления пользователя с таким же именем учетной записи не вернет ему членство в группах и доступ к ресурсам, которые имела удаленная учетная запись. Поэтому рекомендуется сначала отключать учетные записи пользователей, а удалять их только при необходимости.

Системные учетные записи (Администратор и Гость) не могут быть удалены. Однако учетная запись гостя может быть отключена из соображений безопасности.

Управление локальными группами.

Для управления локальными группами раскройте ветвь дерева Управление компьютером -> Локальные пользователи и группы -> Группы.

В списке справа отображаются локальные и встроенные группы. Все операции по управлению группами осуществляются с помощью контекстного меню, которое вызывается нажатием правой кнопки мышки, установив указатель на имя группы. Также можно использовать пункт Действие строчного меню.

Локальные группы создаются администратором данного компьютера или пользователем, имеющим определенные права.

Встроенные группы необходимы для разграничения доступа к файлам, папкам, системным объектам и т. п. Для предоставления пользователям определенных прав в рамках системы рекомендуется включать их в соответствующие системные группы. Например, чтобы предоставить пользователю полномочия администратора системы, его достаточно включить в группу Администраторы. Добавление группы.

Что бы создать новую группу, поместите указатель мышки на поле Группы и нажмите правую кнопку мышки. В контекстном меню выберите создать группу.

В появившемся окне введите имя группы и ее описание. Поле описания не является обязательным, но желательно указать в нем сведения о том, для каких целей создается группа.

Щелкнув кнопку Добавить, можно сразу добавить пользователей в создаваемую группу.

Помимо пользователей, в локальные группы могут быть добавлены любые (локальные, глобальные и универсальные) группы домена.

Кроме пользователей в списке вы увидите ряд псевдогрупп, которые нельзя увидеть в оснастке

Управление пользователями и группами, но можно использовать для назначения прав доступа и включения в другие группы.

После заполнения параметров новой группы щелкните кнопку Создать. Группа будет создана, а консоль управления компьютером предложит вам ввести данные следующей группы. Если вы не будете создавать новую группу, щелкните кнопку Закрыть.

Изменение свойств группы.

Чтобы изменить параметры группы, установите указатель на имя нужной группы и щелкните правой кнопкой мыши. В контекстном меню выберите Свойства

На вкладке Общие вы можете изменять те же параметры, что и при создании новой группы. Обратите внимание, что нельзя изменить имя группы, — это осуществляется только при помощи переименования.

Переименование группы.

Любая группа, включая встроенные, может быть переименована. Это возможно, т. к. Windows в качестве уникального идентификатора группы использует SID, а не ее имя. Переименовать группу вы можете, выбрав соответствующий пункт контекстного меню или нажав клавишу F2. Для переименования укажите новое имя группы и нажмите Enter. Дополнительное подтверждение при переименовании не требуется.

Удаление группы.

Чтобы удалить группу, выберите соответствующий пункт контекстного меню или нажмите клавишу Delete (Del). После подтверждения группа будет удалена.

Очень осторожно относитесь к удалению групп. При удалении группы также теряется ее идентификатор безопасности, поэтому создание новой группы с таким же именем (после удаления группы) не вернет ей права доступа к ресурсам, которые имела удаленная группа.

Встроенные группы не могут быть удалены.

Использование утилит командной строки.

Основные операции по управлению учетными записями пользователей и группами могут быть выполнены при помощи утилит командной строки. Этот способ незаменим при необходимости быстро создать большое количество учетных записей и групп.

При помощи утилиты net могут быть выполнены следующие операции:

- создание, изменение и удаление учетной записи пользователя (net user);
- изменение пароля пользователя (net user);
- создание, изменение и удаление локальной группы (net group);
- изменение состава локальной группы (net group).

Утилита net user имеет следующий синтаксис:

net user [username [пароль | *] [/ADD | /DELETE] [/ACTIVE:][/COMMENT:"комментарий"][/COUNTRYCODE:код][/EXPIRES:][/FULLNAME:"полное_имя"][/HOMEDIR:путь][/PASSWORDCHG:][/PASSWORDREQ:][/PROFILEPATH[:путь]][/SCRIPTPATH:путь][/TIMES:][/USERCOMMENT:"комментарий"] [/WORKSTATIONS:]][/DOMAIN]

Если не указан ключ /ADD или /DELETE , утилита выводит или изменяет информацию об учетной записи пользователя. Информация выводится, если указано только имя учетной записи. Если указан один или более параметров, то производится изменение указанной учетной записи. Параметры /ACTIVE /COUNTRYCODE/EXPIRES/PASSWORDCHG/PASSWORDREQ/TIMES/WORKSTATIONS могут указываться только для учетных записей пользователей домена. Утилита net group имеет следующий синтаксис: netgroup[groupname[/ADD|/DELETE]/COMMENT:"комментарий"]] [/DOMAIN] net group groupname user [...][/DOMAIN] Описание ключей утилиты net group приведено в таблице.

Ключ	Описание
groupname	Имя группы для добавления, удаления или изменения
/ADD	Создает указанную группу или добавляет учетные записи пользователей в существующую группу
/DELETE	Удаляет указанную группу или удаляет учетные записи пользователей из существующей группы
/COMMENT:"комментарий"	Устанавливает комментарий группы. Текст комментария должен быть заключен в кавычки. Максимальная длина - 48 символов
user [...]	Указывает одно или более имен учетных записей пользователей для добавления или удаления из группы. Несколько имен разделяются пробелами
/DOMAIN	Осуществляет указанную операцию на контроллере домена, а не на локальном компьютере

Если не указан ключ /ADD или /DELETE, утилита выводит или изменяет информацию об указанной группе. Информация выводится, если указано только имя группы. Если указан один или более параметров, то производится изменение указанной группы.

Пример создания учетной записи пользователя с именем User1 и паролем 123456: net user User1 123456 /ADD /COMMENT:"Тестовый пользователь" Пример изменения срока действия учетной записи пользователя User1: net user User1 /EXPIRES:31/12/2002 Пример просмотра информации об учетной записи пользователя User1: net user User1 Пример создания группы с именем TestGroup: net group TestGroup /COMMENT:"Тестовая группа" /ADD Пример добавления пользователей Администратор и User1 в группу TestGroup: net group TestGroup Администратор User1 /ADD Пример просмотра информации о группе TestGroup: net group TestGroup

Контроль сетевых пользователей.

Используя консоль Управление компьютером, вы можете контролировать пользователей, подключенных к вашему компьютеру в данный момент, а также какими ресурсами они пользуются. Для этого откройте раздел Общие папки и выберите пункт Сеансы.

Правая часть окна содержит список пользователей, подключенных к вашему компьютеру.

Вы можете узнать имя пользователя, имя компьютера, с которого он подключился, тип операционной системы его компьютера, количество открытых файлов и прочую информацию.

Вы можете отключить пользователя, используя контекстное меню (щелкните правой кнопкой мышки) или выбрав пункт Действие строчного меню.

Если вы хотите отключить сразу всех подключенных пользователей, установите указатель мышки на пунктСеансы и используя контекстное или строчное меню (пункт Действие), выберите отключить все сеансы.

Операционная система Windows автоматически восстанавливает прерванное подключение к общей папке, поэтому после отключения пользователя он автоматически подключится снова.

Что бы окончательно отключить пользователя от вашего компьютера, вам придется отменить доступ пользователя к данному ресурсу или отменить общий доступ к ресурсу, но тогда он будет недоступен всем пользователям.

Чтобы посмотреть какие именно файлы открыл подключившийся пользователь, откройте раздел Общие папки и выберите пункт Открытые файлы. Так же, как и сеанс пользователя, открытые файлы можно отключить.

Вы можете отправить сообщение пользователям, например, предупреждение о завершении работы вашего компьютера. Для этого установите указатель мышки на раздел Общие папки и используя контекстное или строчное меню (пункт Действие), выберите Отправка сообщения консоли. Затем напишите текст сообщения и из списка выберите пользователей, которым это сообщение отправить.

Контрольные вопросы

1. Как создать нового пользователя?
2. Как создать новую группу пользователей?
3. Как производить контроль сетевых пользователей
4. Управление локальными пользователями

Оформление отчета:

1. Цель работы.
2. Постановка задачи.
3. Подробное описание технологии выполнения каждого пункта задания, подкрепленное изображением.
4. Вывод.

Министерство образования и науки Российской Федерации
федеральное государственное бюджетное образовательное учреждение высшего образования
"Российский экономический университет имени Г.В. Плеханова"
МОСКОВСКИЙ ПРИБОРОСТРОИТЕЛЬНЫЙ ТЕХНИКУМ

ПРАКТИЧЕСКАЯ РАБОТА № 4
ДИСЦИПЛИНА: ОПЕРАЦИОННЫЕ СИСТЕМЫ

Тема: PowerShell как средство автоматизации, работа с оснастками, командлеты.

Специальность: 09.02.03 «Программирование в компьютерных системах»
Квалификация: техник-программист

Цель работы: познакомиться с консолью управления MMC, получить навыки работы в консоли.

Время выполнения работы: 2 академических часа.

Теоретический материал.

Консоль управления Microsoft Management Console (MMC группирует средства администрирования, которые используются для администрирования сетей, компьютеров, служб и других системных компонентов.

Консоль MMC непосредственно не выполняет административные функции, однако предоставляет возможности интеграции в нее компонентов или системных приложений, выполняющие эти функции. Основной тип интегрируемых на консоль компонентов называется оснасткой, которые не могут выполняться отдельно без консоли. Среди других добавляемых элементов могут быть элементы управления ActiveX, ссылки на Web-страницы, папки, видов панели задач и собственно задачи для выполнения. Дополнительные теоретические сведения об оснастках и других используемых для интеграции на консоль элементах будут добавлены в дальнейшем, в соответствующих разделах настоящей лабораторной работы.

Базовое окно консоли MMC представляет собой графическую форму с контекстными меню, реализующие дружественный пользовательский интерфейс. Имеется панель инструментов с командами создания, открытия и сохранения консолей и, кроме того, область описания и строка состояния в нижней части окна. Чтобы увидеть базовое окно, а также непосредственно саму консоль MMC, необходимо выполнить следующие действия:

нажмите Пуск | Выполнить,

наберите в появившемся окне MMC.exe (или просто mmc),

нажмите Enter для ввода.

Новая консоль MMC представляет собой отдельное окно, разделенное на две вертикальные области, в левой из которых отображается дерево консоли с его корнем. Дерево консоли показывает доступные элементы и компоненты консоли. Правая область является областью сведений, которая содержит описания элементов и выполняемых ими функций. Содержание области сведений соответствует выбранному элементу в дереве консоли и может включать Web-страницы, графики, диаграммы, таблицы и столбцы.

Создавая надежные средства управления компьютерами сети, можно собрать и настроить собственную консоль MMC, выполняющую заданные функции администрирования. После того как добавлены все необходимые элементы и компоненты консоли, панель главного меню, панель инструментов, а также область описания и строка состояния могут быть скрыты для предотвращения в дальнейшем нежелательных изменений. Созданные таким образом управляющие системы сохраняются в файлах с расширением .msc (Management Saved Console, сохраненная консоль управления) и могут быть, в частности, распространены в пределах всей системы посредством задания к ним доступа с помощью ярлыков или элементов меню Пуск.

Чтобы увидеть консоль управления локальным компьютером в качестве примера готовой и отлаженной консоли MMC, необходимо выполнить:

нажмите Пуск | Выполнить,

наберите в появившемся окне compmgmt.msc (или compmgmt),

нажмите Enter для ввода.

Существует два основных режима доступа консоли администрирования, задающиеся непосредственно при ее создании:

пользовательский, в котором можно администрировать систему, работая с уже существующими консолями,

авторский, в котором можно создавать новые консоли или изменять существующие.

В свою очередь, имеется три уровня режима пользователя, что обусловливает всего четыре варианта предустановленного режима доступа:

авторский режим;

режим пользователя — полный доступ;

режим пользователя — ограниченный доступ, многооконный;

режим пользователя — ограниченный доступ, однооконный.

Консоль ММС, инициализированная в авторском режиме, предоставляет полный доступ ко всем ее возможностям, включая добавление и удаление оснасток, создание новых окон и панелей задач, а также просмотр любых частей дерева консоли и другие. Однако при выборе одного из трех режимов пользователя авторские возможности исключаются. В частности, если для консоли установлен параметр «пользовательский режим — полный доступ», то предоставляются все команды управления окном консоли и полный доступ к ее дереву, но запрещается добавление, удаление оснасток и изменение свойств консоли администрирования.

Изменения консоли ММС в авторском и пользовательском режимах сохраняются по-разному. При закрытии консоли в авторском режиме выводится диалоговое окно с предложением сохранить изменения. Однако в пользовательском режиме и снятом флажке «Не сохранять изменения для этой консоли» изменения будут сохранены автоматически при закрытии.

Если консоль открыта при соблюдении одного из следующих условий:

в базовом окне при загрузке,

с помощью команды контекстного меню Автор,

в командной строке с параметром /a,

то предустановленный режим игнорируется, а открытие консоли осуществляется в авторском режиме.

Очевидно, что загрузка консоли ММС в авторском режиме не требуется рядовым пользователям. Системный администратор может настроить профили пользователей так, чтобы запретить им переход в авторский режим, как из командной строки, так и через контекстное меню. Кроме того, запрет перехода в авторский режим может быть организован при использовании возможностей групповой политики, при которой, в частности, осуществляется ограничение доступа к определенным оснасткам. Рассмотрению базовых возможностей оснастки групповой политики будет посвящена вторая часть настоящей лабораторной работы.

Прежде чем создавать новую консоль ММС, необходимо определить действия, для которых предназначена эта консоль, список администрируемых компонентов, оснасток и других элементов, которые потребуются для выполнения поставленных задач. Следует также рассмотреть необходимость создания видов панели задач. После принятия этих решений можно открыть новую консоль и начать добавлять элементы к дереву консоли. Полное руководство по созданию и настройке консолей ММС находится на Web-узле корпорации Майкрософт (http://www.microsoft.com).

В лабораторной работе предполагается ознакомление с основными принципами организации и построения консоли администрирования ММС, а также с базовыми возможностями основных инструментов системного администратора — оснасток «Локальные пользователи и группы» и «Редактор объекта групповой политики» («Групповая политика»).

Перед началом выполнения заданий в среде ОС Windows XP необходимо выполнить следующее:

запустить виртуальную машину с ОС Windows XP и активировать справочное меню (Пуск | Справка и поддержка);

ознакомиться с описанием и возможностями запуска и применения консоли администрирования ММС;

ознакомиться возможностью получения сведений пункта 2 из альтернативного источника информации, доступного непосредственно в справке консоли администрирования ММС (Справка | Вызов справки);

ознакомиться с описанием и возможностями оснасток «Локальные пользователи и группы» и «Редактор объекта групповой политики» («Групповая политика»).

Содержание задания

Для добавления видов панелей задач и собственно задач в авторском режиме выполните следующее:

1. Создайте новую Консоль управления ММС одним их описанных в пункте I текущего учебного задания способов.
2. Добавьте оснастку Службы в корень консоли ММС.
3. В дереве консоли кликните манипулятором мышь на этой оснастке.
4. В меню Действие или кликнув правой кнопкой манипулятора на оснастке, выберите команду Новый вид панели задач.
5. Следуйте инструкциям «Мастера создания вида панели задач», чтобы добавить на консоль новую панель вида.
6. Если сразу после создания вида панели задач необходимо создать задачи, установите флажок «Запустить мастер создания новой задачи» на последнем экране «Мастера создания вида панели задач».
7. Следуйте инструкциям «Мастера создания новой задачи», чтобы добавить
8. на консоль новую задачу к существующей панели вида.
9. В дереве консоли кликните элемент или компонент (в нашем случае это оснастка), связанный с видом панели задач, затем в меню Действие выберите команду Правка вида панели задач.
10. На вкладке Задачи нажмите кнопку Создать.
11. Повторите инструкции пункта 7 настоящего задания.
12. Не закрывая консоль администрирования ММС, сохраните ее.
13. Измените вид панели задач сохраненной консоли администрирования ММС, выполнив следующие действия:
14. введите новое имя,
15. введите новое описание,
16. установите переключатель Стиль для области сведений в положение, соответствующее новому формату списка,
17. удалите соответствующий флажок, чтобы скрыть стандартную вкладку,
18. установите переключатель Стиль для описания задачи в положение, соответствующее новому стилю задачи,
19. выберите новое значение ширины для вертикального списка или высоты для горизонтального списка,
20. нажмите кнопку Параметры и установите переключатель в одно из необходимых положений,
21. нажмите ОК для подтверждения ввода,
22. изучите полученный результат,
23. сделайте вывод о проделанной работе и запишите его в отчет.

Контрольные вопросы

1. Что такое Microsoft Management Console
2. Пользователи и группы пользователей
3. Что такое остнастки

Оформление отчета:

1. Цель работы.
2. Постановка задачи.
3. Подробное описание технологии выполнения каждого пункта задания, подкрепленное изображением.
4. Вывод.

Министерство образования и науки Российской Федерации
федеральное государственное бюджетное образовательное учреждение высшего образования
"Российский экономический университет имени Г.В. Плеханова"
МОСКОВСКИЙ ПРИБОРОСТРОИТЕЛЬНЫЙ ТЕХНИКУМ

ПРАКТИЧЕСКАЯ РАБОТА № 5
ДИСЦИПЛИНА: ОПЕРАЦИОННЫЕ СИСТЕМЫ

Тема: Установка и предварительная настройка ОС, Windows, Unix.

Специальность: 09.02.03 «Программирование в компьютерных системах»
Квалификация: техник-программист

Цель работы: Целью работы является изучение процесса установки операционных систем Windows 7 и Linux openSUSE 12.2.

Время выполнения работы: 2 академических часа.

Теоретические сведения:

Установка операционной системы Windows 7

Для установки ОС Windows 7 необходимо иметь диск с установочными файлами (загрузочный диск). После того, как диск вставлен в привод ПК, необходимо указать, чтобы загрузка выполнялась с привода, а не с жесткого диска.

Далее начнется загрузка файлов необходимых для запуска установки ОС Windows 7.

Как только файлы загружены, появится окно «Установка Windows».

Далее следуя, инструкция на экране, необходимо выбрать используемый язык для устанавливаемой ОС, а также ознакомится с условиями лицензионного соглашения и принять их. Затем выбирается тип установки: «Обновление» или «Полная установка». Обновление используется только в случае, если установщик был запущен из предыдущей версии ОС Windows.

После того как все пункты выполнены, необходимо настроить жесткий диск. При этом настройка осуществляется в графическом интерфейсе после нажатия кнопки «Настройка диска».

Для того чтобы создать новый раздел на жестком диске необходимо нажать кнопку «Создать» и указать размер данного раздела и затем нажать кнопку «Применить».

Если требуется создать несколько разделов, то опять нажимаем кнопку «Создать» и указываем размер раздела. Общий размер всех разделов не должен превышать общий размер жесткого диска.

После создания раздела, куда будет установлена ОС Windows 7, также создаться специальный системный раздел, который необходим для корректной работы ОС.

Также если разделы уже существуют, то их можно удалить либо стереть с них информацию (форматировать), использовав соответствующие кнопки «Удалить» и «Форматировать».

Далее после того, как разделы созданы, нажимаем кнопку «Далее» и начинается процесс копирования файлов Windows и установки Windows 7.

После завершения процесса копирования файлов и установки, ПК перезагрузится автоматически и далее необходимо, чтобы загрузка осуществлялась с жесткого диска. После загрузки появится окно «Настройка Windows».

Далее необходимо настроить основные параметры системы, такие как имя пользователя, пароль пользователя, часовой пояс, активация Windows. И после настройки произойдет запуск ОС Windows 7.

Для работы ОС Windows 7 необходимо минимум 512Мб оперативной памяти и 20 Гб на жестком диске для установки.

Операционная система Linux openSUSE

openSUSE – дистрибутив Linux, который разрабатывается компанией Novell. Данный дистрибутив является стабильным, легким в использовании и подходит в первую очередь для начинающих пользователей.

Установка openSUSE

Для установки ОС openSUSE необходимо иметь диск с установочными файлами (загрузочный диск). После того, как диск вставлен в привод ПК, необходимо указать, чтобы загрузка выполнялась с привода, а не с жесткого диска.

После того как загрузка с диска осуществилась, на экране появится openSUSE installe, где для установки данного дистрибутива на жесткий диск необходимо нажать кнопку «Installation» и начнется процесс подготовки к установке.

Далее загружается установщик openSUSE, где необходимо настроить параметры устанавливаемой системы: часовой пояс, язык системы и т.п.

Для начала необходимо установить язык установщика и операционной системы на русский. После нажать кнопку «Далее».

Далее устанавливается часовой пояс. После происходит настройка жесткого диска.

Так как используемая файловая система имеет определенную структуру, то рекомендуется использовать предлагаемые настройки жесткого диска. Нажимаем кнопку «Далее».

После выбора разметки, происходит настройка пользователя, т.е. задается имя пользователя и его пароль. В операционных системах Linux существует суперпользователь (системный администратора) – root, поэтому рекомендуется создавать нового пользователя с паролем, который соответствует паролю суперпользователя. Нажимаем кнопку «Далее».

На экране появляются все настроенные параметры устанавливаемой операционной системы openSUSE. Данные параметры проверяются и если всё верно, то нажимается кнопка «Далее». Затем появляется сообщение для пользователя о верности параметров, и чтобы запустить процесс установки необходимо нажать кнопку «Установить».

После завершения установки, операционная система перезагрузится и затем произойдет автоматический вход в систему, так как на этапе установке пароль пользователя был уже введен.

Для openSUSE 12.2 требуется минимум 256Мб оперативной памяти и 8 Гб на жестком диске для установки.

Задание на лабораторную работу

Произвести установку операционных систем Windows 7 и Linux openSUSE 12.2 и ознакомится с основными возможностями их установщиков.

Методика выполнения задания

1. Произвести установку ОС Windows 7
2. Запустить ОС Windows 7
3. Завершить работу ОС Windows 7
4. Произвести установке ОС openSUSE 12.2.
5. Запустить ОС openSUSE 12.2
6. Завершить работу ОС openSUSE 12.2

Контрольные вопросы

1. Определение поянтия фаловой системы
2. Опишите этапы установки операционной системы

Оформление отчета:

1. Цель работы.
2. Постановка задачи.
3. Подробное описание технологии выполнения каждого пункта задания, подкрепленное изображением.
4. Вывод.

Министерство образования и науки Российской Федерации
федеральное государственное бюджетное образовательное учреждение высшего образования
"Российский экономический университет имени Г.В. Плеханова"
МОСКОВСКИЙ ПРИБОРОСТРОИТЕЛЬНЫЙ ТЕХНИКУМ

ПРАКТИЧЕСКАЯ РАБОТА № 6
ДИСЦИПЛИНА: ОПЕРАЦИОННЫЕ СИСТЕМЫ

Тема: Реестр ОС. Работа с реестром в Windows. RegEdit, PowerShell.

Специальность: 09.02.03 «Программирование в компьютерных системах»
Квалификация: техник-программист

Цель работы: «Получить практические навыки при работе с системным реестром ОС Windows»

Время выполнения работы: 2 академических часа.

Теоретические сведения:

Реестр Windows или системный реестр — иерархически построенная база данных параметров и настроек в большинстве операционных систем Microsoft Windows.

Основные свойства:

Реестр содержит информацию и настройки
для аппаратного обеспечения,
программного обеспечения,
профилей пользователей,
предустановки.

Большинство изменений в Панели управления, ассоциации файлов, системные политики, список установленного ПО фиксируются в реестре.

Все возможности ОС могут быть конфигурированы посредством Реестра.

Любое запускаемое в системе приложение может быть выполнено только через обращение к Реестру, поскольку именно там находятся все его параметры.

База данных Реестра хранится в системных файлах ОС, в частности, system.dat и ntuser.dat.

Историческая справка:

Реестр Windows был введён для упорядочения информации, хранившейся до этого во множестве INI-файлов.

Реестр, как древовидная иерархическая база данных впервые появился в Windows 3.1 (апрель 1992). Это был всего один двоичный файл, который назывался REG.DAT и хранился в каталоге C:\Windows\. Реестр Windows 3.1 имел только одну ветку HKEY_CLASSES_ROOT. Он служил для связи DDE объектов (Dynamic Data Exchange — механизм взаимодействия приложений в операционных системах Microsoft Windows и OS/2), а позднее и OLE объектов (Object Linking and Embedding — технология связывания и внедрения объектов в другие документы и объекты).

Одновременно с появлением реестра в Windows 3.1 появилась программа REGEDIT.EXE для просмотра и редактирования реестра.

Первый реестр уже имел возможность импорта данных из *.REG файлов.

В базовой поставке шёл файл SETUP.REG, содержащий данные по основным расширениям и типам файлов.

Реестр Windows 3.1 имел ограничение на максимальный размер файла REG.DAT — 64 Кбайт. Если вдруг реестр превышал этот размер — то файл реестра (REG.DAT) приходилось удалять и собирать заново либо из *.REG файлов, либо вводить данные вручную.

Следующий шаг сделан в Windows NT 3.1 (июль 1993). Произошёл отказ от устаревших файлов MS-DOS: AUTOEXEC.BAT и CONFIG.SYS, а также от INI-файлов, как от основных файлов конфигурации. На «регистрационную базу» (реестр) была переведена вся конфигурация системы. Основой конфигурации системы стал реестр. Он имел 4 корневых раздела:

HKEY_ LOCAL_MACHINE,
HKEY_CURRENT_USER,
HKEY_CLASSES_ROOT,
HKEY_USERS.

Реестр стал «сборным»: на диске он хранился в файлах: DEFAULT, SOFTWARE, SYSTEM, а при запуске системы из этих файлов собиралась единая БД. В комплекте поставки оставался файл REGEDIT.EXE, который по-прежнему позволял просматривать и редактировать только ветку HKEY_CLASSES_ROOT, и появился файл REGEDT32.EXE, который позволял редактировать все ветки реестра.

Далее технология и идеология (назначение) реестра уже не менялись. Все последующие версии Windows (NT 3.5, 95, NT 4.0, 98, 2000, XP, Vista, 7) использовали реестр как основную БД, содержащую все основные данные по конфигурации как самой ОС, так и прикладных программ. Далее менялись названия файлов реестра и их расположение, а также название и назначение ключей.

Место хранения рестра Windows в XP и 7

После установки Windows XP на диске в каталоге C:\Windows\System32\Config\ хранятся файлы system, software, sam, security, default. Все имена файлов без расширений. Копия этих файлов хранится в каталоге C:\Windows\Repair\

Файлы, используемые при построении «рабочей версии» реестра, могут храниться в каталогах:

%SystemDrive%\Documents and Settings\<Username>\ — файл «Ntuser.dat»

%SystemDrive%\Documents and Settings\<Username>\Local Settings\Application Data\Microsoft\Windows\ — файл «UsrClass.dat»

Кроме этого, могут появляться и другие файлы реестра, например, userdiff , userdiff.LOG, TempKey.LOG.

Можно провести некое примерное соответствие файлов и веток реестра, но оно не такое простое, полное и однозначное. Однако примерно можно сказать следующее:

Ветка реестра «HKEY_LOCAL_MACHINE\Software» формируется из файла «%SystemRoot%\system32\config\software».

Ветка реестра «HKEY_LOCAL_MACHINE\System\» формируется из файла «%SystemRoot%\system32\config\system».

Ветка реестра «HKEY_LOCAL_MACHINE\SAM\» формируется из файла «%SystemRoot%\system32\config\SAM».

Ветка реестра «HKEY_LOCAL_MACHINE\SECURITY\» формируется из файла «%SystemRoot%\system32\config\SECURITY».

Ветка реестра «HKEY_LOCAL_MACHINE\HARDWARE\» формируется в зависимости от оборудования(динамически).

Ветка реестра «HKEY_USERS\<SID_пользователя>» формируется из файлов «%USERPROFILE%\ntuser.dat»

Ветка реестра «HKEY_USERS\DEFAULT» формируется из файлов «%SystemRoot%\system32\config\default»

В Windows 7, согласно сведениям из HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\hivelist файлы реестра хранятся в следующих местах:

01= Ветка реестра «HKEY_LOCAL_MACHINE\HARDWARE» формируется в зависимости от оборудования (динамически);

02= Ветка реестра «HKEY_LOCAL_MACHINE\BCD00000000» формируется из файла «%SystemRoot%\Boot\BCD»

03= Ветка реестра «HKEY_LOCAL_MACHINE\SYSTEM» формируется из файла «%SystemRoot%\System32\config\SYSTEM»

04= Ветка реестра «HKEY_LOCAL_MACHINE\SOFTWARE» формируется из файла «%SystemRoot%\System32\config\SOFTWARE»

05= Ветка реестра «HKEY_LOCAL_MACHINE\SECURITY» формируется из файла «%SystemRoot%\System32\config\SECURITY»

06= Ветка реестра «HKEY_LOCAL_MACHINE\SAM» формируется из файла «%SystemRoot%\System32\config\SAM»

07= Ветка реестра «HKEY_USERS\.DEFAULT» формируется из файла «%SystemRoot%\System32\config\DEFAULT»

08= Ветка реестра «HKEY_USERS\S-1-5-18» формируется из файла «%SystemRoot%\System32\config\systemprofile\NTUSER.DAT» (относится к учетной записи system)[1]

09= Ветка реестра «HKEY_USERS\S-1-5-19» формируется из файла «%SystemRoot%\ServiceProfiles\LocalService\NTUSER.DAT» (относится к учетной записи LocalService)

10= Ветка реестра «HKEY_USERS\S-1-5-20» формируется из файла «%SystemRoot%\ServiceProfiles\NetworkService\NTUSER.DAT» (относится к учетной записи NetworkService)

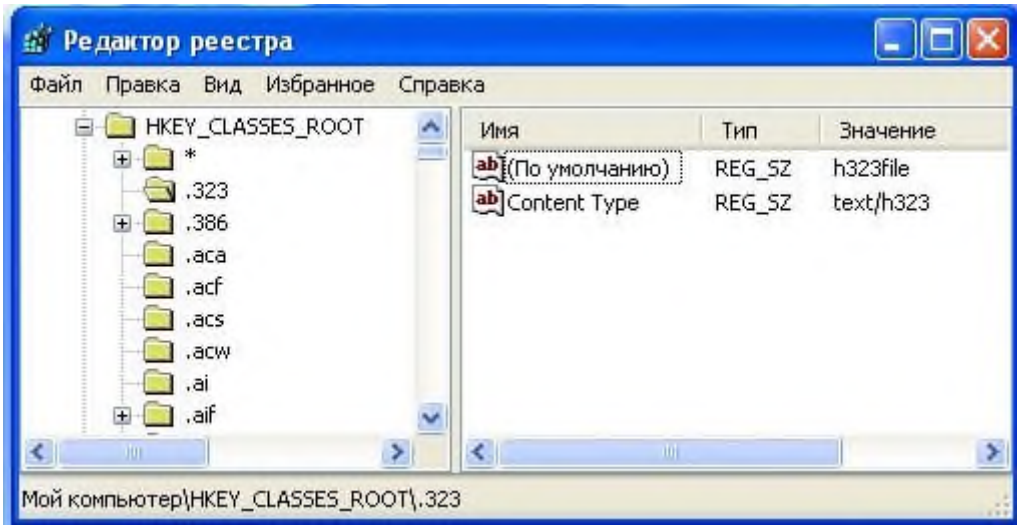
11= Ветка реестра «HKEY_USERS\<SID_пользователя>» формируется из файла «%USERPROFILE%\NTUSER.DAT»

12= Ветка реестра «HKEY_USERS\<SID_пользователя>_Classes» формируется из файла «%USERPROFILE%\AppData\Local\Microsoft\Windows\UsrClass.dat»

Резервные копии файлов реестра DEFAULT, SAM, SECURITY, SOFTWARE и SYSTEM находятся в папке «%SystemRoot%\System32\config\RegBack». Само резервное копирование производится силами Планировщика задач в 0 ч. 00 мин. каждые 10 дней по заданию «RegIdleBackup», расположенному в иерархии задач по пути «\Microsoft\Windows\Registry».

Ключи

Основными элементами структуры Реестра ОС являются ключи. Каждый ключ может иметь набор параметров, каждому из которых соответствует определенное значение, а также подключи – подчиненные ключи более низкого уровня. По отношению к друг другу ключи и подключи организуются в системном Реестре в соответствии с отношением вида «предок-потомок».



Иерархическая структура Реестра ОС представляет собой дерево ключей, организованное в виде кустов или ульев (каждый из которых является двоичным файлом, называемым файлом куста), напоминающей структуру файлов и папок файловой системы (ФС). Корневой ключ (вершина дерева) и подключи по аналогии с ФС можно считать папками, а параметры Реестра – файлами, соответственно.

В качестве кустов корневого ключа HKEY_LOCAL_MACHINE (HKLM) и соответствующих им файлов кустов можно привести следующий пример (табл. 6.1). Каждый из файлов кустов HKLM имеет свой системный путь. В частности, файлы кустов HKLM\SOFTWARE и HKLM\SYSTEM находятся в системном каталоге %SYSTEMROOT%\System32\config

№ п.п.	Куст	Файл куста

	HKLM\SAM	Sam.log
	HKLM\SECURITY	Security.log
	HKLM\SOFTWARE	Software.log, Software.sav
	HKLM\SYSTEM	System.log, System.sav

В таблице отображены не все кусты HKLM, а лишь те из них, которые являются постоянными Реестра ОС. В дополнение имеются два временных куста HKLM, образующиеся при старте системы.

Куст HKLM\SYSTEM корневого ключа HKLM является основным системным кустом, так как в него входит подключ \CurrentControlSet\Control, содержащий параметры, которые компонент ядра ОС, называемый «Менеджер конфигурации» (Configuration Manager), использует при инициализации Реестра.

Значение **hivelist** подключа \CurrentControlSet\Control используется системой при поиске остальных ее файлов куста.

В рассмотренном примере одним из ключей системного Реестра был назван корневой ключ HKEY_LOCAL_MACHINE.

Реестр ОС имеет несколько корневых ключей высшего уровня, каждый из которых определяет некоторую категорию данных, хранимых в Реестре. Полный список корневых ключей, а также их краткое описание представлены ниже. Некоторые ключи и соответствующие им кусты являются временными. К их числу можно отнести корневые ключи HKU, HKDD и некоторые HKLM с соответствующими кустами HKLM\HARDWARE и HKLM\SYSTEM\Clone. ОС создает их каждый раз при загрузке и хранит в оперативной памяти до момента завершения сеанса работы.

1. HKCR HKEY_CLASSES_ROOT. Подключи этого корневого ключа содержат основную информацию о типах файлов, зарегистрированных в системе. Названия подключей совпадают с соответствующими расширениями файлов. Корневому ключу HKCR подчиняются описания различных программных средств обработки этих файлов, а также сведения обо всех категориях зарегистрированных объектов.

2. HKCU HKEY_CURRENT_USER. Эта категория содержит описание параметров, меняющихся в зависимости от профиля пользователя, в данный момент работающего в системе. Изменения, относящиеся к текущему пользователю, следует всегда вносить именно сюда, так как они автоматически копируются для длительного хранения при завершений работы компьютера и восстанавливаются в ходе начальной загрузки ОС.

3. HKLM HKEY_LOCAL_MACHINE. Этот раздел отвечает за информацию об аппаратных компонентах компьютера и средствах, обеспечивающих их работу. Здесь также хранится общая информация об установленном программном обеспечении.

4. HKU HKEY_USERS. Этот раздел содержит подключи, соответствующие всем пользователям, зарегистрированным на данном компьютере. Когда один из пользователей начинает работу в системе, ОС автоматически копирует соответствующий ключ HKU в раздел HKCU. При завершении сеанса пользователя данные копируются обратно.

5. HKCC HKEY_CURRENT_CONFIG. В этом разделе дублируется информация (текущий набор конфигурационных параметров аппаратуры) о некоторых устройствах компьютера, в первую очередь о видеоадаптере и принтере.

