

## Лекция 10. Удаленное администрирование

Учебные вопросы:

1. Инструменты удаленного администрирования
2. Получение информации об удаленной системе

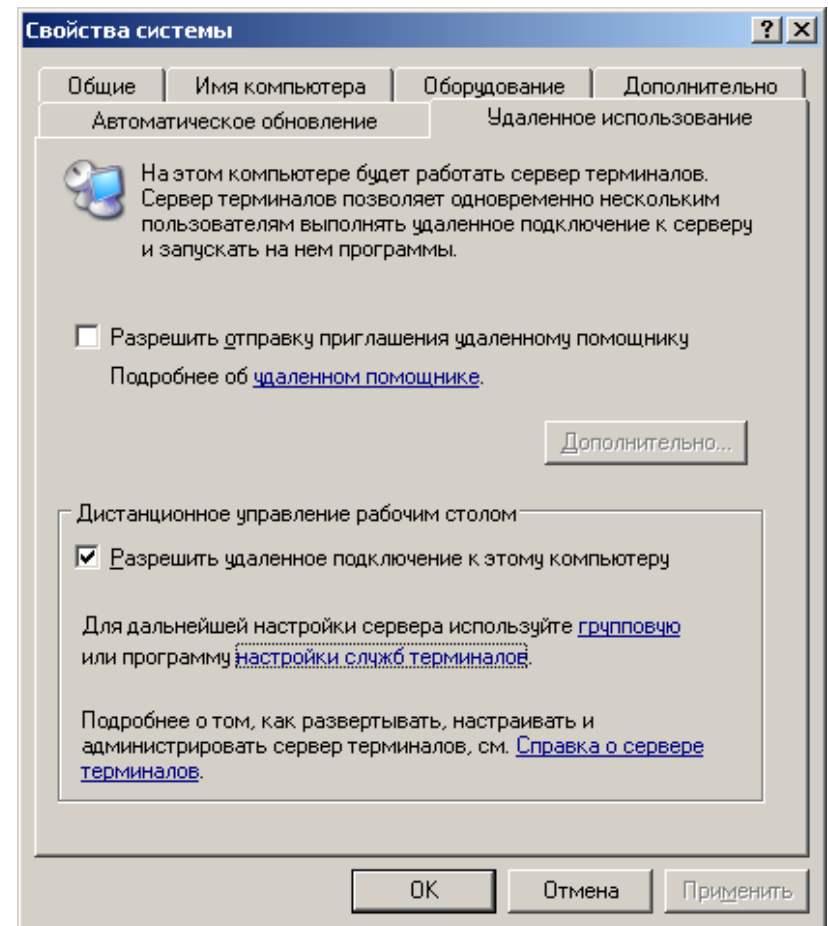
## *1. Инструменты удаленного администрирования*

# Удаленное управление сетевыми ресурсами

- **Удаленное управление** – процесс администрирования компьютера без физического присутствия пользователя за компьютером.
- В состав Windows Server входит ряд средств, обеспечивающих удаленное управление серверов и рабочих станций.
- Для выполнения удаленного управления возможно использование командной строки и графического интерфейса.

# Дистанционное управление рабочим столом

- Инструмент **Дистанционное управление рабочим столом** эквивалентен удаленному администрированию через сервер терминалов, реализованный в Windows.
- Серверная часть данного инструмента производится через закладку **Удаленные сеансы** в **Свойствах системы**. Возможно установить список пользователей, которым будет разрешен доступ к данному компьютеру.
- На клиенте сеансы удаленного управления запускаются с помощью команды **Удаленный рабочий стол**



