**Федеральное государственное бюджетное образовательное учреждение высшего образования  
Национальный исследовательский университет «МЭИ»**

**Отчет к лабораторной работе №2**

**Дисциплины «Защита данных»**

**Изучение программных средств защиты от несанкционированного доступа**

**и разграничения прав пользователей**

**Выполнил студент группы А-13а-20**

**Алибеков А.А.**

**Преподаватель: Хорев П.Б.**

**Москва 2023**

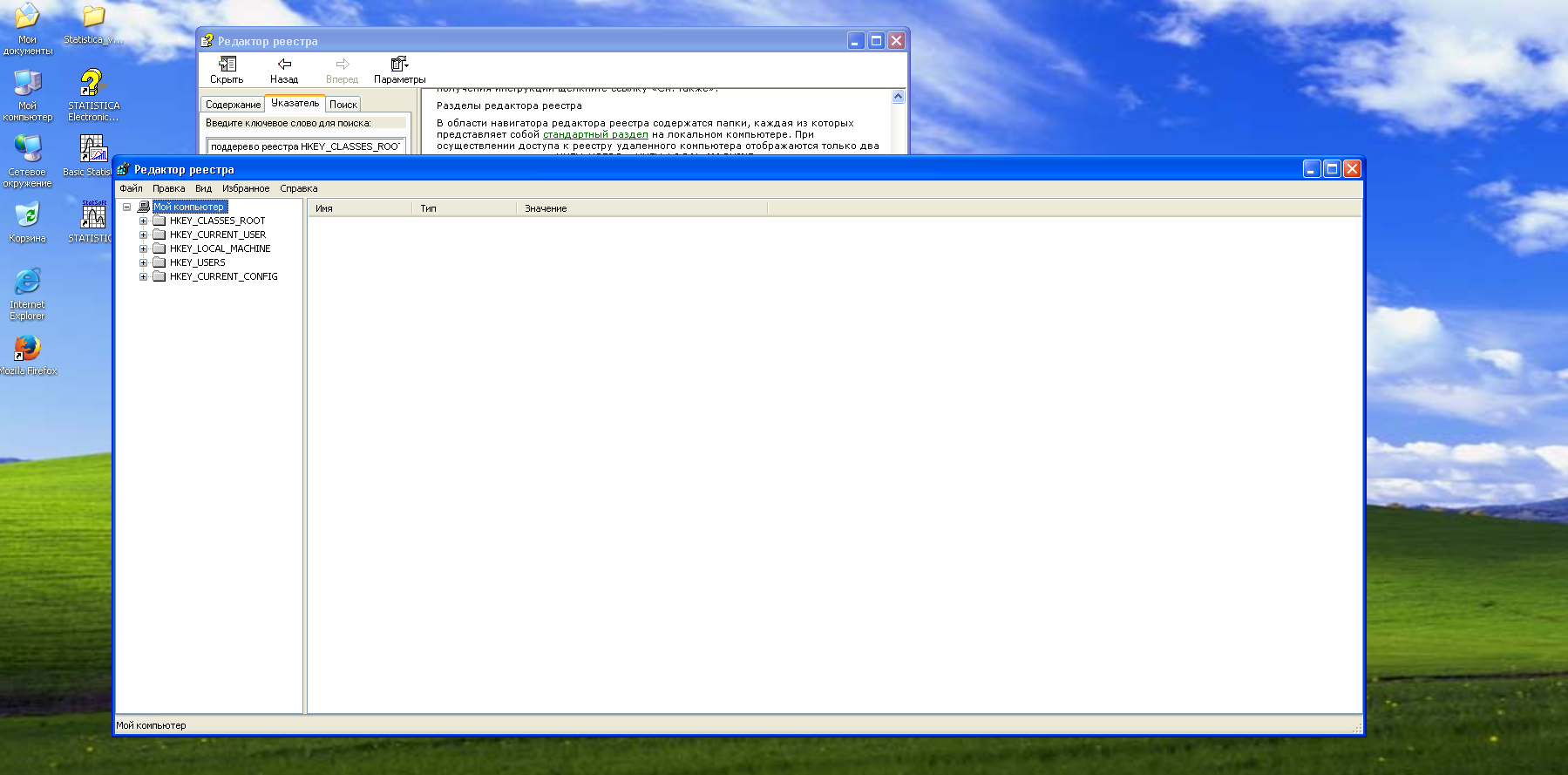
# Этот пункт выполняется в виртуальной машине Windows XP (если работа выполняется в компьютерном классе кафедры) или с правами администратора (если работа выполняется на домашнем компьютере). Запустить программу Редактор реестра Windows regedit.exe. Ознакомиться со структурой реестра.

## Включить в отчет, воспользовавшись, например, Справкой редактора реестра, краткие сведения о содержании основных разделов реестра (HKEY\_CURRENT\_USER и HKEY\_LOCAL\_MACHINE).

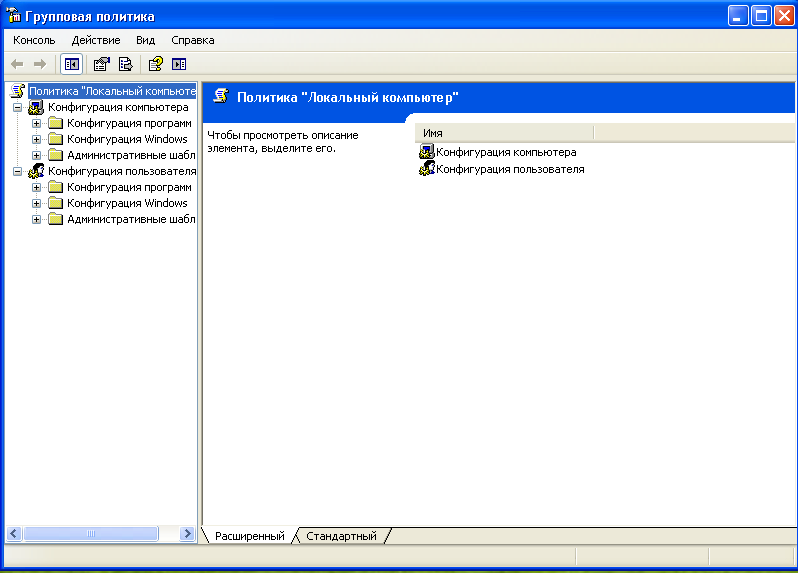
## 



## Включить в электронную версию отчета копии экранных форм, иллюстрирующих использование редактора реестра (рисунок с изображением активной формы помещается в буфер обмена с помощью комбинации клавиш Alt+Print Screen).



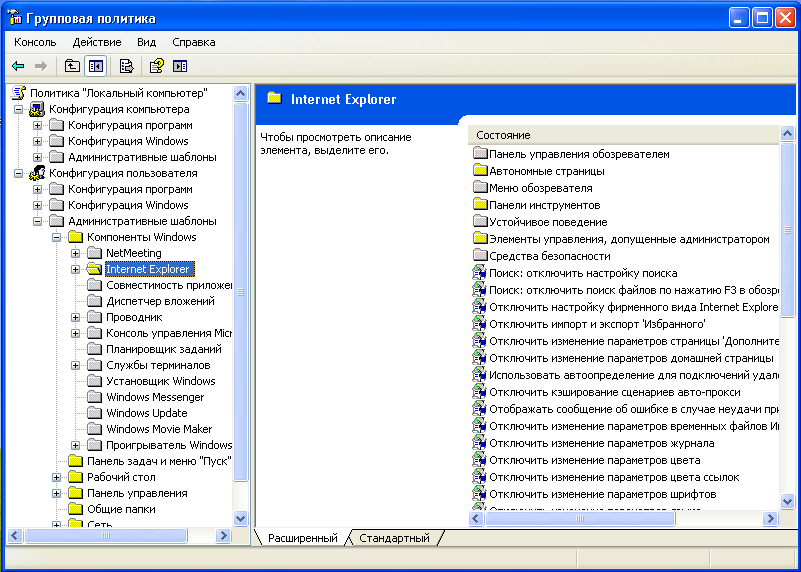
# Пункт выполняются в виртуальной машине Windows XP или с правами администратора. Запустить программу Редактор локальной групповой политики gpedit.msc, позволяющую ограничить возможности пользователей ОС Windows.

****

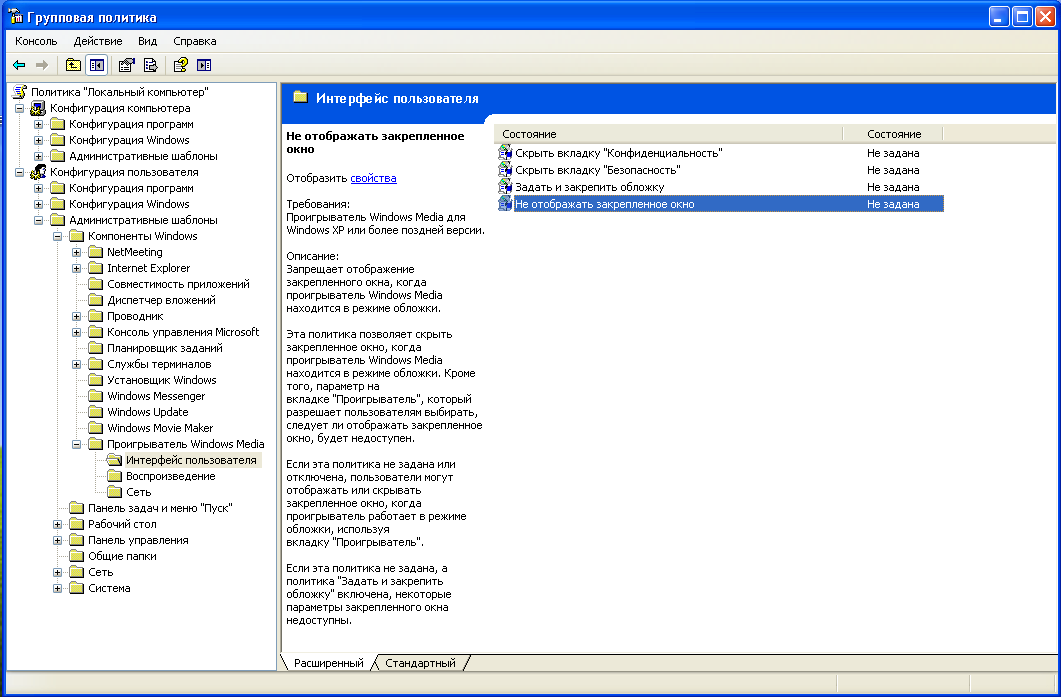
## Включить в отчет сведения о назначении и основных функциях программы.

