**Практическая работа № 1. Исследование средств диагностики операционной системы**

**Цели работы:** исследовать возможности встроенных средств диагностики операционной системы; закрепить знания об основных компонентах ЭВМ и процессах, протекающих в них.

1. Задание к практической работе

**1.1.** Исследовать возможности Диспетчера задач по мониторингу работы компьютера.

**1.2.** Исследовать возможности Системного монитора по мониторингу работы компьютера.

**2.** Программа **Диспетчер задач**

**Диспетчер задач** предоставляет информацию о программах и процессах, запущенных на компьютере, и отображает наиболее общие показатели производительности. С его помощью можно отслеживать статус запущенных программ и завершать приложения, которые перестали отвечать на запросы системы. С помощью диспетчера задач можно отслеживать активность запущенных процессов по 15 параметрам и просматривать графики использования процессора и памяти.

**Порядок выполнения работы**

**2.1.** Запустить программу. Для этого можно использовать один из следующих методов:

1. Щелкнуть **правой кнопкой мыши** на свободном пространстве панели задач и выбрать в контекстном меню пункт **Диспетчер задач**;
2. Нажать комбинацию клавиш **<Ctrl> + <Alt> + <Del>** и нажать в появляющемся окне кнопку **Диспетчер задач**;
3. Вызвать команду **Выполнить** и ввести taskmgr.

**2.2.** Перейти на вкладку **Приложения**. Просмотреть и занести в конспект информацию о выполняющихся приложениях. Изучить состав меню (включая контекстное).

**2.3.** Перейти на вкладку **Процессы**. Изменяя размеры окна и ширину столбцов настроить удобный режим отображения информации. Просмотреть и занести в конспект информацию о выполняющихся процессах. Изучить состав меню (включая контекстное). Отличия в меню занести в конспект.

Выполнить команду меню **Вид** ⮚ **Выбрать столбцы**. Изучить информацию о возможных счетчиках. Включить счетчики **Идентиф. процесса(PID)**, **Загрузка** **ЦП**, **Время ЦП**, **Память – использование**, **Базовый приоритет**, **Счетчик** **потоков**. Просмотреть и проанализировать информацию о запущенных процессах.

**2.4.** Перейти на вкладку **Быстродействие**. Изучить информацию о параметрах системы, представленную на этой вкладке. Изучить состав меню (включая контекстное).

**2.5.** Перейти на вкладку **Приложения**, выбрать приложение Multithreads.exe, и выбрать команду **Снять задачу**. Убедиться, что приложение остановлено и выгружено из памяти.

Закрыть программу **Диспетчер задач**.

**3.** Программа **Системный монитор**

**Системный монитор** позволяет измерять производительность вашего компьютера или других компьютеров в сети:

– собирать и просматривать данные текущей производительности системы на локальном компьютере или на нескольких удаленных компьютерах;

– просматривать текущие данные или данные, собранные ранее с помощью оснастки **Оповещения и журналы производительности**;

– представлять данные в виде графика, гистограммы или отчета, которые можно вывести на печать;

– внедрять возможности System Monitor в Microsoft Word или другие приложения пакета Microsoft Office с помощью автоматизации OLE;

– создавать HTML-страницы для просмотра производительности;

– создавать конфигурации мониторинга, допускающие повторное использование, которые можно инсталлировать на других компьютерах с помощью Microsoft Management Console.

**Порядок выполнения работы**

**3.1.**  Запустить программу **Системный монитор**. Для этого можно использовать один из следующих методов:

1. в **Панели управления** открыть папку **Администрирование** и запустить программу **Системный монитор**;
2. запустить консоль MMC, выполнить команду **Консоль** ⮚ **Открыть**, в окне Открыть найти и открыть файл perfmon.msc
3. Вызвать команду **Выполнить** и ввести perfmon.msc

Запустится указанная программа с заголовком окна **Производительность** (рис. 1).

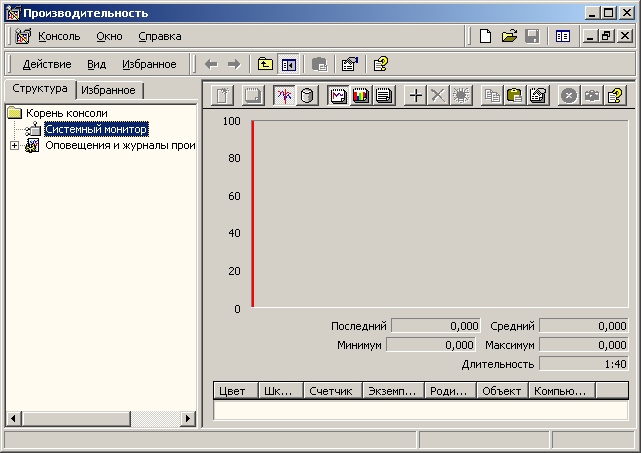


Рис. 1. Окно программы Системный монитор

**3.2.** Ознакомиться с программой, записать ее назначение и основные режимы работы. Для этого воспользоваться встроенной справочной системой.

**3.3.** Настроить внешний вид программы, для чего щелкнуть **правой кнопкой мыши** в панели результатов и выбрать пункт **Свойства**. Изучить назначение и состав вкладок. На вкладке **График** включить отображение линий сетки. Нажать кнопку **OK**.

**3.4.** Исследовать работу **процессора**.

Для этого:

1. щелкнуть **правой кнопкой мыши** в панели результатов и выбрать пункт **Добавить счетчики** (или нажать кнопку **Добавить** в панели инструментов);
2. в открывшемся окне выбрать переключатель **Использовать локальные счетчики**;
3. в списке **Объект** выбрать объект *Процессор*;
4. в списке **Выбрать счетчики из списка** выбрать *% загруженности процессора*;
5. нажать кнопку **Добавить**, затем **Закрыть**.

Появится диаграмма с изменяемыми показаниями загруженности процессора, выраженной в %.

**3.5.** Ознакомиться с программой, записать ее назначение и основные режимы работы, для чего воспользоваться встроенной справочной системой.

**3.6.** Настроить внешний вид программы, для чего щелкнуть **правой кнопкой мыши** в панели результатов и выбрать пункт **Свойства**. Изучить назначение и состав вкладок. На вкладке **График** включить отображение линий сетки. Нажать кнопку **OK**.

**3.7.** Исследовать работу **памяти**. Для этого повторить операции над объектом исследования, указанные в предыдущем пункте. При этом использовать следующие настройки диаграммы:

**Объект**: память;

**Счетчик**: *% использования выделенной памяти*;

**Цвет**: *произвольный*;

**Масштаб**: *по умолчанию*;

остальные установки *не изменять*.

Провести исследования, запуская программы ***Microsoft Excel, Microsoft Access.***

4. Требования к отчету

Отчет должен содержать:

1. Назначение исследуемых программ.
2. Сведения по исследуемым объектам.
3. Параметры и временные диаграммы.
4. Выводы по пунктам задания и по работе.

# Практическая работа № 2. Изучение основных команд для работы с файловой системой в режиме командной строки

**Цель работы:** изучение основных внутренних команд, поддерживаемых интерпретатором Cmd.exe.

**Теоретическая справка.** В операционной системе Windows, как и в других операционных системах, интерактивные (набираемые с клавиатуры и сразу же выполняемые) команды выполняются с помощью так называемого командного интерпретатора, иначе называемого командным процессором или оболочкой командной строки (command shell). Командный интерпретатор или оболочка командной строки — это программа, которая, находясь в оперативной памяти, считывает набираемые вами команды и обрабатывает их. В Windows 9x, как и в MS-DOS, командный интерпретатор по умолчанию был представлен исполняемым файлом command.com. Начиная с версии Windows NT, в операционной системе реализован интерпретатор команд Cmd.exe, обладающий гораздо более мощными возможностями. Некоторые команды распознаются и выполняются непосредственно самим командным интерпретатором — такие команды называются внутренними (например, COPY или DIR). Другие команды операционной системы представляют собой отдельные программы, расположенные по умолчанию в том же каталоге, что и Cmd.exe, которые Windows загружает и выполняет аналогично другим программам. Такие команды называются внешними (например, MORE или XCOPY).

Задание к практической работе

1. На съемном диске создать файловую структуру вида:

F:\

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
|  |  | GAMMA |  |  |
| № группы |  |  | OMEGA |  |
|  | ALFA |  |  |  |
|  |  | TETA |  |  |
|  |  |  | THIRD |  |
|  | BETA |  |  |  |
|  |  |  |  |  |
| FIRST |  | SECOND |  |  |

1. На диске С: в каталоге *№ группы* создать каталог *Lev*. В нем создать группу файлов: *disk.txt, displ.txt, format.txt* (содержимое файлов свободное).
2. Скопировать с диска С: из каталога *Lev* на съемный диск в каталог *№ группы* файлы, начинающиеся на букву *d* c переименованием: имя должно начинаться на букву *r* и расширение *lot*.
3. Все файлы с диска С: из каталога *Lev* скопировать в каталог *TETA*, изменив их расширение при копировании на .abc.
4. В каталоге TETA объединить файлы *format.abc* и *displ.abc* в файл *big.txt.*
5. Вывести оглавление каталога *TETA* в отсортированном порядке по имени.
6. Показать созданную структуру.
7. Удалить с диска F: каталог *ALFA*.
8. Оформить отчет.

