Практикум. Мониторинг системных и сетевых ресурсов.

Задание.

1. Получите сведения о конфигурации аппаратных и программных средств, установленных драйверах и обновлениях, программных компонентах и т. п.
2. Получите сведения об автоматически загружаемых программах, запущенных сервисах и службах.
3. Работа с диспетчером задач:
    - Получите сведения о запущенных приложениях, процессах, загруженности центрального процессора и оперативной памяти, состоянии сети и пользователей системы.
    - Запустите и принудительно завершите какое-либо приложение, например calc.exe.
    - Зайдите в систему под другой учетной записью и запустите какие-либо 2 приложения либо пусть ваш напарник подключится к вашему компьютеру и запустит какие-либо 2 приложения.
    - Снова зайдите в систему под своей учетной записью. Настройте представление запущенных процессов таким образом, чтобы видеть имена пользователей, запустивших эти процессы. Убедитесь, что вы видите активный статус другого пользователя и запущенные им процессы.
    - Принудительно отключите подключившегося пользователя или пользователя, зашедшего под другой учетной записью (предварительно отправив сообщение о том, что пользователь будет отключен).
    - Принудительно завершите процессы, запущенные другим пользователем.
    - Получите сведения о файлах, связанных с какими-либо запущенными процессами.
4. Оцените загрузку основных компонентов системы, используя значения счетчиков, показанные в виде таблиц, выявите узкие места или приложения (процессы), отнимающие значительную часть ресурсов компьютера.

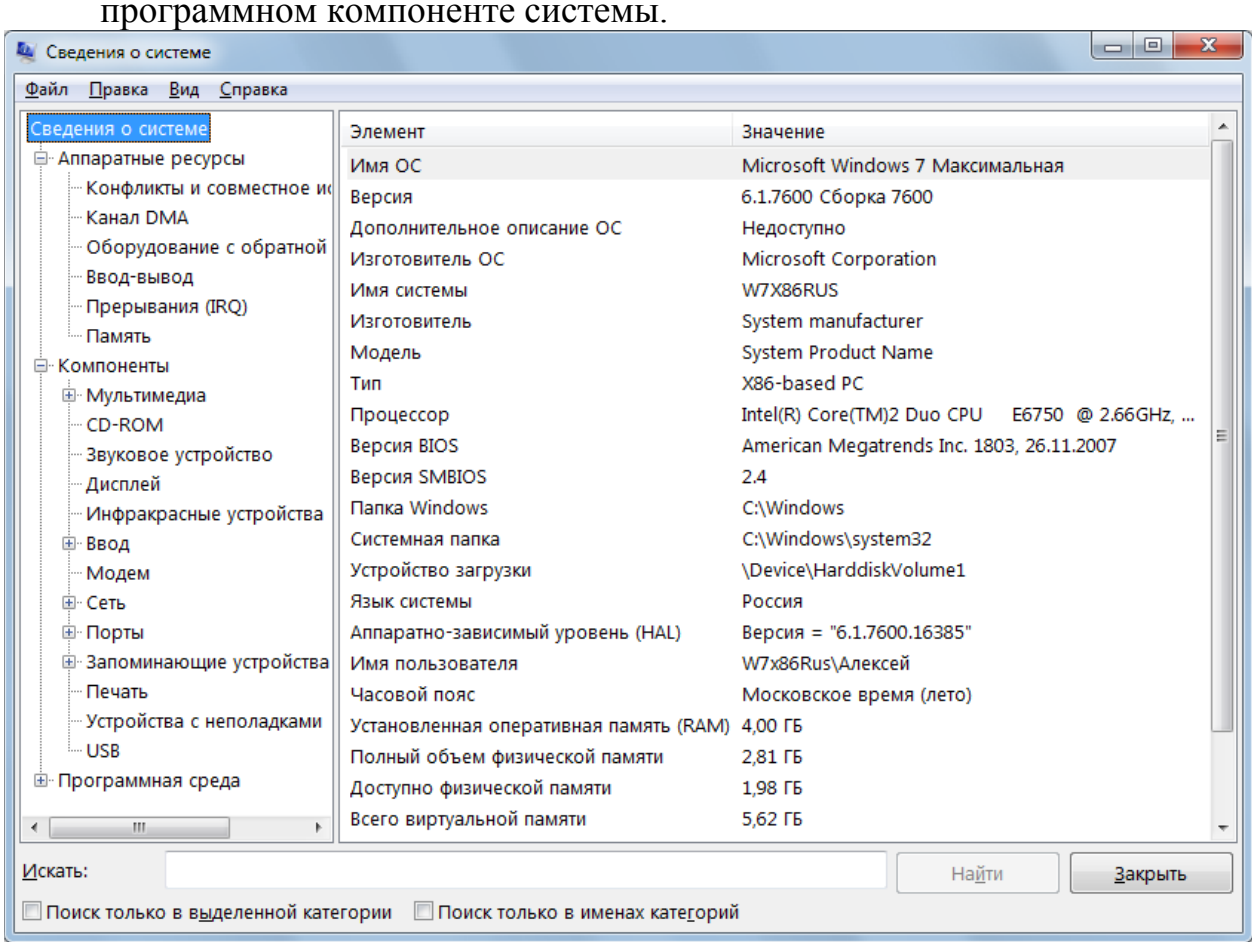
Методические указания по выполнению заданий

Задание 1.

Существует два способа, с помощью которых можно получить полезную информацию о конфигурации аппаратных и программных средств, установленных драйверах и обновлениях, программных компонентах и т. п.

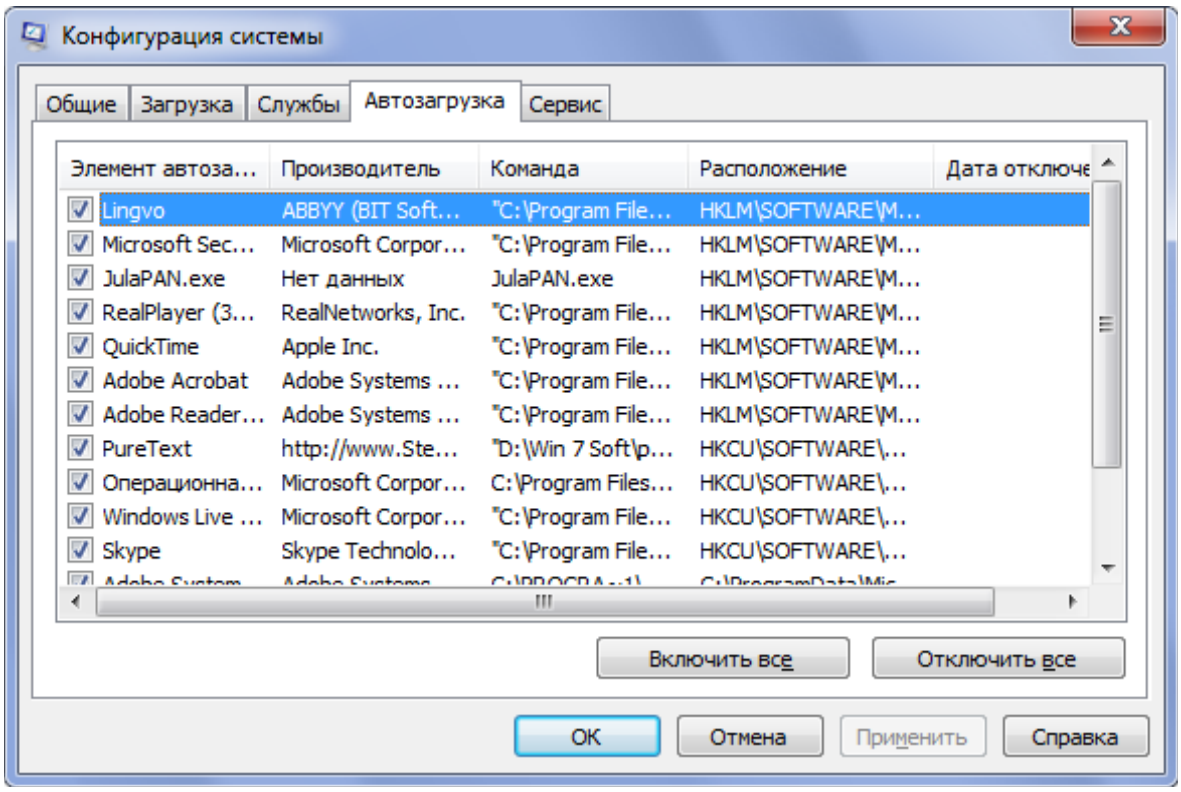
- Уже известная вам утилита командной строки SystemInfo.exe выводит на экран базовую информацию об операционной системе, установленной на локальном или удаленном компьютере (в том числе дату установки, основные параметры оборудования, список установленных обновлений).