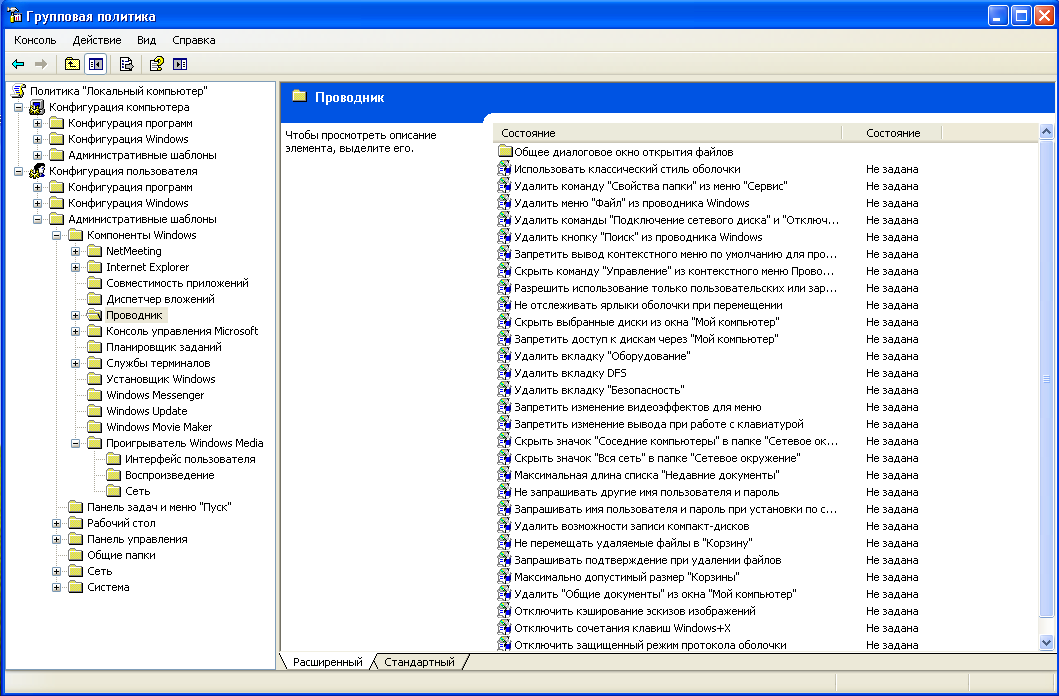
Редактор локальной групповой политики — встроенный инструмент операционной системы Windows, предназначенный для управления групповой политикой компьютеров, не входящих в домен. С помощью этого средства можно настроить работу большого количества параметров операционной системы: включение или отключение функций Windows, запрет запуска определенных программ, применение ограничений для пользователей и т. д.

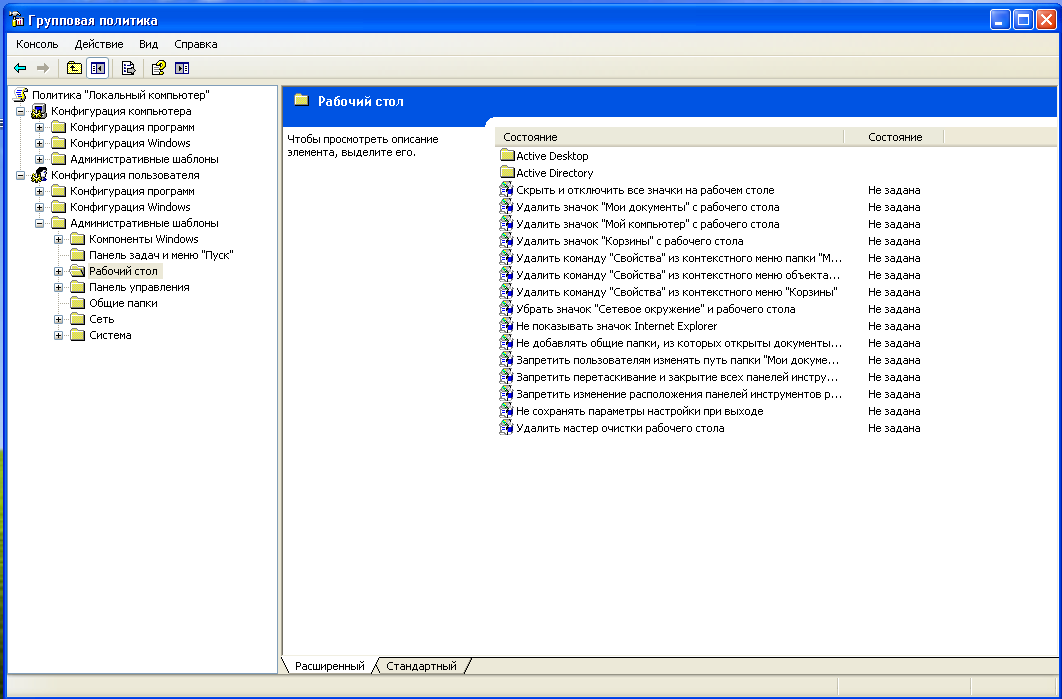
## Освоить управление настройками обозревателя Internet Explorer для пользователя (узел Политика «Локальный компьютер» | Конфигурация пользователя | Административные шаблоны | Компоненты Windows | Internet Explorer).



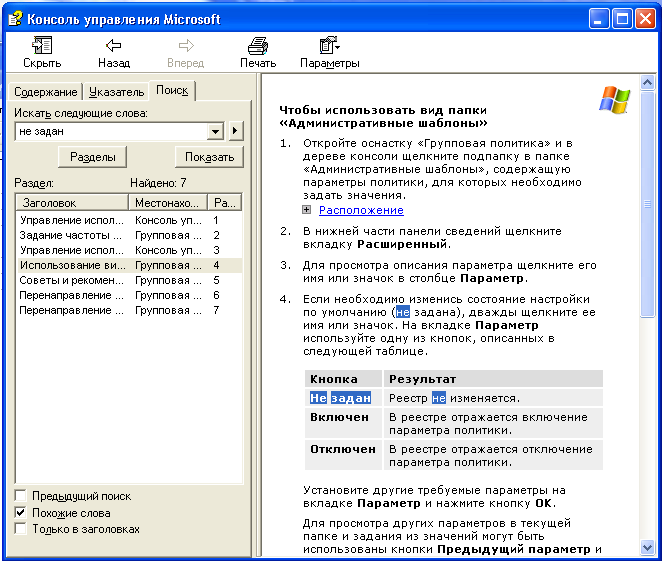
## Освоить установку ограничений возможностей пользователя (узлы группы Политика «Локальный компьютер» | Конфигурация пользователя | Административные шаблоны) по изменению структуры Рабочего стола и Главного меню, использованию функций Панели управления и компонент Windows (Проводника, консоли управления Microsoft, планировщика задач, проигрывателя Windows Media и др.), работе с локальной сетью, использованию общих папок, использованию различных системных функций.



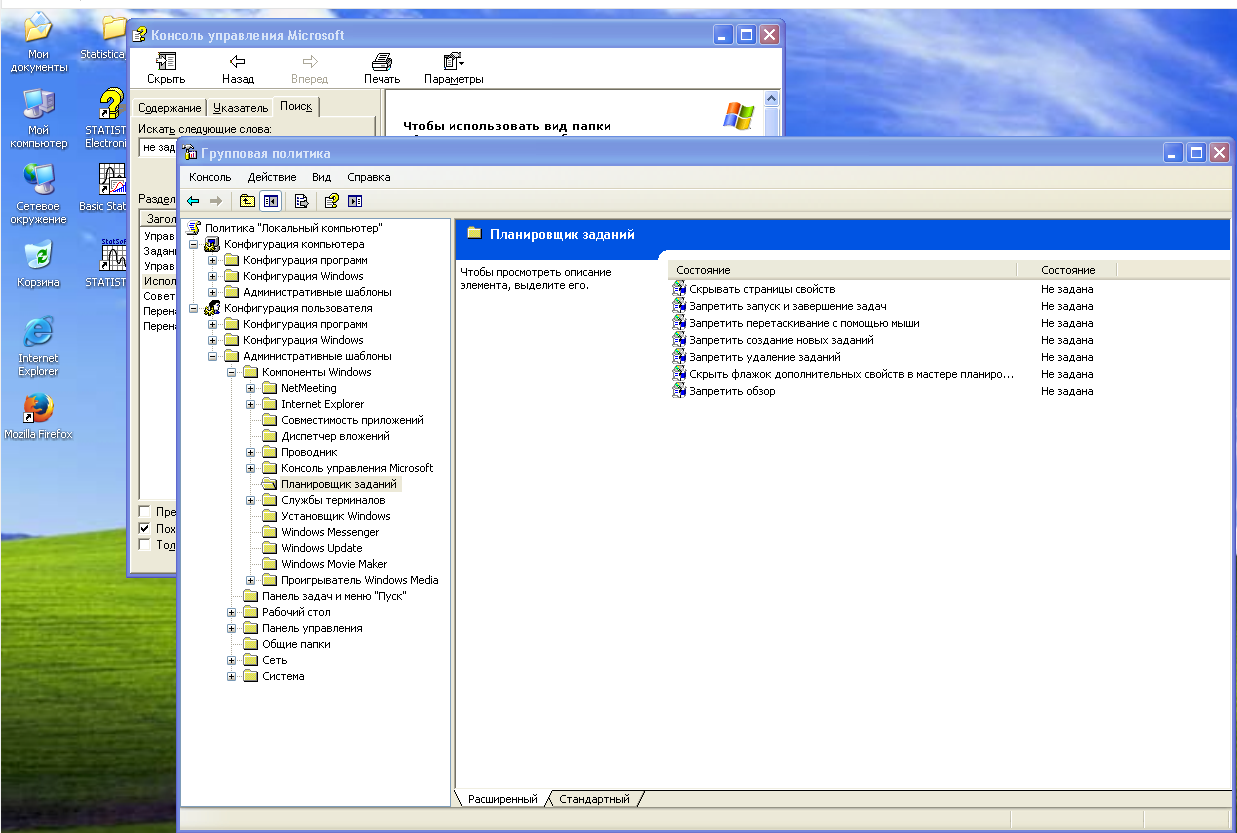




## Включить в отчет, воспользовавшись, например, Справкой Редактора локальной групповой политики, ответ на вопрос, чем отличаются значения параметров «отключен» и «не задан».



