**МЕТОДИЧЕСКИЕ УКАЗАНИЯ**

**К ВЫПОЛНЕНИЮ ПРАКТИЧЕСКИХ РАБОТ**

**ПО ДИСЦИПЛИНЕ ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ**

**Для студентов специальности**

**090905 Организация и технология защиты информации**

СОДЕРЖАНИЕ

[Раздел 1. ЗАЩИТА ОТ ВРЕДОНОСНЫХ ПРОГРАММ. ЗАЩИТА ФАЙЛОВ И ПАПОК В ОПЕРАЦИОННОЙ СИСТЕМЕ WINDOWS XP 3](#_Toc422476914)

[Практическая работа № 1 Основные признаки присутствия на компьютере вредоносных программ 3](#_Toc422476915)

[Практическая работа № 2 Работа с командной строкой. Сетевая активность 13](#_Toc422476916)

[Практическая работа № 3 Управление правами пользователей в Windows XP 24](#_Toc422476917)

[Раздел 2. ЗАЩИТА ДОКУМЕНТОВ MS OFFICE 2010 35](#_Toc422476918)

[Практическая работа 4 Защита документов MS Word 2007 38](#_Toc422476919)

[Практическая работа №5 Защита книг MS Excel 2007 45](#_Toc422476920)

# Раздел 1. ЗАЩИТА ОТ ВРЕДОНОСНЫХ ПРОГРАММ. ЗАЩИТА ФАЙЛОВ И ПАПОК В ОПЕРАЦИОННОЙ СИСТЕМЕ WINDOWS XP

# Практическая работа № 1 Основные признаки присутствия на компьютере вредоносных программ

**Цель:** получение практических навыков по выявлению вредоносных программ на локальном компьютере под управлением Microsoft Windows XP.

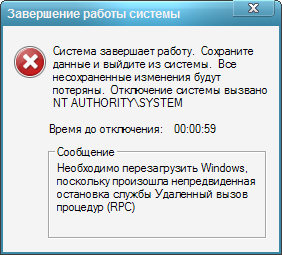
**Методические указания**

Настройку операционной системы или приложений при внесении изменений в ходе выполнения практической работы необходимо вернуть к прежней конфигурации.

**Задание 1. Изучение настроек браузера**

Действия вредоносных программ бывают явными, косвенными и скрытыми. Если первые можно заметить сразу, то косвенные и тем более скрытые требуют от пользователя определенной квалификации - необходимо знать что, где и как нужно искать.

Не все вредоносные программы стремятся спрятаться – многие из них ведут себя весьма активно, то есть явно проявляют себя. Это характерно для троянских и , так называемых, рекламных программ. Явные проявления наиболее часто выражаются в неожиданно появляющихся рекламных баннерах, в изменении домашней страницы в браузере или появляющихся на рабочем столе окнах, как показано на [рис. 1](http://www.intuit.ru/studies/courses/2291/591/lecture/7620?page=1#image.19.1).



**Рис. 1.**

Некоторые рекламные вредоносные программы являются по сути безвредными, так как их основная цель – привлечь внимание к определенному товару или услуге.

Вредоносными программами с косвенными признаками называются программы, которые пытаются отключить или полностью удалить антивирус, блокировать обновление антивирусных баз. Соответственно, если антивирус вдруг ни с того, ни с сего перестал запускаться, либо перестали открываться сайты антивирусных компаний при том, что в целом доступ в Интернет работает нормально, это могут быть проявления вирусов. Вредоносные программы, которые никак не выдают себя, называются скрытыми. Обнаружить их можно только по подозрительным процессам в памяти компьютера, в нестандартной сетевой активности, в изменениях системного реестра.

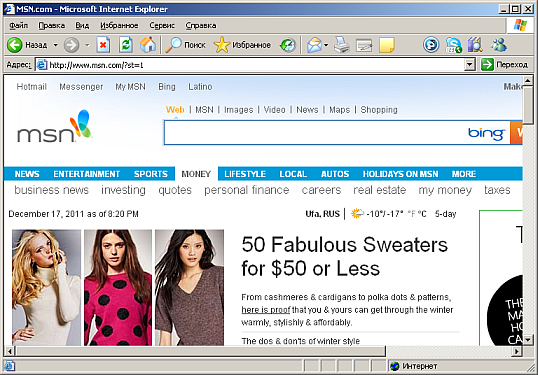
В этом задании предлагается исследовать явные проявления вирусной активности на примере несанкционированного изменения настроек браузера. Этот механизм используется для того, чтобы вынудить пользователей зайти на определенный сайт. Для этого меняется адрес домашней страницы, то есть адрес сайта, который автоматически загружается при каждом открытии браузера.

1. Откройте браузер **Internet Explorer**, воспользовавшись одноименным ярлыком на рабочем столе или в системном меню **Пуск / Программы**



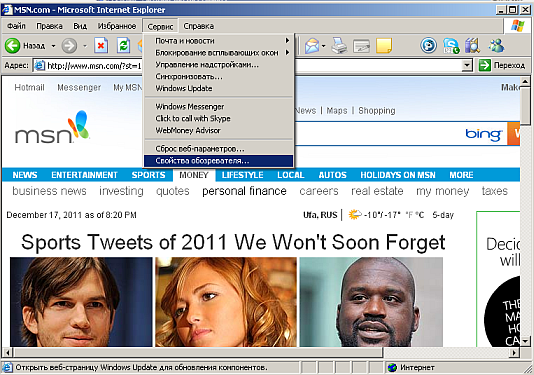
**Рис. 2.**

1. Если у Вас открыт и настроен доступ в Интернет и после установки операционной системы стартовая страница изменена не была, должна открыться страница по умолчанию -  [http://www.msn.com](http://www.intuit.ru/studies/courses/2291/591/lecture/19.http:/www.msn.com).



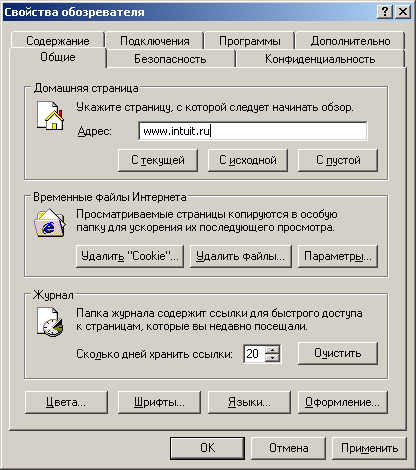
**Рис. 3.**

1. Для того чтобы проверить настройку стартовой страницы воспользуйтесь в меню **Сервис** пунктом **Свойства обозревателя**.



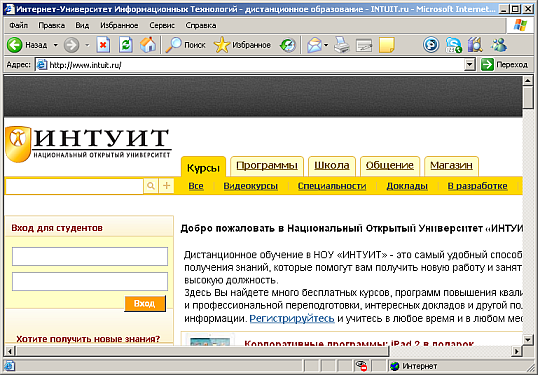
**Рис. 4.**

1. В открывшемся окне **Свойства обозревателя** на закладке **Общие** в поле **Адрес** указан адрес стартовой страницы. Измените поле, введя любой другой адрес, например, [http://www.intuit.ru](http://www.intuit.ru/studies/courses/2291/591/lecture/19.http:/www.intuit.ru), и нажмите ОК. Закройте и снова откройте Internet Explorer.



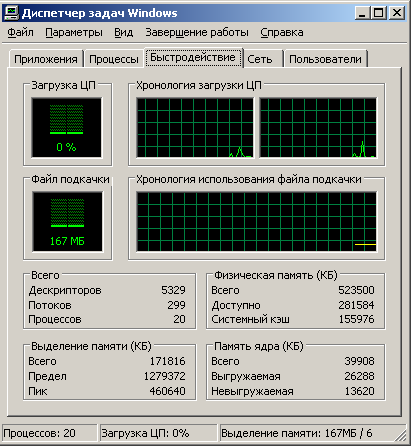
**Рис. 5.**

1. Убедитесь, что теперь первым делом была загружена страница  [http://www.intuit.ru](http://www.intuit.ru/studies/courses/2291/591/lecture/19.http:/www.intuit.ru)



**Рис. 6.**

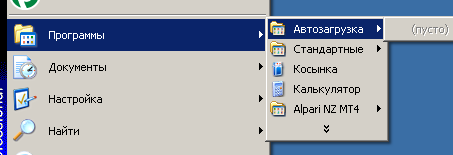
Если Ваш браузер самостоятельно стал при запуске загружать посторонний сайт, проверьте его настройки: какой адрес выставлен в качестве домашней страницы. Некоторые вредоносные программы ограничиваются изменением настройки стартовой страницы, и для устранения последствий их действия необходимо только изменить страницу на желаемую. Однако следует иметь ввиду, что это может быть только частью вредоносной нагрузки. Поэтому при выявлении несанкционированной смены адреса домашней страницы проверьте свой компьютер с помощью антивирусной программы.



**Задание 3. Элементы автозапуска**

Вредоносная программа, так же как любая другая программа, для работы нуждается в запуске. При этом возможно два варианта – сделать так, чтобы пользователь сам запустил вредоносную программу, либо внедриться в конфигурационные файлы и запускаться одновременно с легитимными программами. Оптимальным вариантом для вредоносной программы является "прописывание" себя в автозагрузку при запуске операционной системы.

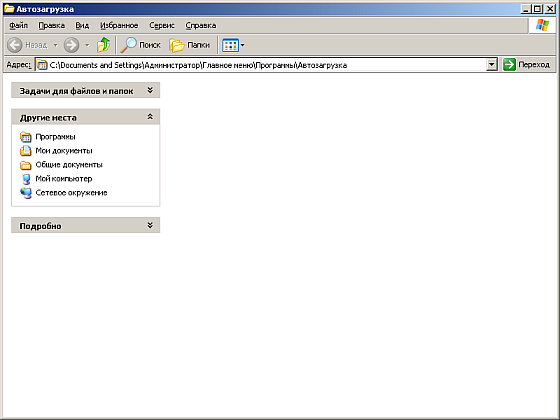
1. Самый простой способ добавить какую-либо программу в автозагрузку - это поместить ее ярлык в раздел **Автозагрузка** системного меню **Пуск / Программы**. По умолчанию, сразу после установки операционной системы этот раздел пуст.



**Рис. 13.**

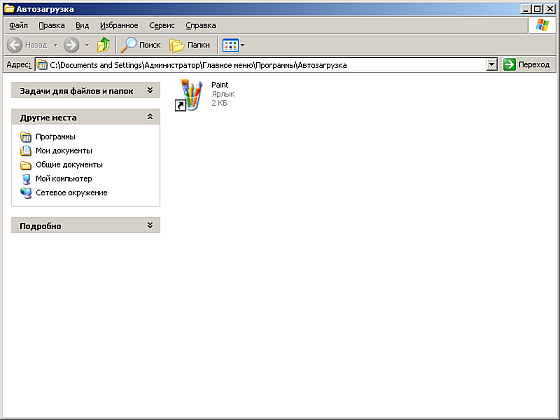
1. Добавьте в список автозагрузки свою программу (создайте ярлык на любую программу, например Калькулятор или Блокнот и поместите его в группу Автозагрузка). Для этого дважды щелкните левой клавишей мыши по названию группы **Автозагрузка**. Откроется папка автозагрузки в стандартном окне – [рис. 14](http://www.intuit.ru/studies/courses/2291/591/lecture/7620?page=3#image.19.14). По умолчанию путь к папке следующий:

**C:\Documents and Settings\Администратор\Главное меню\Программы\Автозагрузка**



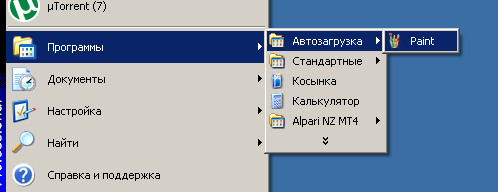
**Рис. 14.**

Всё, что нужно сделать, для того, чтобы программа запускалась автоматически при запуске операционной системы – поместить в данную папку ее ярлык.



**Рис. 15.**

1. Закройте окно и убедитесь, что теперь раздел **Автозагрузка** в меню **Пуск / Программы** содержит **Paint**.

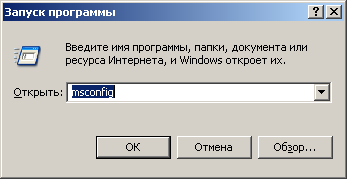


**Рис. 16.**

1. Перезагрузите компьютер. Убедитесь, что в процессе загрузки операционной системы автоматически запустился **Paint**.
2. Отсутствие подозрительных ярлыков в разделе **Автозагрузка** системного меню **Пуск / Программы**, к сожалению, не гарантирует, что ни одна вредоносная программа не запускается автоматически. Технически для автозапуска нужно добавить соответствующую запись в системный реестр операционной системы.