- Программа *"Сведения о системе"* (System Information, Msinfo32.exe), запускаемая из папки **Все программы | Стандартные | Служебные** (All Programs | Accessories | System Tools), позволяет получить практически исчерпывающую информацию о каждом аппаратном и программном компоненте системы.



Задание 2.

Программа *"Конфигурация системы"* (System Configuration; Msconfig.exe), запускаемая из подменю **Администрирование** (Administrative Tools). Например, на вкладке **Автозагрузка** (Startup) перечислены программы, запуск которых разрешен при загрузке системы (ненужные приложения можно отключать). Нужно следить за тем, чтобы в этом списке не оказались шпионские и другие зловредные программы. На вкладке **Службы** (Services) указаны все разрешенные службы. Если какой-то сервис мешает нормальной загрузке системы, его можно отключить.



Задание 3.

В системах Windows главным "подручным" средством мониторинга ключевых показателей производительности компьютера является *Диспетчер задач* (Task Manager; taskmgr.exe). С его помощью можно по многим параметрам отслеживать активность запущенных программ и служб и просматривать диаграммы использования процессора и памяти; кроме того, можно находить несанкционированно запущенные приложения, например, вредоносные программы.

Для запуска диспетчера задач можно использовать множество методов.

- Щелкните правой кнопкой мыши по панели задач и выберите в контекстном меню пункт **Диспетчер задач** (Task Manager).
- Нажмите комбинацию клавиш <Ctrl>+<Shift>+<Esc>. Этот метод работает и в окне командной строки, открытом в режиме восстановления системы.
- Нажмите комбинацию клавиш <Ctrl>+<Alt>+<Del> и в окне безопасности нажмите кнопку **Запустить диспетчер задач** (Start Task Manager).
- Откройте окно **Выполнить** (Run) и введите команду taskmgr; можно задать эту команду непосредственно в поле поиска меню **Пуск** (Start).

Если диспетчер задач запущен, то в правом нижнем углу экрана на панели задач в области уведомлений появляется индикатор загрузки процессора. Если подвести указатель мыши к этому индикатору, то будет отображена степень загруженности процессора. Теперь открывать окно диспетчера задач можно, дважды щелкая мышью по данному значку.

Если нежелательно, чтобы свернутое окно диспетчера оставалось на панели задач и нужно, чтобы был виден только его значок, то в окне

диспетчера в меню **Параметры** (Options) установите флажок **Скрывать свернутое** (Hide When Minimized).

По умолчанию окно диспетчера задач отображается поверх всех окон; такое поведение тоже можно изменить, сбросив флажок **Поверх остальных окон** (Always On Top) в меню **Параметры** (Options).

С помощью команды **Выбрать столбцы** (Select Columns) в меню **Вид** (View) можно добавлять на экран новые столбцы показателей для вкладок

Процессы(Processes), **Сеть** (Networking) и **Пользователи** (Users). Для этого в открывающемся диалоговом окне **Выбор столбцов…** (Select … Columns) установите флажки рядом с теми показателями, которые должны быть отображены в таблице, и нажмите кнопку **ОК**.

Скорость обновления показаний

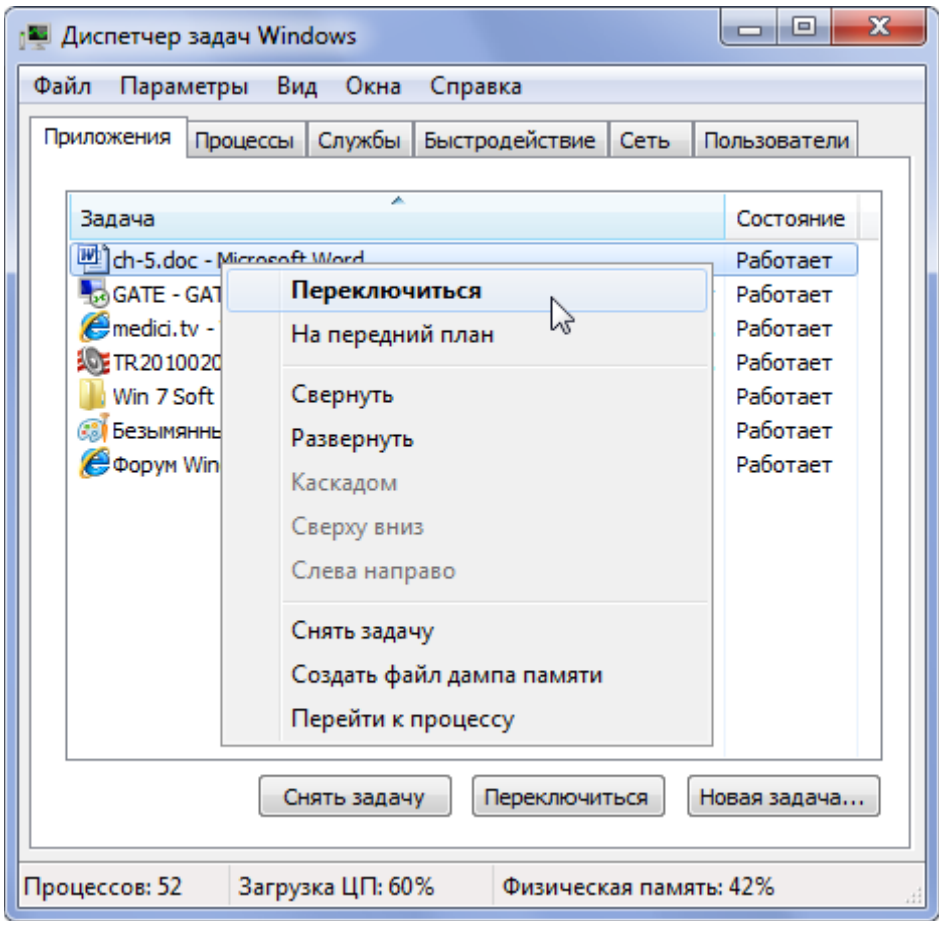
Можно уменьшить или увеличить скорость, с которой обновляются показа-ния диспетчера задач. Это позволяет снизить использование ресурсов при работе диспетчера задач, хотя при низкой скорости обновления показания могут оказаться слишком приближенными. Для выполнения принудительного обновления выполните команду **Обновить** (Refresh Now) в меню **Вид** (View) или нажмите клавишу <F5>.

В диспетчере задач можно задать следующие опции скорости обновления:

- **Высокая** (High) — обновление проводится каждые полсекунды;
- **Обычная** (Normal) — обновление выполняется каждую секунду;
- **Низкая** (Low) — показания обновляются каждые 4 секунды;
- **Приостановить** (Paused) — автоматическое обновление не производит
- ся. Для запуска обновления нажмите клавишу <F5>.

Состояние прикладных программ

На вкладке **Приложения** (Applications) отображается список запущенных программ и их состояние. В том случае, если программа зависла или долго не отвечает, ее можно удалить из памяти с помощью команды **Снять задачу** (End Task). Команда **Переключиться** (Switch To) позволяет быстро перейти в окно выбранной программы. Из данного окна можно запустить любую новую задачу, указав имя исполняемого файла.