**Контрольные вопросы**

1. Как скопировать файл или группу файлов из одного каталога в другой?
2. Как объединить несколько фалов в один?
3. Как удалить файл или группу файлов из каталога?
4. Назовите возможности команды DIR.
5. Перечислите другие команды для работы с файлами и каталогами.

# Практическая работа № 3. Изучение внешних команд для работы с файловой системой в режиме командной строки

**Цель работы:** изучить основные утилиты командной строки.

Задание к практической работе

1. Создать на съемном диске следующую иерархическую структуру:

F: \

LAD RULADA

ТХТ Sort.doc

KIPR Copir.txt

Lira.txt

PIR TIP

Direct.txt Tixe.txt

Antal.txt SIS

Luxe.txt

1. Скопировать все файлы с расширением .тхт из каталогов *KIPR, TIP, SIS* в каталог *PIR*.
2. Переименовать файлы в каталоге PIR, имеющие расширение .txt на файлы с расширением .pir.
3. Скопировать с диска С: на диск F: в каталог TXT все файлы и подкаталоги каталога Lev с созданием каталога Lev на съемном диске.
4. Файлу Sort.doc установить атрибут «только чтение».
5. Вывести на экран дерево каталогов диска F: вместе с файлами.
6. Проверить съемный диск на наличие ошибок с разрешением внесения автоматических исправлений.
7. Удалить каталог PIR и LAD.
8. Оформить отчет.

# Практическая работа № 4. Работа с файлами, каталогами и дисками в операционной оболочке

**Цель работы:** изучение основных приемов и принципов работы с файлами, папками и дисками в Total Commander.

**Теоретическая справка.** Файловый менеджер в русском переводе означает "управляющий файлами", собственно для этого файловые менеджеры и предназначены. Файловые менеджеры - это программы для управления файлами на жестком диске компьютера.

Задание к практической работе

1. Вывести в правую панель содержимое каталога WINDOWS.
2. Вывести в левую панель содержимое каталога МОИ ДОКУМЕНТЫ.
3. Поменять панели местами.
4. Загрузить файл COREL.EXE с панели, когда командная строка пуста, и из командной строки.
5. Используя встроенный редактор, создать файл TEXT1.TXT, записать в него назначение функциональных клавиш.
6. Вывести содержимое файла на экран (тремя способами).
7. Вывести на экран информационную панель.
8. В левой панели вывести полную информацию о файлах.
9. В правой панели вывести файлы в алфавитном порядке по имени, в левой - в порядке убывания даты.
10. На диске С: найти файл размером более 1500 Кбайт и скопировать его в каталог № группы на съемном диске.
11. Для найденного файла установить атрибут «Скрытый».
12. Используя маску, скопировать из каталога ТC в каталог № группы все файлы, имеющие расширение СОМ.
13. Из каталога ТC скопировать файлы, имеющие расширение ЕХЕ, размер группы файлов не должен превышать 650 Кбайт на дискету в каталог GR.
14. Проверить, сколько места занимают файлы в каталоге GR и сколько места осталось на диске.
15. Данные о файлах поместить в таблицу вида:

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Имя файла | Расширение | Размер (в байтах) | Дата создания | Время создания | Атрибуты |
|  |  |  |  |  |  |

1. Оформить отчет.

**Контрольные вопросы**

1. Понятие и назначение файловых менеджеров.
2. Разновидности программ-оболочек.
3. Интерфейс операционных оболочек.
4. Изменение конфигурации файловых менеджеров.
5. «Горячие клавиши» Total Commander.

# 

# Практическая работа № 5. Мониторинг процессов и потоков средствами операционной системы

**Цель работы:** изучение процессов и потоков средствами диспетчера программ и системного монитора на базе ОС Windows XP.

### Теоретическая справка. Приложение, разработанное для Windows, состоит из одного или более процессов. Процесс — это выполняемая программа. Процесс (process) - задание вычислительной системы, представленное в виде программы или части программы и данных, которое операционная система рассматривает как единое целое при распределении ресурсов.

Процесс в Windows состоит из следующих компонентов:

* Объект ядра, через который операционная система управляет процессом.
* Структура данных, содержащая всю информацию о процессе.
* Адресное пространство - диапазон адресов виртуальной памяти, которым может пользоваться процесс.
* Исполняемая программа и данные, проецируемые на виртуальное адресное пространство процесса.

Процессу принадлежат адресное пространство и выделенные ресурсы, а также один или более потоков.

*Поток* (thread) – последовательность команд, выполняемая процессором в выделенное операционной системой для данного потока время.

Чтобы процесс что-нибудь выполнил, в нем нужно создать хотя бы один поток. Потоки отвечают за исполнение кода, содержащегося в адресном пространстве процесса. Именно потокам выделяется такой важный ресурс как процессорное время, называемое *квантом*.

Поток работает в адресном пространстве процесса и использует ресурсы, выделенные процессу. Ресурсами владеют процессы, а не потоки — последние только используют ресурсы, выделенные процессу. Любой процесс содержит хотя бы один поток. Каждый процесс 16-разрядного Windows-приложения или программы MS-DOS имеет только один поток, тогда как процессы 32-разрядных Windows-приложений могут включать их несколько.

При создании процесса первый (точнее, первичный) поток создается системой автоматически. Далее этот поток может породить другие потоки, те в свою очередь — новые и т. д.

Каждый процесс и поток в операционной системе получает свой собственный уникальный идентификационный номер. Для процесса его обозначают PID (Process IDentificator). При создании нового процесса операционная система пытается присвоить ему  свободный номер, больший, чем у процесса, созданного перед ним. Если таких свободных номеров не оказывается (например, мы достигли максимально возможного номера для процесса), то операционная система выбирает минимальный из всех свободных номеров.

Задание к практической работе

### Изучите работу процессов средствами диспетчера задач Windows.

### Изучите работу процессов и потоков средством операционной системы Системный монитор.

### Порядок выполнения работы

##### 1.1. Просмотр списка активных процессов.

* Завершите все работающие программы.
* Просмотрите с помощью **Диспетчера задач**, какие процессы в данный момент активны? Выпишите в отчет список активных процессов.
* Попробуйте завершить процесс *winlogon.exe*. Какова реакция системы?

##### 1.2. Определение идентификационных номеров и имен процессов, создаваемых при запуске приложений.

* Запустите редактор *WordPad*.
* С помощью **Диспетчера** **задач**, определите какой процесс связан с приложением *Документ*-*WordPad*. Для этого:
* В окне **Диспетчера** **задач** перейдите на вкладку **Приложения.**
* В контекстном меню приложения *Документ*-*WordPad* (вызывается щелчком павой кнопкой мышки по имени приложения в списке) выполните **Перейти к процессам.**
* В меню **Вид** выполните команду **Выбрать столбцы**, затем включите **Идентификатор процесса (PID)** и нажмите **Ok**.
* В окне **Диспетчера** **задач** перейдите на вкладку **Процессы**. Какой процесс инициализируется при запуске *WordPad*? Запишите его идентификатор (**PID**).
* Запустите еще один экземпляр редактора *WordPad.* Определите идентификатор связанного с ним процесса.

Отметьте полученный результат в отчете. Ответьте на вопрос, создается ли новый процесс при запуске нового экземпляра приложения WordPad?

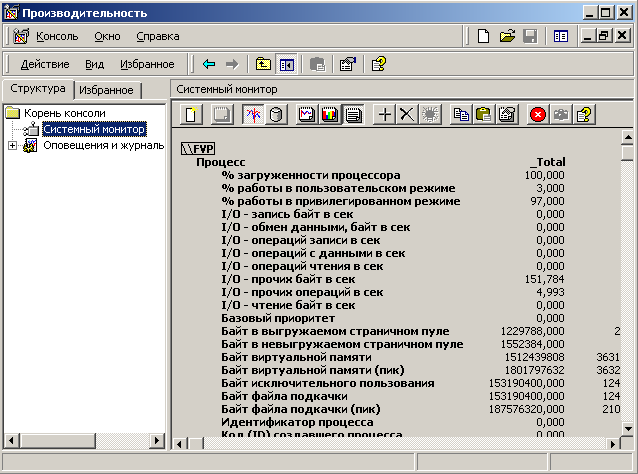
##### 1.3. Определение количества потоков, создаваемых процессами.

* Определите, сколько потоков создается процессом *WordPad*.*exe*. Для этого:
* В окне **Диспетчера** **задач** перейдите на вкладку **Процессы.**
* В меню **Вид** выполните команду **Выбрать столбцы**, затем включите **Счетчик потоков** и нажмите **Ok**.
* Столбец **Потоков** на вкладке **Процессы** и содержит количество потоков, создаваемых соответствующим процессом. Отметьте в отчете, сколько потоков создает процесс *WordPad*.*exe*.
* С помощью **Диспетчера** **задач** определите:
* Создается ли новый процесс при запуске нового экземпляра приложения *Калькулятор*?
* Сколько при этом создается потоков? Результаты внесите в отчет.
* Определите процесс, имеющий максимальный идентификационный номер. Зафиксируйте имя процесса и его PID.
* Запустите приложение *Paint*. Определите, какой идентификационный номер присвоила операционная система соответствующему процессу.