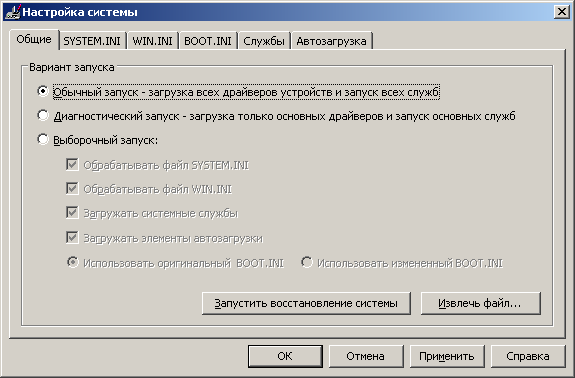
Несмотря на то, что реестр Windows очень большой, существует оболочка, позволяющая с ним работать напрямую - **regedit**. Но делать это рекомендуется только в крайнем случае. Для большинства ситуаций, связанных с автозапуском, достаточно использовать системную утилиту **Настройка системы** .

Запустите ее. Для этого откройте системное меню **Пуск** и перейдите к пункту **Выполнить** и в открывшемся окне **Запуск программы** наберите **msconfig** и нажмите OK.



**Рис. 17.**

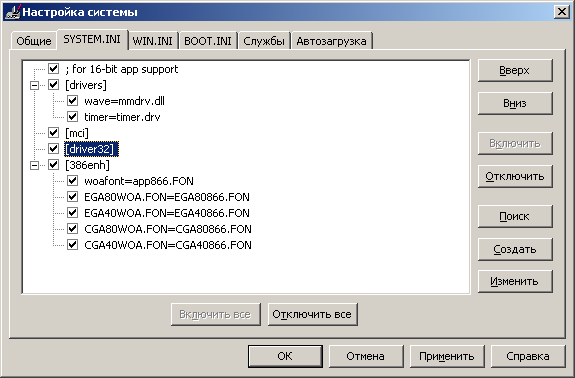
1. Ознакомьтесь с внешним видом окна утилиты **Настройка системы**. На первой закладке **Общие**, можно выбрать вариант запуска операционной системы. По умолчанию отмечен Обычный запуск. Он обеспечивает максимальную функциональность системы. Остальные два варианта запуска предназначены для диагностики.



**Рис. 18.**

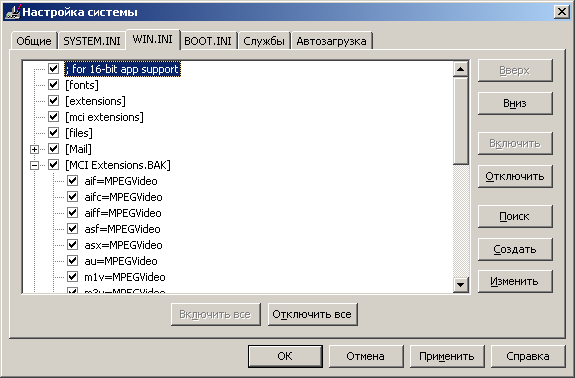
**Диагностический запуск** рекомендуется использовать также при подтвердившемся наличии вредоносной программы - если компьютер уже заражен, сразу установить антивирус в ряде случаев нельзя, например, если вирус сознательно блокирует запуск ряда антивирусных программ. Тогда, если нет возможности удалить или хотя бы временно обезвредить вирус вручную, рекомендует запустить операционную систему в безопасном режиме, инсталлировать антивирус и сразу же проверить весь жесткий диск на наличие вирусов.

1. Ознакомьтесь со списком запускаемых драйверов и других параметров операционной системы, перейдя к закладке SYSTEM.INI . Тут отображаются все ссылки, указанные в одноименном системном файле.



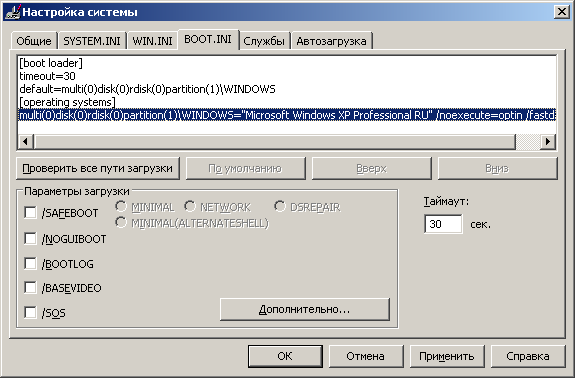
**Рис. 19**

1. Перейдите к аналогичной закладке **WIN.INI** и ознакомьтесь с ее содержимым.



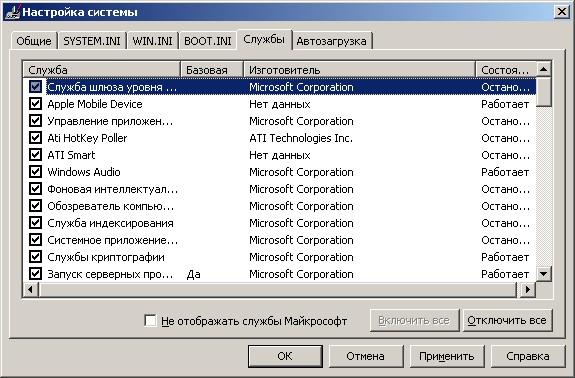
**Рис.**

1. Следующая закладка **BOOT.INI** также отображает данные из одноименного файла. Как и предыдущие две, она также содержит системную информацию. Изменять ее можно только обладая соответствующими знаниями!



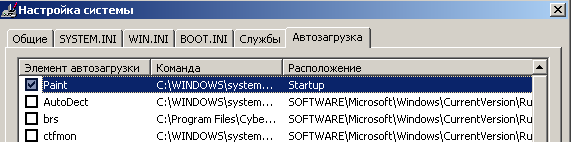
**Рис. 21.**

1. Перейдите на закладку **Службы**. Здесь представлен список всех служб, установленных в системе. Каждая служба представляет собой некое приложение, работающее в фоновом режиме. Например, антивирусный комплекс, обеспечивающий постоянную защиту, также встраивает свою службу, следовательно, она должна присутствовать в этом перечне. Так же и вирус может установить свою службу в системе.



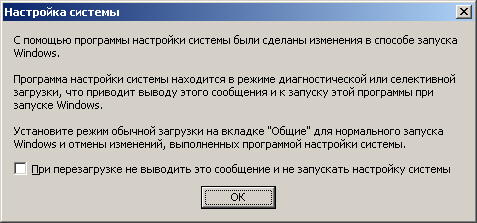
**Рис.**

1. Перейдите к последней закладке **Автозагрузка** и убедитесь, что в списке приложений, автоматически запускаемых при загрузке системы, есть **Paint**.



**Рис.**

1. Отключите автоматическую загрузку **Paint**, убрав галочку напротив него в столбце **Элемент автозагрузки** и нажмите ОК. В открывшемся окне согласитесь на перезагрузку.
2. После того, как компьютер перезагрузится, система выведет предупреждение в виде окна, представленного на [рис. 23](http://www.intuit.ru/studies/courses/2291/591/lecture/7620?page=3#image.19.23).



**Рис. 24.**

1. Откройте окно **Настройка системы**. Обратите внимание, что теперь используется не обычный запуск, а выборочный. При этом полностью обрабатываются все элементы файлов SYSTEM.INI, WIN.INI и BOOT.INI, загружаются все службы, но флаг **Загружать элементы автозагрузки затенен**. Это означает неполную загрузку .
2. Перейдите к закладке **Автозагрузка** и убедитесь, что ее вид не изменился - **Paint** все так же присутствует в списке, но отключен.
3. Не закрывая окна **Настройка системы** проверьте, что Paint автоматически не запустился и раздел **Пуск / Программы / Автозагрузка** теперь снова пуст.
4. Необходимо учесть, что если выбрать после изменений **Обычную загрузку** – все файлы, находящиеся на вкладке **Автозагрузка** будут запускаться снова, в том числе и **Paint**.

**Контрольные вопросы**

1. Перечислите признаки проявления вирусной активности на примере несанкционированного изменения настроек браузера.

2. Назовите способы обнаружения присутствия вредоносных программ на компьютере.

# Практическая работа № 2 Работа с командной строкой. Сетевая активность

**Цель:** получение практических навыков по работе с Командной строкой и по выявлению вредоносных программ на компьютере с Microsoft Windows XP с помощью Командной строки.

**Методические указания**

Настройку операционной системы или приложений при внесении изменений в ходе выполнения практической работы необходимо вернуть к прежней конфигурации.

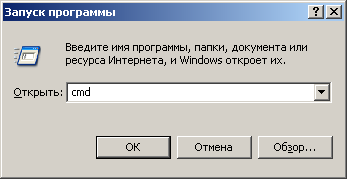
**Задание 1. Работа с Командной строкой**

В операционной системе Windows 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)**.

Таким образом, оболочка командной строки – это отдельный программный продукт, который обеспечивает прямую связь между пользователем и операционной системой. Текстовый пользовательский интерфейс командной строки предоставляет среду, в которой выполняются приложения и служебные программы с текстовым интерфейсом. В операционных системах Windows 9.x командный интерпретатор был представлен исполняемых файлом command.com (как и в MS-DOS). Начиная с Windows NT, он реализован cmd.exe и обладает большими возможностями.

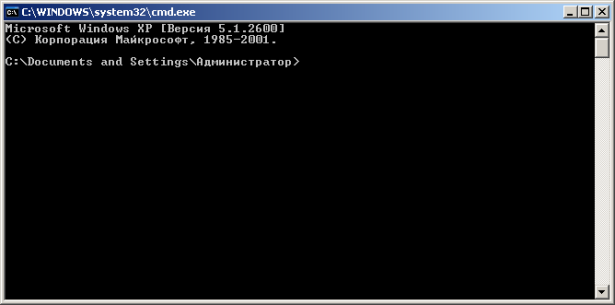
В Windows XP файл **Cmd.exe**, как и другие исполняемые файлы, соответствующие внешним командам операционной системы, находятся в каталоге SYSTEM32.

1. Для открытия сеанса работы с командной строкой выберите **Пуск->Выполнить**. В открывшемся окне наберите **cmd** и нажмите на ОК.



**Рис. 1.**

В результате откроется новое окно, в котором можно запускать команды и видеть результат их работы.



**Рис. 2.**

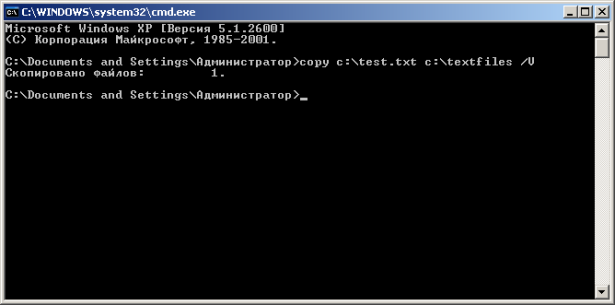
Некоторые команды распознаются и выполняются непосредственно самим командным интерпретатором — такие команды называются **внутренними** (например, copy или dir). Другие команды операционной системы представляют собой отдельные программы, расположенные по умолчанию в том же каталоге, что и Cmd.exe, которые Windows загружает и выполняет аналогично другим программам. Такие команды называются **внешними** (например, more или xcopy).

1. Для того чтобы выполнить команду введите имя этой команды (регистр не важен), ее параметры и ключи (если они необходимы) и нажмите клавишу Enter. Синтаксическая структура выводится в том порядке, в котором следует вводить команду и следующие за ней параметры, если они есть. Следующий пример команды xcopy иллюстрирует разнообразие синтаксических форматов текста.

xcopy источник [результат] [/w] [/p] [/c] [/v] [/q] [/f] [/l] [/g] [/d[:мм-дд-гггг]] [/u] [/i] [/s [/e]] [/t] [/k] [/r] [/h] [{/a|/m}] [/n] [/o] [/x] [/exclude:файл1[+[файл2]][+[файл3]] [{/y|/-y}] [/z]

Создайте на диске C файл **test.txt** и папку **Text files**. В Командной строке наберите

**copy C:\test.txt C:\Textfiles /V**



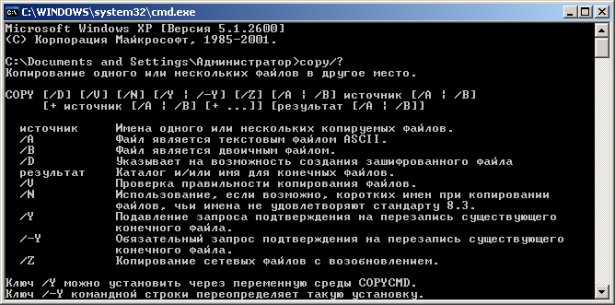
**Рис. 3.**

Имя команды здесь — **copy**, параметры — **C:\test.txt** и **C:\TextFiles**, а ключом является **/V**. Отметим, что в некоторых командах ключи могут начинаться не с символа /, а с символа – (минус), например, **-V**.

Следует обратить внимание, что если в имени папки есть пробел, в команде его быть не должно, как в указанном примере.

