

## ЛАБОРАТОРНАЯ РАБОТА №14. Работа со встроенной утилитой ОС WINDOWS

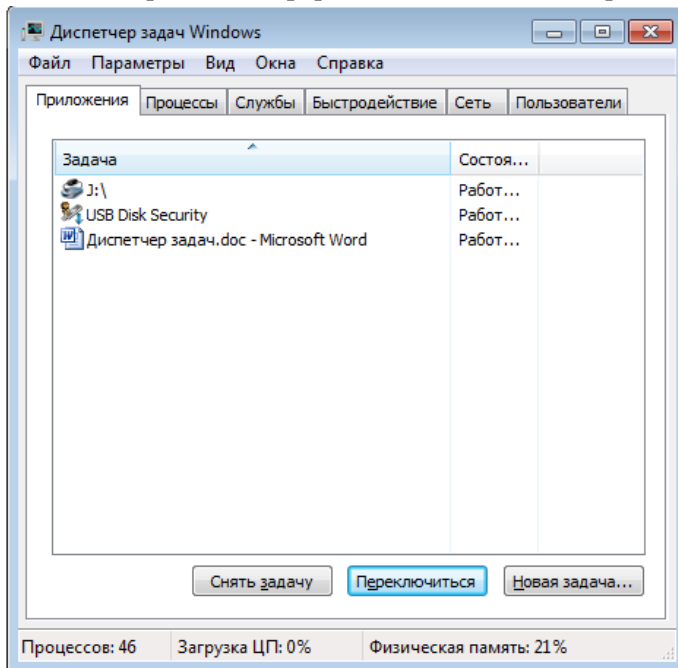
### «Диспетчер задач».

**Цель работы:** получить практические навыки работы с диспетчером задач, изучить его функции и возможности.

#### Задание:

1. Изучите теорию, представленную в методичке.
2. Выполните практические задания и ответьте на вопросы.

**Диспетчер задач** в операционных системах семейства Microsoft Windows – утилита для вывода на экран списка запущенных процессов и потребляемых ими ресурсов (в частности статус, процессорное время и потребляемая оперативная память). Также есть возможность некоторой манипуляции процессами. Другими словами, **Диспетчер задач** – это такая специальная программа, которая показывает нам много разной информации о том, что происходит за компьютером. Что именно показывает диспетчер?



Во-первых, он показывает какие программы запущены на компьютере в данный момент.

Во-вторых, он показывает какие процессы сейчас протекают на компьютере.

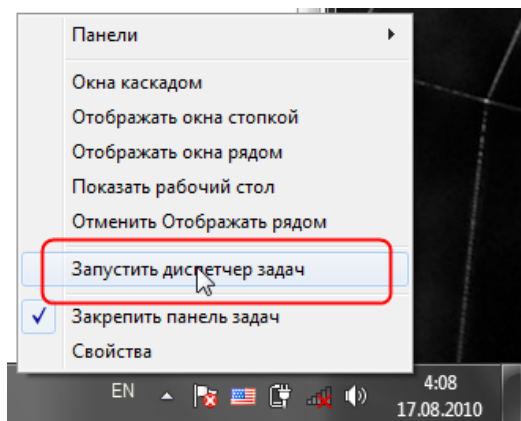
В-третьих – сколько системных ресурсов занимает каждый запущенный процесс и какие ресурсы компьютера процесс занимает.

*Рисунок 1 – Окно программы Диспетчер задач Windows*

#### Способы запуска диспетчера задач

Для запуска диспетчера задач выполните

любое из следующих действий:



1. Щелкните правой кнопкой мыши по пустой области на панели задач и выберите команду Запустить диспетчер задач.

*Рисунок 2 – Окно запуска диспетчера задач*

2. Нажмите клавиши Ctrl+Shift+Esc.

3. Нажмите клавиши Ctrl+Alt+Delete и выберите опцию запустить Диспетчер задач.

После нажатия этих кнопок система выдаст вам довольно обширное меню команд:

- Блокировка компьютера;
- Смена пользователя;
- Завершение сеанса;
- Смена пароля;
- Ссылка же на Диспетчер Задач находится в самом низу этого списка.

4. Нажмите кнопку Пуск, введите в поле Найти слово taskmgr и нажмите клавишу Enter.

Окно Диспетчер задач Windows под основным меню (**Файл, Параметры, Вид, Окна, Завершение работы, Справка**) содержит 6 вкладок, каждая из которых представляет полезную информацию:

- Вкладка *Приложения*. Здесь можно найти список запущенных приложений и их состояние.
- Вкладка *Процессы*. Перечислены все программы и процессы, запущенные в системе, – это основное окно для прекращения работы «зависших» программ или процессов.
- Вкладка *Службы*. Содержит список программ, которые работают в фоновом режиме.
- Вкладка *Быстродействие*. Основная вкладка для оценки производительности операционной системы.
- Вкладка *Сеть*. Отображает объём передаваемых по локальной сети данных.
- Вкладка *Пользователи*. С помощью этой вкладки можно увидеть список всех пользователей, подключенных к вашему компьютеру по локальной сети. В противном случае будет указана только одна учётная запись пользователя.

### **Вкладка «Приложения» (подраздел «Процессы» в новых версиях)**

Переходим на неё, нажимая левой кнопкой мыши. Перед нами список запущенных приложений и два столбца: столбец «Задача» и столбец «Состояние».

Ищем приложение с состоянием «Не отвечает», либо «Не работает», зависит от Windows. Выделяем приложение с таким состоянием, щёлкая левой кнопкой мыши по названию в столбце «Задача».

Нажимаем на кнопку «Снять задачу». Если из списка программа сразу исчезла, то это означает, что она завершилась.

В основном зависшая программа работает некорректно и её придётся завершить вынужденно. В этом случае появится окошко с вопросом: «Завершить сейчас?», нажимаем на кнопку «Завершить сейчас».