Запишите полученный результат в отчет. Прокомментируйте его.

##### 2.1. Получение информации о количестве активных процессов и потоков с помощью Системный монитор.

* Завершите все работающие программы.
* Запустите системный монитор Windows. Для этого:
* В меню **Пуск** выполните **Настройка/Панель управления**.
* В окне **Панель управления** щелкните по **Администрирование**, затем по **Производительность**.

****

* В окне **Системного монитора**.
* Включите режим **Просмотр отчета**, щелкнув по одноименной кнопке на панели инструментов **Системного монитора**.
* Выделите все ранее добавленные элементы отчета и щелкните по кнопке **Удалить**.

В результате вы получите пустое окно системного монитора.

Информация о выбранном объекте отображается в **Системном мониторе** с помощью **Счетчиков**. Для каждого выбранного счетчика системный монитор отображает значение, соответствующее отдельному параметру объекта.

В зависимости от того, как определен счетчик, его значение может представлять одно из следующих:

* Самое последнее значение использования ресурса. Такие счетчики также называются моментальными (например, счетчик **Процесс\Счетчик потоков**, показывающий текущее число потоков определенного процесса).
* Среднее из двух последних значений. Поскольку счетчики никогда не обнуляются, это значение действительно является средним между двумя измерениями (например, счетчик **Память\Страниц/сек**, поставляющий среднее значение частоты смены страниц в секунду последних двух измерений).
* Используя **Системный монитор** определите количество активных в текущий момент процессов и потоков. Для этого:
* Щелкните по инструменту **Добавить**.
* В окне **Добавить счетчики**:
* Включите **Использовать локальные счетчики**;
* В списке **Объект** выберите **Объекты**;
* В списке **Выбрать счетчики из списка** выделите **Счетчик процессов** и **Счетчик потоков** (счетчик добавляется щелчком мыши при нажатой **Ctrl**). Выполните **Добавить**, затем **Закрыть**.

Зафиксируйте в отчете количество процессов и потоков.

* Запустите *WordPad* и *Калькулятор*. Сколько теперь должно быть активных процессов и потоков (см. результаты выполнения предыдущего пункта)?
* Используя **Системный монитор** проверьте правильность ваших расчетов.
* Закройте *WordPad* и *Калькулятор*. Проверьте, вернулось ли количество активных процессов и потоков в исходное состояние.
* Удалите все ранее добавленные элементы отчета в окне **Системного монитора.**

##### 2.2. Получение информации о процессах.

* Выведите в окно **Системного монитора** всю доступную информацию о состоянии процессов. Для этого:
* Щелкните по инструменту **Добавить**.
* В окне **Добавить счетчики**:
* Включите **Использовать локальные счетчики**;
* В списке **Объект** выберите **Процесс**;
* Выберите **Все счетчики**.
* Выберите **Все вхождения**.
* Выполните **Добавить**, затем **Закрыть**.

Какую информацию о процессах, позволяет получить системный монитор? Ответ на поставленный вопрос запишите в отчет.

##### 2.3. Получение информации о потоках.

* Запустите приложение **WordPad.**
* Выведите в окно **Системного монитора** всю доступную информацию о состоянии потоков процесса *WordPad.exe*. Для этого:
* Щелкните по инструменту **Добавить**.
* В окне **Добавить счетчики**:
* Включите **Использовать локальные счетчики**;
* В списке **Объект** выберите **Поток**;
* Выберите **Все счетчики**.
* В списке **Выбрать вхождения из списка** выберите *WordPad/0 и WordPad/1*.
* Выполните **Добавить**, затем **Закрыть**.

Просмотрите, какую информацию о потоках процесса *WordPad*, позволяет получить системный монитор. Ответ на поставленный вопрос запишите в отчет.

##### 2.4. Получение информации об иерархии процессов.

* Закройте все работающие приложения.
* Запустите один из установленных в системе файл-менеджеров, например, **Windows Commander**.
* Через файл-менеджер запустите программу **Калькулятор** (файл calc.exe папка Winnt/System32)
* Запустите редактор WordPad через меню **Пуск/Программы…**
* Выведите в окно **Системного монитора** для всех активных процессов значения идентификатора процесса и код (ID) создавшего процесса. Для этого:
* Щелкните по инструменту **Добавить**.
* В окне **Добавить счетчики**:
* Включите **Использовать локальные счетчики**;
* В списке **Объект** выберите **Процесс**;
* В списке **Выбрать счетчики из списка** выберите счетчики **Идентификатор процесса** и **Код (ID) создавшего процесса**.
* Выберите **Все вхождения**.
* Выполните **Добавить**, затем **Закрыть**.

Заполните и поместите в отчет следующую таблицу:

|  |  |  |
| --- | --- | --- |
| Процесс | Идентификатор процесса | Код (ID) и имя создавшего процесса-родителя |
|  |  |  |
|  |  |  |

В выводе работы сравните эти средства исследования процессов и потоков в ОС.

# Практическая работа № 6. Обеспечение безопасности ресурсов с помощью разрешений файловой системы NTFS.

**Целью работы**: получение навыков по управлению доступом к информации с помощью разрешений файловой системы NTFS.

**Задание к практической работе**

* 1. Планирование и установка разрешений NTFS.
  2. Изменение разрешений NTFS.
  3. Копирование и перемещение папок.

**Порядок выполнения работы**

1. ПЛАНИРОВАНИЕ И УСТАНОВКА РАЗРЕШЕНИЙ NTFS

Определение устанавливаемых по умолчанию разрешений NTFS для папки

1. Для начала работы, используя учетную запись члена группы ***Администраторы*** (Administrators), создайте учетные записи пользователей по следующим данным.

Создайте следующие папки:

**D:\Public;**

**D:\Public\Library.**



2. Щелкните правой кнопкой мыши значок ***Мой компьютер*** (My Computer), затем щелкните пункт меню ***Проводник*** (Explore).

3. Откройте локальный диск **D:**, затем щелкните правой кнопкой мыши значок папки **Public** и выберите пункт меню ***Свойства*** (Properties). В Windows XP Professional откроется диалоговое окно свойств папки Public с активной вкладкой ***Общие*** (General).

4. Перейдите на вкладку ***Безопасность*** (Security) для просмотра раз­решений, установленных для папки Public.   
Если для какого-либо пользователя или группы установлены особые разрешения, выделите пользователя или группу и щелкните кнопку ***Дополнительно*** (Advanced) для просмотра списка особых разрешений. Каковы текущие разрешения для папки?

5. Щелкните ОК, чтобы закрыть диалоговое окно свойств папки Public.

6. Закройте окно ***Проводник*** (Explorer) и завершите сеанс.

Проверка разрешений, установленных для папки Public

1. Войдите в систему, используя учетную запись **User81**, затем запустите ***Проводник***.

2. Перейдите в папку **Public**.

3. В папке **Public** создайте текстовый документ, назовите его **User81** и введите следующий текст: **Проверка разрешений, установленных для папки**. Операция прошла успешно? Почему?

4. Попытайтесь выполнить следующие операции с созданным файлом:

• откройте файл;

• измените файл;

• удалите файл.

Какие действия вы смогли успешно совершить и почему?

5. В папке Public снова создайте текстовый документ **User81**.

6. Завершите сеанс работы с Windows XP Professional.

7. Войдите в систему, используя учетную запись **User82**.

8. Попытайтесь выполнить следующие операции с текстовым документом **User81**:

• откройте файл;

• измените файл;

• удалите файл.

Какие действия вы смогли успешно совершить и почему?

Установка разрешений NTFS

В этом упражнении вы установите разрешения NTFS для папки Public в соответствии со следующей политикой:

• все пользователи должны иметь возможность читать документы и файлы в папке **Public**;

• все пользователи должны иметь возможность создавать документы в папке **Public**;

• все пользователи должны иметь возможность изменять содержание, свойства и разрешения для создаваемых ими документов в папке **Public**;

• пользователь **User82** несет ответственность за подержание папки Public и должен иметь возможность изменять и удалять все файлы в папке **Public**.

В настоящее время ваша регистрационная запись — **User82**. Можете ли вы изменить разрешения, установленные для пользователя **User82**? Почему?

Установка разрешений NTFS для папки

1. Войдите в систему, используя учетную запись члена группы ***Администраторы*** (Administrators). Затем откройте ***Проводник*** (Windows Explorer).

2. Откройте папку **Public**.

3. Щелкните правой кнопкой мыши значок папки **Public**, затем выберите пункт меню ***Свойства*** (Properties).

4. Перейдите на вкладку **Безопасность** (Security) диалогового окна свойств папки.

5. На вкладке ***Безопасность*** (Security) щелкните кнопку ***Добавить*** (Add).