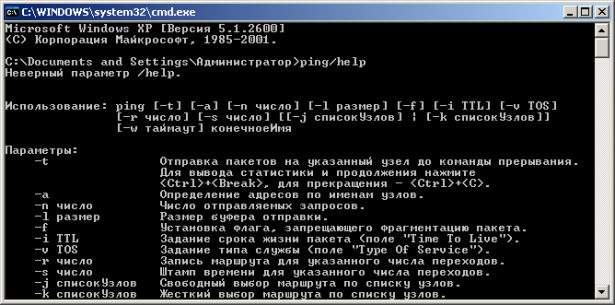
1. Многие команды Windows имеют большое количество дополнительных параметров и ключей, и запомнить их все невозможно или по крайней мере очень трудно. Большинство команд снабжено встроенной справкой, в которой кратко описываются назначение и синтаксис данной команды. Получить доступ к такой справке можно путем ввода команды с ключом **/?** или **/help**. В командной строке наберите

**copy /?**



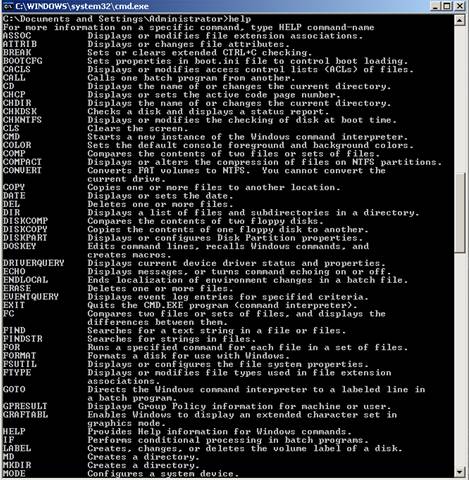
**Рис. 4.**

**ping /help**



**Рис. 5.**

Команда **help** выводит список основных команд Командной строки



**Рис. 6.**

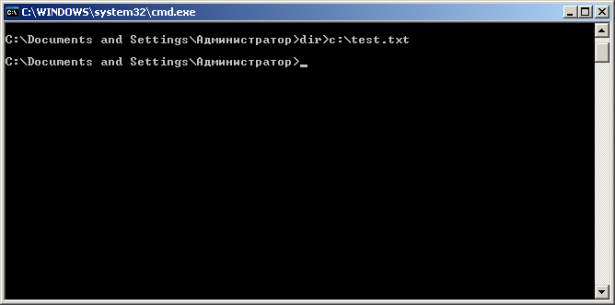
1. С помощью переназначения устройств ввода/вывода одна программа может направить свой вывод на вход другой или перехватить вывод другой программы, используя его в качестве своих входных данных. Таким образом, имеется возможность передавать информацию от процесса к процессу при минимальных программных издержках. Практически это означает, что для программ, которые используют стандартные входные и выходные устройства, операционная система позволяет: выводить сообщения программ не на экран, а в файл, читать входные данные не с клавиатуры , а из заранее подготовленного файла, передавать сообщения, выводимые одной программой, в качестве входных данных для другой программы.

Выходные данные практически всех команд высвечиваются в окне командной строки. Даже команды, выводящие данные на диск или принтер, выдают сообщения и запросы в окне командной строки.

Для перенаправления вывода команд из окна командной строки в файл или на устройство применяется оператор ">". Этот оператор используется с большинством команд. Например, для перенаправления вывода команды dir в файл test.txt введите в Командной строке:

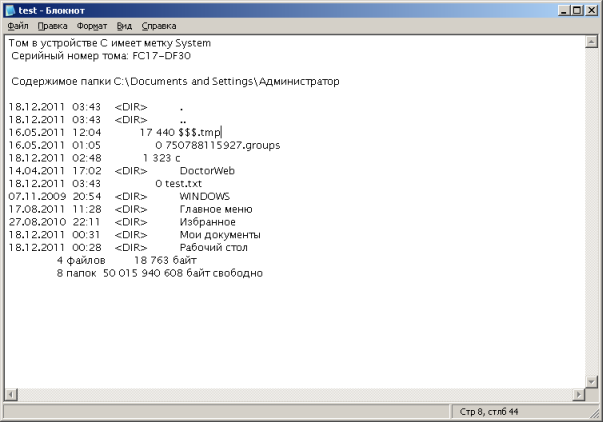
**dir>c:test.txt**

Если указанный файл не существует, интерпретатор команд Cmd.exe создаст его. Если файл существует, Cmd.exe заменит информацию в файле на данные, полученные от команды dir.



**Рис. 7.**

Откройте файл test.txt . В нем будет содержаться результат команды dir.



**Рис. 8.**

Следует отметить, что информация, которая была в файле до этого, будет стерта. Для того чтобы выходные файлы команды добавлялись в конец файла, необходимо использовать символ >>, а не > в синтаксисе команды.

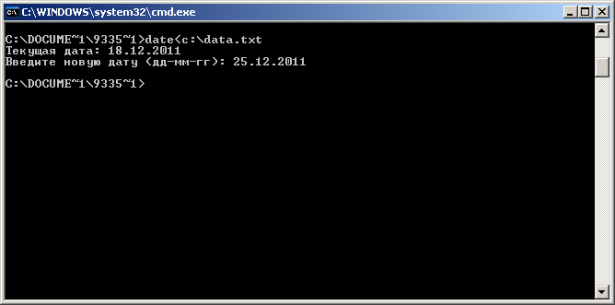
Местоположение потоков ввода и вывода называется дескриптор.

В [таблице 1](http://www.intuit.ru/studies/courses/2291/591/lecture/7621?page=1#table.20.1) описаны операторы перенаправления потоков ввода и вывода команд.

|  |  |
| --- | --- |
| Таблица 1. | |
| **Оператор перенаправления** | **Описание** |
| > | Записывает данные на выходе команды вместо командной строки в файл или на устройство, например, на принтер. |
| < | Читает поток входных данных команды из файла, а не с клавиатуры. |
| >> | Добавляет выходные данные команды в конец файла, не удаляя при этом существующей информации из файла. |
| >& | Считывает данные на выходе одного дескриптора как входные данные для другого дескриптора. |
| <& | Считывает входные данные одного дескриптора как выходные данные другого дескриптора. |
| | | Считывает выходные данные одной команды и записывает их на вход другой команды. Эта процедура известна под названием "канал". |

1. С помощью символа < можно прочитать входные данные для заданной команды не с клавиатуры, а из определенного (заранее подготовленного) файла. На диске С создайте файл data.txt и напишите в нем 25.12.2011. В Командной строке наберите

**Date < c:\data.txt**

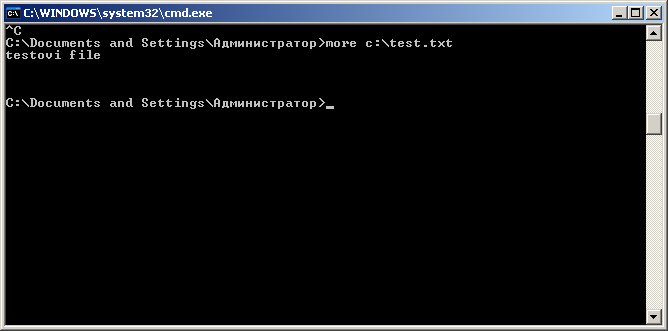


**Рис. 9.**

Проверьте дату на вашем компьютере – она изменилась на 25.12.2011

1. Команда **more** выводит содержимое файла или выхода команды в одном окне командной строки за раз. Например, чтобы отобразить содержимое файла test.txt в одном окне командной строки за раз, введите следующую команду:

**more c:\ test.txt**



**Рис. 10.**

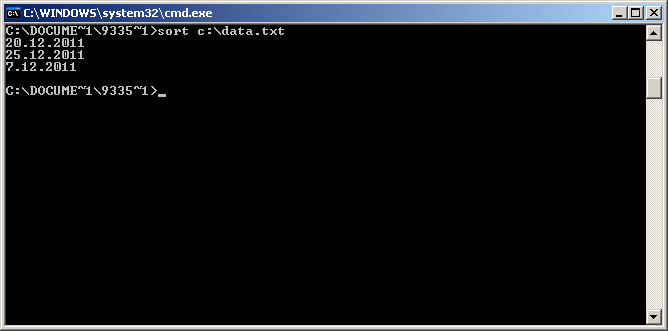
Если файл большой, то отображается одно окно командной строки со сведениями, а затем в нижней части окна командной строки отображается строка **-- More --**. Для остановки просмотра следует ввести комбинацию **CTRL+C**.

Команда **more** полезна при работе с командами, создающими выход более одного окна командной строки. Например, при выводе дерева каталогов жесткого диска.

1. Другой распространенной командой фильтрации является **sort** - она выполняет сортировку по алфавиту текстового файла или выхода команды.

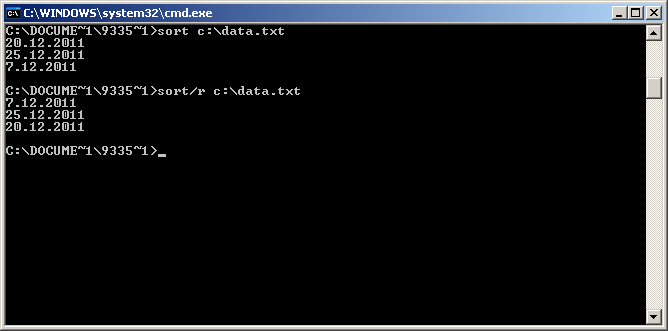
Отредактируйте файл data.txt, добавив туда две другие даты, например, 12.2011 и 7.12.2011.В командной строке наберите:

**sort < C:\data.txt**



**Рис. 11.**

**sort /r < C:\date.txt**



**Рис. 12.**

Ключ **/R** позволяет изменить порядок сортировки на обратный.

**Задание 2. Сетевая активность**

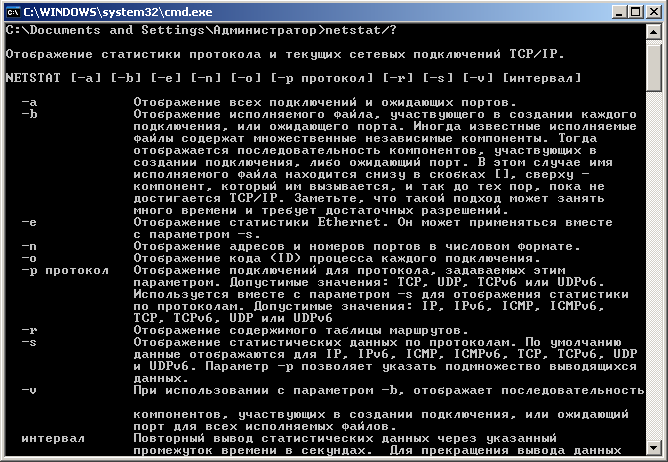
Одним из проявлений наличия вредоносной программы может быть возросшая сетевая активность. Вредоносная программа может отправлять письма, скачивать информацию из Интернета, передавать кому-то по сети конфиденциальную информацию и многое другое. При этом необходимо помнить, что легальные приложения также могут использовать Интернет без действий пользователя – например, антивирусная программа может скачивать обновления антивирусной базы данных.

Для получения полной информации о сетевой активности можно использовать команду **netstat**, которая выводит на экран мгновенную статистику сетевых соединений.

1. В Командной cтроке наберите:

**netstat /?**

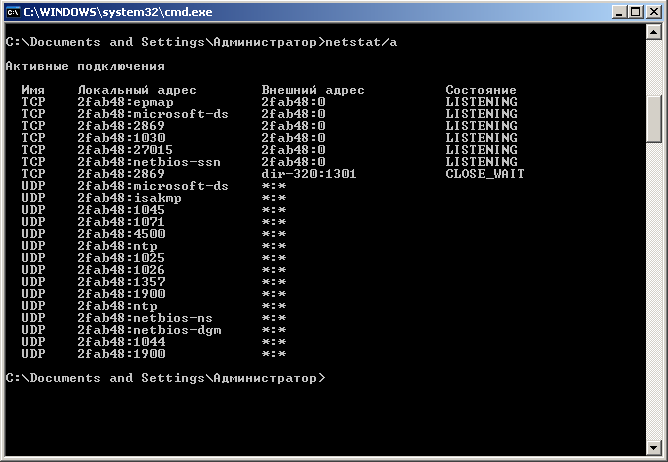
1. Прочитайте описание утилиты netstat. Убедитесь, что для вывода самой полной информации нужно использовать ключ **-a**



**Рис. 13.**

1. В Командной строке наберите:

**netstat/a**



**Рис. 14.**

Результатом выполнения команды является список активных подключений, в который входят установленные соединения и открытые порты.

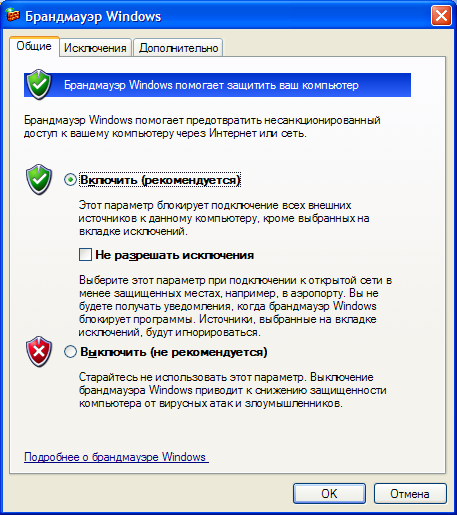
**TCP-порты** обозначаются строкой "TCP" в колонке Имя. Открытые TCP-порты обозначаются строкой "LISTENING" в колонке состояние. Часть портов связана с системными службами Windows и отображается не по номеру, а по названию - epmap, microsoft-ds, netbios-ssn. Порты, не относящиеся к стандартным службам, отображаются по номерам.

**UDP-порты** обозначаются строкой "UDP" в колонке Имя. Они не могут находиться в разных состояниях, поэтому специальная пометка "LISTENING" в их отношении не используется. Как и TCP-порты они могут отображаться по именам или по номерам.

