Задача сетевого администратора сводится к обеспечению работы сетевых систем. Статус системных ресурсов и их загруженность радикально меняются со временем, причем не всегда так, как хочется пользователям и сетевому администратору — останавливаются службы, файловая система испытывает недостаток свободного места, ошибки приложений приводят к системным проблемам, в сеть пытаются проникнуть неавторизованные пользователи. Мониторинг сетевых устройств — это постоянное наблюдение за деятельностью данных устройств, поиск проблем и неисправностей в их работе, принятие решений о ликвидации проблем и неисправностей, повышению эффективности функционирования устройств.

Данный раздел посвящен вопросам мониторинга состояния сетевых узлов на базе систем Windows Server. В разделе обсуждаются вопросы, связанные с просмотром системных событий, аудитом доступа к ресурсам, мониторингом производительности серверов, поиска узких мест в их работе и выработки решений о ликвидации этих узких мест, а также мониторинга сетевой активности.

**Мониторинг сетевых устройств. Мониторинг серверов (просмотр событий, аудит, мониторинг производительности, определение узких мест, мониторинг сетевой активности)**

**Просмотр событий**

Одно из самых часто используемых и наиболее важных средств мониторинга системы — это регистрация различных событий в журналах операционной системы Windows. Регистрацию событий в системе Windows осуществляет служба " *Журнал событий* " ( *Event Log* ). В любой системе семейства Windows всегда присутствуют 3 журнала:

* журнал " **Система** " ( **System** ) — события, записанные в журнал компонентами операционной системы (например, сбой в запуске службы при перезагрузке); расположение журнала по умолчанию — в папке "%SystemRoot%\system32\config\SysEvent.Evt ";
* журнал " **Безопасность** " ( **Security** ) — регистрация событий, относящихся к системе безопасности (например, попытки регистрации пользователей, изменения в политиках безопасности, попытки доступа к различным ресурсам); набор событий, регистрируемых в журнале " *Безопасность* ", настраивается локальной или групповых политик (об управлении аудитом событий безопасности — в следующем подразделе); расположение по умолчанию — " %SystemRoot%\system 32\сопfig\SecEvent.Evt ";
* журнал " **Приложение** " ( **Application** ) — события, порожденные различными приложениями (например, сбой MS SQL при доступе к базе данных); набор событий, регистрируемых в журнале " *Приложения* ", определяется разработчиками приложений; расположение по умолчанию — "%SystemRoot%\system32\config\AppEvent.Evt ".

При установке в системе каких-либо компонент могут появиться журналы, регистрирующие события, относящиеся к работе данных компонент.

При установке службы DNS появляется журнал " **DNS-сервер** " ( **DNS Server** ), регистрирующий события, связанные с работой службы DNS (расположение по умолчанию — " %SystemRoot%\system32\config\DNSEvent.Evt ").

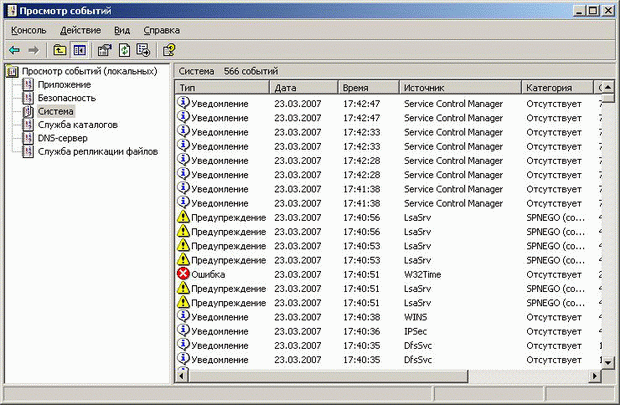
При создании контроллера домена в системе появляются журналы:

* журнал " **Служба каталогов** " ( **Directory Service** ) — события, порожденные службой каталогов Active Directory;. расположение по умолчанию — "%SystemRoot%\system32\config\NTDS.Evt ";
* журнал " **Служба репликации файлов** " ( **File Replication Service** ) — события, связанные с репликацией файлов (в первую очередь файлы в папке SYSVOL и файлы в сетевых папках, управляемых рапределенной файловой системой DFS); расположение по умолчанию — " %SystemRoot%\system32\config\NtFrs.Evt ".

**Работа с журналами**

Открыть системные журналы можно следующими способами:

* открыть консоль " *Управление компьютером* " и в разделе " *Служебные программы* " открыть оснастку " *Просмотр событий* ";
* открыть отдельную консоль " *Просмотр событий* " в разделе " *Администрирование* " Главного меню системы Windows (рис. 16.1).



**Рис. 16.1.**

В левой части консоли будет список имеющихся на данном компьютере журналов, в правой части — список событий для выбранного журнала.

В большинстве журналов события бывают трех видов:

* **Уведомление** — информация о событии, связанным с успешным действием (например, успешный запуск или останов службы, успешное завершение операции какой-либо службы);
* **Предупреждение** — информация о событиях, которые в будущем могут вызвать проблемы в работе системы;
* **Ошибка** — сообщение об ошибке (например, сбой при запуске службы).

В журнале " *Безопасность* " — 2 типа событий:

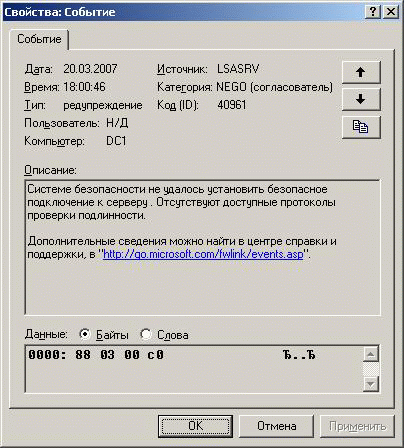
* **Аудит успехов** — событие, связанное с успешным выполнением действия, связанного с системой безопасности (например, успешный вход в систему или успешный доступ к сетевому ресурсу);
* **Аудит отказов** — событие, связанное со сбоем в выполнении действия, связанного с системой безопасности (например, отказ в аутентификации пользователя при входе в систему по причине ввода неверного пароля, блокировка учетной записи после нескольких неудачных попыток входа в систему, отказ в доступе к сетевому ресурсу).

В столбцах журнала, кроме типа события, содержатся следующие данные:

* **Дата и время** регистрации события;
* **Источник** — приложение, служба или системная компонента, записавшие событие в журнал;
* **Категория** — категория события, иногда используемая для его более подробного описания;
* **Событие** — код события;
* **Пользователь** — учетная запись пользователя, действовавшая в момент события;
* **Компьютер** — имя компьютера, на котором произошло событие.

Если открыть какое-либо событие, то можно получить более детальную информацию о нем (рис. 16.2):

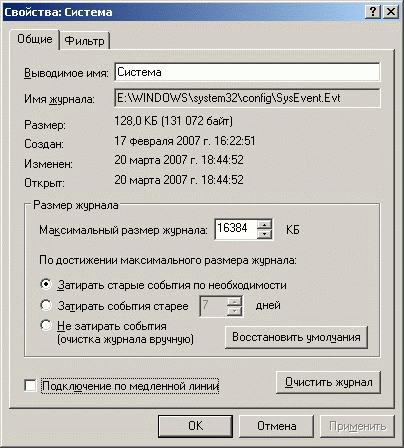
* **Описание** — текстовое описание события;
* **Данные** — любые данные, сгенерированные событием, или связанный с ним код ошибки.



**Рис. 16.2.**

**Настройка параметров журналов событий**

Размер и способ ведения журналов событий можно настраивать. Для настройки параметров надо щелкнуть правой кнопкой на нужном журнале событий и выбрать в контекстном меню команду *Свойства*. Откроется диалоговое окно, показанное на рис. 16.3.



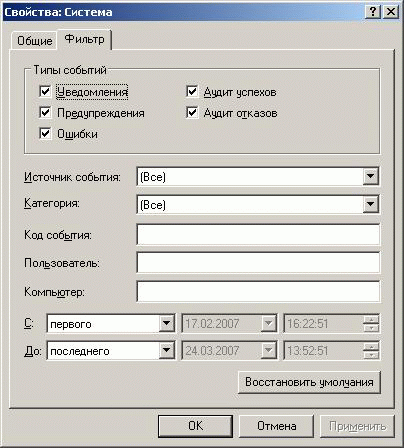
**Рис. 16.3.**

По умолчанию размер большинства журналов системы Windows 2003 — 16 МБ (для журнала безопасности — 128 МБ, в предыдущих версиях системы стандартный размер журнала — 512 КБ). При заполнении журнала старые события будут стираться. Администратор может изменить как размер журнала, так и способ управления записями при достижении максимального размера журнала (например, автоматически затирать события старше какого-то определенного количества дней или вообще не затирать старые события, в этом случае новые события в журнале регистрироваться не будут).

Содержимое журналов можно очищать вручную — щелкнуть правой кнопкой мыши на журнале, выбрать в меню команду " *Стереть все события* ". Система предложит сохранить стираемые события в отдельном файле, нужно выбрать требуемый вариант, и журнал будет очищен. При этом сохранять стираемые записи можно в трех разных вариантах: двоичном (с расширением файла " .evt ", такой файл можно будет просматривать только программой " *Просмотр событий* "), или текстовых (с расширением файла " .txt " —со знаком табуляции в качестве разделителя столбцов, а также с расширением файла " .csv " — с запятой в качестве разделителя). Сохранять содержимое журналов можно и без стирания старых записей. Открыть сохраненные записи можно через меню " *Действие* " консоли "*Просмотр событий* ", выбрав пункт " *Открыть файл журнала* ".