Откроется диалоговое окно ***Выбор:*** ***пользователи или группы.***

6. В текстовом поле ***Введите имена выбираемых объектов*** (Enter The Object Names To Select) введите **User82**, затем щелкните кнопку ***Проверить имена***.

В текстовом поле ***Введите имена выбираемых объектов*** (Enter The Object Names To Select) должна появиться надпись PRO1 \User82. Это свидетельствует, что Windows XP Professional обнаружила пользователя User82 на компьютере PRO1 и что это действительная учетная запись пользователя.

7. Щелкните ОК, чтобы закрыть диалоговое окно Выбор: ***Пользователи или группы***.

Теперь пользователь **User82** включен в список ***Группы или пользователи*** (Group Or User Name) диалогового окна свойств папки **Public**.   
Какие разрешения установлены для пользователя User82?

8. Щелкните кнопку ***Дополнительно*** (Advanced). Откроется диалоговое окно ***Дополнительные параметры безопасности для Public*** (Advanced Security Settings For Public), и вы увидите, что пользователь **User82** (PROl\User82) включен в список ***Элементы разрешений*** (Permissions Entries).

9. Убедитесь, что строка **User82** выделена, и щелкните кнопку ***Изменить*** (Edit). Откроется диалоговое окно ***Элемент разрешения для Public*** (Permission Entry For Public), и вы увидите в текстовом поле ***Имя*** (Name) учетную запись пользователя **User82** (PROl\User82).

10. В колонке ***Разрешить*** (Allow) щелкните ***Полный доступ*** (Full Control). Теперь в колонке ***Разрешить*** (Allow) установлены все флажки.

11. Щелкните ОК, чтобы закрыть диалоговое окно ***Элемент разрешения для Public***.

12. Щелкните ОК, чтобы закрыть диалоговое окно ***Дополнительные параметры безопасности для Public*** (Advanced Security Settings Foi Public).

13. Щелкните ОК, чтобы закрыть диалоговое окно свойств папки **Public**.

14. Закройте ***Проводник*** (Explorer) и завершите сеанс работы.

Проверка разрешений NTFS для папки

1. Войдите в систему, используя учетную запись **User82**, при запросе пароля введите слово **password**.

2. Запустите ***Проводник*** (Explorer).

3. Откройте диск **D:**, затем откройте папку **Public**.

4. Попытайтесь совершить следующие действия с текстовым доку­ментом **User81**:

• измените файл;

• удалите файл.

Какие действия вы смогли совершить и почему?

Проверка разрешений NTFS

Создайте файл в подпапке и проверите, как разрешения NTFS наследуются в иерархии папок.

Проверка разрешений для папки Library

1. Войдите в систему, используя учетную запись User81, затем запустите ***Проводник*** (Windows Explorer).

2. В ***Проводнике*** (Windows Explorer) откройте папку ***Public\Library***.

3. Создайте текстовый документ **User81** в папке **Library**.

4. Завершите сеанс Windows XP Professional.

Проверка разрешений для папки **Library** с использованием подключения с учетной записью **User82**

1. Зарегистрируйтесь в системе, используя учетную запись **User82**. затем запустите ***Проводник*** (Windows Explorer).

2. Откройте папку **Public\Library**.

3. Попытайтесь совершить следующие действия с текстовым документом **User81**:

• открыть файл;

• изменить файл;

• удалить файл.

Какие действия вы смогли совершить и почему?

4. Завершите работу с Windows XP Professional.

2. ИЗМЕНЕНИЕ РАЗРЕШЕНИЙ NTFS

Смена владельца файла

Для смены владельца файла необходимо определить разрешения для файла, установить разрешение ***Смена владельца*** (Take Ownership) для учетной записи пользователя и стать владельцем файла.

Определение разрешений для файла

1. Войдите в систему, используя учетную запись члена группы ***Администраторы***.

2. В папке **Public** создайте текстовый документ и назовите его **OWNER**.

3. Щелкните правой кнопкой мыши значок документа **OWNER**, затем выберите пункт меню ***Свойства*** (Properties).   
В Microsoft Windows XP Professional откроется диалоговое окно ***Свойства: Owner***(Owner Properties) с активной вкладкой ***Общие*** (General).

4. Перейдите на вкладку ***Безопасность*** (Security) для просмотра раз решений, установленных для файла **OWNER**.

5. Щелкните кнопку ***Дополнительно*** (Advanced).

Откроется диалоговое окно ***Дополнительные параметры безопасности для Owner*** (Advanced Security Settings For Owner) с активной вкладкой ***Разрешения*** (Permissions).

6. Перейдите на вкладку ***Владелец*** (Owner). Кто является текущим владельцем файла?

Установка разрешения, позволяющего пользователю сменить владельца

1. В диалоговом окне ***Дополнительные параметры безопасности для Owner*** (Advanced Security Settings For Owner) перейдите на вкладку ***Разрешения*** (Permissions).

2. Щелкните кнопку ***Добавить*** (Add). Откроется диалоговое окно ***Выбор: пользователи или группы*** (Select Users Or Groups).

3. Убедитесь, что в текстовом поле ***Размещение*** (From This Location), которое расположено вверху диалогового окна, выбрано имя вашего компьютера (PRO1).

4. В текстовом поле ***Введите имена выбираемых объектов*** (Enter The Object Names To Select) введите **User81** затем щелкните кнопку ***Проверить имена*** (Check Names).

В списке ***Введите имена выбираемых объектов*** (Enter The Object Names To Select) должна появиться запись **PRO 1 \User81**. Это означает, что учетная запись пользователя **User81** найдена на компьютере с именем PRO1 и является действительной учетной записью.

5. Щелкните ОК. В Windows XP Professional станет активным диалоговое окно ***Эле­мент разрешения для Owner*** (Permission Entry For Owner). Обратите внимание на то, что все элементы разрешений для пользователя **User8l** не отмечены.

6. В колонке ***Разрешения*** (Permissions) установите флажок ***Разрешить*** (Allow) для разрешения ***Сменить владельца*** (Take Ownership).

7. Щелкните ОК. В Windows XP Professional станет активным диалоговое окно ***До­полнительные параметры безопасности для Owner*** (Advanced Security Settings For Owner) с открытой вкладкой ***Разрешения*** (Permissions).

8. Щелкните OK для того, чтобы вернуться к диалоговому окну свойств файла **OWNER.**

9. Щелкните ОК для сохранения изменений и закройте диалоговое окно свойств файла **OWNER**.

10. Закройте ***Проводник*** (Windows Explorer) и выйдите из системы.

Смена владельца файла

1. Зарегистрируйтесь в системе, используя учетную запись **User81** и запустите Проводник.

2. Войдите в папку **Public**.

3. Щелкните правой кнопкой мыши значок файла **OWNER** и выбе­рите пункт меню ***Свойства*** (Properties).

4. Перейдите на вкладку ***Безопасность*** (Security) для просмотра раз решений для файла.

5. Щелкните ***Дополнительно*** (Advanced) для открытия диалогового окна ***Дополнительные параметры безопасности для Owner*** (Advanced Security Settings For Owner) и перейдите на вкладку ***Владелец*** (Owner).

6. В колонке ***Изменить владельца на*** (Change Owner To) выберите **User81**, затем щелкните кнопку ***Применить*** (Apply).   
Кто теперь является владельцем файла OWNER?

7. Щелкните ОК, чтобы закрыть диалоговое окно ***Дополнительные параметры безопасности для Owner*** (Advanced Security Settings For Owner).

8. Щелкните ОК, чтобы закрыть диалоговое окно свойств файла **OWNER**.

Проверка разрешений для файла в качестве владельца

1. Пока вы подключены как **User81**, установите разрешение ***Полный доступ*** (Full Control) пользователю **User81** к текстовому документу OWNER и щелкните кнопку **Применить**.

2. Щелкните кнопку ***Дополнительно*** (Advanced) и снимите флажок Наследовать от родительского объекта применимые к дочерним объек­там разрешения, добавляя их к явно заданным в этом окне (Inherit From Parent The Permission Entries That Apply To Child).

3. В диалоговом окне ***Безопасность*** (Security) щелкните кнопку ***Уда­лить*** (Remove).

4. Щелкните ОК, чтобы закрыть диалоговое окно Дополнительные параметры безопасности для ***Owner*** (Advanced Security Settings For Owner).

5. Щелкните ОК, чтобы закрыть диалоговое окно свойств файла **OWNER**.

6. Удалите текстовый документ **OWNER**.

3. КОПИРОВАНИЕ И ПЕРЕМЕЩЕНИЕ ПАПОК

Создание папки при подключении с учетной записью пользователя

1. Пока вы зарегистрированы в системе под учетной записью **User81**, в ***Проводнике*** (Windows Explorer), в корневой папке диска **D:** создайте папку с именем **Temp1**.

Какие разрешения установлены для этой папки?

Кто является владельцем папки? Почему?

2. Закройте все приложения и закончите работу с Windows XP Professional.