6. HKDD HKEY_DYN_DATA. Этот раздел содержит текущую информацию о работе компьютера, обычно обновляемую в режиме реального времени. Основные подключи содержат данные об устройствах, работающих в настоящее время, а также сведения о текущем значении статистических параметров. Отобразить эти данные позволяет служебный модуль «Системный монитор».

Возвращаясь к вопросу о параметрах ключей и их значениях, следует сказать, что каждый ключ содержит как минимум одно значение какого-либо параметра. У параметра значения имеется имя, в то время как расширение файла похоже на его тип. Данные значения похожи на конкретное содержимое файла. Каждый ключ или подключ имеет одно

или более значений, в свою очередь, каждое из которых характеризуется именем соответствующего параметра, типом и хранимыми в нем данными.

Имя параметра значения (или просто имя значения) представляет собой строку, содержащую до 512 символов в кодировке ANSI (или 256 символов в кодировке Unicode), за исключением символов, зарегистрированных для имен ОС Windows XP. Всего для значений предусмотрено пятнадцать различных типов, три из которых: REG_BINARY, REG_DWORD и REG_SZ являются основными и описывают. Двоичные данные значений типа REG_BINARY, записанные в шестнадцатеричном виде, представляют собой строку байтов произвольной длины. Их обычно применяют в том случае, когда параметр должен хранить набор данных определенной структуры.

Значения типа REG_DWORD имеют длину данных в два машинных слова (четыре байта) и записываются в десятичной или шестнадцатеричной форме. Многие значения в Реестре принадлежат этому типу и используются в качестве логических флагов: 0 или 1, да или нет, истина или ложь; иногда значения этого типа встречаются в миллисекундах (1000 равно 1 секунде), описывающих время.

Ззначение типа REG_SZ представляет собой текст постоянной длины в виде строки символов, например, «Microsoft Windows XP». Каждая строка заканчивается символом null. Приложения не преобразуют значения этого типа, а транслируют и отображают их «как есть».

Контрольные вопросы

1. Что такое реестр и что с помощью него можно сделать?
2. Как работать с реестром через консоль Windows? Какие для этого существуют команды.
3. Как сделать резервную копию реестра?

Оформление отчета:

1. Цель работы.
2. Постановка задачи.
3. Подробное описание технологии выполнения каждого пункта задания, подкрепленное изображением.
4. Вывод.

Министерство образования и науки Российской Федерации
федеральное государственное бюджетное образовательное учреждение высшего образования
"Российский экономический университет имени Г.В. Плеханова"
МОСКОВСКИЙ ПРИБОРОСТРОИТЕЛЬНЫЙ ТЕХНИКУМ

ПРАКТИЧЕСКАЯ РАБОТА № 7
ДИСЦИПЛИНА: ОПЕРАЦИОННЫЕ СИСТЕМЫ

Тема: Файловый менеджер Far Manager. Управление доступом к файловым ресурсам.

Специальность: 09.02.03 «Программирование в компьютерных системах»
Квалификация: техник-программист

Цель работы:

Освоение навыков управления доступом пользователей к файлам и папкам с целью защиты информации от несанкционированного доступа

Время выполнения работы: 2 академических часа.

Теоретические сведения:

Файловые системы современных операционных систем при соответствующей настройке эффективно обеспечивают безопасность и надежность хранения данных на дисковых накопителях. Для операционных систем Windowsстандартной является файловая системаNTFS.

Устанавливая для пользователей определенные разрешения для файлов и каталогов (папок), администраторы могут защитить информацию от несанкционированного доступа. Каждый пользователь должен иметь определенный набор разрешений на доступ к конкретному объекту файловой системы. Кроме того, он может быть владельцем файла или папки, если сам их создает. Администратор может назначить себя владельцем любого объекта файловой системы, но обратная передача владения от администратора к пользователю невозможна.

Назначение разрешений производится для пользователей или групп. Так как рекомендуется выполнять настройки безопасности для групп, то необходимо, чтобы пользователь был членом хотя бы одной группы на компьютере или в домене.

Разрешения могут быть установлены для различных объектов компьютерной системы, однако в этой работе будут рассмотрены разрешения для файлов и папок. Другие задачи, например разрешения для принтеров, решаются аналогичным образом.

Указания к проведению лабораторной работы

Для назначения разрешений для файла или папки администратор выбирает данный файл или папку и при нажатии правой кнопки мыши использует команду Свойства (Properties) и в появившемся окне переходит на вкладку Безопасность (Security). Пример для папки с именем Авиатор приведен на рисунке 1.

В зоне Имя (Name) имеется список групп и пользователей, которым уже назначены разрешения для данного файла или папки.

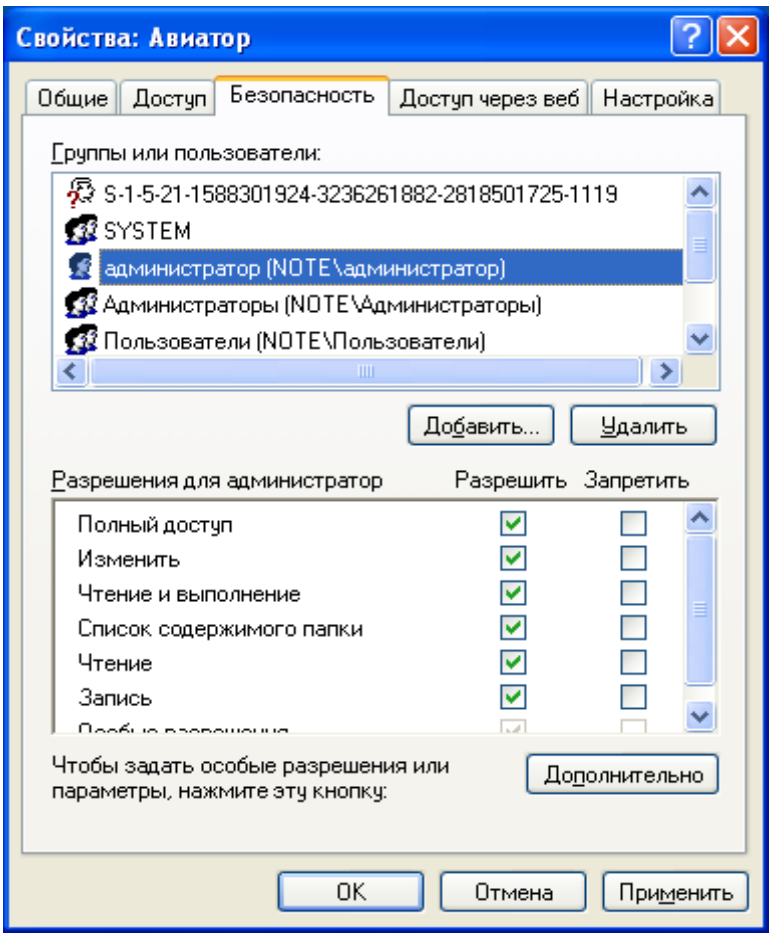


Рисунок 1 Вкладка Безопасность окна свойств папки Авиатор

Для добавления пользователя или группы нажмите кнопку Добавить (Add) или Удалить (Remove). При добавлении появится диалог Выбор: Пользователи, Компьютеры или Группы (SelectUsers,Computers,orGroups). Добавив пользователя или группу мы увидим этот объект в зоне Имя и выделив его, можем задать необходимые разрешения с помощью установки флажков Разрешить (Allow) или Запретить (Deny) в зоне Разрешения (Permissions).

Стандартные разрешения для файлов:

- Полный доступ (Full Control);
- Изменить (Modify);
- Чтение и выполнение (Read&Execute);
- Чтение (Read);
- Запись (Write).

Стандартные разрешения для папок:

- Полный доступ (Full Control);
- Изменить (Modify);
- Чтение и выполнение (Read&Execute);
- Список содержимого папки
- Чтение (Read);
- Запись (Write).

Разрешение Чтение позволяет просматривать файлы и папки и их атрибуты.

Разрешение Запись позволяет создавать новые файлы и папки внутри папок, изменять атрибуты и просматривать владельцев и разрешения.

Разрешение Список содержимого папки позволяет просматривать имена файлов и папок.

Разрешение Чтение и выполнение для папок позволяет перемещаться по структуре других папок и служит для того, чтобы разрешить пользователю открывать папку, даже если он не имеет прав доступа к ней, для поиска других файлов или вложенных папок. Разрешены все действия, право на которые дают разрешения Чтение и Список содержимого папки. Это же разрешение для файлов позволяет запускать файлы программ и выполнять действия, право на которые дает разрешение Чтение.

Разрешение изменить позволяет удалять папки, файлы и выполнять все действия, право на которые дают разрешения Запись и Чтение, и выполнение.

Разрешение Полный доступ позволяет изменять разрешения, менять владельца, удалять файлы и папки и выполнять все действия, на которые дают право все остальные разрешения NTFS.

Разрешения для папок распространяются на их содержимое: подпапки и файлы.

При назначении пользователю или группе разрешения на доступ к файлу или папке руководствуются тем уровнем доступа, который достаточен для данной группы или пользователя при выполнении им своих рабочих обязанностей.

Рассмотренные разрешения относятся к пользователям данного компьютера, совершившим вход локально непосредственно на данную машину. Такие разрешения называются разрешениями файловой системы.

Так как файловая система Windows называется NTFS, то разрешения файловой системы для Windows называют разрешениями NTFS.

Разрешения для пользователей, получившим доступ к папке или файлу через сеть, регулируются отдельно с помощью так называемых разрешений общего доступа. Эти разрешения распространяются только на папки, к которым предоставлен общий доступ через сеть и действуют только для пользователей, обращающихся к папке через сеть. Возможности пользователя задаются разрешениями, представленными ниже:

- Полный доступ (Full Control);
- Изменить (Change);
- Чтение (Read);

Доступ к средствам настройки разрешений общего доступа выполняется через свойства папки, предоставленной в общий доступ (рисунок 2)

Разрешения общего доступа являются средством обеспечения безопасности данных при коллективной работе с документами и поэтому должны устанавливаться очень тщательно и обоснованно. При этом администратору рекомендуется действовать следующим образом.

- Для каждого ресурса общего доступа определить, каким группам пользователей необходим доступ к нему и какой требуется уровень доступа;
- Для упрощения администрирования назначайте разрешения группам, а не отдельным пользователям;
- Устанавливайте максимально строгие разрешения, которые, однако, должны позволять пользователям совершать необходимые действия;
- Организуйте ресурсы общего доступа таким образом, чтобы папки с одинаковым уровнем требований безопасности находились в одной папке. Затем установите общий доступ только к ней, все вложенные папки наследуют настройки безопасности;
- Для папок общего доступа применяйте интуитивно понятные пользователям имена, корректно отображаемые всеми клиентскими операционными системами, используемыми на предприятии.
- Если в общих папках предполагается хранить программы-приложения, то целесообразно поместить их в одну папку – единое место хранения и обновлении я приложений;

Несколько общих папок, доступных членам группы Администраторы, так называемые скрытые Административные общие папки, создаются операционной системой автоматически. Имена этих папок заканчиваются знаком $. Это корневые каталоги каждого тома на жестком диске (C$,D$ и т.д.), папкаAdmin$ для доступа к системному каталогу, папкаPrint$ для доступа к файлам драйверов принтеров.

Кроме того, скрытую папку с общим доступом можно создать с целью доступа к ней только тех пользователей, которые будут знать имя скрытой папки.

Получить доступ к общим папкам других компьютеров можно используя компоненты Сетевое окружение, Мой компьютер, Мастер добавления в сетевое окружении и команду выполнить (Run).

Соединение с общей папкой через Сетевое окружение выполняется двойным щелчком по ресурсу, к которому необходимо получить доступ. Если общий ресурс отсутствует в списке доступных, выберите значок Добавить новый элемент в сетевое окружение и укажите адрес подключаемого ресурса.

Соединение с общей папкой через компонент Мой компьютер выполняется через меню Сервис этого компонента в пункте Подключить сетевой диск при указании пути к общему ресурсу. Если необходимо пользоваться этим соединением постоянно, нужно чтобы флажок восстанавливать при входе в систему был установлен. Соединение будет доступно в разделе Сетевые диске окна Мой компьютер.

Для соединения с общей папкой с помощью команды Выполнить щелкните Пуск, затем Выполнить и введите путь к папке в формате UNC (\\имя_ компьютера\имя_общей папки).

Рассмотрим, как пользоваться средствами установки разрешений файловой системы и общего доступа.

После выбора объекта, для которого будет выполняться настройка разрешений файловой системы, в диалоговом окне свойств файла или папки необходимо выбрать вкладку Безопасность, показанную на рисунке 4.3.

В данном случае показано, что для папки Авиатор для группы Администраторы установлены разрешения уровня Полный доступ, а для группы Все разрешения ограничены на уровне Чтение.

При установке разрешений в списке групп можно заметить имена так называемых встроенных системных групп, невидимых при использовании оснасток для управления группами и пользователями. Эти группы не имеют определенных членств, которые можно назначить или изменить, но в них система включает различных пользователей в различное время, в зависимости от того, каким образом пользователь получает доступ к системе или ресурсам.

Встроенные системные группы были рассмотрены выше в лабораторной работе №3. В данном случае имеется в виду группа Все, в которую во время своей работы входят все, кто получил доступ к компьютеру или домену.

Разрешения можно не только устанавливать, но запрещать. Запрет имеет больший приоритет, чем разрешение. Запрет разрешений как метод контроля ресурсов Microsoftприменять не рекомендует, и он используется, в основном, для дополнительной настройки разрешений конкретным пользователям, в отличие от разрешений для других пользователей группы.

Рассмотренные разрешения называются стандартными и позволяют решить большинство задач, связанных с регулированием уровня доступа групп к ресурсам.

Кнопка Дополнительно служит для задания специальных разрешений. Каждое стандартное разрешение состоит из нескольких специальных, например стандартное разрешение Запись состоит из шести специальных разрешений: создание файлов/запись данных, Создание папок/дозапись данных, запись атрибутов, Запись дополнительных атрибутов, чтение разрешений, синхронизация. Специальные разрешения можно использовать для более тонкой настройки в нестандартных ситуациях.

В окне специальных разрешений имеются закладки Аудит, Владелец.и Эффективные разрешения.

Аудит - это процесс, позволяющий фиксировать события, происходящие в системе и имеющие отношения к безопасности. На данной вкладке производится выбор пользователя или группы, для которых данная папка (или файл) будет объектом аудита. Аудит изучается в лабораторной работе № 6.

Закладка Владелец обеспечивает такое свойство безопасности, как право владения объектом файловой системы. Администратор всегда может стать владельцем любого объекта файловой системы, любой пользователь является владельцем созданных им объектов и, если локальные или доменные политики безопасности разрешат, пользователь может назначать себя владельцем других файлов и папок.

Подробное рассмотрение вопросов владения выходит за рамки данного пособия, однако отметим, что многие операции с файлами и папками, например смена разрешений, шифрование и дешифрование привязаны к факту владения данным объектом.

Список управления доступом (ACL) хранится на диске NTFS для каждого файла или папки. В нем перечислены пользователи и группы, для которых установлены разрешения для файла или папки, а также сами назначенные разрешения.

Каждому пользователю или группе могут быть установлены множественные разрешения через участие в нескольких группах с разным набором разрешений. В этом случае действуют эффективные разрешения – пользователь обладает всеми назначенными ему разрешениями.

Действует приоритет разрешений для файлов над разрешениями для папок и приоритет запрещения над разрешением.

Разрешения, назначенные родительской папке, по умолчанию наследуются всеми подпапками и файлами, содержащимися в папках. Однако есть возможность предотвратить наследование для любой вложенной папки и в этом случае эта папка сама становится родительской для вложенных в нее папок.

Если папка предоставлена для общего доступа, то на нее распространяются разрешения двух видов:

- разрешения файловой системы, установленные для пользователей данного компьютера;
- разрешения общего доступа, объявленные для пользователей, получивших доступ через сеть.

Обычно для папок общего доступа задают разрешения полного доступа, а ограничения вводят установкой разрешений NTFS[4,5].

В этом случае действует объединение разрешений NTFSи разрешений для общей папки, при котором наиболее строгое разрешение имеет приоритет над другими.

Задание к проведению лабораторной работы

- Создайте папку, в которую поместите текстовый файл и приложение в виде файла с расширением exe. Например, одну из стандартных программ Windows, такую какnotepad.exe(Блокнот).
- Установите для этой папки разрешения полного доступа для одного из пользователей группы администраторы, и ограниченные разрешения для пользователя с ограниченной учетной записью.
- Выполните различные действия с папкой и файлами для обеих учетных записей и установите, как действуют ограничения, связанные с назначением уровня доступа ниже, чем полный доступ.
- Установите общий доступ к папке и подключитесь к ней через сеть с другого виртуального компьютера.
- Установите разрешения общего доступа так, чтобы администратор не имел ограничений, а пользователь имел ограниченный уровень доступа.

- Экспериментально убедитесь в правилах объединения разрешений NTFSи разрешений общего доступа.
- Составьте отчет о проведенных экспериментах.
- Разработайте стратегию регулирования безопасности при коллективном доступе к общим папкам для различных групп пользователей.

Контрольные вопросы

- Какое из следующих разрешений NTFS для папок позволяет вам удалять папку?
- Чтение
- Чтение и выполнение
- Изменение
- Администрирование
- Какое разрешение NTFSдля файлов следует установить для файла, если вы позволяете пользователям удалять файл, но не позволяете становиться владельцами файла?
- Какие объекты по умолчанию наследуют разрешения, установленные для родительской папки?
- Кто может устанавливать разрешения для отдельных пользователей и групп? (выберите все правильные ответы)
- Члены группы Администраторы
- Члены группы Опытные пользователи
- Пользователи, обладающие разрешением Полный доступ
- Владельцы файлов и папок

5. Какой из следующих вкладок диалогового окна свойств файла или папки следует воспользоваться для установки или изменений разрешений NTFS:

- Дополнительно
- Разрешения
- Безопасность
- Общие

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

Оформление отчета:

1. Цель работы.
2. Постановка задачи.
3. Подробное описание технологии выполнения каждого пункта задания, подкрепленное изображением.
4. Вывод.

Министерство образования и науки Российской Федерации
федеральное государственное бюджетное образовательное учреждение высшего образования
"Российский экономический университет имени Г.В. Плеханова"
МОСКОВСКИЙ ПРИБОРОСТРОИТЕЛЬНЫЙ ТЕХНИКУМ

ПРАКТИЧЕСКАЯ РАБОТА № 8
ДИСЦИПЛИНА: ОПЕРАЦИОННЫЕ СИСТЕМЫ

Тема: Основы работы в Unix-системах.

Специальность: 09.02.03 «Программирование в компьютерных системах»
Квалификация: техник-программист

Цель работы: ознакомиться с операционной системой Unix, получить практические навыки работы в наиболее распространенном командном интерпретаторе bash, изучить принципы организации файловой системы Unixи базовых команд управления файлами.
Время выполнения работы: 2 академических часа.
Теоретические сведения:

Система Unix различает БОЛЬШИЕ и малые буквы.

Если вы уничтожили какой-нибудь файл, то восстановить уничтоженный файл в системе Unix НЕВОЗМОЖНО. В Unix отсутствует команда unerase

В имени файла директории отделяются от последующей части символом если имя начинается со слэша — значит, это полное маршрутное имя. Простое имя файла может состоять из ЛЮБЫХ символов. Длина простого имени не более 256 символов. Длина полного маршрутного имени файла не более 1024 символов.

Для задания шаблона имен используются символы "*" (произвольная последовательность символов) и "?" (один произвольный символ). Имя из одной точки "." обозначает текущую директорию, имя из двух точек ".." - вышележащую (родительский

каталог).

Чтобы запустить программу на выполнение, достаточно набрать ее имя и, если нужно, другие аргументы командной строки. Имя программы - это маршрутное имя файла, в котором эта программа находится. Аргументы разделяются одним или несколькими пробелами и табуляторами. Ключи команды обычно (но не всегда) выделяются знаком "-".

команда -ключи -ключи ... прочие разные аргументы ...

Если командная строка кончается знаком &, то команда запустится параллельно (фоном). На терминале печатается номер, который получает запущенный процесс. После чего можно продолжать работу, не дожидаясь завершения фоновой задачи.

команда -разные аргументы ... &

1.7. Команда имеет три предопределенных направления ввода-вывода - стандартный ввод, стандартный вывод и стандартный протокол. Как правило, команда берет исходные данные из стандартного ввода и печатает результаты в стандартный вывод. В стандартный протокол печатаются сообщения об ошибках и диагностика. Первоначально стандартные ввод, вывод и протокол назначены на терминал, однако их можно переназначить, используя следующие конструкции:

команда > имя_файла

(для стандартного вывода),

команда < имя_файла

(для переназначения стандартного ввода),

команда 2> имя_файла

(для стандартного протокола - системной диагностики).

Если вывод назначен в файл, то перед началом выполнения команды создается пустой файл с соответствующим именем (если файл уже существовал, он опустошается), а затем в него помещается информация. Если информацию нужно дописать в конец существующего файла, следует воспользоваться конструкцией

команда >> имя файла

команда 2>> имя файла

1.8. Пользователи системы Unix объединяются в группы, и каждая из групп обладает определенным набором прав доступа к файлам.

Дерево каталогов в Unix.

Файловая система - собрание файлов и иерархия каталогов.

/	Корневой каталог, аналог «Моего компьютера» в Windows
/bin	``binaries" (т.е. двоичные или выполняемые файлы). Здесь находится много важных системных программ(cp, ls, mv, и др). Это и есть программы

	соответствующих команд. Когда, например, вы используете команду cp, выполняете программу /bin/cp.
/dev	``devices``. "Файлы" в /dev известны как драйверы устройств - они используются для доступа к устройствам и ресурсам системы, таким как диски, модемы, память и т.д. Например, как вы можете читать данные из файла, точно также вы можете читать входные сигналы от мыши, имея доступ к /dev/mouse.
/etc	Содержит множество всевозможных системных файлов конфигурации. Они включают /etc/passwd (файл паролей), /etc/rc (командный файл инициализации) и т.д.
/mnt	Содержит каталоги для монтирования (подключения) файловых систем. К примеру, здесь может находиться каталоги /mnt/floppуи /mnt/cdrom– в них соответственно фалы, находящиеся на дискете и компакт-диске, вставленных в приводы.
/sbin	``system binaries`` (т.е системные двоичные или выполняемые файлы). Используется для хранения важных системных двоичных файлов, используемых системным администратором.
/home	Содержит домашние каталоги пользователей. Например, /home/ik11-04 - домашний каталог пользователя ``ik11-04". На вновь инсталлированной системе этот каталог может быть пуст в связи с временным отсутствием зарегистрированных пользователей.
/proc	"Виртуальная файловая система", в которой файлы хранятся в памяти, а не на диске. Они связаны с различными процессами, происходящими в системе, и позволяют получить информацию о том, что делают программы и процессы в указанное время.
/tmp	Временный каталог, многие программы нуждаются в создании рабочих файлов, которые нужны короткое время. Каноническое место для этих файлов в /tmp
/usr	Состоит из ряда подкаталогов, которые в свою очередь содержат наиболее важные и полезные программы и файлы конфигурации, используемые системой. Различные каталоги, описанные выше, необходимы для нормального функционирования системы, но большинство программ, содержащихся в /usr необязательны для системы. Содержит много больших программных пакетов и конфигурационных файлов, которые их сопровождают.
/usr/X11R6	Содержит TheXWindowSystem(если она установлена).TheXWindowSystem-это мощная графическая среда, которая содержит большое количество графических утилит и программ, отображающих "окна" на вашем экране. Каталог /usr/X11R6 содержит все выполняемые и конфигурационные файлы X Window, а также файлы поддержки.
/usr/bin	Каталог для различных программ Unix. Он содержит большинство выполняемых программ, которых нет ни в каких других местах, например, в том же /bin их нет.

/usr/etc	Точно так же, как и /etc, содержит всевозможные системные программы и конфигурационные файлы, утилиты и файлы. В общем, файлы, находящиеся в /usr/etc, несущественны для системы, в отличие от тех, которые находятся в /etc.
/usr/include	Содержит include-файлы для компилятора Си. Эти файлы, большинство имен которых заканчивается на .h (от слова ``header'') объявляют имена структур данных, подпрограмм и констант, используемых при написании программ на Си. Те файлы, которые находятся в/usr/include/sys, в общем случае, используются при программировании на системном уровне Unix.
/usr/lib	``libraries`` (т.е библиотеки). Содержит образы разделяемых библиотек (shared library images). Эти файлы содержат код, который могут использовать многие программы. Вместо того, чтобы каждая программа имела свою собственную копию этих выполняемых файлов, они хранятся в одном общедоступном месте - в /lib.
/usr/local	В большой степени похоже на /usr - он содержит различные программы и файлы, несущественные для системы. В общем, программы, находящиеся в /usr/local, специализируются на специфике вашей системы, т.е. /usr/local сильно отличается в различных UNIX. Здесь вы найдете такие большие программные пакеты, как TeX (система форматирования документов) и Emacs(большой и мощный редактор), если они установлены.
/usr/local/man	Этот каталог содержит страницы Руководства. Здесь два подкаталога для каждого "раздела" Руководства. (С помощью команды "man man" вы можете получить более подробную информацию).
/usr/src	Содержит исходные коды (неоткомпилированные программы) для различных программ вашей системы.
/var	Содержит каталоги, которые часто меняются в размере или имеют тенденцию быстро расти. Многие из этих каталогов перешли в /usr, но поскольку мы стремимся сделать его достаточно стабильным, каталоги, которые часто меняются были перенесены в /var.
/var/log	Содержит различные файлы, фиксирующие ошибки и проблемы (лог-файлы), возникающие в системе.
/var/spool	Содержит файлы, которые предварительно формируются для других программ. Например, если ваша машина подключена к сети, входная почта будет помещаться в /var/spool/mail до тех пор, пока вы не прочитаете ее или не удалите. Входящие и исходящие новости помещаются в /var/spool/newsи т.д.

Предопределенные пользователи и группы

При установке системы в файлы /etc/passwd и /etc/group автоматически записываются сведения о предопределенных пользователях и группах. Это делается для того, чтобы было проще управлять правами доступа к системным файлам.

Предопределенные группы и пользователи требуются для того, чтобы от их имени работали системные службы, и в то же время доступ к файлам этих служб был ограничен для всех остальных.

Привилегированный пользователь

Один из предопределенных пользователей - это пользователь root с UID, равным нулю.

Пользователь с таким UID называется суперпользователем (superuser) или привилегированным пользователем и всегда имеет имя root. Он имеет неограниченные права на доступ к любому объекту в системе.

Тот, кому доверен пароль суперпользователя, должен хорошо знать основные процедуры администрирования UNIX и работать в системе так, чтобы не навредить ей. Системный администратор отвечает за безопасность системы, ее стабильную работу, добавление и удаление пользователей, регулярное резервное копирование и т.д. Он должен хранить пароль суперпользователя как зеницу ока. Доверять пароль суперпользователя многим людям не следует: системный администратор всегда должен точно знать, что любое действие от имени root сделал проверенный человек. Круг работ, которые выполняет системный администратор, всегда следует очень четко делить между несколькими людьми, а еще лучше - поручать эту работу единственному сотруднику.

Вход в систему под именем root разрешен только с терминалов, непосредственно присоединенных к UNIX-машине. Подключение через сеть от имени root запрещено. При надобности выполнить команду от имени root через сеть следует подключиться от имени обычного пользователя, а затем выполнить команду "превращения" в привилегированного пользователя (su). Пользователь root никогда не должен иметь пустой пароль.

Как стать привилегированным пользователем

В UNIX можно "перевоплотиться" в любого пользователя. Для этого служит команда su (switch user):

```
su имя_пользователя
```

Команда su без параметров эквивалентна su root.

Для перевоплощения в другого пользователя нужно знать его пароль. В некоторых системах UNIX дать команду su для того, чтобы работать от имени root, по умолчанию может только член группы wheel. Так, например, установлено во FreeBSD. В системах, где для аутентификации используется подсистема PAM, такой эффект достигается следующей строкой в файле /etc/pam.d/su:

```
auth required /lib/security/pam_wheel.so
```

Подсистема PAM в настоящее время поддерживается во всех основных системах UNIX: Solaris, HP-UX, FreeBSD и всех новых версиях Linux

"Перевоплощение" означает, что дальнейшая работа будет происходить в командном процессоре, который программа su запускает от имени другого пользователя - того, в которого вы перевоплотились. Каждому пользователю, кроме root, для того, чтобы начать работу от имени другого пользователя, требуется знать его пароль.

Команда su по умолчанию запускает командный процессор от имени другого пользователя, но сохраняет среду окружения старого, т.е. среда окружения наследуется от того командного процессора, в котором выполнена команда su. Это мешает перевоплотиться полностью. Например, если пользователь alen выполнил команду su, то работать от имени root он сможет, а читать почту из почтового ящика root - нет. Потому что почтовая программа проверяет переменную mail и (или) user, которая унаследуется от старого командного процессора.

Чтобы получить среду окружения в том виде, в котором ее получает другой пользователь при своем входе в систему, следует дать команду

```
su - имя_пользователя
```

Обратите внимание на знак - (минус) после команды su.

Например, для полного перевоплощения в пользователя breatney следует дать команду

```
su - breatney
```

В некоторых системах UNIX есть программа sudo, с помощью которой любой пользователь может выполнить команду от имени другого пользователя. Системный администратор должен заранее отредактировать файл /etc/sudoers, в котором определяется, кто и что может запускать от чужого имени. При выполнении программа sudo спросит у

пользователя его пароль, чтобы убедиться, что ее запускает не тот, кто случайно подошел к терминалу с незакрытой сессией работы.

В Solaris нет sudo, зато есть более сложный способ делегирования части полномочий администратора другим пользователям. Для этого используется управление доступом на основе ролей (RBAC - role based access control). Его смысл состоит в том, что среди всех полномочий системного администратора выделяются их группы, а затем некоторые пользователи наделяются таким подмножеством полномочий, которое соответствует их реальной роли в администрировании системы.

Что делать, если вы забыли пароль суперпользователя

Если пользователь забыл свой пароль, то сообщить ему, какой он был, невозможно. Надо просто установить ему новый. Это можно сделать командой

```
passwd user
```

Включение и выключение компьютера

Что происходит после нажатия на кнопку включения компьютера? Начинается загрузка - сначала BIOS, затем - операционной системы. При загрузке UNIX сначала загружается ядро, затем - все остальное. Подробно процесс загрузки описан в лекции 9.

На всех терминалах после загрузки будут светиться приглашения " login:".

Во время загрузки будут запущены сетевые и системные приложения, такие как сервер протоколирования syslogd, web-сервер, сервер баз данных.

Solaris, так же, как и любая другая UNIX-система, предназначен для круглосуточной работы в течение неограниченного времени. Однако в некоторых ситуациях, например, для проведения планового обслуживания или замены оборудования, компьютер может понадобиться выключить.

Однако нельзя выключать Solaris когда угодно. Перед выключением следует обязательно дать команду shutdown или halt.

В разных системах UNIX эта команда имеет разные ключи и совершает разные действия по умолчанию. Программа shutdown, вызванная без параметров, выдает на все активные терминалы, подключенные к системе, сообщение о завершении работы, ждет одну минуту, затем останавливает систему.

В Solaris команда shutdown имеет ключ g, который задает время в секундах, через которое следует начать процедуру выключения системы. Для немедленного останова следует дать команду

```
shutdown -g 0
```

По команде shutdown Solaris переходит в режим работы 0. В этом режиме система завершает работу, и питание компьютера выключается. Выключение питания должно поддерживаться аппаратно. Если это не так, система выключается и предлагает ввести пароль root для продолжения работы в однопользовательском режиме или Ctrl-D для перезагрузки в многопользовательский режим. Подробнее о режимах работы системы говорится ниже в разделе "режимы работы системы" и в лекции 9.

В случае перехода в однопользовательский режим можно, не опасаясь потери чьих-либо данных, дать команду halt, которая вызывает немедленный останов системы без выдачи предупреждений на терминалы.

Перезагрузку системы следует выполнять по команде reboot.

Выключать UNIX простым отключением питания без предварительного предупреждения (в виде shutdown или halt) нежелательно, так как данные, еще не записанные на диск и хранящиеся в оперативной памяти, будут потеряны. Иногда это приводит к ошибкам в файловой системе на диске и может потребовать их исправления программой fsck (аналог scandisk в Windows). Команду shutdown может дать только root.

Пользовательский интерфейс

Интерфейс пользователя в UNIX может быть текстовым и графическим. Текстовый интерфейс является основным для большинства систем UNIX. Однако в Solaris часто используется графический интерфейс. Мы рассмотрим оба типа интерфейсов. Фактически,

все команды, которые выполняются в текстовом интерфейсе, могут быть выполнены в текстовом окне в графическом интерфейсе. Графический интерфейс редко применяется для встроенных систем Solaris, например, там, где Solaris управляет автоматической телефонной станцией или технологическим процессом на заводе. Поэтому системный администратор должен уметь работать, используя любой интерфейс.

Вход в систему и выход из системы

Для входа в систему следует набрать имя пользователя (login) и пароль (password). После загрузки система работает самостоятельно, независимо от того, вошел кто-то в нее или нет. Под "войти в систему" мы подразумеваем начало интерактивного сеанса работы с системой, когда пользователь отдает ей команды, сидя перед клавиатурой и экраном.

После входа пользователя в систему для него запускается программа - командный процессор. Эта программа также часто называется интерпретатором команд, оболочкой или "шеллом" (shell). В среде этой программы проходит весь сеанс работы пользователя с системой. При входе с графической консоли Solaris вся работа проходит в среде программы-менеджера окон. Графический интерфейс пользователя и программы, которые его обеспечивают, в Solaris называется CDE (Common Desktop Environment

Для выхода из системы следует дать команду logout или нажать кнопку Exit в центре внизу экрана, если вы работаете в CDE. При работе в командном процессоре в текстовом режиме достаточно нажать Ctrl-D или дать команду exit (это эквивалентно Ctrl-D). Если в процессе работы вы запустили несколько командных процессоров, то команду exit или Ctrl-D придется давать до тех пор, пока, выходя из запущенных командных процессоров, вы не доберетесь до самого первого, который запустился при вашем входе в систему.

Режимы работы системы

UNIX может работать в однопользовательском режиме (single-user mode) или в многопользовательском режиме (multi-user mode).

Для обычной работы система загружается в многопользовательском режиме. В нем пользователи могут одновременно входить в систему локально или через сеть, посылать программам, работающим в системе, запросы различного характера по сети. В этом режиме множество пользователей одновременно могут работать в системе. Их число ограничивается размером таблиц ядра. Ограничение числа одновременно работающих пользователей связано не с числом одновременно запущенных командных процессоров или сеансов связи, а с количеством запущенных процессов и потребляемых ими ресурсов. Поэтому в каждый момент времени максимальное число пользователей, имеющих возможность работать с системой, может меняться.

Однопользовательский режим используется системным администратором для настройки, резервного копирования или ремонта системы (например, запуска программы fsck, которая выполняет проверку и исправление ошибок в файловых системах дисков, или программы dump, которая выполняет резервное копирование).

Для загрузки системы в однопользовательском режиме следует дать команду

```
boot -s
```

или

```
b -s
```

программе-загрузчику.

Для перехода из многопользовательского режима в однопользовательский дайте команду

```
init s
```

или

```
init S
```

Тот же эффект даст выполнение команды shutdown без параметров.

Для того чтобы перевести систему из однопользовательского режима в многопользовательский, нужно перезагрузить компьютер или выйти из командного процессора однопользовательского режима (exit или Ctrl-D, работает в большинстве

случаев). Кроме этого, можно запустить программу init с параметром-названием режима работы, например

```
init 3
```

Существует несколько режимов работы (runlevels) операционной системы. Режим с номером 1 соответствует однопользовательскому режиму, с номером 3 - многопользовательскому. Режим номер 0 - это останов (на этот уровень систему переводит команда shutdown).

Подробнее о режимах работы системы говорится в руководстве по системе:

```
man init
```

Понятие терминала

Терминал - это экран и клавиатура, с помощью которых осуществляется связь с компьютером.