## Включить в электронную версию отчета копии экранных форм, используемых при работе с программой gpedit.msc. Завершить работу с программой gpedit.msc.



# Пункт выполняется на компьютере с профессиональной версией Windows. С помощью процесса входа Winlogon, активизируемого комбинацией клавиш Ctrl+Alt+Del, заблокировать работу с используемой рабочей станцией на период временного отсутствия пользователя (если эта возможность не запрещена администратором). Разблокировать работу рабочей станции.

## Включить в отчет сведения о порядке защиты рабочей станции на период временного отсутствия пользователя и о других функциях Процесса входа, доступных при этом наряду с блокировкой.

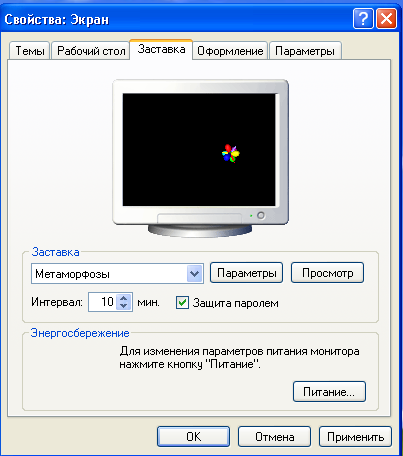
На сочетание клавиш Ctrl+Alt+Del открывается диспетчер задач.

Доступны функции:

1. Lock (Заблокировать)
2. Switch user (Сменить пользователя)
3. Sign out (Выйти)
4. Change a password (Изменить пароль)
5. Task Manager (Диспетчер задач)

Ещё можно использовать Win+L(блокировка компьютера). Либо использовать блокировку по истечению времени бездействия.

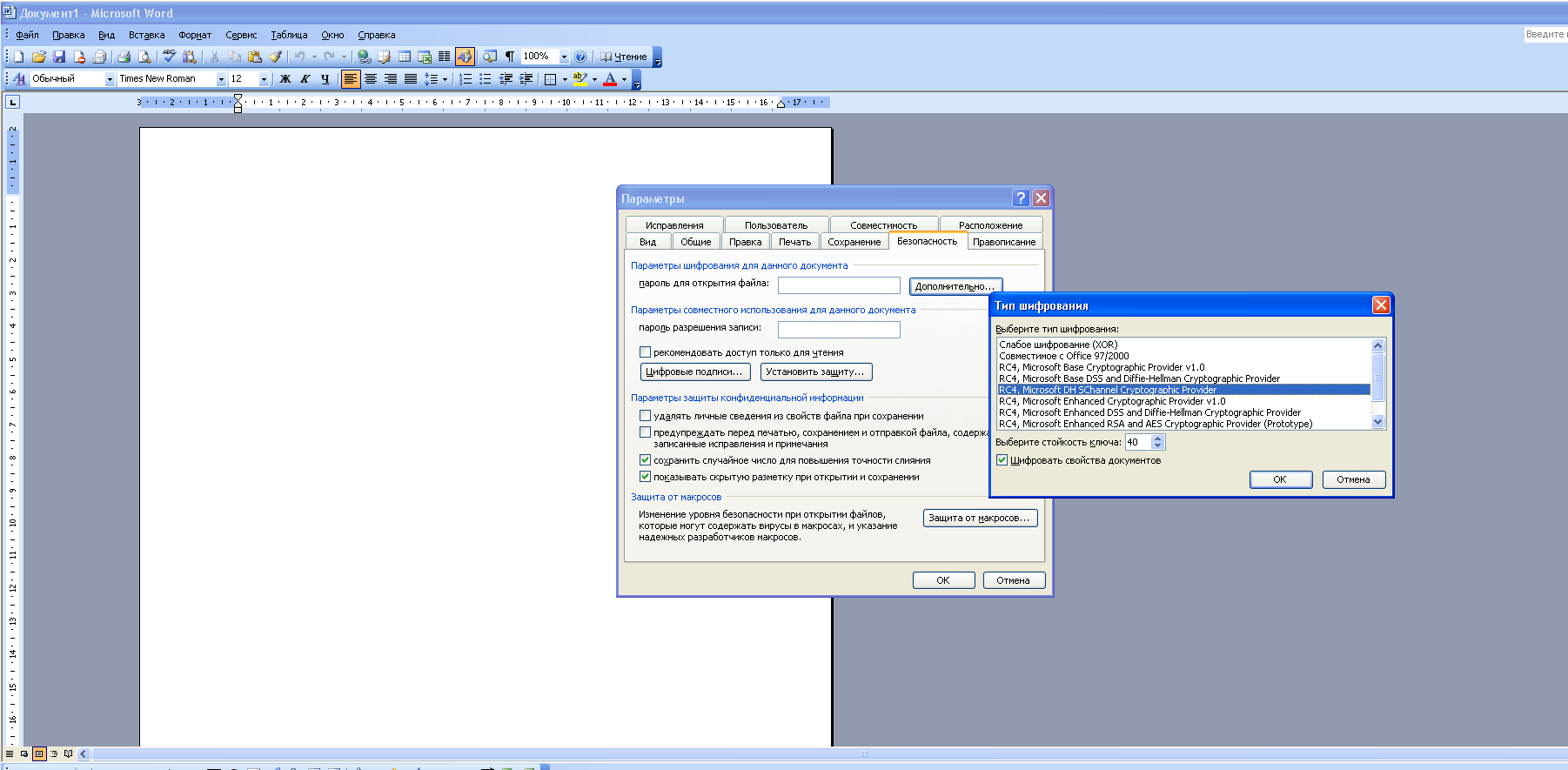
## С помощью функции Заставка в окне свойств или персонализации экрана, вызываемого из его контекстного меню, ознакомиться с другой возможностью блокировки компьютера на период временного отсутствия пользователя. Отразить полученные сведения в отчете. Включить в электронную версию отчета копии экранных форм, полученных при выполнении этого пункта.

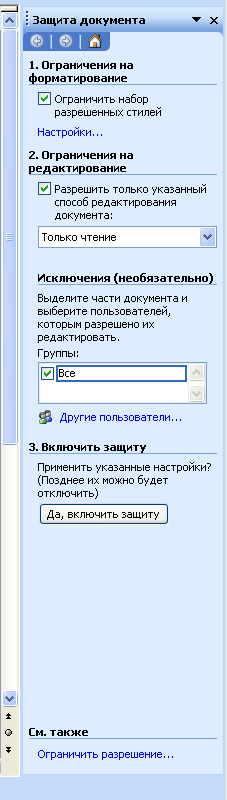


# Открыть (или создать) произвольный документ в текстовом процессоре Word.

## Изучить порядок использования паролей для защиты документов в Microsoft Word от чтения и записи (два разных типа паролей) и включить в отчет соответствующие сведения (в Office 2013 использовать команду Файл | Сведения | Защита документа, в Office 2010 использовать команду Файл | Сведения | Защитить документ, в Office 2007 – Кнопка Microsoft Office | Подготовить и Рецензирование | Защитить документ, в Office 2003 – Сервис | Параметры | Безопасность).

Пароли вводятся с учетом регистра и могут содержать не более 15 знаков.  
Также можно выбрать тип шифрования и стойкость ключа.





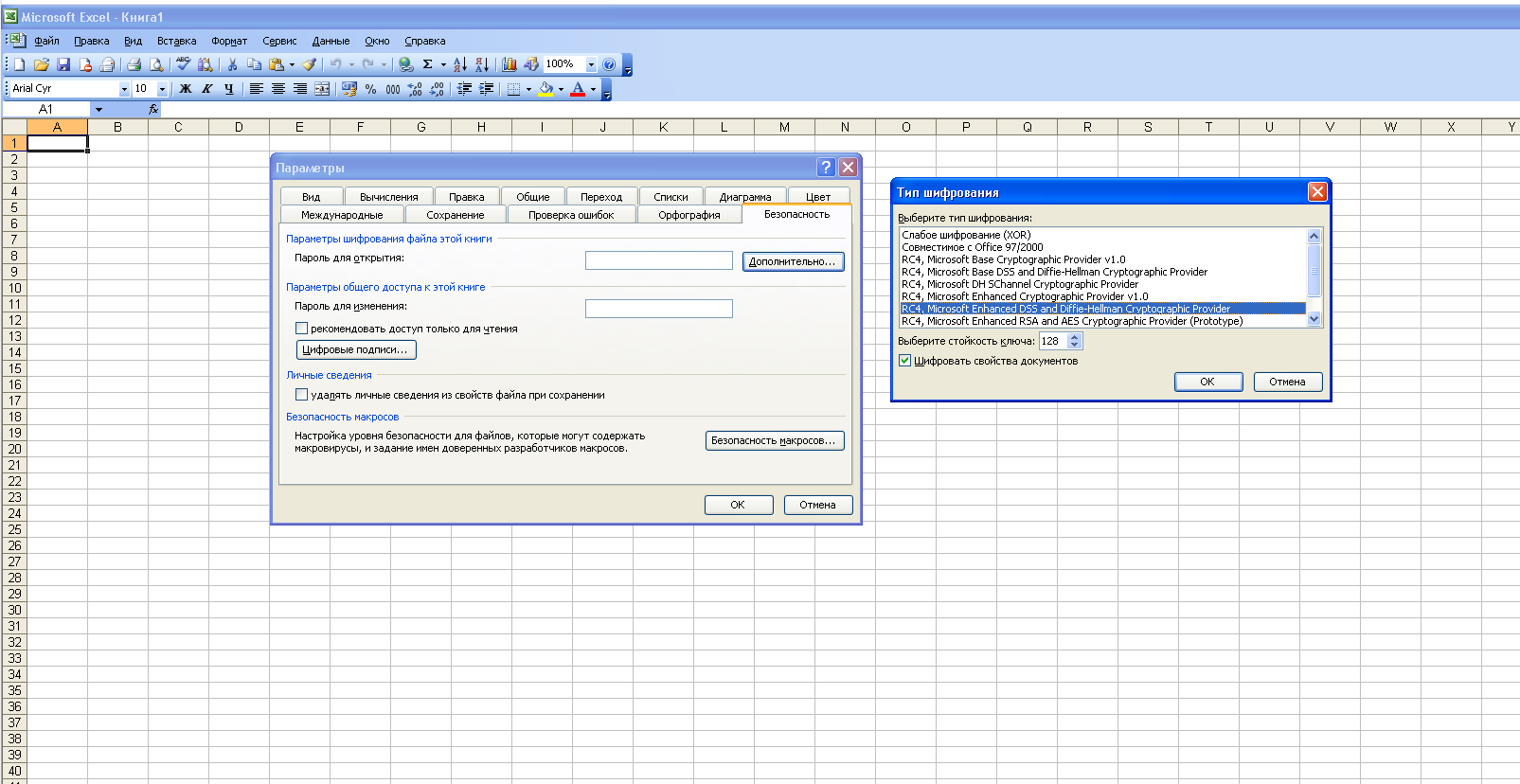
## Включить в электронную версию отчета копии экранных форм, использованных при выполнении данного пункта. Завершить работу с Word.