Создание папки при подключении с учетной записью члена группы ***Администраторы*** (Administrators)

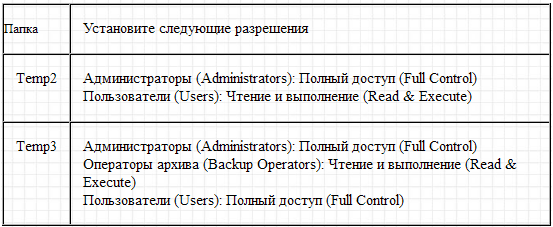
1. Войдите в систему, используя учетную запись члена группы ***Администраторы*** и запустите ***Проводник*** (Windows Explorer).

2. В корневой папке диска **D:** создайте папки **Теmр2** и **Теmр3**. Каковы разрешения для папок **Теmр2** и **Теmр3**, которые вы только что создали?

3. Установите разрешения для папок **Теmр2** и **Теmр3** (таблица 3.8.).

Снимите фла­жок ***Наследовать от родительского объекта применимые к дочер­ним объектам разрешения,* *добавляя их к явно заданным в этом окне*** (Inherit From Parent The Permission Entries That Apply To Child Objects). В открывшемся диалоговом окне щелкните ***Удалить*** (Remove) для удаления всех разрешений, кроме указанных явно.

*Параметры разрешения для папок Теmр2 и Теmр3.                Таблица 3.8*



Копирование папки в другую папку на одном и том же томе NTFS в Windows XP Professional

1. Пока вы находитесь в системе под учетной записью члена группы ***Администраторы*** (Administrators), в ***Проводнике*** (Windows Explorer), скопируйте папку **D:\Temp2** в папку **D:\Temp1**. Так как была произведена операция копирования, должны суще­ствовать обе папки: **D:\Temp2** и **D:\Templ\Temp2**.

2. Выделите **D:\Templ\Temp2**, затем сравните разрешения и права владельца с папкой **D:\Temp2**. Кто владелец папки **D:\Templ\Temp2** и какие разрешения для нее установлены?

Перемещение папки на одном и том же томе

1. Зарегистрируйтесь в системе как пользователь **User81**.

2. В ***Проводнике*** (Windows Explorer) выделите значок папки **D:\Temp3**. затем переместите ее в папку **D:\Templ**. Что произошло с разрешения и владельцем для папки **D:\Templ\Теmр3**?

3. Закройте все окна и завершите сеанс работы.

Удаление файла, для которого установлен запрет на все разрешения

Создайте файл в папке **Теmр3**, к которой предоставлено разре­шение ***Полный доступ*** (Full Control) группе ***Пользователи*** (Users), но запретите все разрешения для него.

Создание файла и запрет доступа к нему

1. Войдите в систему, используя учетную запись члена группы ***Ад­министраторы*** (Administrators).

2. В папке **D:\Templ\Temp3** создайте текстовый документ с именем **NOACCESS**.

3. Запретите для группы ***Пользователи*** (Users) разрешение ***Полный доступ*** (Full Control) для текстового документа **NOACCESS**.   
В Windows XP Professional отобразится диалоговое окно ***Безопасность*** (Security) со следующим сообщением:

«Вы запретили доступ для NOACCESS.txt. Никто не сможет полу­чить доступ к NOACCESS.txt, и только владелец сможет изменить разрешения. Продолжить выполнение операции?».

4. Щелкните ***Да*** (Yes), чтобы изменения вступили в силу и чтобы закрыть диалоговое окно ***Безопасность*** (Security).

5. Щелкните ОК, чтобы закрыть диалоговое окно свойств файла **NOACCESS**.

Просмотр результата запрета разрешения ***Полный доступ*** (Full Control) к папке

1. В ***Проводнике*** (Windows Explorer) дважды щелкните значок тексто­вого документа NOACCESS в папке Теmр3 для того, чтобы от­крыть его.   
Операция прошла успешно? Почему?

2. Щелкните ***Пуск*** (Start), затем — ***Выполнить*** (Run). Windows XP Professional откроется диалоговое окно ***Выполнить*** (Run).

3. Введите в текстовом поле ***Открыть*** (Open) cmd и щелкните ОК.

4. Перейдите в папку D:\Templ\Temp3.

5. Введите Del NOACCESS.TXT и нажмите клавишу ENTER. Операция прошла успешно? Почему?

Как предотвратить удаление пользователями, имеющими разрешение ***Полный доступ*** (Full Control) к папке, файла в этой папке, для которого установлен запрет на разрешение ***Полный доступ*** (Full Control)?

**Указания по оформлению отчета**

Отчет должен содержать:

* название работы;
* цель работы;
* функциональное назначение этапов работы;
* порядок действий по выполнению практической работы;
* устанавливаемые в процессе работы параметры;
* выводы по результатам проделанной работы;
* ответы на контрольные вопросы.

**Контрольные вопросы**

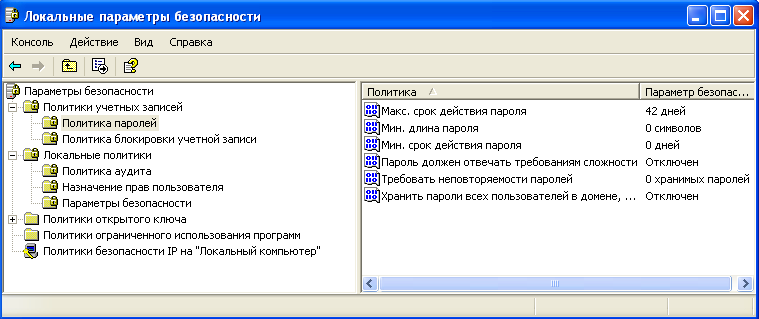
* + 1. Как определить устанавливаемые по умолчанию разрешения NTFS для папки?
    2. Как изменить разрешения NTFS?
    3. Какое разрешение позволяет пользователю сменить владельца?
    4. Как копировать и перемещать папки с сохранением разрешений NTFS?

# Практическая работа № 7. Аутентификация в Windows

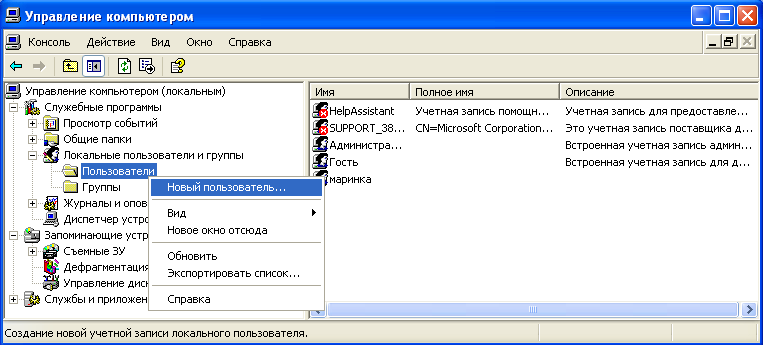
#### Цель работы: обучение методам, средствам и подходам к организации идентификации, аутентификации и авторизации пользователей на рабочих станциях и серверах, работающих под управлением ОС семейства Windows.

**Задание к практической работе**

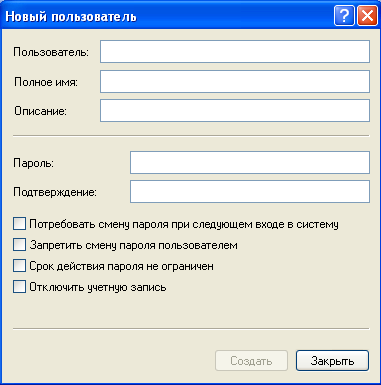
1. Войти в систему с полномочиями администратора.
2. Найти и открыть консоль настроек локальной политики безопасности (Local Security Settings). Для этого можно воспользоваться одним из способов:
   1. меню *Пуск→ Панель управления→ (перейти к классическому виду) → Администрирование → Локальная политика безопасности→ выбрать Параметры безопасности;*
   2. меню *Пуск→ Программы → Администрирование → Локальная политика безопасности→ выбрать Параметры безопасности;*
   3. меню *Пуск→ Выполнить→ в окне Запуск программы ввести:* gpedit.msc (gpedit.msc – это одна из распространенных консолей политики безопасности) *→ в окне Групповая политика выбрать: Параметры безопасности.*
3. Оценить адекватность текущей политики безопасности в части аутентификации. Для этого необходимо изучить все Параметры безопасности, поочередно, раскрывая каждую политику и просматривая их ограничения и параметры:



1. ЗАПОМНИТЬ ОГРАНИЧЕНИЯ НА ПАРОЛИ ПОЛЬЗОВАТЕЛЯ!!!
2. Введите следующие ограничения на пароли пользователей:
   * минимальный и максимальный срок действия пароля;
   * минимальную допустимую длину пароля;
   * минимальное допустимое количество смен пароля до первого повторения;
   * должна ли проводиться проверка качества пароля при смене пароля пользователем;
   * максимально допустимое количество неудачных попыток входа в систему;
   * срок, по истечении которого счетчик неудачных попыток входа в систему обнуляется;
   * срок, на который пользователю запрещается вход в систему в случае превышения максимально допустимого количества неудачных попыток входа в систему (может быть неограниченным, в этом случае запрет на вход пользователя в систему может быть снят только администратором);
   * могут ли пользователи самостоятельно менять пароль в случае истечения максимального срока его действия, или они должны уведомлять администратора о случившемся.
3. Результат показать преподавателю.
4. ВЕРНУТЬ ВСЕ НАСТРОЙКИ К ИСХОДНОМУ СОСТОЯНИЮ!!!
5. Зарегистрировать в системе несколько учетных записей пользователей. Для этого можно воспользоваться одним из способов:
   1. меню *Пуск→ Панель управления→ Учетные записи пользователей → Создание учетной записи;*
   2. меню *Пуск→ Панель управления→ (перейти к классическому виду) → Администрирование → Управление компьютером → Локальные пользователи и группы → Пользователи → контекстное меню Пользователей → Новый пользователь:*



В окне *Новый пользователь* заполнить информацию новой учетной записи:



1. Установить для них различные параметры аутентификации.
2. Войти в систему под каждой из учетных записей, зарегистрированных на предыдущем шаге (для этого перезагрузить компьютер), определить, как влияют параметры аутентификации на работу пользователя в системе. Ответ дать преподавателю.
3. Установить автоматическую блокировку учетной записи после заданного количества неудачных попыток аутентифицироваться.