Терминалы бывают графические и текстовые. Графические терминалы могут работать и в графическом, и в текстовом режиме.

Терминал предназначен исключительно для ввода информации и ее отображения на экране. Терминалы бывают физическими (еще их называют реальными), виртуальными и псевдотерминалами (т.е. программами, которые "притворяются" терминалами).

Физический терминал - это устройство, состоящее из экрана и клавиатуры, обычно подключенное к компьютеру через последовательный интерфейс, например, с помощью кабеля или модема. Если вы соединяетесь с UNIX-машиной с помощью эмулятора терминала через модем своего компьютера, позвонив на другой модем, подключенный непосредственно к UNIX-машине, то с точки зрения UNIX вы работаете на физическом терминале. В этом случае связка модем - телефонная сеть - модем рассматривается как единый кабель.

В старых версиях Solaris неофициально поддерживались виртуальные терминалы. В версии 9 эта поддержка отсутствует. Основа виртуального терминала — это монитор и клавиатура, непосредственно подключенные к компьютеру. Однако, хотя монитор всего один, виртуальных терминалов может быть несколько. Вы можете по очереди работать с разными виртуальными терминалами, нажимая клавиши Alt-Fx, где x - номер терминала. С монитором и клавиатурой связано несколько независимых виртуальных терминалов. При работе в графическом режиме надо использовать клавиши Ctrl-Alt-Fn для переключения между виртуальными терминалами.

Виртуальные терминалы, как правило, текстовые, хотя один из них может быть графическим.

Виртуальные терминалы чаще всего используются в компьютерах на платформе i386, потому что терминалы, подключаемые к компьютерам на других платформах, обычно постоянно работают в графическом режиме, а в этом режиме вместо нескольких виртуальных терминалов проще открыть несколько окон эмуляторов терминала. Виртуальные терминалы широко используются в Linux и FreeBSD.

При работе с графическим терминалом для получения нескольких терминалов достаточно просто открыть несколько окон и в каждом из них запустить терминальную программу. Так, в Solaris можно запустить несколько приложений, обозначенных в меню CDE как "console". Программа, которая запускается при выборе приложения "console", называется dtconsole. Выбрав в меню "This host", вы запустите терминальную программу dtterm.

Консоль - это терминал, который используется для загрузки операционной системы.

Проще говоря, если системный администратор при загрузке использует некий терминал для наблюдения за процессом загрузки и (возможно) вмешательства в него, то этот терминал называется консолью. Для UNIX-систем консоль — это либо непосредственно подключенный к компьютеру монитор и клавиатура, либо подключенный к первому последовательному порту терминал. В приложении к виртуальным терминалам консолью является первый виртуальный терминал (Alt-F1).

Псевдотерминал — это программа-эмулятор терминала, которая соединяется с UNIX-компьютером через сеть или запускается в графическом режиме (например, dtterm).

Любой терминал (физический, виртуальный или псевдотерминал) может быть графическим. Эмулятор графического терминала базируется на программе X-Server.

Текстовые терминалы могут отображать только текст и псевдографику. Мы будем рассматривать значительную часть команд Solaris в предположении, что мы работаем с текстовым терминалом. В то же время, когда в Solaris доступна и полезна программа с графическим интерфейсом, которая часто нужна системному администратору в работе, мы будем рассматривать и такие случаи.

Существует большое количество разных текстовых терминалов. Наиболее известны терминалы ANSI и VT-100. Разные терминалы отличаются друг от друга управляющими последовательностями. Например, чтобы передать терминалу команду "поднять курсор на одну строку вверх", терминалу VT-100 нужно передать последовательность <Esc>[A. Описания терминалов (и соответствующих управляющих последовательностей) содержатся в файле /etc/termcap и базе данных в подкаталогах /usr/share/lib/terminfo.

Переменная среды окружения TERM должна иметь значение типа терминала, на котором вы работаете. Возможно, ее придется переопределить, если в начале вашей работы система неверно определила тип вашего терминала. Фактический тип вашего терминала может отличаться от того, что принят в системе по умолчанию. Переопределение выполняется путем присваивания переменной нужного значения:

```
TERM='VT100'; export TERM
```

Вывести на экран значение переменной TERM можно командой

```
echo $TERM
```

Если переменная TERM определена неверно, терминал будет вести себя непредсказуемо. Например, при нажатии Enter не произойдет перевода строки, или при нажатии стрелки "вверх" на экране появится [[A, а курсор вверх не сдвинется. Некоторые терминалы практически совместимы между собой, например, ANSI и VT-100. Однако отдельные управляющие последовательности могут не совпадать. Поэтому лучше, чтобы в TERM был записан тип именно того терминала, на котором вы работаете.

Таблица 2.1. Управляющие комбинации клавиш	
Ctrl-C	прерывание выполнения программы (termination)
Ctrl-D	конец ввода текста
Ctrl-S	остановка вывода на экран
Ctrl-Q	продолжение вывода на экран
Ctrl-U	стирание введенной строки
Ctrl-Z	остановка выполнения программы (suspend)
<backspace>	удаление последнего введенного символа

Управляющие комбинации клавиш

Текстовый терминал воспринимает и передает активной программе коды следующих управляющих комбинаций клавиш, которые любая программа должна интерпретировать стандартным образом:

Некоторые терминалы не воспринимают клавишу <backspace> стандартным образом, вместо нее на таких терминалах можно использовать клавишу <Delete>.

В старых системах клавиша <Delete> могла использоваться вместо <Ctrl-C> для прерывания работы программы.

Команда Ctrl-D (конец ввода текста) может использоваться в командном интерпретаторе для выхода из него. При работе в текстовом режиме выход из командного интерпретатора, запущенного для пользователя при входе в систему (такой экземпляр интерпретатора называется login shell), означает автоматическое завершение сеанса работы с системой (logout).

В некоторых системах командный интерпретатор по умолчанию настраивается так, чтобы такого завершения работы не происходило. В этом случае выйти из системы пользователь может, только дав команду logout.

Настройка терминала: команда stty

Проверить, как настроен терминал, можно с помощью программы stty:

```
stty -a
```

Эта команда позволяет узнать все настройки терминала, в том числе скорость и другие физические параметры передачи символов, а также управляющие комбинации

Основные команды для работы в консоли

Операции с файлами.

Этот раздел представляет некоторые наиболее полезные базовые команды Unix, включая те, о которых говорили в предыдущем разделе.

Обратите внимание, что опции обычно начинаются с ``-" и во многих случаях несколько однобуквенных опций могут следовать за одним минусом, записанные слитно. Например, вместо использования ls -l -F, можно использовать ls -lF.

Вместо перечисления всех возможных опций каждой команды, мы будем говорить только о тех, которые полезны или важны в данное время. Действительно, большинство из этих команд имеет большое число опций (большинство из которых почти никогда не используется).

Вы можете для каждой команды с помощью man посмотреть все возможные опции. Обратите также внимание на то, что многие из команд берут список файлов или каталогов, как аргументы, обозначенные как``<file1> ... <fileN>". Например, команда cp берет в качестве аргументов список файлов, которые надо копировать, за которыми следует имя целевого файла или каталога. При копировании нескольких файлов в качестве целевого может выступать только каталог.

pwd	Возвращает название текущего рабочего каталога, тоесть того, где сейчас находится пользователь (pwd–printworkdirectory). Синтаксис: pwd
	Пример: [root#franzycd]pwd /usr [root#franzycd] Т.е текущий каталог - /usr
cd	Изменяет текущий рабочий каталог (cd - change directory). Синтаксис: cd <directory>; <directory> - каталог, в который перейти (``." Ссылается на текущий каталог, ``.." - на родительский каталог).
	Пример: [/home@target ~$]cd /home/ik11-04 [root#franzycd]
ls	Выдает информацию о файлах в каталоге (ls-list). Синтаксис: ls <file1> ... <fileN> Где <file1> ... <fileN> имена файлов или каталогов, информацию про которые надо выдать. Если каталог не задан – выводится информация о содержимом текущего каталога Опции: Наиболее часто используемые: -F для представления информации о типах файлов -l выдает в длинном (``long") формате информацию о размерах файлов, владельцах, правах доступа и т.д.
	Пример: [root#franzycd]ls -lF /home/name

	total 842 drwxr-xr-x 7 ness users 1536 8 июн 15:20 . drwxr-xr-x 753 root wheel 13824 27 май 00:04 .. -rwxr-xr-x 1 ness users 496 10 сен 2002 .Sig -rw------- 1 ness users 201 26 фев 19:43 .Xauthority -rwxr-xr-x 1 ness users 2488 19 авг 2002 .bashrc -rwxr-xr-x 1 root users 19 10 фев 18:26 .htpasswd -rwxr-xr-x 1 ness users 371 13 янв 18:45 .mail_aliases -rwxr-xr-x 1 ness users 331 16 авг 2002 .mailrc drwxr-xr-x 3 root users 512 8 июн 15:20 .mc -rwxr-xr-x 1 ness users 17390 10 сен 2002 .muttrc -rwxr-xr-x 1 ness users 500 10 сен 2002 .signature -rwxr-xr-x 1 ness users 6947 8 июн 14:11 .viminfo -rwxr-xr-x 1 ness users 10 16 авг 2002 .vimrc [root#franzycd]
cp	Копирует файл(ы) в файл или каталог (cp–copy). Синтаксис: cp <file1> ... <fileN> <destination> Где <file1> ... <fileN> имена копируемых файлов, а <destination> файл или каталог, в который копируют.
	Пример: [root#franzycd]cp .Sig .copySig [root#franzycd] Копируем файл .Sig в файл .copySig
mv	Перемещает файл(ы) в другой файл или каталог (mv-move). Эта команда не эквивалентна копированию с последующим уничтожением оригинала. Она может быть использована для переименования файлов, как командаRENAMEизMS-DOS. Синтаксис: mv <file1> ... <fileN> <destination> Где <file1> ... <fileN> имена перемещаемых файлов, а<destination> имя файла или каталога, в который перемещают.
	Пример: [root#franzycd]mv .Sig .copySig [root#franzycd] Перемещаем файл .Sig в файл с названием .copySig (т.е переименование)
rm	Удаляет файлы (rm–remove). Имейте в виду, когда в Unix удаляются файлы, они не восстановимы (не как в MS-DOS, где вы можете восстановить файл). Синтаксис: rm <file1> ... <fileN> Где <file1> ... <fileN> имена удаляемых файлов. Опции: -iпотребует вашего подтверждения перед удалением файла. -Rрекурсивное удаление, относительно папки, которую удаляют -fудаление файлов(каталогов) без подтверждения
	Пример: [root#franzycd]rm -i .Sig remove .Sig? y [root#franzycd] Удаляем файл .Sig в папке /home/ik11-04
mkdir	Создает новые каталоги (mkdir – make directory). Синтаксис: mkdir <dir1> ... <dirN> Где <dir1> ... <dirN> создаваемые каталоги.
	Пример: [[root#franzycd]mkdir /home/name/test

	[root#franzycd] Создает каталог test в каталоге /home/name
rmdir	Эта команда удаляет пустые каталоги (rmdir–removedirectory). При использовании rmdir ваш текущий рабочий каталог должен находиться вне удаляемого каталога. Синтаксис: rmdir <dir1> ... <dirN> Где <dir1> ... <dirN> удаляемые каталоги.
	Пример: [root#franzycd]rmdir /home/name/test [root#franzycd] Удаляет каталог /home/name/test, если он пустой.

Получение справки и помощи в Unix.

Практически каждый UNIX имеет то, что называется "Руководство" - man (``manual pages"). Эта команда man содержит документацию на различные команды системы, ресурсы, конфигурационные файлы.

Для ее использования необходимо набрать man<имя команды>, в результате чего на экран будет выведена информация по использованию данной команды. Для примера посмотрим как можно использовать (с какими параметрами) саму команду man:

Команда INFO также позволяет пользователю перемещаться по ссылкам на соответствующую дополнительную информацию. Для этого необходимо клавишами курсора (Вверх-Вниз-Влево-Вправо) установить курсор на ссылке, обозначенной двойным двоеточием (::), и нажать Ввод или Пробел.

Используя команды MAN и INFO Вы также должны знать, что получая информацию, можете воспользоваться клавишами Вверх-Вниз, что просмотреть полученное на экране Руководство. Для использования поиска в командной строке MAN и INFO необходимо ввести:

/<шаблон>, где<шаблон> - информация, которую необходимо найти в выданной командами информации

Для выхода из MAN / INFO необходимо ввести q в команду строке.

Практическое задание

1. Вход в систему
2. Просмотр и перемещение по директориям.

Сразу после входа в систему под пользователем rootвы окажетесь в каталоге /root– это домашний каталог суперпользователя (это единственное исключение: все вновь создаваемые пользователи и их начальные каталоги по умолчанию помещаются в каталог/home).

Проверьте, верно ли это утверждение.

Для этого наберите команду pwd.

Далее просмотрите файлы, находящиеся в этой директории(команда ls).

Перейдите в каталог /root(либо тот, который указал преподаватель). Просмотрите его содержимое в кратком и полном форматах (командаls).

3. Создание каталогов и файлов.

В каталоге /root(либо том, который указал преподаватель) попробуйте создать свой домашний каталог вида /root/<свое имя>. (Например/root/name). Для создания каталога воспользуйтесь командойmkdir.

Скопируйте файл /etc/rc.confв ваш домашний каталог. Воспользуйтесь командой ср.Просмотритеего содержимое с помощью утилиты просмотра текстовых файловless. Ее параметры и ключи самостоятельно найдите на страницах справочного руководства. Для этого необходимо набрать man less. Для выхода из утилиты просмотра необходимо нажать клавишу «q».

Переименуйте файл /root/name/rc.conf под именем /root/name/name1.conf. Сделайте 3 копии этого файла с именами name2.conf name3.conf name4. conf.

Скопируйте каталог /etcc вложенными подкаталогами и файлами в ваш домашний каталог. Для этого необходимо вести команду cpc ключом рекурсивного копирования. Самостоятельно найдите этот ключ на страницах руководства. Теперь просмотрите содержимое скопированного каталога в полном формате.

Скопируйте каталог/root/name/etc в каталог /root/name/eee

Создайте еще одну пустую директорию с именем /root/name/conf/. Переместите туда 2 файлаname3.conf и name4.conf.

3. Удаление файлов и каталогов.

Удалите файл name3.conf из директории /root/name/conf/.

Перейдите в каталог /home/name/eee/. Удалите рекурсивно все файлы и подкаталоги этого каталога. Проверьте, получилось ли у вас это.

Контрольные вопросы:

1. Что такое среда пользователя? Опишите, как добавить новую переменную в среду, как изменить значение существующей переменной для одного пользователя и всех пользователей в системе.
2. Опишите одну реальную ситуацию, когда вам может понадобиться изменить переменную среды при запуске приложения.
3. Какие основные каталоги системы вы знаете? Каково их назначение?
4. Как обратиться к файлу, который находится в каталоге, расположенном выше относительно текущего в дереве каталогов системы?

Оформление отчета:

1. Цель работы.
2. Постановка задачи.
3. Подробное описание технологии выполнения каждого пункта задания, подкрепленное изображением.
4. Вывод.

Министерство образования и науки Российской Федерации
федеральное государственное бюджетное образовательное учреждение высшего образования
"Российский экономический университет имени Г.В. Плеханова"
МОСКОВСКИЙ ПРИБОРОСТРОИТЕЛЬНЫЙ ТЕХНИКУМ

ПРАКТИЧЕСКАЯ РАБОТА № 9
ДИСЦИПЛИНА: ОПЕРАЦИОННЫЕ СИСТЕМЫ

Тема: Linux: Работа с конфигурационными файлами, настройка системы. Средства администрирования системы.

Специальность: 09.02.03 «Программирование в компьютерных системах»
Квалификация: техник-программист

Цель работы: получить представление о работе с устройствами и планировщике заданий в Unix системах.

Время выполнения работы: 2 академических часа.

Теоретические сведения:

Основные конфигурационные файлы Linux

Операционная система Linux в отличие от Windows не имеет общего реестра для хранения настроек системы, все настройки хранятся в конфигурационных файлах. Большинство этих файлов размещено в папке /etc/.

Настройки большинства системных и сторонних программ находятся в этих файлах, это могут быть настройки графического сервера, менеджера входа, системных служб, веб-сервера, системы инициализации.

Только часть файлов конфигурации находятся в других папках, например, файлы настройки рабочего окружения в домашнем каталоге пользователя. Новичкам очень важно понимать, за что отвечают те или иные конфигурационные файлы, чтобы при необходимости очень быстро сориентироваться. В этой статье мы рассмотрим основные конфигурационные файлы Linux, их расположение и предназначение.

Конфигурационные файлы Linux

На самом деле в самой системы Linux конфигурационных файлов нет. Поскольку операционная система — это всего лишь набор программ и ядро, то все эти файлы были созданы определенными программами и читаются ими же для настройки поведения. Большинство файлов, которые мы привыкли считать стандартными, относятся к системе инициализации или к другим системным утилитам.

Как я уже сказал, большинство файлов размещено в /etc. Название этой папки расшифровывается как «et cetera», что с латинского означает «и другие» или «и так далее». Сначала давайте посмотрим содержимое каталога /etc Linux:

```
ls -l /etc/
```

Здесь достаточно много различных файлов. Дальше мы рассмотрим назначение многих из них. Список отсортирован по алфавиту.

1. /etc/adjtime

Этот конфигурационный файл отвечает за настройку формата системного времени и читается службой systemd-timedated. Время может быть представлено в двух вариантах: LOCAL — время текущего часового пояса и UTC — время по Гринвичу. Вы можете вручную менять значение или воспользоваться утилитой timedatectl.

2. /etc/bash.bashrc

Этот файл принадлежит командной оболочке bash. Это не совсем конфигурационный файл — а скрипт, его содержимое выполняется при запуске каждого экземпляра bash для настройки оболочки. Точно так же выполняется содержимое файла ~/.bashrc для каждого пользователя.

3. /etc/crontab

Crontab — файл настройки планировщика cron. Здесь записываются все задания, которые должен выполнить планировщик, а также время и периодичность. Этот файл не принято редактировать напрямую. Для этого используется утилита crontab -e.

/etc/environment

Здесь содержатся переменные окружения, которые будут загружены для каждого сеанса терминала, независимо от того запущен он на локальной машине или по ssh. Файл читается скриптами Bash во время инициализации оболочки.

5. /etc/fstab

Наверное, все уже знают файл /etc/fstab. Здесь выполняется настройка монтирования файловых систем во время загрузки. В современных системах он читается systemd и все записи на ходу транслируются в юнит-файлы, с помощью которых уже выполняется монтирование. Смотрите также: автоматическое монтирование fstab.

6. /etc/group

В этом файле хранятся все группы пользователей, которые есть в системе. С помощью него вы можете посмотреть список групп, их идентификаторы или добавить новые. Но добавлять группы с помощью редактирования файла не принято, для этого есть утилита usermod.

7. /etc/hostname

В этом файле содержится имя хоста, файл будет прочитан во время загрузки системы и указанное имя компьютера установится в системе. Вы будете его видеть в приглашении ввода терминала или в информации о системе

8. /etc/hosts

Файл /etc/hosts позволяет задавать псевдонимы для различных сетевых узлов. Таким образом, компьютер не обращается к DNS для получения IP домена, а берет его из hosts. Это позволяет, например, заблокировать доступ к нежелательным сайтам просто перенаправив их на localhost или же получить доступ к сайту по ip, которому еще не присвоен домен.

9. /etc/hosts.allow и /etc/hosts.deny

С помощью этих двоих файлов можно настраивать права доступа ко всем локальным службам. Например, вы можете разрешить доступ к службе apache только с локального компьютера. Это очень сильно повысит безопасность системы, если ваш компьютер подключен к публичной сети.

10. /etc/issue и /etc/issue.net

Баннер, который будет выводиться при входе в командную оболочку локально или по SSH. Обычно там выводится версия ядра и дистрибутива Linux, но вы можете заменить эту информацию по своему усмотрению.

11. /etc/ld.so.conf

В этом файле содержатся пути к папкам, в которых компоновщик linux ld.so будет искать динамические библиотеки во время запуска программ. Папки /lib64, /lib, /usr/lib64 и /usr/lib будут проверены автоматически.

12. /etc/localtime

Это символическая ссылка, которая указывает на файл часового пояса в папке /usr/share/zoneinfo/. Редактировать файл не нужно, а для изменения настроек нужно создать символическую ссылку на другую временную зону.

13. /etc/login.defs

Файл /etc/login.defs отвечает за настройку поведения утилиты управления пользователями и параметры входа в систему. Вы можете настроить какой минимальный и максимальный id нужно выдавать, что делать с папкой пользователя при удалении и многое другое, количество попыток входа и таймаут, а также многое другое.

14. /etc/mime.types

В этом файле содержатся общесистемные правила преобразования расширений файлов в понятные системе MIME типы данных. Затем уже система выбирает, чем открыть тот или иной тип данных.

15. /etc/modprobe.d/

Папка /etc/modprobe содержит конфигурационные файлы со списками модулей ядра, которые не нужно загружать при старте системы, псевдонимами для существующих модулей, а также позволяет задавать настройки для модулей.

16. /etc/modules-load. d/

Папка /etc/modules-load. d/ содержит файлы со списками модулей, которые должны быть загружены при запуске системы. Имя файла не важно, но он должен иметь расширение.conf.

17. /etc/nsswitch.conf

Этот файл задает настройки порядка разрешения имен в системе для всех программ, написанных на Си или C++. Например, нужно сначала просматривать локальную сеть и систему, или сразу же отправлять запрос к DNS.

18. /etc/ntp.conf

Файл ntp.conf отвечает за настройку службы синхронизации времени — ntpd. В файле указаны адреса ntp серверов, с которых служба будет получать время, а также общие настройки.

19. /etc/os-release

Отображает очень подробную информацию об установленном дистрибутиве:

20. /etc/passwd

Файл содержит список всех зарегистрированных в системе пользователей, а также дополнительные настройки для них, например, оболочку, дату смены пароля и дату отключения аккаунта, кроме самого пароля. Напрямую файл лучше не редактировать, а использовать утилиту для управления пользователями adduser или deluser.

21. /etc/profile

Файл /etc/profile, точно так же, как и /etc/environment загружается и выполняется при запуске любой командной оболочки в системе. Но в отличие от environment, это скрипт, а значит, он может задавать не только переменные, но и выполнять различные команды для инициализации оболочки.

22. /etc/resolv.conf

В этом файле содержатся IP адреса DNS серверов, которые будет использовать компьютер. В большинстве дистрибутивов вы можете редактировать файл вручную или же использовать специальные утилиты.

23. /etc/sddm.conf

Это конфигурационный файл Linux для настройки менеджера входа sddm, для других менеджеров входа будут свои файлы настройки. Здесь можно изменить максимальный и минимальный ID пользователя, который может войти в систему, например, чтобы разрешить авторизацию root, изменить тему, добавить вход без пароля и многое другое.

Контрольные вопросы:

1. Что такое MBR.
2. Что такое утилита DD и какую работы мы с помощью неё может выполнить?
3. Что такое fdisk и какую работы с помощью неё мы можем выполнить?
4. Что такое crontab и для чего он может нам пригодиться?

Оформление отчета:

1. Цель работы.
2. Постановка задачи.
3. Подробное описание технологии выполнения каждого пункта задания, подкрепленное изображением.
4. Вывод.

Министерство образования и науки Российской Федерации
федеральное государственное бюджетное образовательное учреждение высшего образования
"Российский экономический университет имени Г.В. Плеханова"
МОСКОВСКИЙ ПРИБОРОСТРОИТЕЛЬНЫЙ ТЕХНИКУМ

ПРАКТИЧЕСКАЯ РАБОТА № 10
ДИСЦИПЛИНА: ОПЕРАЦИОННЫЕ СИСТЕМЫ

Тема: Работа с файлами и каталогами в Linux. Файловые менеджер Midnight Commander. Bash. Gparted.

Специальность: 09.02.03 «Программирование в компьютерных системах»
Квалификация: техник-программист

Цель работы: приобрести практические навыки работы с файлами и директориями в ОС
Время выполнения работы: 2 академических часа.
Оборудование:
Аппаратная часть: персональный компьютер с правами администратора.
Программная часть: программаVirtualBox, виртуальная машина с установленной ОС Linux Ubuntu, текстовый процессор Microsoft Word.
Теоретические сведения:

сновные операции над файлами и каталогами и их формат при использовании в командном интерпретаторе ОС Linux:

ls – список файлов и каталогов

ls -al – форматированный список со скрытыми каталогами и файлами

file file1 – вывести информацию о типе file1

cd dir1 – сменить текущую директорию на dir1

cd – сменить текущую директорию на домашний каталог

pwd – показать текущий каталог

mkdir dir1 – создать каталог dir1

rm file1 – удалить file1

rm -r dir1 / rmdir dir1 – удалить каталог dir1

cp file1 file2 – скопировать file1 в file2

cp -r dir1 dir2 – скопировать dir1 со всем его содержимым в dir2; команда создаст каталог dir2, если он не существует

mv file1 file2 – переименовать file1 в file2

mv file1 dir1 – переместить file1 в каталог dir1

ln -s file1 ссылка – создать символическую ссылку (ярлык) к file1

chmod список_прав_доступа file1 – изменить права доступа к file1

find dir1 dir2 dir3 критерий_поиска – искать нужный файл в указанных директориях

touch file1 – создать file1

cat file1 – создать file1; вывести на экран содержимое file1 полностью

cat file1 > file2 – перенаправить вывод file1 в file2 (создать копию file1)

cat file1 file2 file3 file 4 > file5 – произвести конкатенацию файлов file1, file2, file3, file4 и сохранить результат в file5

more file1 / less file1 – вывести содержимое file1 поэкранно

head file1 – вывести первые 10 строк file1

tail file1 – вывести последние 10 строк file1

tail -f file1 – вывести содержимое file1 по мере роста, начинает с последних 10 строк

lpr file1 – вывести содержимое file1 на печать

Задание 1. Создайте дерево заданной структуры.

Порядок работы:

1. Создайте каталог ПОРТФЕЛЬ: mkdir ПОРТФЕЛЬ
2. Просмотрите оглавление корневого каталога: ls

Будет показан список видимых элементов каталога в строке. Для получения более полной информации о файлах нужно выполнить следующую команду: ls –al

3. Создайте каталог КОМНАТА: mkdir КОМНАТА
4. Откройте каталог КОМНАТА: cd КОМНАТА
5. Просмотрите оглавление каталога КОМНАТА: ls

Так как каталог пуст, данная команда не даст никакого результата.

6. Создайте файл БАМБУК.txt: touch БАМБУК.txt
7. Введите текст в созданный файл БАМБУК.txt: echo Бамбук – растение из семейства мятликовые, или злаки, больше известен как растение, дающее строительные материалы, но некоторые его виды ценятся как овощные растения. > БАМБУК.txt
8. Просмотрите содержимое созданного файла: cat БАМБУК.txt
9. Просмотрите оглавление каталога КОМНАТА.
10. Создайте каталог ПОЛКА.
11. Просмотрите оглавление каталога КОМНАТА (с получением полной информации о файлах).
12. Откройте каталог ПОЛКА.
13. Просмотрите оглавление каталога ПОЛКА. Сделайте вывод о результате выполнения этой команды.
14. Создайте файл ЛОТОС.txt (аналогично предыдущему файлу).
15. Введите текст в созданный файл ЛОТОС.txt: Лотос – растение из семейства кувшинковые. Водное растение, у которого используют в пищу корневища и плоды, орешки.
16. Просмотрите содержимое созданного файла.
17. Просмотрите оглавление каталога ПОЛКА.
18. Создайте файл ЯМС.txt.
19. Введите текст в созданный файл ЯМС.txt: Ямс – растение из семейства диоскорейные, клубненосное тропическое растение. Его высокопитательные крахмалистые клубни достигают размера до 1 м и массы до 50 кг.
20. Просмотрите содержимое созданного файла.
21. Просмотрите оглавление каталога ПОЛКА.
Создание структуры завершено!
Задание 2. Скопируйте файл БАМБУК.txtв каталог ПОЛКА с темже именем.
Порядок работы:
1. Закройте каталог ПОЛКА и перейдите в родительский для него каталог КОМНАТА: cd ..
2. Скопируйте файл БАМБУК.txt: cp БАМБУК.txt ПОЛКА
3. Перейдите в каталог ПОЛКА.
4. Просмотрите результаты копирования – оглавление каталога ПОЛКА.
Задание 3.Скопируйте файл ЯМС.txtв каталог КОМНАТА сименем YAMS.txt.
Порядок работы:
1. Скопируйте файл ЯМС.txt в каталог КОМНАТА.
2. Перейдите в каталог КОМНАТА.
3. Просмотрите результаты копирования.
4. Переименуйте файл ЯМС.txt: mv ЯМС.txt YAMS.txt
5. Просмотрите результаты переименования – оглавление каталога КОМНАТА.
Задание 4. Переместите файл БАМБУК.txtв каталог ПОРТФЕЛЬ стем же именем.
Порядок работы:
1. Переместите файл БАМБУК.txt: mv БАМБУК.txt ../ПОРТФЕЛЬ/
При перемещении файлов символ «/» в конце строки обязателен!
2. Просмотрите результаты перемещения.
3. Перейдите в каталог ПОРТФЕЛЬ.
4. Просмотрите оглавление каталога ПОРТФЕЛЬ.
Задание 5. Переместите файлYAMS.txtиз каталога КОМНАТА вкаталог ПОЛКА с именем DIOSCOREA.txt.
Порядок работы:
1. Перейдите в каталог ПОЛКА.
2. Просмотрите оглавление каталога ПОЛКА.

3. Переместите файл YAMS.txt: mv ../YAMS.txt DIOSCOREA.txt

4. Просмотрите каталог ПОЛКА.

5. Перейдите в каталог КОМНАТА.

6. Просмотрите каталог КОМНАТА.

Задание 6. Соедините файлы БАМБУК.txt, ЛОТОС.txt, ЯМС.txt в каталоге ПОЛКА. Результат поместите в каталог ПОРТФЕЛЬ с именем ОВОЩИ.txt.

Порядок работы:

1. Перейдите в каталог ПОЛКА.

2. Соедините указанные в задании файлы: cat БАМБУК.txt ЛОТОС.txt ЯМС.txt >../../ПОРТФЕЛЬ/ОВОЩИ.txt

3. Просмотрите результаты слияния:

- проверьте наличие результирующего файла в нужном каталоге;
- просмотрите содержимое результирующего файла.

Задание 7. Скопируйте все файлы из каталога ПОЛКА в каталог ПОРТФЕЛЬ.

Порядок работы:

1. Перейдите в каталог ПОЛКА.

2. Скопируйте все файлы в каталог ПОРТФЕЛЬ: cp БАМБУК.txt ЛОТОС.txt ЯМС.txt DIOSCOREA.txt ../../ПОРТФЕЛЬ/

3. Перейдите в каталог ПОРТФЕЛЬ.

4. Просмотрите оглавление каталога.

5. Перейдите в корневой каталог: cd ..

6. Отобразите всю созданную структуру: ls -R.

Задание 8. Удалите полученную структуру.

Порядок работы:

1. Удалите содержимое каталога ПОРТФЕЛЬ: rm БАМБУК.txt ЛОТОС.txt ЯМС.txt DIOSCOREA.txt

Для упрощения данной команды можно воспользоваться шаблоном для объединения всех текстовых файлов: rm *.txt

2. Просмотрите результат удаления.

Сделайте вывод о результате выполнения этой команды.

3. Перейдите в корневой каталог.

4. Удалите каталог ПОРТФЕЛЬ.

5. Просмотрите результат удаления.

6. Перейдите в каталог КОМНАТА.

7. Перейдите в каталог ПОЛКА.

8. Удалите содержимое каталога ПОЛКА.

9. Просмотрите результат удаления.

10. Удалите каталог ПОЛКА.

После удаления каталога ПОЛКА вы окажетесь в каталоге КОМНАТА.

11. Удалите каталог КОМНАТА.

12. Просмотрите результат удаления.

Задание 9. Письменно (в отчете по данной практической работе) ответить на контрольные вопросы.

Задание 10. Зафиксировать в конспекте по дисциплине «Операционные системы» форматы команд работы с файлами и директориями в ОС Linux,

Контрольные вопросы:

1. Назовите основные команды работы с директориями в ОС Linux.
2. Назовите основные команды работы с файлами в ОС Linux.
3. Перечислите команды вывода на экран содержимого файла с указанием их особенностей.

Оформление отчета:

1. Цель работы.

2. Постановка задачи.
3. Подробное описание технологии выполнения каждого пункта задания, подкрепленное изображением.
4. Вывод.

Министерство образования и науки Российской Федерации
федеральное государственное бюджетное образовательное учреждение высшего образования
"Российский экономический университет имени Г.В. Плеханова"
МОСКОВСКИЙ ПРИБОРОСТРОИТЕЛЬНЫЙ ТЕХНИКУМ

ПРАКТИЧЕСКАЯ РАБОТА № 11
ДИСЦИПЛИНА: ОПЕРАЦИОННЫЕ СИСТЕМЫ

Тема: Управление пользователями и группами в ОС Unix.

Специальность: 09.02.03 «Программирование в компьютерных системах»
Квалификация: техник-программист

Цель работы: получить практические навыки по работе с учётными записями и группами пользователей

Время выполнения работы: 2 академических часа.

Оборудование: ПК, ОС с установленной системой виртуализации(Virtual Box, VMWare), образ виртуальной машины ОС Linux

Теоретические сведения:

Для создания, изменения и удаления учетных записей все версии ОС UNIX предлагают три команды, **useradd**, **usermod** и **userdel** соответственно. Они в большинстве систем имеют следующий синтаксис:

useradd	[-g **группа**] [-G **группа**[[, **группа**]...]] [-d **каталог**] [-s **shell**] [-c **комментарий**] [-m [-k **skel_dir**]] [-f **inactive**] [-e **expire**] **рег_имя**
usermod	[-g группа] [-G группа[[, группа]...]] [-d каталог [-m]] [-s shell] [-c комментарий] [-l новое_рег_имя] [-f inactive] [-e expire] рег_имя
userdel	[-r] рег_имя

Эти команды позволяют выполнить только согласованные и допустимые изменения в файлах **/etc/passwd**, **/etc/shadow** и **/etc/group**. Команды управления учетными записями, в общем случае, может выполнять только пользователь **root**. Основные опции команд управления учетными записями представлены в табл

Основные опции команд управления учетными записями	
Опция	Назначение
-g группа	Целочисленный идентификатор или символьное имя существующей группы. Эта опция задает *основную группу* (primary group) для нового пользователя. В ОС FreeBSD и Linux обычно принято по умолчанию создавать для каждого пользователя отдельную приватную основную группу, имя которой совпадает с именем пользователя.
-G группа[[,группа]...]	Один или несколько элементов в списке через запятую, каждый из которых представляет собой целочисленный идентификатор или символьное имя существующей группы. Этот список определяет принадлежность к *дополнительным группам* (supplementary group membership) для пользователя. Повторения игнорируются.
-d каталог	*Начальный каталог* (home directory) нового пользователя. По умолчанию используется /home/рег_имя, где /home – базовый каталог для начальных каталогов новых пользователей, а рег_имя – регистрационное имя нового пользователя.
-s shell	Полный путь к программе, используемой в качестве начального командного интерпретатора для пользователя сразу после регистрации. В Linux по умолчанию в этом поле используется стандартный командный интерпретатор /bin/bash.
-c комментарий	Любая текстовая строка. Обычно, это краткое описание регистрационного имени, например, фамилия и имя реального пользователя. Эта информация хранится в записи пользователя в файле /etc/passwd. Длина этого поля не должна превосходить 128 символов.
-m	Создает начальный каталог нового пользователя, если он еще не существует. Если каталог уже существует, добавляемый пользователь должен иметь права на доступ к указанному каталогу.