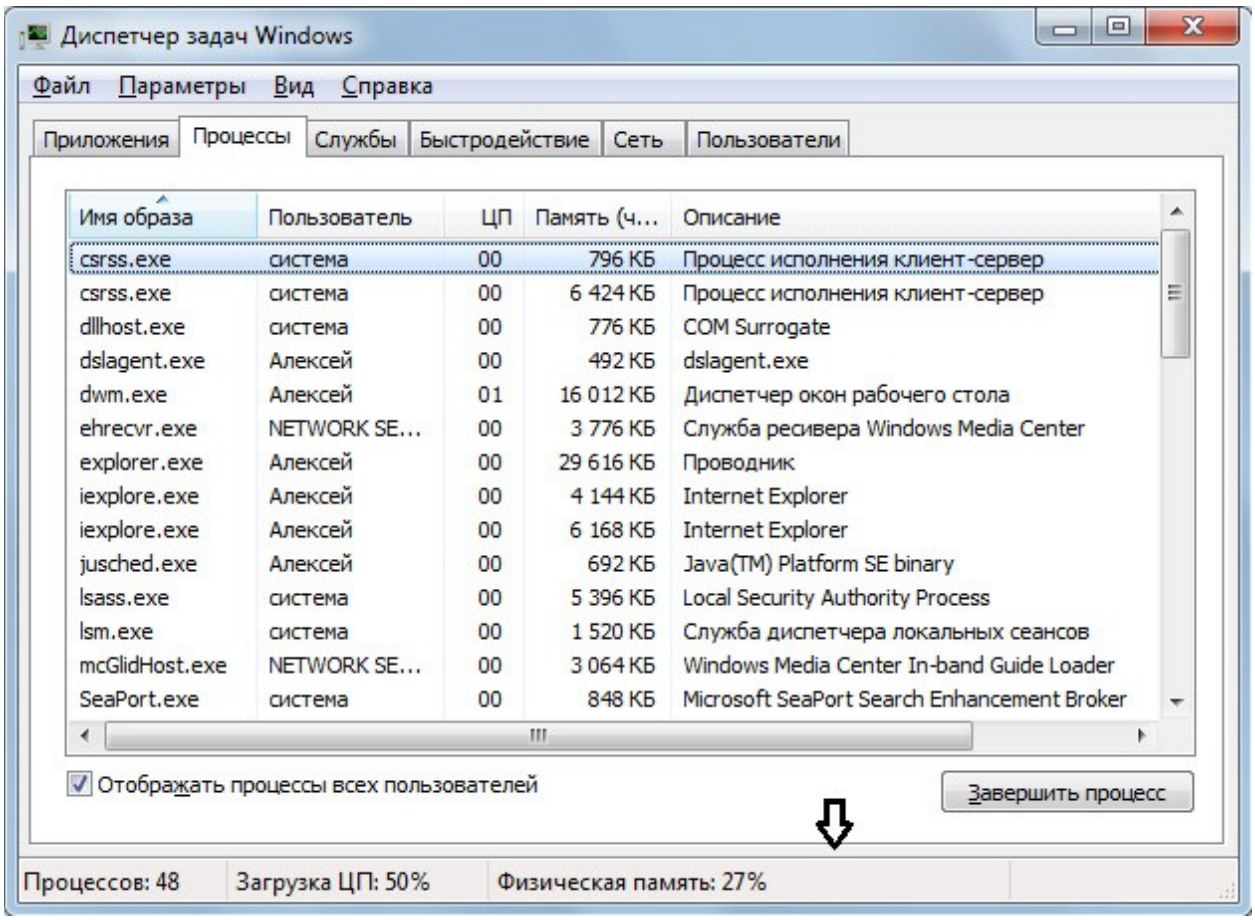


С помощью команды **Перейти к процессу** (Go To Process) легко перейти на вкладку **Процессы** (Processes), где автоматически будет выделен процесс, соответствующий выбранной изначально прикладной программе. Это особенно удобно в тех случаях, когда неизвестно имя исполняемого файла для конкретной программы.

Мониторинг системных и прикладных процессов

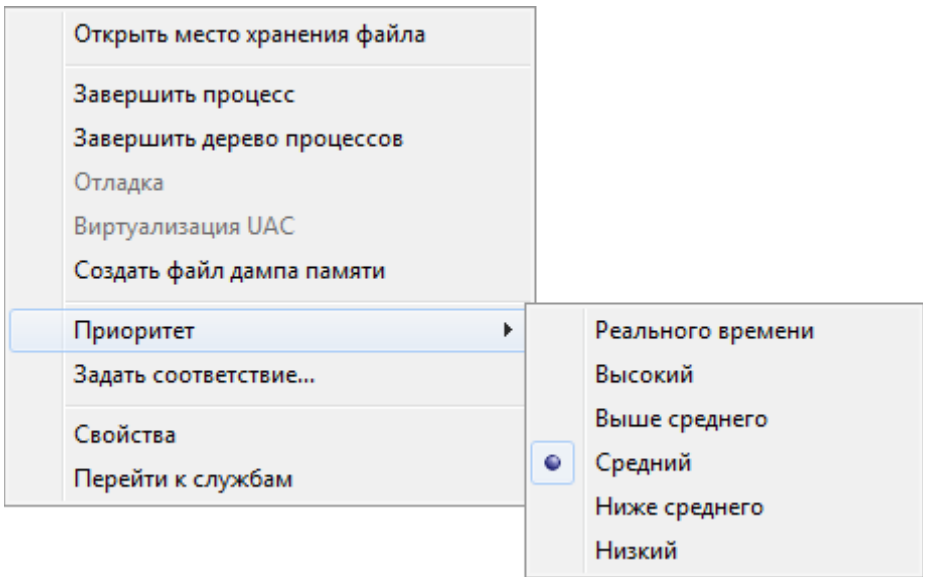
Для просмотра запущенных процессов и показателей их производительности выберите в окне диспетчера задач вкладку **Процессы** (Processes).

Таблица процессов содержит все процессы, запущенные в собственном адресном пространстве, включая все приложения и системные сервисы. Обратите внимание на то, что по умолчанию для каждого процесса отображается его описание — это значительно упрощает анализ происходящего, поскольку не нужно запоминать имена образов десятков процессов и названия соответствующих программ.



В контекстном меню любого процесса присутствуют две важные команды.

1. Открыть место хранения файла (Open File Location) — открывает новое окно Проводника (Windows Explorer), где отображается папка, содержащая исполняемый файл, связанный с данным процессом. Такая функция, например, очень полезна в тех случаях, когда имя и "происхождение" процесса вызывают подозрение (например, если на компьютер попал вирус или "троянский конь") и нужно получить дополнительную информацию о прикладной программе. Здесь также может помочь команда **Свойства** (Properties), с помощью которой открывается окно свойств исполняемого файла - в нем на вкладке **Подробно** (Details) обычно имеются сведения о разработчике приложения, описание программы и т. п.