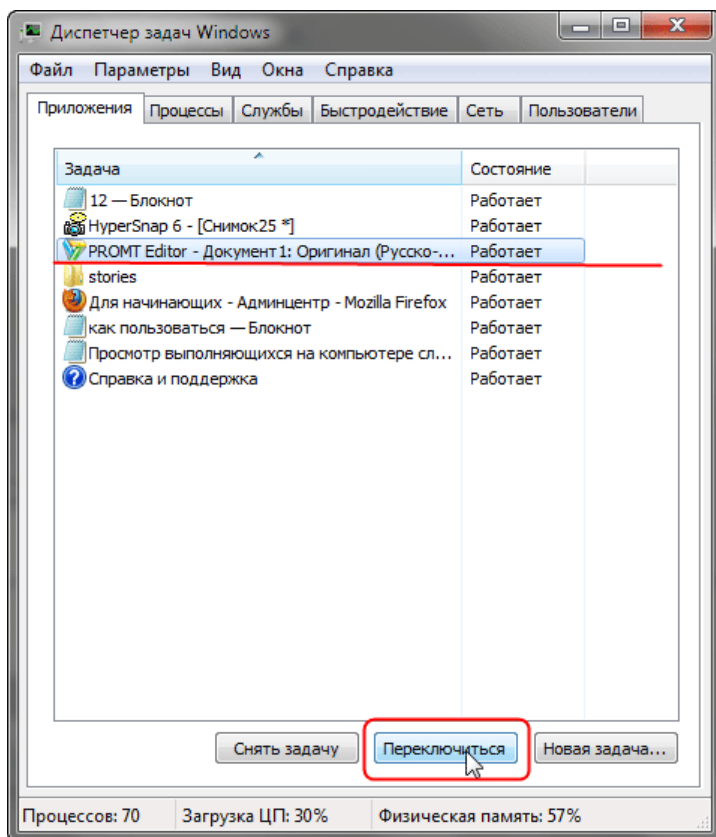
Все несохранённые изменения, выполненные в этом приложении, будут потеряны. Если несохранённые данные важны для пользователя, есть смысл дождаться отклика программы.

«Программы, которые зависли/дали сбой, в среде Windows называются «неотвечающими»; пользователь может поместить курсор мыши в окно программы, но она не будет реагировать на щелчки мыши или нажатия клавиш. Если программа не отвечает, это не значит, что пользователь должен перезагружать компьютер. Воспользуйтесь Диспетчером задач и закройте зависшую программу. Перед тем как закрывать программу, убедитесь в том, что она действительно не отвечает. Подождите некоторое время; возможно, операционная система Windows пытается выделить для программы дополнительные ресурсы памяти. Например, если пользователь запускает макрос VisualBasic в программе MicrosoftExcel или Word, ему может показаться, что программа «зависла». Сложное изменение форматирования или выполнение операций по поиску и замене в объёмном документе могут создать впечатление того, что текстовый редактор «не отвечает». Открытое диалоговое окно или окно сообщения могут не позволить пользователю выполнять никакие действия в определенной программе; поищите их под текущим окном.»

Если какая-либо программа часто «зависает», то можно попробовать найти решение этой проблемы в интернете, создав отчет об ошибке.

Отчеты об ошибках Windows можно использовать, чтобы сообщать в корпорацию Майкрософт о проблемах на компьютере. Корпорация Майкрософт использует отчеты о проблемах для поиска решений, соответствующих описаниям проблем. В ОС Windows отображается уведомление при наличии возможных решений проблемы, а также о возможности поиска дополнительных сведений в Центре поддержки. Если же решения нет, то сведения, отсылаемые в сообщении о проблеме, могут помочь Microsoft найти или создать новое решение.

Если решение проблемы, о которой сообщил компьютер, существует, оно появится в Центре поддержки.



Кнопка Переключиться – откроет выделенную программу.

Рисунок 8 – Кнопка переключиться

Кнопка Новая задача – откроет диалоговое окно Выполнить. С помощью команды Выполнить можно быстро запускать программы, открывать файлы и папки, а также переходить на веб-сайты, если компьютер подключен к Интернету.

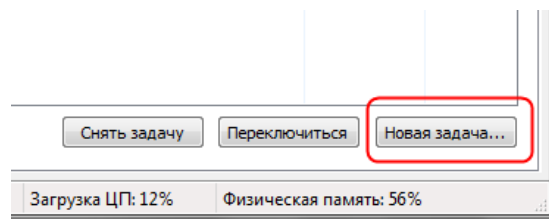


Рисунок 9 – Новая задача

С каждой программой, выполняемой на компьютере, связан определенный процесс, который запускает эту программу. Если программа перестает отвечать (или «зависает»), определение связанного с этой программой процесса может помочь в устранении возникших неполадок. Например, если известно, какой процесс используется для запуска данной программы, то чтобы закрыть зависшую программу, необходимо завершить этот процесс.

Чтобы определить, какой процесс используется программой, щелкните правой кнопкой мыши нужную программу и выберите команду Перейти к процессу. Связанный с данной программой процесс будет выделен на вкладке Процессы.

1. Проверьте все способы запуска Диспетчера задач, занесите в отчёт, запомните для себя самый подходящий способ.
2. Посмотрите с помощью Диспетчера задач (вкладка «Приложения»), какие задачи у пользователя работают в данный момент.
3. Как в новой версии запустить новую задачу?

### Вкладка «Процессы»

Для просмотра сведений о процессах, выполняющихся в данный момент на компьютере, можно использовать Диспетчер задач.

**Процесс** – это файл, например, исполняемый файл, имя которого заканчивается расширением EXE. Этот файл используется компьютером для непосредственного запуска программ и других служб в специально выделенной для него области оперативной памяти. Каждое запущенное приложение имеет соответствующий ему процесс.

Перейдите на вкладку **Процессы**. В диспетчере задач отображаются процессы, выполняющиеся в данный момент под текущей учётной записью пользователя.