-k skel_dir	Копирует содержимое *скелетного каталога* skel_dir в начальный каталог нового пользователя, вместо содержимого стандартного скелетного каталога, /etc/skel. Каталог skel_dir должен существовать. Стандартный скелетный каталог содержит стандартные файлы, определяющие среду работы пользователя. Заданный администратором каталог skel_dir может содержать аналогичные файлы и каталоги, созданные для определенной цели.
-f inactive	Максимально допустимое количество дней между регистрациями, когда это имя еще не объявляется недействительным. Обычно в качестве значений используются положительные целые числа.
-e expire	Дата, начиная с которой регистрационное имя больше нельзя будет использовать; после этой даты никакой пользователь не сможет получить доступ под этим регистрационным именем. (Эта опция удобна при создании временных регистрационных имен.) Вводить значение аргумента expire (представляющего собой дату) можно в любом поддерживаемомформате (кроме Julian date). Например, можно ввести 10/6/99 или October 6, 1999.
-l новое_рег_имя	Строка печатных символов, задающая новое регистрационное имя для пользователя. Она не должна содержать двоеточий (:) и переводов строк (\n). Кроме того, она не должна начинаться с прописной буквы.
-r	При удалении учетной записи удалить начальный каталог пользователя из системы. Этот каталог должен существовать. После успешного выполнения команды файлы и подкаталоги в начальном каталоге будут недоступны.
рег_имя	Строка печатных символов, задающая регистрационное имя для нового пользователя. В ней не должно быть двоеточий (:) и символов перевода строки (\n). Она также не должна начинаться с прописной буквы.

Следует помнить, что вновь созданная учетная запись блокируется до тех пор, пока не будет выполнена команда passwd рег_имя, задающая пароль новому пользователю. В дальнейшем пользователь может изменить свой пароль с помощью команды passwd. Привилегированные пользователи могут запускать passwd для выполнения этих функций для любого пользователя, а также для установки атрибутов пароля для любого пользователя.

Для создания, изменения и удаления групп все версии ОС UNIX предлагают три команды, groupadd, groupmod и groupdel, соответственно. Они имеют следующий синтаксис:

- groupadd группа
- groupmod [-n новое имя] группа
- groupdel группа

Полную информацию по синтаксису команд можно получить из справки, вызываемой командой manимя_команды, напримерmanuseradd (выход из справки – q);

- Задание 1 создать следующих пользователей (пароль у всех 123):
- student с созданием одноименной группы (группа создается по умолчанию);
- ivanov с назначением первичной группы student;
- petrov (одноименная группа создается по умолчанию);
- по фамилии студента (латинскими буквами), например, salimova;

- создать группу st1 и назначить ее в качестве первичной группы пользователю stud1;
- Задание 2 запустить файловый менеджер Midnight Commander (с помощью команды mc).
- Проанализировать записи о созданных пользователях и группах в файлах:
- /etc/passwd– пользователи,
- /etc/group– группы,
- /etc/shadow– зашифрованные пароли.
- Представить преподавателю записи созданных учетных записей.

Задание 3 при помощи команды userdel удалить учетную запись пользователя petrov вместе с его домашним каталогом и проверить результат удаления учетной записи пользователя, его группы и домашнего каталога.

Контрольные вопросы:

1. Как кодируются в атрибутах файла и каталога права доступа? Какие форматы записи прав бывают?
2. Кто может изменять права доступа к файлам?
3. Какие команды для изменения символьных кодов прав доступа Вы знаете? Перечислите и расскажите о назначении каждой из команд.
4. Что означает право на выполнение, применительно к каталогу?
5. Какими правами надо обладать, чтобы удалить файл или каталог?

Оформление отчета:

1. Цель работы.
2. Постановка задачи.
3. Подробное описание технологии выполнения каждого пункта задания, подкрепленное изображением.
4. Вывод.

Министерство образования и науки Российской Федерации
федеральное государственное бюджетное образовательное учреждение высшего образования
"Российский экономический университет имени Г.В. Плеханова"
МОСКОВСКИЙ ПРИБОРОСТРОИТЕЛЬНЫЙ ТЕХНИКУМ

ПРАКТИЧЕСКАЯ РАБОТА № 12
ДИСЦИПЛИНА: ОПЕРАЦИОННЫЕ СИСТЕМЫ

Тема: Управление процессами ОС Linux.

Специальность: 09.02.03 «Программирование в компьютерных системах»
Квалификация: техник-программист

Цель работы: ознакомится с основными принципами работы с процессами и демонами в ОС Linux
Время выполнения работы: 2 академических часа.
Оборудование: ПК, ОС с установленной системой виртуализации (Virtual Box, VMWare), образ виртуальной машины ОС Linux
Теоретические сведения:
Понятие процесса

В самом первом приближении можно считать, что процесс — это программа, выполняющаяся в оперативной памяти компьютера. Но такая формулировка как бы подразумевает, что речь идет только о наборе машинных инструкций, последовательно выполняемых процессором. Фактически же в многозадачных системах понятие процесса является значительно более сложным.

В любой многозадачной системе одновременно может быть запущено много программ, то есть много процессов. Впрочем, слово "одновременно" здесь применено не совсем корректно, поскольку на самом деле в каждый момент времени выполняется только один процесс. Ядро (точнее, особый процесс ядра – планировщик) выделяет каждому процессу небольшой квант времени и по истечении этого кванта передает управление следующему процессу. Кванты времени, выделяемые каждому процессу, так малы, что у пользователя создается иллюзия одновременного выполнения многих процессов. Но, чтобы организовать переключение между процессами по истечении кванта времени, приходится делать как бы «мгновенный снимок» состояния программы и сохранять этот снимок где-то в памяти. Этот «снимок» содержит информацию о состоянии регистров центрального процессора на момент прерывания программы, указание на то, с какой команды возобновить исполнение программы (состояние счетчика команд), содержимое стека и тому подобные данные. Когда процесс снова получает в свое распоряжение ЦП, состояние регистров ЦП и стека восстанавливается из сделанного «снимка» и выполнение программы возобновляется в точности с того места, где она была остановлена. Примерно такие же действия выполняются в тех случаях, когда какому-то процессу необходимо вызвать некоторую системную функцию (вызов ядра).

Для хранения всех данных, которые необходимо запоминать в целях организации работы процессов, в памяти, выделенной для ядра, создается для каждого процесса особая структура данных типа task_struct (структура задачи). В ней можно выделить следующие функциональные группы данных:

- - идентификационная информация о процессе;
- - статус процесса;
- - информация для планировщика;
- - информация для организации межпроцессорного взаимодействия;
- - ссылки и связи процесса;
- - информация о времени исполнения и таймеры;
- - информация об используемых процессом ресурсах файловой системы;
- - информация о выделенном процессу адресном пространстве;
- - контекст процесса – информация о состоянии регистров процессора, стеке и т.д.
- Среди всех процессов можно выделить несколько особых типов процессов.

Системные процессы являются частью ядра и всегда находятся в оперативной памяти. Такие процессы не имеют соответствующих им программ в виде исполняемых файлов и запускаются особым образом при инициализации ядра системы. Примерами системных процессов являются планировщик процессов, диспетчер свопинга, диспетчер буферного кэша, диспетчер памяти ядра. Такие процессы являются фактически потоками ядра.

Демоны отличаются от обычных процессов только тем, что они работают в неинтерактивном режиме. Если с обычным процессом всегда ассоциирован какой-то терминал или псевдотерминал, через который осуществляется взаимодействие процесса с пользователем, то демон такого терминала не имеет. Демоны обычно используются для выполнения сервисных функций, обслуживания запросов от других процессов, причем не обязательно выполняющихся на данном компьютере. Пользователь не может непосредственно управлять демонами, он может влиять на их работу, только посылая им какие-то задания, например, отправляя документ на печать.

Одним из главных, если можно так выразиться, демонов в системе является демон init. Как уже говорилось, init является прародителем всех процессов в системе и имеет идентификатор 1. Выполнив задачи, поставленные в ему в файле inittab, демон init не завершает свою работу – он постоянно находится в памяти и отслеживает выполнение других процессов.

Прикладные процессы – это все остальные процессы, выполняющиеся в системе. Как правило, эти процессы порождаются в рамках сеанса работы пользователя. В каждом таком сеансе работы вначале запускается оболочка (командный интерпретатор) shell. Этот экземпляр оболочки называется login shell и завершение соответствующего процесса приводит к отключению пользователя от системы.

Основные команды для работ с процессами.

Все запущенные процессы имеют уникальные номера - PID.

```
# ps axjf
# Показать все загруженные процессы;
# pgrep -l sshd
# Показать PID определенного процесса – sshd;
# echo $$
# Показать PID вашей оболочки;
# fuser -va 22/tcp
# Показать PID процесса использующий порт 22;
# fuser -va /home
# Показывает PID процесса имеющего доступ к /home;
# lsof /home
# Показывает список процессы, которые используют /home;
# killall 0 httpd
# Выводит на экран текущее состояние процесса httpd;
# kil 4712
# «Убить» процесс с PID 4712;
# [sudo] killall TERM 4712
# Посылает процессу с PID`ом 4712 сигнал TERM - завершить процесс;
# [sudo] killall HUP httpd
# Посылает процессу с именем httpd сигнал HUP - остановить процесс;
# [sudo] fuser -k -TERM -m /home
# “Убить” все процессы имеющие доступ к /home;
```

Задание для выполнения практической работы:

1. Изучите при помощи man опцию -l команды ls. Просмотрите права каталогов /etc, /bin и домашнего каталога. Просмотрите права файлов, содержащиеся в этих каталогов. Выявите тенденции (файлов с какими правами в каких каталогах больше). Сделайте вывод.
2. Изучите материал, посвящѐнный пользователям и группам пользователей.

Изучите руководство по командам chown и chgrp. Выясните, кто является владельцем и

к какой группе владельцов принадлежат файлы вашего домашнего каталога, каталогов

/etc, /root, /bin и /dev.

3. Определите атрибуты файлов /etc/shadow и /etc/passwd попробуйте вывести на экран содержимое этих файлов. Объясните результат.

Контрольные вопросы:

1. Что такое «demon»?
2. Что такое прикладные процессы?
3. Рассказать про demon init?
4. Какие команды для работы с процессами были использованны в работе?

Оформление отчета:

1. Цель работы.
2. Постановка задачи.
3. Подробное описание технологии выполнения каждого пункта задания, подкрепленное изображением.
4. Вывод.

Министерство образования и науки Российской Федерации
федеральное государственное бюджетное образовательное учреждение высшего образования
"Российский экономический университет имени Г.В. Плеханова"
МОСКОВСКИЙ ПРИБОРОСТРОИТЕЛЬНЫЙ ТЕХНИКУМ

ПРАКТИЧЕСКАЯ РАБОТА № 13
ДИСЦИПЛИНА: ОПЕРАЦИОННЫЕ СИСТЕМЫ

Тема: Создание пользовательских скирптов ОС Unix.

Специальность: 09.02.03 «Программирование в компьютерных системах»
Квалификация: техник-программист

Цель работы: Целью работы является изучение методов создания и выполнения командных файлов на языке Shell – интерпретатора

Оборудование: ПК, ОС с установленной системой виртуализации (Virtual Box, VMWare), образ виртуальной машины ОС Linux

Время выполнения работы: 2 академических часа.

Теоретические сведения:

В предыдущих лабораторных работах взаимодействие с командным интерпретатором Shell осуществлялось с помощью командной строки. Однако, Shell является также и языком программирования, который применяется для написания командных файлов (shell - файлов). Командные файлы также называются скриптами и сценариями. Shell - файл содержит одну или несколько выполняемых команд (процедур), а имя файла в этом случае используется как имя команды.

Переменные командного интерпретатора:

Для обозначения переменных Shell используется последовательность букв, цифр и символов подчеркивания; переменные не могут начинаться с цифры. Присваивание значений переменным проводится с использованием знака = , например, PS2 = '<' . Для обращения к значению переменной перед ее именем ставится знак $. Их можно разделить на следующие группы:

- позиционные переменные вида $n, где n - целое число;
- простые переменные, значения которых может задавать пользователь или они могут устанавливаться интерпретатором;
- специальные переменные # ? - ! $ устанавливаются интерпретатором и позволяют получить информацию о числе позиционных переменных, коде завершения последней команды, идентификационном номере текущего и фонового процессов, о текущих флагах интерпретатора Shell.

Простые переменные. Shell присваивает значения переменным:

- z=1000
- x= $z
- echo $x
- 1000

Здесь переменной x присвоено значение z.

Позиционные переменные. Переменные вида $n, где n - целое число, используются для идентификации позиций элементов в командной строке с помощью номеров, начиная с нуля. Например, в командной строке

cat text_1 text_2...text_9

аргументы идентифицируются параметрами $1...$9. Для имени команды всегда используется S0. В данном случае $0 - это cat, $1 - text_1, $2 - text_2 и т.д. Для присваивания значений позиционным переменным используется команда set, например,

set arg_1 arg_2... arg_9

здесь $1 присваивается значение аргумента arg_1, $2 - arg_2 и т.д.

Для доступа к аргументам используется команда echo, например:

echo $1 $2 $9

arg_1 arg_2 arg_9

Для получения информации обо всех аргументах (включая последний) используют метасимвол *. Пример:

echo $*

arg_2 arg_3 ... arg_10 arg_11 arg_12

С помощью позиционных переменных Shell можно сохранить имя команды и ее аргументы. При выполнении команды интерпретатор Shell должен передать ей аргументы, порядок которых может регулироваться также с помощью позиционных переменных.

Специальные переменные. Переменные - ? # $! устанавливаются только Shell. Они позволяют с помощью команды echo получить следующую информацию:

- — текущие флаги интерпретатора (установка флагов может быть изменена командой set);

— число аргументов, которое было сохранено интерпретатором при выполнении какой-либо команды;

? — код возврата последней выполняемой команды;

$ — числовой идентификатор текущего процесса PID;

! — PID последнего фонового процесса.

Арифметические операции

Команда expr (express -- выражать) вычисляет выражение expression и записывает результат в стандартный вывод. Элементы выражения разделяются пробелами; символы, имеющие специальный смысл в командном языке, нужно экранировать. Строки, содержащие специальные символы, заключают в апострофы. Используя команду expr, можно выполнять сложение, вычитание, умножение, деление, взятие остатка, сопоставление символов и т. д.

Пример. Сложение, вычитание:

b=190

a=` expr 200 - $b`

где ` - обратная кавычка (левая верхняя клавиша). Умножение *, деление /, взятие остатка %:

d=` expr $a + 125 "*" 10`

c=` expr $d % 13`

Здесь знак умножения заключается в двойные кавычки, чтобы интерпретатор не воспринимал его как метасимвол. Во второй строке переменной с присваивается значение остатка от деления переменной d на 13.

Сопоставление символов с указанием числа совпадающих символов:

concur=` expr "abcdefgh" : "abcde"`

echo $concur

ответ 5.

Операция сопоставления обозначается двоеточием (:). Результат - переменная concur.

Подсчет числа символов в цепочках символов. Операция выполняется с использованием функции length в команде expr:

chain="The program is written in Assembler"

str=` expr length "$chain"`

Echo $str

ответ 35. Здесь результат подсчета обозначен переменной str.

2.3. Встроенные команды

Встроенные команды являются частью интерпретатора и не требуют для своего выполнения проведения последовательного поиска файла команды и создания новых процессов. Встроенные команды:

cd [dir] - назначение текущего каталога;

exec [cmd [arg...]] <имя файла> - выполнение команды, заданной аргументами cmd и arg, путем вызова соответствующего выполняемого файла.

umask [-o | -s] [nnn] - устанавливает маску создания файла (маску режимов доступа создаваемого файла, равную восьмеричному числу nnn: 3 восьмеричных цифры для пользователя, группы и других). Если аргумент nnn отсутствует, то команда сообщает текущее значение маски. При наличии флага -o маска выводится в восьмеричном виде, при наличии флага -s - в символьном представлении;

set, unset - режим работы интерпретатора, присваивание значений параметрам;

eval [-arg] - вычисление и выполнение команды;

sh <filename.sh> выполнение командного файла filename.sh;

exit [n] - приводит к прекращению выполнения программы, возвращает код возврата, равный нулю, в вызывающую программу;

trap [cmd] [cond] - перехват сигналов прерывания, где: cmd - выполняемая команда; cond=0 или EXIT - в этом случае команда cmd выполняется при завершении интерпретатора; cond=ERR - команда cmd выполняется при обнаружении ошибки; cond - символьное или числовое обозначение сигнала, в этом случае команда cmd выполняется при приходе этого сигнала;

export [name [=word]...] - включение в среду. Команда exportобъявляет, что переменные name будут включаться в среду всех вызываемых впоследствии команд;

wait [n] - ожидание завершения процесса. Команда без аргументов ожидает завершения процессов, запущенных синхронно. Если указан числовой аргумент n, то waitожидает фоновый процесс с номером n;

read name - команда вводит строку со стандартного ввода и присваивает прочитанные слова переменным, заданным аргументами name.

Пример. Пусть имеется shell-файл data, содержащий две команды:

```
echo -n "Please write down your name:"
read name
```

Если вызвать файл на выполнение, введя его имя, то на экране появится сообщение:

Please write down your name:

Программа ожидает ввода с клавиатуры (в данном случае - фамилии пользователя). После ввода фамилии и нажатия клавишиEnter команда выполнится и на следующей строке появится знак - приглашение.

Управление программами

Команды true и false служат для установления требуемого кода завершения процесса: true - успешное завершение, код завершения 0; false - неуспешное завершение, код может иметь несколько значений, с помощью которых определяется причина неуспешного завершения. Коды завершения команд используются для принятия решения о дальнейших действиях в операторах цикла while и until и в условном операторе if. Многие команды LINUX вырабатывают код завершения только для поддержки этих операторов.

Условный оператор if проверяет значение выражения. Если оно равно true, Shell выполняет следующий за if оператор, если false, то следующий оператор пропускается. Формат оператора if:

```
if <условие>
then
list1
else
list2
fi
```

Команда test (проверить) используется с условным оператором ifи операторами циклов. Действия при этом зависят от кода возврата test. Test проводит анализ файлов, числовых значений, цепочек символов. Нулевой код выдается, если при проверке результат положителен, ненулевой код при отрицательном результате проверки.

В случае анализа файлов синтаксис команды следующий:

```
test [ -rwfds] file
```

где

-r — файл существует и его можно прочитать (код завершения 0);

-w — файл существует и в него можно записывать;

-f — файл существует и не является каталогом;

-d — файл существует и является каталогом;

-s — размер файла отличен от нуля.

При анализе числовых значений команда test проверяет, истинно ли данное отношение, например, равны ли A и B . Сравнение выполняется в формате:

-eq A = B

-ne A <> B

test A -ge B эквивалентно A >= B

-le A <= B

-gt A > B

-lt A < B

Отношения слева используются для числовых данных, справа — для символов.

Кроме команды test имеются еще некоторые средства для проверки:

! - операция отрицания инвертирует значение выражения, например, выражение if test true эквивалентно выражению if test ! false;

o - двуместная операция "ИЛИ" (or) дает значение true, если один из операндов имеет значение true;

a - двуместная операция "И" (and) дает значение true, если оба операнда имеют значение true.

2.5. Циклы

Оператор цикла с условием while true и while false. Команда while(пока) формирует циклы, которые выполняются до тех пор, пока команда while определяет значение следующего за ним выражения как true или false.
Формат оператора цикла сусловием while true:

while list1

do

list2

done

Здесь list1 и list2 - списки команд. While проверяет код возврата списка команд, стоящих после while, и если его значение равно 0, то выполняются команды, стоящие между do и done. Оператор цикла с условием while false имеет формат:

until list1

do

list2

done

В отличие от предыдущего случая условием выполнения команд между do и done является ненулевое значение возврата. Программный цикл может быть размещен внутри другого цикла (вложенный цикл). Оператор break прерывает ближайший к нему цикл. Если в программу ввести оператор break с уровнем 2 (break 2), то это обеспечит выход за пределы двух циклов и завершение программы.

Оператор continue передает управление ближайшему в цикле оператору while.

Оператор цикла с перечислением for:

for name in [wordlist]

do

list

done

где name - переменная; wordlist - последовательность слов; list - список команд. Переменная name получает значение первого слова последовательности wordlist, после этого выполняется список команд, стоящий между do и done. Затем name получает значение второго слова wordlist и снова выполняется список list. Выполнение прекращается после того, как кончится список wordlist.

Ветвление по многим направлениям case. Команда caseобеспечивает ветвление по многим направлениям в зависимости от значений аргументов команды. Формат:

case <string> in

s1) <list1>;;

s2) <list2>;;

.

.
.
sn) <listn>;;
*) <list>
esac

Здесь list1, list2 ... listn - список команд. Производится сравнение шаблона string с шаблонами s1, s2 ... sk ... sn. При совпадении выполняется список команд, стоящий между текущим шаблоном sk и соответствующими знаками ;;. Пример:

```
echo -n 'Please, write down your age'
read age
case $age in
test $age -le 20) echo 'you are so young' ;;
test $age -le 40) echo 'you are still young' ;;
test $age -le 70) echo 'you are too young' ;;
*)echo 'Please, write down once more'
esac
```

В конце текста помещена звездочка * на случай неправильного ввода числа.

Задание для выполнения лабораторной работы:

Составьте и выполните shell - программы, включающей следующие действия:

1. Вывод на экран списка параметров командной строки с указанием номера каждого параметра.
2. Присвоение переменным A, B и C значений 10, 100 и 200, вычисление и вывод результатов по формуле D=(A*2 + B/3)*C.
3. Формирование файла со списком файлов в домашнем каталоге, вывод на экран этого списка в алфавитном порядке и общего количества файлов.
4. Переход в другой каталог, формирование файла с листингом каталога и возвращение в исходный каталог.
5. Запрос и ввод имени пользователя, сравнение с текущим логическим именем пользователя и вывод сообщения: верно/неверно.
6. Запрос и ввод имени файла в текущем каталоге и вывод сообщения о типе файла.
7. Циклическое чтение системного времени и очистка экрана в заданный момент.
8. Циклический просмотр списка файлов и выдача сообщения при появлении заданного имени в списке.

Оформление отчета:

1. Цель работы.
2. Постановка задачи.
3. Подробное описание технологии выполнения каждого пункта задания, подкрепленное изображением.
4. Вывод.

Министерство образования и науки Российской Федерации
федеральное государственное бюджетное образовательное учреждение высшего образования
"Российский экономический университет имени Г.В. Плеханова"
МОСКОВСКИЙ ПРИБОРОСТРОИТЕЛЬНЫЙ ТЕХНИКУМ

ПРАКТИЧЕСКАЯ РАБОТА № 14
ДИСЦИПЛИНА: ОПЕРАЦИОННЫЕ СИСТЕМЫ

Тема: Настройка и работа с сетью. Конфигурирование сети ОС Unix.

Специальность: 09.02.03 «Программирование в компьютерных системах»
Квалификация: техник-программист

Цель работы: ознакомится с основными принципами настройки сети в ОС Linux.
Время выполнения работы: 2 академических часа.
Теоретические сведения:
Команды для организации поддержки сети:
ifconfig – выводит текущую сетевую конфигурацию
root@mpt:/home/evg# ifconfig
eth0
Link encap: Ethernet HWaddr 00:0c:29:2d:dd:d2
inet addr:192.168.0.5 Bcast:192.168.0.255 Mask:255.255.255.0
inet6 addr: fe80::20c:29ff:fe2d:ddd2/64 Scope:Link
UP BROADCAST RUNNING MULTICAST MTU:1500 Metric:1
RX packets:286954874 errors:0 dropped:0 overruns:0 frame:0
TX packets:337402395 errors:0 dropped:0 overruns:0 carrier:0
collisions:0 txqueuelen:1000
RX bytes:2260610588 (2.1 GiB) TX bytes:3667765477 (3.4 GiB)
Lo
Link encap:Local Loopback
inet addr:127.0.0.1 Mask:255.0.0.0
inet6 addr: ::1/128 Scope:Host
UP LOOPBACK RUNNING MTU:16436 Metric:1
RX packets:16190055 errors:0 dropped:0 overruns:0 frame:0
TX packets:16190055 errors:0 dropped:0 overruns:0 carrier:0
collisions:0 txqueuelen:0
RX bytes:1649706773 (1.5 GiB) TX bytes:1649706773 (1.5 GiB)
для настройки интерфейса команда ifconfig используется следующим образом
ifconfig eth0 192.168.3.214/24 – eth0 – сетевой интерфейс, 192.168.3.214 – IP адресс компьютера, /24 префикс сети
следующим шагом является настройка маршрутизации
команда Route
для настройки маршрутизации необходимо выполнить следующую команду
route add default gw 192.168.3.1 – где 192.168.3.1 ip адресс маршрутизатора
последним шагом настройки сети является комфигурация файла
/etc/resolv.conf
Приме файла
nameserver 192.168.0.5
Настройка менеджера пакетов APT
Для настройки необходимо выполнить следующее
Добавляем источники в файл /etc/apt/source.list
Например:
deb http://ftp.ru.debian.org/debian/ squeeze main
deb-src http://ftp.ru.debian.org/debian/ squeeze main
deb http://security.debian.org/ squeeze/updates main
deb-src http://security.debian.org/ squeeze/updates main
deb http://ftp.ru.debian.org/debian/ squeeze-updates main
deb-src http://ftp.ru.debian.org/debian/ squeeze-updates main
выполняем команду обновления источников apt-get update

После чего командами apt-get install и apt-get remove можно выполнять управления пакетами

FTP (англ. File Transfer Protocol - протокол передачи файлов) - протокол, предназначенный для передачи файлов в сетях передачи данных. FTP позволяет подключаться к серверам FTP, просматривать содержимое каталогов и загружать файлы с сервера или на сервер; кроме того, возможен режим передачи файлов между серверами.

FTP является одним из старейших прикладных протоколов, появившимся задолго до HTTP, в 1971 году. Он и сегодня широко используется для распространения программного обеспечения и доступа к удалённым хостам.

Протокол FTP относится к протоколам прикладного уровня и для передачи данных использует транспортный протокол TCP. Команды и данные, в отличие от большинства других протоколов, передаются по разным портам. Исходящий порт 20, открываемый на стороне сервера, используется для передачи данных, порт 21 для передачи команд. Порт для приема данных клиентом определяется в диалоге согласования. В случае, если передача файла была прервана по каким-либо причинам, протокол предусматривает средства для докачки файла, что бывает очень удобно при передаче больших файлов.

Vsftpd (Very Secure FTP Daemon или Очень Защищенный FTP Демон) является одним из самых простых в конфигурировании и наиболее часто используемым FTP сервером. Vsftpd обслуживает ftp серверы debian, redhat, ubuntu и прочих крупных компаний. Благодаря предельной простоте настройки, поднятие ftp сервера с помощью vsftpd редко занимает более 5 - 10 минут.

В данной лабораторной работе предполагается показать принцип создания файлового сервера, на который все пользователи смогут складывать файлы, удалять их, создавать директории и т.д.

Установка vsftpd

Установка vsftpd. Перед установкой необходимо проверить, что есть соединение с Internet.

```
work@work:~$ sudo apt-get install vsftpd
Чтение списков пакетов... Готово
Построение дерева зависимостей
Чтение информации о состоянии... Готово
```

Настройка vsftpd

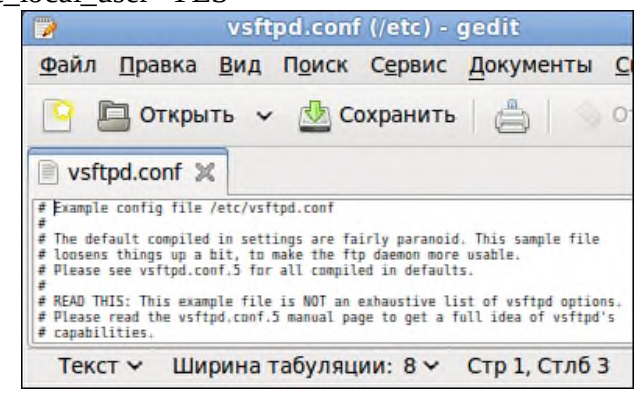
Конфигурирование vsftpd осуществляется редактированием файла /etc /vsftpd.conf. Комментариев (при минимальном знании английского) обычно достаточно, чтобы разобраться что к чему:

- anon_root - директория для анонимных пользователей (/var/ftp/ по умолчанию в большинстве дистрибутивов);
- anonymous_enable - разрешить доступ анонимным пользователям;
- local_enable - разрешить доступ локальным пользователям;
- write_enable - разрешить запись;
- anon_upload_enable - разрешить запись анонимным пользователям

Таким образом, можно отредактировать эти записи в конфиге следующим образом (не стоит удалять остальные опции, если вы не знаете, что они делают):

```
#возможность работы в автономном режиме
listen=YES
#позволяем анонимных пользователей, учетки anonymous и ftp являются синонимами
anonymous_enable=YES
#разрешаем локальных пользователей (локальные пользователи - это те, которые
#зарегестрированы в системе, то есть на них есть учетные записи)
local_enable=YES
#разрешаем любые формы записи на FTP сервер
write_enable=YES
#разрешаем анонимным пользователям upload
anon_upload_enable=YES
#разрешаем анонимным пользователям создавать директории
anon_mkdir_write_enable=YES
#разрешаем анонимным пользователям переименовывать файлы
anon_other_write_enable=YES
```

#у анонимов пароль спрашивать не будем
no_anon_password=YES
#директория для доступа анонимных пользователей (если пользователь присутствует)
anon_root=/home/ftp/
#разрешаем соединение по 20 порту
connect_from_port_20=YES
#поддержка древних FTP клиентов
async_abor_enable=YES
#используем родное время, а не GMT
use_localtime=YES
#небольшое приветствие
ftpd_banner=Hello! We come in peace!
#возможность работы как фоновый процесс
background=YES
# Должны ли пользователи находится только в своих директориях
YES/NO chroot_local_user=YES



Telnet

TELNET (англ. TErminaL NETwork) - сетевой протокол для реализации текстового интерфейса по сети (в современной форме - при помощи транспорта TCP). Название «telnet» имеют также некоторые утилиты, реализующие клиентскую часть протокола. Современный стандарт протокола описан в RFC 854.

Выполняет функции протокола прикладного уровня модели OSI.

Назначение протокола TELNET в предоставлении достаточно общего, двунаправленного, восьмибитного байт-ориентированного средства связи. Его основная задача заключается в том, чтобы позволить терминальным устройствам и терминальным процессам взаимодействовать друг с другом. Предполагается, что этот протокол может быть использован для связи вида терминал-терминал («связывание») или для связи процесс-процесс («распределенные вычисления»).

В протоколе не предусмотрено использование ни шифрования, ни проверки подлинности данных. Поэтому он уязвим для любого вида атак, к которым уязвим его транспорт, то есть протокол TCP. Для функциональности удалённого доступа к системе в настоящее время применяется сетевой протокол SSH (особенно его версия 2), при создании которого упор делался именно на вопросы безопасности. Так что следует иметь в виду, что сессия Telnet весьма беззащитна, если только не осуществляется в полностью контролируемой сети или с применением защиты на сетевом уровне (различные реализации виртуальных частных сетей). По причине ненадёжности от Telnet как средства управления операционными системами давно отказались.

Сетевой протокол ssh

SSH — это специальный сетевой протокол, позволяющий получать удаленный доступ к компьютеру с большой степенью безопасности соединения.

В основном, ssh реализован в виде двух приложений – ssh-сервера и ssh-клиента. В Ubuntu используется свободная реализация клиента и сервера ssh - OpenSSH. При подключении клиент проходит процедуру авторизации у сервера и между ними устанавливается зашифрованное соединение. OpenSSH сервер может работать как с протоколом ssh1, так и с протоколом ssh2. В настоящее время протокол ssh1 считается небезопасным, поэтому его использование крайне не рекомендуется.
Установить OpenSSH можно так:

```
work@work:~$ sudo aptitude install ssh
```

Метапакет ssh содержит в себе и клиент и сервер, при этом скорее всего будет установлен только сервер, т. к. клиент часто бывает установлен в Ubuntu по умолчанию.

SSH сервер автоматически прописывается в автозагрузку при установке. Управлять его запуском/остановкой или перезапуском можно при помощи команд:
sudo service ssh stop|start|restart

Основным файлом конфигурации ssh-сервера является файл /etc/ssh/sshd_config, который должен быть доступным для чтения/редактирования только суперпользователю. После каждого изменения этого файла необходимо перезапустить ssh-сервер для применения изменений.

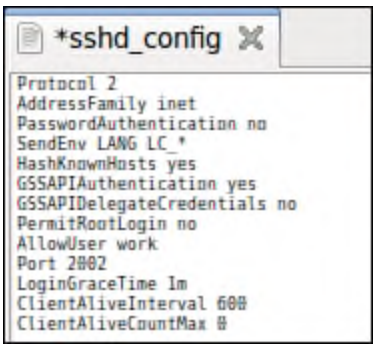
Сам по себе, неправильно настроенный ssh сервер - огромная уязвимость в безопасности системы, т. к. у возможного злоумышленника есть возможность получить практически неограниченный доступ к системе. Помимо этого, у sshd есть много дополнительных полезных опций, которые желательно включить для повышения удобства работы и безопасности.

Для правильной настройки ssh с точки зрения безопасности необходимо отредактировать всего семь параметров:

- PermitRootLogin – отключение возможности авторизации под суперпользователем;
- AllowUsers, AllowGroups - предоставление доступа только указанным пользователям или группам;
- DenyUsers, DenyGroups - блокировка доступа определенным пользователям или группам;
- Port - изменение порта SSHD;
- LoginGraceTime - изменение времени ожидания авторизации;
- ListenAddress - ограничение авторизации по интерфейсу;
- ClientAliveInterval - рассоединение при отсутствии активности в шелле.

Сменить стандартный порт (22) на котором слушает sshd. Это связано с тем, что многочисленные сетевые сканеры постоянно пытаются соединиться с 22-м портом и как минимум получить доступ путем перебора логинов/паролей из своей базы. Даже если у вас и отключена парольная аутентификация - эти попытки сильно засоряют журналы и (в большом количестве) могут негативно повлиять на скорость работы ssh-сервера. Если же вы по какой-либо причине не желаете изменить стандартный порт вы можете использовать как различные внешние утилиты для борьбы брутфорсерами, например fail2ban, так и встроенные, такие как MaxStartups.

По умолчанию root-доступ разрешен. Это означает, что клиент при подключении в качестве пользователя может указать root, и во многих случаях получить контроль над системой. При условии, что по умолчанию в Ubuntu пользователь, добавленный при установке системы имеет возможность решать все административные задачи через sudo, создавать возможность root доступа к системе как минимум странно. Рекомендуется отключить эту опцию совсем.

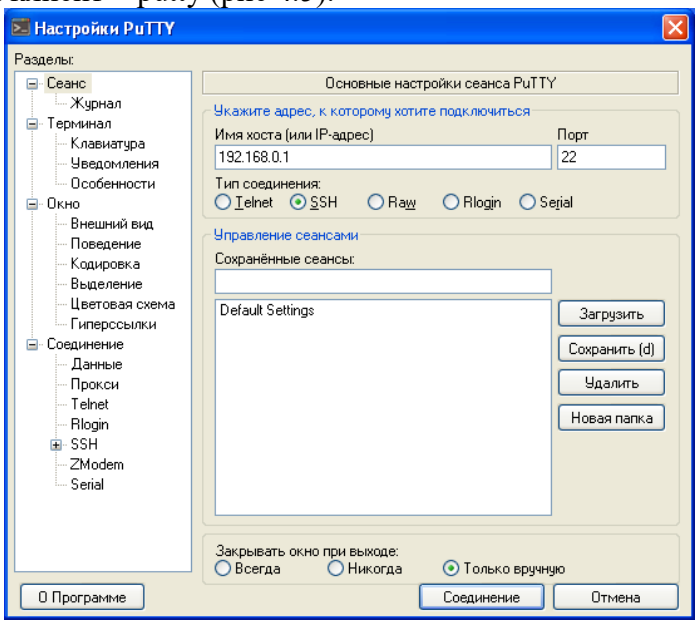


Разрешенная по умолчанию парольная аутентификация является практически самым примитивным способом авторизации в ssh. С одной стороны, это упрощает конфигурацию и подключение новых пользователей (пользователю достаточно знать свой системный логин/пароль), с другой стороны пароль всегда можно подобрать, а пользователи часто пренебрегают созданием сложных и длинных паролей. Специальные боты постоянно сканируют доступные из интернета ssh сервера и пытаются авторизоваться на них путем перебора логинов/паролей из своей базы. Настоятельно не рекомендуется использовать парольную аутентификацию.