См. предыдущий пункт.

# Открыть (или создать) произвольную таблицу Excel.

## Изучить порядок использования паролей для защиты документов или их частей в табличном процессоре Microsoft Excel от чтения и записи и включить в отчет соответствующие сведения.

Пароли вводятся с учетом регистра и могут содержать не более 15 знаков.  
Также можно выбрать тип шифрования и стойкость ключа.



## Включить в электронную версию отчета копии экранных форм, использованных при выполнении данного пункта. Завершить работу с Excel.

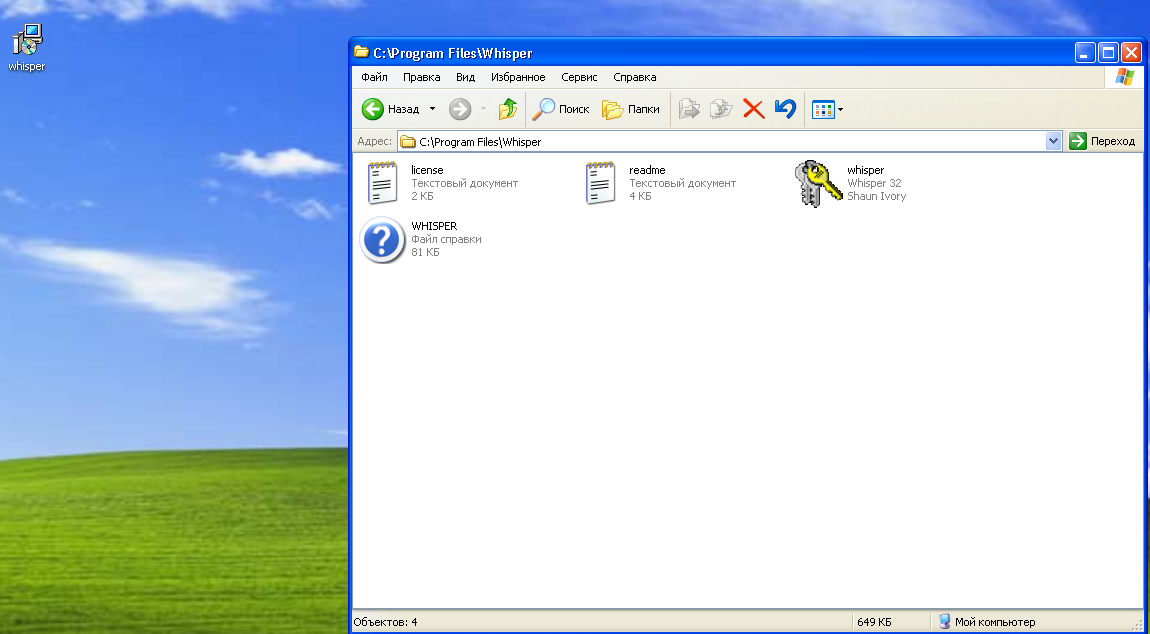
См. предыдущий пункт.

# Пункты 6-8 выполняются в виртуальной машине Windows XP или с правами администратора. Скопировать в личную папку на локальном жестком диске файл whisper.msi.

Сделано.

# Если программа Whisper 32 не установлена (соответствующий пункт отсутствует в главном меню), то установить ее с помощью файла whisper.msi.

Программа успешно установлена.



# Запустить программу whisper.exe, предназначенную для создания и ведения базы данных паролей пользователя.

## Изучить назначение и основные функции программы и включить в отчет соответствующие сведения.

Whisper 32 - программа, предназначенная для создания и ведения базы данных паролей пользователя. Хранит все имена пользователей и пароли в одном защищенном паролем файле. Вы можете распечатать список или скопировать его в буфер обмена.

Есть возможность программного генерирования паролей. В форме генератора паролей нужно указать используемые символы и длину пароля. Также есть возможность указания срока действия пароля. По истечении этого периода программа выдаст сообщение об изменения пароля. Данная возможность обеспечивает дополнительную безопасность от несанкционированного доступа к личному кабинету на сайтах. В свойствах программы можно настроить автоматическое резервное копирование списка.

## Создать 2-3 записи о паролях к различным ресурсам (записи обязательно должны содержать фамилию и инициалы студента в полях имени учетной записи или комментария).

## 

## 

## Включить в электронную версию отчета копии экранных форм, использованных при выполнении данного пункта. Завершить работу с программой whisper.exe

См. предыдущий пункт.

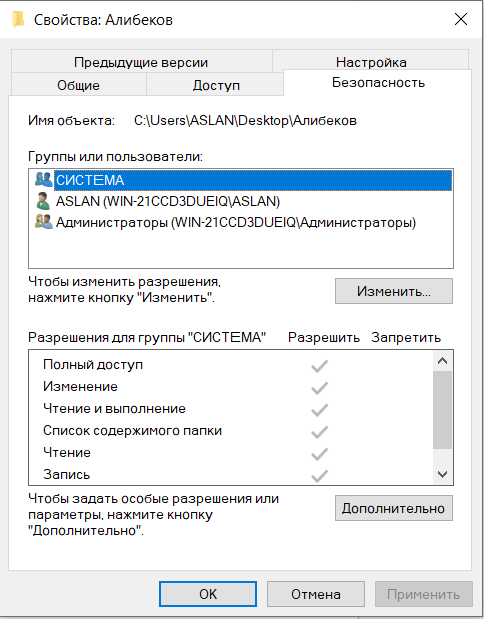
# Ознакомиться (на примере папок c: \ Пользователи \ Имя пользователя \ Мои документы \ Папка с фамилией студента и c: \ Пользователи \ Общие \ Общие документы или, при работе в Windows XP Professional, c:\ Documents and Settings \ Имя пользователя \ Документы \ Папка с фамилией студента и c:\ Documents and Settings \ All Users \ Документы) с порядком разграничения доступа к ресурсам в операционной системе Windows (с помощью команды Свойства | Безопасность контекстного меню объекта и элементов управления соответствующих диалоговых окон). Если команда Безопасность недоступна (при работе в ОС Windows XP Professional), то выключить режим «Использовать простой общий доступ к файлам» на вкладке «Вид» окна свойств папки.

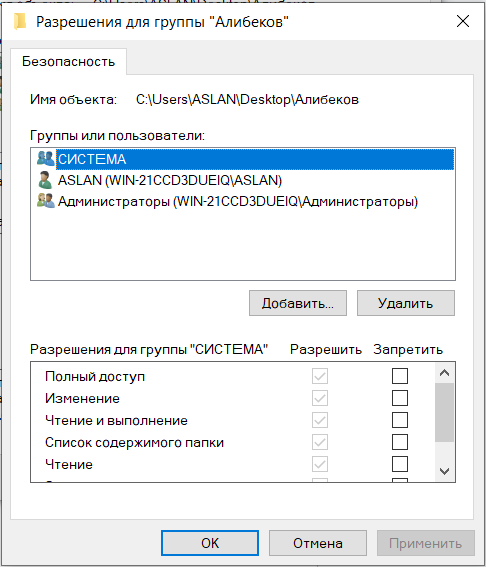
## Включить в отчет сведения об особенностях управления доступом к папкам и файлам (родовых (generic, общих) правах доступа, полном наборе специальных и стандартных прав доступа, владельце объекта, действующих разрешениях на доступ к объекту для конкретного субъекта). Для выполнения этого задания обязательно открыть все вкладки окна дополнительных параметров безопасности папки.