# Дистанционное управление рабочим столом

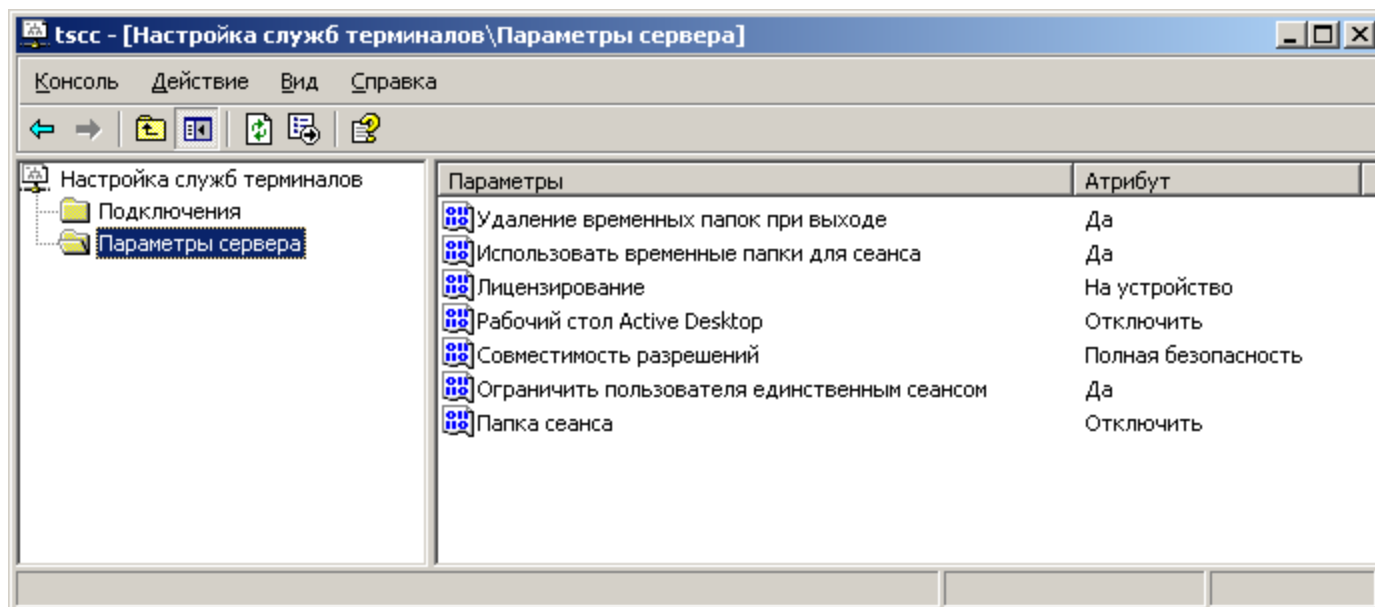
- Инструмент Дистанционное управление рабочим столом можно настроить на использование в качестве клиента веб-браузер, например Internet Explorer.
- Преимущества данного подхода – возможность подключения для администрирования сервера с помощью обычного веб-браузера с машины под управлением версий Windows.

# Сервер терминалов

- Для управления удаленными подключениями к серверу используется несколько инструментов администрирования:
  - Настройка служб терминалов;
  - Диспетчер служб терминалов;
  - Лицензирование сервера терминалов.