Как уже было сказано, ssh может работать с протоколами ssh1 и ssh2. При этом использование небезопасного ssh1 крайне не рекомендуется.

В конечном итоге файл конфигурации

Для удаленного доступа с операционной системы Windows необходимо установить на ней специальный клиент – putty (рис 4.5).



Для настройки сессии введите IP хоста (192.168.0.1). Так же настройте кодировку в пункте Translation, поменяв её на UTF-8.

Веб-сервер

Apache HTTP-сервер – свободный веб-сервер. Apache является кроссплатформенным программным обеспечением, поддерживает операционные системы Linux, BSD, Mac OS, Microsoft Windows, Novell NetWare, BeOS.

Основными достоинствами Apache считаются надёжность и гибкость конфигурации. Он позволяет подключать внешние модули для предоставления данных, использовать СУБД для аутентификации пользователей, модифицировать сообщения об ошибках и т. д. Поддерживает IPv6.

Для установки apache2 введите команду

```
work@work:~$ sudo apt-get install apache2
Чтение списков пакетов... Готово
Построение дерева зависимостей
Чтение информации о состоянии... Готово
```

Файлы конфигурации Apache2 находятся в директории: /etc/apache2:

- conf.d/
- sites-available/
- sites-enabled/
- mods-available/
- mods-enabled/
- apache2.conf
- envvars
- httpd.conf
- ports.conf

В Ubuntu основным файлом настройки Apache2 является apache2.conf. Он играет роль системного файла, в котором собраны основные и самые важные настройки сервера.

Файл httpd.conf - пустой и предназначен для добавления дополнительных настроек, он включен в основной файл настройки apache2.conf

В файле envvars описаны переменные среды, необходимые для функционирования Apache-сервера.

В ports.conf вынесены настройки портов на которые можно будет подключиться к серверу или конкретному сайту на нем.

В папке conf.d находятся дополнительные конфигурационные файлы.

Для описания всех доступных сайтов используется папка sites-available в которой расположены файлы с описанием виртуальных хостов - VirtualHosts, опубликованные же сайты находятся в папке sites-enabled в виде ссылок на файлы доступных сайтов из папки sites-available.

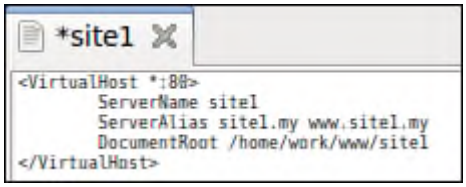
Таким же образом в папках mods-available и mods-enabled настраивается доступность модулей, используемых сервером.

Теперь необходимо подготовить компьютер к работе веб-сервера. Прежде всего необходимо создать единую папку для всех сайтов, которые будут там размещаться, например, /home/user/www. Лучшее место для такой папки — это домашний каталог пользователя. Далее в этой папке необходимо создать папку сайта. Например, /home/user/www/site1. И в эту папку кинуть файлы сайта.

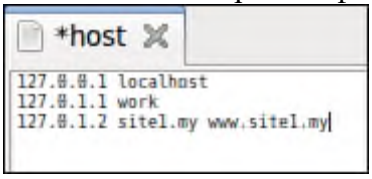
Следующая команда создает запись виртуального хостинга копируя стандартную запись из файла конфигурирования Apache:

```
work@work:~$ sudo cp /etc/apache2/sites-availab
le/default /etc/apache2/sites-available/site1
```

Теперь необходимо отредактировать файл, который находится по директории /etc/apache2/sites-available/site1. Необходимо настроить имя сервера, URL сервера и директорию, по которой находятся файлы сайта. После настроек файл конфигурации должен выглядеть так.



Теперь необходимо как-то научить операционную систему распознавать домен .my. Для этого достаточно прописать необходимые строки в файле /etc/hosts, например, так



Для начала необходимо разместить ссылку на VirtualHost в папку sites-enabled, и перечитать конфигурацию сервера Apache. Для создания ссылки можно выполнить такую команду и перечитать параметры (рис. 4.10). После этого ваш сайт, файлы которого

размещаются в директории /home/user/www/site1 будет отображаться в браузере по адресу: site1.my или www.site1.my.

```
work@work:~$ sudo a2ensite site1
Site site1 already enabled
work@work:~$ sudo /etc/init.d/apache2 reload
 * Reloading web server config apache2
apache2: Could not reliably determine the serve
r's fully qualified domain name, using 127.0.1.
1 for ServerName
                                          [ OK ]
```

- Разрешите анонимный доступ для всех пользователей на данный ftp-сервер. Проверьте работу ftp-сервера с данной конфигурацией с вашей основной операционной системы;
- Настройте разграничение прав доступа к определенным кактологам пользователей на ftp-сервере. Проверьте работу ftp-сервера с данной конфигурацией с вашей основной операционной системы;
- Настройте смешанный режим доступа анонимных и зарегестрированных пользователей. Проверьте работу ftp-сервера с данной конфигурацией с вашей основной операционной системы;
- Установить ssh-сервер на вашу операционную систему Linux. Настройет ssh с точки зрения безопасности;
- На вашей основной операционной системе установить ssh-клиент (если основная операционная система Linux) или pytty (если основная операционная система Windows). Проверьте работу ssh, настроив клиент соответствующим образом;
- Установить веб сервер на Linux Ubuntu;
- Создайте простую html-страничку. Разместите её на веб-сервере по веб-адресам: work.my и www.work.my.

Задание для выполнения лабораторной работы:

- Выполнить настройку сети в Linux
- Подключить дополнительные источники ПО
- Обновить источники
- Установить программы sudo;
- Удалить одну из двух программ
- Оформить отчет
- Разрешите анонимный доступ для всех пользователей на данный ftp-сервер. Проверьте работу ftp-сервера с данной конфигурацией с вашей основной операционной системы;
- Настройте разграничение прав доступа к определенным кактологам пользователей на ftp-сервере. Проверьте работу ftp-сервера с данной конфигурацией с вашей основной операционной системы;
- Настройте смешанный режим доступа анонимных и зарегестрированных пользователей. Проверьте работу ftp-сервера с данной конфигурацией с вашей основной операционной системы;
- Установить ssh-сервер на вашу операционную систему Linux. Настройет ssh с точки зрения безопасности;
- На вашей основной операционной системе установить ssh-клиент (если основная операционная система Linux) или pytty (если основная операционная система Windows). Проверьте работу ssh, настроив клиент соответствующим образом;
- Установить веб сервер на Linux Ubuntu;
- Создайте простую html-страничку. Разместите её на веб-сервере по веб-адресам: work.my и www.work.my.

Контрольные вопросы

- Каково назначение ftp-сервера?
- Каким образом производится настройка vsftpd?
- Каково назначение сетевого протокола SSH?
- Какие основные параметры рекомендуется менять при настройке SSH с точки зрения его безопасности и почему?
- Каково назначение Telnet? Почему Telnet не рекомендуется использовать?
- Каково назначение Apache?
- Какие основные конфигурационные файлы Apache существуют?

Оформление отчета:

1. Цель работы.
2. Постановка задачи.
3. Подробное описание технологии выполнения каждого пункта задания, подкрепленное изображением.
4. Вывод.

Министерство образования и науки Российской Федерации
федеральное государственное бюджетное образовательное учреждение высшего образования
"Российский экономический университет имени Г.В. Плеханова"
МОСКОВСКИЙ ПРИБОРОСТРОИТЕЛЬНЫЙ ТЕХНИКУМ

ПРАКТИЧЕСКАЯ РАБОТА № 15
ДИСЦИПЛИНА: ОПЕРАЦИОННЫЕ СИСТЕМЫ

Тема: Установка и настройка WEB-сервера ОС Unix, ОС Windows.

Специальность: 09.02.03 «Программирование в компьютерных системах»
Квалификация: техник-программист

Цель работы: получить опыт установки и настройки Web-сервера Apache
Оборудование: ПК, ОС с установленной системой виртуализации (Virtual Box, VMWare), образ виртуальной машины ОС Linux
Время выполнения работы: 4 академических часа.
Теоретические сведения:
Установка lamp Ubuntu 16.04

Операционная система Linux — отличная платформа для создания и тестирования веб сайтов. Учитывая, что большинство веб серверов используют Linux в качестве операционной системы, то и тестировать сайты лучше в этой системе, с использованием тех же инструментов, даже если это домашний компьютер. Намного удобнее иметь все под рукой и не боятся повредить сайт на сервере.

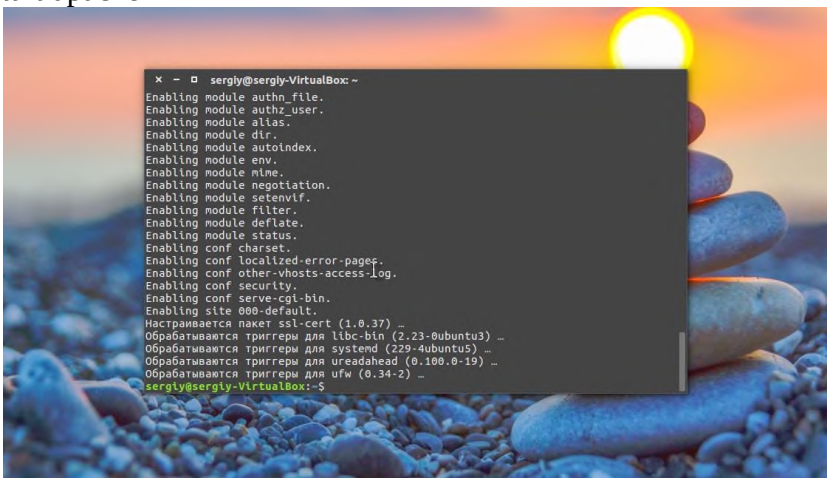
Сегодня мы поговорим о LAMP. На самом деле, это не программа, это стек программ с открытым исходным кодом необходимых для работы веб-сайтов, название лишь формальное и походит оно от первых букв названий входящих туда программ. Linux Apache MySQL PHP, а вместе LAMP, это те программы, которые нужно установить и настроить, для того, чтобы начать разрабатывать сайты или веб-приложения на домашнем компьютере. Linux — тут все понятно, это наша операционная система, Apache — веб сервер, MySQL — программа для управления базами данных и PHP — на данный момент, самый популярный язык для веб-программирования.

В этой инструкции будет рассмотрена установка LAMP ubuntu 16.04 рассмотрим, как установить Apache 2.4, MariaDB в качестве базы данных mysql и самую новую версию языка PHP 7. Для начала будет выполнена установка Apache ubuntu 16.04, так как это главный компонент всей системы, а уже потом подключим к нему дополнительные компоненты.

Установка Apache Ubuntu 16.04

Apache — это кроссплатформенный веб-сервер с открытым исходным кодом. Он поддерживает все необходимые функции веб-сервера, включая CGI, SSL, и виртуальные домены.

Установить Apache в Ubuntu очень просто, для этого достаточно выполнить:
sudo apt-get install apache2
После установки добавим программу в автозагрузку:
sudo systemctl enable apache2
И запустим веб-сервер сейчас:
sudo systemctl start apache2



Теперь можно проверить что получилось, откройте браузер и наберите в адресной строке localhost:

Как видите, установка apache ubuntu 16.04 завершена и веб-сервер уже работает. Но это еще не все. Все отлично, если у вас один сайт, который нужно тестить на локальной машине, но если их несколько собирать все в под папках веб-сервера не совсем удобно, да и не все движки нормально относятся к этому, потому давайте рассмотрим как настроить виртуальные хосты.

Создайте новую папку для нашего виртуального хоста:

sudo mkdir /var/www/test.site

Дадим права на доступ:

sudo chmod -R 755 /var/www

Необходимо создать небольшой файл, index.html, чтобы он открылся когда вы откроете этот сайт:

sudo vi /var/www/test.site/public_html/index.html

<html><head><title>Welcome to Test!</title></head><body><h1>Success! Virtual host is working!</h1></body></html>

Теперь можно добавлять виртуальный хост, для этого создайте файл и наполните его содержимым:

sudo vi /etc/apache2/sites-available/test.site.conf

<VirtualHost *:80>ServerName test.siteServerAlias www.test.siteServerAdmin webmaster@localhostDocumentRoot /var/www/test.site/public_htmlErrorLog ${APACHE_LOG_DIR}/error.logCustomLog ${APACHE_LOG_DIR}/access.log combined</VirtualHost>

Вот что значат некоторые строки:

ServerName — имя нашего сайта, виртуального хоста

ServerAlias — сайт будет доступен также по этому имени

DocumentRoot — корневой каталог с файлами сайта

Теперь сохраните файл, далее нужно активировать наш хост:

sudo a2ensite test.site.conf

Перезапускаем веб сервер:

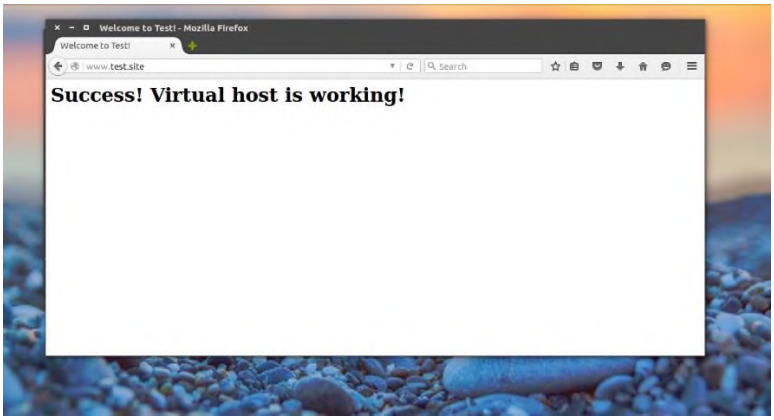
sudo systemctl restart apache2

Теперь необходимо завернуть трафик с этого домена на локальный сервер, для этого добавьте строчку в /etc/hosts:

sudo vi /etc/hosts

127.0.0.1 test.site

Откройте браузер и в адресной строке наберите test.site:



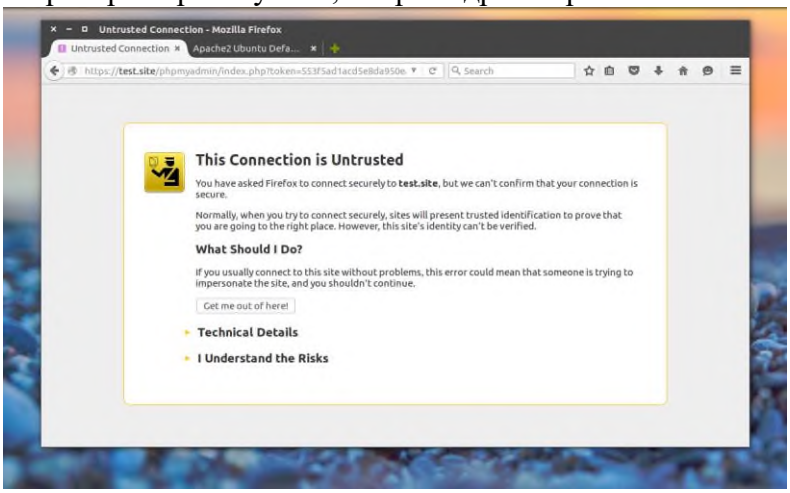
Кроме того, мы можем включить поддержку ssl для нашего веб-сервера. Для этого выполните:

a2enmod ssl$ a2ensite default-ssl

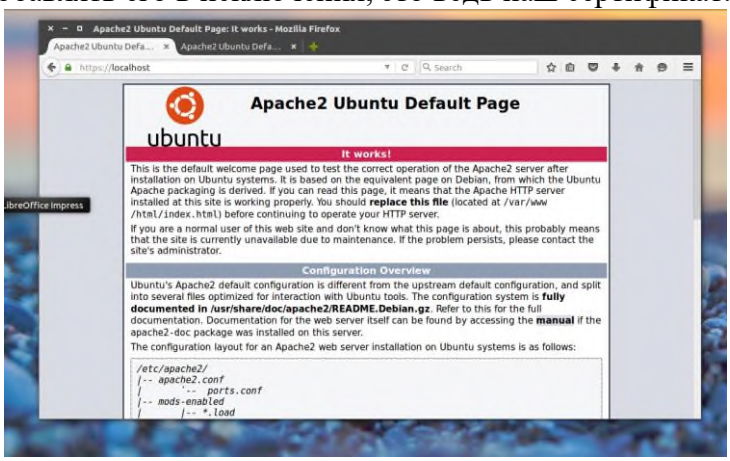
После этого нужно будет перезагрузить веб-сервер:

sudo systemctl restart apache2

Теперь вы можете проверить работу SSL, набрав адрес https://localhost.



Браузер не доверяет нашему сертификату, поскольку он самоподписанный, но мы можем спокойно добавлять его в исключения, это ведь наш сертификат. Теперь работает:



Установка PHP 7

Без языка программирования установка и настройка lamp в Ubuntu будет не завершена. PHP — это самый популярный язык программирования в веб. Его название, это рекурсивный акроним — PHP Hypertext Processor. Кроме того, что этот язык используется в веб, его можно применять, как язык общего назначения, язык сценариев.

Установка php 7 Ubuntu 16.04 выполняется следующей командой:

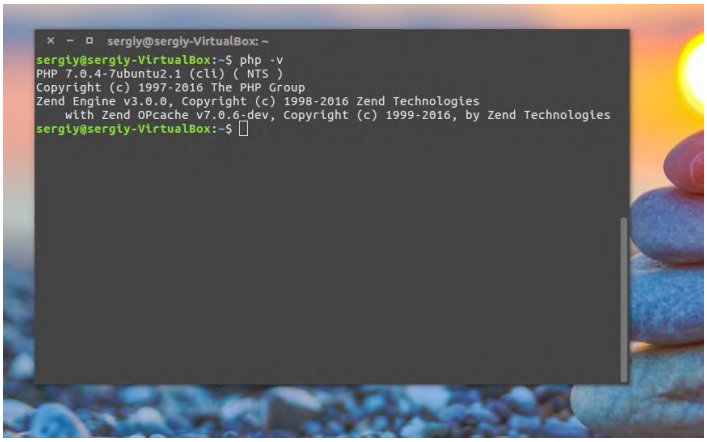
sudo apt-get install php7.0-mysql php7.0-curl php7.0-json php7.0-cgi php7.0 libapache2-mod-php7.0

Если вы хотите установить все доступные модули php, чтобы в будущем не было проблем, вы можете выполнить команду:

sudo apt-get install php*

После завершения установки проверим версию php:

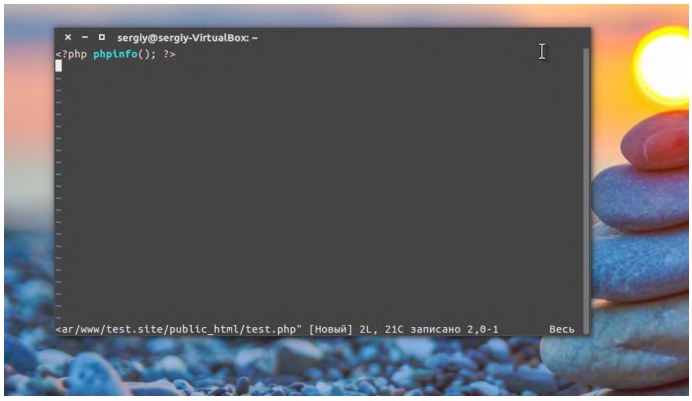
php -v



Теперь пора проверить как все работает. Для этого создайте файл со следующим кодом на php:

sudo vi /var/www/test.site/public_html/test.php

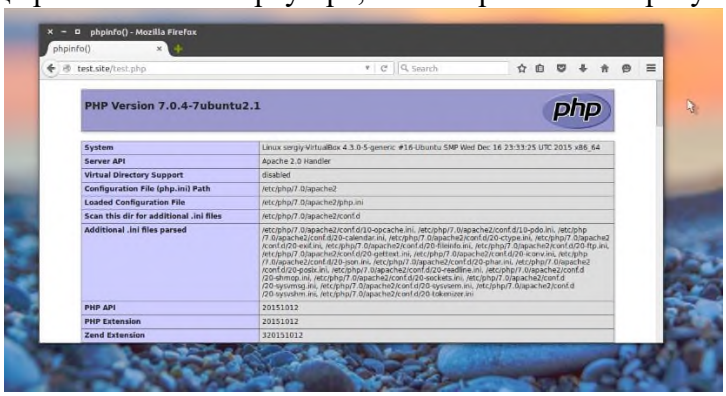
<? php phpinfo(); ?>



Осталось перезапустить apache2:

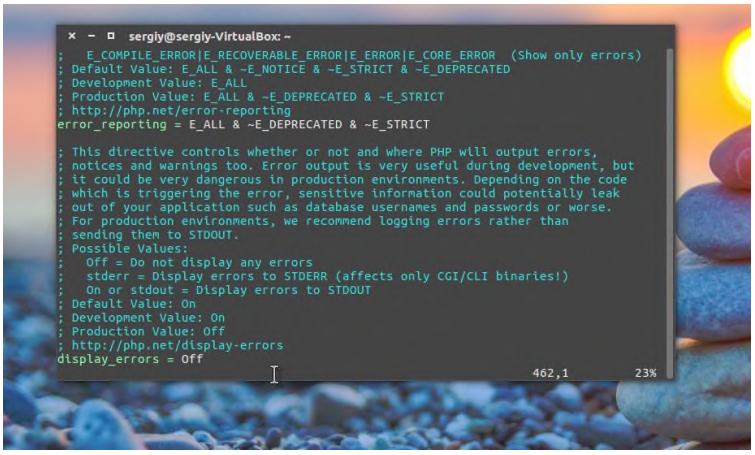
sudo systemctl restart apache2

Откройте еще раз наш сайт в браузере, на этот раз нас интересует страница test.php:



Установка php 7 ubuntu 16.04 завершена и все очень хорошо работает. Но нужно еще кое-что настроить, а именно включить отображение ошибок в php. Иначе при возникновении ошибки вы увидите просто пустую страницу. Для этого откройте файл /etc/php/7.0/apache2/php.ini, найдите строку display_errors = Off и поменяйте off на on:

vi /etc/php/7.0/apache2/php.ini



Теперь переходим к следующему этапу.

Установка MySQL Ubuntu 16.04

Базы данных используются сейчас почти в каждом движке интернет-сайтов. Поэтому важно иметь на своем компьютере и это программное обеспечение. Установка Lamp Ubuntu 16.04 не может обойтись без базы данных, но в этой инструкции вместо Mysql мы будем использовать ее улучшенную и оптимизированную версию — MariaDB. Это очень надежный и масштабируемый сервер SQL со множеством улучшений и усовершенствованием.

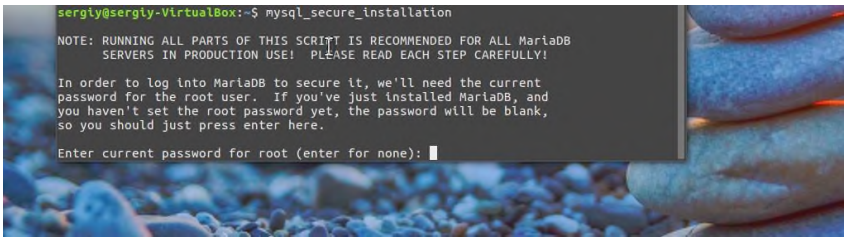
Установка mariadb ubuntu 16.04 выполняется с помощью команды:

sudo apt-get install mariadb-server mariadb-client

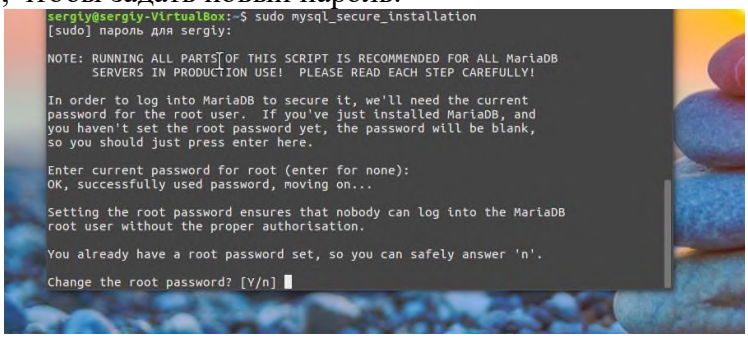
Когда установка mysql ubuntu 16.04 будет завершена, мы можем переходить к настройке базы данных, для этого выполните команду:

sudo mysql_secure_installation

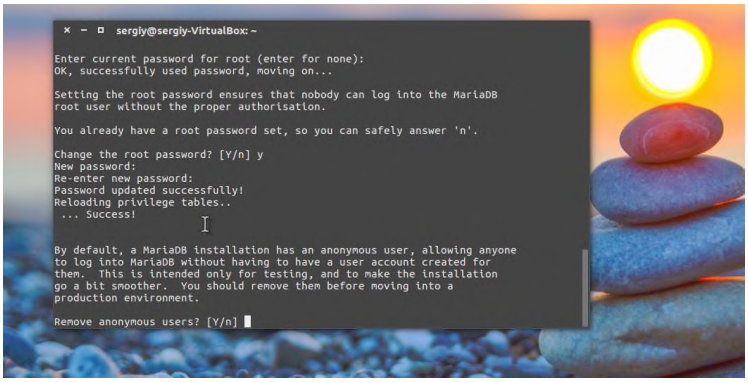
Сначала необходимо ввести текущий пароль root, просто нажимаем Enter, поскольку он еще не задан:



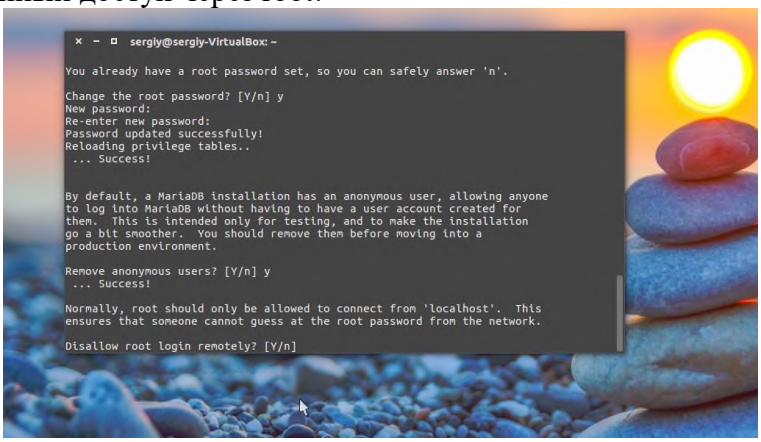
Далее нажимаем y, чтобы задать новый пароль:



Затем отключаем гостевые аккаунты:

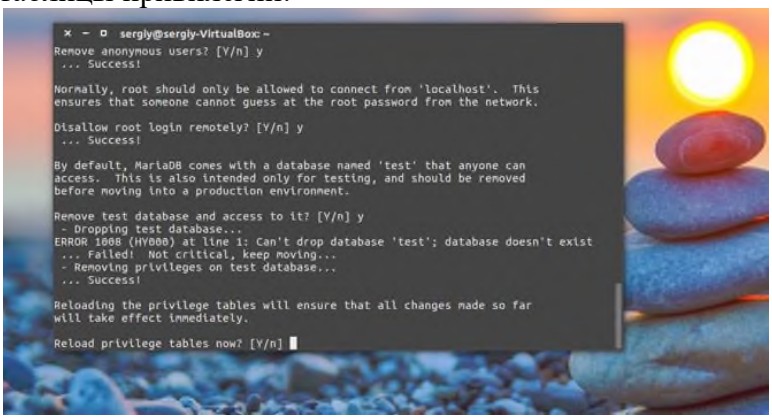


Отключаем удаленный доступ через root:



Удаляем тестовые базы данных:

Перезаписываем таблицы привилегий:



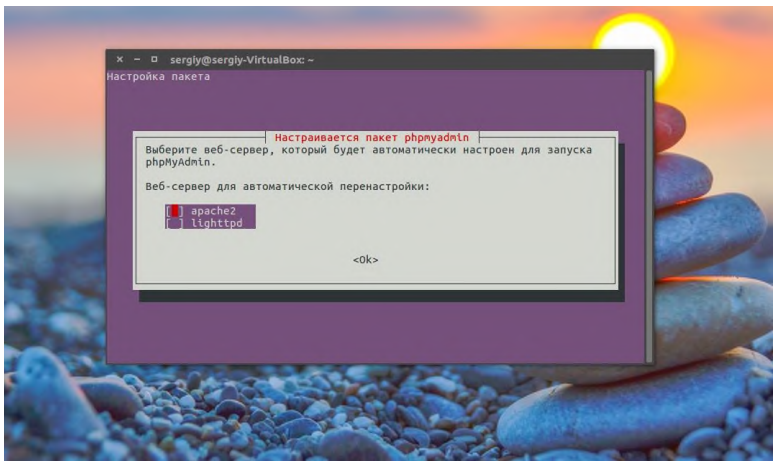
Вот и все, установка mysql ubuntu 16.04 завершена и база данных готова к работе.

Установка phpmyadmin ubuntu 16.04

Установка и настройка lamp в ubuntu 16.04 также будет включать установку Phpmyadmin. Phpmyadmin — это бесплатный инструмент, с открытым исходным кодом, для реализации веб-интерфейса управления базами данных MySQL. Он доступен в официальных репозиториях Ubuntu 16.04, установим его с помощью команды:

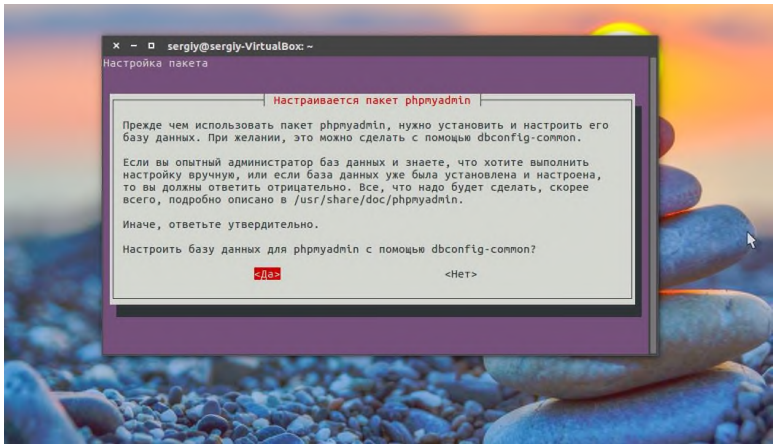
sudo apt-get install phpmyadmin php-mbstring php-gettext

Но тут уже во время установки потребуется немного конфигурации. Сначала нужно выбрать наш веб-сервер:

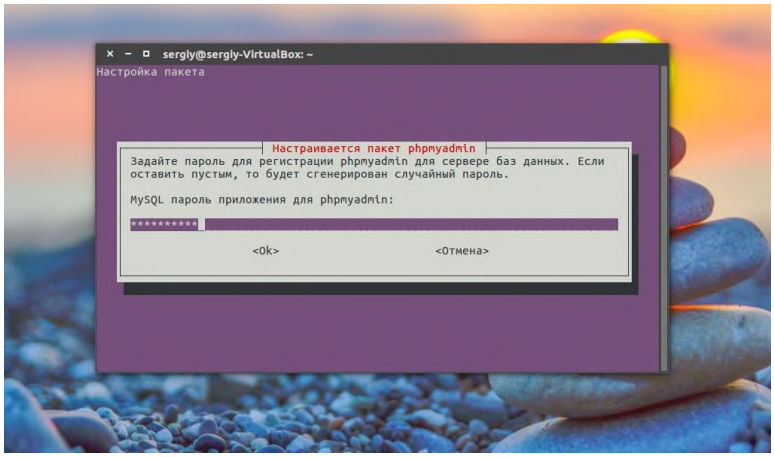


Для перемещения по пунктам используйте стрелки вверх/вниз, для выбора пробел, для переключения — Tab.

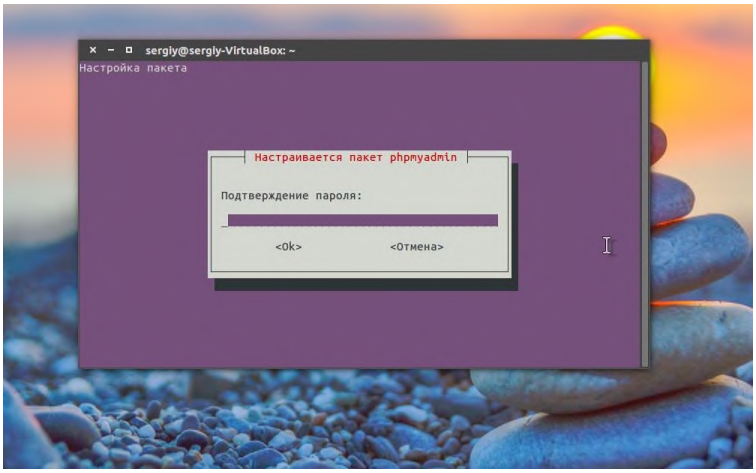
В следующем окне мастера нам предлагают настроить базу данных phpmyadmin, соглашаемся:



Вводим пароль, который будет использован для подключения phpadmin к базе данных:



Подтверждение пароля:

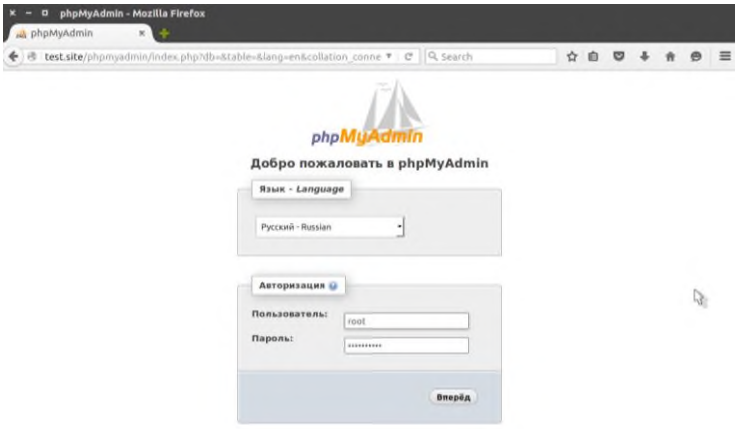


По умолчанию в MariaDB есть плагин под названием unix_socket, он предотвращает вход под именем пользователя root в phpmyadmin или с помощью других TCP интерфейсов. Для его отключения выполните:

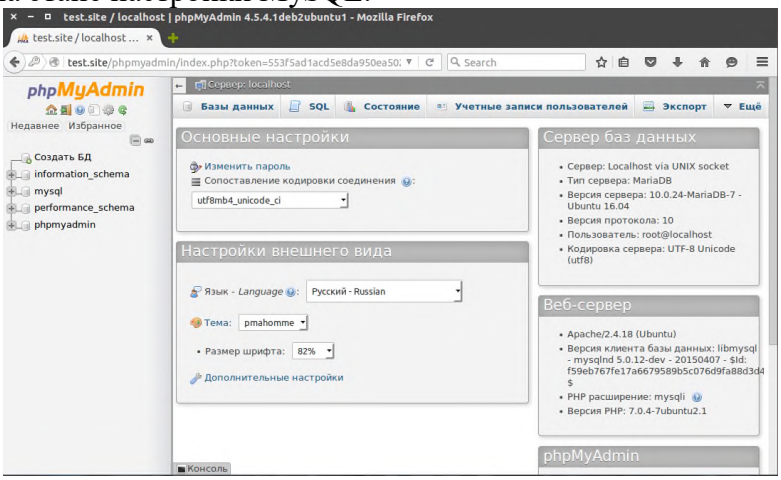
sudo -i

$ echo "update user set plugin='' where User='root'; flush privileges;" | mysql -u root -p mysql

Когда установка phpmyadmin ubuntu 16.04 будет завершена откройте браузер и наберите в адресной строке localhost/phpmyadmin:



Все работает, для доступа к базе данных вы можете ввести логин root и его пароль, который задали на этапе настройки MySQL:



Задание к практической работе:

1. Установить и настроить LAMP
2. Продемонстрировать результат

Контрольные вопросы:

1. Что такое Apache?