**Просмотр журналов (фильтрация событий)**

В каждом из журналов накапливается большое количество событий, в которых трудно иногда найти нужные события. Заметим вначале, что щелчок мышью на заголовке любого столбца в консоли (оснастке) " *Просмотр событий* " позволяет отсортировать события по убыванию или возрастанию значений данного столбца. Для более точного отбора искомых событий служат средства фильтрации в " *Просмотре событий* ". Если открыть свойства какого-либо журнала, то в открывшейся панели, кроме закладки " *Общие* ", имеется также закладка " *Фильтр* ", позволяющая установить правила для отбора событий. Посмотрим внимательно на данную закладку (рис. 16.4):

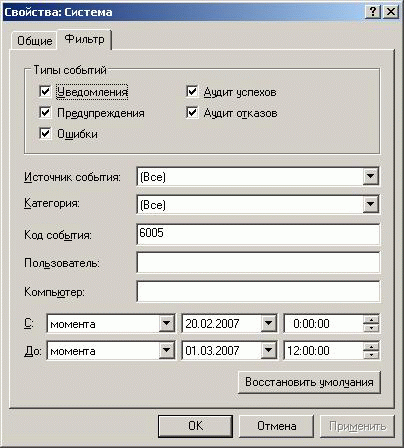


**Рис. 16.4.**

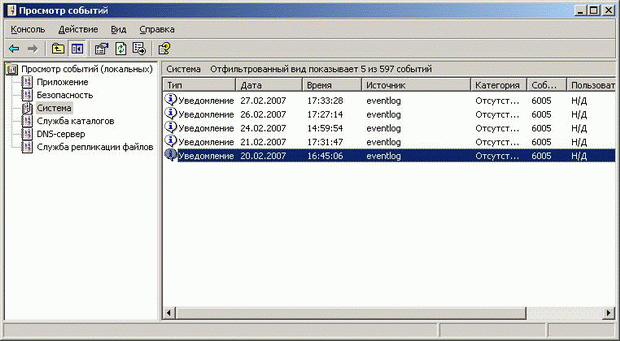
Можно установить правила отбора:

* по типу событий — уведомления, предупреждения, ошибки, аудит успехов, аудит отказов;
* по источнику (например, компоненты системы *Alerter*, *Browser*, *DCOM*, *DHCP*, *disk*, *eventlog*, *Server*, *System* и др.);
* по категории (например, *Диск*, *Оболочка*, *Принтеры*, *Сеть*, *Службы*, *Устройства* и др.);
* по известному коду события;
* по имени пользователя;
* по имени компьютера;
* задать период времени — с какого по какой момент времени отобрать события.

На рис. 16.5 изображен фильтр, отбирающий события с кодом 6005 с 00 ч 00 мин 20.02.2007 до 12 ч 00 мин 01.03.2007. Результат применения фильтра — на рис. 16.6 (с помощью данного фильтра были отобраны события, регистрирующие процесс запуска системной службы " *Журнал событий* ).

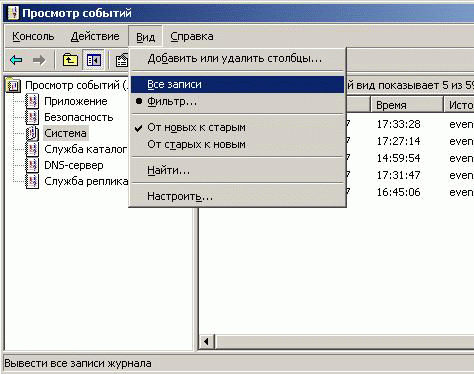


**Рис. 16.5.**



**Рис. 16.6.**

Вернуться к полному просмотру всех событий можно, выбрав в меню " *Вид* " команду " *Все записи* " (рис. 16.7):



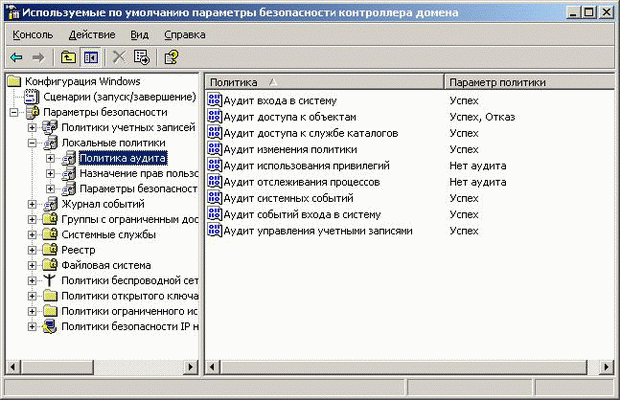
**Рис. 16.7.**

**Аудит**

Настройка политик аудита — важный фактор обеспечения безопасности и целостности системы. Каждая компьютерная система в сети должна быть настроена для протоколирования определенных событий, относящихся к системе безопасности. Политики аудита определяют, какие именно события в области безопасности системы должны регистрироваться в журнале " *Безопасность* ".

Процесс аудита безопасности настраивается с помощью групповых политик (напомним, что групповые политики можно определять для сайта, домена или организационного подразделения, а также для отдельной рабочей станции или сервера). Параметры аудита безопасности находятся в разделе " *Параметры безопасности* — *Локальные политики* — *Политики аудита* " любого *объекта групповых политик*.

На рис. 16.8 изображены стандартные политики аудита для организационного подразделения " *Контроллеры домена* ".



**Рис. 16.8.**

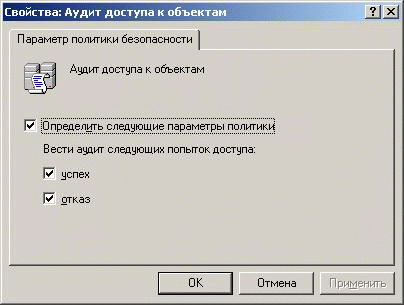
Рассмотрим параметры этого раздела:

* **Аудит входа в систему** регистрирует события, связанные с регистрацией пользователя на данном компьютере, окончанием сеанса работы и *удаленными соединениями* с сетевыми системами;
* **Аудит доступа к объектам** регистрирует попытки доступа пользователей к различным объектам — файлам, папкам, принтерам и объектам Active Directory;
* **Аудит доступа к службе каталогов** регистрирует доступ к Active Directory;
* **Аудит изменения политики** регистрирует изменения разрешений доступа пользователей, аудита и доверительных отношений;
* **Аудит использования привилегий** регистрирует применение разрешений доступа и привилегий пользователя (например, использование прав резервного копирования файлов и каталогов);
* **Аудит отслеживания процессов** регистрирует системные процессы и ресурсы, используемые процессами;
* **Аудит системных событий** регистрирует запуск, выключение и перезагрузку системы, а также действия, влияющие на безопасность системы или на журнал безопасности;
* **Аудит событий входа в систему** регистрирует события, связанные с регистрацией пользователя в домене;
* **Аудит управления учетными записями**регистрирует управление учетными записями посредством консоли " *Active Directory - пользователи и компьютеры* " (события генерируются каждый раз, когда учетные записи пользователя, компьютера или группы создаются, изменяются или удаляются).

**Аудит доступа к объектам**

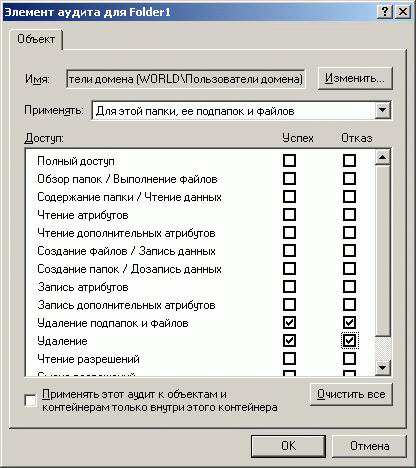
Рассмотрим подробнее аудит доступа к объектам. Необходимость регистрации событий доступа к объектам возникает, когда есть подозрения, что кто-то из пользователей пытается получить несанкционированный доступ к информации, к которой он не должен иметь доступа.

По умолчанию на обычном сервере или рабочей станции политики аудита доступа к объектам отключены. Включим данные политики (на уровне сайта, домена или нужного нам ОП) — откроем данный параметр в редакторе политик и установим регистрацию как успешных, так и неуспешных попыток доступа к объектам (рис. 16.9).



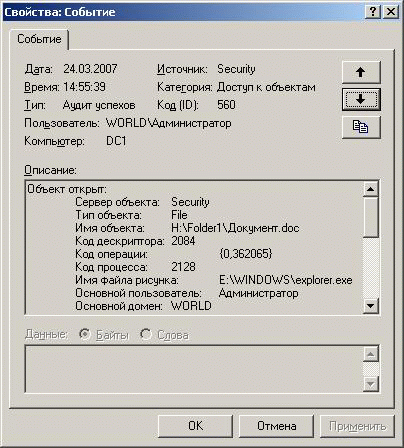
**Рис. 16.9.**

После применения политик настроим аудит доступа для нужных объектов (например, для папки Folder1 на сервере *DC1* ) — откроем *Свойства* данной папки (папка должна быть размещена на разделе с файловой системой NTFS), перейдем на закладку " *Безопасность* ", нажмем кнопку " *Дополнительно* " и перейдем на закладку " *Аудит* ". Добавим в список пользователей, для которых будут отслеживаться попытки доступа к папке Folder1, группу " *Пользователи домена* " и установим, какие именно попытки будут регистрироваться в журнале " *Безопасность* " (например, попытки удаления папок и файлов, успешные и неуспешные, рис. 16.10).

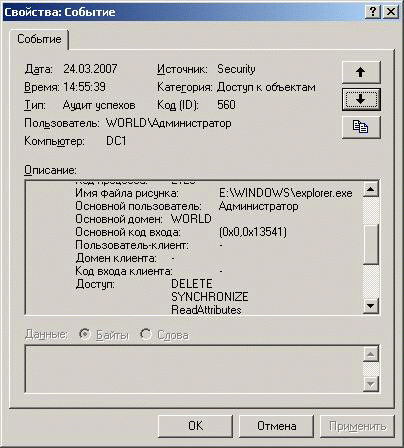


**Рис. 16.10.**

Теперь для проверки работы механизма аудита удалим какой-нибудь файл в этой папке, а затем просмотрим соответствующие события, появившиеся в журнале "*Безопасность* ". Пример события, зарегистрировавшего в журнале безопасности удаление файла " Документ.doc ", показан на рис. 16.11 и 16.12:



**Рис. 16.11.**



**Рис. 16.12.**

На рис. 16.11 видно, что пользователь *Администратор* получил *успешный* доступ к файлу " H:\Folder1\Документ.doc " на компьютере *DC1*, а на рис. 16.12 показан вид доступа — *DELETE* ( *Удаление* ).