Для этого, например, можно: меню *Пуск→ Программы → Администрирование → Локальная политика безопасности→ выбрать Параметры безопасности → Политики учетных записей → Политика блокировки учетной записи.*

Убедиться, что блокировка работает.

1. Несколько раз поменять пароль одной из зарегистрированных учетных записей. Для этого можно воспользоваться одним из способов:
   1. *Управление компьютером → Локальные пользователи и группы → Пользователи → контекстное меню Пользователей → Задать пароль;*
   2. меню *Пуск→ Панель управления→ Учетные записи пользователей → Учетные записи пользователей → выбрать изменяемую учетную запись → Создание пароля;*
   3. Заблокировать компьютер через *Ctrl + Alt + Del* *→ Смена пароля (но этот способ требует точного и правильного написания имени пользователя).*

Определить, как действуют правила аутентификации, относящиеся к смене пароля.

1. Удалить созданные вами учетные записи.
2. Вызвать контекстное меню системной папки: диск С: *→ Доступ (безопасность).*
3. Проверить, какая файловая система используется вашим компьютером. Если NTFS, то открыть закладку *Безопасность* и установить необходимые параметры аутентификации. Для ФС FAT нельзя выполнить эту операцию.

**Контрольные вопросы**

1. Как осуществить проверку одной из следующих привилегий:

* входить в систему интерактивно;
* входить в систему через сеть;
* запускать сервис от своего имени;
* запускать пакетное задание (*batch job*) от своего имени.

# Практическая работа № 8. Аудит в ОС Windows

**Цель работы**: приобретение практических навыков работы с аудитом, изучение основных методов управления политикой аудита на примере ОС Windows XP.

### Теоретическая справка. Аудит — это процесс, позволяющий фиксировать события, происходящие в операционной системе и имеющие отношение к безопасности: например, регистрация в системе или попытки создания объекта файловой системы, получения к нему доступа или удаления. Информация о подобных событиях заносится в файл журнала событий операционной системы.

**Политика аудита** *-* это совокупность правил, определяющая то, какие события должны регистрироваться в журнале аудита.

Для обеспечения надежной защиты операционной системы в журнале аудита должны обязательно регистрироваться следующие события:

1. попытки входа/выхода пользователей из системы;
2. попытки изменения списка пользователей;
3. попытки изменения политики безопасности, в том числе и политики аудита.

При определении политики аудита не следует ограничиваться регистрацией событий из перечисленных классов. Окончательный выбор того, какие события должны регистрироваться в журнале аудита, а какие не должны, возлагается, на аудиторов.

При выборе адекватной (оптимальной) политики аудита следует учитывать ожидаемую скорость наполнения журнала аудита. Если политика аудита предусматривает регистрацию слишком большого числа событий, это не только не повышает защищенность операционной системы, но, наоборот, снижает ее. Если новые записи добавляются в журнал аудита слишком часто, аудиторам будет трудно выделить в огромном объеме информации те события, которые на самом деле представляют угрозу безопасности системы. Кроме того, чем быстрее заполняется журнал аудита, тем чаще его нужно очищать, и тем больше вероятность временного выхода из строя операционной системы из-за переполнения журнала аудита.

Политику аудита не следует рассматривать как нечто неизменное, заданное раз и навсегда. Политика аудита должна оперативно реагировать на изменения в конфигурации операционной системы, в характере хранимой и обрабатываемой информации, и, особенно, на выявленные попытки атаки операционной системы.

**Журнал аудита** Windows представляет собой файл сименем secevent.evt, расположенный в поддиректории system32/config системной директории. Информация хранятся в журнале аудита в открытом виде, защита журнала аудита организуется исключительно средствами подсистемы разграничения доступа. Для просмотра журнала аудита используется стандартная утилита Event Viewer, которую можно использовать и для просмотра других системных журналов. Эта утилита разрешает читать журнал аудита только членам группы Administrators, а также пользователям, обладающим привилегией аудитора.

Пользователи, не имеющие возможности читать журнал аудита с помощью утилиты Event Viewer, но обладающие правом чтения файла secevent.evt, могут читать этот файл с помощью других программных средств. Поэтому права доступа субъектов к этому файлу должны быть ограничены.

Размер журнала аудита по умолчанию ограничен величиной 512К, однако администратор операционной системы может установить любое другое значение, кратное 64К. Администратор также может определить поведение операционной системы при переполнении журнала аудита.

Windows позволяет регистрировать в журнале аудита события следующих категорий:

1. вход/выход пользователя из системы;
2. аутентификация пользователя;
3. доступ субъектов к локальным объектам;
4. доступ субъектов к объектам активного каталога;
5. использование субъектами доступа опасных привилегий;
6. изменения в списке пользователей;
7. изменения в политике безопасности;
8. системные события;
9. запуск и завершение процессов.

Для каждого класса событий могут регистрироваться либо только успешные события (соответствующая операция выполнена успешно), либо только неуспешные (при выполнении операции произошла ошибка), либо и те, и другие, либо никакие.

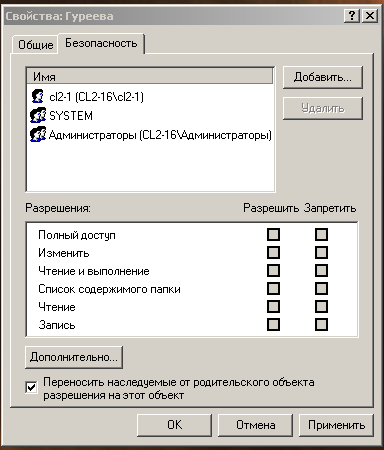
**Задание к практической работе**

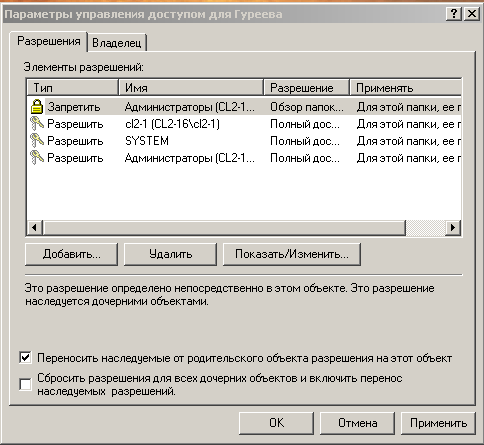
* 1. Настройка адекватной политики аудита для любого объекта;
  2. Настройка адекватной политики аудита, удовлетворяющей обеспечению надежной защиты операционной системы;
  3. Просмотр событий в журнале аудита.

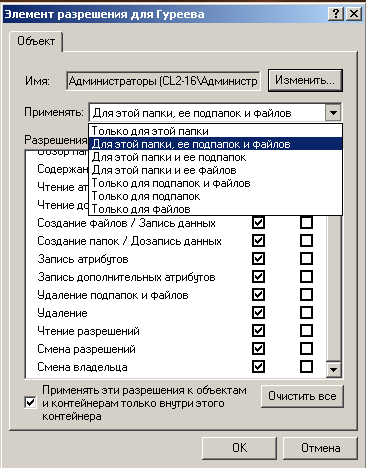
**Порядок выполнения работы**

Для того чтобы настроить политику аудита для *конкретного объекта* надо:

1. Создайте папку (это будет объект). Вызовите контекстное меню этой папки, в котором выберите команду *Свойства* или *Доступ и Безопасность…*
2. В раскрывшемся диалоговом окне выбрать закладку *Безопасность*:

