Некоммерческое акционерное общество

АЛМАТИНСКИЙ УНИВЕРСИТЕТ ЭНЕРГЕТИКИ И СВЯЗИ

Кафедра информационных систем

АДМИНИСТРИРОВАНИЕ ИНФОРМАЦИОННЫХ СИСТЕМ И СЕТЕЙ

Методические указания по выполнению лабораторных работ
для студентов специальностей 5В070300 -Информационные системы,
5В060200-Информатика

Алматы 2016

СОСТАВИТЕЛЬ: Г.С.Нурмагамбетов. Администрирование информационных систем и сетей. Методические указания по выполнению лабораторных работ для студентов специальностей 5В070300 - Информационные системы, 5В060200-Информатика. - Алматы: АУЭС, 2016. - 56 с.

Настоящие методические указания составлены в соответствии с учебной программой курсов для бакалавров специальностей 5В070300 - Информационные системы, 5В060200-Информатика.

Ил.55, библиограф – 7 наименований.

Рецензент: канд.техн.наук Л.К.Ибраева

Печатается по плану издания некоммерческого акционерного общества «Алматинский университет энергетики и связи» на 2016 г.

© НАО «Алматинский университет энергетики и связи», 2016 г.

Содержание

Введение 4
1 Лабораторная работа № 1. Применение технологии виртуализации для решения задач администрирования 5
2 Лабораторная работа № 2. Назначение прав пользователей при произвольном управлении доступом в Windows2003(XP) 14
3 Лабораторная работа № 3. Настройка параметров регистрации и аудита в Windows 2003 (XP) 24
4 Лабораторная работа № 4. Управление шаблонами безопасности в Windows 2003 (XP) 32
5 Лабораторная работа № 5. Конфигурации системы реестра операционной системы Windows 2003(XP) 39
6 Лабораторная работа № 6. Инструменты администрирования и управления серверной системой 45
7 Лабораторная работа № 7. Создание учетных записей и групп в среде ОС Linux. Организация рабочей среды пользователя 50
Список литературы 55

Введение

Согласно рабочему учебному плану, «Администрирование информационных систем и сетей» является элективной дисциплиной для студентов специальности 5В070300 - Информационные системы. Она изучается студентами третьего курса после изучения таких дисциплин как «Информатика» и «Компьютерные сети».

Для закрепления знаний теоретического материала, полученного на лекциях, студенты выполняют лабораторные работы по администрированию информационных систем и сетей.

Известно, что дициплина «Администрирование информационных систем и сетей» состоит из двух дисциплин «Компьютерные сети», «Администрирование информационных систем». В связи с этим, для первоначального ознакомления студентов с основами администрирования информационных систем и сетей им предлагается выполнить семь лабораторных работ.

В качестве программной модели выбраны операционные системы Windows XP и Windows Server 2003, представленные компанией Microsoft, которые содержат базовые функции. Их совместное использование позволяет администратору построить гармонично законченную, гармонично работающую и безопасную инфраструктуру. Практика применения операционных систем Windows XP и Windows Server 2003 показала, что наибольшую эффективность от внедрения их обеспечивает переход к современным операционным системам Windows 7 и Windows Server 2008 R2, позволяющий решать более сложные, комплексные задачи, в частности, проблемы, связанные с информационными системами. В связи с этим, для будущих специалистов по информационным системам является важным получение первичных навыков администрирования информационных систем и сетей и передачи информации в этих сетях.

Каждая лабораторная работа снабжена краткими методическими указаниями и рекомендациями. Для допуска к выполнению лабораторной работы студент обязан изучить необходимые для ее выполнения теоретические материалы по указанной ниже литературе, и ответить на контрольные вопросы. Каждая работа завершается сдачей и защитой отчета по ней. Отчеты по лабораторным работам должны быть выполнены и оформлены в соответствии с требованиями фирменного стандарта Алматинского университета энергетики и связи СТ НАО 56023-1910-04-2014 «Учебно-методические и учебные работы. Общие требования к построению, изложению, оформлению и содержанию учебно-методических и учебных работ».