Не рекомендуем злоупотреблять применением политик аудита доступа к объектам и регистрацией доступа к большому числу объектов, т.к. системой генерируется очень большое число записей, отыскать среди которых нужные будет весьма непросто. К тому же надо будет постоянно заботиться о сохранении старых записей и очистке журнала. Наиболее рациональный способ применения аудита доступа к объектам — настройка данного аудита в те моменты, когда есть обоснованные опасения о наличии в сети попыток несанкционированного доступа.

**Мониторинг производительности**

Мы рассмотрим два основных инструмента мониторинга производительности систем Windows Server — программу " *Диспетчер задач* ", которая предназначена для мониторинга работы приложений и служб сервера в реальном времени, и консоль "*Производительность* ", которая может осуществлять мониторинг производительности как в реальном времени, так и путем накопления статистики о работе системы за определенный период времени, причем консоль " *Производительность* " может показывать и собирать данные одновременно с нескольких систем.

**Диспетчер задач**

Чтобы открыть " *Диспетчер задач* ", основной инструмент мониторинга и управления системными процессами иприложениями, нужно выполнить одно из перечисленных действий:

* нажать комбинацию клавиш CTRL+SHIFT+ESC;
* нажать комбинацию клавиш CTRL+ALT+DELETE и нажать кнопку " *Диспетчер задач* ";
* нажать кнопку " *Пуск* ", выбрать пункт меню " *Выполнить* ", ввести taskmgr и нажать кнопку " *ОК* ";
* щелкнуть правой кнопкой мыши на панели задач и выбрать в контекстном меню команду " *Диспетчер задач* ".

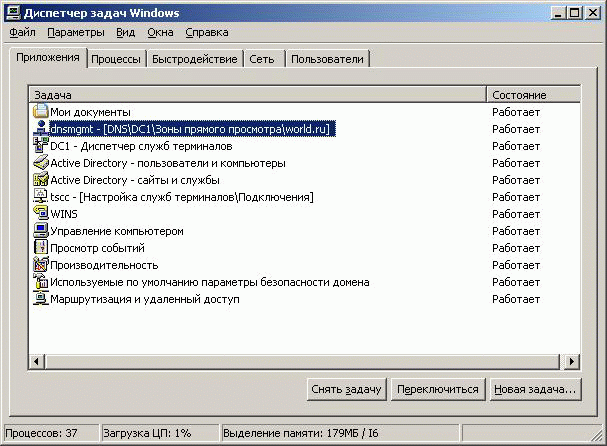
Настройка общих параметров " *Диспетчера задач* "

Прежде чем изучать работу данной программы по управлению приложениями и процессами, сделаем некоторые настройки, позволяющие повысить удобство использования программы:

* в меню " *Параметры* " уберем галочку у параметра "Поверх остальных окон" ("Диспетчер задач" не будет перекрывать окна других программ);
* в меню " *Вид* " у параметра " *Скорость обновления* " установим значение " *Низкая* " (это снизит нагрузку на процессор системы со стороны самого " *Диспетчера задач* ").

**Управление приложениями**

На закладке " *Приложения* " показан статус программ, работающих в данный момент в системе (рис. 16.13):



**Рис. 16.13.**

Кнопки в нижней части вкладки предназначены для выполнения следующих действий:

* остановка работы приложения — выберите приложение и щелкните кнопку " *Снять задачу* ";
* переход к окну нужного приложения — выберите приложение и щелкните кнопку " *Переключиться* ";
* запуск новой программы — щелкните кнопку " *Новая задача* " и введите команду для запуска приложения (кнопка " *Новая задача* " функционально аналогична команде " *Выполнить* " из меню " *Пуск* ").

**Замечание**. В столбце " *Состояние* " для каждого приложения указано, нормально ли выполняется данное приложение. Статус " *Не отвечает* " свидетельствует о том, что приложение, возможно, "зависло" и надо завершить связанные с ним процессы. Однако некоторые приложения не отвечают назапросы системы в ходе выполнения интенсивных расчетов. Поэтому, прежде чем закрыть приложение, убедитесь, что оно действительно "зависло".

Контекстное меню списка приложений

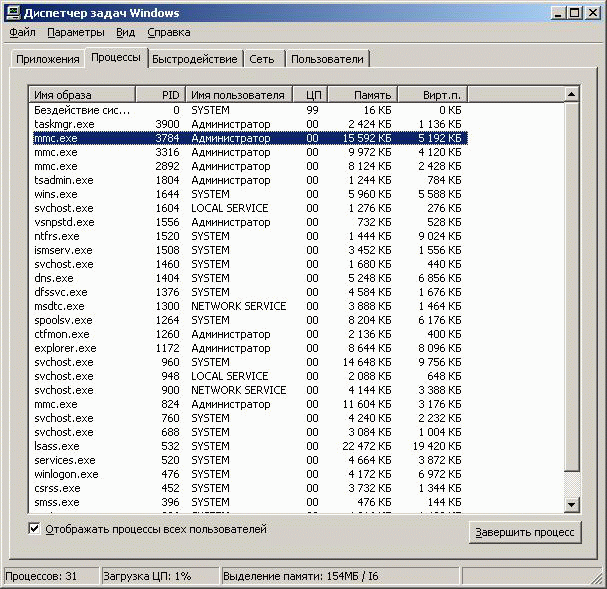
При щелчке правой кнопкой мыши на строке приложения или группы приложений в списке отображается контекстное меню, позволяющее:

* переходить к приложению и делать его активным;
* переводить приложение на передний план;
* сворачивать и восстанавливать приложение;
* изменять расположение окон приложений;
* закрывать приложение;
* выделять на вкладке " *Процессы* " процесс, связанный с этим приложением.

**Замечание**. Команда " *Перейти к процессу* " полезна, когда необходимо найти основной процесс для приложения, запустившего несколько процессов.

**Управление процессами**

Подробная информация о выполняемых процессах отображается на закладке " *Процессы* " (рис. 16.14):



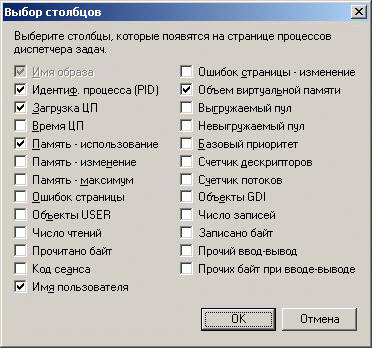
**Рис. 16.14.**

По умолчанию в этом окне перечислены только процессы, запущенные ОС, локальными службами, сетевыми службами и интерактивным пользователем, т. е. пользователем, локально зарегистрировавшимся на компьютере. Чтобы увидеть процессы, запущенные удаленными пользователями, например подключившимися с помощью удаленного рабочего стола, надо установить галочку у поля " *Отображать процессы всех пользователей* ".

В столбцах на закладке " *Процессы* " содержится информация о выполняемых процессах. Она позволяет выявить те из них, которые поглощают системные ресурсы, например, процессорное время или память. По умолчанию отображаются следующие столбцы:

* *Имя образа* — имя процесса или исполняемого файла, запустившего процесс;
* *Имя пользователя* — имя пользователя или системной службы, запустившей процесс;
* *ЦП* — доля ресурсов ЦП (в процентах), занимаемая данным процессом;
* *Память* — объем оперативной памяти, занятой процессом в данный момент.

При выборе в меню " *Вид* " команды " *Выбрать столбцы* ", откроется диалоговое окно, из которого на закладку " *Процессы* " можно добавить другие столбцы (рис. 16.15):



**Рис. 16.15.**

Некоторые из них могут оказаться очень полезными при поисках причин системной проблемы.

* *Идентиф. процесса (PID)* — цифровой идентификатор процесса в системе (позволяет найти процесс по его номеру, отображаемому не только в " *Диспетчере задач* ", но и в других утилитах управления);
* *Объем виртуальной памяти* — объем памяти данного процесса в килобайтах, выгруженной в данный момент в файл подкачки;
* *Базовый приоритет* — мера объема системных ресурсов, выделенных процессу; чтобы задать приоритет процесса, щелкните его правой кнопкой мыши, раскройте подменю " *Приоритет* " и выберите нужный вариант — " *Низкий* ", " *Ниже среднего* ", " *Средний* ", " *Выше среднего* " и " *Реального времени* "; большинству процессов по умолчанию назначен средний приоритет; наивысший приоритет назначается процессам реального времени;
* *Время ЦП* — процессорное время, затраченное на выполнение процесса с момента его запуска; чтобы найти процессы, на выполнение которых расходуется больше всего времени, отобразите этот столбец и щелкните его заголовок, чтобы отсортировать процессы по содержимому столбца;
* *Выгружаемый пул, Невыгружаемый пул* — выгружаемым пулом называется область системной памяти, предназначенная для объектов, которые при ненадобности можно хранить на диске; невыгружаемый пул — это область системной памяти для объектов, которые на диск записывать нельзя (стоит обращать внимание на процессы, которым требуется значительный объем невыгружаемой памяти — если на сервере недостаточно свободной памяти, эти процессы могут стать причиной большого количества ошибок);
* *Ошибок страницы* — ошибка страницы возникает, если процесс запрашивает страницу памяти, а система не находит ее по указанному адресу; если запрашиваемая страница хранится в другой области памяти, ошибка называется программной; если запрашиваемую страницу приходится считывать с диска, ошибка называется ошибкой физической памяти; процессоры, как правило, справляются с большинством программных ошибок; ошибки физической памяти могут существенно замедлить работу системы
* *Память - максимум* — максимальный объем памяти, использованной процессом (на разницу между этим параметром и текущим объемом памяти, занятой процессом, тоже следует обращать внимание — если приложению, например, Microsoft SQL Server, в моменты пиковых нагрузок требуется гораздо больше памяти, чем при обычной работе, возможно, стоит сразу при запуске выделять ему больше памяти);
* *Счетчик дескрипторов* — полное число дескрипторов файлов, поддерживаемых процессом; эта характеристика позволяет оценить, насколько процесс зависит от файловой системы (С некоторыми процессами связаны тысячи дескрипторов открытых файлов, и каждый из них занимает некоторый объем системной памяти);
* *Счетчик потоков* — текущее число потоков, используемых процессом; большинство серверных приложений являются многопотоковыми, что позволяет одновременно выполнять несколько запросов процесса; некоторые приложения способны динамически управлять числом одновременно исполняемых потоков, что позволяет повысить их производительность; чрезмерное увеличение количества потоков ухудшает производительность, так как ОС приходится слишком часто переключать контексты потоков;
* *Число чтений, Число записей* — полное число операций чтения с диска и записи на диск с момента запуска процесса; этот параметр показывает, насколько активно процессом используется диск (если рост числа операций ввода-вывода не согласуется с реальной активностью сервера, процесс, вероятно, не способен кэшировать файлы или кэширование файлов неверно настроено).