2. Что LAMP и какие его варианты бывают?
3. Для каких целей может понадобиться сервер?
4. Какой командой устанавливаются программы под Linux?
5. Что такое PHP?

Оформление отчета:

1. Цель работы.
2. Постановка задачи.
3. Подробное описание технологии выполнения каждого пункта задания, подкрепленное изображением.
4. Вывод.

Министерство образования и науки Российской Федерации
федеральное государственное бюджетное образовательное учреждение высшего образования
"Российский экономический университет имени Г.В. Плеханова"
МОСКОВСКИЙ ПРИБОРОСТРОИТЕЛЬНЫЙ ТЕХНИКУМ

ПРАКТИЧЕСКАЯ РАБОТА № 16
ДИСЦИПЛИНА: ОПЕРАЦИОННЫЕ СИСТЕМЫ

Тема: Резервное копирование и восстановление данных в Windows, Unix.

Специальность: 09.02.03 «Программирование в компьютерных системах»
Квалификация: техник-программист

Цель работы: ознакомится с основными принципами настройки сети в ОС Linux
Оборудование: ПК, ОС с установленной системой виртуализации (Virtual Box, VMWare), образ виртуальной машины ОС Linux
Время выполнения работы: 2 академических часа.
Теоретические сведения:
Архивация и восстановление

Мастер архивации и восстановления (Backup or Restore Wizard) создает копию файлов и папок на указанном пользователем носителе информации. В случае потери или повреждения пользовательских данных их можно восстановить из файла резервной копии. Частота архивации (резервного копирования) зависит от частоты изменений файлов, так как в случае потери данных придется повторно создать то, что было сделано после последней архивации. По этой причине многие компании создают резервные копии важных файлов ежедневно. Пользователь может выбирать различные типы архивации в зависимости от его требований.

- Для типа Обычная (Normal) происходит архивация всех выбранных файлов и системных настроек для определенной папки или диска, и каждый файл маркируется как прошедший архивацию (имеющий резервную копию).
- Для типа Копирование (Copy) происходит архивация всех выбранных файлов и системных настроек для определенной папки или диска, но файлы не маркируются как прошедшие архивацию.
- Для типа Добавочная (Incremental) происходит архивация только тех файлов, которые были созданы или изменены вслед за последней обычной или добавочной архивацией, и каждый файл маркируется как прошедший архивацию.
- Для типа Разностная (Differential) происходит архивация только тех файлов, которые были созданы или изменены вслед за последней обычной или добавочной архивацией, но файлы не маркируются.
- Для типа Ежедневная (Daily) происходит архивация только тех файлов, которые были созданы или изменены в данный день, но файлы не маркируются.

Тип архивации, который применяется, определяет, насколько сложным будет процесс восстановления. Для восстановления после нескольких добавочных или разностных архиваций необходимо выполнить восстановление из последней обычной резервной копии и из всех добавочных или разностных копий, полученных после обычной архивации и вплоть до настоящего момента.

Выполняя архивацию данных, пользователь указываете имя и место для файла резервной копии. По умолчанию файлы резервных копий сохраняются с расширением .bkf. Файлы архивации можно сохранять на жестком диске, на гибком диске или на любом другом типе съемного носителя. При выборе места для резервной копии нужно учитывать размер файла архивации, типы имеющихся носителей, а также возможное требование того, что файлы резервных копий нужно хранить отдельно от компьютера на случай катастрофы.
Функция восстановления системы

Восстановление системы позволяет выполнить откат состояния операционной системы к одной из точек восстановления, фиксирующих состояние на момент, когда система стабильно работала. Преимуществом данной функции заключается в том, что она предоставляет возможность быстрого восстановления ("отката" состояния системы к с остоянию, в котором она находилась в один из предыдущих моментов во времени) без переустановки системы, а также не подвергает риску случайного перезаписывания рабочих файлов пользователей. Возможно выполнение отката к любому из следующих типов контрольных точек и точек восстановления.

- Начальная контрольная точка (initial system checkpoint) системы создается при первом запуске компьютера с вновь установленной ОС.

- Точки восстановления для автоматических обновлений (Automatic update restore points) создаются, когда инсталлируются обновления, которые загружаются с помощьюWindows Update.
- Точки восстановления при восстановлении с резервной копии (Backup recovery restore points) создаются, когда пользователь использует мастер архивации или восстановления (Backup or Restore Wizard).
- Пользователь может создавать свои собственные точки восстановления вручную ("ручные" контрольные точки - manual checkpoints) в любой момент с помощью мастера восстановления системы (System Restore Wizard).
- Точки восстановления при инсталляции программ (Program name installation restore points) создаются, при установке программного обеспечения.
- Точки восстановления для операции восстановления (Restore operation restore points) создаются каждый раз, когда пользователь осуществляете какое-либо восстановление.
- Системные контрольные точки (System checkpoints) - это запланированные точки восстановления, которые создаются компьютером регулярно, даже если пользователь не вносил никаких изменений в систему.
- Точки восстановления для неопознанного устройства (Unsigned device driver restore points) создаются, когда устанавливается драйвер устройства, который не был опознан или сертифицирован.

Средство Восстановление системы (System Restore) обычно сохраняет набор контрольных точек восстановления за период от одной до трех недель. Количество контрольных точек восстановления, доступных в любой заданный момент времени, ограничено объемом пространства, которое выделено пользователем для работы системы восстановления. Максимальный размер пространства, которое можно выделить, составляет приблизительно 12 процентов.

В ходе процедуры восстановления происходит восстановление ОС и программ, инсталлированных на компьютере, к состоянию, в котором они находились на момент выбранной контрольной точки восстановления. Этот процесс не затрагивает личные файлы пользователя (включая сохраненные документы, сообщения электронной почты, адресную книгу, списокИзбранные (Favorites) и список Журнал (History) Интернет Explorer).

Все изменения, внесенные утилитой Восстановление системы (System Restore), полностью обратимы, и если пользователя не удовлетворяют результаты, то можно восстановить предыдущие настройки и выполнить все снова.

Выполнение работы

Задание 1. Выполните резервное копирование системных конфигурационных файлов.

- Запустите виртуальную машину VM-1 и загрузите ОС Windows.
- Запустите Мастер Архивации (Пуск/Программы/Стандартные/Служебные/Архивация данных).
- ознакомьтесь с информацией мастера и щелкните Далее.
- Выберите возможность мастера – Архивация файлов и параметров и щелкните Далее.
- Укажите выбор элементов архивирования в самостоятельном режиме – Предоставить возможность выбора объектов для архивации и щелкните Далее.
- Укажите элементы для архивации – папки Documents and Settings и Program Files и щелкните Далее.
- Укажите место хранения архива:
- откройте диалоговое окно сохранить как кнопкой Обзор;
- перейдите в корневой каталог диска С;
- введите в поле Имя Файла – имя сохраняемого файла - Резервная Копия;

- сохраните файл кнопкой Сохранить;
- подтвердите введенные данные кнопкой Далее.
- Настройте дополнительные параметры архивации:
- откройте диалоговое окно дополнительных параметров кнопкой. Дополнительно;
- выберите в раскрывающемся списке тип архивации – Обычный и щелкните далее;
- установите флажок проверять данные после архивации (Далее);
- укажите способ добавления архива – Добавить этот архив к существующему (Далее);
- укажите время архивации:
- установите радиокнопку позднее;
- введите имя задания в соответствующее поле;
- откройте диалоговое окно Запланированное задание кнопкой Расписание;
- введите в поле Время начала время на 2 минуты позже текущего (например, если сейчас 12.40, то вам необходимо ввести 12.42);
- подтвердите введенные параметры кнопкой ОК;
- завершите ввод времени выполнения архивации кнопкой. Далее;
- введите данные пользователя от имени которого будет выполняться архивирование:
- введите в поле Пользователь имя пользователя на компьютере - USER;
- введите в поля Пароль и Подтверждение пароля для пользователя USER;
- подтвердите ввод данных кнопкой ОК;
- завершите работу мастера кнопкой Готово.
- Запустите Мастер Архивации (Пуск/Программы/Стандартные/Служебные/Архивация данных).
- Ознакомьтесь с информацией мастера и щелкните Далее.
- Выберите возможность мастера – Восстановление файлов и параметров и щелкните Далее.
- Выберите для восстановления в левом списке с содержимым архива, папку Мои рисунки (Далее);
- Ознакомьтесь с выбранными параметрами и активизируйте восстановление кнопкой Готово.
- Откройте отчет кнопкой Отчет и просмотрите его.
- Закройте диалоговое окно Ход восстановления кнопкой Закрыть.
- Создайте точку восстановления.
- Запустите мастер Восстановление системы (Пуск/Программы/Стандартные/Служебные).
- Ознакомьтесь с информацией мастера.
- Создайте точку восстановления:
- Установите радиокнопку создать точку восстановления (Далее);
- введите в текстовое поле Описание контрольной точки восстановления - Тестовая точка восстановления;
- создайте точку восстановления кнопкой Создать.
- Завершите работу мастера кнопкой Закрыть.

Контрольные вопросы:

1. Что такое резервное копирование?
2. Какие бывают виды резервного копирования?
3. На какие носители информации можно сделать "бэкап"?
4. Для чего создаются резервные копии?
5. Какие схемы ротации носителей информации используются?

Оформление отчета:

1. Цель работы.

2. Постановка задачи.
3. Подробное описание технологии выполнения каждого пункта задания, подкрепленное изображением.
4. Вывод.

Министерство образования и науки Российской Федерации
федеральное государственное бюджетное образовательное учреждение высшего образования
"Российский экономический университет имени Г.В. Плеханова"
МОСКОВСКИЙ ПРИБОРОСТРОИТЕЛЬНЫЙ ТЕХНИКУМ

ПРАКТИЧЕСКАЯ РАБОТА № 17
ДИСЦИПЛИНА: ОПЕРАЦИОННЫЕ СИСТЕМЫ

Тема: Брандмауэры, основы работы в Unix..

Специальность: 09.02.03 «Программирование в компьютерных системах»
Квалификация: техник-программист

Цель работы: Приобретение навыков работы с антивирусными средствами и брендмауэрами.
Оборудование: ПК, ОС с установленной системой виртуализации (Virtual Box, VMWare), образ виртуальной машины ОС Linux
Время выполнения работы: 2 академических часа.
Теоретические сведения:

В Linux есть отличная система управления сетевыми пакетами на уровне ядра, называемая iptables, которую можно настроить как непосредственно из командной строки, так и через разнообразные графические интерфейсы администрирования. Одним из наиболее мощных интерфейсов управления брандмауэром является система Firewall Builder, созданная для того, чтобы можно было отделить политику защиты от реализации защиты, и чтобы можно было сосредоточиться на том, что вы хотите, чтобы делал брандмауэр, а не на том, как вы хотите, чтобы он это делал.

В интерфейсе Firewall Builder в качестве объектов используются хосты, маршрутизаторы, брандмауэры, сети и протоколы, и вы можете с помощью мышки перетаскивать эти объекты, когда определяете политику вашего брандмауэра. Затем Firewall Builder скомпилирует вашу политику в фактические правила, которые необходимы для соблюдения этой политики, причем есть много компиляторов политики, которые предназначены для различных типов брандмауэров. Вы можете определить свою политику с помощью Firewall Builder, который работает на настольном компьютере с Ubuntu, а затем откомпилировать эту политику для брандмауэра, работающего с *iptables* на Linux, с *ipfilter* на BSD, или с приблизительно полудюжиной других технологий брандмауэров. Политика может определяться одним и тем же способом независимо от технологии, которая используется на целевом брандмауэре. И поскольку Firewall Builder может одновременно поддерживать несколько брандмауэров, вы можете использовать его в качестве центральной консоли управления для настройки различных брандмауэров и отдельных хостов всей вашей сети в качестве единого унифицированного интерфейса.

Вы можете, если захотите, запустить Firewall Builder непосредственно на вашем брандмауэре, но поскольку политика общая, хорошо, чтобы ваш брандмауэр минимально использовал возможности системы, так как лучше всего иметь в качестве брандмауэра отдельную машину, а Firewall Builder запустить на управляющей машине, которой может быть персональный компьютер или ноутбук. Затем, когда вы захотите обновить политику брандмауэра, вы можете запустить Firewall Builder на управляющей машине для создания новых правил и переноса их в брандмауэр.

Первоначальная настройка брандмауэра

Начните с настройки вашей машины с брандмауэром и установите минимальный вариант Ubuntu: запустите программу установки и установите сервер поскольку в этом случае будут установлены только основные пакеты. Также желательно установить хотя бы одну дополнительную карту Ethernet, что позволит отделить ненадежный трафик интернета от внутренней сети. При стандартном подходе на брандмауэре запускается три сетевых интерфейса: один к внутренней сети (или *downstream*), один для подключения к сети интернет (или *upstream*) и один к отдельной локальной сети, называемой демилитаризованной зоной (или *DMZ*), в которой вы можете разместить серверы, открытые для доступа из интернета. Сконфигурируйте сетевые интерфейсы под соответствующие сети, к которым они подключены, и, с помощью команды ping, проверьте, чтобы были доступны хосты каждой сети.

Теперь ваша машина, предназначенная для брандмауэра, настроена как шлюз между интернетом, вашей внутренней сетью, а также любыми серверами, которые вы захотите запускать, но еще неизвестно, как передавать данные из одной сети в другую так, чтобы все было эффективно изолировано. Для того, чтобы ваш брандмауэр передавал пакеты с одного сетевого интерфейса на другой и выполнял фильтрацию пакетов и трансляцию сетевых

адресов / портов, вам нужно установить *iptables*, а также включить дистанционное управление брандмауэром, поэтому вам нужно установить SSH-сервер:

$ sudo apt-get install iptables ssh

Первоначальная настройка управляющей машины

Установите на вашей управляющей машине Firewall Builder, а также RCS и пакеты с документацией по Firewall Builder:

$ sudo apt-get install fwbuilder rcs fwbuilder-doc

Теперь вы готовы выполнить остальные шаги.

Создайте новый проект

Сначала запустите Firewall Builder:

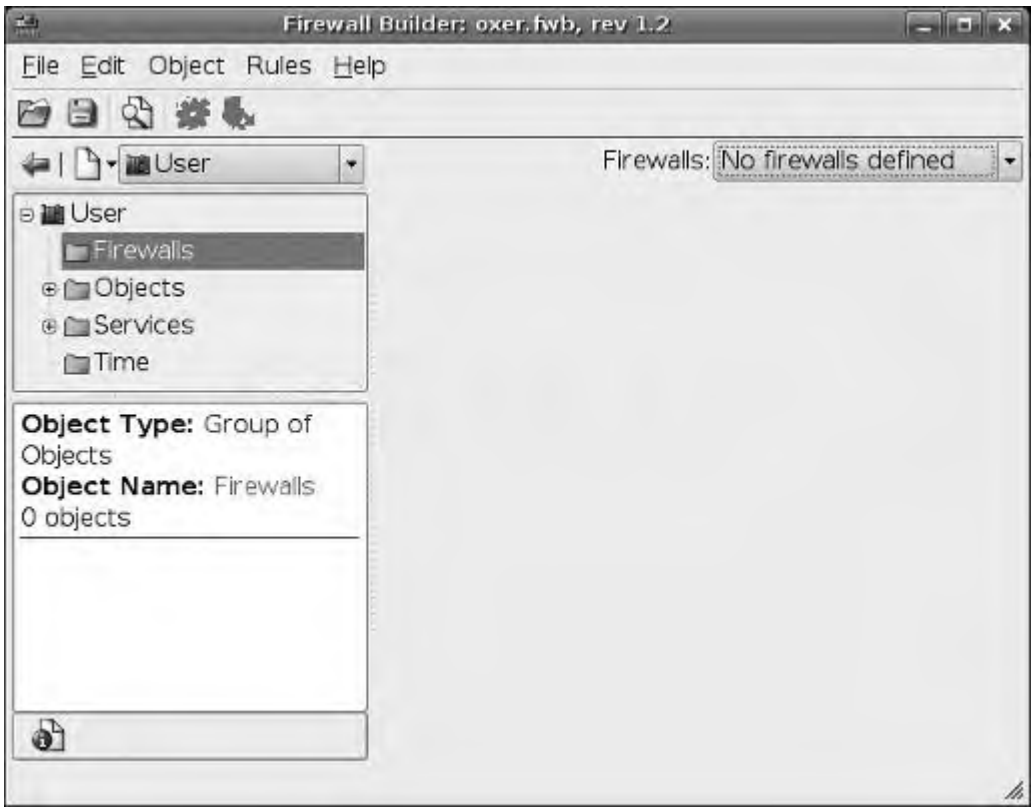
$ fwbuilder

Выберите Create New Project File (Создать новый файл с проектом) и укажите место, где он будет сохранен. Будет хорошо, если вы создадите специальный директорий для хранения файла с проектом, поскольку Firewall Builder будет в том же самом директории создавать другие файлы и будет проще делать резервные копии настроек вашего брандмауэра, если все находится в одном месте.

После этого вы сможете активировать контроль версий проекта, а также настроить, чтобы проект автоматически открывался при запуске Firewall Builder. Включите обе эти возможности.

Возможность контроля версий требует от Firewall Builder сохранять конфигурационный файл в RCS, что позволит видеть всю историю файла, в том числе все его изменения, которые когда-либо были в нем сделаны. Эта возможность может быть очень полезной в случае, если в процессе настройки ваш брандмауэр выйдет из строя и вам потребуется вернуться к заведомо исправной рабочей конфигурации.

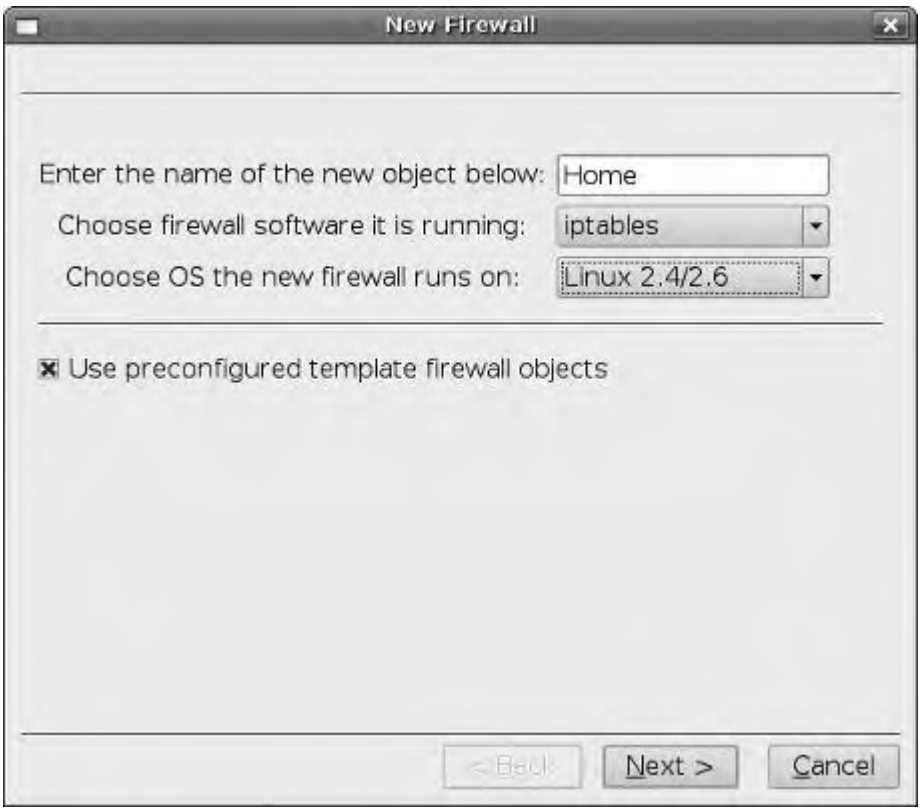
Firewall Builder начнет свою работу с пустой конфигурации, содержащей только ряд предопределенных сервисов из двух библиотек (см. рис.7-1). Библиотеки называются User (Пользовательская) и Standard (Стандартная) и вы можете переключаться между ними с помощью выпадающего меню, расположенного в левом верхнем углу окна. Библиотека Standard (Стандартная), поставляемая в комплекте с Firewall Builder, является библиотекой, из которой объекты можно только читать и в которой находятся предопределенные сервисы практически для любого сервиса TCP и UDP для типичных случаев их использования, а также предопределенные диапазоны сетевых адресов и интервалы времени. Библиотека User (Пользовательская) является библиотекой, в которой можно запоминать объекты, которые вы определили, в том числе брандмауэры, настроенные сервисы TCP и UDP, а также настроенные диапазоны сетевых адресов.



Определяем новый брандмауэр

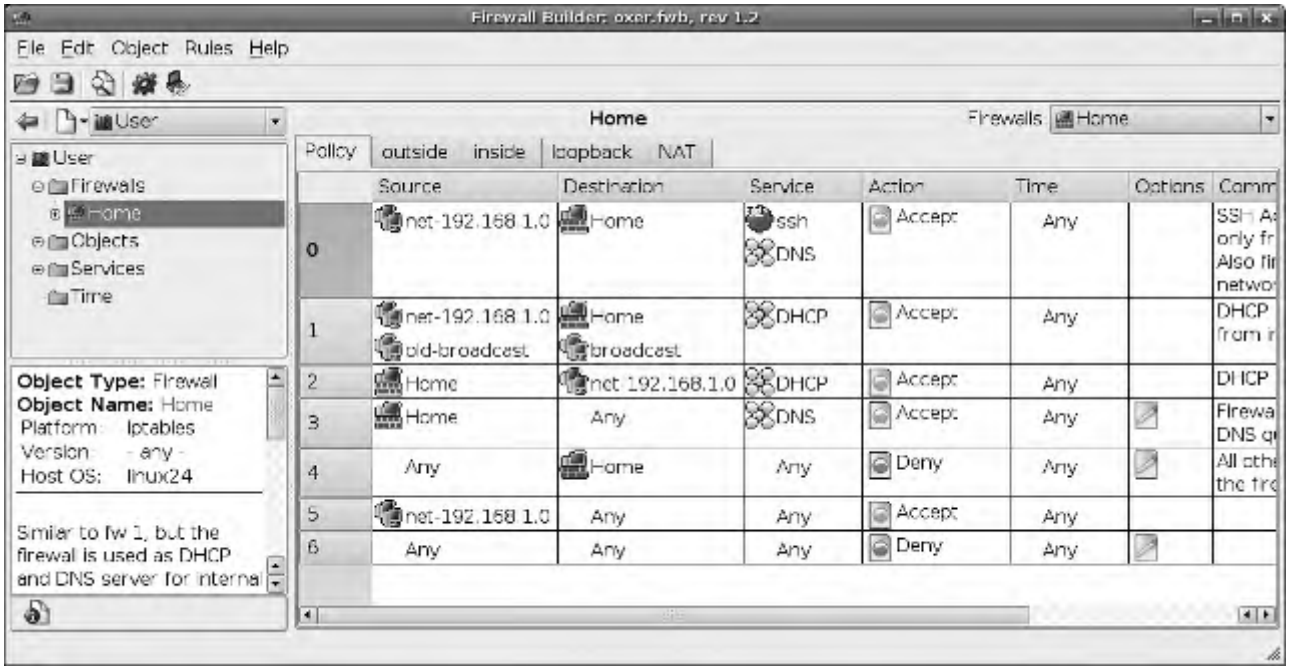
Убедитесь, что выбрана библиотека User (Пользователь), щелкните правой кнопкой мыши по директории Firewalls (Брандмауэры) и выберите вариант New Firewall (Новый брандмауэр). Откроется диалоговое окно New Firewall (Новый брандмауэр) так, как это показано на рис.7-2. Задайте для вашего брандмауэра имя, выберите программу, с помощью которой реализуется брандмауэр (как правило, "Iptables", если на машине с брандмауэром вы запускаете Linux), и выберите операционную систему вашего брандмауэра (Linux 2.4/2.6). Теперь видно, насколько гибок Firewall Builder и насколько много типов брандмауэров он поддерживает.

У вас также есть возможность использовать объекты с предварительно сконфигурированным шаблоном брандмауэра, что хорошо в случае, если вы только знакомитесь с Firewall Builder. Шаблоны позволяют очень легко начать работать с типичными сценариями брандмауэра, а не начинать с нуля с абсолютно пустой конфигурации. После того как вы сделаете свой выбор, нажмите кнопку Next (Далее).



Пощелкайте по именам всех шаблонов брандмауэров и посмотрите их схемы и краткие пояснения их работы. В большинстве малых сетей хорошо подойдет вариант "fw template 1", в котором задан типичный брандмауэр с динамическим внешним адресом, статическими внутренними адресами сети 192.168.1.0/24, неограниченным исходящим трафиком из сети и с доступом к самому брандмауэру только из внутренней сети через SSH. Вариант "fw template 2" похож на предыдущий, но в нем брандмауэр работает как сервер DHCP и DNS во внутренней сети.

После того, как вы выберете шаблон, вы вернетесь к основному окну Firewall Builder, предназначенному для управления политикой, но теперь у вас уже есть для вашего нового брандмауэра политика, определяемая по умолчанию. Firewall Builder отображает правила политики в виде списка, в котором правила упорядочены в порядке их использования, которые проверяются с самого верхнего правила и далее вниз до тех пор, пока не будет найдено соответствие.



С помощью вкладок, расположенных в верхней части списка, можно получить доступ к нескольким спискам правил. Главным списком является список Policy, в котором указаны правила, с помощью которых запрещаются и разрешаются действия для всего брандмауэра. Кроме того для каждого интерфейса брандмауэра имеется отдельный список правил, и, наконец, есть список NAT, который позволяет настраивать правила трансляции сетевых адресов Network Address Translation. Как правило, вам не следует беспокоиться об отдельных интерфейсах, большинство изменений будет касаться списков Policy и NAT.

Добавляем политику, относящуюся к конкретному хосту

Чтобы понять, как с помощью списков Policy и NAT осуществляется управление, попробуйте добавить конкретный сценарий, например, предоставьте доступ извне к внутреннему веб-серверу.

Сначала добавьте к серверу объект Host (Хост). Перейдите по дереву объектов User→Objects→Hosts (Пользователь → Объекты → Хосты), щелкните правой кнопкой мыши по Hosts (Хосты) и выберите New Host (Новый хост). Введите имя для вашего нового хоста, например, www.example.com, установите флажок на Use Preconfigured Template Host Objects (Использовать хост с предварительно сконфигурированным шаблоном), а затем нажмите кнопку Next (Далее).

Выберите шаблон "PC with 1 interface" и нажмите кнопку Finish ("Готово"). В ваш список хостов будет добавлен объект с предварительно определенным интерфейсом, так что перейдите по User→Objects→Hosts→<www.example.com>→eth0→<www.example.com> (Пользователь → Объекты → Хосты → <www.example.com> → eth0 → <www.example.com>, а затем дважды щелкните по www.example.com и отредактируйте значения, заданные в интерфейсе. Измените IP адрес так, чтобы он соответствовал фактическому внутреннему адресу вашего сервера, подтвердите сделанные изменения и закройте диалоговое окно.

Предположим, что у вас есть диапазон общедоступных статических IP-адресов, назначенных внешнему интерфейсу вашей сети. Щелкните правой кнопкой мыши по "eth0" и выберите пункт Add IP Address (Добавить IP-адрес). Введите общедоступный IP адрес и маску сети, подтвердите сделанные изменения и закройте окно.

Теперь для вашего сервера определены два IP адреса: реальный адрес, назначенный его интерфейсу, и общедоступный адрес, через который люди могут к нему осуществлять доступ.

Теперь щелкните по вкладке NAT, расположенной в верхней части списка правил. Добавьте новое пустое правило NAT либо при помощи щелчка правой кнопкой мыши по существующему правилу, либо выбрав в меню Rules→Add Rule Below (Правила → Добавить ниже правило).

Теперь с помощью перетаскивания иконок объектов в соответствующие места вы можете создать свое правило NAT. В правиле имеются следующие столбцы:

Original Src

Исходный адрес источника пакетов перед трансляцией

Original Dst

Исходное назначение пакетов перед трансляцией

Original Srv

Исходный сервис (порт), на который поступают пакеты

Translated Src

Новый исходный адрес пакетов, указывающий, что с него поступили пакеты

Translated Dst

Новый адрес назначения, используемый в пакетах

Translated Srv

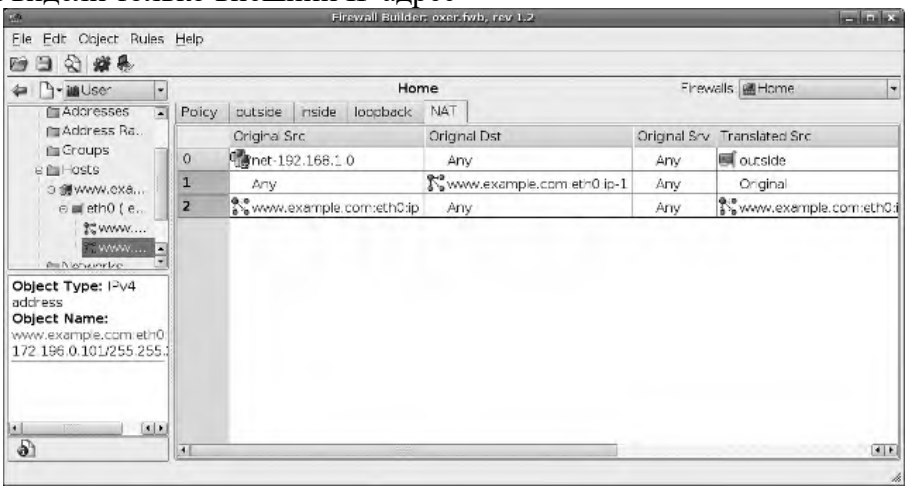
Новый порт, на который направляются пакеты

Первое правило создано именно для того, чтобы транслировать пакеты, которые направлены от брандмауэра на сервер. Щелкните по иконке, представляющей внешний IP

адрес сервера, и перетащите ее в поле Original Dst, а затем щелкните по иконке внутреннего IP адреса и перетащить ее в поле Translated Dst.

Теперь добавьте еще одно пустое правило и настройте его так, чтобы оно транслировало пакеты, направляемые от сервера во внешний мир. Щелкните по иконке с внутренним IP адресом и перетащите ее в поле Original Src, а иконку с внешним IP адресом перетащите в поле Translated Src.

Теперь у вас есть правила, в соответствии с которыми будут изменяться пакеты так, чтобы они перенаправлялись на сервер и с сервера через брандмауэр, но так, чтобы внешние компьютеры видели только внешний IP адрес



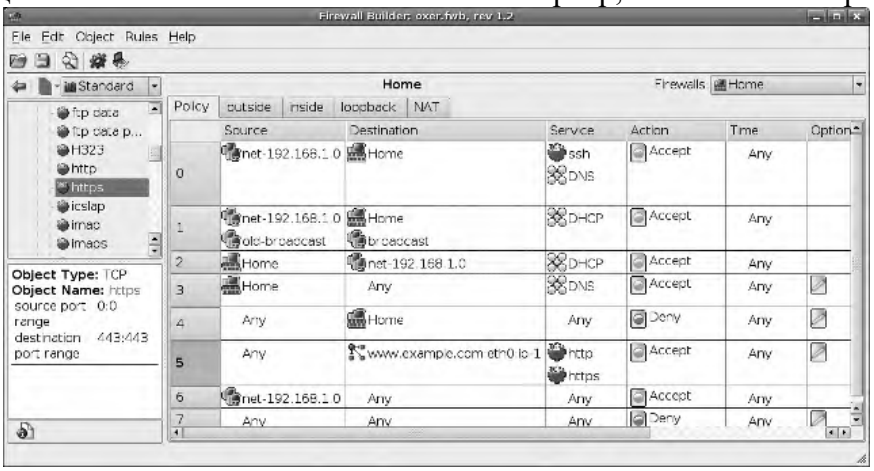
В этих примерах транслируются только IP адреса. Но вы также можете применить правила трансляции и к сервисам. Например, у вас может быть реверсный прокси сервер, который внутри сети работает как ускоритель доступа веб-серверу по внутреннему порту 8080, и вы хотите, чтобы внешние пользователи могли получать к нему доступ через стандартный порт HTTP - порт 80. С помощью перетаскивания сервисов в поля Original Srv и Translated Srv из библиотеки Standard (Стандартная) и, в случае необходимости, создания сервисов в библиотеке User (Пользовательская), вы можете выполнять трансляцию портов точно также, как и трансляцию адресов. С помощью Firewall Builder вы можете по собственному усмотрению преобразовывать адреса и порты источника пакетов и назначения пакетов, поэтому настраивайте правила NAT до тех пор, пока сетевой трафик не будет транслироваться так, как вы хотите.

Однако самих правил NAT недостаточно. Без соответствующего правила политики, пакеты не будут проходить через брандмауэр даже если они будут соответствовать правилам NAT. Хотя в правилах NAT определено, что *может* происходить, правила политики определяют, чему *разрешено* происходить. Последнее слово за правилами политики.

Щелкните по вкладке Policy (Политика) и, спускаясь по списку существующих правил, найдите подходящее место, куда можно добавить правила для вашего хоста. Скорее всего, это будет почти в конце списка перед общим сетевым правилом и правилом, запрещающим все, что не разрешено Deny All. Щелкните правой кнопкой мыши по колонке с номером правила и добавьте правило. Перетащите иконку с внешним IP адресом вашего веб сервера в поле Destination, а затем щелкните правой кнопкой мыши по иконке Deny (Запретить), расположенной в столбце Action (Действие) и замените ее на иконку Allow (Разрешить).

Если вы разрешаете извне вашей сети полный доступ к любому порту на вашем веб-сервереи, то это все, что нужно было сделать. Но безопаснее задать более конкретные правила и разрешать использовать только определенные сервисы, так что выберите из выпадающего меню User/Standard, находящегося в верхнем левом углу, библиотеку Standard (стандартная). Перейдите далее по Standard→Services→TCP→"http" (Стандартная → Сервисы → TCP → "http") и перетащите иконку этого протокола в поле Service вашего

нового правила. Если вы также хотите разрешить соединение по SSL, вы можете в то же самое поле также перетащить иконку "https". Теперь у вас есть правило, которое явно разрешает подключения с любого хоста на ваш веб-сервер, но только на порты 80 и 443.



Компилируем и устанавливаем политику

Как только вам все будет нравиться в политике, которую вы создали, ее следует применить к брандмауэру. С помощью Firewall Builder это делается в два этапа. Сначала политика компилируется в скрипт в соответствии с тем, какая программа используется в качестве брандмауэра, а затем скрипт переносится на брандмауэр и загружается.

Чтобы заставить Firewall Builder откомпилировать ваши правила, выберите Rules→Compile (Правила → Компилирование) или щелкните по иконке с изображением автомобильной коробки передач. Появится диалоговое окно, информирующее о ходе выполнения работы, а когда все завершится, у вас в рабочем директории, используемом Firewall Builder, вдобавок к файлу проекта будет находиться новый скрипт. Теперь вы можете через SSH скопировать этот скрипт на брандмауэр и, выполнив его, применить правила. Чтобы все было в порядке, создайте на брандмауэре новый директорий для хранения скрипта:

$ sudo mkdir /etc/firewall

Затем скопируйте скрипт в этот директорий и для того, чтобы его проверить, выполните его вручную. Несмотря на то, что этот скрипт имеет расширение. fw, это, на самом деле, простой шелл скрипт, который можно запустить обычным способом:

$ sudo /etc/firewall/ firewallname. fw

В Firewall Builder есть большое количество конфигурационных параметров, позволяющих для каждого брандмауэра управлять процессом генерации скрипта, так что если скрипт на брандмауэре не работает должным образом, вам, возможно, потребуется щелкнуть правой кнопкой мыши в дереве объектов по иконке брандмауэра, выбрать вариант Edit (Изменить), а затем щелкнуть по кнопке Firewall Settings (Настройки брандмауэра). С помощью вкладок, расположенные в верхней части, вы можете получить доступ к большому количеству параметров настроек, так что внимательно с ними ознакомьтесь и выберите те, которые применимы к вашему брандмауэру, а затем откомпилируйте правила и снова их проверьте.