1 Лабораторная работа №1. Применение технологии виртуализации для решения задач администрирования

Цель работы: изучить технологии виртуальных машин «Orac1e VirtualBox».

1.1 Задание к лабораторной работе

Изучить теоретический материал по данной теме:

-следуя методическим указаниям, создать виртуальный жесткий диск и подключить образ CD/DVD диска в менеджере виртуальных машин;

-создать виртуальную машину и настроить ее конфигурацию;

-запустить виртуальную машину;

-установить ОС Windows 2003(XP);

-создать снимок состояния;

-установить расширенный набор инструментов в виртуальной машине;

-завершить работу виртуальной машины;

1.2 Порядок выполнения лабораторной работы

1.2.1 Использование технологии виртуализации.

В настоящее время технологии виртуализации активно используются для решения различных задач администрирования информационных сетей и систем. В основе виртуализации лежит возможность одного компьютера эмулировать работу нескольких ПК благодаря распределению его ресурсов по нескольким средам. Созданная с помощью специального программного инструмента виртуальная машина представляет собой конкретный экземпляр некой виртуальной вычислительной среды («виртуального компьютера»). Механизмы администрирования виртуальной машины позволяют создавать снимки состояния, которые фиксируют текущие параметры установленной на ВМ гостевой ОС и запущенных гостевых приложений. Запускаем консоли управления виртуальными машинами. Запустить консоль управления виртуальными машинами можно с помощью соответствующего ярлыка, расположенного на рабочем столе (рисунок 1.1) или через «Пуск»/«Меню» из программной группы «Orac1e VirtualBox».

Рисунок 1.1 - Ярлык программы «Orac1e VirtualBox»

При первом запуске консоль виртуальных машин выглядит следующим образом (рисунок 1.2).