**Замечание**. В списке процессов присутствует процесс " *Бездействие системы* ". Он отслеживает объем неиспользуемых ресурсов. Так, число 99 в столбце ЦП (CPU) означает, что 99% системных ресурсов в настоящий момент не используется. Приоритет этого процесса задать нельзя.

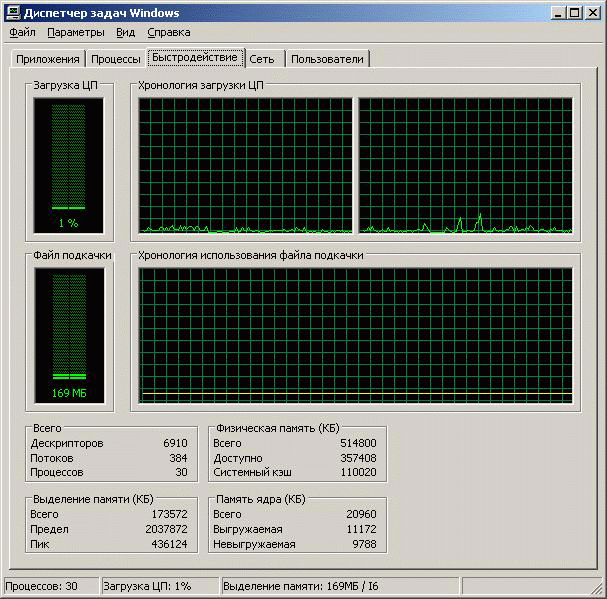
Просматривая информацию о процессах, надо помнить, что одно приложение может породить несколько процессов. Обычно все они зависят от родительского процесса и формируют расходящееся от него дерево процессов. Чтобы найти главный (родительский) процесс для данного приложения, на закладке "Приложения" щелкните приложение правой кнопкой мыши и выберите команду " *Перейти к процессу* ". Чтобы корректно завершить работу приложения с помощью " *Диспетчера задач* ", останавливайте либо само приложение, либо его главный процесс. Не останавливайте по отдельности зависимые процессы.

Остановить главный процесс приложения и порожденные им вторичные процессы можно несколькими способами:

* выделить приложение на закладке " *Приложения* " и щелкнуть кнопку " *Снять задачу* ";
* на закладке "Процессы" щелкнуть правой кнопкой мыши главный процесс приложения и выбрать команду " *Завершить процесс* ";
* на закладке "Процессы" щелкнуть правой кнопкой мыши главный или вторичный процесс приложения и выбрать команду " *Завершить дерево процессов* ".

**Мониторинг загруженности системы**

На закладке " *Быстродействие* " в виде графиков и статистических данных отображается степень использования процессора и памяти (рис. 16.16).



**Рис. 16.16.**

Эта информация позволяет быстро оценить нагрузку на системные ресурсы. Чтобы получить более подробные сведения, необходимо используйте консоль "*Производительность* ".

На графиках закладки " *Быстродействие* " отображена следующая информация:

* *Загрузка ЦП* — процент используемых в данный момент ресурсов процессора;
* *Хронология загрузки ЦП* — график изменения нагрузки на процессор (если в компьютере несколько процессоров, то по умолчанию для каждого процессора будет отображаться свой график загруженности); чтобы увеличить диаграмму, щелкните ее дважды, повторный двойной щелчок вернет обычный режим просмотра;
* *Файл подкачки* — объем файла подкачки (т. е. виртуальной памяти), занятый системой в настоящий момент;
* *Хронология использования файла подкачки* — график использования файла подкачки.

**Замечание**. Если нагрузка на процессор остается неизменно высокой даже в обычных условиях, для выяснения причин этого стоит заняться более детальным исследованием работы системы. Зачастую причина снижения производительности скрыта в памяти. Проверьте эту возможность, прежде чем принимать решение об обновлении процессора или о добавлении дополнительных процессоров.

Отображение графиков можно настроить или обновить с помощью команды меню Вид.

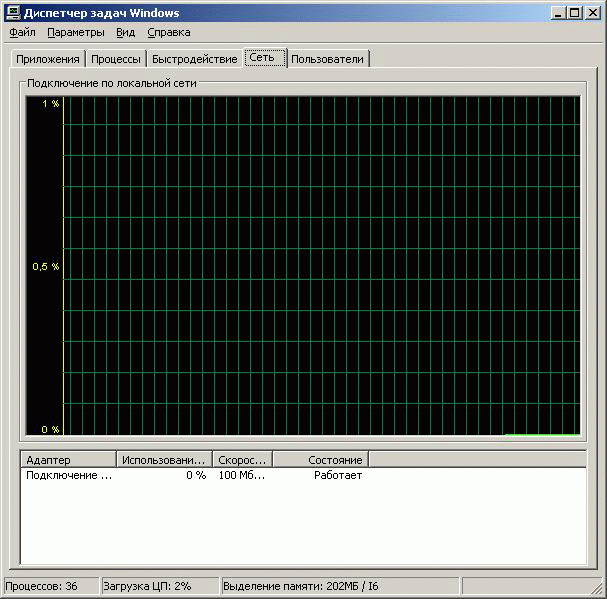
* команда " *Скорость обновления* " позволяет изменить скорость обновления графиков, а также приостановить обновление; вариант " *Низкая* " соответствует обновлению каждые 4 секунды, вариант " *Обычная* " — обновлению каждые 2 секунды, вариант " *Высокая* " — обновлению дважды в секунду;
* команда " *Загрузка ЦП* " в многопроцессорных системах позволяет задать отображение графиков для отдельных процессоров (отдельная диаграмма для каждого процессора) или все графики на одной диаграмме;
* команда " *Вывод времени ядра* " позволяет отобразить процессорное время, использованное ядром операционной системы (ресурсы, используемые ядром, на графиках отображаются красными линиями).

Под графиками приведены статистические данные:

* *Всего* — общая информация о загрузке процессора; в поле " *Дескрипторов* " указано количество используемых дескрипторов ввода-вывода, в поле " *Потоков* " — число потоков, в поле " *Процессов* " — число процессов;
* *Выделение памяти* — информация об общем объеме памяти, используемой ОС; в поле " *Всего* " отображается объем физической и виртуальной памяти, используемой в *данный момент*, в поле " *Предел* " — вся доступная физическая и виртуальная память, в поле " *Пик* " — максимальный объем памяти, использованный системой с момента загрузки;
* *Физическая память* — информация об общем объеме оперативной памяти в системе; в поле " *Всего* " указан объем физической оперативной памяти, в поле "*Доступно* " — оперативная память, не используемая в данный момент, в поле " *Системный кэш* " — память, используемая ОС для кэширования (если доступный объем памяти невелик, скажем, менее 5% всей физической памяти, стоит подумать об установке дополнительной памяти);
* *Память ядра* — информация о памяти, используемой ядром ОС; значительная часть ядра должна работать в оперативной памяти и не может выгружаться в виртуальную память, объем этой памяти указан в поле " *Невыгружаемая* ", объем памяти ядра, которую допустимо выгружать в виртуальную память, отображен в поле " *Выгружаемая* ", общий объем памяти, используемой ядром, указан в поле " *Всего* ".

**Мониторинг производительности сети**

На закладке " *Сеть* " приводятся сведения о сетевых адаптерах, используемых системой, — процент загрузки, скорость соединения и статус. Если в системе установлен единственный сетевой адаптер, на сводной диаграмме (рис. 16.17) показана информация об изменении со временем трафика через этот адаптер:



**Рис. 16.17.**

Если сетевых адаптеров в системе несколько, на диаграмме отображается сводный показатель использования всех сетевых подключений. По умолчанию это суммарное количество байт, переданных по сети.

В полях закладки " *Сеть* " содержится множество сведений о входящем и исходящем сетевом трафике сервера. С их помощью можно, например, установить объем поступающих на сервер данных. По умолчанию отображаются следующие поля:

* *Адаптер* — имя, под которым адаптер значится в папке Сетевые подключения;
* *Использование сети* — загрузка сети в процентах от исходной скорости подключения для данного интерфейса (например, адаптер с исходной скоростью подключения 100 Мбит/с и текущим трафиком 10 Мбит/с загружен на 10%);
* *Скорость линии* — скорость подключения через данный интерфейс;
* *Состояние* — состояние сетевого адаптера.

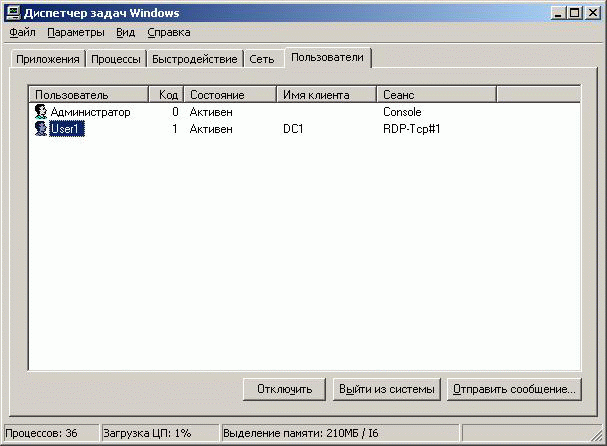
**Замечание**. Если загрузка адаптера часто достигает 50% или больше, внимательнее следите за сетевой активностью сервера и подумайте о приобретении дополнительных сетевых адаптеров.

Для исследования работы сети могут понадобиться дополнительные столбцы на закладке " *Сеть* ". Можно выбрать в меню " *Вид* " пункт " *Выбрать столбцы* " и установить отображение следующих столбцов:

* *Пропускная способность отправки* — процент использования текущей полосы пропускания исходящим трафиком;
* *Пропускная способность получения* — процент использования текущей полосы пропускания входящим трафиком;
* *Пропускная способность всего* — процент использования текущей полосы пропускания всем трафиком через данный адаптер;
* *Отправлено байт* — полное число байт, отправленных по данному подключению;
* *Получено байт* — полное число байт, полученных по данному подключению;
* *Байт* — полное число байт, переданных по данному подключению в обоих направлениях.