Сколько процессов выполняется на данный момент времени, можно увидеть в нижней части диспетчера.

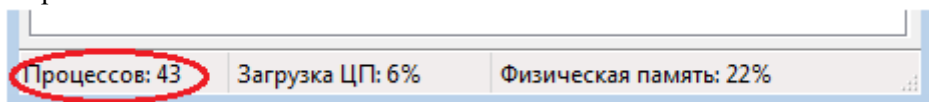


Рисунок 12 – Наличие процессов

В действительности процессов может быть намного больше. Где остальные процессы и почему они скрыты? Всё дело в том, что по умолчанию отображаются лишь процессы, на которые может влиять пользователь. Стоит лишь установить флажок *Отображать процессы всех пользователей*, как в основном окне появятся все процессы, поскольку будут добавлены процессы с атрибутами SYSTEM (системные процессы), NETWORK (сетевые процессы) и LOCALSERVICE (локальные службы). Останавливать выполнение этих процессов не рекомендуется, поэтому не устанавливайте данный флажок без необходимости.

По умолчанию для каждого процесса отображается следующая информация:

- *Имя образа*– название процесса;
- *Пользователь* – имя пользователя, запустившего процесс;
- *ЦП*– процент мощности процессора, используемый процессом;
- *Память (частный рабочий набор)* – объём памяти, используемый процессом в ходе работы.

### Распространённые процессы:

**svchost.exe**– это главный системный процесс для тех служб, которые запускаются из динамически загружаемых библиотек (DLL-файлов). И действительно несколько экземпляров процесса svchost.exe могут быть запущены одновременно (но с разными PID\* (PID — это идентификатор пакета.)). Так как каждый из таких экземпляров представляет собой определённую преимущественно системную службу или же группу служб. Эти группы определены в следующем разделе реестра:

#### HKEY\_LOCAL\_MACHINE Software Microsoft WindowsNT Current VersionSvcHost

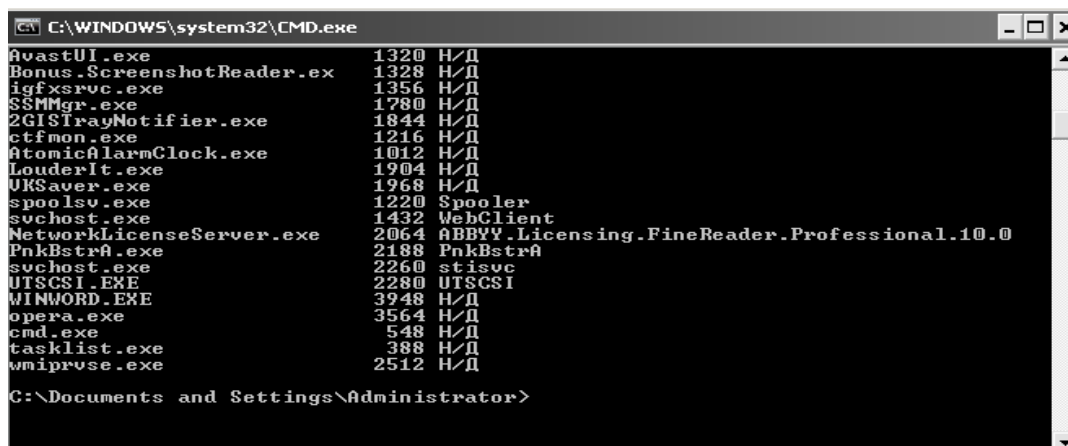
Каждое значение в этом разделе представляет отдельную группу Svchost и отображается при просмотре активных процессов как отдельный экземпляр. Каждое из этих значений имеет тип REG\_MULTI\_SZ и содержит службы, выполняемые в этой группе Svchost. Каждая группа Svchost может содержать одно или несколько имен служб, извлекаемых из следующего раздела реестра, в котором подраздел Parameters содержит значение ServiceDLL:

#### HKEY\_LOCAL\_MACHINE\System\CurrentControlSet\Services\Служба

Чтобы просмотреть список служб, работающих в процессе Svchost, выполните описанные ниже действия.+

1. Запустите командную строку.
2. Введите команду Tasklist /SVC и нажмите клавишу ENTER.
3. Перечислите процессы, обеспечивающие работу более, чем одной службы.