**

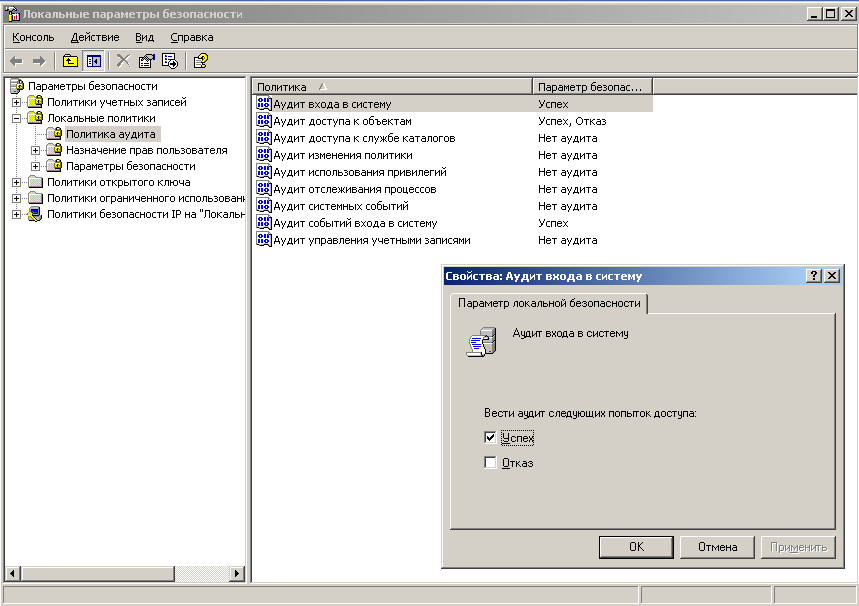
1. Выбрать учетную запись для которой вы желаете фиксировать события, происходящие с этой папкой. Нажмите *Дополнительно* и затем кнопку *Показать/Изменить*:



1. Используя раскрывающийся список *Применять* установите для каких событий этой папки вы желаете настроить аудит и установите разрешения на события, которые разрешаете этому пользователю делать с этой папкой или запрещаете.

Для того чтобы настроить политику аудита *для операционной системы Windows* надо:

1. Найти и открыть консоль настроек локальной политики безопасности (Local Security Settings), для этого выбрать вкладку *Локальная политика безопасности* в меню *Пуск / Настройка / Панель управления / Администрирование.*
2. В открывшейся консоли, раскрыть раздел *Локальные политики* и выбрать раздел *Политика аудита,* вправом окне консоли будут перечислены события, аудит которых позволяет вести ОС Windows.
3. Проанализировать представленные события и выбрать из них те, которые эквиваленты событиям, перечисленными в задании.
4. Настроить политику аудита, непосредственно установив регистрацию выбранных событий. Для этого необходимо выбрать свойства конкретного события (двойным щелчком левой клавиши мышки) и в появившемся окне свойств события установить какой тип события (Успех/Отказ) регистрировать, затем нажать *Применить* и *ОК.* Таким образом, политика аудита настроена.



1. В открывшейся консоли выбрать раздел *Безопасность (Security).* В правом окне консоли будут отображены записи, содержащие все события, зарегистрированные системой и находящиеся в журнале аудита.
2. Для демонстрации работы подсистемы аудита ОС Windows, необходимо инициировать какое - нибудь событие из перечисленных в задании, например попытку изменения политики безопасности. Для этого, изменим политику аудита, используя пункты 5,6 и 8. Далее воспользуемся журналом аудита (secevent.evt), в который заносятся все зарегистрированные системой события, этот журнал вместе с журналами ошибок системы и приложений отображается в консоли просмотра событий (Event Viewer). Для доступа к консоли необходимо выбрать в меню *Пуск / Настройка / Панель управления / Администрирование /* закладка *Просмотр событий.*
3. Рассмотрите права доступа субъектов к файлу secevent.evt. Могут ли читать этот файл администратор, пользователь, опытный пользователь, гость с помощью других программных средств? Ограничьте доступ любых субъектов к этому файлу.
4. Установите фиксацию всех событий в журналах. Выполните несколько событий: смену пользователя, запуск приложений, перезагрузку компьютера, неправильный ввод пароля и т.д. Просмотрите файлы журнала и сделайте соответствующие выводы.
5. Настройте режим аудита, в котором видно, что некоторый пользователь пытается подобрать пароль. В каком режиме подобных действий не видно?
6. Приведите пример адекватной политики аудита состоящей из списка событий, которые необходимо регистрировать, по вашему мнению, для создания адекватной политики безопасности.
7. Опишите каждое поле записи из журнала аудита, для одного любого зарегистрированного события и составьте общий вывод на основе анализа всех полей этой записи касательно безопасности системы.
8. Оформить отчет по практической работе, фиксируя все события, инициируемые в каждом пункте.

**Контрольные вопросы**

1. Понятие аудита.

2. Определение политики аудита.

3. Понятие журнала аудита.

4. Может ли размер журнала аудита в Windows составлять 1282К?

5. Какие типы событий регистрируются в журналах?

# Практическая работа № 9. Операционная система Linux. Знакомство с графической средой

# Цель работы: изучение особенностей графической среды операционной системы Linux, выполнение основных операций с файлами и папками.

### Теоретическая справка. В современных дистрибутивах  Linux наибольшее распространение получили графические среды KDE (K Desktop Environment) и GNOME (GNU Network Object Model Environment). Графическая рабочая среда — это среда, организующая единый стилистический интерфейс для приложений, написанных для нее, предоставляющая приложениям стандартизованные методы взаимодействия процессов и стандартные библиотеки. Приложения, входящие в графическую среду, отлично друг с другом взаимодействуют и представляют законченный интерфейс для домашнего и офисного использования.

KDE — самая популярная рабочая среда в мире Linux и занимает это место по достоинству. Она изящно выглядит, весьма удобна, солидна и обладает богатыми возможностями. Вы можете положиться на нее в деле отправки и получения электронной почты, с помощью ее браузеров можете путешествовать по Всемирной Сети, ее приложения помогут вам запи­сывать компакт-диски и просматривать кинофильмы, работать с текстовыми документами и крупноформатными таблицами. Одна из основных задач, которые ставили разработчики, — сделать  систему, напоминающую Windows, но значительно лучше.

Графическая среда GNOME реализована для разных платформ, что позволяет запускать ее в  ОС Linux, BSD и Solaris. Система очень гибкая, использует внешний менеджер окон, который можно выбирать. Его возможности во многом схожи  с KDE и предоставляют приблизительно одинаковую функциональность.

Указанные среды имеют встроенную справочную систему, где подробно описаны все возможности по индивидуальной настройке рабочей среды, элементы графического интерфейса, правила выполнения файловых операций и многое другое.

### Задание к практической работе

1. Назовите основные элементы графической среды, в которой вы работаете.
2. Объясните, что такое виртуальный рабочий стол (рабочее место)? Как осуществляется переключение между рабочими местами?
3. Настройте панель так, чтобы она автоматически скрывалась. Как добавить на панель какой-либо объект?
4. Запустите файловый менеджер (обозреватель файлов). Изучите интерфейс этой программы. Как использовать навигационную (боковую) панель?
5. Создайте свою папку в домашнем каталоге, в ней – текстовый файл, а на рабочем столе – ссылку на этот файл.
6. Продемонстрируйте копирование, переименование, перемещение и удаление файла или папки.
7. Объясните, как изменить права доступа к файлу?
8. Настройте отображение краткой информации о файле в окне менеджера файлов.
9. При открытых нескольких окнах передайте фокус рабочему столу.
10. Оформите отчет.

**Контрольные вопросы**

1. Что называется графическим интерфейсом?
2. Перечислите основные элементы графического интерфейса операционной системы Linux.
3. Как настроить графическую среду Linux?

# Практическая работа №10. Обработка текста в OpenOffice Writer

**Цель работы:** изучение основных методов и премов оформления текстовых документов в операционной системы Linux.

**Теоретическая справка.** OpenOffice (полное название - OpenOffice.org) - это полноценный офисный пакет программ. Он включает в себя:

* Текстовый редактор и текстовый процессор Writer;
* Редактор HTML файлов, т.е. WWW-страниц;
* Систему электронных таблиц Calc;
* Систему подготовки презентаций Impress;
* Редактор рисунков Draw;
* Редактор формул Math.

OpenOffice во многом похож на другие, давно известные и привычные офисные наборы программ. Однако есть у него и важные отличия:

* Существуют версии OpenOffice и под операционную систему Linux, и под Windows (поддерживаются также другие операционные системы - FreeBSD, Mac OS X). Это позволяет полноценно работать с одними и теми же документами на компьютерах с разными ОС.
* OpenOffice легально свободно распространяется с исходными текстами. Таким образом, отсутствует проблема нелицензионного программного обеспечения.
* Форматы файлов OpenOffice открыты, документированы и широко известны. Кроме того, OpenOffice может успешно работать с файлами многих форматов, включая и файлы, созданные другими известными офисными пакетами.

Во многом работа в OpenOffice схожа с работой в любом другом офисном пакете.

**Задание к практической работе**

1. Запустите текстовый процессор OpenOffice Writer.

2. Изучите меню приложения и основные панели инструментов.

3. Введите в новый документ текст по предложенному образцу.

КЛАССИФИКАЦИЯ ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ

В зависимости от функций, выполняемых программным обеспечением, его можно разделить на две группы: базовое (системное) ПО и прикладное ПО.

Состав базового ПО: операционные системы, трансляторы языков программирования, программы технического обслуживания.

Различают следующие типы прикладных программ: общего назначения (универсальные), проблемно-ориентированные, глобальных сетей.