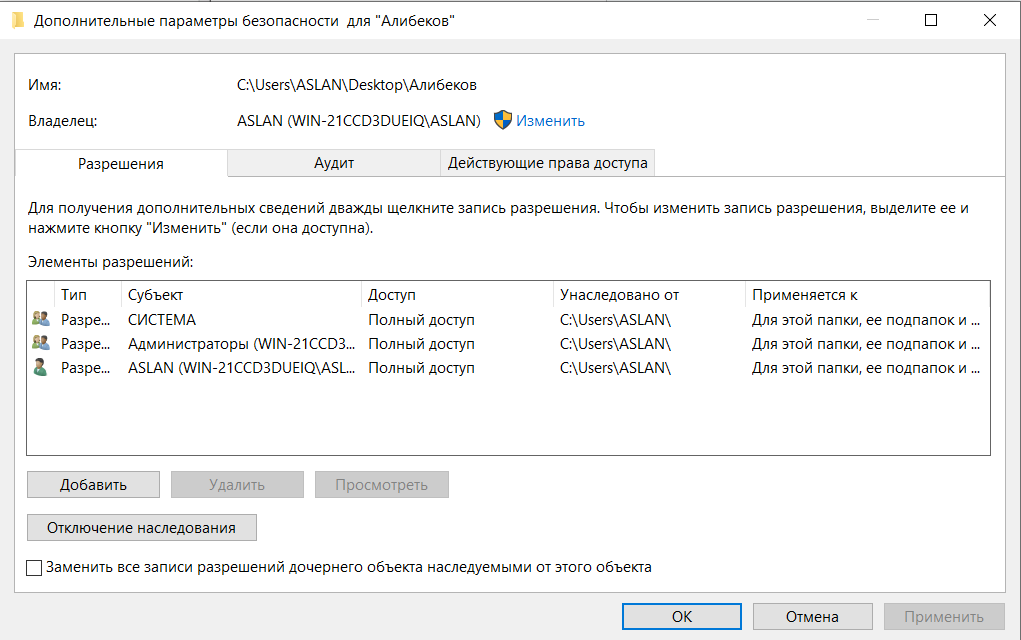
Управление доступом заключается в предоставлении пользователям, группам и компьютерам определенных прав на доступ к объектам по сети или на компьютере.

На вкладке «Безопасность» можно изменить разрешения для файла.

1. Владение объектами:   
   При создании объекта ему назначается владелец. По умолчанию владельцем объекта назначается тот, кто его создал. Какие бы разрешения ни были установлены для объекта, владелец объекта всегда может изменить эти разрешения.
2. Наследование разрешений:  
   Механизм наследования облегчает администраторам задачи назначения разрешений и управления ими. Благодаря этому механизму разрешения, установленные для контейнера, автоматически распространяются на все объекты этого контейнера.
3. Права и привилегии пользователей:  
   Права пользователей позволяют пользователям и группам в компьютерной среде пользоваться особыми привилегиями и правами на вход в систему. Администраторы могут назначать права учетным записям групп или отдельных пользователей. Эти права позволяют пользователям выполнять конкретные действия, такие как интерактивный вход в систему или архивирование файлов и каталогов.
4. Аудит объектов:  
   Обладая правами администратора, можно контролировать успешные и неудавшиеся попытки доступов пользователей к объектам.







## Включить в электронную версию отчета копии экранных форм, использованных при выполнении данного пункта.

См. предыдущий пункт.

# Ознакомиться с порядком разграничения доступа к принтерам (с помощью Панели управления Windows | Устройства и принтеры | Свойства принтера).

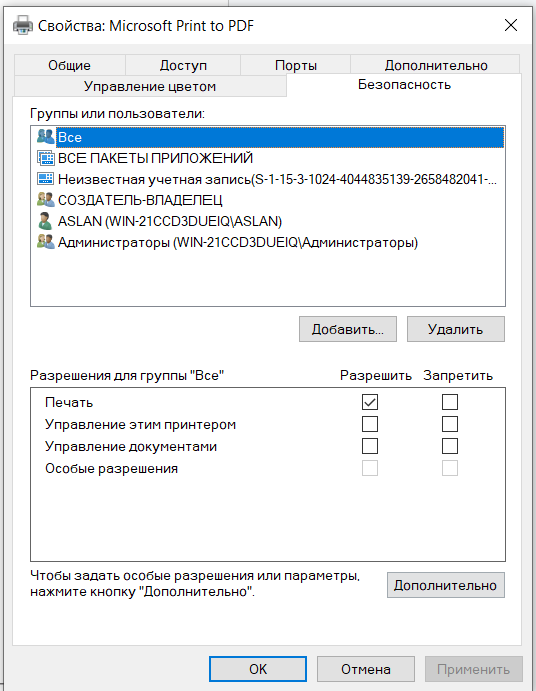
## Включить в отчет сведения об особенностях управления доступом к принтерам (родовых правах доступа, полном наборе специальных и стандартных прав доступа, владельце объекта, действующих разрешениях на доступ к объекту для конкретного субъекта). Для выполнения этого задания обязательно открыть все вкладки окна дополнительных параметров безопасности объекта.

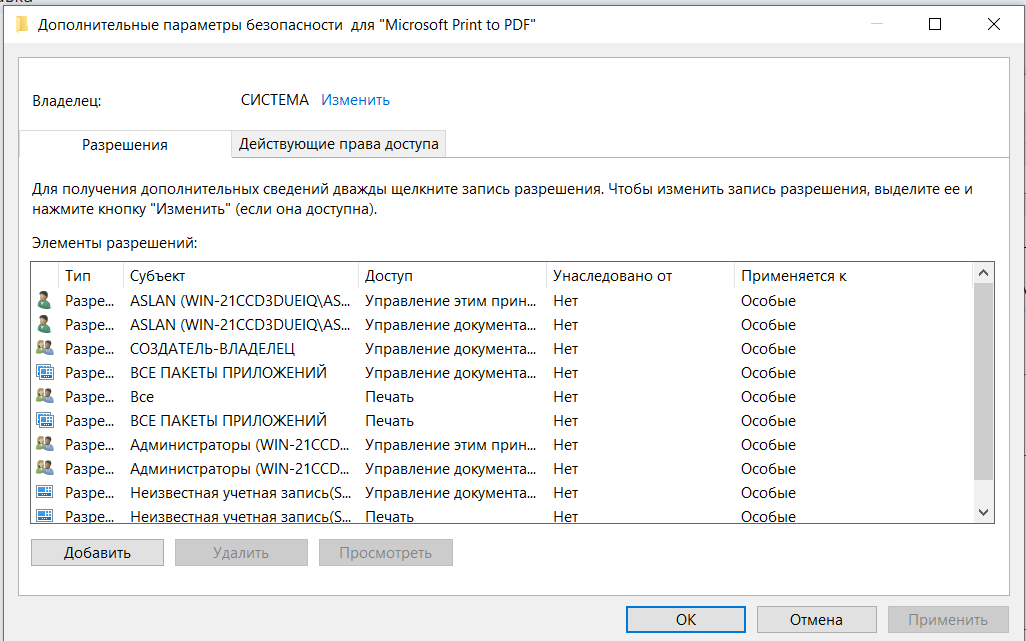
По умолчанию все пользователи могут посылать задания на печать на принтер. Часто требуется выполнить настройку, обеспечивающую возможность вывода на печать на указанные принтеры только для заданных групп. У каждого принтера существует три основных разрешения печати.

1. Печать - позволяет пользователю или группе посылать задания на принтер.

1. Управление принтерами - позволяет пользователю или группе изменять свойства принтера, включая разрешения печати.

1. Управление документами - пользователи или группы, обладающие этим разрешением, могут приостанавливать, перезапускать или удалять любые документы в очереди принтера, независимо от их принадлежности. По умолчанию пользователи обладают разрешением «Управление документами» по отношению к собственным заданиям печати.





## Включить в электронную версию отчета копии экранных форм, использованных при выполнении данного пункта.

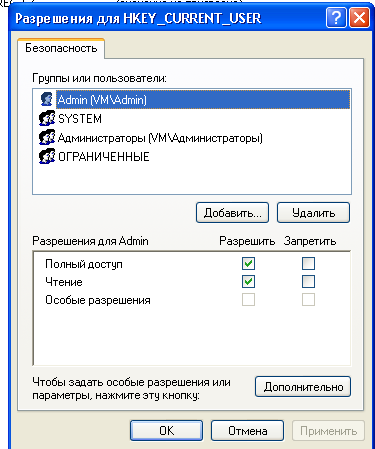
См. предыдущий пункт.

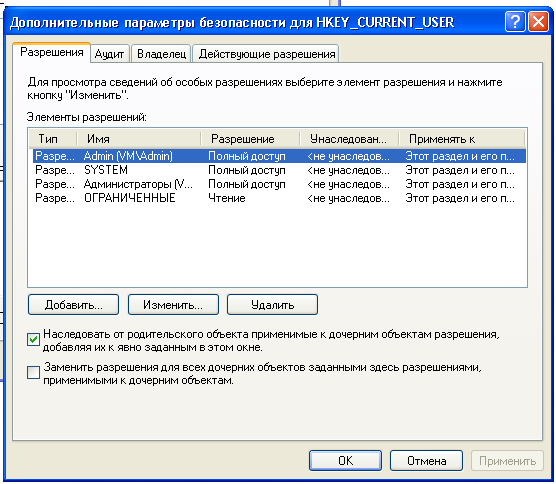
# Ознакомиться с порядком разграничения доступа к разделам реестра (с помощью команды меню редактора реестра Правка | Разрешения, пункт выполняется в виртуальной машине Windows XP или с правами администратора).

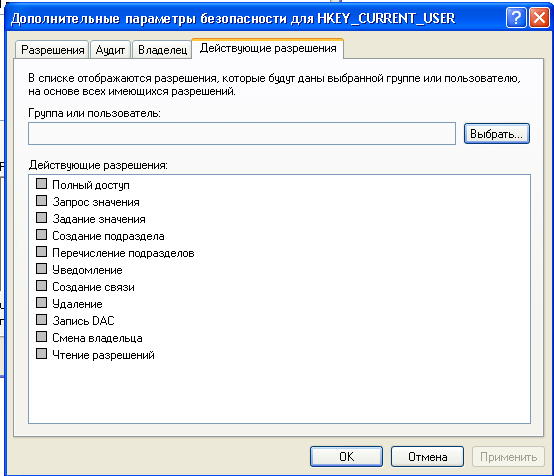
## Включить в отчет сведения об особенностях управления доступом к разделам реестра (родовых правах доступа, полном наборе специальных и стандартных прав доступа, владельце объекта, действующих разрешениях на доступ к объекту для конкретного субъекта). Для выполнения этого задания обязательно открыть все вкладки окна дополнительных параметров безопасности объекта.