Автоматический запуск политики

Скрипт брандмауэра должен запускаться каждый раз, когда загружается ваш брандмауэр, так что воспользуйтесь вашим любимым редактором для того, чтобы открыть файл /etc/rc.local и перед строкой exit 0 добавьте путь к скрипту. Конец файла /etc/rc.local должен выглядеть следующим образом:

/etc/firewall/firewallname. fw

exit 0

Всякий раз, когда Ubuntu переходит на новый многопользовательский уровень, после выполнения всех других скриптов будет выполняться файл rc. local. Ссылка на ваш скрипт, указанная в нем, обеспечит, что скрипт будет запускаться после всех других

сервисов, запускающих сеть, но при загрузке в однопользовательском режиме он запускаться не будет. Это удобно, если вы используете загрузку в однопользовательском режиме для исправления проблем с конфигурацией компьютера.

Автоматическая установка политики

После того как вы убедитесь, что правила вашего брандмауэра, генерируются правильно, на последующие обновления вы тратите меньше усилий, если настроите Firewall Builder так, чтобы он вместо вас выполнял установку и активацию скрипта. Выберите значок брандмауэра, который расположен в User→Firewalls (Пользователь → Брандмауэры), щелкните правой кнопкой мыши, выберите Edit (Изменить), в результате чего откроется диалоговое окно Firewall (Брандмауэр). Щелкните по Firewall Settings (Настройки брандмауэра) для того, чтобы вновь войти в диалоговое окно настройки брандмауэра. Щелкните по вкладке Installer (Инсталлятор), на которой указаны настройки, позволяющие выполнить скрипт, который установит и активирует правила брандмауэра. В нижней части диалогового окна имеются два текстовых поля ввода, в которых можно указать вызов любого внешнего скрипта или команды, которые вы захотите выполнить. Так, например, можно написать скрипт, который с помощью SCP скопирует скрипт на брандмауэр, а затем с помощью SSH выполнит его. В Firewall Builder есть пример такого скрипта, который установлен в /usr/bin/fwb_install и выполняет как раз то, что вам. Полная информация об использовании скрипта fwb_install приведена на странице его описания:

$ man fwb_install

В Firewall Builder также есть свой собственный механизм установки политики, которого вполне достаточно в большинстве случаев.

Чтобы автоматически устанавливать политику, сначала на брандмауэре создайте группу, например, fwadmin, а затем создайте пользователя и сделайте его членом этой группы:

$ sudo addgroup fwadmin

$ sudo adduser fwadmin -G fwadmin

$ sudo mkdir -m 0770 /etc/firewall $ sudo chown fwadmin: fwadmin /etc/firewall.

Сконфигурируйте sudo так, чтобы созданный пользователь мог без ввода пароля выполнять скрипт настройки брандмауэра. Для этого запустите

$ sudo visudo

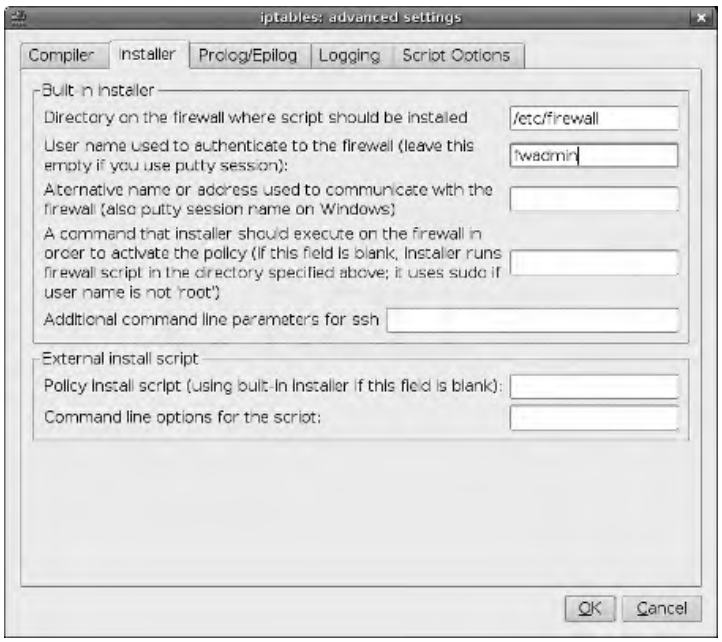
и добавьте в конце файла /etc/sudoers следующую строку:

%fwadmin = NOPASSWD:/etc/firewall/firewallname.fw

Имя firewallname. fw следует заменить на имя реально существующего скрипта, который был сгенерирован для этого брандмауэра с помощью Firewall Builder.

Дополнительно вы можете настроить шифрование с открытым ключом для доступа на брандмауэре к учетной записи fwadmin.

В диалоговом окне Firewall Settings (Настройки брандмауэра) на вкладке Installer (Инсталлятор) укажите путь к директорию, который вы создали на брандмауэре, и имя пользователя, созданного вами.



Контрольные вопросы:

1. Что такое брандмауэр?
2. Для каких целей применяется Брандма́уэр?

Оформление отчета:

1. Цель работы.
2. Постановка задачи.
3. Подробное описание технологии выполнения каждого пункта задания, подкрепленное изображением.
4. Вывод.

Министерство образования и науки Российской Федерации
федеральное государственное бюджетное образовательное учреждение высшего образования
"Российский экономический университет имени Г.В. Плеханова"
МОСКОВСКИЙ ПРИБОРОСТРОИТЕЛЬНЫЙ ТЕХНИКУМ

ПРАКТИЧЕСКАЯ РАБОТА № 18
ДИСЦИПЛИНА: ОПЕРАЦИОННЫЕ СИСТЕМЫ

Тема: Основные правила и требования шифрованию данных в операционных системах. ПО обеспечивающие пользовательское шифрование.

Специальность: 09.02.03 «Программирование в компьютерных системах»
Квалификация: техник-программист

Цель работы: Целью практической работы является изучение способов шифрования информации с помощью средств, предоставляемых операционными системами Windows, и применение данных средств на практике на примере шифрованной файловой системы Windows.

Время выполнения работы: 2 академических часа.

Теоретические сведения:

Шифрование папок и файлов – способ защиты их от нежелательного доступа.

Шифрованная файловая система (Encrypting File System — EFS) — средство Windows,

позволяющее сохранять сведения на жестком диске в шифрованном формате. Шифрование – это самый надежный способ защиты данных, предоставляемый Windows. Данная функция шифрования присутствует в операционных системах Windows только в выпусках: Профессиональная — Professional, Корпоративная — Enterprise, Максимальная — Ul-timate.

Шифрование обеспечивается при помощи шифрующей файловой системы, которая фактически представляет собой надстройку файловой системы NTFS. Вследствие этого шифрование данного вида недоступно на разделах файловой системы FAT32. Все этапы шифрования производятся при сохранении и открытии файла и проходят практически незаметно.

EFS работает, шифруя каждый файл с помощью алгоритма симметричного шифрования, зависящего от версии операционной системы и настроек. При этом используется случайно сгенерированный ключ для каждого файла, называемый File Encryption Key (FEK), выбор симметричного шифрования на данном этапе объясняется его скоростью по отношению к асимметричному шифрованию. FEK (случайный для каждого файла ключ симметричного шифрования) защищается путём асимметричного шифрования, использующего открытый ключ пользователя (сертификат пользователя), шифрующего файл, и алгоритм RSA.

Для расшифрования данных драйвер шифрованной файловой системы прозрачно для пользователя расшифровывает FEK, используя закрытый ключ пользователя, а затем и необходимый файл с помощью расшифрованного файлового ключа.

Войдя в систему под своей учетной записью, пользователь может открывать и редактировать зашифрованные ранее файлы. При добавлении нового файла в зашифрованный каталог он также будет зашифрован. Перемещение или копирование файла из зашифрованного каталога не приводит к автоматическому расшифрованию, при условии, что файл перемещается в раздел NTFS. Остальные пользователи не смогут получить доступ к содержимому файла. Но если они имеют соответствующие разрешения на уровне NTFS, они могут беспрепятственно переименовать или удалить файл.

Рекомендуется шифровать не отдельные файлы, а каталоги — это приведет к шифрованию всех файлов, сохраненных в данной папке.

Порядок выполнения работы

Практическая работа выполняется на виртуальной машине с установленной операционной системой Windows 7 Ultimate, для запуска которой используется программа

VMware Player.

Прежде чем приступить к изучению шифрованной файловой системы Windows, необходимо выбрать файлы, с которыми будет вестись дальнейшая работа. Для этого на локальном диске D создайте два произвольных файла, например, два текстовых файла Файл№1.txt и Файл №2.txt (рисунок 1.3). Каждому из них затем будут назначены свои параметры шифрования.

Теперь зашифруем первый файл. Для этого необходимо выполнить следующие действия:

- Вызвать контекстное меню нужного объекта (файла или папки) и выбрать пункт «Свойства».

- Перейти на вкладку «Общие» и нажать кнопку «Другие», что приведет к открытию окна «Дополнительные атрибуты».
- Активировать параметр «Шифровать содержимое для защиты данных»
- Закрыть оба окна при помощи кнопки «ОК».

Если шифрование было применено к отдельному файлу, который расположен не в корне локального диска, а в какой-либо папке, то система выдаст дополнительный запрос на запуск шифрования только данного файла или всей папки, в которой этот файл расположен

Если шифрование было применено к папке, то система выдаст дополнительный запрос на запуск шифрования всего каталога

После этого файл (папка с файлами) будет зашифрован, а название файла станет отображаться зелёным цветом. Если нужно отключить шифрование, то необходимо снова открыть панель «Дополнительные атрибуты» и отключить параметр «Шифровать содержимое для защиты данных».

При первой настройке функции шифрования отобразится предложение о создании архивной копии сертификата и ключа шифрования (рисунок 1.8). Данную процедуру обязательно необходимо произвести, поскольку есть шанс потерять зашифрованные файлы, например, после переустановки системы или удаления учетной записи.

Для этого выберите пункт «***Архивировать сейчас (рекомендуется)***», после чего появится окно мастера экспорта сертификатов

Нажмите «Далее», в следующем окне также нажмите «Далее», не изменяя никаких параметров (рисунок

Затем необходимо ввести пароль, являющийся защитой закрытого ключа пользователя. Введите произвольный пароль, который обязательно необходимо запомнить, и нажмите «Далее».

Выберите расположение экспортирования файла, содержащего сертификат и закрытый ключ

В случае успешного завершения операции будет выведено соответствующее сообщение.

Чтобы проверить, что данный файл зашифрован, создайте учетную запись второго пользователя.

Откройте «Пуск», затем «Панель управления» и в режиме просмотра по категориям откройте «Добавление и удаление учетных записей пользователей» в категории «Учетные записи пользователей и семейная безопасность». Создайте новую учетную запись с обычным доступом и войдите в систему под данной учетной записью. Попробуйте открыть файл, зашифрованный первым пользователем. Будет выведено сообщение об отказе доступа к файлу.

Теперь зашифруйте второй файл из-под учетной записи второго пользователя, а также создайте архивную копию сертификата и закрытого ключа второго пользователя. Перейдите на учетную запись первого пользователя и попробуйте открыть файл, зашифрованный вторым пользователем. Также отобразится сообщение об отказе доступа к фай-лу.

Если по какой-либо причине будут потеряны данные о сертификате и закрытом ключе пользователя, то и сам пользователь не сможет получить доступ к зашифрованным им файлам и папкам. Удалим данный сертификат вручную у первого пользователя:

1) Откройте меню «Пуск», в поле поиска введите название утилиты «certmgr.msc» и нажмите Enter.
2) В открывшемся окне управления хранилищем сертификатов откройте сертификаты раздела «Личное».
3) Удалите сертификат первого пользователя.

Чтобы изменения вступили в силу, завершите сеанс первого пользователя и снова зайдите под учетной записью первого пользователя. Теперь доступ от первого пользователя к файлам, зашифрованным первым пользователем не доступен.

Чтобы вернуть доступ, необходимо восстановить сертификат и закрытый ключ пользователя. Для этого снова откройте хранилище сертификатов, перейдите в сертификаты раздела «Личное» и, вызвав правой кнопкой контекстное меню, выберите «Все задачи/Импорт…». Запустится мастер импорта сертификатов, нажмите «Далее» Укажите нужный сертификат, при этом нужно сменить указанный тип файлов с .cer.crt на .pfx, так как по умолчанию в программе задаются сертификаты без закрытого ключа, нажмите «Далее».

В следующем окне необходимо ввести пароль, указанный при архивировании сертификата первого пользователя. Введите пароль и нажмите «Далее»

Поместите сертификат в хранилище сертификатов «Личное», нажмите «Далее»

Восстановление сертификата с закрытым ключом завершено. Теперь доступ к файлам восстановлен.

Использовать шифрование файлов можно и при совместном использовании одного файла несколькими пользователями. Общий доступ для папок не устанавливается. Сделаем доступным второй файл первому пользователю. Для этого откройте личное хранилище сертификатов первого пользователя, выделите восстановленный сертификат, вызовите контекстное меню и выполните команду «Все задачи/Экспорт…».

При этом выполнится экспорт сертификата без закрытого ключа первого пользователя.

Представим, что данный сертификат был передан второму пользователю. Перейдите на учетную запись второго пользователя и откройте хранилище серти-

фикатов второго пользователя. Перейдите в раздел сертификатов «Личное», вызовите контекстное меню и выполните команду «Все задачи/Импорт». Импортируйте сертификат первого пользователя без закрытого ключа в раздел «Доверенные лица».

Откройте свойства второго файла, перейдите на вкладку «Общие» и нажмите кнопку «Другие». В окне «Дополнительные атрибуты» нажмите кнопку «Подробно», откроется окно доступа к файлу.

Нажмите кнопку «Добавить…» и выберите сертификат первого пользователя.

Проверьте доступ к данному файлу для первого пользователя. Чтобы убедиться, что данный файл доступен только первому и второму пользователю – создайте третьего пользователя и попробуйте через его учетную запись открыть второй файл.

Контрольные вопросы:

1) В каких выпусках операционных систем Windows присутствует шифрованная файловая система?
2) Опишите алгоритм работы шифрованной файловой системы Windows.
3) Для каких файловых систем применима шифрованная файловая система?
4) Для чего нужно архивировать закрытый ключ и сертификат пользователя?
5) Какие действия необходимо выполнить, чтобы включить шифрование.

Оформление отчета:

1. Цель работы.
2. Постановка задачи.
3. Подробное описание технологии выполнения каждого пункта задания, подкрепленное изображением.
4. Вывод.

Министерство образования и науки Российской Федерации
федеральное государственное бюджетное образовательное учреждение высшего образования
"Российский экономический университет имени Г.В. Плеханова"
МОСКОВСКИЙ ПРИБОРОСТРОИТЕЛЬНЫЙ ТЕХНИКУМ

ПРАКТИЧЕСКАЯ РАБОТА № 19
ДИСЦИПЛИНА: ОПЕРАЦИОННЫЕ СИСТЕМЫ

Тема: Осуществление настройки сетевых протоколов серверов и рабочих станций.

Специальность: 09.02.03 «Программирование в компьютерных системах»
Квалификация: техник-программист

Цель работы: изучить способы диагностики настроек стека протоколов TCP/ IP; получить сведения о настройке TCP/IP для работы с DHCP сервером.

Время выполнения работы: 4 академических часа.

Теоретические сведения:

На концептуальной модели взаимодействия открытых систем OSI основан стек протоколов TCP/IP (Transmission Control Protocol - протокол управления передачей / Internet Protocol – Интернет-протокол), который предоставляет ряд стандартов для связи компьютеров и сетей.

Стек протоколов TCP/IP – промышленный стандарт, который позволяет организовать сеть масштаба предприятия и связывать компьютеры, работающие под управлением различных операционных систем.

Применение стека протоколов TCP/IP дает следующие преимущества:

- поддерживается почти всеми операционными системами; почти все большие сети основаны на TCP/IP;
- технология позволяет соединить разнородные системы;
- надежная, расширяемая интегрированная среда на основе модели «клиент — сервер»;
- получение доступа к ресурсам сети Интернет.

Каждый узел TCP/IP идентифицирован своим логическим IP-адресом, который идентифицирует положение компьютера в сети почти таким же способом, как номер дома идентифицирует дом на улице.

Реализация TCP/IP позволяет узлу TCP/IP использовать статический IP-адрес или получить IP-адрес автоматически с помощью DHCP-сервера (Dynamic Host Configuration Protocol- протокол динамической конфигурации хоста).

Для простых сетевых конфигураций, основанных на локальных сетях (LAN, Local Area Network), он поддерживает автоматическое назначение IP-адресов.

По умолчанию компьютеры клиентов, работающие под управлением ОС Windows или Linux, получают информацию о настройке протокола TCP/IP автоматически от службы DHCP.

Однако даже в том случае, если в сети доступен DHCP-сервер, необходимо 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.

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

Параметр	Описание
IP-адрес	Логический 32-битный адрес, который идентифицирует TCP/IP узел. Каждой плате сетевого адаптера в компьютере с запущенным протоколом TCP/IP необходим уникальный IP-адрес, такой, как 192.168.0.108. 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 — 192.168.0, и ID узла — 108.
Маска подсети	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. При соединении узлов TCP/IP, маска подсети определяет, где находится

	узел получателя: в локальной или удаленной сети. Для связи в локальной сети компьютеры должны иметь одинаковую маску подсети.
Шлюз по умолчанию	Промежуточное устройство в локальной сети, на котором хранятся сетевые идентификаторы других сетей предприятия или Интернета. 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 достигнет шлюза, связанного с указанным адресатом.

TCP/IP если сервер с запущенной службой DHCP доступен в сети, он автоматически предоставляет информацию о параметрах TCP/IP клиентам DHCP.

Задание 1. Проверьте работоспособность стека протоколов TCP/IP.

- Запустите виртуальную машину VM-1 и загрузите ОС Windows.
- Запустите консоль (Пуск/Программы/Стандартные/Командная строка).
- В командной строке введите ipconfig /all | more.
- Используя приведенную ниже информацию, создайте в своей папке текстовый документ со следующими данными:
- Имя компьютера;
- Основной DNS-суффикс;
- Описание DNS-суффикса для подключения;
- Физический адрес;
- DHCP включен;
- Автоконфигурация включена;
- IP-адрес автоконфигурации;
- Маска подсети;
- Шлюз по умолчанию.
- Убедитесь в работоспособности стека TCP/IP, отправив эхо-запросы на IP-адреса. Для этого воспользуйтесь командой ping:
- отправьте эхо-запросы на локальный адрес компьютера (loopback) ping 127.0.0.1 (на экране должны появиться сообщения о полученном ответе от узла 127.0.0.1);
- отправьте эхо-запрос по другому IP-адресу, например, 172.21.5.1.

Задание 2. Настройте стек протоколов TCP/IP для использования статического IP-адреса.

- Откройте окно Сетевые подключения (Пуск/Панель управления/Сетевые подключения).
- Вызовите свойства подключения по локальной сети. Для этого можно воспользоваться контекстным меню.
- В появившемся диалоговом окне на вкладке Общие откройте свойства Протокол Интернета TCP/IP.
- Щелкните переключатель использовать следующий IP-адрес и введите в соответствующие поля данные: IP_адрес; Маску подсети; Основной шлюз; Предпочитаемый DNS.
- Примените параметры кнопкой ОК.
- Закройте окно свойств подключения кнопкой ОК (если потребуется, то согласитесь на перезагрузку компьютера).
- Проверьте работоспособность стека протоколов TCP/IP.

Задание 3. Настройте TCP/IP для автоматического получения IP-адреса.

- Откройте окно Сетевые подключения.
- Вызовите свойства Подключения по локальной сети.
- Откройте свойства Протокол Интернета TCP/IP.
- Установите переключатель получить IP-адрес автоматически.

- Закройте диалоговое окно Свойства: Протокол Интернета TCP/IP кнопкой ОК.
- Примените параметры кнопкой ОК.
- Проверьте настройку стека протоколов TCP/IP.
- Получите другой адрес для своего компьютера. Для этого:
- запустите консоль (командную строку);
- введите команду для сброса назначенных адресов - ipconfig /release;
- введите команду для получения нового адреса ipconfig / renew;
- Проверьте работоспособность стека протоколов TCP/IP.

Контрольные вопросы

Назовите основное назначение и возможности технологии применения масок переменной длины (VLSM).

Назовите основное назначение и возможности технологии бесклассовой междоменной маршрутизации (CIDR).

Объясните основные функции, выполняемые шлюзомв коммуникационной схеме протокола IP.

КакимобразОм, машины, работающиевIP сети, определяют, когдапакет необходимо доставить шлюзу, а в каком случае доставка выполняется непосредственно с помощью протоколов канального уровня?

Оформление отчета:

1. Цель работы.
2. Постановка задачи.
3. Подробное описание технологии выполнения каждого пункта задания, подкрепленное изображением.
5. Вывод.

Министерство образования и науки Российской Федерации
федеральное государственное бюджетное образовательное учреждение высшего образования
"Российский экономический университет имени Г.В. Плеханова"
МОСКОВСКИЙ ПРИБОРОСТРОИТЕЛЬНЫЙ ТЕХНИКУМ

ПРАКТИЧЕСКАЯ РАБОТА № 20
ДИСЦИПЛИНА: ОПЕРАЦИОННЫЕ СИСТЕМЫ

Тема: WindowsServer: Обеспечение работы системы регистрации и авторизации пользователей сети.

Специальность: 09.02.03 «Программирование в компьютерных системах»
Квалификация: техник-программист

Цель работы: изучить способы диагностики настроек стека протоколов TCP/ IP; получить сведения о настройке TCP/IP для работы с DHCP сервером.
Время выполнения работы: 2 академических часа.
Теоретические сведения:

Основополагающим компонентом доменных служб в каждой организации являются принципалы безопасности (оригинальное название - Security Principal), которые предоставляют пользователей, группы или компьютеры, которым требуется доступ к определенным ресурсам в сети. Именно таким объектам, как принципалам безопасности можно предоставлять разрешения доступа к ресурсам в сети, причем каждому принципалу во время создания объекта присваивается уникальный идентификатор безопасности (SID), который состоит из двух частей. Идентификатором безопасности SID называется числовое представление, которое уникально идентифицирует принципал безопасности. Первая часть такого идентификатора представляет собой идентификатор домена. Ввиду того, что принципалы безопасности расположены в одном домене, всем таким объектам присваивается один и тот же идентификатор домена. Второй частью SID являетсяотносительный идентификатор (RID), который используется для уникальной идентификации принципала безопасности по отношению к ведомству, которое выдает SID.

Несмотря на то, что планирование и развертывание инфраструктуры доменных служб в большинстве организаций выполняется лишь один раз и в большинство объектов изменения вносятся очень редко, к важному исключению из этого правила можно отнести принципалы безопасности, которые необходимо периодически добавлять, изменять, а также удалять. Одним из основополагающих компонента идентификации являются учетные записи пользователей. По сути, учетные записи пользователей представляют собой физические объекты, в основном людей, которые являются сотрудниками вашей организации, но бывают исключения, когда учетные записи пользователей создаются для некоторых приложений в качестве служб. Учетные записи пользователей играют важнейшую роль в администрировании предприятии. К таким ролям можно отнести:

- Удостоверение личности пользователей, так как созданная учетная запись позволяет входить на компьютеры и в домены именно с теми данными, подлинность которых проверяет домен;
- Разрешения доступа к ресурсам домена, которые назначаются пользователю для предоставления доступа к доменным ресурсам на основании явных разрешений.

Объекты учетных записей пользователей можно отнести к самым распространенным объектам в Active Directory. Именно пользовательским учетным записям администраторы обязаны уделять особое внимание, так как пользователям свойственно приходить работать в организацию, перемещаться между отделами и офисами, жениться, выходить замуж, разводиться и даже увольняться из компании. Такие объекты представляют собой набор атрибутов, причем только одна пользовательская учетная запись может содержать свыше 250 различных атрибутов, что в несколько раз превышает количество атрибутов на рабочих станциях и компьютеров, работающих под операционной системой Linux. Во время создания учетной записи пользователя создается ограниченный набор атрибутов, а уже потом вы можете добавлять такие пользовательские учетные данные как организационные сведения, адреса проживания пользователей, телефонные номера и многое другое. Поэтому важно обратить внимание на то, что одни атрибуты являются обязательными, а остальные – опциональными.

Создание пользователей при помощи оснастки «Active Directory – пользователи и компьютеры»

В подавляющем большинстве случаев системные администраторы для создания основных принципалов безопасности предпочитают использовать оснастку «Active Directory – пользователи и компьютеры», которая добавляется в папку «Администрирование» сразу после установки роли «Доменные службы Active Directory» и повышения сервера до контролера домена. Этот метод является наиболее

удобным, так как для создания принципалов безопасности используется графический пользовательский интерфейс и мастер создания учетных записей пользователя очень прост в применении. К недостатку данного метода можно отнести тот момент, что при создании учетной записи пользователя вы не можете сразу задать большинство атрибутов, и вам придется добавлять необходимые атрибуты путем редактирования учетной записи. Для того чтобы создать пользовательскую учетную запись, выполните следующие действия:

- Откройте оснастку «Active Directory – пользователи и компьютеры». Для этого вам нужно открыть панель управления, в ней открыть раздел «Система и безопасность», затем «Администрирование» и в появившемся окне открыть оснастку «Active Directory – пользователи и компьютеры». Также вы можете воспользоваться комбинацией клавиш +R для открытия диалога «Выполнить» и в диалоговом окне «Выполнить», в поле «Открыть» ввести *dsa.msc*, а затем нажать на кнопку «ОК»;
- В дереве оснастки, разверните узел своего домена и перейдите к подразделению, в котором будет создаваться пользовательская учетная запись. Для создания пользовательских учетных записей рекомендуется создавать дополнительные подразделения, после чего добавлять учетные записи пользователей в подразделения, отличающиеся от стандартного подразделения Users. Щелкните на этом подразделении правой кнопкой мыши и из контекстного меню выберите команду «Создать», а затем «Пользователь», как показано на следующей иллюстрации:
- В появившемся диалоговом окне «Новый объект - Пользователь» введите следующую информацию:
- В поле «Имя» введите имя пользователя;
- В поле «Инициалы» введите его инициалы (чаще всего инициалы не используются);
- В поле «Фамилия» введите фамилию создаваемого пользователя;
- Поле «Полное имя» используется для создания таких атрибутов создаваемого объекта, как основное имя (Common Name) CN и отображения свойств имени. Это поле должно быть уникальным во всем домене, и заполняется автоматически, а изменять его стоит лишь в случае необходимости;
- Поле «Имя входа пользователя» является обязательным и предназначено для имени входа пользователя в домен. Здесь вам нужно ввести имя пользователя и из раскрывающегося списка выбрать суффикс UPN, который будет расположен после символа @;
- Поле «Имя входа пользователя (Пред-Windows 2000)» предназначено для имени входа для систем, предшествующих операционной системе Windows 2000. В последние годы в организациях все реже встречаются обладатели таких систем, но поле обязательно, так как некоторое программное обеспечение для идентификации пользователей использует именно этот атрибут;

После того как заполните все требуемые поля, нажмите на кнопку «Далее»:

На следующей странице мастера создания пользовательской учетной записи вам предстоит ввести начальный пароль пользователя в поле «Пароль» и подтвердить его в поле «Подтверждение». Помимо этого, вы можете выбрать атрибут, указывающий на то, что при первом входе пользователя в систему пользователь должен самостоятельно изменить пароль для своей учетной записи. Лучше всего использовать эту опцию в связке с локальными политиками безопасности «Политика паролей», что позволит создавать надежные пароли для ваших пользователей. Также, установив флажок на опции «Запретить смену пароля пользователем» вы предоставляете пользователю свой пароль и запрещаете его изменять. При выборе опции «Срок действия пароля не ограничен» у пароля учетной записи пользователя срок действия пароля никогда не истечет и не будет необходимости в его периодическом изменении. Если вы установите флажок «Отключить учетную запись», то данная учетная запись будет не предназначена для дальнейшей работы и пользователь с

такой учетной записью не сможет выполнить вход до ее включения. Данная опция, как и большинство атрибутов, будет рассмотрена в следующем разделе данной статьи. После выбора всех атрибутов, нажмите на кнопку «Далее». Эта страница мастера изображена на следующей иллюстрации:

На последней странице мастера вы увидите сводную информацию о введенных вами параметрах. Если информация внесена корректно, нажмите на кнопку «Готово» для создания пользовательской учетной записи и завершения работы мастера.

Создание пользователей на основании шаблонов

Обычно в организациях существует множество подразделений или отделов, в которые входят ваши пользователи. В этих подразделениях пользователи обладают схожими свойствами (например, название отдела, должности, номер кабинета и пр.). Для наиболее эффективного управления учетными записями пользователей из одного подразделения, например, используя групповые политики, целесообразно их создавать внутри домена в специальных подразделениях (иначе говоря, контейнерах) на основании шаблонов. Шаблоном учетной записи называется учетная запись, впервые появившаяся еще во времена операционных систем Windows NT, в которой заранее заполнены общие для всех создаваемых пользователей атрибуты. Для того чтобы создать шаблон учетной записи пользователя, выполните следующие действия:

Откройте оснастку «Active Directory – пользователи и компьютеры» и создайте стандартную учетную запись пользователя. При создании такой учетной записи желательно чтобы в списке пользователей в подразделении имя данной записи выделялось из общего списка, и всегда было расположено на видном месте. Например, чтобы такая учетная запись всегда находилось первой, задайте для создаваемого шаблона имя с нижними подчеркиваниями, например, _Маркетинг_. Также, на странице ввода пароля установите флажок «Отключить учетную запись». Так как эта запись будет использоваться только в качестве шаблона, она должна быть отключена;

В области сведений оснастки выберите созданную вами учетную запись (значок объекта данной учетной записи будет содержать стрелку, направленную вниз, что означает, что данная учетная запись отключена), нажмите на ней правой кнопкой мыши и из контекстного меню выберите команду «Свойства»;

Для того чтобы некоторые атрибуты продублировались в свойствах учетных записей пользователей, которые в последствии будут создаваться на основании вашего шаблона, нужно заполнить необходимые для вас поля в свойствах шаблона учетной записи. Вкладки, которые чаще всего используются при редактировании свойств учетных записей, предоставлены ниже:

- Общие. Данная вкладка предназначена для заполнения индивидуальных пользовательских атрибутов. К этим атрибутам относятся имя пользователя и его фамилия, краткое описания для учетной записи, контактный телефон пользователя, номер комнаты, его электронный ящик, а также веб-сайт. Ввиду того, что данная информация является индивидуальной для каждого отдельного пользователя, данные заполненные на этой вкладке не копируются;
- Адрес. На текущей вкладке вы можете заполнить почтовый ящик, город, область, почтовый индекс и страну, где проживают пользователи, которые будут созданы на основании данного шаблона. Так как у каждого пользователя названия улиц обычно не совпадают, данные из этого поля не подлежат копированию;
- Учетная запись. В этой вкладке вы можете указать точно время входа пользователя, компьютеры, на которые смогут заходить пользователи, такие параметры учетных записей как хранение паролей, типы шифрования и пр., а также срок действия учетной записи;
- Профиль. Текущая вкладка позволяет вам указать путь к профилю, сценарий входа, локальный путь к домашней папке, а также сетевые диски, на которых будет размещена домашняя папка учетной записи;

- Организация. На этой вкладке вы можете указать должность сотрудников, отдел, в котором они работают, название организации, а также имя руководителя отдела;
- Члены групп. Здесь указывается основная группа и членство в группах.

Это основные вкладки, которые заполняются при создании шаблонов учетной записи. Помимо этих шести вкладок, вы можете еще заполнять информацию в 13 вкладках. Большинство из этих вкладок будут рассмотрены в последующих статьях данного цикла.

На следующем шагу создается учетная запись пользователя, основанная на текущем шаблоне. Для этого нажмите правой кнопкой мыши на шаблоне учетной записи и из контекстного меню выберите команду «Копировать»;

В диалоговом окне «Копировать объект - Пользователь» введите имя, фамилию, а также имя входа пользователя. На следующей странице введите пароль и подтверждение, а также снимите флажок с опции «Отключить учетную запись». Завершите работу мастера;

После создания учетной записи перейдите в свойства созданной учетной записи и просмотрите добавляемые вами свойства в шаблон. Отконфигурированные атрибуты будут скопированы в новую учетную запись.

Создание пользователей средствами командной строки

Как и в большинстве случаев, в операционной системе Windows есть утилиты командной строки с аналогичными функциями графического пользовательского интерфейса оснастки «Active Directory – пользователи и компьютеры». Такие команды называются командами DS, так как они начинаются с букв DS. Для создания принципалов безопасности используется команда Dsadd. После самой команды указываются модификаторы, которые определяют тип и имя DN объекта. В случае с созданием учетных записей пользователей вам нужно указать модификатор user, который является типом объекта. После типа объекта необходимо ввести DN имя самого объекта. DN (Distinguished Name) объекта является результирующим набором, который содержит отличительное имя. Следом за DN обычно указывают имя пользователя UPN или имя входа предыдущих версий Windows. Если в имени DN присутствуют пробелы, то такое имя нужно заключить в кавычки. Синтаксис команды, следующий:

Dsadd user DN_имя –samid имя_учетной_записи –UPN_имя –pwd пароль –дополнительные параметры

С данной командой можно использовать 41 параметр. Рассмотрим самые распространенные из них:

- -samid – имя учетной записи пользователя;
- -upn – имя входа пользователя пред-Windows 2000;
- -fn – имя пользователя, которое в графическом интерфейсе заполняется в поле «Имя»;
- -mi – инициал пользователя;
- -ln – фамилия пользователя, указываемая в поле «Фамилия» мастера создания пользовательской учетной записи;
- -display – указывает полное имя пользователя, которое автоматически генерируется в пользовательском интерфейсе;
- -empid – код сотрудника, который создается для пользователя;
- -pwd – параметр, определяющий пользовательский пароль. В том случае, если вы укажете символ звездочки (*), вам будет предложено ввести пароль пользователя в защищенном от просмотра режиме;
- -desc – краткое описание для пользовательской учетной записи;
- -memberof – параметр, определяющий членство пользователя в одной или нескольких группах;
- -office – местонахождения офиса, где работает пользователь. В свойствах учетной записи этот параметр можно найти во вкладке «Организация»;
- -tel – номер контактного телефона текущего пользователя;

- -email – адрес электронной почты пользователя, который можно найти во вкладке «Общие»;
- -hometel – параметр, указывающий номер домашнего телефона пользователя;
- -mobile – телефонный номер мобильного пользователя;
- -fax – номер факсимильного аппарата, который использует текущий пользователь;
- -title – должность пользователя в данной организации;
- -dept – этот параметр позволяет указать наименование отдела, в котором работает данный пользователь;
- -company – название компании, в которой работает создаваемый пользователь;
- -hmdir – основной каталог пользователя, в котором будут расположены его документы;
- -hmdrv – путь к сетевому диску, на котором будет размещена домашняя папка учетной записи
- -profile – путь профиля пользователя;
- -mustchpwd – данный параметр указывает на то, что при последующем входе в систему пользователь обязан изменить свой пароль;
- -canchpwd – параметр, определяющий, должен ли пользователь изменять свой пароль. Если значением параметра указано «yes», то у пользователя будет возможность изменения пароля;
- -reversiblepwd – текущий параметр определяет хранение пароля пользователя с применением обратного шифрования;
- -pwdneverexpires – параметр, указывающий на то, что срок действия пароля никогда не истечет. Во всех этих четырех параметрах, значениями могут выступать только «yes» или «no»;
- -acctexpires – параметр, определяющий, через сколько дней срок действия учетной записи истечет. Положительное значение представляет собой количество дней, через которое учетная запись истечет, а отрицательное означает, что срок действия уже закончен;
- -disabled – указывает, что учетная запись уже отключена. Значениями для этого параметра также выступают «yes» или «no»;
- -q – указание тихого режима для обработки команды.
- Пример использования:

Dsadd user “cn=Алексей Смирнов,OU=Маркетинг,OU=Пользователи,DC=testdomain,DC=com” -samid Alexey.Smirnov -upn Alexey.Smirnov
-pwd * -fn Алексей -ln Смирнов -display “Алексей Смирнов” -tel “743-49-62” -email Alexey.Smirnov@testdomain.com -dept Маркетинг
-company TestDomain -title Маркетолог -hmdir \\dc\profiles\Alexey.Smirnov -hmdrv X -mustchpwd yes -disabled no

Еще одна утилита командной строки CSVDE позволяет импортировать или экспортировать объекты Active Direcoty, представленные в виде cvd-файла – текстового файла с разделительными запятыми, которые можно создавать при помощи табличного процессора Microsoft Excel или простейшего текстового редактора Блокнот. В этом файле каждый объект представляется одной строкой и должен содержать атрибуты, которые перечислены в первой строке. Стоит обратить внимание на то, что при помощи данной команды вы не можете импортировать пользовательские пароли, то есть, сразу после завершения операции импорта пользовательские учетные записи будут отключены. Пример такого файла, следующий:

Синтаксис команды, следующий: Csvde –i –f filename.csv –k
где:

- -i. Параметр, который отвечает за режим импорта. Если вы не укажите данный параметр, то эта команда будет использовать по умолчанию режим экспорта;
- -f. Параметр, идентифицирующий имя файла, которое предназначено для импорта или экспорта;
- -k. Параметр, предназначенный для продолжения импорта пропуская все возможные ошибки;
- -v. Параметр, используя который вы можете вывести подробную информацию;
- -j. Параметр, отвечающий за расположение файла журнала;
- -u. Параметр, позволяющий использовать режим Юникода.