К программам общего назначения относятся: редакторы, электронные таблицы, системы управления базами данных.

4. Настройте формат первого абзаца по следующим параметрам:

* + отступ слева и справа – 1 см, отступ первой строки – 1,5 см;
  + междустрочный интервал – полуторный;
  + выравнивание – по ширине;
  + интервал перед абзацем 2 см;

5. На основе настроек этого абзаца создайте свой новый стиль абзаца.

6. Примените свой стиль к остальным абзацам.

7. Создайте свой стиль страницы, включающий альбомную ориентацию, верхний колонтитул с вашей фамилией и нижний – с номером страницы. Примените стиль к вашему документу.

8. Добавьте вторую страницу документа.

9. На основе предложенного текста выполните классификацию программного обеспечения в виде многоуровневого нумерованного списка, используя стиль *Цифровой* *со* *всеми* *уровнями*.

10. Покажите результаты работы преподавателю.

# 

# Практическая работа № 11. Табличные вычисления в OpenOffice Calc

# Цель работы: получение навыков создания и оформления таблиц средствами OpenOffice Calc.

**Теоретическая справка.** OpenOffice Calc (ОО Calc) — табличный процессор, входящий в состав офисного пакета OpenOffice.org. С его помощью можно анализировать вводимые данные, заниматься расчётами, прогнозировать, сводить данные с разных листов и таблиц, строить диаграммы и графики.

# Задание к практической работе

1.  Запустить приложение OpenOffice.org Calc.

2.  Изучите меню приложения и основные панели инструментов.

3. Сформировать таблицу по образцу, отвечающую следующим требованиям:

* для заполнения первого и последнего столбцов использовать автозаполнение;
* дополнить таблицу записями о 7 студентах;
* последний столбец должен иметь формат даты.

**График сдачи задания №1**

|  |  |  |  |
| --- | --- | --- | --- |
| **№ п/п** | **ФИО** | **Оценка** | **Дата сдачи** |
| 1. | Иванов И. И. | 5 | 27.09.08 |
| 2. | Петров П. П. | 4 | 29.09.08 |

4.  Текущему листу дать имя «Задание№1».

5.  Определить средний балл группы разными способами.

6.  Посчитать количество оценок каждого вида, используя подходящую функцию из категории *Математические*. Результаты оформить в виде таблицы. Продемонстрировать копирование формулы.

7.  Выбрать фамилии студентов, сдавших задание №1, например, в период с 28.09.08 по 5.10.08. Сохранить результаты отбора отдельно от основной таблицы.

8.  Выполнить сортировку таблицы по убыванию успеваемости.

9.  Построить диаграмму успеваемости группы: либо круговую, используя данные о количестве оценок каждого вида, либо гистограмму, используя данные об оценках каждого студента. Диаграмма должна отвечать следующим требованиям:

* диаграмма должна иметь заголовок;
* гистограммы должна иметь подписи осей;
* в случае круговой диаграммы должны быть легенда и подписи полей.

10. Покажите результаты работы преподавателю.

# Практическая работа № 12. Команды и утилиты Linux

**Цель работы:** изучение основных команд для работы в консоли Linux.

**Теоретическая справка.** Операционная система Linux имеет сотни команд. Рассмотрим некоторые простые полезные команды:

|  |  |
| --- | --- |
| **Команда** | **Краткое описание** |
| **whoami** | Сообщает имя, с которым вы вошли в систему в данном сеансе работы |
| **who** | Сообщает, какие пользователи работают в данный момент в системе |
| **pwd** | Сообщает имя текущего каталога |
| **date** | Показывает дату и время |
| **df** | Показывает, сколько свободного пространства осталось на дисках |
| **cal** | Показывает календарь |
| **echo** *текст* | Отображает текст, написанный после команды, на экране |
| **tty** | Идентифицирует виртуальный терминал |
| **cat** *имя\_файла* | Выводит на экран содержимое указанного после команды файла (или нескольких файлов) |
| **man** *имя\_команды* | Получение справочной информации об указанной команде |
| **wc** *имя\_файла* | Подсчитывает количество слов в указанном текстовом файле или введенных с клавиатуры после команды (без параметра) |
| **ls**  *имя\_каталога* | Выдает список файлов и подкаталогов указанного каталога (если имя каталога не указано, то — текущего) |
| **cd** *имя\_каталога* | Осуществляет смену текущего каталога на указанный |
| **rm** *имя\_файла* | Удаление указанного файла |
| **cat** *список\_файлов* | Конкатенация (объединение) нескольких файлов в стандартный выходной поток (вывод на экран содержимого файлов) |
| **ср** *имя\_файла1 имя\_файла2* | Создание копии файла *имя\_файла1* с именем *имя\_файла2* |
| **mkdir** *имя\_каталога* | Создание каталога с указанным именем |
| **rmdir** *имя\_каталога* | Удаление пустого каталога с указанным именем |
| **mv** *имя\_файла1 имя\_файла2* | Создание копии файла *имя\_файла1* с именем *имя\_файла2*, с последующим удалением файла *имя\_файла1* (перемещение файла) |
| **chmod** *права* *имя\_файла* | Изменение прав доступа к файлу |

# Задание к практической работе

1. Запустить эмулятор консоли.
2. В домашнем каталоге создать свою папку. Убедиться, что она создана.
3. Создать в своей папке текстовый файл, содержащий текущую дату.
4. Создать в своей папке еще один текстовый файл, в который ввести с клавиатуры свои имя, фамилию, группу в отдельных строках.
5. Объединить созданные текстовые файлы в стандартный выходной поток.
6. Назначить конкатенации двух созданных файлов имя stud.
7. Посчитать количество слов, символов и строк в файле stud.
8. Показать права на использование файла stud.
9. Добавить права группе и остальным пользователям на запись и исполнение.
10. Скопировать файл stud в домашнюю папку.
11. Найти в файле stud свое имя.
12. Вывести на экран данные из файла stud упорядоченные обратном порядке.
13. Выведите на экран первые три объекта Рабочего стола.
14. Найдите в домашнем каталоге обычный файл, размер которого не превышает 100Кб.
15. Удалить созданные файлы.
16. Удалить созданную папку.
17. Оформить отчет.

**Контрольные вопросы**

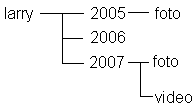
1. Как в Linux содержимое файла связано с его расширением?
2. Какими рекомендациями следует руководствоваться при названии файлов и папок в Linux?
3. Что такое автодополнения терминала и как его вызвать?
4. Вы имеете текстовый файл с текстом на русском языке в кодировке Windows. Можно ли прочитать, работая под Linux?
5. Какие файлы в Linux называются исполняемыми и от какого свойства это зависит?
6. Какой каталог при запуске терминала является текущим по умолчанию? Как сменить каталог? Как вернуться в предыдущий каталог? Как вернуться в домашний каталог?

**Практическая работа № 13. Исследование файловой системы**

**Цель работы:** получение навыков создания файловых структур, закрепление навыка работы в консоли Linux.

**Задание к практической работе**

1. Создать пользователя larry без пароля (adduser larry).
2. Войти в систему от его имени (su larry).
3. В домашнем каталоге данного пользователя создать следующую структуру каталогов:



1. Создать пользователя karl (без пароля).
2. Перейти в его домашний каталог и просмотреть содержимое.
3. Вернуться в свой домашний каталог.
4. Просмотреть содержимое каталога /etc.
5. Просмотреть содержимое каталога /usr/bin.
6. Скопировать файл termcap из каталога etc в домашний каталог пользователя larry.
7. Скопировать файл shells из каталога etc в домашний каталог пользователя larry.
8. Скопировать файл shells из каталога etc в каталог video под новым именем bells.
9. Переместить файл termcap из домашнего каталога пользователя larry в новый файл cells.
10. Переместить файл cells в каталог 2005 с тем же именем.
11. Удалить файлы bells и cells.
12. Просмотреть содержимое файла shells из каталога video с помощью двух команд.
13. Найдите информацию об опциях команды ls и rm.
14. Удалите все созданные вами файлы и каталоги.
15. Оформите отчет.

**Контрольные вопросы**

* 1. Какие команды используются для создания и удаления каталога?
  2. Как перейти в домашний каталог пользователя, корневой каталог, в надкаталог, в подкаталог?
  3. Какие команды используются для копирования и перемещения файлов?
  4. Какие команды используются для просмотра содержимого текстовых файлов?
  5. Как удалить непустой каталог?

**Литература**

1. Гордеев А. В. Операционные системы: Учебник для вузов. 2-е изд. - СПб.: Питер, 2007.
2. Назаров С.В. Операционные среды, системы и оболочки. Учеб. Пособие. – М.: КУДИЦ-ПРЕСС, 2007.
3. Партыка Т.Л., Попов И.И. Операционные системы, среды и оболочки: учебное пособие. – М.: ФОРУМ: Инфра – М, 2009.
4. Сетевые операционные системы / В.Г. Олифер. - СПб.: Питер, 2010
5. Танненбаум Э. Современные операционные системы. 3-е изд., СПб.: Питер, 2010.