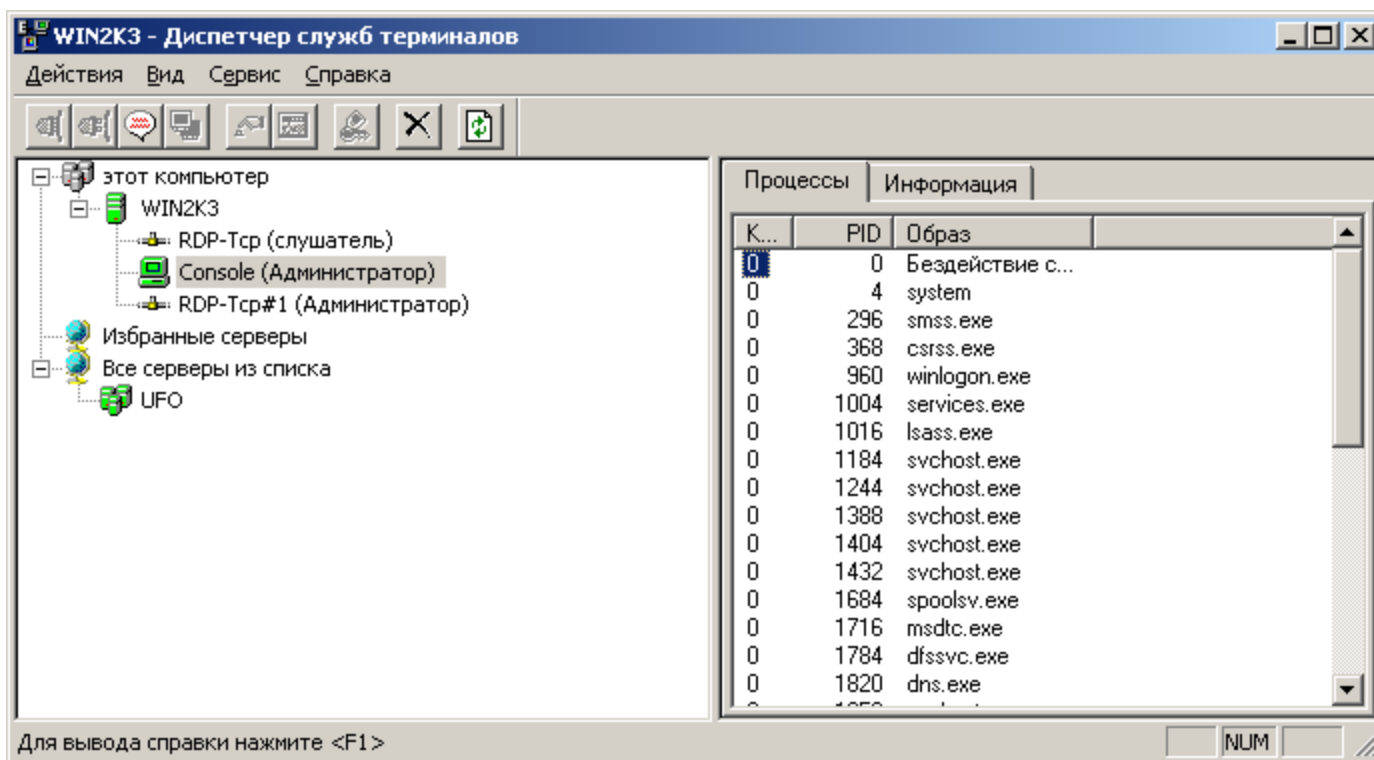
# Настройка служб терминалов

- Данный инструмент позволяет:
  - Создать набор подключений, определяющих сетевые интерфейсы и параметры подключения;
  - Определить параметры сервера, такие как тип лицензирования, ограничения на число сеансов пользователя и так далее.