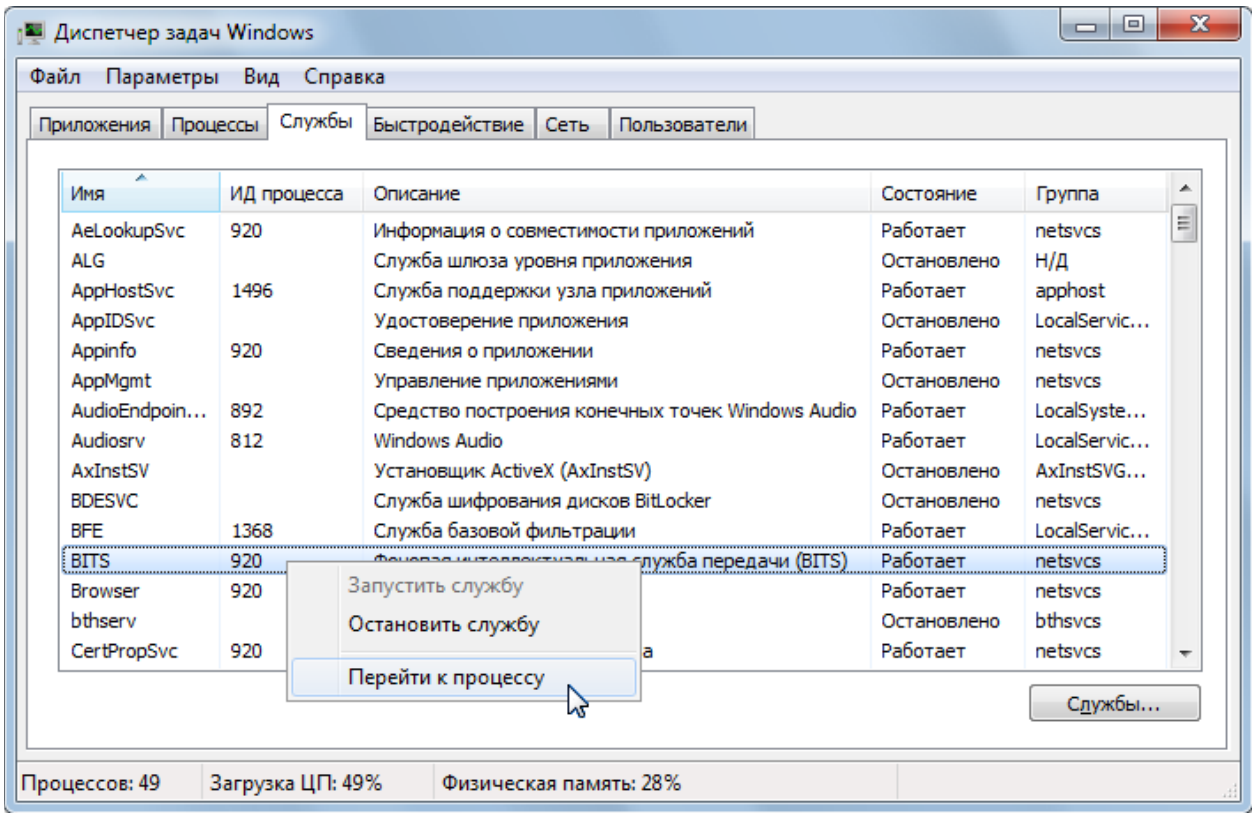


2. Перейти к службам (Go to Service(s)) — выполняет переход на вкладку **Службы** (Services) к службе, соответствующей данному процессу (если таковая имеется).

По умолчанию отображаются процессы только для зарегистрированного пользователя. Администратор может установить флажок **Отображать процессы всех пользователей** (Show processes from all users) и увидеть системные процессы и процессы, запущенные другими пользователями (например, при удаленном доступе или при переключении пользователей).

Проверка состояния системных служб

На вкладке **Службы** (Services) перечислены все службы (сервисы), имеющиеся в системе, дано их описание и указаны текущее состояние и учетная запись безопасности, которая используется при запуске службы. Для каждой работающей службы указан идентификатор (ID) соответствующего процесса (зная этот идентификатор, проще следить за тем, какие ресурсы использует процесс). В этом окне службу можно запустить или остановить; прямо отсюда можно запустить оснастку **Службы** (Services) (см. кнопку в правом нижнем углу).



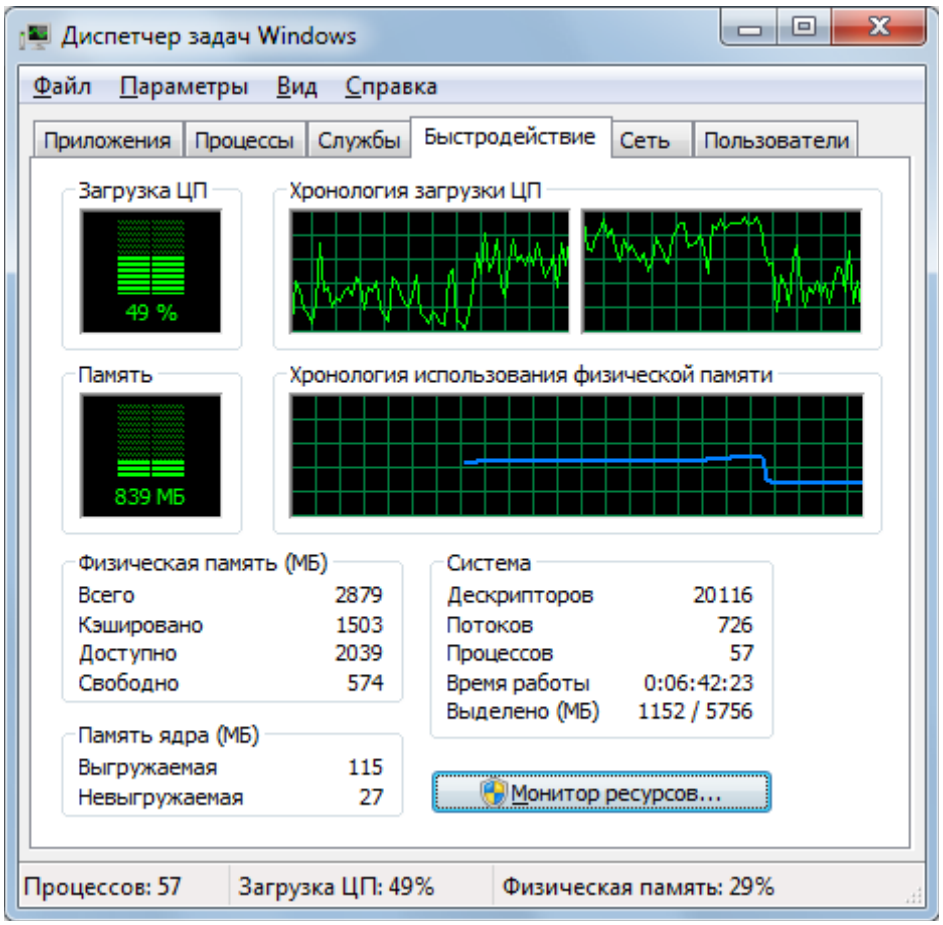
Если в контекстном меню некоторой запущенной службы выполнить коман-ду **Перейти к процессу** (Go to Process), то откроется вкладка **Процессы** (Processes), на которой будет выбран процесс, связанный с этой службой, и, следовательно, можно увидеть, какие ресурсы использует выбранная служба.

Это особенно удобно для процесса svchost.exe, который является хост-процессом для многих системных служб, и не всегда можно понять, какой его экземпляр связан с конкретной службой (или наоборот).

Список многочисленных служб можно сортировать по любому столбцу. Это позволяет, например, выбирать группы по их состоянию или по принадлежности к определенной группе.

Анализ загрузки процессора и памяти

Для отслеживания загрузки системы (процессора и памяти) откройте в окне диспетчера задач вкладку **Быстродействие** (Performance).



Для отображения на диаграмме **Загрузка ЦП** (CPU Usage) доли процессорного времени, в течение которого процессор работал в режиме ядра (это время будет представлено линией красного цвета), установите в меню **Вид** (View) флажок **Вывод времени ядра** (Show Kernel Times).

В многоядерных (многопроцессорных) системах в меню **View** (Вид) по умолчанию выбран переключатель **Загрузка ЦП | По графику на каждый ЦП** (CPU History | One Graph Per CPU), и отображается индивидуальная диаграмма занятости для *каждого* процессора. На рисунке выше видна кнопка **Монитор ресурсов** (Resource Monitor), которая впервые появилась в Windows Vista, но еще больший интерес представляет в Windows 7: нажав эту кнопку, можно перейти в окно одноименного компонента, который в новой версии системы кардинально переработан и предоставляет пользователю намного больше сведений по загрузке процессора, диска, сети и памяти.