Порты, используемые вредоносными программами, чаще всего являются нестандартными и поэтому отображаются согласно их номерам. Впрочем, могут встречаться троянские программы, использующие для маскировки стандартные для других приложений порты, например 80, 21, 443 - порты, используемые на файловых и веб-серверах.

Команда **netstat**, в отличие от Диспетчера задач Windows, не работает в режиме реального времени, а отображает мгновенную статистику. Следовательно, для просмотра активности соединений, скажем, через минуту, нужно заново выполнить команду.

http://www.intuit.ru/EDI/07_11_13_1/1383686256-5639/tutorial/428/objects/21/files/3_7.jpg



**Контрольные вопросы**

1. Перечислите основные правила и особенности работы с Командной строкой.
2. Каким образом вредоносные программы на компьютере с Microsoft Windows XP обнаруживаются с помощью Командной строки?
3. Каким образом получается полная информация о сетевой активности?

**Практическая работа № 3  
Управление правами пользователей в Windows XP**

**Цель:** ознакомиться с процедурами создания ученых записей пользователей и управления их правами.

**Теоретическая часть**

В операционной системе Windows XP на одном и том же компьютере могут работать разные пользователи, каждый под своим именем. При входе в ОС запрашиваются имя и пароль, на основе которых происходит аутентификация пользователя.

Компьютер может работать автономно, а может быть рабочей станцией в сети. Если компьютер загружается для автономной работы или для работы в одноранговой сети, то пользователь регистрируется, используя внутренний (локальный) список имен пользователей системы.

Если компьютер загружается для работы в сети с выделенным сервером, то пользователь регистрируется, используя имя, которое ему выдал администратор сети. Список с этими именами хранится на сервере.

Данные о пользователе находятся в специальной базе данных на локальных компьютерах и на сервере. На каждого пользователя заводится отдельная учетная карточка, которая носит название учетная запись.

Windows XP использует три типа учетных записей пользователей:

1. Локальные учетные записи для регистрации пользователей локального компьютера. База локальных учетных записей хранится на каждом компьютере своя, и содержит информацию о пользователях только данного компьютера. Создаются учетные записи администратором этого компьютера.
2. Встроенные учетные записи пользователей создаются автоматически при установке Windows XP. Встроенных учетных записей две — Администратор и Гость. Встроенные учетные записи хранятся в той же базе, что и локальные учетные записи.
3. Учетные записи пользователей домена хранятся на выделенном сервере и содержат данные о пользователях локальной сети.

Локальная учетная запись - это учетная запись, которой могут быть предоставлены разрешения и права на вашем компьютере. Для удобства управления локальными пользователями, их можно объединять в группы и управлять группами, чтобы не устанавливать одни и те же настройки для каждого пользователя в отдельности. Ограничения, установленные для группы, распространяются на всех пользователей этой группы.

Домен или глобальные пользователи и группы управляются сетевым администратором. Имеется возможность добавить локальных пользователей, глобальных пользователей и глобальные группы в локальные группы. Однако невозможно добавить локальных пользователей и локальные группы в глобальные группы.

Пользователи и группы важны для безопасности Windows XP поскольку позволяют ограничить возможность пользователей и групп выполнять определенные действия путем назначения им прав и разрешений. Право дает возможность пользователю выполнять на компьютере определенные действия, такие как архивирование файлов и папок или завершение работы компьютера. Разрешение представляет собой правило, связанное с объектом (например, файлом, папкой или принтером), которое определяет, каким пользователям и какого типа доступ к объекту разрешен.

Операционная система содержит несколько встроенных учетных записей пользователей и групп, которые не могут быть удалены:

* **Учетная запись администратора**

Учетная запись пользователя с именем "Администратор" используется при первой установке рабочей станции или рядового сервера. Эта учетная запись позволяет выполнять необходимые действия до того, как пользователь создаст свою собственную учетную запись. Администратор является членом группы администраторов на рабочей станции или рядовом сервере.

Учетную запись "Администратор" нельзя удалить, отключить или вывести из группы администраторов, что исключает возможность случайной потери доступа к компьютеру после уничтожения всех учетных записей администраторов. Это свойство отличает пользователя "Администратор" от остальных членов локальной группы "Администраторы".

* **Учетная запись гостя**

Учетная запись гостя предназначена для тех, кто не имеет реальной учетной записи на компьютере. Учетную запись "Гость" нельзя удалить, но можно переименовать или отключить. Учетной записи пользователя "Гость", как и любой другой учетной записи, можно предоставлять права и разрешения на доступ к объектам. Учетная запись "Гость" по умолчанию входит во встроенную группу "Гости", что позволяет пользователю войти в систему с рабочей станции или рядового сервера. Дополнительные права, как любые разрешения, могут быть присвоены группе "Гости" членом группы администраторов.

К стандартным группам Windows XP относятся следующие группы:

* **Администраторы**

Пользователи, входящие в группу "Администраторы", имеют полный доступ на управление компьютером. Это единственная встроенная группа, которой автоматически предоставляются все встроенные права и возможности в системе. По умолчанию туда входит учетная запись "Администратор".

* **Операторы архива**

Члены группы "Операторы архива" могут архивировать и восстанавливать файлы на компьютере, независимо от всех разрешений, которыми защищены эти файлы. Также они могут входить на компьютер и выключать его, но не могут изменять параметры безопасности.

* **Опытные пользователи**

Члены группы опытных пользователей могут создавать учетные записи пользователей, но могут изменять и удалять только созданные ими учетные записи. Они могут создавать локальные группы и удалять пользователей из локальных групп, которые они создали. Они также могут удалять пользователей из групп "Опытные пользователи", "Пользователи" и "Гости".

Они не могут изменять группы "Администраторы" и "Операторы архива", не могут являться владельцами файлов, не могут выполнять архивирование и восстановление каталогов, не могут загружать и выгружать драйверы устройств или управлять журналами безопасности и аудита.

* **Пользователи**

Члены группы пользователей могут выполнять наиболее распространенные задачи, например запуск приложений, использование локальных и сетевых принтеров, завершение работы и блокировка рабочих станций. Пользователи могут создавать локальные группы, но изменять могут только те, которые они создали. Пользователи не могут организовывать общий доступ к каталогам или создавать локальные принтеры.

* **Гости**

Группа "Гости" позволяет случайным или разовым пользователям войти в систему со встроенной учетной записью гостя рабочей станции и получить ограниченные возможности. Члены группы "Гости" могут только прекратить работу компьютера.

Управление учетными записями пользователей и группами осуществляется пользователями, входящими в группу Администраторы.

**Методические указания**

Настройку операционной системы или приложений при внесении изменений в ходе выполнения практической работы необходимо вернуть к прежней конфигурации.

**Выполнение работы**

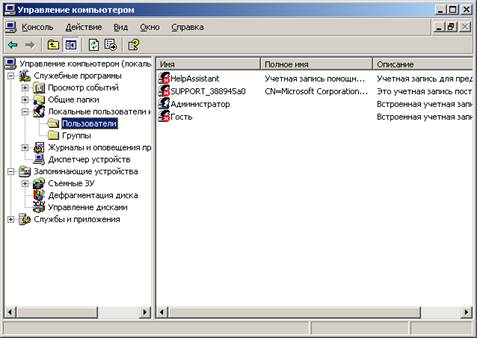
**Задание 1. Управление учетными записями пользователя**

Для управления учетными записями используется компонент "Управление компьютером". Чтобы его открыть выберите Пуск->Настройка->Панель управления.

Дважды щелкните значок Администрирование http://www.intuit.ru/EDI/07_11_13_1/1383686256-5639/tutorial/428/objects/22/files/4_k1.jpgзатем дважды щелкните значок Управление компьютером http://www.intuit.ru/EDI/07_11_13_1/1383686256-5639/tutorial/428/objects/22/files/4_k2.jpg. Второй способ открыть "Управление компьютером" нажать правой кнопкой на значке "Мой компьютер" и в появившемся контекстном меню выбрать "Управление".

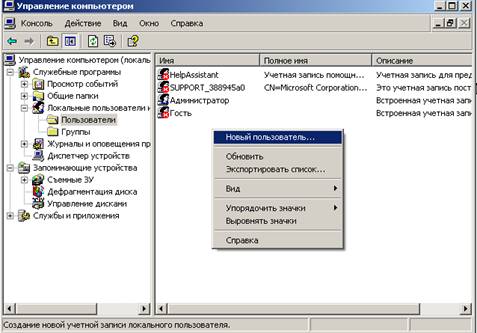
**Создание новой учетной записи пользователя**

1. Откройте компонент "Управление компьютером" одним из описанных выше способов.
2. В дереве консоли выберите компонент "Локальные пользователи и группы" и щелкните в нем узел Пользователи.



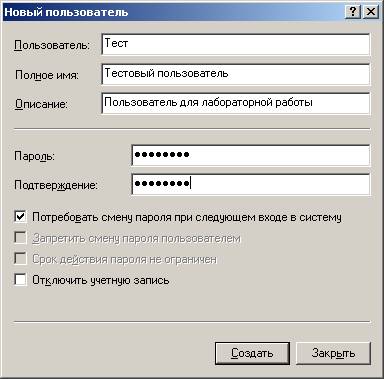
**Рис. 1.**

1. Нажмите правой кнопкой мыши в окне со списком пользователей и в появившемся меню выберите команду Новый пользователь.



**Рис. 2.**

1. В появившемся окне заполните поля по аналогии с [рис. 3](http://www.intuit.ru/studies/courses/2291/591/lecture/7623?page=2#image.22.3).



**Рис. 3.**

По умолчанию стоит опция "потребовать смену пароля при следующем входе в систему". То есть система при первом входе пользователя в ОС потребует от него сменить пароль. Если убрать галочку с этого пункта, появится возможность выбрать следующие опции:

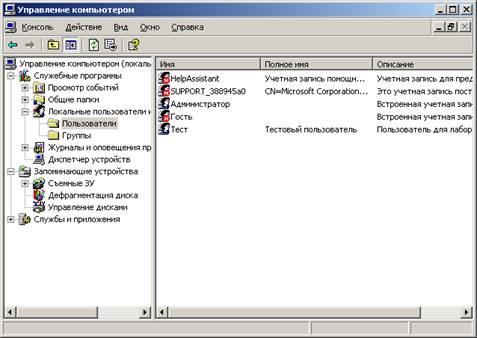
* + запретить смену пароля пользователем. То есть пользователь будет использовать пароль, заданный при создании учетной записи;
  + срок действия пароля не ограничен – то есть пароль никогда не истекает.

Опция "Отключить учетную запись" делает вход в систему данного пользователя невозможным.

Чтобы завершить работу, нажмите кнопку Создать, а затем Закрыть.

Если есть необходимость в создании сразу нескольких пользователей нужно нажать на Создать и повторить все предыдущие шаги. После заведения последнего пользователя нажать на Создать и затем сразу на Закрыть.

После этого заведенные пользователи появляются в списке, как показано на [рис. 4](http://www.intuit.ru/studies/courses/2291/591/lecture/7623?page=2#image.22.4).



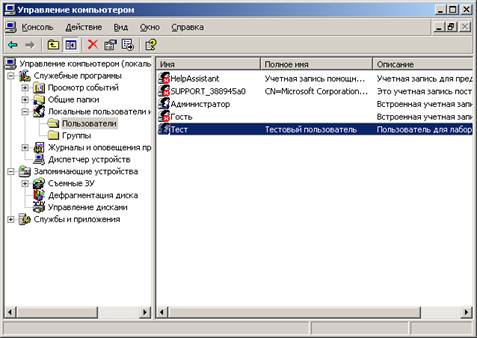
**Рис. 4.**

**Изменение учетной записи пользователя**

1. Откройте компонент "Управление компьютером".

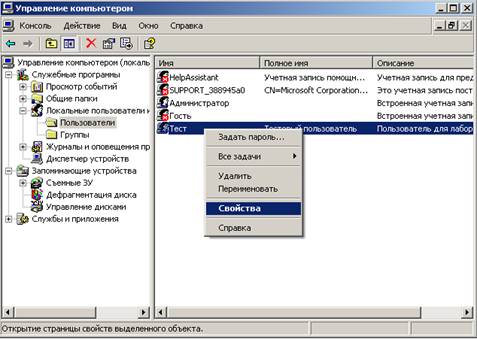
2. В дереве консоли выберите компонент "Локальные пользователи и группы" и перейдите к Пользователям.

3. Выберите учетную запись, которую требуется изменить.



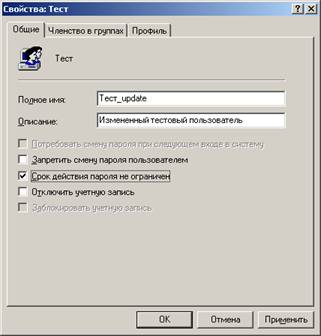
**Рис. 5.**

4. Нажмите на учетную запись правой кнопкой мыши и в контекстном меню выберите "Свойства".



**Рис. 6.**

5. Внесите нужные изменения и нажмите кнопку ОК.