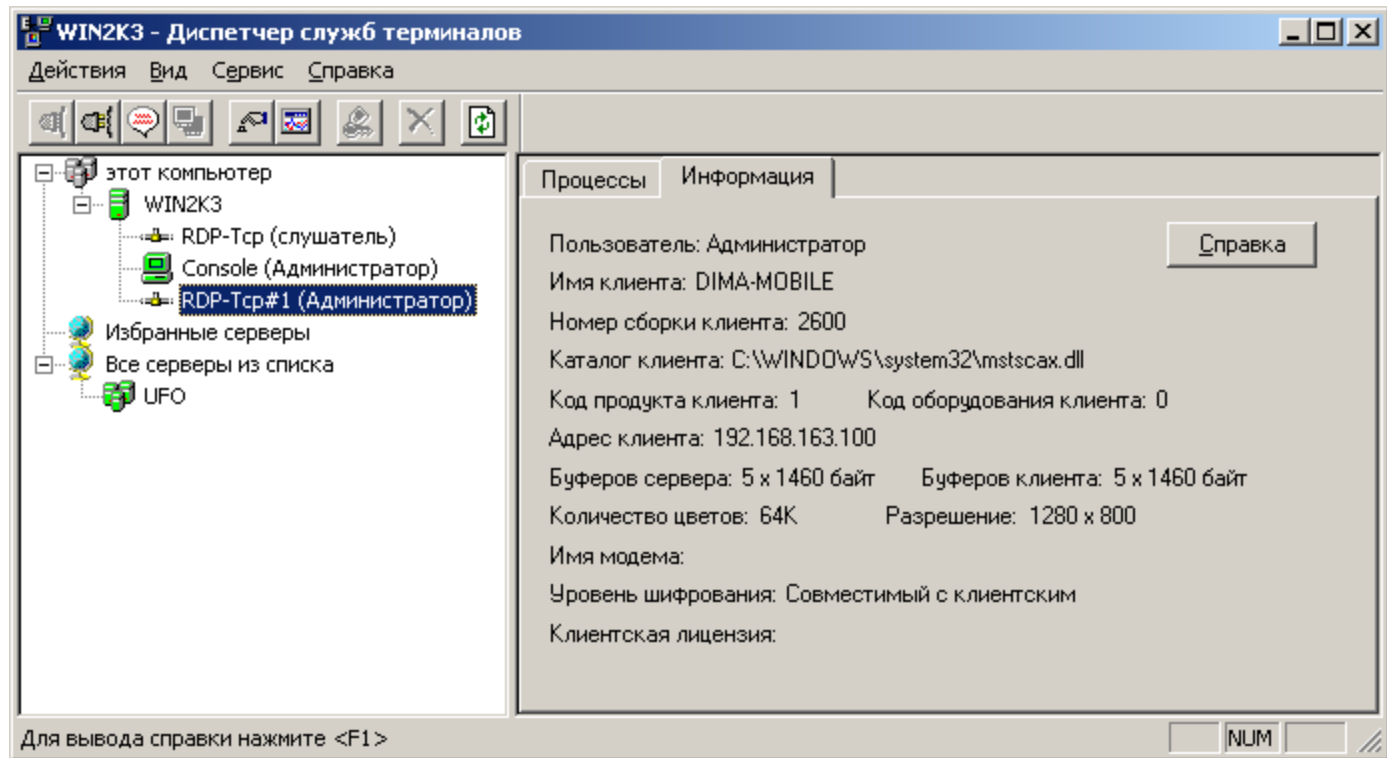
# Диспетчер служб терминалов

- **Диспетчер служб терминалов** позволяет просматривать сведения о серверах терминалов в доверенных доменах.
  - Данная служебная программа используется для наблюдения за пользователями, сеансами и приложениями на каждом сервере терминалов и дает возможность выполнять различные действия для управления сервером.
- С помощью Диспетчера можно просмотреть информацию о запущенных процессах.



# Диспетчер служб терминалов

- Информация о подключенных удаленных пользователях:



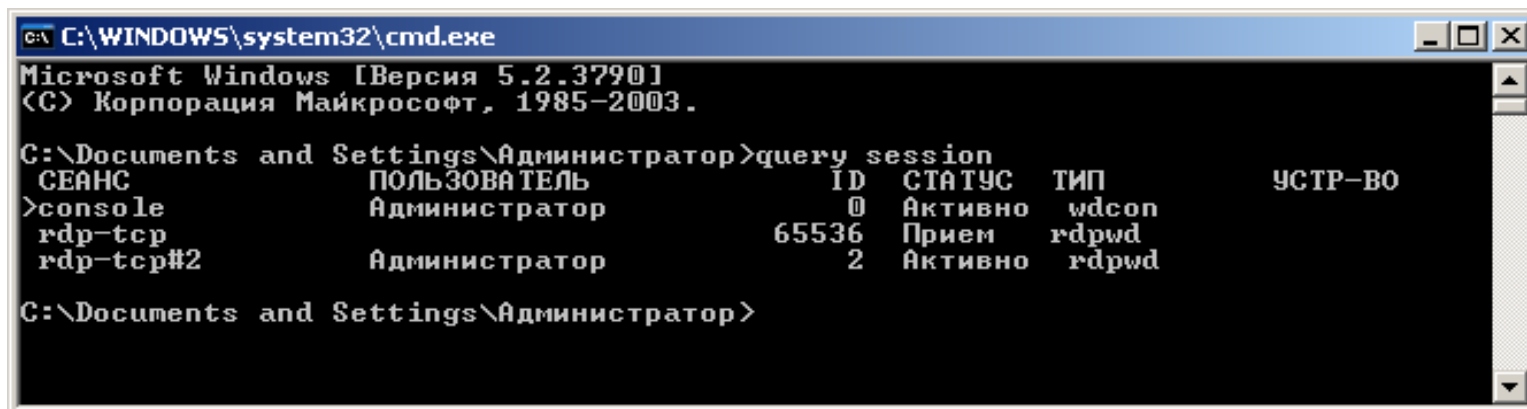


# Использование команд для дистанционного управления рабочим столом

- При каждом подключении к удаленному столу на сервере инициализируется консольный сеанс, обеспечивающий доступ к удаленному рабочему столу.
- Администратор имеет эффективные средства по просмотру и прекращению данных сеансов:
  - `query session` – выводит текущие сеансы на сервере
  - `change logon /disable` – отключает все виды сетевых подключений
  - `change logon /enable` – разрешает подключения к серверу;
  - `logoff <имя сеанса>` – принудительно завершает сеанс на основании его имени
  - `logoff <код сеанса>` – принудительно завершает сеанс на основании его кода

# Командный режим управления

- Примеры управления удаленными подключениями к рабочему столу.
- Дополнительными командами являются:
  - `reset session <код сеанса>` - принудительно закрывает все приложения и завершает сеанс
  - `tsdiscon <код сеанса>` - принудительно разрывает подключение сеанса. Сеанс становится зависшим.



```
C:\WINDOWS\system32\cmd.exe
Microsoft Windows [Версия 5.2.3790]
(C) Корпорация Майкрософт, 1985-2003.

C:\Documents and Settings\Администратор>query session
СЕАНС                ПОЛЬЗОВАТЕЛЬ          ID  СТАТУС  ТИП                УСТР-ВО
>console              Администратор          0   Активно  wdcon
rdp-tcp                65536  Прием        rdpwd
rdp-tcp#2              Администратор          2   Активно  rdpwd

C:\Documents and Settings\Администратор>
```