**Мониторинг удаленных подключений**

Удаленные пользователи подключаются к системе через службы терминалов, или удаленные рабочие столы. Подключения с помощью удаленного рабочего стола активизируются автоматически при установке Windows Server 2003. " *Диспетчер задач* " предоставляет один из способов управления такими подключениями. Перейдите на закладку " *Пользователи* ", где перечислены пользовательские сеансы как для локальных, так и для удаленных пользователей (рис. 16.18):



**Рис. 16.18.**

Для каждого подключения указаны: имя пользователя, код сеанса, состояние, клиентский компьютер и тип сеанса. Пользователю, зарегистрировавшемуся локально, соответствует тип сеанса " *Консоль* " ( *Console* ). Для других пользователей в этом столбце указаны тли и протокол подключения, например, *RDP*-Tcp для подключения с помощью протокола *RDP* ( *Remote Desktop Protocol* ) и транспортного протокола TCP. Щелкнув сеанс правой кнопкой мыши, получаем доступ к следующим командам:

* *Подключить* — подключение неактивного сеанса;
* *Отключить* — отключение пользовательского сеанса, с сохранением в сеансе всех запущенных пользователем приложений;
* *Выход из системы* — принудительное завершение пользовательского сеанса;
* *Удаленное управление* — переход к удаленному управлению пользовательским сеансом из сеанса администратора (совместная работа в сеансе);
* *Отправить сообщение* — отправка сообщения пользователям, зарегистрировавшимся на сервере терминалов.

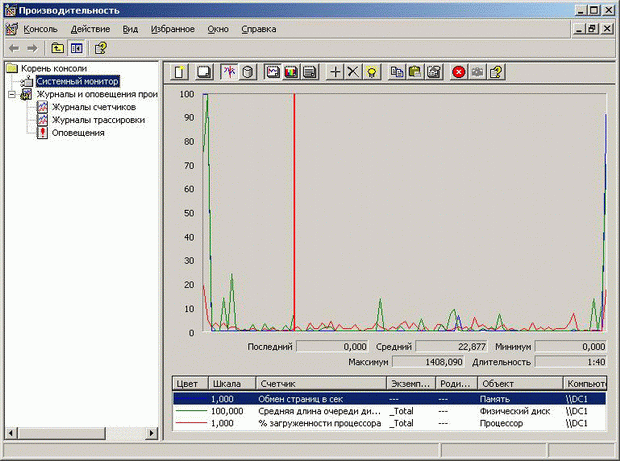
**Консоль "Производительность"**

Консоль " *Производительность* " (находящая в разделе " *Администрирование* " Главного меню системы Windows) позволяет более детально исследовать функционирование системы по сравнению с " *Диспетчером задач* ". И, кроме того, данная консоль позволяет накапливать статистику о работе системы в фоновом режиме, без непосредственного наблюдения администратором системы, а также собирать данные о производительности с нескольких компьютеров одновременно. Данная консоль содержит два раздела — " *Системный монитор* " и " *Журналы и оповещения производительности* ". " *Системный монитор* " предназначен для наблюдения за системой (или системами в режиме реального времени), " *Журналы и оповещения производительности* ". используются для накопления статистики в фоновом режиме и последующего изучения накопленных данных.

Работа консоли " *Производительность* " основана на понятиях " *Объект* " и " *Счетчик* ". Понятие " *Объект* " относится к той или иной компоненте системы или к определенному приложению и состоит из набора " *Счетчиков* ", числовых показателей, измеряющих степень загруженности данной компоненты. Набор доступных объектов и счетчиков обновляется при установке служб и дополнительных компонент. Например, после установки на сервере службы DNS консоль " *Производительность* " пополняется рядом объектов и счетчиков для отслеживания работы этой службы.

" *Системный монитор* "

Если открыть консоль " *Производительность* ", то мы сразу попадем в раздел " *Системного монитора* ". При этом на экране отображаются 3 самых важных с точки зрения операционной системы счетчика: " *Обмен страниц в сек* " (объекта " *Память*"), " *Средняя длина очереди диска* " (объекта " *Физический диск* ") и " *% загруженности процессора* " (объекта " *Процессор*"); обновление данных на экране производится раз в секунду (Рис. 16.19).



**Рис. 16.19.**

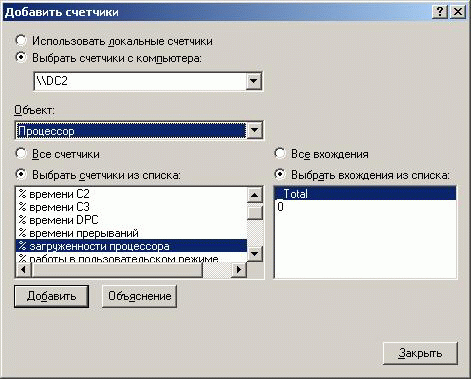
Для выбранного мышью активного процесса регистрируются показатели:

* *Последний* — последнее полученное значение счетчика;
* *Средний* — среднее из всех полученный значений счетчика;
* *Минимум* — минимальное значение счетчика за период наблюдений;
* *Максимум* — максимальное значение счетчика за период наблюдений.

Если открыть *Свойства* счетчика, то можно изменить способ отображения данного счетчика на экране: цвет, толщину и стиль линии и масштаб (от 1:10000000 до 10000000:1), также изменить частоту сбора показаний.

Нажатием комбинации клавиш CTRL+H можно выделить активный счетчик белым цветом (так лучше видно активный счетчик среди большого количества счетчиков).

Нажатием кнопки со знаком "+" на панели инструментов можно добавить другие счетчики, в том числе полученные с других компьютеров сети (рис. 16.20):



**Рис. 16.20.**

" *Журналы и оповещения производительности* "

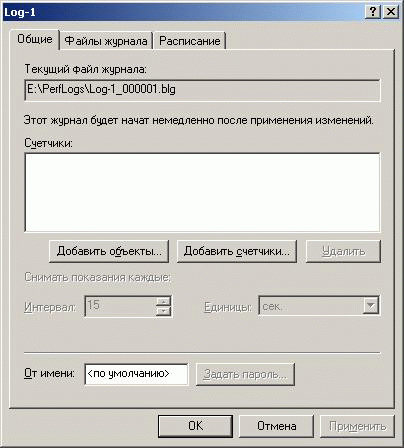
Раздел " *Журналы и оповещения производительности* " в свою очередь состоит из трех частей:

* " *Журналы счетчиков* " — выполняют ту же задачу, что и " *Системный монитор* ", но делают это в фоновом режиме и накапливают данные в файле журнале на жестком диске или в базе данных (это наиболее часто используемый раздел журналов производительности);
* " *Журналы трассировки* " — отслеживание запуска и работы приложений (универсальный системный отладчик, позволяет определить некоторые ошибки в функционировании тех или иных приложений и системных задач);
* " *Оповещения* " — отслеживание значений счетчиков, но не для накопления в журнале, а для отправки оповещения назначенным для этой задачи пользователям (по электронной почте, с помощью системной компоненты " *Оповещатель* " ( *Messenger* ), и др.).

Рассмотрим подробнее использование " *Журналов счетчиков* ".

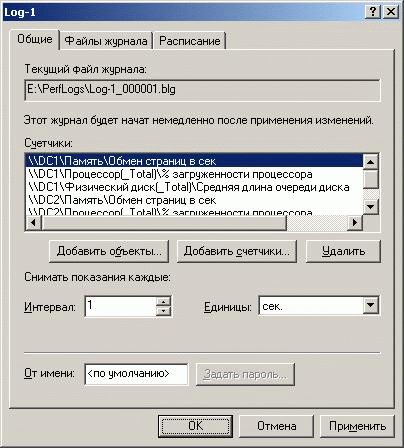
Основное назначение этих журналов — накопление статистики загруженности системы, поиск "узких мест" в работе сервера и выработка рекомендаций по модернизации или замене системы (если возникает такая потребность).

Для создания нового журнала в меню " *Действие* " необходимо выбрать пункт " *Новые параметры журнала* ". Далее надо задать имя журнала (к введенному администратором имени система добавит последовательность цифр, отображающую номер журнала, при каждом новом запуске журнала его номер будет увеличиваться, рис. 16.21).



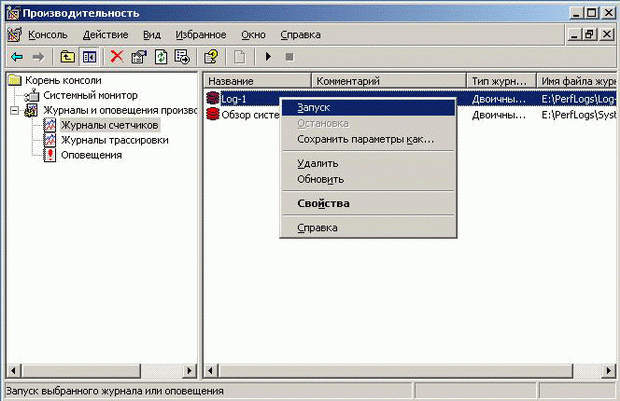
**Рис. 16.21.**

При создании самого первого журнала на томе с системой Windows создастся папка Perflogs, в которой и будут сохраняться все файлы с журналами. Далее нажатием кнопок " *Добавить объекты* " или " *Добавить счетчики* " можно добавить соответственно необходимые для мониторинга объекты (целиком со всем набором счетчиков) или отдельные счетчики. Для примера создадим журнал с именем Log-1, выберем счетчики " *Память\Обмен страниц в сек* ", " *Процессор\% загруженности процессора* " и " *Физический диск\Средняя длина очереди диска* " для сервера *DC1*, установим интервал опроса для сбора данных — 1 секунду (рис. 16.22). Нажмем кнопку " *Применить* ".



**Рис. 16.22.**

Теперь можно менять другие параметры журнала. На закладке " *Файлы журнала* " можно указать, где накапливать данные — в двоичном файле с расширением ".blg " (по умолчанию), в текстовом с разделителями в виде табуляции или запятой, в базе данных. На закладке " *Расписание* " задается время и дата запуска журнала. Назначим режим запуска журнала " *Вручную* " и нажмем кнопку " *ОК* ". Теперь запустим журнал для накопления данных (рис. 16.23). Саму консоль "*Производительность* " можно закрыть (и даже завершить сеанс работы в системе).