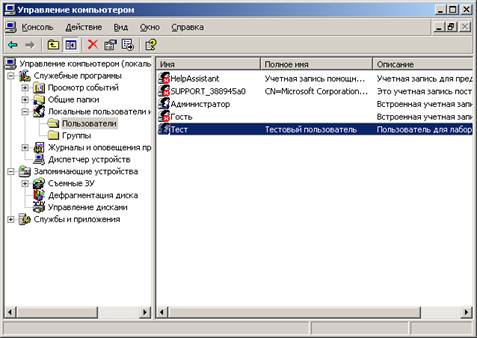
**Рис. 7.**

**Изменение пароля для пользователя**

1. Откройте компонент "Управление компьютером".

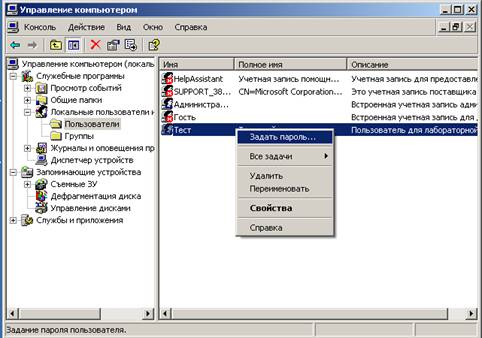
2. В дереве консоли выберите компонент "Локальные пользователи и группы" и щелкните в нем узел Пользователи.

3. Выберите учетную запись, которую требуется изменить.



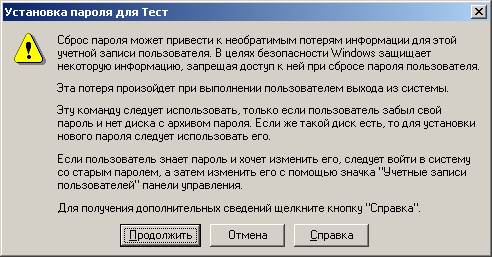
**Рис. 8.**

4. В контекстном меню выберите пункт "Задать пароль".



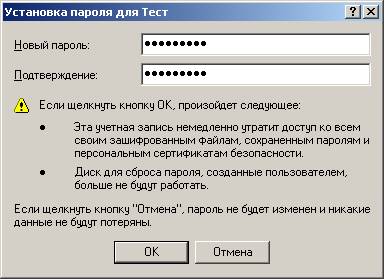
**Рис. 9.**

5. Вылезет окошко, извещающее о том, что принудительная смена пароля администратором является крайней мерой. Нажмите кнопку "Продолжить".



**Рис. 10.**

6. В появившемся окне задайте новый пароль для пользователя и нажмите на ОК. Теперь пользователь сможет войти в систему только с новым паролем.



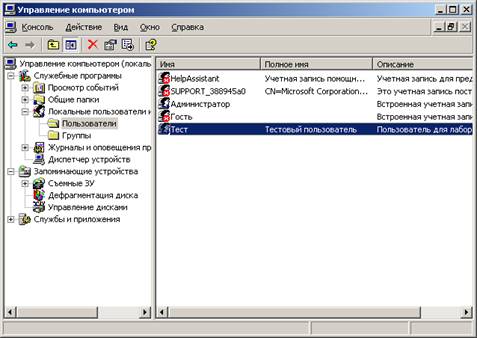
**Рис. 11.**

**Отключение и активизации учетной записи пользователи**

1. Откройте компонент "Управление компьютером".

2. В дереве консоли выберите компонент "Локальные пользователи и группы" и щелкните в нем узел Пользователи.

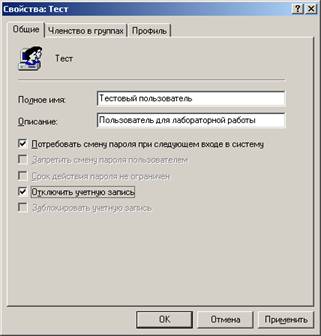
3. Выберите учетную запись, которую требуется изменить.



**Рис. 12.**

4. В меню контекстном меню выберите Свойства.

5. Чтобы отключить выбранную учетную запись пользователя, установите флажок "Отключить учетную запись".



**Рис. 13.**

**Удаление учетной записи пользователи**

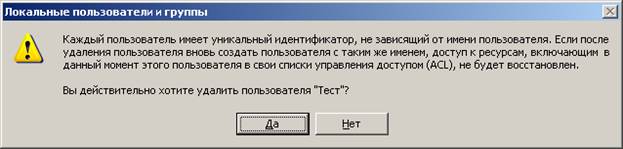
1. Откройте компонент "Управление компьютером".

2. В дереве консоли выберите компонент "Локальные пользователи и группы" и щелкните в нем узел Пользователи.

3. Выберите учетную запись, которую требуется удалить.

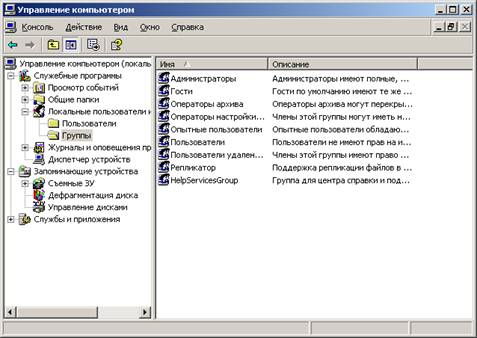
4. В контекстном меню учетном записи выберите Удалить.

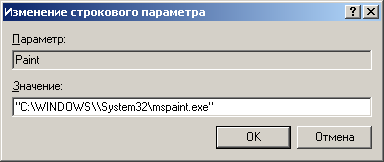
5. Появится окно, предупреждающее о последствиях удаления пользователя. Выберите ДА.



**Рис. 14.**

6. Пользователь исчезнет из списка.





**Контрольные вопросы**

1. Какова процедура создания ученых записей пользователей и управления их правами?
2. Каковы правила задания имени и пароля пользователя?
3. Каким образом происходит аутентификация пользователя?

# Раздел 2. ЗАЩИТА ДОКУМЕНТОВ MS OFFICE 2010

**Теоретические сведения**

В документах MS Office предусмотрено несколько уровней защиты, позволяющих управлять доступом к данным и их изменением.

Просмотр документов MS Word, книг MS Excel и баз данных MS Access может быть ограничен с помощью парольной защиты (пароль для открытия файла). При установке пароля на открытие документа содержимое файла шифруется (алгоритм шифрования AES).

Для документов MS Word и MS Excel также имеется возможность установки парольной защиты на сохранение внесенных изменений (пароль разрешения записи). Если пользователю не известен пароль разрешения записи, он может открыть документ в режиме «только для чтения». В этом случае возможно внесение изменений в текст документа, однако нельзя сохранить измененный файл документа под старым именем. Для сохранения изменений требуется ввести новое имя файла.

Пароль на открытие, пароль разрешения записи устанав­лива­ются на файл, то есть относятся к документу/книге в целом.

Кроме паролей на файл в целом, имеются возможности защиты отдельных элементов документов MS Office:

* Парольная защита от просмотра элементов книги Excel (строк, столбцов, листов). Невозможно защитить от просмотра часть документа MS Word, отдельные ячейки книги MS Excel;
* Парольная защита от изменения частей (разделов) документа Word, содержимого отдельных ячеек и их диапазонов в Excel, структуры листа (вставка, удаление и форматирование строк и столбцов), структуры книги (добавление и удаление листов, отображение, скрытые листов), изменение размеров, положения или видимости окна, настроенного для отображения книги Excel;
* Разграничение доступа (возможность изменения) к диапазонам ячеек Excel для локальных и сетевых пользователей ОС Windows;
* Разграничение доступа аутентифи­ци­ро­ванн­ных пользователей к фрагментам текста MS Word, задание ограничений на несанкционированное распространение документа (пересылка по электронной почте, изменение, копирование) требует установки дополнительного программного обеспечения (сервера аутентификации, WRM – клиентa управления правами Windows).

Следует учитывать, что функциональные возможности парольной защиты на отдельные элементы MS Excel (скрытие данных и защита листов и книг) и MS Word (защита разделов) не предназначены для защиты данных или важных сведений в документах MS Office.

Они используются для более понятного представления сведений, скрывая сведения или формулы, которые могут сбить с толку некоторых пользователей. Эти средства служат также для предотвращения случайного изменения данных пользователями. Скрытые или защищенные паролем данные внутри документов MS Office не шифруются. При определенных усилиях и наличии времени пользователи смогут просмотреть и изменить все сведения внутри документа MS Office, если они имеют доступ к самому документу (пароль на открытие документа не установлен или известен).

Чтобы предотвратить изменение данных и обеспечить безопасность важных сведений, следует ограничить доступ к файлам (пароль на открытие файла), содержащим подобные сведения, сохранив их в расположениях, доступных только пользователям, прошедшим аутентификацию (разграничение доступа к файлам и папкам средствами ОС).

В документах MS Office имеется возможность заверять цифровой подписью как документ в целом, так и внедренный в документ код макросов на языке VBA. Наличие действительной цифровой подписи гарантирует целостность (неизменность) содержимого, а также аутентичность и неотрекаемость (подлинность авторства и невозможность отказа от авторства).

Полноценная проверка подлинности цифровых подписей возможна в том случае, если они выданы сетевым сервером аутентификации (в домене локальной сети), либо доверенным центром сертификации в Интернете. Если же используется локальный сертификат, создаваемый самим пользователем с помощью утилиты ***selfcert.exe*** (Digital Certificate for VBA Projects, Цифровой сертификат для проектов VBA), то проверить на другом компьютере подлинность подписи, созданной с его помощью, будет невозможно. Кроме того, другие пользователи локального компьютера также не будут доверять такой подписи.

В MS Access 2007 предусмотрена модель безопасности, которая упрощает процесс защиты базы данных и ее открытия с включенной защитой:

* возможен просмотр данных даже при отключенном коде MS Visual Basic для приложений (VBA) или отключенных компонентах в базе данных;
* eсли файлы базы данных расположены в надежном месте, например в папке или в общем сетевом ресурсе, которые указаны как надежные, они будут открываться и обрабатываться без сообщений с предупреждениями и запроса о включении или отключении содержимого. Однако, код VBA в подписанных базах данных не будет работать, пока издатель не будет признан надежным, а также в том случае, если подпись станет недействительной.

Когда центр управления безопасностью определяет, что база данных не имеет состояния доверенной, MS Access 2007 открывает ее в режиме отключения, то есть отключает любое выполняемое содержимое:

* Код VBA и все ссылки в нем, а также все небезопасные выражения;
* Небезопасные макрокоманды во всех макросах. «Небезопасными» являются команды, позволяющие пользователю изменять базу данных или получать доступ к ресурсам вне базы данных;
* Запросы на изменение (добавляют, обновляют или удаляют данные);
* Управляющие запросы (DDL-запросы, используются для создания или изменения объектов базы данных, таких как таблицы и процедуры);
* SQL-запросы к серверу (отправляют команды непосредственно на сервер базы данных, поддерживающий стандарт Open Database Connectivity (ODBC). Запросы к серверу работают с таблицами на сервере, минуя ядро базы данных Access);
* Элементы управления ActiveX.

В предыдущих версиях Access для применения сертификата безопасности к индивидуальным компонентам базы данных использовался редактор Visual Basic. MS Access 2007 упрощает и ускоряет процесс добавления подписи и распространения базы данных. После создания ACCDB или ACCDE-файла можно упаковать его, применить к пакету цифровую подпись, а затем распространить подписанный пакет среди других пользователей. Средство подписывания пакетов помещает базу данных в файл развертывания Access (с расширением .ACCDC), подписывает пакет, а затем помещает пакет, подписанный кодом, в указанное расположение. Пользователи затем могут извлекать базу данных из пакета и работать непосредственно в ней, а не в файле пакета.

При извлечении базы данных из подписанного пакета и перемещении в надежное расположение ее открытие происходит без отображения панели сообщений. Если база данных из подписанного пакета отправляется в ненадежное расположение, но имеется надежный сертификат пакета, и подпись действительна, то также нет необходимости решать вопрос о доверии.

В MS Access 2007 применяется стойкий алгоритм шифрования баз данных с использованием пароля. В процессе шифрования происходит перемешивание данных в таблицах, что исключает их несанкционированный просмотр.

MS Access 2007 не предусматривает защиту на уровне пользователя для баз данных, созданных в новом формате (файлы с расширением .ACCDB или .ACCDE). Поэтому при открытии базы данных MS Access 2007 все пользователи имеют возможность просмотра всех ее объектов. Однако при открытии базы данных из более ранней версии Access, имеющей защиту на уровне пользователя, в MS Access 2007 установленные для пользователей ограничения доступа к объектам базы данных будут продолжать работать. При преобразовании подобной базы данных в новый формат все параметры безопасности автоматически удаляются и применяются правила защиты файлов .ACCDB и .ACCDE.

# Практическая работа 4 Защита документов MS Word 2007

**Цель:** изучить способы защиты документов MS Word 2007

**Методические указания**

Задания работы сохраняются в отдельные электронные документы на ресурсе указанном преподавателем. При установке паролей для защиты документа, не забываете сохранить (записать) для себя пароль в цель защиты от его **утраты.**

Ответы на контрольные вопросы дайте письменно в тетради для практических работ. К работе записывается название и ее цель.

**Выполнение работы**

**Задание 1.** Создайте шаблон делового письма, содержащий текст шапки и подписи стандартного письма организации, с защищенными от изменения реквизитами. Средняя часть письма (содержание письма) доступно для изменения.

При этом в защищенных шапке и подпись письма следует предусмотреть возможность изменения следующих данных:

* исходящий номер и дата создания письма могут быть изменены (набраны) с клавиатуры;
* фамилия исполнителя может быть выбрана из списка.