Команда Tasklist выводит список активных процессов



```
C:\WINDOWS\system32\CMD.exe
AvastUI.exe           1320  H/П
Bonus.ScreenshotReader.exe 1328  H/П
igfxsvc.exe          1356  H/П
SSMgr.exe            1780  H/П
2GISTrayNotifier.exe 1844  H/П
ctfmon.exe           1216  H/П
AtomicAlarmClock.exe 1012  H/П
LouderIt.exe         1904  H/П
UKSaver.exe          1968  H/П
spoolsv.exe          1220  Spooler
svchost.exe          1432  WebClient
NetworkLicenseServer.exe 2064  ABBYY.Licensing.FineReader.Professional.10.0
PnkBstrA.exe         2188  PnkBstrA
svchost.exe          2260  stisvc
UTSCSI.EXE           2280  UTSCSI
WINWORD.EXE          3948  H/П
opera.exe            3564  H/П
cmd.exe              548   H/П
tasklist.exe         388   H/П
wmiprvse.exe         2512  H/П

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

Рисунок 13 – Список активных процессов

Параметр /SVC используется для вывода списка активных служб в каждом процессе. Для получения дополнительных сведений о процессе введите следующую команду и нажмите клавишу ENTER:

***Tasklist /FI «PID eq идентификатор\_процесса» (кавычки обязательны).***

Получите дополнительные сведения о процессе, ассоциированном с Диспетчером задач.

**DLL**(англ. Dynamic-linklibrary–динамически подключаемая библиотека)–понятие операционных систем MicrosoftWindows и IBMOS/2; динамическая библиотека, позволяющая многократное применение различными программными приложениями. KDLL относятся также элементы управления ActiveX и драйверы. В мире UNIX аналогичные функции выполняют т. н. sharedobjects («разделяемые объекты»).

### **Цели введения DLL**

Первоначально предполагалось, что введение DLL позволит эффективно организовать память и дисковое пространство, используя только один экземпляр библиотечного модуля для различных приложений. Это было особенно важно для ранних версий MicrosoftWindows с жёсткими ограничениями по памяти. Далее, предполагалось улучшить эффективность разработок и использования системных средств за счёт модульности. Замена DLL–программ с одной версии на другую должна была позволить независимо наращивать систему, не затрагивая приложений. Кроме того, библиотеки DLL могли использоваться разнотипными приложениями — например, MicrosoftOffice,MicrosoftVisualStudioи т. п.

В дальнейшем идея модульности выросла в концепцию COM (ComponentObjectModel – объектная модель компонентов, компьютерная технология, разработанная компанией Microsoft.)

Фактически, полных преимуществ от внедрения DLL (Dynamic-linklibrary –библиотека динамической компоновки) получить не удалось по причине явления, называемого DLLhell («ад DLL»). DLLHell возникает, когда несколько приложений требуют одновременно различные, не полностью совместимые, версии DLL–библиотек, что приводит к сбоям в этих приложениях. Когда система выросла до определённых размеров, количество DLL стало превышать многие тысячи килобайт не все из них обладали полной надёжностью и совместимостью, и конфликты типа DLLHell стали возникать очень часто, резко понижая общую надёжность системы. Поздние версии MicrosoftWindows стали разрешать параллельное использование разных версий DLL, что уничтожало преимущества изначального принципа модульности.

Пользуясь командой WHERE и шаблоном поиска найдите все DLL-файлы в папке c:\windows (поиск должен быть рекурсивным, т.е. по всем вложенным папкам). Сделайте скриншот фрагмента поиска, назовите общее число таких файлов.

**Службы Windows** (англ. WindowsService, сервисы) – приложения, автоматически запускаемые системой при запуске Windows и выполняющиеся вне зависимости от статуса пользователя. Имеет общие черты с концепцией. В процессе загрузки на основании записей в реестре Svchost.exe составляет список служб, которые необходимо запустить. Одновременно могут быть запущены несколько экземпляров процесса Svchost.exe. Каждый сеанс Svchost.exe содержит группу служб, следовательно, отдельные службы могут выполняться в зависимости от того, как и когда был запущен Svchost.exe. Таким образом улучшается контроль и упрощается отладка. Файл Svchost.exe расположен в папке %SystemRoot%\System32. В других каталогах под именем Svchost.exe может скрываться вирусы (Троянская программа, вирус или сетевой червь). Наиболее известные злонамеренные программы, скрываются под именем системного процесса Svchost.exe – W32.Welchia.Worm, W32/Jeefo и W32.Assarm@mm. В этом случае злонамеренный процесс должен быть немедленно завершён.

С помощью команды ECHO и параметра %SystemRoot% выведите путь до системной папки. Приведите примеры нескольких переменных среды Windows 10, исследовав этот вопрос самостоятельно.