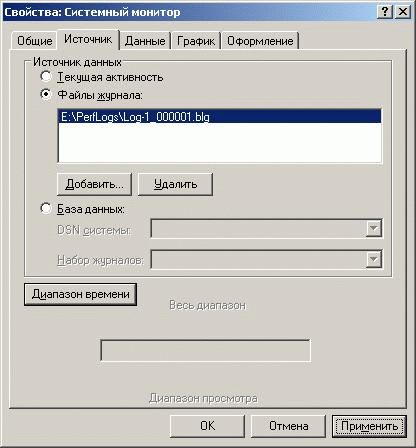
**Рис. 16.23.**

Для тестового примера запустим подряд несколько управляющих консолей и приложений, а также процесс копирования большого объема данных из одной папки в другую (все это в совокупности достаточно сильно нагрузит и процессор, и дисковую подсистему), причем сделаем это несколько раз в течение определенного интервала времени.

По окончании процесса накопления данных снова запустим консоль " *Производительность* " и удалим автоматически открытые счетчики. Для того чтобы открыть файл журнала для анализа накопленных данных, выполним следующие действия: нажмем кнопку " *Просмотр данных журнала* " (рис. 16.24) или комбинацию клавиш CTRL+L, выберем для источника данных вариант " *Файлы журнала* ", нажмем кнопку " *Добавить* ", укажем путь к файлу с накопленными данными, откроем этот файл, нажмем кнопку " *Применить* " (рис. 16.25).

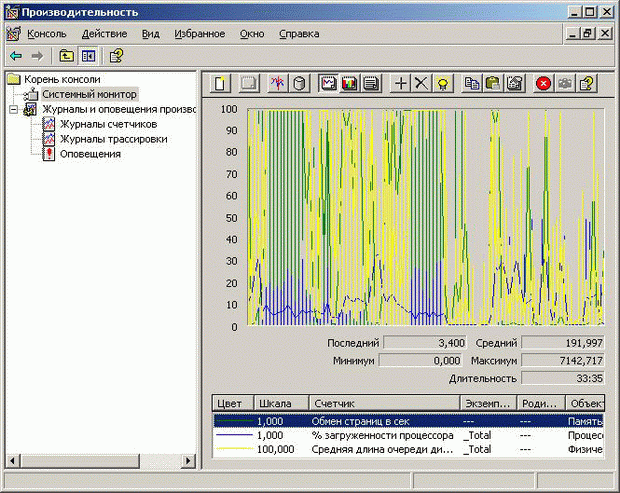
http://www.intuit.ru/department/os/sysadmswin/16/09-24.gif

**Рис. 16.24.**



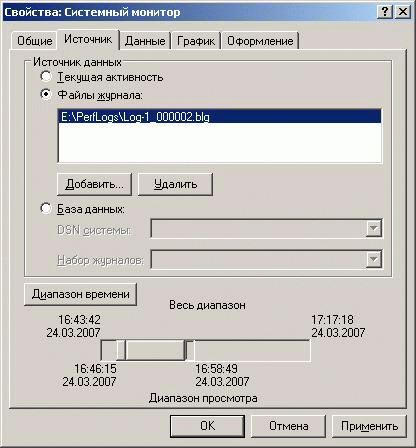
**Рис. 16.25.**

Перейдем на закладку " *Данные* " и добавим нужные счетчики. Нажмем " *ОК* ". Если период накопления был достаточно долгий, то данных будет накоплено много и картинка получится не очень разборчивая (рис. 16.26).



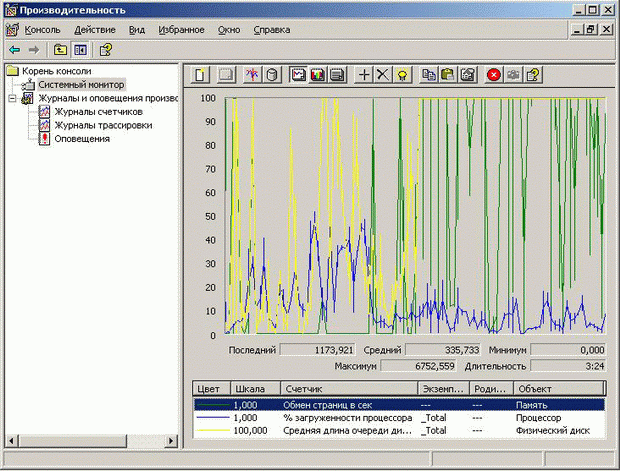
**Рис. 16.26.**

Для сужения интервала времени, который подвергается анализу, откроем *Свойства* любого из счетчиков и перейдем на закладку " *Источник* ". В нижней части панели подвинем границы анализируемого интервала и установим нужный нам " *Диапазон просмотра* " (рис. 16.27).



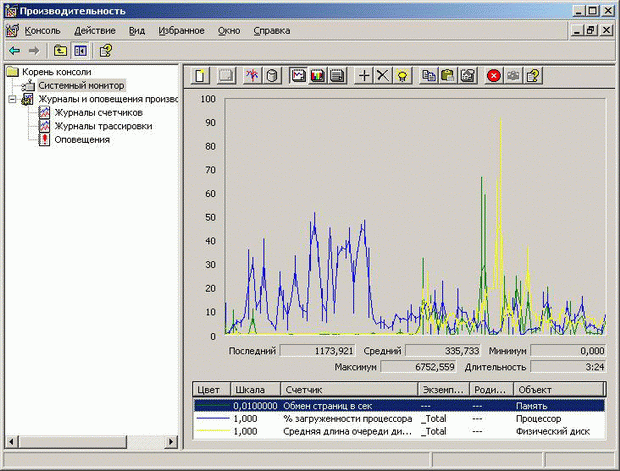
**Рис. 16.27.**

После этого график приобретет вид (рис. 16.28):



**Рис. 16.28.**

Чтобы значения некоторых графиков не выходили за границы экрана просмотра, произведем масштабирование этих графиков. В итоге получится картинка, вполне пригодная для изучения и анализа (рис. 16.29):



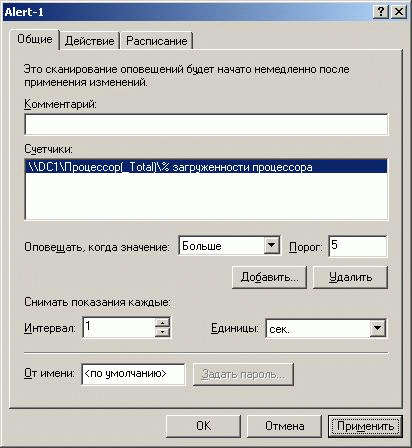
**Рис. 16.29.**

Диапазон просмотра можно менять и переключаться на другие промежутки времени. Соответственно может потребоваться настроить масштаб отображения графиков.

**Журнал оповещений**

Основное назначение этих журналов — обнаружение ситуации, когда какие-то показатели превышают или становятся меньше определенных критических значений, и выполнение каких-либо действий в качестве реакции на данное событие (регистрация события в системном журнале, отправка сообщения администратору, запуск соответствующей программы).

Для создания нового журнала в меню " *Действие* " необходимо выбрать пункт " *Новые параметры оповещений* ", после чего надо задать имя журнала. Для нашего примера сразу же определим счетчик, значения которого будет отслеживать данный журнал оповещений — " *Процессор\%загруженности процессора* ", пороговое значение — 5%, отношение — "Больше", и интервал опроса показаний системы — 1 секунда. Нажмем кнопку " *Применить* " (рис. 16.30):



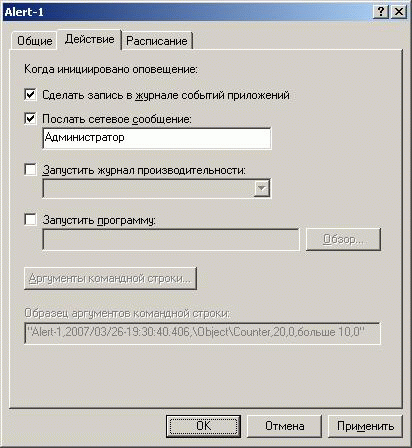
**Рис. 16.30.**

Эти настройки означают, что журнал оповещений с именем " Alert-1 " будет реагировать на события, когда суммарная загруженность процессоров сервера превысит 5%.

На закладке " *Действие* " определим те действия, которые будет выполнять система в случае возникновения данного события:

* *Сделать запись в журнале событий приложений* — если включить данный параметр, то при наступлении события в журнале " *Приложение* " будет сделана соответствующая запись;
* *Послать сетевое сообщение* — в данном случае система пошлет сообщение на тот компьютер или тому пользователю, чье имя указано в настройках (в примере — пользователю " *Администратор* "), для отправки и получения сообщений на сервере-отправителе и на компьютере-получателе должна работать служба "*Оповещатель* " ( *Messenger* ; по умолчанию эта служба отключена);
* *Запустить журнал производительности* — позволяет запустить созданный и настроенный журнал производительности на данном сервере, чтобы начать сбор статистики по интересующим параметрам;
* *Запустить программу* — запустить любую программу (можно при этом задать параметры командной строки, необходимые для программы).

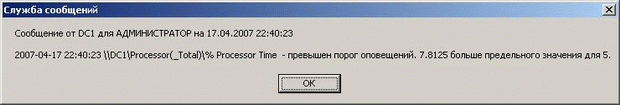
В нашем примере включим первые 2 параметра (рис. 16.31):



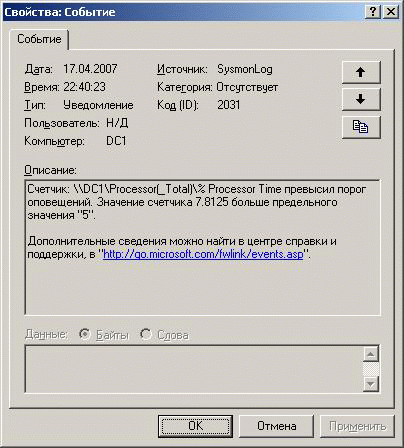
**Рис. 16.31.**

На закладке " *Расписание* " задается расписание запуска данного журнала (установим ручной режим запуска и запустим данный журнал, при этом включим и запустим службу " *Оповещатель* ").