# Удаленный запуск программ

- Существуют другие способы выполнения административных функций на других компьютерах в сети.
- Данные методы используют сценарии входа, пакетные файлы и реестры для запуска программ.
- Команда для запуска программы на компьютере по расписанию – **at**
  - `at \\<компьютер> <время_суток> <команда>` - назначает время выполнения команды на сетевом компьютере
  - `at \\<компьютер> <время_суток> /EVERY:M|T|W|TH|F|S|SU <команда>` - назначает день недели и время выполнения команды на сетевом компьютере
  - `at \\<компьютер> <время_суток> /INTERACTIVE <команда>` - назначает время выполнения команды на сетевом компьютере, разрешая обмен данными с текущим пользователем

# Удаленный запуск программ

- Для удаленного запуска программ можно использовать и групповые политики.
- При создании групповой политики существует возможность включить запуск сценариев при включении компьютера, при входе/выходе пользователя и при выключении компьютера.
- Сценарии могут представлять собой файлы написанные на различных сценарных языках:
  - Visual Basic Scripting Edition
  - JScript;
  - Windows Script (основан на использовании xml);
  - bat-файл.
- Располагаются файлы сценариев в специальной папке, например:
  - C:\WINDOWS\System32\GroupPolicy\Machine\Scripts\Startup

## 2. Получение информации об удаленной системе

# Информация об удаленной системе

- Системный администратор должен отслеживать используемое программное обеспечение и аппаратные ресурсы компьютеров в сети.
- Вывод системной информации о компьютерах сети осуществляется с помощью команд:
  - `systeminfo /s <компьютер> /u <пользователь> /p <пароль>` - вывод системной информации (быстродействие процессора, версия BIOS, версия Windows и т.п.)
  - `systeminfo /s <компьютер> /u <пользователь> /p <пароль> /fo TABLE|LIST|CSV /NH` - вывод системной информации в формате таблицы, списка, с разделяющими запятыми

# Пример информации об удаленной системе

```
C:\WINDOWS\system32\cmd.exe
Microsoft Windows [Версия 5.2.3790]
(C) Корпорация Майкрософт, 1985-2003.

C:\Documents and Settings\Администратор>systeminfo /s radiowave /u office\wildim
/p

Имя узла:                RADIOWAUE
Название ОС:             Microsoft(R) Windows(R) Server 2003, Standard Ed
ition
Версия ОС:               5.2.3790 Service Pack 1 сборка 3790
Изготовитель ОС:         Microsoft Corporation
Параметры ОС:           Рядовой сервер
Сборка ОС:              Multiprocessor Free
Зарегистрированный владелец: Admin
Зарегистрированная организация: RosNOU
Код продукта:           69890-012-4074175-42909
Дата установки:         05.01.2005, 10:53:02
Время работы системы:   2 дн., 18 час., 22 мин., 31 сек.
Изготовитель системы:    Intel
Модель системы:         SE7210TP1-E
Тип системы:            X86-based PC
Процессор(ы):           Число процессоров - 2.
tel ~3192 МГц           [01]: x86 Family 15 Model 3 Stepping 4 GenuineIn
tel ~3192 МГц           [02]: x86 Family 15 Model 3 Stepping 4 GenuineIn
Версия BIOS:            A M I - 9000408
Папка Windows:          C:\WINDOWS
Системная папка:       C:\WINDOWS\system32
Устройство загрузки:    \Device\HarddiskVolume1
Язык системы:           ru;Русский
Язык ввода:             en-us;Английский (США)
```

# Информация об удаленной системе

- Следующая команда позволяет вывести список установленных драйверов устройств на удаленном компьютере:
  - `driverquery /s <компьютер> /u <пользователь> /p <пароль>`
  - `driverquery /s <компьютер> /u <пользователь> /p <пароль> /fo TABLE|LIST|CSV /NH` вывод информации о драйверах в формате таблицы, списка, с разделяющими запятыми
  - `driverquery /s <компьютер> /u <пользователь> /p <пароль> /si` вывод информации о подписанных драйверах