Мониторинг сети

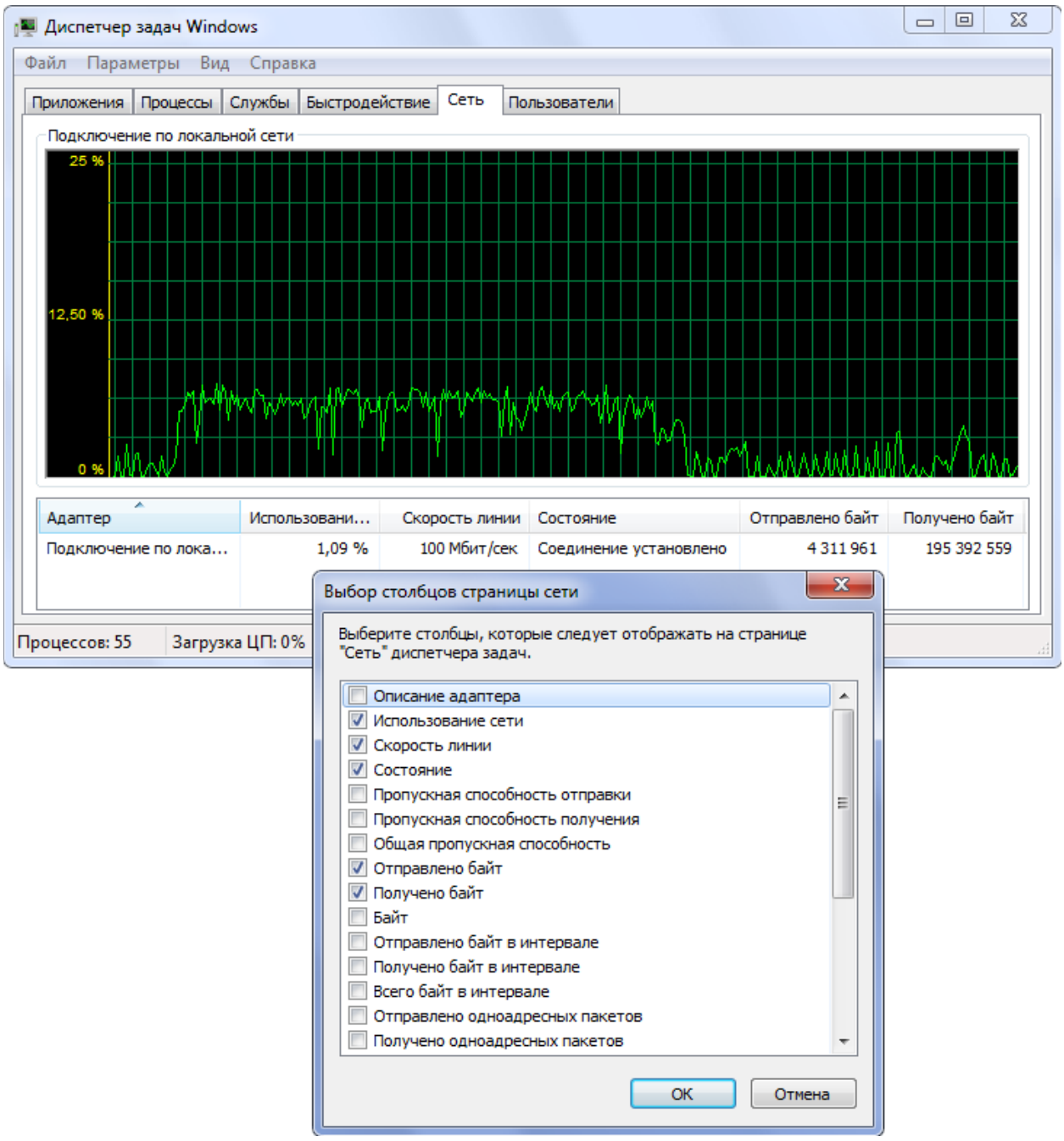
На вкладке **Сеть** (Networking) можно в виде графика видеть объем информации, передаваемой компьютером по сети в каждый момент времени.

Если на компьютере установлены несколько сетевых адаптеров, то на вкладке **Сеть** (Networking) для каждого адаптера будет отображаться отдельная панель, на которой будет представлена кривая, показывающая загрузку конкретного адаптера.

С помощью команды **Вид | Выбрать столбцы** (View | Select Columns) можно перейти в окно отображаемых столбцов и выбрать, к примеру, вывод в таблице числа *полученных* (Bytes Received) и/или *отправленных байтов* (Bytes Sent) для сетевого адаптера.

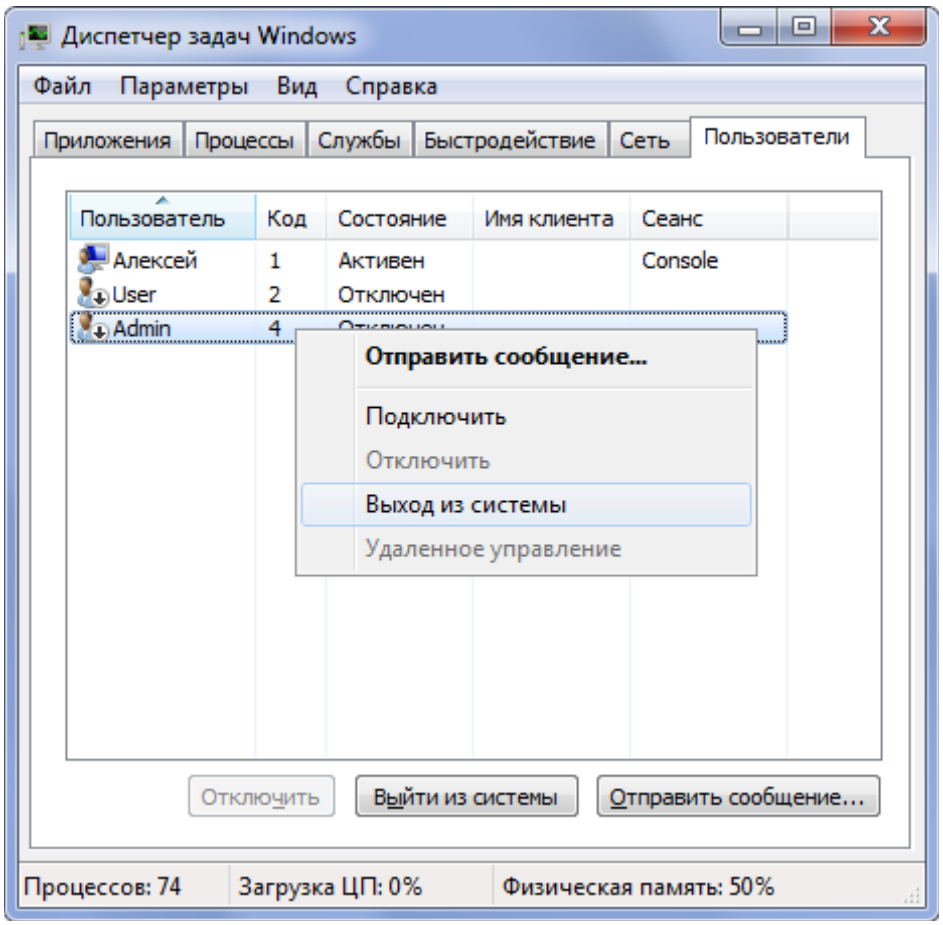
Команда **Вид | Журнал сетевого адаптера** (View | Network Adapter History) позволяет отдельно отображать на графике число полученных (**Получено байт** (Bytes Received)) и/или отправленных байтов (**Отправлено байт** (Bytes Sent)) для сетевого адаптера. При необходимости можно добавить столбцы, в которых будет отображаться общее количество переданных байт, причем если установить флажок **Параметры | Отображать накапливаемые данные** (Options | Show Cumulative Data), то будут учитываться не только те данные, которые были получены при запущенном диспетчере задач, но и суммарные — с момента загрузки системы. Если, например, отображается окно адаптера, через который осуществляется подключение к Интернету, то на вкладке **Сеть** (Networking) можно весьма точно оценивать внешний сетевой трафик (правда, до определенного предела, поскольку после приблизительно 4 Гбайт значения счетчиков сбрасываются).