При превышении загрузки процессора порогового значения 5% на экране рабочего места пользователя с именем " *Администратор* " будут появляться сообщения, изображенные на рис. 16.32, а в журнале " *Приложение* " будут регистрироваться аналогичные записи (рис. 16.33).



**Рис. 16.32.**



**Рис. 16.33.**

**Рекомендации по критическим значениям счетчиков**

Определенный набор счетчиков являются очень наглядными индикаторами загруженности системы. Регулярное превышение предельных значений этих счетчиков является показателем перегруженности тех или иных компонент системы. Перечислим эти счетчики в табл. 16.1.

|  |  |  |
| --- | --- | --- |
| **Таблица 16.1.** | | |
| **Счетчик** | **Предельно значение** | **Описание** |
| *Память - Страницы/сек* | 20 | Данный счетчик показывает суммарное количество чтений и записи страниц файла подкачки в секунду. Если значение данного счетчика превышает значение 20, это говорит о том, что в системе идет слишком интенсивный обмен страниц файла подкачки, что, в свою очередь, сигнализирует о недостатке оперативной памяти. |
| *Физический диск - Средняя длина очереди* | Число жестких дисков (число шпинделей) + 2 | Данный счетчик показывает *среднюю длину очереди* системных запросов на выполнение операций ввода/вывода на жесткий диск. Постоянное превышение этого показателя говорит о том, что либо в системе имеется нехватка оперативной памяти (и слишком интенсивный обмен страниц файла подкачки), либо дисковая подсистема недостаточно производительна для выполнения задач, возложенных на данную систему. |
| *Процессор - % Проц. времени* | 85 | Постоянная загруженность процессора более чем на 85% как правило является показателем перегруженности сервера вычислительными задачами.  Хотя иногда высокий показатель является требуемым значением для данного сервера.  В некоторых случаях высокая загруженность процессора может возникать при сбоях в какой-либо подсистеме или приложении. Такие приложения и системные модули надо определять и корректировать ошибки (например, устанавливать исправления или даже удалять некорректные приложения). |
| *Система - Длина очереди процессора* | 2 | Данный счетчик отображает число потоков, ожидающих очереди на исполнение. Очередь потоков хранится в одной области для всех процессоров системы. Если длина очереди систематически превышает 2, процессоры нужно обновлять.  Этот счетчик является более объективным показателем загруженности процессорной системы в многопроцессорных серверах, чем счетчик " *Процессор - % Проц. времени* ". |

В каждой системе могут быть и другие важные счетчики, значения которых показывают те или иные перегрузки или недостаток ресурсов (например, % свободного пространства на логических дисках). Для отдельных приложений имеются свои специфические счетчики (в частности, для MS SQL Server). Описание мониторинга данных счетчиков и их предельные значения приводятся в документации по соответствующим приложениям.

*Мониторинг сетевой активности*

Системы семейства Windows Server позволяют осуществлять мониторинг сетевой активности на низком уровне — на уровне сетевых фреймов, передаваемых и принимаемых сетевыми адаптерами компьютера. Для выполнения этой задачи служит компонента системы " *Сетевой монитор* " (*Network Monitor*). Правда, штатная компонента " *Сетевой монитор* " имеет ограничение — она захватывает только те сетевые пакеты, которые передаются данному компьютеру (на котором запущен "*Сетевой монитор* ") или отправляются с данного компьютера, в том числе широковещательные пакеты. " *Сетевой монитор* " — мощный инструмент для обнаружения различных сетевых проблем и неполадок, позволяющий детально изучать содержимое передаваемых по сети пакетов.

Все данные, пересылаемые по сети от одного сетевого адаптера другому, состоят из фреймов (кадров). Каждый фрейм содержит следующую информацию:

* *Адрес источника (отправителя)* — MAC-адрес сетевого адаптера, с которого отправлен кадр;
* *Адрес назначения (получателя)* — MAC-адрес сетевого адаптера, которому предназначался кадр (этот адрес может также определять группу сетевых адаптеров);
* *Данные заголовка* — информация, содержащая описание для каждого протокола, используемого при передаче кадра;
* *Данные* — передаваемые данные (или часть данных).

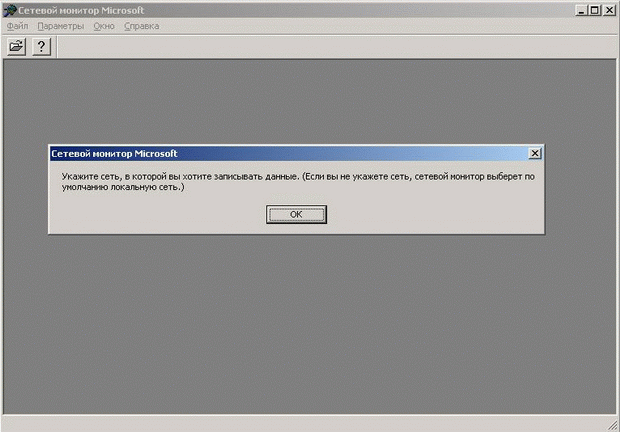
В обычном состоянии каждый сетевой адаптер принимает только те фреймы, которые адресованы данному адаптеру (или всем сетевым адаптерам при отправке широковещательных пакетов). Все остальные фреймы сетевыми адаптерами игнорируются. Все захватываемые в процессе работы " *Сетевого монитора* " фреймы сохраняются в буфере захвата (по умолчанию размер буфера 1 МБ, поэтому " *Сетевой монитор* " хранит только последний мегабайт захваченных фреймов). Захваченные фреймы после окончания процесса захвата и изучения можно сохранить в файле с расширением " .cap " для последующего более детального изучения.

Установка " *Сетевого монитора* "

" *Сетевой монитор* " устанавливается так же, как и другие компоненты системы: " *Панель управления* " — " *Установка и удаление программ* " — кнопка " *Установка компонентов Windows* " — " *Средства управление и наблюдения* " — кнопка " *Состав* " — " *Средства сетевого монитора* ". После установки " *Сетевого монитора* " в разделе " *Администрирование* " *Главного меню* системы появляется соответствующий ярлык.

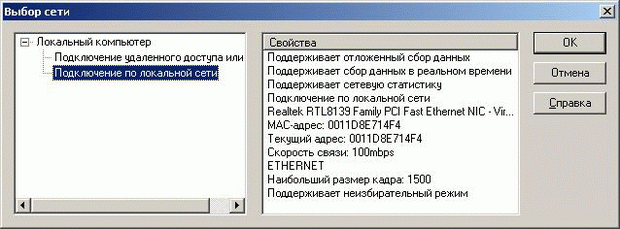
Запуск " *Сетевого монитора* " и выбор сетевого интерфейса

При запуске " *Сетевого монитора* " администратору необходимо выбрать тот интерфейс, для которого будет производиться захват сетевых пакетов. " *Сетевой монитор* " может перехватывать фреймы для различных типов интерфейсов — сетевые адаптеры, модемы, VPN-соединения. После запуска " *Сетевого монитора* " администратор видит запрос, изображенный на рис. 16.34:



**Рис. 16.34.**

Выберем " *Подключение по локальной сети* " (рис. 16.35). Для выбранного подключения программа показывает краткую сводку: модель сетевого адаптера, MAC-адрес адаптера, скорость передачи данных, максимальный размер фрейма (в данном примере — 1500 байт).



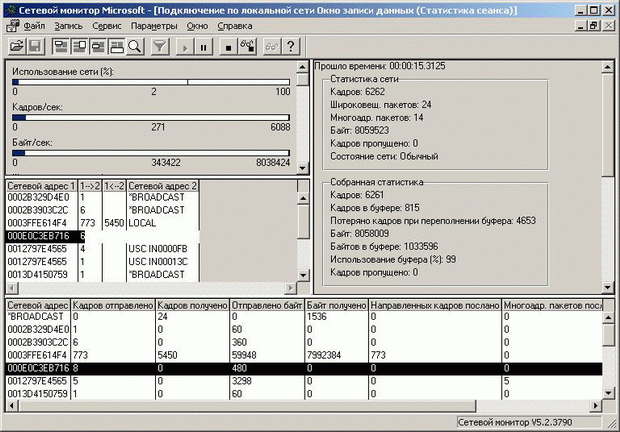
**Рис. 16.35.**

**Первоначальная настройка параметров**

В начале работы можно указать размер буфера захвата для временного хранения перехваченных фреймов: пункт меню " *Запись* " — " *Параметры буфера* ".

Запуск захвата сетевых пакетов

Запуск захвата фреймов осуществляется через меню " *Запись* " — " *Запустить* " или нажатием кнопки " *Начать запись данных* " на панели инструментов (кнопкаКнопка). В процессе работы " *Сетевой монитор* " показывает статистику сетевой активности данного компьютера (рис. 16.36).



**Рис. 16.36.**

Левая верхняя панель показывает процент загруженности сетевого сегмента, скорость передачи кадров и скорость передачи байтов.

Панель слева посередине окна показывает физические адреса адаптеров, с которыми происходит обмен данными.

Нижняя панель показывает детальную статистику обмена пакетами для всех сетевых адаптеров, с которых получены или на которые отправлены фреймы.

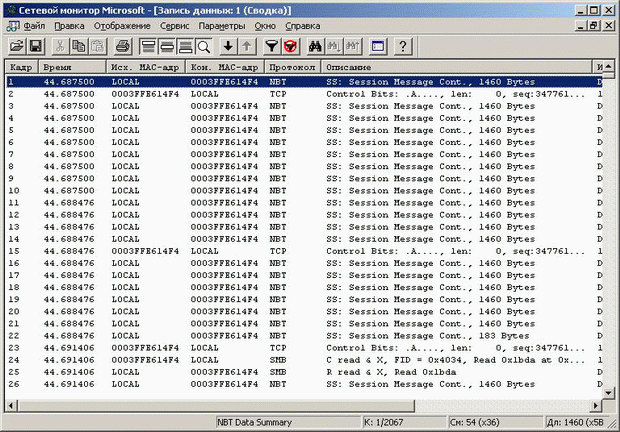
Панель справа вверху показывает общую статистику сети.