# Пример вывода информации о драйверах системы

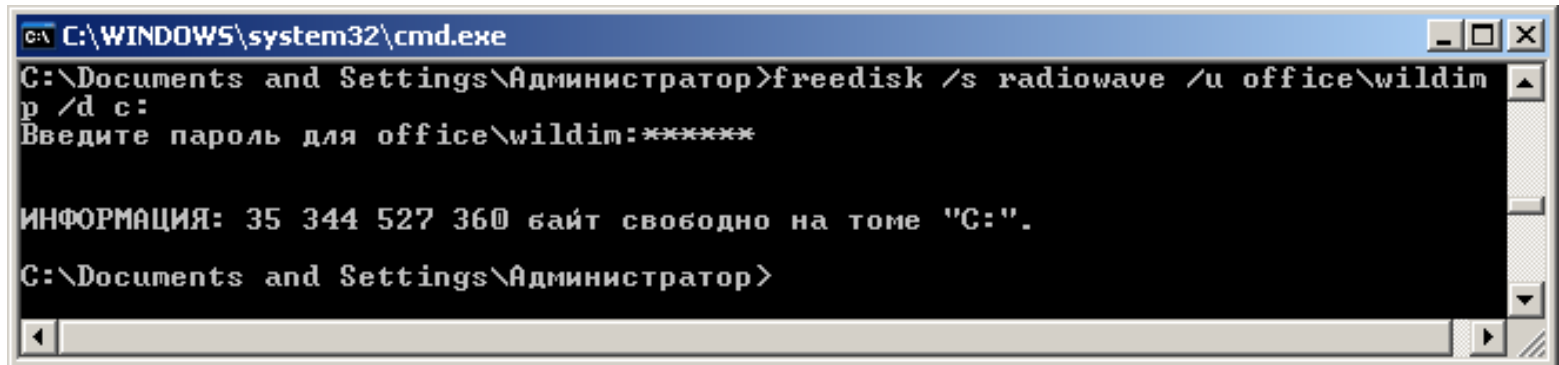
```
C:\WINDOWS\system32\cmd.exe
C:\Documents and Settings\Администратор>driverquery /s radiowave /u office\wildim /p
Введите пароль для office\wildim: *****
```

| Модуль    | Название               | Тип драйвера | Дата ссылки         |
|-----------|------------------------|--------------|---------------------|
| ACPI      | Драйвер Microsoft ACPI | Kernel       | 25.03.2005 3:34:09  |
| ACPIEC    | ACPIEC                 | Kernel       | 25.03.2003 10:16:26 |
| AFD       | Среда сетевой поддержк | Kernel       | 25.03.2005 3:40:43  |
| AsyncMac  | Драйвер асинхронного н | Kernel       | 25.03.2003 10:11:27 |
| atapi     | Стандартный контроллер | Kernel       | 25.03.2005 3:28:49  |
| ati2mpad  | ati2mpad               | Kernel       | 19.07.2002 5:13:20  |
| Atmarpc   | Протокол клиента ATM A | Kernel       | 25.03.2005 3:27:22  |
| audstub   | Драйвер заглушки аудио | Kernel       | 25.03.2003 10:09:12 |
| Beep      | Beep                   | Kernel       | 25.03.2003 10:03:04 |
| cbidf2k   | cbidf2k                | Kernel       | 25.03.2003 10:05:00 |
| Cdfs      | Cdfs                   | File System  | 25.03.2005 3:40:55  |
| Cdrom     | Драйвер CD-ROM дисково | Kernel       | 25.03.2005 3:28:57  |
| ClusDisk  | Драйвер дисков кластер | Kernel       | 25.03.2005 3:35:52  |
| crcdisk   | CRC драйвер фильтра ди | Kernel       | 25.03.2005 3:29:40  |
| DfsDriver | DfsDriver              | File System  | 25.03.2005 3:30:28  |
| Disk      | Драйвер диска          | Kernel       | 25.03.2005 3:28:58  |
| dmboot    | dmboot                 | Kernel       | 25.03.2005 3:30:03  |
| dmio      | Драйвер диспетчера лог | Kernel       | 25.03.2005 3:30:02  |
| dmload    | dmload                 | Kernel       | 25.03.2003 10:08:08 |
| E1000     | Intel(R) PRO/1000 Adap | Kernel       | 15.08.2003 1:46:47  |
| E100B     | Intel(R) PRO Adapter D | Kernel       | 04.03.2003 22:56:25 |
| Fastfat   | Fastfat                | File System  | 25.03.2005 3:40:20  |
| Fdc       | Драйвер контроллера ги | Kernel       | 25.03.2005 3:28:43  |
| Fips      | Fips                   | Kernel       | 25.03.2005 3:40:33  |
| Flpydisk  | Flpydisk               | Kernel       | 25.03.2003 10:04:32 |



# Просмотр свободного пространства

- Команда **freedisk** позволяет вывести количество свободного дискового пространства на удаленном компьютере:
  - `freedisk /s <компьютер> /u <пользователь> /p <пароль> /d <имя диска>`



```
C:\WINDOWS\system32\cmd.exe
C:\Documents and Settings\Администратор>freedisk /s radiowave /u office\wildim
p /d c:
Введите пароль для office\wildim:*****

ИНФОРМАЦИЯ: 35 344 527 360 байт свободно на томе "C:".
C:\Documents and Settings\Администратор>
```