**csrss.exe**– процесс управляет отображением окон в Windows. Если пользователь откроет новое окно, доступ к нему обеспечит csrss.exe. Одновременно csrss.exe отвечает и за управление другими

процессами. Если пользователь обнаружил более двух записей csrss.exe в списке Диспетчера задач и эти файлы сильно загружают процессор, это означает что за этим скрывается вредоносная программа. В этом случае выполните проверку вашего компьютера с помощью программ Антивирус Касперского или Dr.Web.

**smss.exe**— процесс отвечает за запуск сеансов пользователей. Данный процесс запускается системным потоком и отвечает за различные действия, в частности, за запуск процессов winlogon и win32 (csrss.exe) и за установку системных переменных. После того как указанные процессы запущены, процесс smss ожидает завершения работы winlogon или csrss. Если это происходит «нормально», система может завершить свою работу; если же это происходит неожиданным образом, smss.exe вызывает зависание системы (система перестаёт реагировать на запросы).

**lsass.exe**— процесс отвечает за программы и настройки безопасности Windows и поэтому очень важен. lsass.exe очень часто является целью хакерских атак. Поэтому следует внимательно следить за этим процессом в Диспетчере задач. Если lsass.exe заражён, не стоит самостоятельно пытаться завершить этот процесс или удалить файл. С этой задачей прекрасно справится Антивирус Касперского, он в состоянии вылечить файлы. Многие вирусы используют для маскировки маленькую хитрость – в списке Диспетчера задач в их имени вместо прописной буквы «i» используется заглавная буква «I».

**explorer.exe**— процесс отвечает, в частности, за отображение Рабочего стола и содержания дисков. Очень часто можно встретить вирусы или «программы-шпионы», которые используют имя explorer.exe. Подобные вредители и «настоящий» файл, как правило, находятся в разных папках.

**ctfmon.exe**— процесс управляет технологиями альтернативного ввода данных. Он запускает языковую панель в системе при старте операционной системы, и работает в фоновом режиме даже после закрытия всех программ пакета Microsoft Office, независимо от того, запускались ли программы Office XP.

**avp.exe**— процесс, который зарегистрирован в качестве Kaspersky Anti-Virus

**vmtoolsd.exe**— Virtual Machine Additions Services Application

**vmtoolsd.exe** – Virtual Machine Additions службы общего доступа к папкам. Работа в Microsoft Virtual PC или Virtual Server и установлена виртуальная машина дополнений, которые обеспечивают интеграцию виртуальный ПК / сервер с операционной системой. Эта услуга специально реализует VirtualMachineAdditions функция, которая позволяет VirtualPC, / Server, чтобы использовать папки с хост-компьютера (локальные и сетевые папки) для совместного использования и обмена файлами между ПК хозяина и VirtualPC, / Server.

**spoolsv.exe**— процесс отвечает за обработку процессов печати на локальном компьютере в операционных системах Microsoft Windows. Служба spooler ответственна за управление заданиями на печать и передачу факсимильных сообщений.

**taskmgr.exe**— собственно менеджер задач.

**services.exe**— служба Plug&Play – Позволяет компьютеру распознавать изменения в установленном оборудовании и подстраиваться под них, либо не требуя вмешательства пользователя, либо сводя его к минимуму. Остановка или отключение этой службы может привести к нестабильной работе системы. Этот процесс запускает первый svchost.

**system**— большинство системных потоков режима ядра выполняются от имени процесса system.

**winlogon.exe**— процесс управляет входом пользователей в систему и выходом из неё. Winlogon активируется только при нажатии клавиш CTRL+ALT+DEL, после чего появляется окно «Безопасность Windows».



**wmiprvse.exe**— инструментарий Windows, обеспечивает обмен управляющей информацией с устройствами.

Выведите список процессов с PID в диапазоне от 0 до 700+№ студента по списку\*10. Какие из перечисленных в теоретической части процессов попадают в этот список? Выполните перезагрузку системы, затем повторите указанные действия, сравните результат с предыдущим, сделайте вывод.