Права доступа, которые можно установить:

|  |  |
| --- | --- |
| **Тип доступа** | **Описание** |
| Чтение (Read) | Позволяет пользователям, внесенным в список, просматривать содержимое раздела реестра, не позволяя сохранять изменения |
| Полный доступ (Full Control) | Позволяет пользователям, внесенным в список, получать доступ к разделу, редактировать его содержимое и изменять к нему уровень прав доступа |







## Включить в электронную версию отчета копии экранных форм, использованных при выполнении данного пункта.

См. предыдущий пункт.

# Пункты 12-15 выполняются в виртуальной машине Windows XP или с правами администратора. Ознакомиться (с помощью функции Панели управления Администрирование | Управление компьютером – административная оснастка compmgmt.msc, узел Локальные пользователи и группы) с порядком создания и изменения учетных записей пользователей и групп в защищенных версиях операционной системы Windows.

## Включить в отчет соответствующие сведения.

Оснастка “**Локальные пользователи и группы**” предназначена для создания новых пользователей и групп, управления учетными записями, задания и сброса паролей пользователей.

***Локальный пользователь*** – это учетная запись, которой могут быть предоставлены определенные разрешения и права на вашем компьютере. Учетная запись всегда имеет свое имя и пароль (пароль может быть пустым).

Узел **Пользователи** оснастки “Локальные пользователи и группы” отображает список учетных записей пользователей: встроенные учетные записи (например, “Администратор” и “Гость”), а также созданные вами учетные записи реальных пользователей ПК.

Встроенные учетные записи пользователей создаются автоматически при установке Windows и не могут быть удалены. При создании нового пользователя вы должны будете присвоить ему имя и пароль, а также определить, в какую группу будет входить новый пользователь. Каждый пользователь может входить в одну или несколько групп.

В узле **Группы** отображаются как встроенные группы, так и созданные администратором. Встроенные группы создаются автоматически при установке Windows.

Для добавления новой учетной записи раскройте оснастку “Локальные пользователи и группы” – выделите папку “Пользователи” – затем в правом окне щелкните на пустом месте правой кнопкой мыши – выберите пункт “Новый пользователь”:

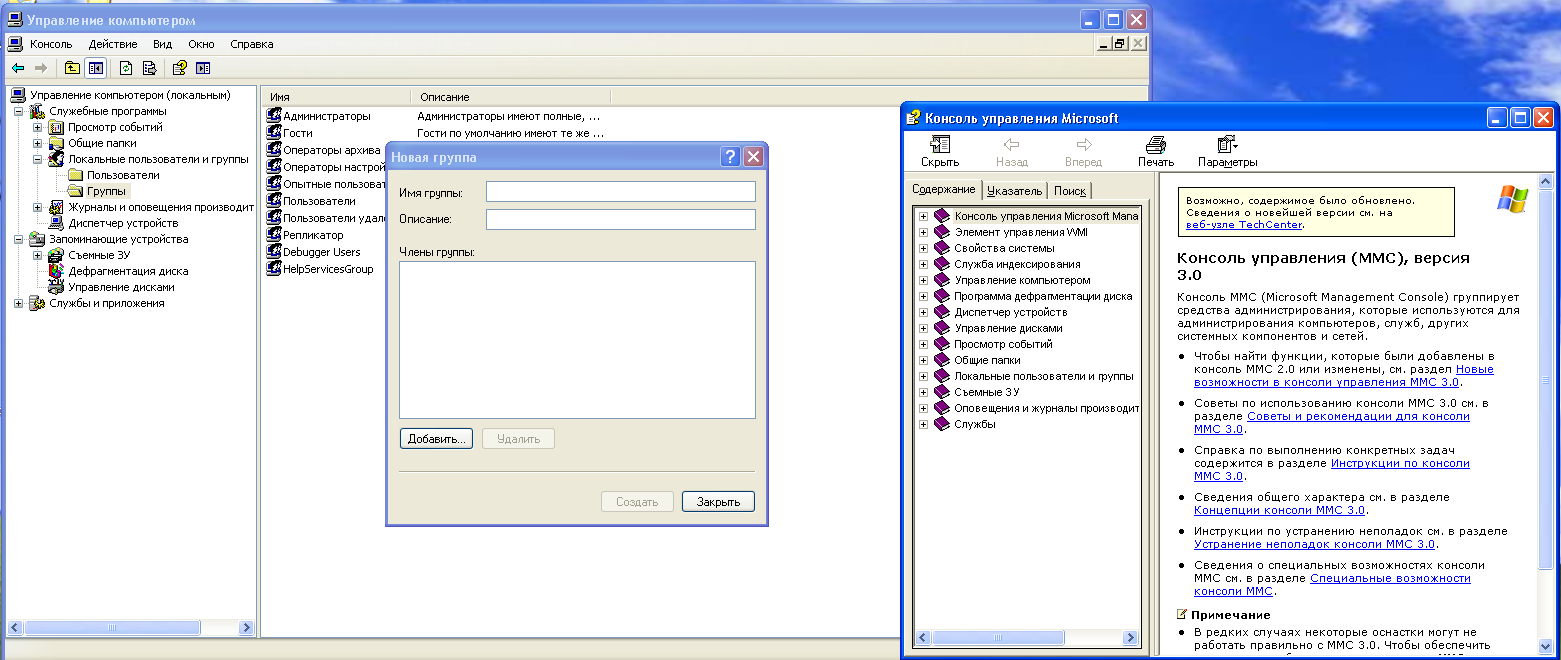
В появившемся окне задайте имя пользователя и описание. Также задайте для пользователя.  
Затем настройте дополнительные параметры – поставьте или снимите флажки напротив нужных пунктов.

После нажатия кнопки “Создать” в списке пользователей появится новая учетная запись. Щелкните по ней дважды мышкой и в открывшемся окне перейдите на вкладку “Членство в группах”. Здесь нажмите кнопку “Добавить” – “Дополнительно” – “Поиск”. Затем выберите группу, в которую должен входить пользователь (рекомендуется группа “Пользователи” или “Опытные пользователи”) и нажмите “ОК” во всех отобразившихся окнах. После этого здесь же во вкладке “Членство в группах” удалите из списка все группы, кроме той, которую только что выбрали. Нажмите “ОК”:

Если учетная запись пользователя больше не нужна, ее можно удалить. Но во избежание различного рода проблем учетные записи пользователей перед удалением рекомендуется сначала отключить.

Группа создается аналогично.

## Включить в электронную версию отчета копии соответствующих экранных форм.



# Ознакомиться (с помощью функции Панели управления Администрирование | Локальная политика безопасности | Локальные политики | Назначение прав пользователя – административная оснастка secpol.msc, узел Локальные политики | Назначение прав пользователя) с порядком назначения прав пользователям и группам.

## Включить в отчет соответствующие сведения.

**Назначение прав пользователя**  - Это меню позволяет настраивать разрешение или же запрет на выполнение тех или иных действий пользователям данного компьютера.

Перечислим основные параметры:

* Запретить вход в систему через службы удаленных рабочих столов

Этот параметр безопасности определяет, каким пользователям и группам будет запрещено входить в систему как клиенту служб удаленных рабочих столов.

* Запретить локальный вход

Этот параметр безопасности определяет, каким пользователям будет отказано во входе в систему. Этот параметр политики заменяет параметр "Разрешить локальный вход в систему", если к учетной записи применяются обе политики.

Если этот параметр безопасности применяется к группе "Все", никто не сможет войти в систему локально.

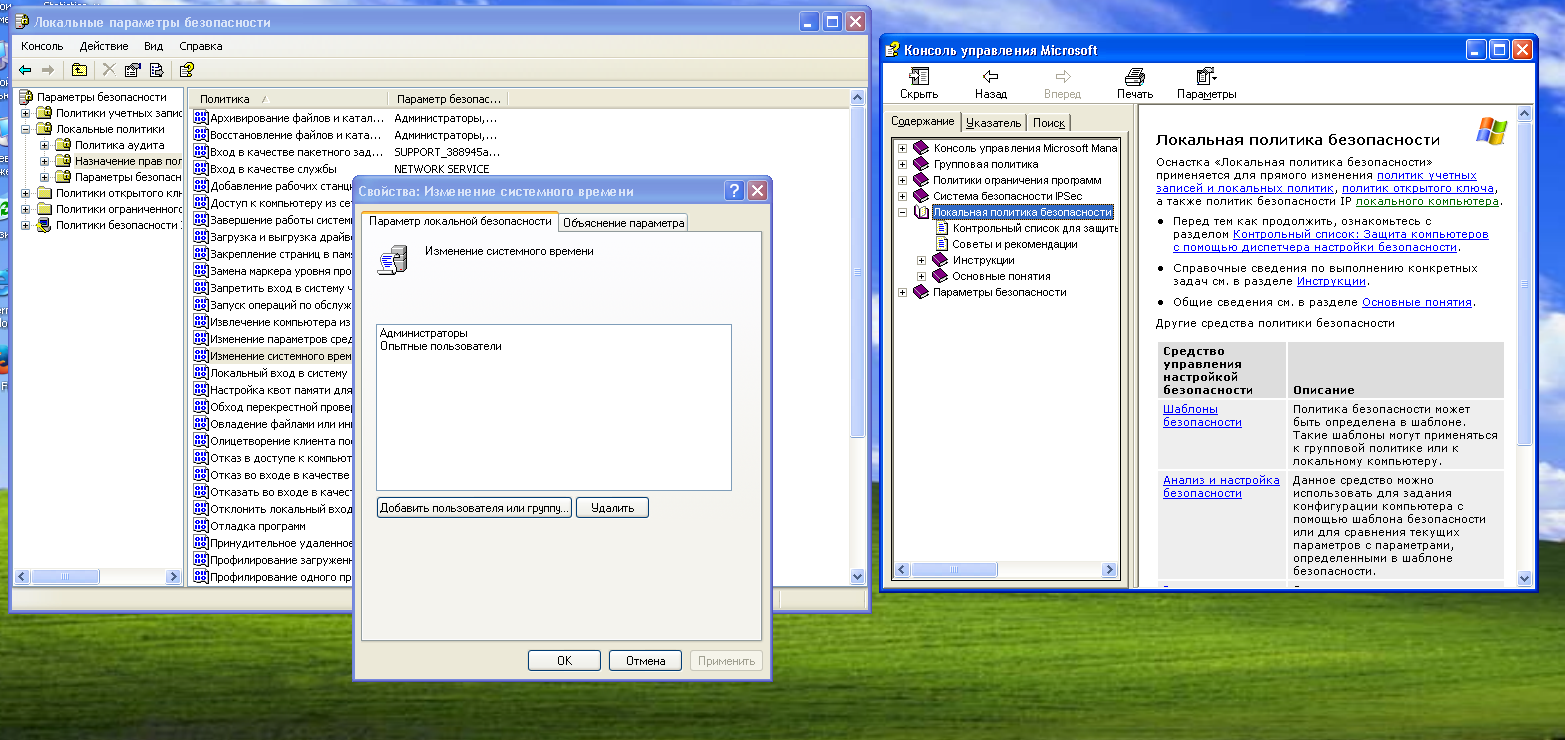
* Отказать в доступе к этому компьютеру из сети

Этот параметр безопасности определяет, каким пользователям будет отказано в доступе к компьютеру из сети. Этот параметр заменяет параметр политики "Разрешить доступ к компьютеру из сети", если к учетной записи пользователя применяются об политики.