# Команды работы с реестром

- Информацию об установленном программном обеспечении можно получить и из реестра Windows:
  - `reg query \\компьютер\ключ` - выводит записи реестра удаленного компьютера, хранящиеся в ключе КЛЮЧ
  - `reg query \\компьютер\ключ /s` - выводит записи реестра удаленного компьютера, хранящиеся в ключе КЛЮЧ, и подключи всей структуры заданного ключа
  - `reg query \\компьютер\ключ /v <запись>` - выводит данные записей заданного ключа, хранящиеся в ключе КЛЮЧ

# Просмотр и управление списком задач

- Администратор системы имеет возможность просматривать списки запущенных задач и удалять процессы на удаленном компьютере:
  - `tasklist /s <компьютер> /u <пользователь> /p <пароль>`  
- выводит список всех процессов;
  - `tasklist /s <компьютер> /u <пользователь> /p <пароль> /fo TABLE|LIST|CSV /NH` - - выводит список всех процессов в формате таблицы, списка, с разделяющими запятыми;
  - `sc \\компьютер query` – выводит список всех служб удаленного компьютера



# Управление процессами

- **Taskkill** - завершает одно или несколько заданий или процессов. Процессы могут быть уничтожены кодом процесса или именем образа.
- **Синтаксис**
  - **taskkill** [/s *компьютер*] [/u *домен\имя\_пользователя*] [/p *пароль*]  
{/fi *имя\_фильтра* [{/pid *ID\_процесс* | /im *имя\_образа*}] | /pid  
*ID\_процесс* | /im *имя\_образа*} [/f] [/t]