**Бездействие системы**— процесс имеет по одному потоку на каждом процессоре и его единственная задача — учитывать время, в течение которого система не занята другими потоками. В диспетчере задач можно видеть, что этому процессу, как правило, соответствует большая часть процессорного времени.

Все процессы, кроме указанных выше, можно удалять, не опасаясь за работу системы. Однако некоторые из них возражают против такого действия (вирусы, вредоносные программы и некоторые антивирусы), в этом случае удаляем из автозапуска лишние программы с помощью **AnVir Task Manager** перезапускаем систему.

1. За что отвечает вкладка «Приложения»?
2. Существуют ли приложения, которые не следует завершать?
3. Какая информация содержится во вкладке «Процессы»?
4. Изучите список процессов на вашем компьютере, будьте готовы рассказать о любом из них.

### Вкладка «Службы»

Диспетчер задач можно использовать для просмотра сведений о службах, выполняющихся в данный момент на компьютере. Перейдите на вкладку Службы, чтобы увидеть службы, выполняющиеся в данный момент под текущей учетной записью пользователя.

Можно также просматривать сведения о процессах, связанных с конкретной службой.

Чтобы просмотреть процесс, связанный со службой, щелкните правой кнопкой мыши требуемую службу и выберите команду Перейти к процессу. Если команда Перейти к процессу отображается затененной, значит выбранная служба в данный момент остановлена. Состояние службы (выполняется или остановлена) отображается в столбце Статус.

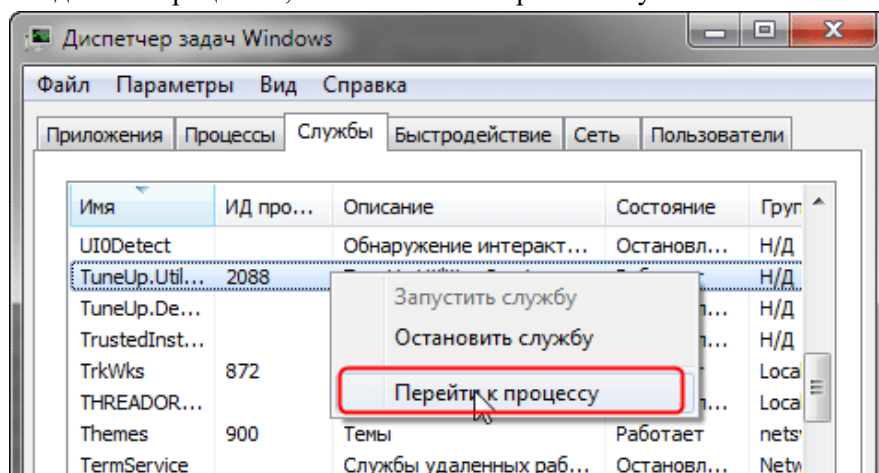


Рисунок 15 –Процесс связанный со службой

Если после выбора команды Перейти к процессу процесс не выделен на вкладке Процессы, значит он не выполняется под текущей учетной записью пользователя. Чтобы просмотреть все процессы, перейдите на вкладку Процессы и установите флажок Отображать процессы всех пользователей. При появлении запроса пароля администратора или подтверждения введите пароль или предоставьте подтверждение. Перейдите на вкладку Службы и повторите попытку просмотреть сведения о процессе.

При нажатии кнопки Службы в нижней части вкладки Службы откроется оснастка консоли управления (MMC), где опытные пользователи могут просматривать более подробные сведения о службах и настраивать дополнительные параметры.

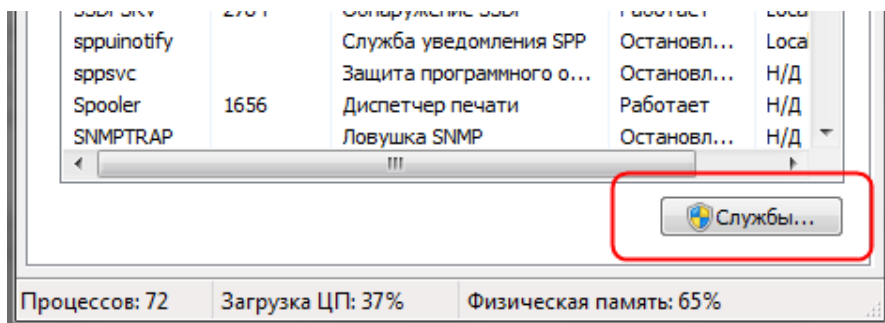


Рисунок 16 – Кнопка Службы

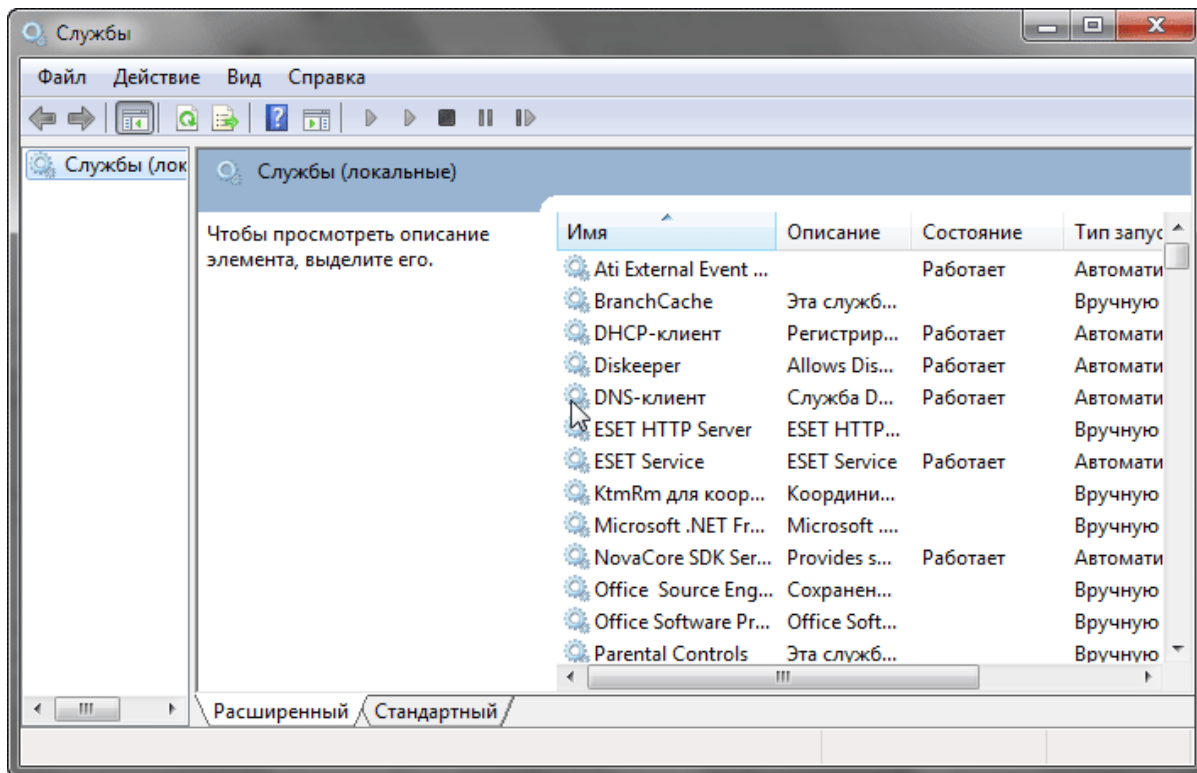


Рисунок 17 – Подробные сведения о службах

Выпишите названия служб: криптографии, маршрутизации и удалённого доступа, диспетчера печати. Есть ли в списке службы с одинаковыми ИД процесса? Если да, то приведите пример и объясните почему?

### Вкладка «Быстродействие» («Производительность»)

На вкладке Быстродействие диспетчера задач приведены дополнительные сведения об использовании компьютером системных ресурсов, например, памяти (ОЗУ) и ресурсов центрального процессора (ЦП).

На этой вкладке отображается четыре графика. Два графика вверху показывают загруженность ЦП как в текущий момент, так и за несколько последних минут.

Высокое процентное значение показывает, что программы или процессы используют большой объём ресурсов процессора, что может замедлить работу компьютера. Приложение может не отвечать, когда процентный показатель фиксируется или приближается к значению 100%.

Процентное значение загрузки процессора показано так же в нижней части диспетчера задач.

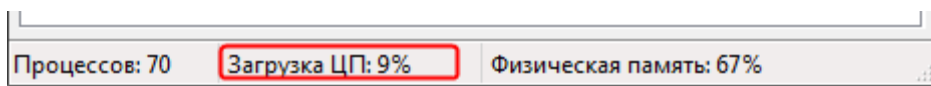


Рисунок 19 – Загрузка ЦП



Два графика внизу показывают объём используемого ОЗУ, или физической памяти, в мегабайтах (МБ) как в текущий момент, так и за несколько последних минут.

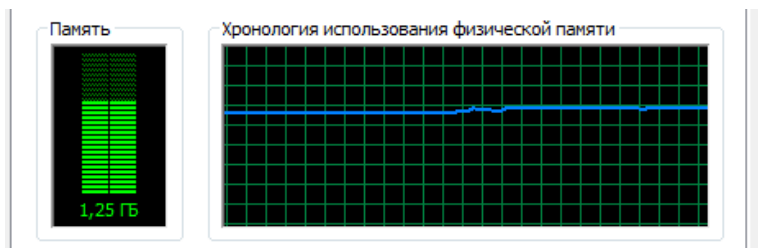


Рисунок 20 – Файл подкачки и хронология использования файла подкачки