* Разрешать вход в систему через службы удаленных рабочих столов

Этот параметр безопасности определяет, какие пользователи или группы имеют право входа в систему в качестве клиента служб удаленных рабочих столов

## Включить в электронную версию отчета копии соответствующих экранных форм.



# Ознакомиться (с помощью функции Панели управления Администрирование | Локальная политика безопасности | Политики учетных записей | Политика паролей – административная оснастка secpol.msc, узел Политики учетных записей | Политика паролей) с порядком определения параметров безопасности для парольной аутентификации.

## Включить в отчет соответствующие сведения.

Максимальный срок действия пароля

Этот параметр безопасности определяет период времени (в днях), в течение которого пароль можно использовать, пока система не потребует от пользователя сменить пароль. Срок действия пароля может составлять от 1 до 999 дней; значение 0 соответствует неограниченному сроку действия пароля. Если значение максимального срока действия пароля составляет от 1 до 999 дней, то значение минимального срока действия пароля должно быть меньше максимального. Если значение максимального срока действия пароля равно 0, то значением минимального срока действия пароля может быть любое количество дней от 0 до 998.

Минимальная длина пароля

Этот параметр безопасности определяет минимальное количество символов, которое должно содержаться в пароле пользователя. Можно установить значение от 1 до 14, либо 0, если пароль не требуется.

Минимальный срок действия пароля

Этот параметр безопасности определяет период времени (в днях), в течение которого пользователь должен использовать пароль перед тем, как сможет сменить его. Можно установить значение от 1 до 998 дней либо разрешить изменять пароль сразу, установив значение 0 дней.

Пароль должен отвечать требованиям сложности

Этот параметр безопасности определяет требования сложности для паролей.

Если эта политика включена, пароли должны удовлетворять следующим минимальным требованиям:

- Пароль не должен содержать имя учетной записи пользователя или фрагменты имени пользователя длиной больше двух символов.

- Пароль должен состоять не менее чем из шести символов.

- Пароль должен содержать символы, относящиеся к трем из следующих четырех категорий:

- латинские заглавные буквы (A - Z);

- латинские строчные буквы (a - z);

- цифры (0 - 9);

- отличные от букв и цифр символы (например, !, $, #, %).

Проверка соблюдения этих требований выполняется при изменении или создании паролей.

Требовать неповторяемости паролей

Этот параметр безопасности определяет количество новых паролей, которые необходимо связать с учетной записью пользователя перед повторным использованием старого пароля. Значение должно быть в диапазоне от 0 до 24.

Эта политика позволяет администраторам повысить уровень безопасности, предотвращая постоянное использование старых паролей.

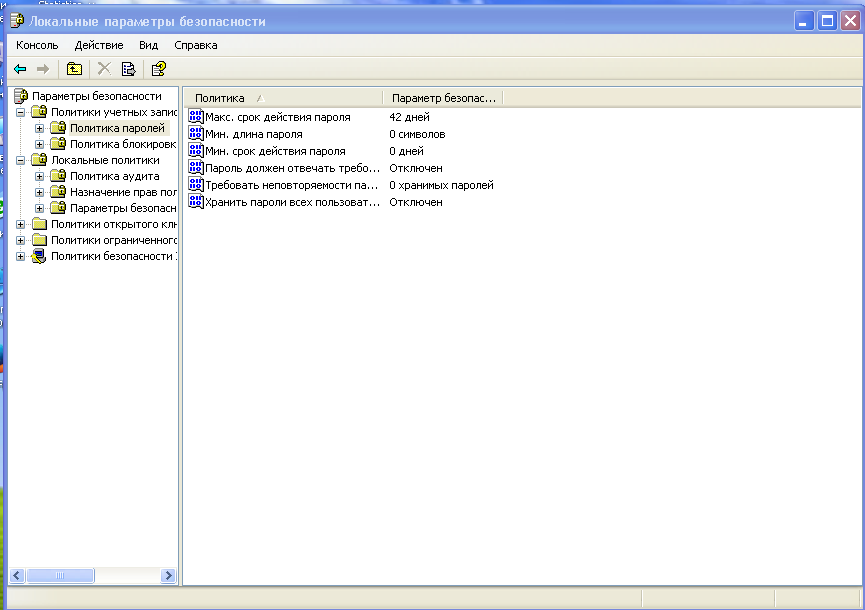
Хранить пароли, используя обратимое шифрование

Этот параметр безопасности определяет, используется ли в операционной системе обратимое шифрование для хранения паролей.

Эта политика обеспечивает поддержку приложений, использующих протоколы, которым для проверки подлинности необходимо знать пароль пользователя. Хранение паролей, зашифрованных обратимыми методами, аналогично хранению их в текстовом виде. Поэтому данную политику следует использовать лишь в исключительных случаях, если потребности приложения оказываются важнее, чем защита пароля.

Эта политика является обязательной при использовании протокола проверки подлинности CHAP (Challenge-Handshake Authentication Protocol) в средствах удаленного доступа или службах IAS (Internet Authentication Services). Она также необходима при использовании краткой проверки подлинности в службах IIS (Internet Information Services).

## Включить в электронную версию отчета копии соответствующих экранных форм.



# Ознакомиться (с помощью функции Панели управления Администрирование | Локальная политика безопасности | Политики учетных записей | Политика блокировки учетных записей – административная оснастка secpol.msc, узел Политики учетных записей | Политика блокировки учетных записей) с порядком определения параметров безопасности для политики блокировки учетных записей.

## Включить в отчет соответствующие сведения.

**Блокировка учетной записи** на

Блокировка учетной записи на

Этот параметр безопасности определяет число минут, в течение которых учетная запись остается заблокированной, прежде чем будет автоматически разблокирована. Этот параметр может принимать значения от 0 до 99 999 минут. Если для длительности блокировки учетной записи установлено значение 0, она останется заблокированной до тех пор, пока не будет явно разблокирована администратором.

Если определено пороговое значение блокировки, данный интервал блокировки должен быть больше или равен интервалу сброса.

Пороговое значение блокировки

Этот параметр безопасности определяет количество неудачных попыток входа в систему, приводящее к блокировке учетной записи пользователя. Заблокированная учетная запись не может использоваться до тех пор, пока не будет восстановлена администратором, либо пока не истечет период блокировки этой учетной записи. Количество неудачных попыток входа в систему может составлять от 0 до 999. Если установить это значение равным 0, то учетная запись никогда не будет разблокирована.

Неудачные попытки ввода паролей на рабочих станциях или рядовых серверах, заблокированных с помощью сочетания клавиш CTRL+ALT+DEL или с помощью защищенных паролем заставок, считаются неудачными попытками входа в систему.

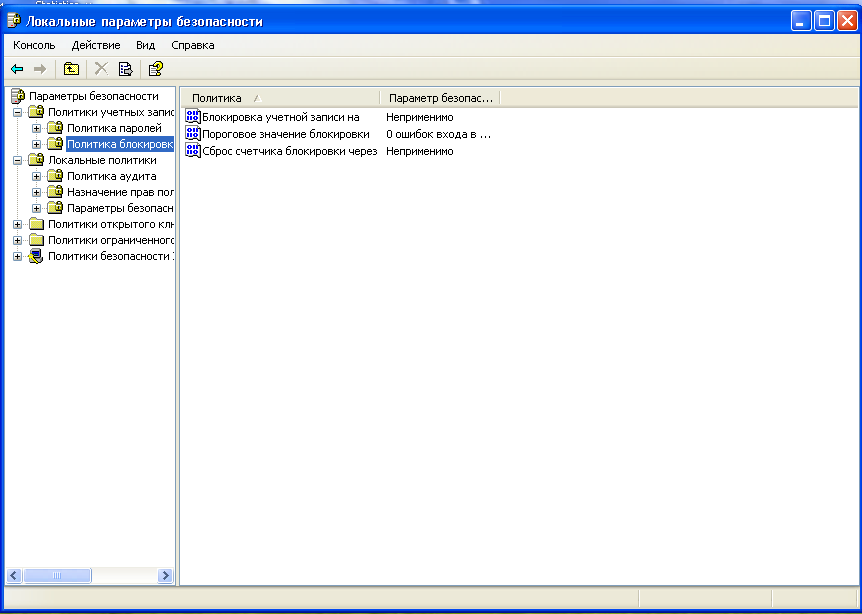
Сброс счетчика блокировки через

Этот параметр безопасности определяет, сколько минут должно пройти после неудачной попытки входа в систему, прежде чем счетчик неудачных попыток будет сброшен в 0. Этот параметр может принимать значения от 1 до 99 999 минут.

Если определено пороговое значение блокировки, данный интервал сброса не должен быть больше интервала "Блокировка учетной записи на".

По умолчанию: "Отсутствует", поскольку данный параметр имеет смысл только при заданном параметре "Пороговое значение блокировки".

## Включить в электронную версию отчета копии соответствующих экранных форм.



# Включить в отчет титульный лист и сохранить файл с электронной версией отчета.

# Предъявить преподавателю электронную версию отчета о лабораторной работе с копиями использовавшихся экранных форм и соответствующими им номерами пунктов задания.