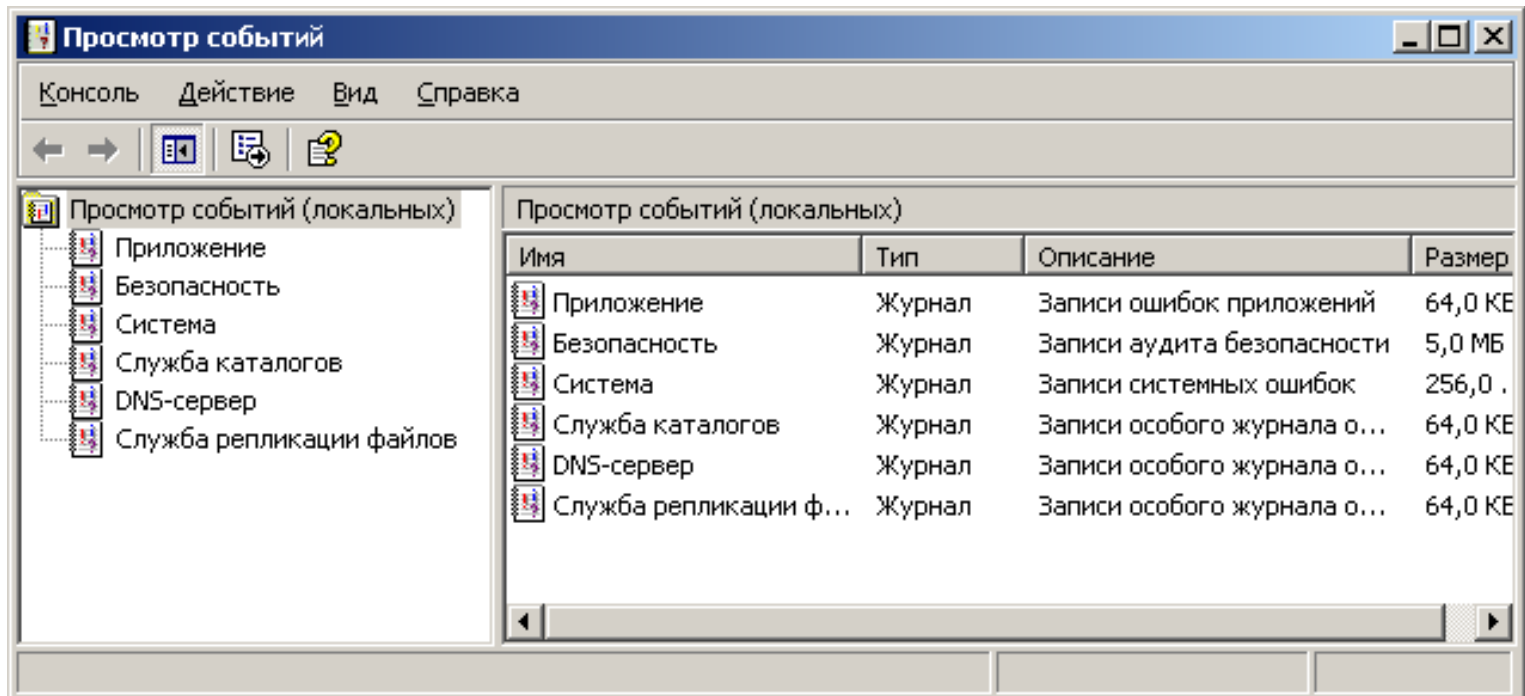
# Управление процессами

- **Параметры команды taskkill**

- **/s компьютер** Указывает имя или IP-адрес удаленного компьютера (не используйте обратную косую черту). По умолчанию используется локальный компьютер.
- **/u домен\имя\_пользователя** Выполняет команду с разрешениями учетной записи пользователя, который указан как *имя\_пользователя* или *домен\имя\_пользователя*.  
По умолчанию используются разрешения текущего вошедшего пользователя компьютера, с которого поступила эта команда.
- **/p пароль** Определяет пароль учетной записи пользователя, заданной параметром **/u**.
- **/fi имя\_фильтра** Задаёт типы процессов, которые следует завершить и не следует. Допустимыми именами фильтров, операторами и значениями являются следующие.
- **/pid код\_процесса** Указывает код процесса, который необходимо завершить.
- **/im имя\_образа** Указывает имя образа процесса, который необходимо завершить. Используйте подстановочный знак (\*) для указания всех имен образа.
- **/f** Указывает, что процесс(ы) должен быть принудительно завершен. Этот параметр не действует для удаленных процессов, все удаленные процессы завершаются принудительно.
- **/t** Выполняет указанный процесс и любой дочерний, начатый этим процессом. В таблице в определении для параметра **/fi** измените строку "статус" на:
- **/?** Отображает справку в командной строке

# Просмотр событий

- При управлении операционной системой важное значение имеет аудит событий. Система аудита позволяет фиксировать и накапливать важные события для функционирования системы.
- Для просмотра произошедших событий можно использовать специальную оснастку **Просмотр событий** в группе **Администрирование**.



# Просмотр событий

- Другой вариант использовать командного режима. Команда **eventquery** позволяет вывести список событий на локальном или удаленном компьютере
- **Синтаксис команды**
  - **eventquery[.vbs] [/s компьютер [/u домен\пользователь [/p пароль]]] [/fi имя\_фильтра] [/fo {TABLE | LIST | CSV}] [/r диапазон\_событий] [/nh] [/v] [/l [APPLICATION] [SYSTEM] [SECURITY] ["DNS server"]] [заданный\_пользователем\_журнал] [имя\_журнала\_каталога]**



# Просмотр событий

- **Параметры команды eventquery**

- */s компьютер* - задание имени или IP-адреса удаленного компьютера (не используйте обратную косую черту). По умолчанию используется локальный компьютер.
- */u домен\пользователь* - запускает сценарий с разрешениями учетной записи пользователя, указанный в **пользователь** или *домен\пользователь*.
  - По умолчанию используются разрешения текущего вошедшего пользователя компьютера, с которого поступила эта команда.
- */p пароль* - указание пароля учетной записи пользователя, заданной параметром */u*.
- */fi имя\_фильтра* - задание типов событий, которые следует включить в запрос или исключить из него. Допустимыми именами фильтров, операторами и значениями являются следующие.
- */v* - задание отображения подробных сведений о событиях в выходных данных.
- */l [APPLICATION] [SYSTEM] [SECURITY] ["DNS server"]*  
*[заданный\_пользователем\_журнал] [имя\_журнала\_каталога] [\*]* - задание журналов для просмотра. Допустимые значения:
  - **Application**,
  - **System**,
  - **Security**,
  - **"DNS server"** (значение **"DNS server"** является допустимым только в том случае, если на компьютере, заданном параметром */s*, запущена служба DNS)
- Для задания несколько журналов для просмотра, повторно воспользуйтесь параметром */l*. Допускается использование подстановочного знака (\*), который указывается по умолчанию.

# Сбор удаленных сетевых данных

- Для получения информации о mac-адресах используется команда:
  - `getmac /s <компьютер>`
- Команда `net time` позволяет просматривать, устанавливать и синхронизировать время на разных компьютерах
  - `net time \\компьютер`