Открытие файла письма должно быть защищено паролем.

***Создание документа, разбиение его на части и защита документа и его частей***

1. Создать новый документ Word, согласно рис.1, вставив в нужном месте графический элемент – линию, для этого:

* создать новый документ и сохранить его с именем «Письмо». Ввести и отформатировать текст документа в соответствии с рис.1.
* Добавить пустую строку между реквизитами организации и исходящим номером письма, установить для нее форматирование абзаца без отступов по бокам, без красной строки, выравнивание: по центру;
* Установить курсор в начало пустой строки и вставить графическую линию, выполнив команду **Вставка|Клип**. В области команды нажать кнопку **Поиск**, выделить изображение понравившейся линии в коллекции клипов и щелкнуть по нему мышью для вставки в документ.
* Закрыть область вставки клипов.

|  |
| --- |
|  |

Рис.1. Текст шаблона стандартного письма

1. После слов «Исх.№», «от» и «/» ввести поля формы для занесения данных в защищенном от изменения документе. Для этого следует сначала настроить приложение MS Word для работы с элементами управления форм:

**Отображение вкладки «Разработчик»**

1. Откройте вкладку Файл.
2. Нажмите кнопку Параметры.
3. Нажмите кнопку Настройка ленты.
4. Выберите команду Настройка ленты и в разделе Основные вкладки установите флажок Разработчик.

* В строке меню MS Word 2010 появится вкладка **Разработчик**.
* На вкладке **Разработчик** в группе **Элементы управления** нажать кнопку **Режим конструктора Изображение ленты**.
* Установить курсор после слов «Исх.№ », затем щелкнуть элемент управления **Форматированный текст** Изображение ленты для ввода произвольного текста.
* Аналогичным образом следует вставить элемент управления **Дата** Изображение лентыпосле слова «от » для выбора даты;
* После слов «Исполнитель /» вставить элемент управления **Раскрывающийся список** Изображение ленты для выбора фамилии исполнителя из списка.
* После вставки поля **Раскрывающийся список** следует задать варианты для выбора (элементы списка). Для того, чтобы задать элементы списка, следует выделить вставленный элемент списка, щелкнув на нем мышью, а затем нажать кнопку **Свойства** Изображение лентыв группе **Элементы управления**.
* В окне свойств списка (рис.2) нажать кнопку **Добавить** и ввести в окне *Добавить вариант* фамилию первого исполнителя, нажать **ОК**. Затем добавить еще две-три фамилии исполнителей. Удалить пункт «Выберите элемент» из значений списка, для чего следует выделить данный вариант мышью, а затем нажать кнопку **Удалить**.

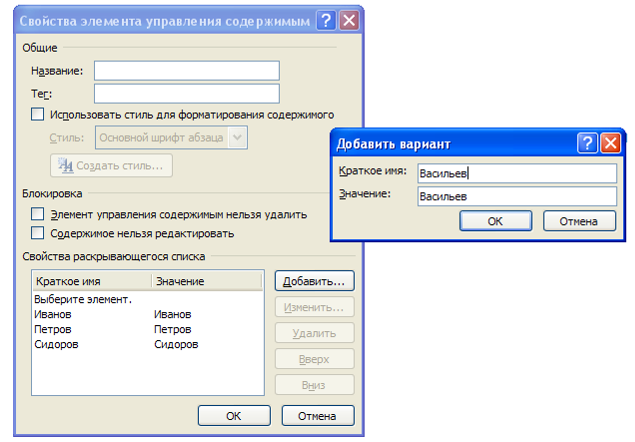


Рис.2. Формирование списка исполнителей

* Задать написание фамилии исполнителя курсивом. Для этого в окне свойств списка установить флажок ***Использовать стиль для форматирования содержимого***, затем щелкнуть на кнопке **Создать стиль** и создать новый стиль, основанный на стиле абзаца, с написанием курсивом. Для сохранения стиля нажать **ОК**.
* Для выхода из окна свойств списка нажать **ОК**.

1. Проверить действие текстового поля, поля и поля со списком (возможен ввод текста, выбор даты, выбор из списка). Если поля не действуют, следует нажать кнопку **Режим конструктора**.
2. Разбить документ на три части (раздела) в соответствии с рис.3:

первый раздел – содержит шапку письма с исходящим номером и датой создания письма;

второй раздел – пустые строки в середине письма, предназначенный для последующего набора текста письма;

третий раздел – включающий подпись и фамилию исполнителя.

|  |
| --- |
|  |

Рис.3. Разбиение документа шаблона письма на разделы

Для того, чтобы вставляемые линии разрывов отображались на экране, на вкладке **Главная** следует включить режим отображения непечатаемых символов – нажать кнопку .

Вставить два разрыва раздела (первый – после строки с исходящим номером, второй – перед словом «Исполнитель»), оставив между ними пустые строки. Для вставки разрыва:

* установить курсор в место вставки разрыва;
* перейти на вкладку **Разметка страницы** и открыть группу **Разрывы**. В группе **Разрывы** выбрать **Разрывы разделов/ Текущая страница**.

1. Установить защиту от изменения текста первого и третьего разделов документа, содержащих шапку и подпись стандартного письма с паролем ***high***:

* На вкладке **Разработчик** или **Рецензирование** открыть группу **Защита**, выбрать команду **Ограничить редактирование**
* в области команды *Ограничить форматирование и редактирование* установить флажок ***Разрешить только указанный способ редактирования документа*** в группе *Ограничения на редактирование* и выбрать из выпадающего списка ***Ввод данных в поля форм***.
* Затем щелкнуть мышью на появившейся ссылке ***Выбор разделов*** и установить флажки только напротив разделов 1 и 3 (рис.4), подтвердить выбор защищаемых разделов, нажав **ОК**.

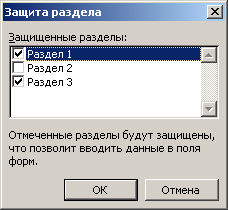
**

Рис.4. Установка защиты отдельных разделов документа

* Активировать введенные ограничения, щелкнув на кнопке **Да, включить защиту**, дважды ввести пароль ***high*** (в поле ввода пароля и поле подтверждения), нажать **ОК**.
* Проверить, что защита установлена, то есть можно менять только текст содержимого письма (Раздел 2 документа), а также менять значения элементов управления в шапке письма и выбирать фамилию исполнителя из списка.

1. Установить парольную защиту просмотра документа «Письмо» с помощью пароля на открытие (пароль ***low***):

* Откройте вкладку **Файл.**
* Щелкните элемент **Сведения**.
* Щелкните **Защитить документ** → **Зашифровать паролем.**
* В поле **Шифрование документа** введите пароль и нажмите кнопку ОК.
* Еще раз введите пароль в поле **Подтверждение пароля** и нажмите кнопку ОК.

1. Сохранить документ «Письмо». Проверить действие парольной защиты, закрыв и заново открыв документ.
2. Установить для документа «Письмо» режим «только чтение» или **Разрешение записи**, защищенный паролем.

Для этого:

Выполнить команду **Файл** → **Сохранить как**, щелкнуть на кнопке **Сервис** и выбрать пункт **Общие параметры**. В окне общих параметров уже задан *пароль для открытия файла* (отображается черными точками), поставить галочку в окне «Рекомендовать доступ только для чтения» или ввести пароль ***medium*** в строку *пароль разрешения записи.* Нажать **ОК**, а затем ввести ***medium*** еще раз в строке подтверждения ввода пароля. Затем нажать кнопку **Сохранить** в окне сохранения документа.

1. Проверить действие пароля разрешения записи, закрыв и вновь открыв документ «Письмо».

**Задание 2.** На основе общего шаблона письма создать шаблон делового письма конкретного исполнителя.

***Снятие ограничений доступа к документу и защиты его частей, запрет изменения содержимого элементов управления в документе.***

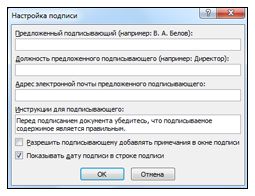
1. Открыть документ «Письмо», выполнить команду **Сохранить как**, в окне команды ввести новое имя файла «Письмо1», рекомендовать для нового файла открытие в режиме «только чтение», удалив в группе **Сервис/Общие параметры** пароль разрешения записи и установив флажок ***Рекомендовать доступ только для чтения***.
2. Проверить действие новых параметров, закрыв и вновь открыв документ «Письмо1». При открытии документа его следует открыть в режиме записи изменений, ответив во втором окне предупреждения НЕТ.
3. Ввести номер, выбрать дату и фамилию исполнителя в полях документа. Занести произвольный текст письма. В конце текста письма набрать строку текста: «Последнее изменение» и вставить текущую дату и время, щелкнув на кнопке **Дата и время** группы *Текст* на вкладке **Вставка**. Выбрать формат даты с указанием числа и времени с точностью до секунд. Включить флажок ***Обновлять автоматически***. Для вставки поля даты в документ нажать **ОК**.
4. Проверить действие поля даты. Запомнить вставленное значение времени (минуты, секунды). Сохранить документ. Затем закрыть и заново открыть документ в режиме записи изменений (см.п.11). Проверить, что значение времени последнего изменения документа изменилось.
5. Запретить изменение фамилии исполнителя. Для этого:

* Снять защиту частей документа «Письмо1», щелкнув в окне команды **Рецензирование/Защитить документ/Ограничить форматирование и редактирование** кнопку **Отключить защиту**.
* Выделить поле с фамилией исполнителя, щелкнув на ней мышью. На вкладке **Разработчик** щелкнуть на кнопке **Свойства**. В окне свойств элемента управления включить флажки ***Элемент управления содержимым нельзя удалить*** и ***Содержимое нельзя редактировать***.
* Проверить действие установленных флажков.

1. Установить защиту первого и третьего разделов документа «Письмо1» с паролем ***high***. Сохранить изменения в документе.

**Задание 3.** Создать окончательную версию делового письма, заверенную цифровой подписью исполнителя.

***Удаление метаданных из документа, использование цифровой подписи документа.***

1. Открыть документ «Письмо1» и сохранить его под новым именем «Письмо 2», оставив из ограничений доступа только пароль на открытие документа (в окне команды **Сохранить как/Сервис/Общие параметры** снять флажок ***Рекомендо­вать доступ только для чтения***).
2. Окончательно отредактировать текст документа (при необходимости сменить дату письма на актуальную). Отключить защиту разделов внутри документа «Письмо2».
3. Просмотреть свойства документа и убедиться, что были очищены все свойства на вкладке ***Документ***.
4. Создать собственный цифровой сертификат: в Главном меню Windows (**Пуск/Программы**) выбрать в группе **Microsoft Office/Средства Microsoft Office** (Microsoft Office Tools) средство  **Цифровой сертификат для проектов VBA** (Digital Certificate for VBA Projects), и ввести в строку создания сертификата свое имя.
5. Заверить документ «Письмо2» своей цифровой подписью. Для этого:
6. Поместите указатель мыши в то место в документе или на листе, где необходимо создать строку подписи.
7. На вкладке **Вставка** в группе **Текст** раскройте список **Строка подписи** и выберите пункт **Строка подписи Microsoft Office.**
8. В диалоговом окне Настройка подписи введите сведения, которые будут отображены под строкой подписи.  
   
9. Предложенный подписывающий. Полное имя подписывающего лица.
10. Должность предложенного подписывающего. Должность подписывающего лица (если таковая имеется).
11. Адрес электронной почты предложенного подписывающего Адрес электронной почты подписывающего лица (при необходимости).
12. Инструкции для подписывающего. Инструкции для подписывающего лица.
13. Установите один или оба указанных ниже флажка.
14. Разрешение подписывающему добавлять примечания в окне подписи. Разрешение подписывающему указать цель добавления подписи.
15. Показывать дату подписи в строке подписи. Отображение даты подписи вместе с подписью

**Контрольные вопросы:**

1. Чем различается действие защиты от изменения текста документа, установленной с помощью защиты форм (команда **Защитить документ**) и защиты в режиме «только для чтения» (установка на файл пароля разрешения записи)?
2. Чем различается действие защиты от изменения в случае задания пароля разрешения записи и в случае рекомендации открытия документа в режиме «только для чтения»?
3. Почему после подписания документа невозможно внести изменения в его текст?

# Практическая работа №5 Защита книг MS Excel 2007

**Цель:** изучить встроенные способы защиты рабочих книг, листов MS Excel 2007; научиться применять их.

**Методические указания**

Задания работы сохраняются в отдельные электронные документы на ресурсе указанном преподавателем. При установке паролей для защиты документа, не забываете сохранить (записать) для себя пароль в цель защиты от его **утраты.**

Ответы на контрольные вопросы дайте письменно в тетради для практических работ. К работе записывается название и ее цель.