# После проверки электронной версии отчета преподавателем удалить программу Whisper 32 с помощью Панели управления Windows.

# 

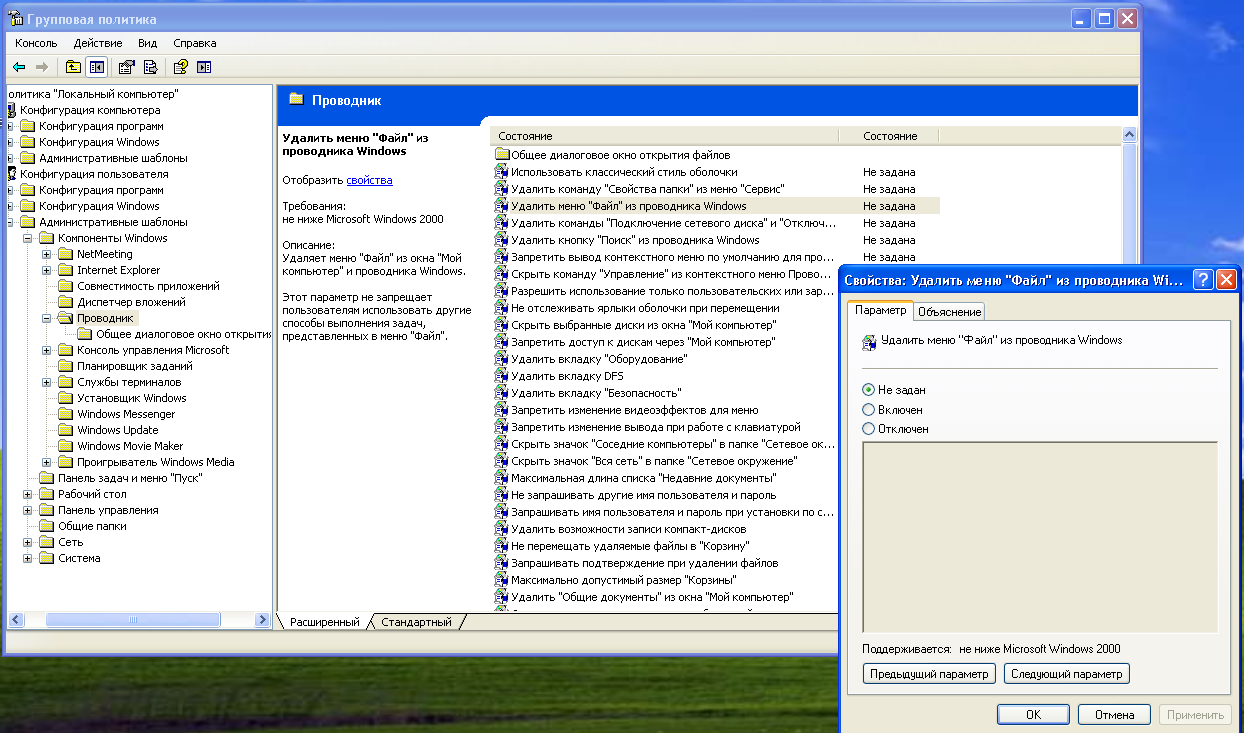
# Включить в отчет ответы на контрольные вопросы, номера которых выбираются в соответствии с номером варианта и прилагаемой ниже таблицей.

# Предъявить преподавателю для защиты лабораторной работы отчет на твердом носителе, содержащий

# Контрольные вопросы:

|  |  |
| --- | --- |
| № | Номера вопросов |
| 23 | 3, 11, 13, 18, 36, 38 |

1. **Как удалить меню Файл из меню Проводника с помощью редактора групповой политики?**

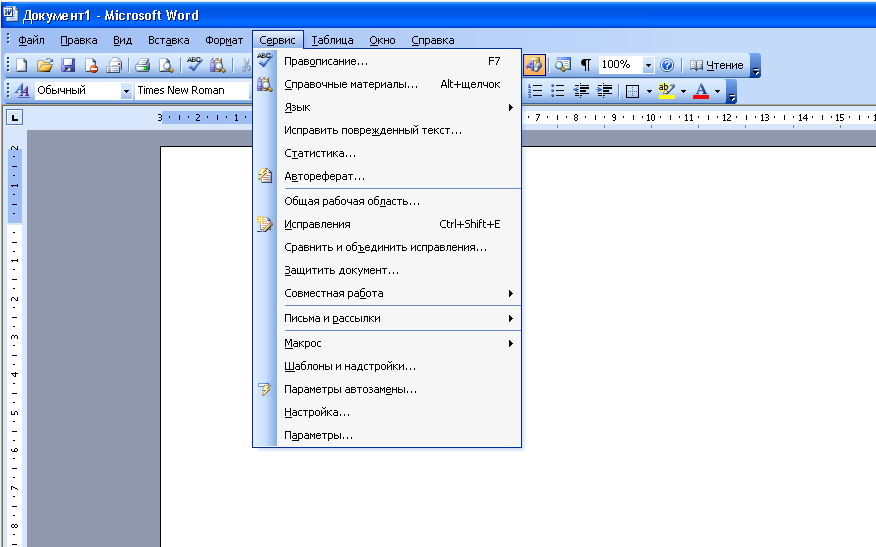
****

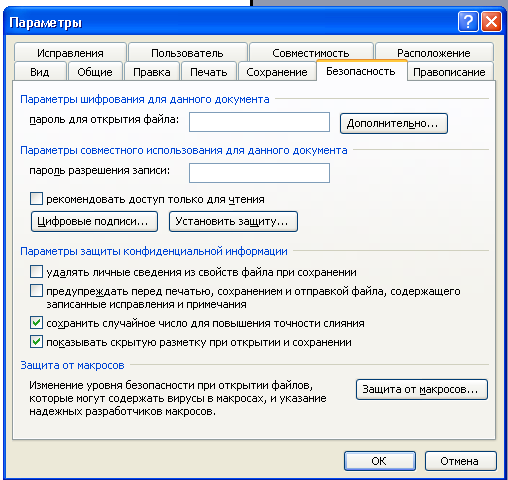
1. **Как изменяется документ Microsoft Office после установки защиты от чтения с помощью паролей?**

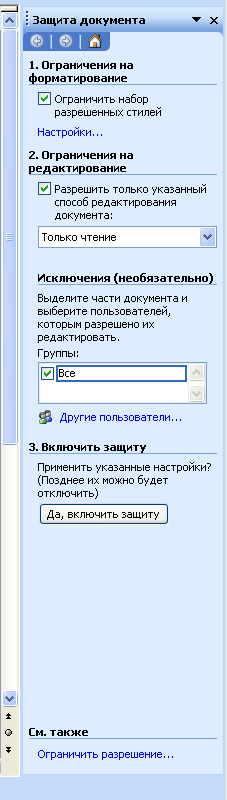
**Требуется пароль для открытия:** После установки защиты от чтения с паролем, документ становится зашифрованным. При попытке открыть такой документ в Microsoft Office приложении (например, Word, Excel или PowerPoint), система запросит у вас пароль. Если вы не введете правильный пароль, вы не сможете открыть и просмотреть содержимое документа.

**Ограничен доступ без пароля:** Без правильного пароля пользователи не смогут просматривать, редактировать, копировать или печатать содержимое документа. Это обеспечивает защиту конфиденциальности информации, которая содержится в документе.

1. **Как устанавливается защита от изменения документов Microsoft Word и таблиц Microsoft Excel?**

****

****

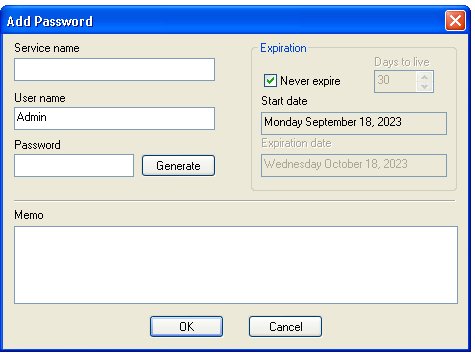


Аналогично для Microsoft Excel.

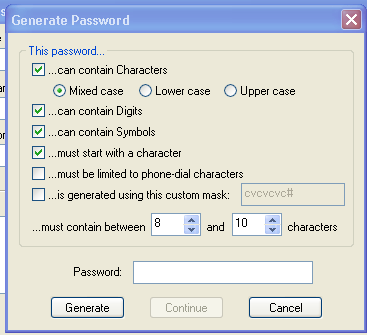
1. **Как добавить новый пароль в базу данных программы whisper.exe?**

Заходим в whisper.exe.

Edit -> Add entry



Вводим необходимую информацию, вводим пароль/генерируем (устанавливаем параметры), жмем ОК



File -> Save

1. ***Для чего предназначены все параметры создаваемой учетной записи пользователя?***

Для того, чтобы разные пользователи могли иметь разные права в системе.

Механизм учетных записей пользователей предназначен для решения следующих задач:

• Разграничение прав пользователей на доступ к информации;

• Индивидуальная настройка пользовательского интерфейса и элементов рабочего стола для каждого пользователя данного компьютера;

• Защита параметров настройки компьютера и конфиденциальной информации;

• Быстрое переключение между разными пользователями без закрытия работающих программ и приложений.

1. **В чем целесообразность разбиения множества пользователей на группы?**

**Управление доступом:** Группировка пользователей позволяет упростить управление доступом к ресурсам и данным. Вместо установки индивидуальных прав доступа для каждого пользователя можно назначить права доступа для целой группы.

**Упрощение администрирования:** Администраторы могут выполнять множество задач, связанных с управлением пользователями, группами и ресурсами более эффективно, когда пользователи разбиты на группы. Они могут легко назначать и отзывать права доступа для целых групп, а не для каждого пользователя по отдельности.

**Повышение безопасности:** Группировка пользователей позволяет легче реализовывать принцип наименьших привилегий (Least Privilege Principle). Администраторы могут назначать минимально необходимые права доступа для выполнения задачи конкретной группой пользователей, что снижает риск несанкционированного доступа.