Самая частая причина замедления работы системы под управлением Windows –заполнение физической памяти. При этом Windows начинает так называемую «подкачку» (paging) – перемещение блоков кода и данных программ (каждый такой блок называется страницей–page) из физической памяти на жесткий диск. Обращение к файлу подкачки время от времени–нормальное явление, не ухудшающее производительность системы, но частые запросы данных из файла на диске могут заметно снизить общую скорость работы системы. Эта проблема становится особенно заметной при переключении между несколькими программами, активно использующими память, на компьютере, который не содержит достаточного количества физической памяти. В результате диск почти постоянно находится в работе, потому что система пытается «перекачать» данные с него в память и обратно.

Самый быстрый способ получить информацию об использовании памяти в данный момент – запустить Диспетчер задач Windows и взглянуть на строку состояния внизу любой вкладки. Статистика использования памяти приведена в правой части вкладки в виде двух чисел, а точнее дроби. Первое число (числитель) представляет собой текущий объём выделенной памяти – количество физической и виртуальной памяти, используемой всеми выполняемыми процессами. (*Виртуальная память, собственно, и есть файл подкачки.*) Знаменатель –общее количество доступной памяти (физической и виртуальной). Само по себе это число способно лишь предупредить вас о том, что память скоро закончится совсем, – другими словами, выделенная память примерно совпадает с доступной.

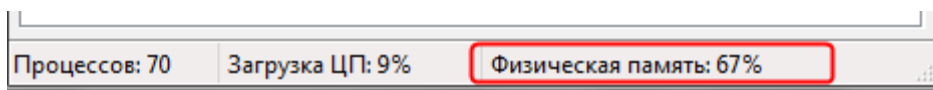


Рисунок 21 – Физическая память

Для того чтобы узнать об использовании памяти подробнее, переключитесь на вкладку Быстродействие и взгляните на таблицы в нижней части диалогового окна. Учтите: числа и подписи к ним могут означать абсолютно не то, что видно изначально.

В трех дополнительных таблицах под графиками содержатся сведения об использовании памяти и ресурсов.

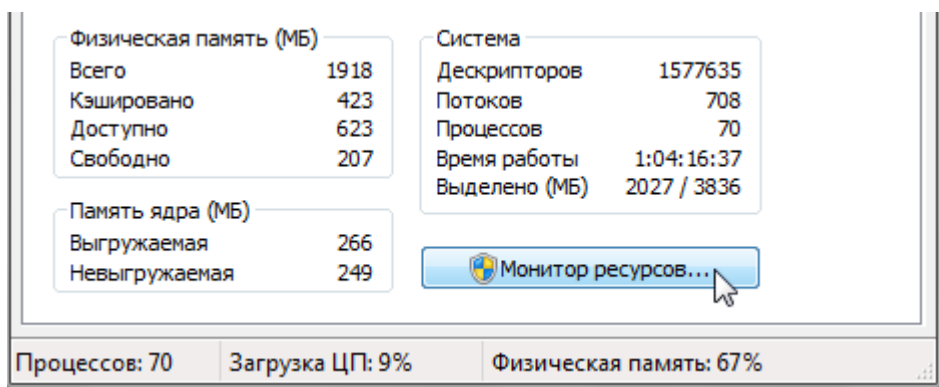


Рисунок 22 – Сведения об использовании памяти и ресурсов

Под заголовком Физическая память (МБ) значение:

- **Всего** — то объём в мегабайтах (Мбайт) оперативной памяти, установленной на компьютере.
- **Кэшировано** — это объём физической памяти, использованной за последнее время для системных ресурсов.
- **Доступно** — это объём памяти, непосредственно доступный для использования процессами, драйверами и операционной системой.
- **Свободно** — это то количество памяти, которое в данный момент не используется или не содержит полезной информации (в отличие от кэшированных файлов, которые содержат полезную информацию).

Под заголовком Память ядра (МБ):

- **Выгружаемая** — это объём виртуальной памяти, используемый основной частью Windows, называемой ядром.
- **Невыгружаемая** — это объём оперативной памяти, используемый ядром.

Подзаголовком Система:

- **Дескрипторы.** Число уникальных идентификаторов объектов, используемых процессами. Это значение представляет интерес главным образом для ИТ-специалистов и программистов.
- **Потоки.** Число объектов или процессов, выполняющихся внутри более крупных процессов или программ. Это значение представляет интерес главным образом для ИТ-специалистов и программистов.
- **Процессы.** Число отдельных процессов, исполняемых на компьютере (эти сведения можно видеть и на вкладке «Процессы»).
- **Время работы.** Время, прошедшее после перезагрузки компьютера.
- **Выделено (МБ).** Описание использования виртуальной памяти (также называемой файлом подкачки). Страничный файл — это место на жестком диске, используемое Windows в дополнение к ОЗУ. Первое число представляет собой объём используемой в данное время оперативной и виртуальной памяти, а второе — объём доступной оперативной и виртуальной памяти.

Для того чтобы узнать об использовании памяти подробнее, переключитесь на вкладку Быстродействие и взгляните на таблицы в нижней части диалогового окна. Учтите: числа и подписи к ним могут означать абсолютно не то, что видно изначально.

Ниже представлены некоторые замечания по поводу значений, которые помогут выполнять мониторинг параметров памяти.

- если значение *Физическая память (КБ): Доступно* приближается к нулю, это означает, что данной системе не хватает ресурсов памяти. Причина этого может заключаться в следующем: в системе одновременно работает довольно большое количество программ или одна большая программа использует практически все ресурсы памяти.