**Выполнение работы**

**Задание 1**.Создайте книгуMS Excel, содержащую данные о сотрудниках организации.

***Создание таблиц и ограничений на ввод данных***

1. Открыть приложение MS Excel. Создать новую книгу, сохранить ее в рабочую папку с именем ***Организация***.
2. Переименовать Лист1 в «Отчет», Лист2 – в «Ведомость», Лист3 – в «Справочники». Для этого щелкнуть правой кнопкой мыши по ярлычку листа и выбрать команду **Переименовать** из контекстного меню.
3. Перейти на лист «Справочники». Создать таблицу «Данные о подразделениях»: выделить диапазон ячеек **A1:C5**, выделить границы диапазона (вкладка **Главная**, группа **Шрифт/ Границы** ). Объединить ячейки **A1:C1** (выделить диапазон **A1:C1**, выполнить команду  на вкладке **Главная**, группа **Выравнивание**). Ввести в объединенную ячейку текст заголовка таблицы: «Данные о подразделениях». В ячейки **A2**, **B2** и **С2** соответственно ввести текст заголовков столбцов таблицы: «Код подразделения», «Наименование», «Руководитель».
4. Задать ограничения на ввод данных в столбец «Код подразделения»:

* Выделить интервал ячеек **A3:A5**, перейти на вкладку **Данные** и выполнить команду **Проверка данных**  (в группе **Работа с данными**),
* В окне команды *Проверка вводимых значений* на вкладке *Параметры* выбрать *Тип данных*: ***Список***, в строку *Источник* набрать: 1;2;3 (через точку с запятой) – рис.6.
* Для выхода из окна команды нажать **ОК**. После этого в таблицу можно заносить данные, выбирая их из списка.

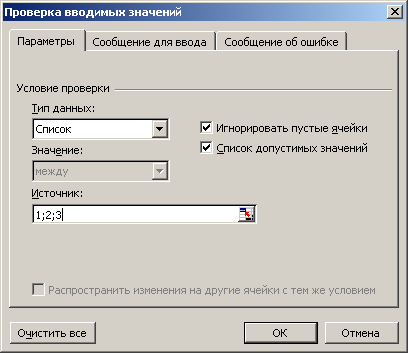


Рис.6. Задание ограничений на ввод данных в столбец «Код подразделения»

1. Заполнить данными таблицу «Данные о подразделениях».
2. В диапазоне ячеек **A7:D21** создать таблицу «Данные о сотрудниках»: ячейки **A7:D7** – заголовок таблицы (объединить ячейки), ячейки **A8:D8** – заголовки столбцов («Фамилия», «Дата поступления», «Разряд», «Подразделение»), ячейки **A9:D21** – данные.
3. Задать ограничения на ввод данных в столбец «Разряд»:

* Выделить интервал ячеек **С9:С21**, на вкладке **Данные** в группе **Работа с данными** выполнить команду **Проверка данных** ,
* В окне команды *Проверка вводимых значений* на вкладке *Параметры* выбрать *Тип данных*: ***Целое число***, *Значение*: ***между***, в строке *Минимум* набрать: 10, в строке *Максимум* – 17 – рис.7.
* На вкладке *Сообщение об ошибке* окна команды в строке *Заголовок:* ввести текст Несуществующий разряд, а в строке *Сообщение:* Разряд от 10 до 17.
* Для выхода из окна команды нажать **ОК**.

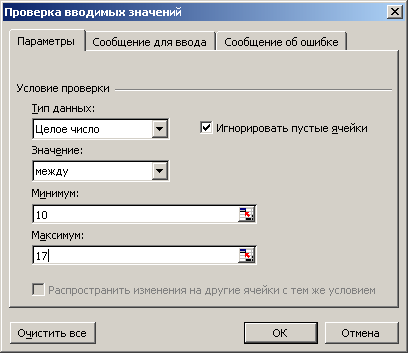


Рис.7. Задание ограничений на ввод данных в столбец «Разряд»

1. Задать ограничения на ввод данных в столбец «Подразделение»:

* Выделить интервал ячеек **D9:D21**, выполнить команду **Проверка данных**,
* В окне команды *Проверка вводимых значений* на вкладке *Параметры* выбрать *Тип данных*: Список, перейти в строку *Источник*, а затем, не выходя из окна команды, выделить на листе «Справочники» диапазон ячеек **A3:A5** таблицы «Данные о подразделениях», содержащий коды подразделений – ссылка на диапазон будет занесена в строку *Источник* – рис.8.
* Для выхода из окна команды нажать **ОК**.

1. Заполнить данными таблицу «Данные о сотрудниках». Сохранить изменения. Таблицы на листе «Справочники» с данными представлены на рис.9.

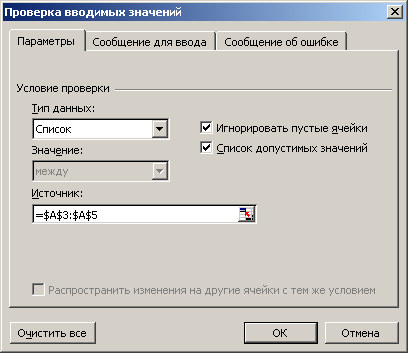


Рис.8. Определение ограничений на ввод данных в столбец «Подразделение»

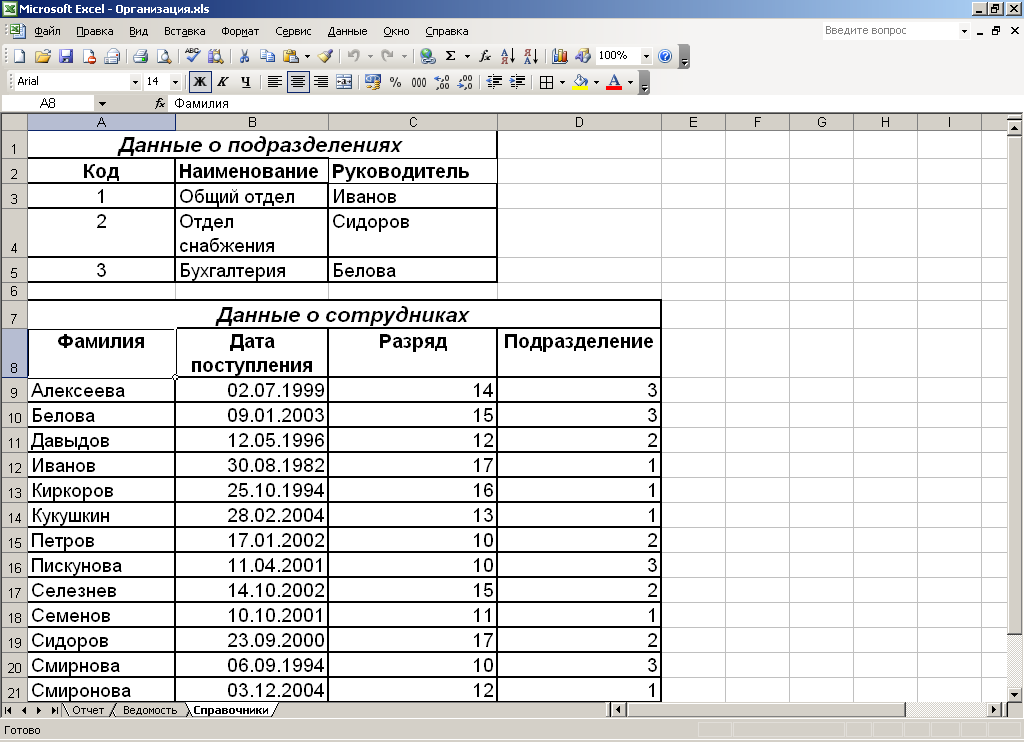


Рис.9. Данные таблиц на листе «Справочники»

**Задание 2**. Выполните расчет начислений сотрудникам, итоговых значений.

***Выполнение расчетов в таблицах, подсчет итогов***

1. Перейти на лист «Ведомость». В диапазоне ячеек **A1:F15** создать таблицу «Сводная ведомость»: ячейки **A1:F1** – заголовок таблицы, ячейки **A2:F2** – заголовки столбцов («Фамилия», «Код подразделения», «Стаж, в годах», «Оклад», «Премия», «Начислено»), ячейки **A3:F15** – данные.
2. Продублировать в диапазоне **A3:A15** листа «Ведомость» данные из столбца «Фамилия» таблицы «Данные о сотрудниках» (диапазон **A9:A21** листа «Справочники») –выделить диапазон **A3:A15** листа «Ведомость», в строке формул нажать знак =, перейти на лист листа «Справочники», выделить диапазон **A9:A21**, а затем ввести сформированную формулу как формулу массива, для чего следует одновременно нажать клавиши CTRL+SHIFT+ENTER.
3. Заполнить столбец «Код подразделения» таблицы «Сводная ведомость»:

* Выделить ячейку **B3** листа «Ведомость», щелкнув на ней мышью. Перейти на вкладку Функции и выбрать функцию **ВПР** в группе **Библиотека функций/Ссылки и массивы **;
* В окне конструктора функции **ВПР** выбрать *Искомое\_значение*: ячейка этой же строки, содержащая фамилию (**A3**), *Таблица*: выделить область данных таблицы «Данные о сотрудниках» с листа «Справочники», ссылку преобразовать в абсолютную, нажав кнопку **F4** (**Справочники!$A$9:$D$21**), *Номер\_столбца*: ввести номер столбца «Подразделение» по счету в таблице «Данные о сотрудниках» (**4**), *Интервальный\_просмотр*: ***ложь***. Вид функции **ВПР** в конструкторе приведен на рис.10. Нажать **OК**.
* Результирующий вид функции **ВПР** в ячейке **B3**:

**=ВПР(A3;Справочники!$A$9:$D$21;4;ЛОЖЬ)**

* Скопировать ячейку **B3** на весь диапазон данных столбца «Код подразделения» таблицы «Сводная ведомость» (**B4:B15**) – для этого подвести указатель мыши к правому нижнему углу ячейки **B3** так, чтобы указатель принял вид черного крестика, затем нажать левую кнопку мыши и не отпуская ее растащить ячейку на весь диапазон **B4:B15**.

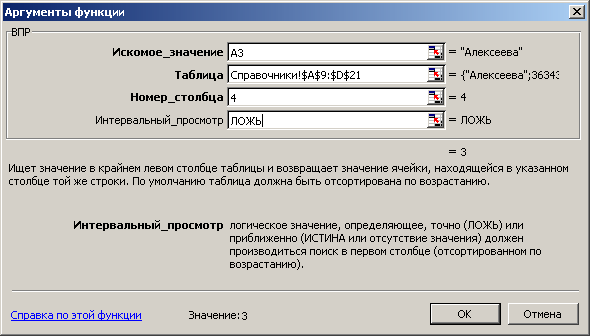


Рис.10. Задание параметров функции ВПР в конструкторе

1. Заполнить столбец «Стаж, в годах» таблицы «Сводная ведомость»:

* Задать числовой формат данных для столбца «Стаж, в годах», для этого: выделить диапазон ячеек **C3:C15**, щелкнуть правой кнопкой мыши, выбрать из контекстного меню пункт **Формат ячеек**, на вкладке *Число* выбрать тип ***Числовой*** и нажать ***ОК***.
* Сформировать в ячейке **С3** формулу для вычисления стажа: для получения даты поступления из справочника используется аналогичная предыдущему заданию функция **ВПР**, данные о дате берутся из 2 столбца справочной таблицы; для вычисления текущей даты используется функция **СЕГОДНЯ** (группа **Дата и время** ), для перевода временного интервала из дней в годы – функция **ДОЛЯГОДА** (группа **Дата и время**). Результирующий вид формулы в ячейке **C3**:

**=ДОЛЯГОДА(ВПР(A3;Справочники!$A$9:$D$21;2;ЛОЖЬ);СЕГОДНЯ())**

Примечание: Если функция ДОЛЯГОДА не доступна стаж в годах можно вычислить как отношение разности между текущей датой (функция СЕГОДНЯ) и даты поступления на работу к 365 (числу дней в году).

* Скопировать ячейку **C3** на весь диапазон данных столбца «Стаж, в годах» таблицы «Сводная ведомость» (**C4:C15**).

1. Заполнить столбец «Оклад» таблицы «Сводная ведомость»:

* Примем базовую ставку равной 7000 руб., надбавку за каждый разряд – 500 руб. Тогда начисления по окладу будут рассчитываться по следующей формуле:

Оклад = 7000 + 500 \* (Разряд – 10).

* Сформировать в ячейке **D3** формулу для вычисления оклада: для получения разряда из справочника используется аналогичная предыдущему заданию функция **ВПР**, данные о разряде берутся из 3 столбца справочной таблицы. Результирующий вид формулы в ячейке **D3**:

**=7000+500\*(ВПР(A3;Справочники!$A$9:$D$21;3;ЛОЖЬ)-10)**

* Скопировать ячейку **D3** на весь диапазон данных столбца «Оклад» таблицы «Сводная ведомость» (**D4:D15**).

1. Заполнить столбец «Премия» таблицы «Сводная ведомость»:

* Сформировать в ячейке **E3** формулу для вычисления размера премии: используется функция **ЕСЛИ** (группа **Логические** ). Результирующий вид формулы в ячейке **E3**:

**=ЕСЛИ(C3>7;D3\*0,5;0)**

* Скопировать ячейку **E3** на весь диапазон данных столбца «Премия» таблицы «Сводная ведомость» (**E4:E15**).

1. Заполнить столбец «Начислено» таблицы «Сводная ведомость»: в ячейку **F3** поместить формулу **=D3+E3**, затем скопировать ячейку **F3** на весь диапазон данных столбца «Начислено» таблицы «Сводная ведомость» (**F4:F15**). Результирующий вид таблицы «Сводная ведомость» (текущая дата 29.01.2008) приведена на рис.11.
2. Перейти на лист «Отчет». В диапазоне ячеек **A1:B7** создать таблицу «Сводные данные по подразделениям». В ячейки **A2:A7** занести текст «Подразделение», «Наименование», «Руководитель», «Общая численность сотрудников», «Сумма премий», «Всего начислено».