По умолчанию график загрузки сети появляется на вкладке **Сеть** (Networking) *с момента выбора этой вкладки, и предыдущие показания видеть нельзя. Если в меню* ***Параметры*** *(Options) установить флажок* ***Вкладка всегда активна*** *(Tab Always Active), то информация об использовании сети начинает собираться сразу же после запуска диспетчера задач, даже если вкладка* ***Сеть*** *(Networking) и не открывалась. В этом случае после выбора вкладки можно в виде графика видеть уже накопленные данные.*



Просмотр списка зарегистрированных пользователей

На вкладке **Пользователи** (Users) отображаются имена всех пользователей, зарегистрированных в данный момент на компьютере локально (благодаря наличию опции быстрого переключения пользователей (Fast User Switching)) или удаленно (при использовании функций Удаленный рабочий стол (Remote Desktop) или Удаленный помощник (Remote Assistance)). В первом случае в столбце **Сеанс** (Session) пишется **Console**, а во втором — указывается код сеанса удаленного доступа, например, **RDP-Tcp#0**. На рисунке ниже иллюстрируется ситуация, когда три пользователя зарегистрированы локально в результате выполнения операции смены пользователей (активным может быть только один из них).



На вкладке **Пользователи** (Users) выбранному пользователю можно послать сообщение с помощью команды контекстного меню или кнопки **Отправить сообщение** (Send Message). "Лишних" пользователей можно просто отключить (кнопка **Отключить** (Disconnect); при этом все запущенные пользователем задачи сохраняются, и он сможет вернуться к ним после повторного подключения) или "разрегистрировать" их в системе (кнопка **Выйти из системы** (Logoff); в этом случае пользователь прекращает работу в системе). Для этого, разумеется, нужно иметь права администратора компьютера.

Команда **Подключить** (Connect) в контекстном меню позволяет подключиться к сеансу выбранного пользователя, указав при этом пароль его учетной записи. При этом текущие окна не закрываются, и приложения продолжают работать.

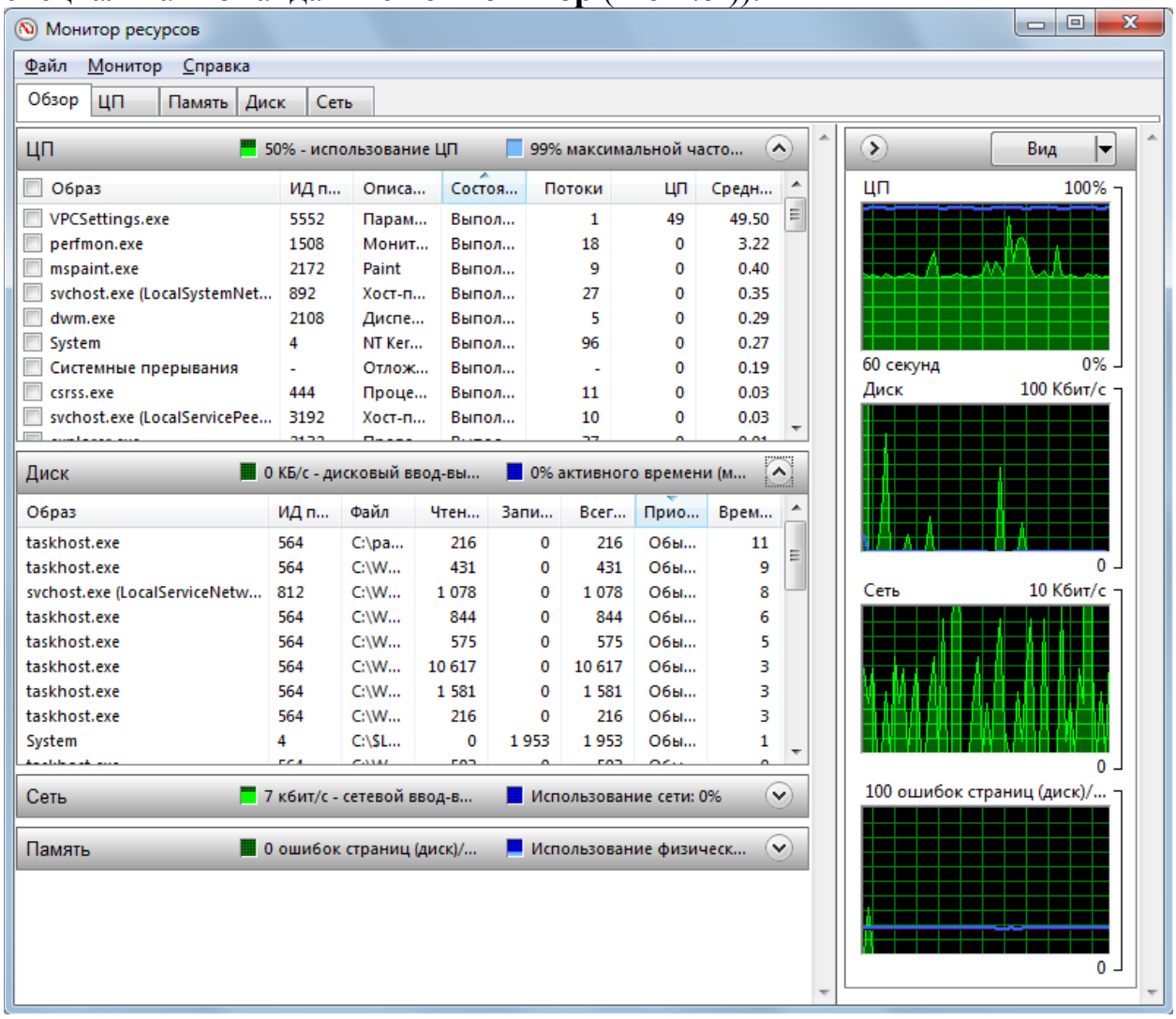
ВНИМАНИЕ! Даже если пользователь, имя которого присутствует в списке на вкладке **Пользователи** (Users), отключен, то программы, запущенные им в течение сеанса работы, будут выполняться. Поэтому отключение пользователя (как и выключение компьютера в подобной ситуации) должно выполняться с осторожностью, нужно учитывать возможность потери данных.

Задание 4.

Новый компонент систем Windows 7 — *Монитор ресурсов*1 (Resource Monitor, resmon.exe) позволяет в реальном времени видеть, как используются процессор, диск, сеть и оперативная память. Монитор ресурсов можно запустить, нажав одноименную кнопку в окне диспетчера задач на вкладке **Быстродействие** (Performance) или выбрав команду в подменю **Пуск | Все программы | Стандартные | Служебные** (Start | All programs | Accessories | System Tools). (Также для запуска можно использовать команду perfmon /res или имя файла программы.)

Общие сведения

Окно монитора ресурсов, открытое на вкладке **Обзор** (Overview), показано на рисунке ниже. Общая информация, представленная в виде графиков в правой части окна программы, позволяет быстро оценить загрузку основных компонентов системы, а значения счетчиков, показанные в виде таблиц, помогают выявить узкие места или приложения (процессы), отнимающие значительную часть ресурсов компьютера. Мониторинг можно вести по каждому процессору в отдельности (для выбора имеется специальная команда в меню **Монитор** (Monitor)).