Пример использования команды: Csvde -i -f d:\testdomainusers.csv -k

Импорт пользователей средствами LDIFDE

Утилита командной строки Ldifde позволяет также импортировать или экспортировать объекты Active Directory, используя файловый формат LDIF (Lightweight Directory Access Protocol Data Interchange File). Данный файловый формат состоит из блока строк, которые образуют конкретную операцию. В отличие от файлов CSV, в данном файловом формате каждая отдельная строка представляет собой набор атрибутов, после которого следует двоеточие и само значение текущего атрибута. Также как и в CSV файле, первой строкой обязан быть атрибут DN. За ним следует строка changeType, которая указывает тип операции (add, change или delete). Для того чтобы научиться разбираться в этом файловом формате, вам нужно выучить по крайней мере ключевые атрибуты принципалов безопасности. Пример предоставлен ниже:

```
dn: CN=Иван Котов,ou=Маркетинг,ou=Пользователи,dc=testdomain,dc=com
changetype: add
objectClass: user
CN: Иван Котов
sAMAccountName: Ivan.Kotov
userPrincipalName: Ivan.Kotov
givenName: Иван
sn: Котов
displayName: Иван Котов
mail: Ivan.Kotov@testdomain.com
titile: Маркетолог
department: Маркетинг
```

Контрольные вопросы

1. Для чего служит утилита Ldifde
2. Для чего сужит утилита Active Directory
3. Кто такие контроллеры доменов

Оформление отчета:

1. Цель работы.
2. Постановка задачи.
3. Подробное описание технологии выполнения каждого пункта задания, подкрепленное изображением.
4. Вывод.

Министерство образования и науки Российской Федерации
федеральное государственное бюджетное образовательное учреждение высшего образования
"Российский экономический университет имени Г.В. Плеханова"
МОСКОВСКИЙ ПРИБОРОСТРОИТЕЛЬНЫЙ ТЕХНИКУМ

ПРАКТИЧЕСКАЯ РАБОТА № 21
ДИСЦИПЛИНА: ОПЕРАЦИОННЫЕ СИСТЕМЫ

Тема: WindowsServer: Осуществление системного администрирования локальных сетей.

Специальность: 09.02.03 «Программирование в компьютерных системах»
Квалификация: техник-программист

Цель работы: Изучить задачи администратора и инструментарий, применяемый для их решения. Получение навыков по применению механизмоврезервного копирования и восстановления.

Время выполнения работы: 2 академических часа.

Теоретические сведения:

Введение в Windows Server 2003

Система Windows Server 2003 — это развитие системы Windows 2000. Для администраторов, работающих с сетями Windows 2000, развертывание этой новой версии Windows не станет сложной задачей, поскольку основы изменились не слишком сильно. Для администраторов, работающих с сетями Windows NT, эта превосходно настроенная версия корпоративной операционной системы Microsoft содержит столько инструментов администрирования и средств управления, что у них не найдется причин для того, чтобы продолжать работать с NT.

Версии Windows Server 2003

Windows Server 2003 поставляется в виде следующих четырех версий (изданий):

Windows Server 2003, Standard Edition, разработана для предоставления служб и ресурсов другим системам в сети. Она сменила Windows NT 4.0 Server и Windows 2000 Server. Эта ОС обладает богатым набором функций и конфигурационных параметров. Windows Server 2003 поддерживает до двух центральных процессоров и до 4 Гбайт оперативной памяти.

Windows Server 2003, Enterprise Edition, расширяет возможности Windows Server 2003, Standard Edition, обеспечивая поддержку служб кластеров, служб метакаталогов и служб для Macintosh. В ней также поддержи каются 64-разрядные процессоры Intel Itanium, оперативная память с возможностью ≪горячей≫ замены и неоднородный доступ к памяти (nonuniform memory access, NUMA). Эта версия поддерживает до 32 Гбайт оперативной памяти на процессорах x86, до 64 Гбайт оперативной памяти на процессорах Itanium и до 8 центральных процессоров.

Windows Server 2003, Datacenter Edition, — самый надежный Windows-сервер. Эта версия поддерживает более сложную кластеризацию и способна работать с большими объемами оперативной памяти — до 64 Гбайт на процессорах x86 и до 128 Гбайт на процессорах Itanium. Минимальное количество процессоров для работы Datacenter Edition — 8, максимальное — 32.

Windows Server 2003, Web Edition, предназначена для запуска служб Web при развертывании Web-узлов и Web-приложений. Для решения этих задач в данную версиювключены Microsoft .NET Framework, Microsoft Internet Information Sendees (IIS), AS P.NET и функции для равномерного распределения нагрузки на сеть, Многие другие функции, в частности Active Directory, в ней отсутствуют. Строго говоря, из стандартной компоненты Windows в этой версии предусмотрены лишь распределенная файловая система DFS, шифрованная файловая система EFS и удаленный рабочий стол. Версия Windows Server 2003, Web Edition, поддерживает до 2 Гбайт оперативной памяти и до двух центральных процессоров.

Все версии поддерживают одни и те же базовые функции и средства администрирования. Т. е. методики, описанные в этой книге, можно применять независимо от того, какой версией Windows Server 2003 вы пользуетесь. Помните, что в версии Web Edition нет Active Directory, поэтому сервер, работающий под управлением этой версии, нельзя сделать контроллером домена. Он, тем не менее, может быть частью домена Active Directory.

Различия в администрировании

Сети Microsoft Windows поддерживают две модели служб каталогов: рабочую группу (workgroup) и домен (domain).

- Рабочие группы — это свободные объединения компьютеров, в которых каждый компьютер управляется независимо.

- Домены — это объединения компьютеров, коллективно управляемых с помощью контроллеров домена, т. е. систем Windows Server 2003, регулирующих доступ к сети, базе данных каталога и общим ресурсам.

Для организаций, внедряющих Windows Server 2003, модель домена наиболее предпочтительна. Модель домена характеризуется единым каталогом ресурсов предприятия — Active Directory, — которому доверяют все системы безопасности, принадлежащие домену. Поэтому такие системы способны работать с субъектами безопасности (учетными записями пользователей, групп и компьютеров) в каталоге, чтобы обеспечить защиту ресурсов. Служба Active Directory, таким образом, играет роль идентификационного хранилища и сообщает «кто есть, кто» в этом домене.

Впрочем, Active Directory — не просто база данных. Это коллекция файлов, включая журналы транзакций и системный том (Sysvol), содержащий сценарии входа в систему и сведения о групповой политике. Это службы, поддерживающие и использующие БД, включая протокол LDAP (Lightweight Directory Access Protocol), протокол безопасности Kerberos, процессы репликации и службу FRS (File Replication Service). БД и ее службы устанавливаются на один или несколько контроллеров домена. Контроллер домена назначается Мастером установки Active Directory, который можно запустить с помощью Мастера настройки сервера или командой DCPROMO из командной строки. После того как сервер становится контроллером домена, на нем хранится копия (реплика) Active Directory, и изменения БД на любом контроллере реплицируются на все остальные контроллеры домена.

Домены, деревья и леса

Active Directory не может существовать без домена и наоборот. Домен — это основная административная единица службы каталогов. Однако предприятие может включить в свой каталог Active Directory более одного домена. Когда несколько моделей доменов совместно используют непрерывное пространство имен DNS, они образуют логические структуры, называемые деревьями (tree). Например, домены contoso.com, us.contoso.com и europe.contoso.com совместно используют непрерывное пространство имен DNS и, следовательно, составляют дерево.

Домены Active Directory с разными корневыми доменами образуют несколько деревьев. Они объединяются в самую большую структуру Active Directory — лес (forest). Лес Active Directory содержит все домены в рамках службы каталогов. Лес может состоять из нескольких доменов в нескольких деревьях или только из одного домена. Когда доменов несколько, приобретает важность компонент Active Directory, называемый глобальным каталогом (global catalog): он предоставляет информацию об объектах, расположенных в других доменах леса.

Групповая политика

Организационные подразделения (ОП) также используются для объединения одинаково настроенных объектов — компьютеров и пользователей. Групповая политика Active Directory позволяет централизованно управлять практически любыми конфигурационными изменениями системы. С ее помощью можно указать настройки безопасности, развернуть ПО и настроить поведение ОС и приложений, даже не прикасаясь к компьютерам пользователей. Вы просто реализуете свою конфигурацию в рамках одного объекта групповой политики (ОГП).

ОГП состоят из сотен возможных конфигурационных параметров: от прав и привилегий пользователя до ПО, которое разрешено запускать на системе. ОГП подключается к контейнеру внутри Active Directory (обычно к ОП, но может и к доменам или даже сайтам), и после этого его настройки распространяются на всех пользователей и компьютеры внутри этого контейнера.

Любой сервер может поддерживать одну или более следующих ролей.

- Контроллер домена (Domain controller) — сервер, на котором работают службы каталогов и располагается хранилище данных каталога. Контроллеры домена также

отвечают за вход в сеть и поиск в каталоге. При выборе этой роли на сервере будут установлены DNS и Active Directory. Почтовый сервер (POPS, SMTP) [Mail server (POP3, SMTP)] - сервер, на котором работают основные почтовые службы POP3 (Post Office Protocol 3) и SMTP (Simple Mail Transfer Protocol), благодаря чему почтовые POP3-клиенты домена могут отправлять и получать электронную почту. Выбрав эту роль, вы определяете домен по умолчанию для обмена почтой и создаете почтовые ящики. Эти службы удобны в небольших компаниях или при удаленном соединении, когда электронная почта необходима, но вполне может обойтись без функциональности Microsoft Exchange Server.

Сервер печати (Print, server) — сервер, организующий доступ к сетевым принтерам и управляющий очередями печати и драйверами принтеров. Выбор этой роли позволит вам быстро настроить параметры принтеров и драйверов.

Сервер потоков мультимедиа (Streaming media server) — сервер, предоставляющий мультимедийные потоки другим системам сети или Интернета. Выбор этой роли приводит к установке служб Windows Media. Эта роль поддерживается только в версиях Standard Edition и Enterprise Edition.

Сервер приложений (Application server) — сервер, на котором выполняются Web-службы XML, Web-приложения и распределенные приложения. При назначении серверу этой роли на нем автоматически устанавливаются IIS, COM+ и Microsoft .NET Framework. При желании вы можете добавить к ним серверные расширения Microsoft FrontPage, а также включить или выключить ASP.NET.

Сервер терминалов (Terminal Server) — сервер, выполняющий задачи для клиентских компьютеров, которые работают в режиме терминальной службы. Выбор этой роли приводит к установке Terminal Server. Для удаленного управления сервером устанавливать Terminal Server не нужно. Необходимый для этого удаленный рабочий стол (Remote Desktop) устанавливается автоматически вместе с ОС.

Сервер удаленного доступа или VPN-сервер (Remote access/VPN server) — сервер, осуществляющий маршрутизацию сетевого трафика и управляющий телефонными соединениями и соединениями через виртуальные частные сети (virtual private network, VPN). Выбрав эту роль, вы запустите Мастер настройки сервера маршрутизации и удаленного доступа (Routing and Remote Access Server Setup Wizard). С помощью параметров маршрутизации и удаленного доступа вы можете разрешить только исходящие подключения, входящие и исходящие подключения или полностью запретить доступ извне.

Узел кластера серверов (Server cluster node) — сервер, действующий в составе группы серверов, объединенных в кластер. Выбор этой роли приводит к запуску Мастера создания кластера (New Server Cluster Wizard), позволяющего создать новую кластерную группу, или Мастера добавления узлов (Add Nodes Wizard), который поможет добавить сервер к существующему кластеру. Эта роль поддерживается только в версиях Enterprise Edition и Datacenter Edition.

Файл-сервер (File server) — сервер, предоставляющий доступ к файлам и управляющий им. Выбор этой роли позволит вам быстро настроить параметры квотирования и индексирования. Вы также можете установить Web-приложен и для администрирования файлов. В этом случае будет установлен IIS и включены страницы ASP (Active Server Pages).

DHCP-сервер (DHCP Server) — сервер, на котором запущен DHCP (Dynamic Hose Configuration Protocol), позволяющий автоматизировать назначение IP-адресов клиентам сети. При выборе этой роли на сервере будет установлен DHCP и запущен Мастер создания области (New Scope Wizard).

DNS-сервер (DNS Server) — сервер, на котором запущена служба DNS, разрешающая имена компьютеров в IP-адреса и наоборот. При выборе этой роли на сервере будет установлена DNS и запущен Мастер настройки DNS-сервера (Configure DNS Server Wizard).

WINS-сервер (WINS server) — сервер, на котором запущена служба WINS (Windows Internet Name Service), разрешающая имена NetBIOS в IP-адреса и наоборот. Выбор этой роли приводит к установкеWINS.

Управление выбранными ролями сервера осуществляется с помощью программы Управление данным сервером (Manage Your Server), в окне которой сосредоточены все основные инструменты для управления Windows Server 2003. В частности, здесь перечислены текущие роли сервера. Чтобы открыть это окно, воспользуйтесь меню Администрирование (Administrative Tools).

Таблица 1. Краткий справочник основных средств администрирования Windows Server 2003

Средство администрирования	**Назначение**
Active Directory — домены и доверие (Active Directory Domains and Trusts)	Управление доверительными отношениями между доменами
Active Directory — пользователи и компьютеры (Active Directory Users and Computers)	Управление пользователями, группами, компьютерами и другими объектами Active Directory
Active Directory — сайты и службы (Active Directory Sites and Service)	Создание сайтов для управления репликацией Active Directory
DHCP	Конфигурация и управление службой DHCP
DNS	Управление службой системы доменных имен (DNS)
WINS	Управление службой WINS, преобразующей имена NetBIOS в IP-адреса
Администратор кластеров (Cluster Administrator)	Управление службой Cluster
Администратор серверных расширений (Server Extensions Administrator)	Управление серверными расширениями, например FrontPage
Внешнее хранилище (Remote Storage)	Управление службой Remote Storage
Диспетчер служб Интернета (Internet Information Services Manager)	Управление Web-, FTP- и SMTP-серверами
Диспетчер служб терминалов (Terminal Services Manager)	Управление и МОЕНПЧЛШНГ пользователей, сеансов и процессов Terminal Service
Источники данных (ODBC) [Data Sources (ODBC)]	Добавление, удаление и настройка источников данных и драйверов ODBC (Open Database Connectivity)
Контроль допуска QpS (QoS Admission Control)	Управление службой Quality of Service(QpS) Admissions Control для регулировки пропускной способности сети
Лицензирование (Licensing)	Управление лицензированием доступа клиентов к серверным продуктам
Маршрутизация и удаленный доступ к сети (Routing and Remote Access)	Конфигурация и управление службой Routing and Remote Access, контролирующей интерфейсы маршрутизации, динамическую IP-маршрутизацию и удаленный доступ
Настройка сервера (Configure Your Server)	Добавление, удаление и конфигурация служб Windows для сети

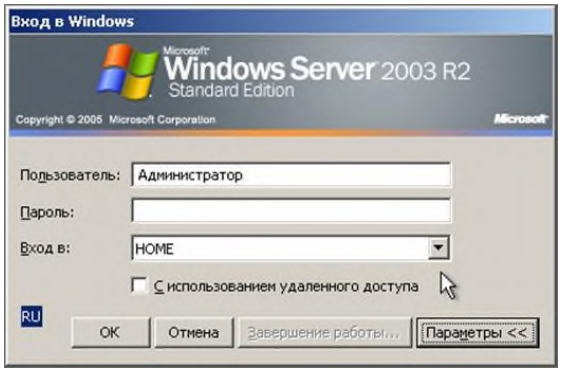
Настройка служб терминалов (Terminal Services Configuration)	Управление настройкой протокола Terminal Service и параметрами сервера
Пакет администрирования диспетчера подключений (Connection Manager Administration Kit)	Конфигурирование и настройка диспетчера подключений
Политика безопасности домена (Domain Security Policy)	Просмотр и редактирование политики безопасности в домене
Политика безопасности контроллера домена (Domain Controller Security Policy)	Просмотр и редактирование политики безопасности для организационного полразделения контроллера домена
Производительность (Performance)	Отображение графиков производительности системы и настройка журналов и сигналов оповещения
Просмотр событий (Event Viewer)	Управление событиями и журналами
Распределенная файловая система DIFS (Distributed File System)	Создание и управление распределенными файловыми системами, объединяющими общие папки из разных компьютеров
Сетевой монитор (Microsoft Network Monitor)	Мониторинг сетевого трафика и устранение неисправностей в сети
Службы (Services)	Управление запуском и настройка служб Windows
Службы компонентов (Component Services)	Конфигурация и управление приложениями COM-, управление событиями и службами
Удаленные рабочие столы (Remote Desktop)	Настройка удаленных подключений и просмотр сеансов удаленных подключений
Управление компьютером(Computer Management)	Запуск и остановка служб, управление дисками и доступ к другим средствами управления системой
Центр сертификации (Certification Authority)	Управление сертификационными службами

Регистрация пользователя в системе

Защиту ресурсов реализуют несколько процессов на разных уровнях операционной системы. Первый из них — механизм регистрации — обеспечивает защиту доступа к домену или компьютеру.

Чтобы получить доступ к ресурсам, пользователям необходимо сначала зарегистрироваться — идентифицировать себя в домене или на компьютере.

При регистрации пользователя, в зависимости от выбранного способа регистрации в системе, появляется диалоговое окно «Операционная система Windows» с текстом «Нажмите Ctrl+Alt+Delete».



Параметры диалогового окна «Вход в Windows».

Таблица 2. Параметры диалогового окна "Вход в Windows"

Параметры	Описание
User Name (Имя)	Введите уникальную учетную запись пользователя, присвоенную Вам администратором. Эта учетная запись должна присутствовать в базе данных каталогов на контроллерах домена, чтобы обеспечивать регистрацию в домене, и в базе данных каталогов локального компьютера — для регистрации на локальном компьютере
Password (Пароль)	Введите пароль, присвоенный указанному Вами имени пользователя, учитывая регистр символов. Чтобы пароль не стал достоянием посторонних, при его вводе символы на экране заменяются звездочками (*)
Domain (Домен)	Чтобы зарегистрироваться в домене, укажите его имя. При попытке регистрации пользователя в домене база данных контроллера домена проверяется на наличие соответствующего элемента. Регистрация по указанной учетной записи разрешается, если введенное имя пользователя, пароль и имя домена соответствуют данным в базе данных контроллера домена. Чтобы зарегистрироваться на локальном компьютере, укажите его имя. Локальный компьютер проверит наличие информации о Вас в локальной базе данных каталогов. Регистрация по указанной учетной записи разрешается, если введенное имя пользователя, пароль и имя компьютера соответствуют данным в локальной базе данных каталогов. Пользователь может зарегистрироваться на локальном компьютере, только указав имя пользователя, имеющееся в локальной базе данных каталогов. Серверы и компьютеры под управлением Windows 2003 содержат встроенные локальные учетные записи*Administrator* (Администратор) и *Guest* (Гость).

Проверка глобальной учетной записи

Когда пользователь щелкнет кнопку **ОК,** компьютер передает имя домена, имя пользователя и пароль контроллеру домена. Последний сначала проверяет имя домена, а затем ищет имя пользователя и пароль в базе данных домена. Далее события могут разворачиваться по одному из трех сценариев.

- Если имя домена указано верно, а имя пользователя и пароль соответствуют имеющейся учетной записи, сервер уведомляет компьютер, что регистрация разрешена.
- Если пользователь указал имя домена, не совпадающее с именем домена контроллера, но контроллер распознает его как имя доверяемого домена, то он передает информацию контроллеру этого домена. Последний выполняет аутентификацию и возвращает соответствующую информацию.
- Если имя домена не совпадает с именем контроллера домена и тот не распознает указанный домен, то контроллер запрещает доступ к домену.

Проверка локальной учетной записи

Когда пользователь щелкает кнопку **ОК,** компьютер сначала проверяет указанное имя компьютера, а затем ищет имя пользователя и пароль в локальной базе данных каталогов. Если имена совпадают, регистрация разрешается, и пользователь получает доступ к локальным ресурсам. Если же нет, пользователь не получает доступ к компьютеру.

Функции администратора Windows 2003

Администрирование Windows NT подразумевает выполнение как специальных операций после установки системы, так и рутинных каждодневных действий.

Функции администратора можно разделить на пять категорий.
Таблица 3. Функции администратора

Категория	Характерные задачи
Администрирование учетных записей пользователей и групп	Планирование, создание и ведение учетных записей пользователей и групп для обеспечения каждому пользователю возможности регистрации в сети и доступа к необходимым ресурсам
Администрирование защиты	Планирование и реализация стратегии безопасности для защиты данных и общих сетевых ресурсов, в том числе папок, файлов и принтеров
Администрирование принтеров	Настройка локальных и сетевых принтеров для обеспечения пользователям доступа к ресурсам печати. Устранение обычных проблем печати
Мониторинг событий и ресурсов сети	Планирование и реализация стратегии аудита событий в сети с целью обнаружения нарушений защиты. Управление ресурсами и контроль их использования
Резервное копирование и восстановление данных	Планирование и выполнение регулярных операций резервного копирования для обеспечения быстрого восстановления важных данных

Средства администратора Windows 2003

Средства администрирования входят в состав Windows 2003 и могут применяться или для администрирования любого компьютера домена, или для администрирования локального компьютера.

Таблица 4. Средства администрирования

Средство	Назначение
Администратор кластеров	Администратор кластеров - это основное средство администрирования и конфигурирования объектов кластера серверов, таких как узлы, группы и другие ресурсы. Это позволяет вам управлять кластером серверов без необходимости физического присутствия в одном из узлов.
Диспетчер балансировки сетевой нагрузки	Обеспечивает балансирование IP-трафика между несколькими серверами. Не обеспечивает переход по отказу (failover) для приложений и данных.
Диспетчер служб терминалов	Позволяет управлять конфигурацией сервера служб терминалов
Конфигурация платформы Microsoft.NET Framework 1.1	Позволяет настраивать среду .NET Framework
Лицензирование	Утилита, позволяющая управлять клиентскими лицензиями в масштабах предприятия

Средство	Назначение
Лицензирование сервера терминалов	Утилита, позволяющая управлять клиентскими лицензиями для служб терминалов (Terminal Services), работающих в режиме выполнения приложений
Маршрутизация и удалённый доступ	Служит для управления маршрутизацией и удаленным доступом
Мастер настройки сервера	Мастер, позволяющий администратору настроить сервер в соответствии с выбранными ролями (файловый сервер, сервер служб Интернета и т. д.)
Производительность	Каждый компьютер с Windows Server 2003 содержит компоненты, мониторинг которых можно выполнять с помощью оснастки Performance (Производительность). Это могут быть аппаратные или программные компоненты, которые выполняют задачи или поддерживают рабочую нагрузку. Многие из этих компонентов имеют показатели, отражающие определенные аспекты их функционирования, которые можно точно измерить как скорость выполнения задач.
Просмотр событий	Служит для просмотра и управления системным журналом, журналами безопасности и приложений
Распределенная файловая системаDFS	Создает и управляет распределенными файловыми системами, объединяющими совместно используемые папки на различных компьютерах
Службы	Запускает, останавливает и конфигурирует службы (сервисы) Windows
Службы компонентов	Конфигурирует и управляет службами компонентов COM+
Удалённые рабочие столы	Позволяет управлять многочисленными сессиями терминального доступа к удаленным компьютерам
Управление данным сервером	Мастер, представляющий собой информационный центр для управления различными ролями сервера, обращения к службам поддержки и вспомогательным инструментам, а также позволяющий быстро находить информацию об обновлениях, способах решения проблем и т. п.
Управление компьютером	Предоставляет функции администрирования системы. Содержит в своем составе ряд изолированных оснасток и оснасток расширения
Центр сертификации	Позволяет работать с центрами сертификации, развернутыми в корпоративной сети
Active Directory - домены и доверие	Служит для управления доменами и доверительными отношениями
Active Directory —сайты и службы	Определяет топологию и расписание репликации Active Directory. Обеспечивает изменение служб корпоративного уровня

Средство	Назначение
Политика безопасности домена	Служит для управления параметрами безопасности (представленными в узле Security Settings объекта групповой политики, привязанного к объекту домена) для всего домена
Политика безопасности контроллера домена	Служит для управления параметрами безопасности (представленными в узле Security Settingsобъекта групповой политики, привязанного к подразделению Domain Controllers) на контроллерах домена

Мониторинг ресурсов

Сведения о системе

Утилита System Information (Сведения о системе) (Winmsd.exe) представляет исчерпывающую информацию об аппаратном обеспечении компьютера, системных компонентах и программной среде. Системная информация разделена на категории, которым в окне структуры соответствуют следующие узлы System Summary (Сведения о системе), Hardware Resources (Ресурсы аппаратуры), Components(Компоненты), Software Environment (Программная среда) и Internet Settings (Параметры Интернета).

Узел System Summary отображает общую информацию о компьютере и операционной системе: версию ОС и номер сборки, тип процессора, объем ОЗУ, версию BIOS, региональные установки, а также информацию об объеме физической и виртуальной памяти на компьютере.

Узел Hardware Resources отображает информацию об аппаратных установках, таких как каналы DMA, номера прерываний (IRQ), адреса ввода/вывода (I/O) и адреса памяти. Узел Conflicts/Sharing (Конфликты/ Совместное использование) идентифицирует устройства, которые совместно используют ресурсы или конфликтуют с другими ресурсами. Такая информация помогает выявлять проблемы, возникающие с аппаратными устройствами.

Узел Components отображает информацию о конфигурации Windows и используется для определения статуса драйверов устройств, сетевых устройств и программного обеспечения мультимедийных устройств. Кроме того, данный узел содержит обширную информацию об истории драйверов с записью всех изменений, которые производились с компонентами.

Узел Software Environment отображает "снимок" программного обеспечения, загруженного в память компьютера. Данная информация может быть использована для просмотра списка выполняющихся задач или для выяснения номера версии продукта.

Узел Internet Settings содержит, в частности, информацию о настройках программы Internet Explorer.

Составление и печать сводки

Информация, предоставляемая программой System Information (Сведения о системе), нужна не только организации, осуществляющей поддержку, — напечатанная сводка может пригодиться службе инвентаризации. Из сводки можно быстро узнать объем оперативной памяти и дискового пространства на конкретном компьютере, а также, какие устройства на нем установлены.

Распечатать постранично или всё целиком можно из меню Файл-> Печать. Сохранить общий отчёт можно из меню Файл-> Экспорт.

Управление компьютером

Инструмент (и одноименная оснастка) Computer Management (Управление компьютером) является одним из основных средств системного администратора для конфигурирования компьютера. Данную оснастку можно использовать для администрирования, как локальной системы, так и удаленных компьютеров (в том числе

систем Windows 2000 и — с некоторыми ограничениями — компьютеров с Windows NT 4.0). Это позволяет администратору со своего рабочего места устранять проблемы и конфигурировать любой компьютер в сети, на котором установлена Windows Server 2003.

Для запуска оснастки Computer Management можно пользоваться двумя способами: выбрать соответствующую команду в меню Start | Administrative Tools или щелкнуть правой кнопкой мыши на команде My Computer (Мой компьютер) в меню Startи выбрать в контекстном меню пункт Manage (Управление).

Просмотр пользовательских сеансов

Оснастка Shared Folders (Общие папки) позволяет просматривать информацию о соединениях и использовании ресурсов локального или удаленного компьютеров. Данная оснастка используется вместо программы Server в Control Panel системы Windows NT 4.0. Оснастка Shared Folders содержит три узла: Shares (Ресурсы), Sessions (Сеансы) и Open Files (Открытые файлы). При выборе данных узлов в панели результатов отображается содержание соответствующего узла.

С помощью оснастки можно выполнять следующие задачи:

создавать, просматривать, изменять свойства и удалять общие ресурсы на локальном или удаленном компьютерах (Windows NT 4.0/2000/XP и Windows Server 2003) и устанавливать разрешения на доступ к ним. Кроме того, можно управлять режимом кэширования общих папок (в случае их использования в качестве изолированных папок). В системах Windows XP и Windows Server 2003 появилась очень удобная новая возможность управления процессом публикации общей папки в каталоге Active Directory— можно сразу после создания общей папки опубликовать ее в каталоге, не прибегая к помощи оснастки Active Directory Users and Computers. Все необходимые действия достаточно очевидны из содержания приведенного примера: в данном случае публикуется общая папка службы факсов, содержащая клиентское программное обеспечение для систем, не имеющих его (например, Windows 9x);

просматривать список удаленных пользователей, подключенных к компьютеру, и отключать их;

просматривать список файлов, открытых удаленными пользователями, и закрывать открытые файлы.

Windows 2003 Backup

Регулярное резервное копирование информации с серверов и локальных жестких дисков предотвращает утрату и повреждение данных из-за поломки жесткого диска, отключения питания, воздействия вирусов и т.д. Резервное копирование при грамотном планировании и наличии надежного оборудования позволяет безболезненно справиться с последствиями катастрофы.

Графическое инструментальное средство Windows 2003 Backup предназначено для автоматического и ручного резервного копирования и восстановления файлов, расположенных на разделах файловых систем FAT и NTFS.

Выбор стратегии резервного копирования

Перед тем как приступать к резервному копированию файлов, нужно разработать стратегию, отвечающую потребностям Вашей организации и гарантирующую восстановление утраченных данных. Эффективное архивирование и восстановление информации — одна из самых важных задач администратора.

Отбор файлов для резервного копирования

По степени важности (а следовательно, и по частоте создания резервных копий) папки и файлы можно разделить на три категории:

- важные — их резервные копии создаются всегда;
- полезные — их резервные копии создаются изредка;
- малозначимые — их резервные копии не создаются никогда.
- Отбирая файлы для резервного копирования, учитывайте следующие правила:
- всегда создавайте резервные копии

- файлов, жизненно важных для работы Вашей организации;
- реестров всех главных и резервных контроллеров домена (каждый контроллер домена имеет свою копию базы данных каталогов; резервное копирование реестра контроллера домена предотвращает потерю информации об учетных записях пользователей и защите).
- резервные копии файлов, изменяемых редко или не представляющих особой ценности, следует создавать лишь время от времени.
- -не сохраняйте временные файлы, так как они постоянно изменяются, и вряд ли могут быть использованы для восстановления данных.

Выбор типа резервного копирования

Windows 2003 Программа архивации (Backup Utility) предлагает пять вариантов резервного копирования: *обычное* (normal), *копирующее* (copy), *инкрементальное* (incremental), *разностное* (differential) и *ежедневное* (daily). Выбор стратегии резервного копирования определяется тем, сколько времени отводится на сохранение данных и каковы требования к скоростям поиска резервных копий и восстановления файлов.

Краткая характеристика перечисленных выше типов резервного копирования приведена в таблице.

Таблица 5. Варианты резервного копирования

Варианты резервного копирования	**Характеристика**
Обычное или полное	Архивирует выбранные файлы и помечает их как сохраненные. Обычное резервное копирование позволяет быстро восстанавливать файлы, так как наиболее свежие файлы находятся на последней ленте. Для создания первой резервной копии всегда следует применять обычное резервное копирование всех файлов
Инкрементальное или добавочное	Архивирует только файлы, созданные или измененные с момента выполнения последнего обычного или инкрементального резервного копирования. Эти файлы помечаются флажком архивации. Если Вы сочетаете обычное и инкрементальное резервное копирование, то воссоздание информации начинается с восстановления последней обычной резервной копии, а затем последовательно восстанавливаются файлы инкрементальных копий
Разностное	Архивирует файлы, созданные или измененные со времени последнего обычного (или инкрементального) резервного копирования. Файлы при этом не помечаются флажком архивации. При комбинации обычного и разностного резервного копирования для восстановления данных требуются лишь 2 ленты: с последней обычной и с последней разностной копиями
Копирующее	Архивирует выбранные файлы, не помечая их флажком архивации. Тем самым не оказывает влияния на операции обычного и инкрементального резервного копирования и может применяться для промежуточного сохранения данных
Ежедневное копирование	Архивирует выбранные, файлы, которые были изменены во время ежедневного копирования. Файлы не помечаются флажком архивации. Эта операция полезна,

	например, когда Вы берете работу на дом и хотите быстро выбрать файлы, над которыми сегодня работали

Журналы резервного копирования

Журнал резервного копирования (backup log) — это текстовый файл, в котором регистрируются операции резервного копирования. Он полезен при восстановлении данных. Его можно либо распечатать, либо посмотреть в любом текстовом редакторе. Журнал хранится на диске, поэтому в случае повреждения каталога архива на ленте обратитесь к нему, чтобы найти нужный файл.

Журнал резервного копирования содержит следующую информацию:

- дату создания архива;
- название варианта резервного копирования;

местонахождение накопителя.

Шаблон плана резервного копирования

Типы резервного копирования:

О = Обычное, Д = Инкрементальное, Р = Разностное, К = Копирующее, ЕК = Ежедневное копирование

Порядок выполнения работы

- Изучить предлагаемый теоретический материал.
- Получить следующую информацию с помощью утилиты System Information (Сведения о системе):
  - свойства компьютера
  - пользовательские сеансы
  - список ресурсов, открытых на сервере
  - Построить отчет с максимальным объемом данных о компьютере (системе).
  - Создать план резервного копирования
  - Выполнить резервное копирование различного типа с помощью программы Backup Utility (**Start** (Пуск) – **Programs** (Программы) -**Accessories** (Стандартные) - **System Tools** (Служебные) - **Backup** (Архивация данных)):
    - Полное
    - Инкрементное
    - Ежедневное
  - Проанализировать журнал резервного копирования. Сделать выводы на основании анализа.

Контрольные вопросы:

Как называется служба, которую позволяет реплицировать данные между файловыми серверами под управлением в Windows Server 2003R2?

что используется для анализа проблем в операционной системе?

как называется объект Active Directory, который хранит информацию об учетных записях, общих ресурсах, подразделениях?

Оформление отчета:

1. Цель работы.
2. Постановка задачи.
3. Подробное описание технологии выполнения каждого пункта задания, подкрепленное изображением.
4. Вывод.