- если значение *Физическая память (КБ): Системный кэш* более чем в половину меньше значения *Физическая память (КБ): Всего*, это означает, что данная система функционирует не настолько эффективно, насколько могла бы, потому что Windows не удаётся сохранять достаточное количество недавно использовавшихся данных в памяти. Поскольку Windows не использует *системный кэш*, когда ей требуется физическая память, закройте программы, которые не нужны.
- если значение *Выделение памяти(КБ): Всего* превышает значение *Физическая память(КБ): Всего* (и остаётся таковым), это означает, что Windows постоянно выгружает данные в страничный файл (pagefile, или pagingfile) и загружает их из него, а это существенно снижает степень производительности.
- если значение *Выделение памяти(КБ): Пик* выше значения *Физическая память (КБ): Всего*, это означает, что в какой-то момент во время текущего сеанса Windows пришлось

прибегнуть к помощи страничного файла. Если на текущий момент времени значение *Выделение памяти (КБ): Всего* меньше значения *Физическая память (КБ): Всего*, критически высокое значение, скорее всего, было лишь временным событием, однако, чтобы быть абсолютно уверенным в этом, за данным значением лучше понаблюдать.

Кнопка Монитор ресурсов предназначена для просмотра дополнительных сведений об используемой памяти и ресурсах ЦПУ. Монитор ресурсов предоставляет графические сведения подобно тем, которые отображаются в диспетчере задач, но в более подробном виде. Здесь также приводятся дополнительные сведения о ресурсах, такие как использование дисков и сети.

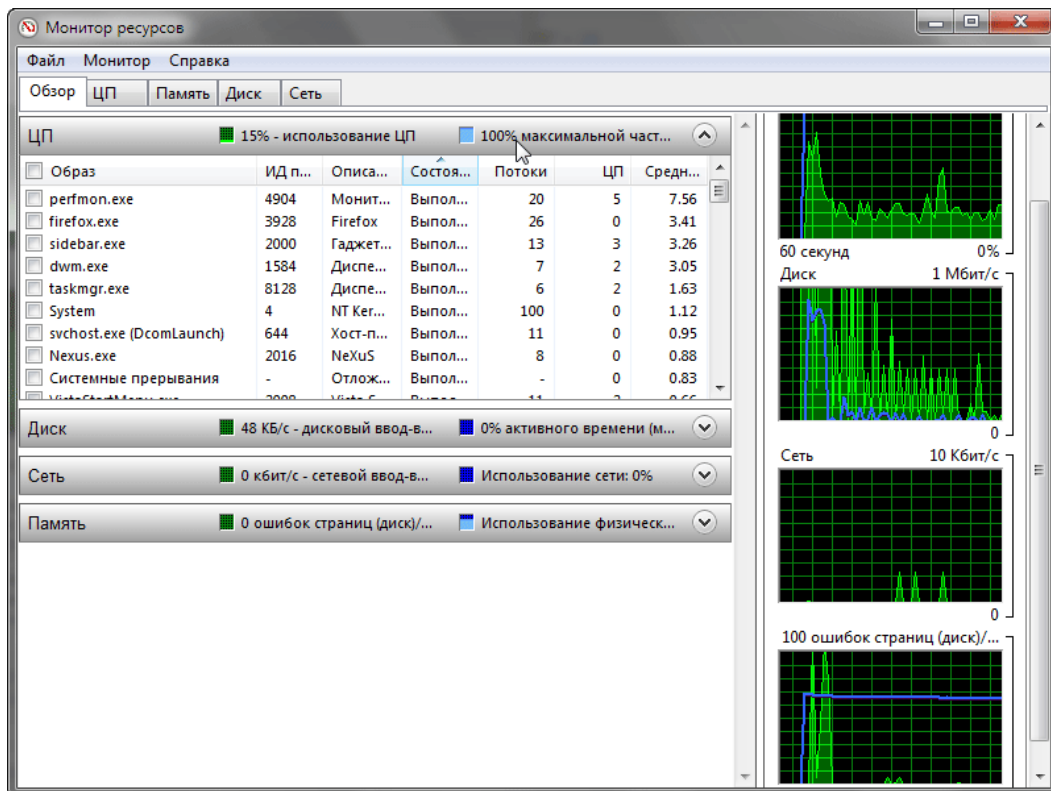


Рисунок 24 – Кнопка Монитор

1. Какую информацию предоставляет вкладка Службы?
2. Зачем нужна вкладка Быстродействие?
3. Что такое файл подкачки? Можно ли задать его размер?

### Вкладка «Сеть»

При наличии сетевого оборудования на этой вкладке вы увидите список имеющихся сетевых подключений и графики их активности. С их помощью можно определить интенсивность использования сети и её пропускную способность.

В нижней части вкладки присутствует таблица с текущими параметрами сетевых подключений. Для детального анализа работы сетевого адаптера пользователь может использовать более двух десятков дополнительных сетевых параметров, которые можно отобразить в таблице, выполнив команду **Вид** → **Выбрать столбцы**.

А с помощью команды **Вид** → **Журнал сетевого адаптера** можно включать или выключать отображение дополнительных графиков.

Существуют способы наложения запрета на автозагрузку программ через записи в реестре, указанные выше. Используются параметры типа DWORD. Все параметры должны храниться в разделе `KLMSoftware\Microsoft\Windows\CurrentVersion\Policies\Explorer`

Для запрета запуска программ, прописанных в подразделе Run раздела LOCALMACHINE используется параметр `DisableLocalMachineRun` со значением 1. В этом случае система игнорирует содержимое списка Run, находящегося в LOCALMACHINE. Аналогично действует запрет списка

RunOnce для LOCALMACHINE. За состояние этой политики отвечает параметр DisableLocalMachineRunOnce. Система игнорирует содержимое RunOnce в LOCALMACHINE.

### **Вкладка «Пользователи»**

Данная вкладка позволяет просмотреть список активных пользователей и при необходимости выполнить для выбранного пользователя операции отключения или выхода из системы с помощью кнопок в нижней части окна.

Закреть окно Диспетчера задач Windows.

1. Что показывает вкладка Сеть?
2. Можно ли по сетевой активности судить о вирусной активности?
3. Какие функции показывает вкладка Пользователи.

### **Контрольные вопросы:**

1. Сколько экземпляров svchost.exe может быть запущено на компьютере? Почему?
2. Что такое spoolsv.exe?
3. Чем отличается файл подкачки от виртуальной памяти? Где можно увидеть?
4. Дескриптор файла это -...
5. Что такое службы? Для чего предназначены?
6. Что необходимо сделать, чтобы запустить настройку системы?
7. Что обеспечивает обычный запуск операционной системы?
8. В каком случае рекомендуется использовать диагностический запуск?
9. Что такое system.ini? Для чего он нужен?
10. Что обеспечивает раздел boot?
11. Какие функции возложены на файл boot.ini?
12. Что такое Application Layer Gateway Service?
13. Что такое timeout, rdisk(0), disk(0), default?
14. Что делает Computer Browser?
15. Расскажите про Cryptographic Services?