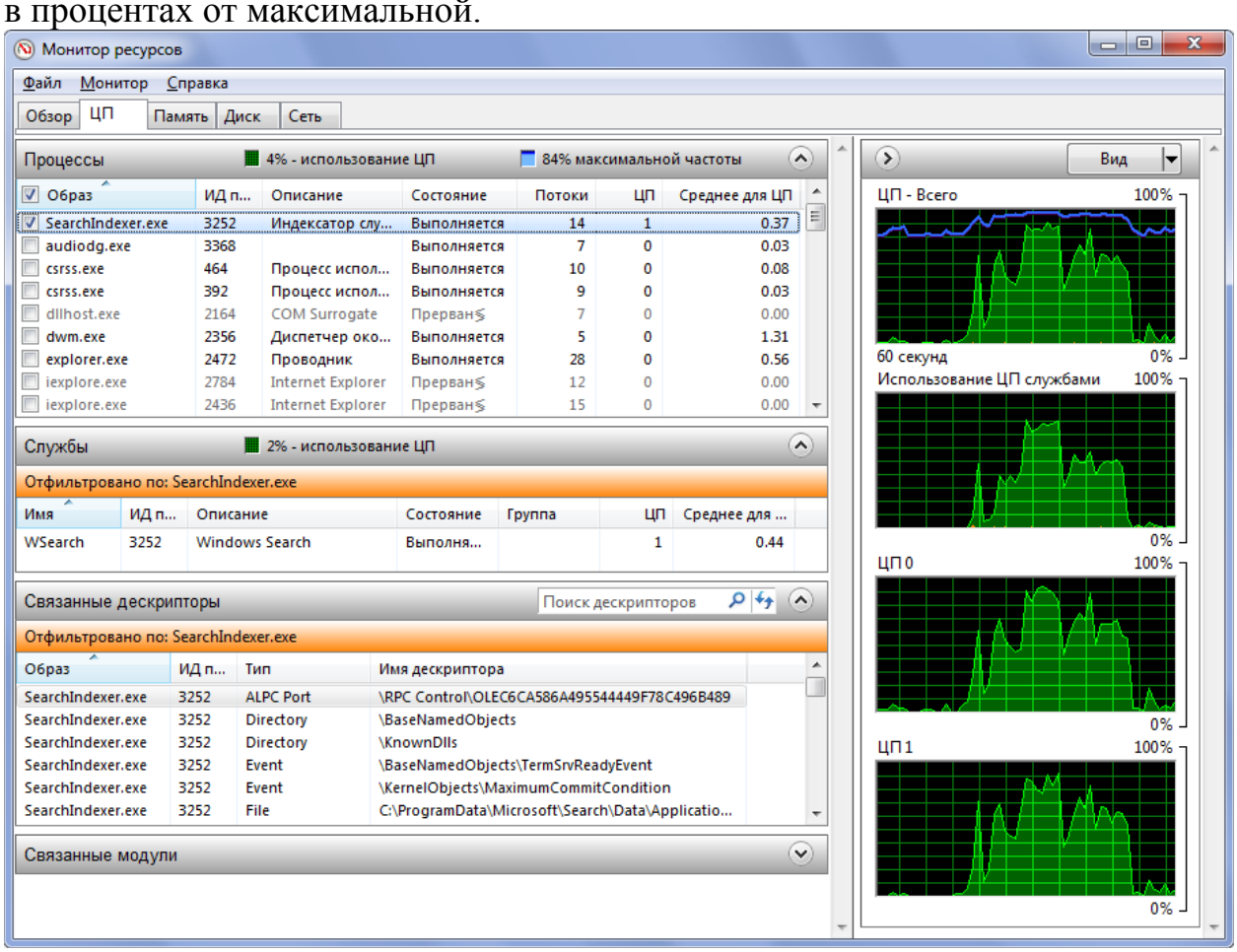


Помимо стандартных столбцов, можно выбирать и дополнительные (как в диспетчере задач). Для некоторых панелей их довольно много, и имеет смысл ознакомиться с имеющимися наборами счетчиков. На рисунке выше обратите внимание на наличие столбца с описанием процесса, он присутствует также и на вкладке **ЦП** (CPU) и помогает ориентироваться в принадлежности процессов.

Другие вкладки в окне монитора ресурсов позволяют более детально контролировать работу отдельных подсистем.

Центральный процессор

На вкладке **ЦП** (CPU) отображается более детальная информация о запущенных процессах (системных и связанных с прикладными задачами) и службах (работающих и остановленных). Показаны графики загрузки процессора в целом и по каждому ядру; отдельно показано использование процессора системными службами. Также отображается частота процессора в процентах от максимальной.



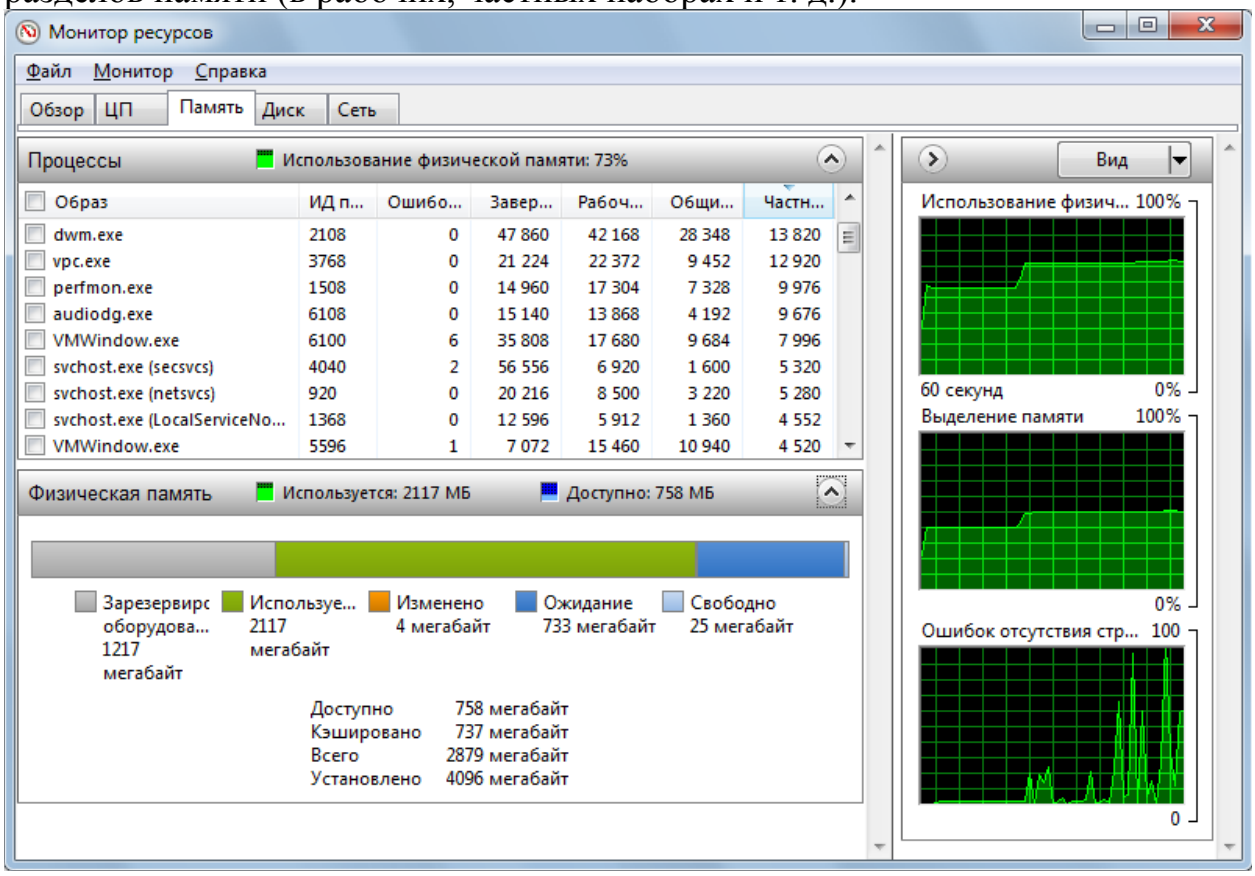
В списке процессов можно также видеть информацию о *прерванных* процес-сах (закрытых приложениях и т. п.). Эти сведения непродолжительное время остаются в окне, и их можно отличить по соответствующей записи в столбце **Состояние** (Status).

Если отфильтровать список процессов, установив флажок около имени интересующего вас процесса, то на соответствующих панелях можно увидеть

списки дескрипторов и связанных модулей, относящихся к данному процессу (которых может быть выбрано несколько).