Останов захвата пакетов

Для останова процесса захвата фреймов нужно выбрать пункт меню " *Запись* " — " *Остановить* " (просто для останова) или " *Запись* " — " *Остановить и просмотреть*" (чтобы после останова сразу перейти в режим просмотра захваченных фреймов), а также нажатием кнопок соответственно " *Закончить запись данных* " (Кнопка) или " *Закончить запись и отобразить данные* " (Кнопка).

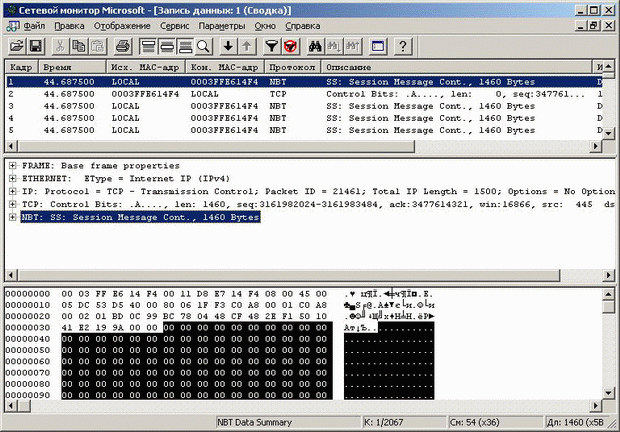
Просмотр захваченных фреймов

Если вы сразу после останова записи фреймов не перешли в режим их просмотра, это можно сделать через меню " *Запись* " — " *Отобразить записанные данные* " или нажатием кнопки " *Отобразить записанные данные* " (Кнопка). Первоначально при переходе в режим просмотра окно " *Сетевого монитора* " примет вид, изображенный на рис. 16.37 (в окне отображается полный список захваченных фреймов с краткой информацией о каждом из них):



**Рис. 16.37.**

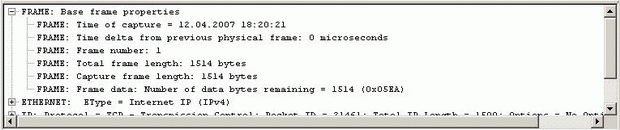
Двойным щелчком мыши на любом из фреймов мы переходим в режим просмотра содержимого захваченных фреймов (рис. 16.38).



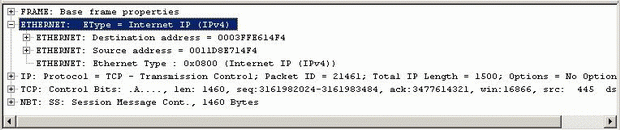
**Рис. 16.38.**

На данном рисунке:

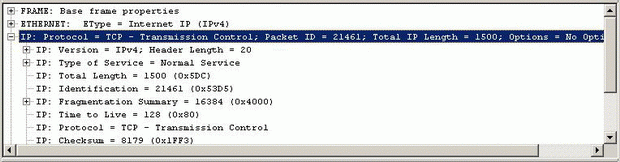
* верхняя панель — полный список захваченных "Сетевым монитором" фреймов;
* средняя панель — структура выделенного в верхней панели фрейма; рис. 16.39 — общие сведения о фрейме (дата, время, размер); рис. 16.40 — информация о протоколе канального уровня Ethernet (физические адреса адаптера-отправителя и адаптера-получателя, тип протокола — IPv4); рис. 16.41 — содержимое заголовка протокола IP; рис. 16.42 — содержимое заголовка протокола TCP; рис. 16.43 — сама информация, передающаяся по сети (в данном случае — информация о сессии протокола NetBIOS);
* нижняя панель — содержимое фрейма в шестнадцатиричном и символьном виде; содержимое той части фрейма, которая выделена в средней панели, в нижней панели выделено инверсным цветом (рис. 16.44).



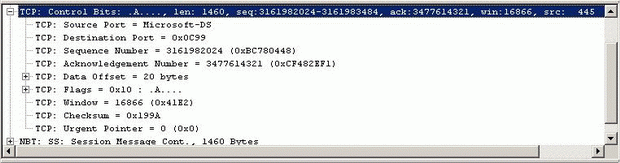
**Рис. 16.39.**



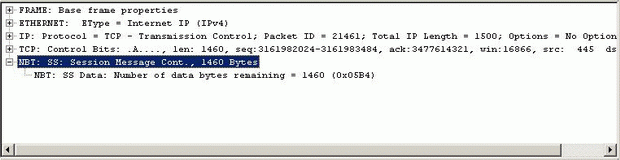
**Рис. 16.40.**



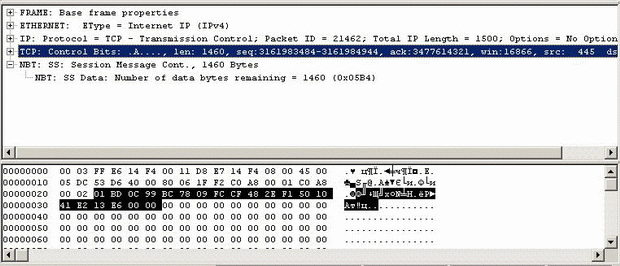
**Рис. 16.41.**



**Рис. 16.42.**



**Рис. 16.43.**



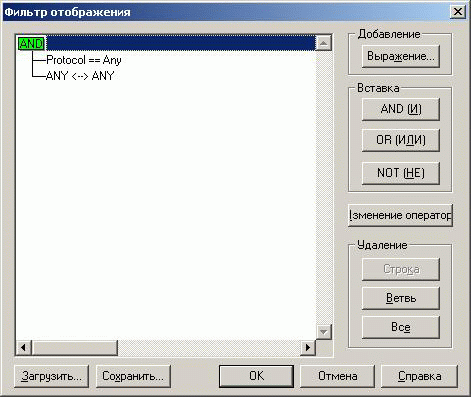
**Рис. 16.44.**

**Фильтрация просматриваемых данных**

В окне просмотра данных, захваченных " *Сетевым монитором* " можно установить фильтры, ограничивающих множество просматриваемых пакетов. Фильтры просмотра используются для отбора кадров по следующим критериям:

* по адресу отправителя или получателя;
* по протоколу передачи кадров;
* по свойствам и значениям, которые содержит кадр.

Включить фильтр просмотра можно через меню " *Отображение* " — " *Фильтр* " или кнопкой " *Изменить фильтр отображения* " на панели инструментов (Кнопка). Панель редактирования фильтра изображена на рис. 16.45:

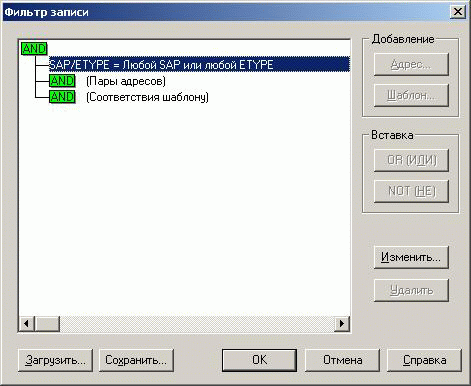


**Рис. 16.45.**

Нажатие кнопок логических операторов AND ( И ), OR ( ИЛИ ), NOT ( НЕ ) и значений выражений можно накладывать условия на тип протокола или адреса компьютеров. По умолчанию выбираются все протоколы (" Protocol == Any ") и все сетевые адреса с передачей пакетов в обоих направлениях (" ANY <-> ANY ").

Фильтрация захватываемых данных

Чтобы уменьшить количество захватываемых фреймов, можно установить фильтр захвата до начала процесса захвата фреймов (меню " *Запись* " — " *Фильтр* "). Нарис. 16.46 изображена панель редактирования фильтра захвата (записи):



**Рис. 16.46.**

**Резюме**

Данный раздел посвящен вопросам мониторинга сетевых узлов и состоит из четырех частей:

* просмотр событий, регистрируемых системой;
* аудит, т.е. целенаправленное отслеживание определенных видов событий;
* мониторинг производительности;
* мониторинг сетевой активности.

Консоль " *Просмотр событий* " позволяет просматривать события, регистрируемые системой и относящиеся к функционированию различных системных компонент:

* самой операционной системы (журнал " *Система* ");
* подсистемы безопасности (журнал " *Безопасность* ");
* подсистемы исполнения приложений (журнал " *Приложения* ");
* службы каталогов (для контроллеров доменов, журнал " *Служба каталогов* ");
* службы DNS (если на сервере установлена служба DNS, журнал " *DNS-сервер* ");
* службы репликации файлов (для контроллеров доменов, журнал " *Служба репликации файлов* ").

Задача сетевого администратора — регулярный просмотр системных журналов с целью своевременного обнаружения уже возникших или предупреждения потенциальных неисправностей или атак злоумышленников. Для более удобного просмотра событий можно создать отдельную консоль, в которой будут отображаться события группы серверов и, возможно, отдельных рабочих станций.

Аудит различных событий заключается в разработке и реализации в системе политик аудита. Набор категорий событий, подлежащих аудиту, необходимо формировать на основе требований безопасности компании/организации и потенциальных угроз системе безопасности.

После определения и настройки политик аудита задача администратора снова сводится к регулярному просмотру журналов событий (в первую очередь — журнала " *Безопасность* ").

Третья часть раздела посвящена описанию мониторинга производительности системы Windows. Рассмотрены два основных инструмента — " *Диспетчер задач* " и консоль " *Производительность* ". " *Диспетчер задач* " предназначен для наблюдения и оценки параметров производительности в реальном времени. Консоль "*Производительность* " позволяет как просматривать параметры производительности в реальном времени, так и накапливать статистику загруженности компонент системы в фоновом режиме с последующим детальным анализом, причем статистика может собираться с нескольких систем одновременно. Работа в режиме оповещений позволяет настроить отправку оповещений администратору в случае отклонения каких-либо параметров от допустимых значений.

Задача сетевого администратора — оценка функционирования системы с точки зрения производительности с целью обнаружения узких мест и принятия решения о перераспределении нагрузки между серверами или приобретении более мощных серверов.

В четвертой части рассказано о мониторинге сетевой активности не сточки зрения производительности и пропускной способности сети, а с точки зрения содержимого передаваемых по сети пакетов (фреймов). Изучение содержимого сетевых пакетов позволяет определить и ликвидировать некоторые сложные*сетевые проблемы*.

Задача сетевого администратора при анализе сетевой активности — поиск сетевых проблем на основе данных, содержащихся в сетевых фреймах.