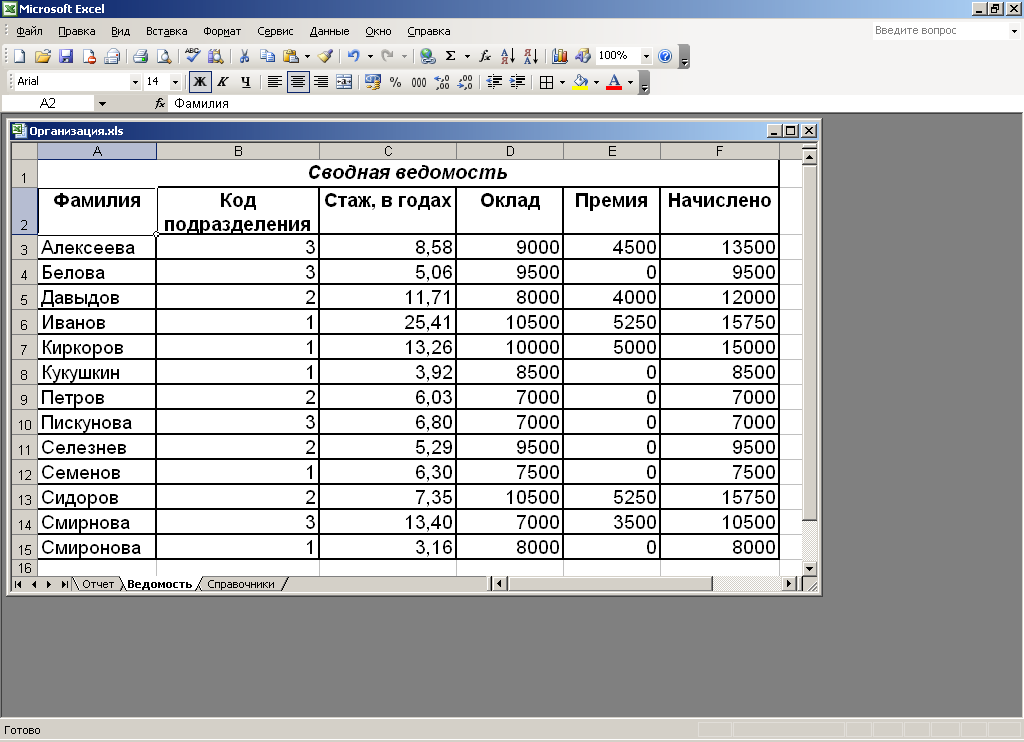


Рис.11. Данные таблицы на листе «Ведомость»

1. Ячейку **В2** для выбора кода подразделения выделить цветом (вкладка **Главная**, группа **Шрифт**, **цвет заливки** ).
2. Задать ограничения на ввод данных в ячейку **B2** – значения выбираются из списка 1;2;3 (аналогично п.5, рис.5).
3. В ячейке **B3** сформировать формулу для поиска в справочной таблице «Данные о подразделениях» наименования подразделения (функция **ВПР**):

**=ВПР(B2;Справочники!A3:C5;2;ЛОЖЬ)**

1. В ячейке **B4** сформировать формулу для поиска в справочной таблице «Данные о подразделениях» фамилии руководителя подразделения (функция **ВПР**):

**=ВПР(B2;Справочники!A3:C5;3;ЛОЖЬ)**

1. В ячейке **B5** сформировать формулу для подсчета общей численности сотрудников выбранного отдела по таблице «Сводная ведомость» (этот итог можно также подсчитать по таблице «Данные о сотрудниках») с помощью функции **СЧЕТЕСЛИ** (группа **Другие функции/Статистические**):

**=СЧЁТЕСЛИ(Ведомость!B3:B15;B2)**

1. В ячейке **B6** сформировать формулу для подсчета суммы премий сотрудников выбранного отдела по таблице «Сводная ведомость» (функция **СУММЕСЛИ**, группа **Математические **):

**=СУММЕСЛИ(Ведомость!B3:B15;B2;Ведомость!E3:E15)**

1. В ячейке **B7** сформировать формулу для подсчета суммы начислений сотрудников выбранного отдела по таблице «Сводная ведомость» (функция **СУММЕСЛИ**):

**=СУММЕСЛИ(Ведомость!B3:B15;B2;Ведомость!F3:F15)**

Результирующий вид таблицы на листе «Отчет» (текущая дата 29.01.2008) приведена на рис.12.

1. Сохранить изменения в книге ***Организация***

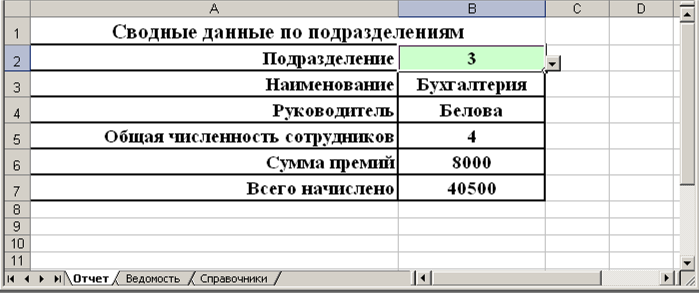


Рис.12. Данные таблицы на листе «Отчет»

**Задание 3**. Установите защиту книги таким образом, что:

* Несанкционированные пользователи не могут просматривать данные книги;
* Пользователи, знающие пароль нижнего уровня, могут просматривать только статистические (итоговые) данные о сотрудниках фирмы, исключая суммы начислений;
* Сотрудники, знающие пароль нижнего и среднего уровней, могут просматривать итоговые и частные данные о сотрудниках, за исключением сумм начислений;
* Сотрудники, знающие пароль верхнего уровня и остальные пароли, могут как просматривать, так и изменять все данные.

***Защита книги и ее элементов***

1. Придумать три пароля. Пусть пароль нижнего уровня для открытия книги – ***low***, пароль среднего уровня для изменения структуры книги – ***medium***, пароль верхнего уровня для изменения данных на листах книги – ***high***.
2. Ограничить доступ к книге «Организация», установив пароль для открытия:

* Выполнить **Файл** → **Сведения** → **Защитить документ →** **Зашифровать паролем**
* В окне команды *Шифрование документа* ввести пароль ***low*** и нажать **ОК**. В появившемся окне *Подтверждение пароля* ввести пароль ***low*** еще раз и нажать **ОК**.
* Сохранить книгу. Закрыть ее и открыть заново, введя при открытии пароль ***low***.

1. На листе «Ведомость» скрыть столбцы с данными о начислениях («Оклад», «Премия», «Начислено»):

* Перейти на лист «Ведомость». Выделить столбцы **D**, **E**, **F**, щелкнув мышью на заголовках столбцов при удерживаемой клавише SHIFT.
* Выполнить команду **Скрыть** из контекстного меню (для вызова контекстного меню щелкнуть правой клавишей мыши в области выделения).

1. Защитить от изменений лист «Ведомость»:

* Находясь на листе «Ведомость», выполнить команду **Защитить лист**  на вкладке **Рецензирование**,
* В окне команды ввести пароль ***high***, установить разрешения для защищенного листа: *выделение заблокированных ячеек, выделение незаблокированных ячеек* (установлены по умолчанию), нажать **ОК**, ввести пароль ***high*** еще раз в окне подтверждения пароля, нажать **ОК**.
* Проверить действие установленной защиты листа «Ведомость»: выделить столбцы **С** и **G**, смежные со скрытыми столбцами, и проверить, что невозможно отобразить скрытые столбцы (команда **Отобразить** в контекстном меню недоступна), невозможно внесение изменений в ячейки листа.

1. Перейти на лист «Справочники». Защитить лист «Справочники» с паролем ***high***.
2. Скрыть лист «Справочники»: щелкнуть правой кнопкой мыши на ярлыке листа «Справочники» и выполнить команду **Скрыть** из контекстного меню.
3. Скрыть лист «Ведомость».
4. Защитить структуру книги «Организация»:

* На вкладке **Рецензирование** выбрать группу **Защитить книгу**  и выполнить команду **Защита структуры и окон**. В окне команды установить флажок *структуру* и ввести пароль ***medium***, нажать **ОК**. Ввести пароль ***medium*** еще раз в окне подтверждения и нажать **ОК**.
* Проверить действие защиты. Убедиться, что невозможно отобразить скрытые листы, невозможно удалить лист «Отчет» (в контекстном меню листа «Отчет» команды **Отобразить**, **Удалить** недоступны), нельзя добавить в книгу новый лист.

1. На листе «Отчет» сделать доступным выбор кода подразделения в ячейке **B2** даже после установки защиты. Для этого:

* Выделить ячейку **B2**, в контекстном меню или на вкладке **Главная** в группе **Ячейки/Формат** выполнить команду **Формат ячеек**,
* В окне команды *Формат ячеек* перейти на вкладку *Защита*, снять флажок параметра *Защищаемая ячейка* и нажать **ОК**.

1. Скрыть текст формул на листе «Отчет». Для этого:

* Выделить диапазон ячеек **B3:B7**, содержащие формулы, выполнить команду **Формат ячеек**,
* В окне команды *Формат ячеек* перейти на вкладку *Защита*, установить флажок параметра *Скрыть формулы* и нажать кнопку **ОК**. (Скрытие формул начнет действовать только после установки защиты листа).

1. На листе «Отчет» скрыть строки, содержащие данные о суммах премий и общих начислений: выделить любые две ячейки в строках с номерами **6** и **7**. На вкладке **Главная** в группе **Ячейки/Формат** выбрать группу **Видимость/Скрыть или отобразить** и выполнить команду **Скрыть строки**.
2. Установить защиту листа «Отчет» с паролем ***high***, оставив в окне команды лишь флажки, установленные по умолчанию (выделение заблокированных и незаблоки­рованных ячеек).
3. Проверить возможность внесения изменений в ячейку **B2** и отсутствие такой возможности для остальных ячеек листа «Отчет». Проверить невозможность отображения скрытых строк на листе «Отчет» (команда **Отобразить строки** на вкладке **Главная** в группе **Ячейки/Формат/Видимость/ Скрыть или отобразить** не доступна).
4. Сохранить изменения в книге «Отчет», закрыть книгу.

**Задание 4**. Создате открытую копию книги, для которой снять установленную ранее защиту от просмотра и редактирования книги и всех ее элементов.

***Снятие защиты книги и ее элементов***

1. Открыть книгу отчет с паролем **low**.
2. Сохранить защищенную книгу «Организация» под новым именем, например, «Организация\_защита\_снята» (Файл → **Сохранить как**).
3. Снять пароль на открытие для книги «Организация\_защита\_снята». В окне команды **Сохранить как** нажать кнопку **Сервис,** перейти на вкладку *Общие параметры* и удалить пароль в строке *Пароль на открытие*. Нажать **ОК**, сохранить изменения книги.
4. Проверить, что пароль удален: закрыть и вновь открыть книгу «Организация\_защита\_снята» – при открытии книги не требуется введение пароля.
5. Отобразить скрытые листы:

* В группе **Рецензирование** выполнить команду **Защитить книгу/Защита структуры и окон**. В окне *Снять защиту книги* ввести пароль ***medium***, нажать **ОК**.
* Щелкнуть правой кнопкой мыши на ярлычке листа «Отчет» и выполнить команду **Отобразить** в контекстном меню, в окне команды выбрать лист «Ведомость», нажать **ОК**.
* Щелкнуть правой кнопкой мыши на ярлычке любого из видимых листов и выполнить команду **Отобразить** в контекстном меню, в окне команды выбрать лист «Справочники», нажать **ОК**.

1. Сделать лист «Справочники» доступным для редактирования, сняв защиту листа:

* Перейти на лист «Справочники», на вкладке **Рецензирование** выполнить команду **Снять защиту листа **, в окне команды ввести пароль ***high***.
* Проверить, что на листе «Справочники» можно вносить изменения.

1. Сделать лист «Ведомость» доступным для редактирования, отобразить скрытые данные о начислениях:

* Перейти на лист «Ведомость» и выполнить команду **Снять защиту листа**, ввести пароль ***high***.
* Выделить любой диапазон ячеек в столбцах, смежных со срытыми (например, в столбцах **C** и **G**), а затем на вкладке **Главная** в группе **Ячейки/Формат/Видимость/Скрыть или отобразить** выполнить команду **Отобразить столбцы**.

1. Сделать лист «Отчет» доступным для редактирования, отобразить скрытые данные о начислениях:

* Перейти на лист «Отчет» и выполнить команду **Снять защиту листа**, ввести пароль ***high***.
* Выделить заголовки строк, смежных со срытыми (строки **5** и **8**), а затем выполнить команду **Отобразить** из контекстного меню выделения.
* Проверить, что в ячейки листа «Отчет» можно вносить изменения.

1. Сохранить изменения книги «Организация\_защита\_снята».
2. Показать книги «Организация» и «Организация\_защита\_снята» преподавателю.

**Контрольные вопросы:**

1. Чем различается действие защиты от изменения содержимого ячеек листа, установленной с помощью команды **Защитить лист**) и защиты в режиме «только для чтения» (установка на файл книги пароля для изменения)?
2. Чем различается разблокирование на защищенном листе ячеек (диапазонов ячеек) с помощью команды **Формат ячеек** (вкладка *Защита*)и с помощью команды **Разрешить изменение диапазонов**.
3. Для чего служит команда **Защитить книгу**. Какую команду следует применить, если стоит задача защитить от изменения ячейки всех листов книги?