Память

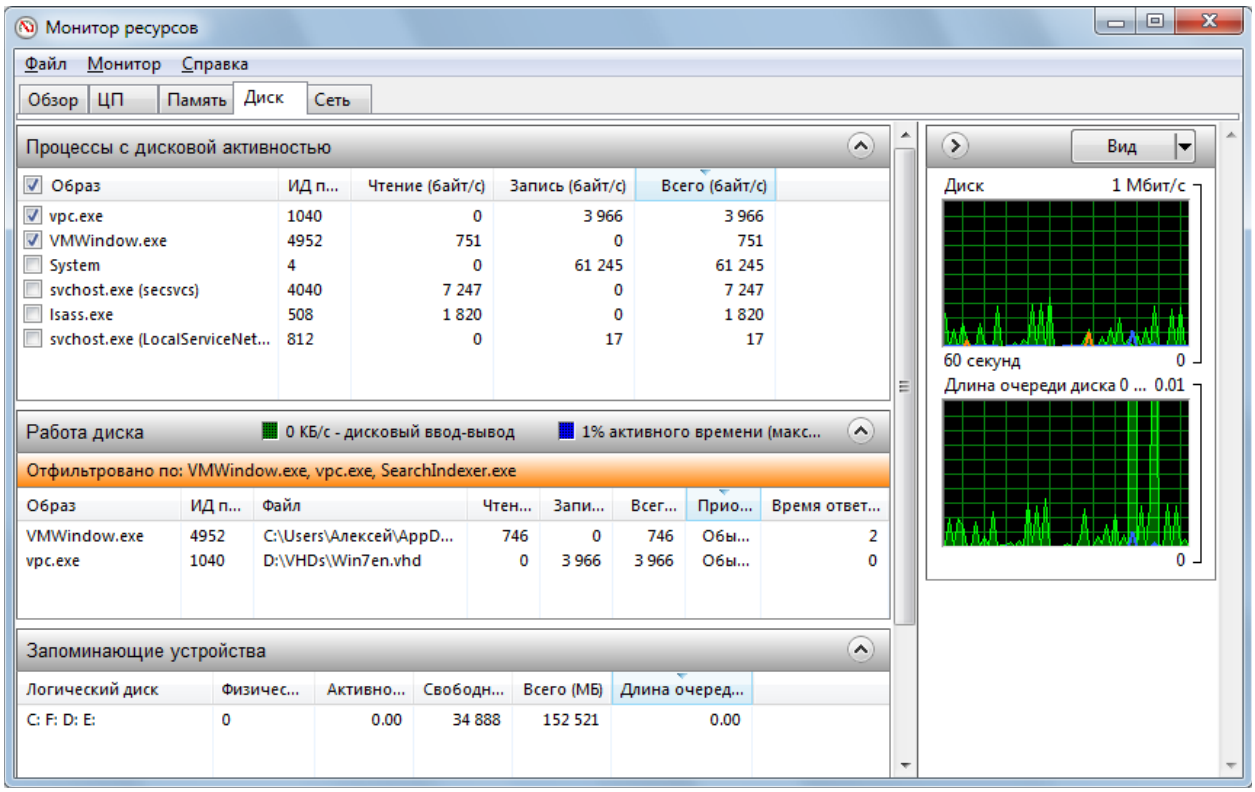
На рисунке ниже представлена вкладка **Память** (Memory), где перечислены запущенные процессы и указаны значения использованных ими разделов памяти (в рабочих, частных наборах и т. д.).



Основные (критичные для оценки производительности компьютера) параметры представлены в виде графиков. (Например, при наличии большого числа ошибок отсутствия страниц в течение *длительного времени* (на протяжении десятков минут или всего времени, пока запущено приложение) можно сказать, что для работающих приложений памяти не хватает.) В нижней части в виде диаграммы показаны общие сведения о распределении физической памяти.

Диск

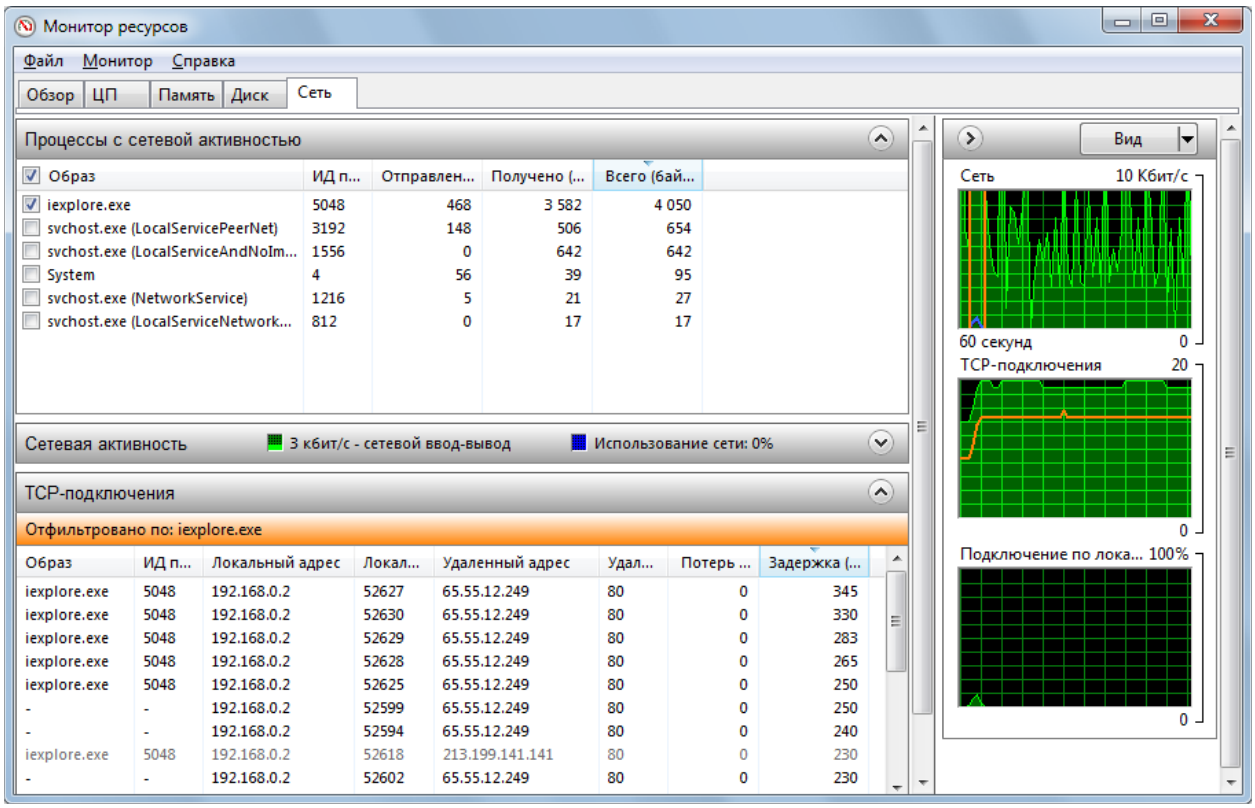
На вкладке **Диск** (Disk) можно видеть, как работает дисковая подсистема. Установив флажки для интересующих вас процессов, можно получить для них более подробную и отфильтрованную информацию (при этом дополнительные столбцы можно включать на всех панелях и на всех вкладках). Все отмеченные процессы отображаются в *начале* списка — это особенно удобно, когда список длинный (он сортируется по именам образов). Выделение процессов распространяется на все вкладки, поэтому для выбранного процесса легко получить данные по всем подсистемам.



Важным показателем при работе с дисками является длина очереди диска (она отображается и графически, и в виде числовых значений). Если в процессе работы каких-то приложений длина очереди все время превышает несколько единиц, то это свидетельствует о серьезной перегрузке дисковой подсистемы, и требуется ее модернизация.

Сеть

На рисунке ниже показана вкладка **Сеть** (Network), где перечисляются все процессы, обращающиеся к сети. Само по себе это уже весьма информативно, поскольку сразу можно увидеть "подозрительные" процессы.



Включив фильтрацию, очень легко получить сведения о том, куда именно обращается программа, какие порты использует и как быстро она получает ответы. Таким образом, упрощается контроль за сетевой деятельностью компьютера.