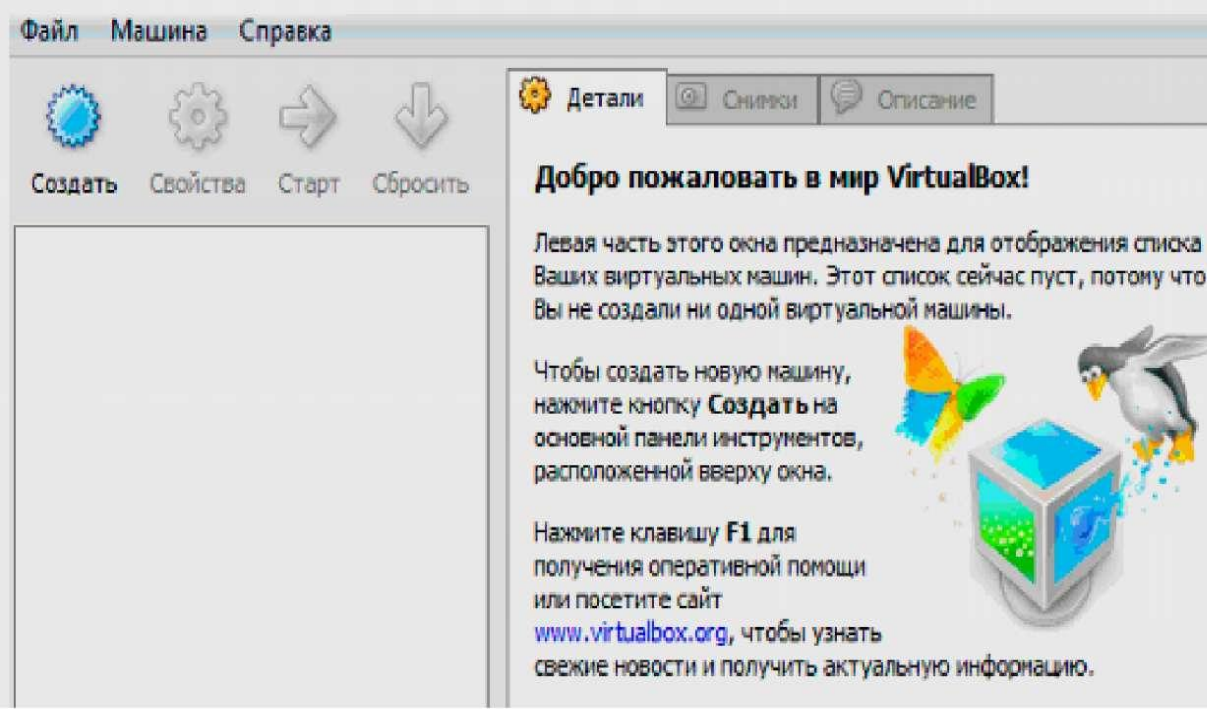

Рисунок 1.2 - Консоль виртуальных машин «Oracle VirtualBox»

Консоль разделена на несколько областей: область инструментов - для управления виртуальными машинами; список установленных виртуальных машин; область аппаратной конфигурации виртуальных машин.

1.2.2 Создание виртуального жесткого диска.

1. Подключить ранее созданные виртуальные диски к менеджеру виртуальных машин.

2. В меню «Файл» выбрать «Менеджер виртуальных носителей» или воспользоваться сочетанием клавиш «Ctrl + D». В результате откроется окно управления виртуальными носителями (рисунок 1.3).

3. Для добавления виртуального жесткого диска необходимо перейти на вкладку «Жесткие диски» и нажать кнопку «Создать» на панели инструментов. После чего откроется окно создания нового виртуального жесткого диска.

4. В открывшемся окне «Создать новый виртуальный жесткий диск» нажать «Next».

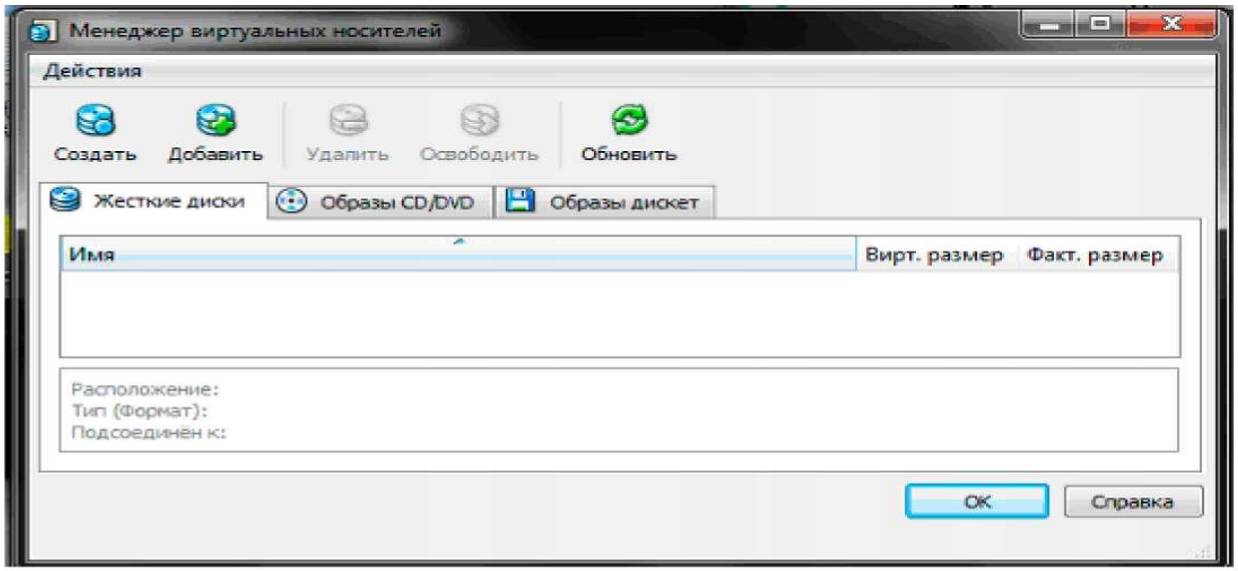

Рисунок 1.3 - Диалоговое окно «Менеджер виртуальных носителей»

5. Далее, следуя указателям, выбрать тип образа виртуального жесткого диска «Образ фиксированного размера» и нажать кнопку «Next» (рисунок 1.4)

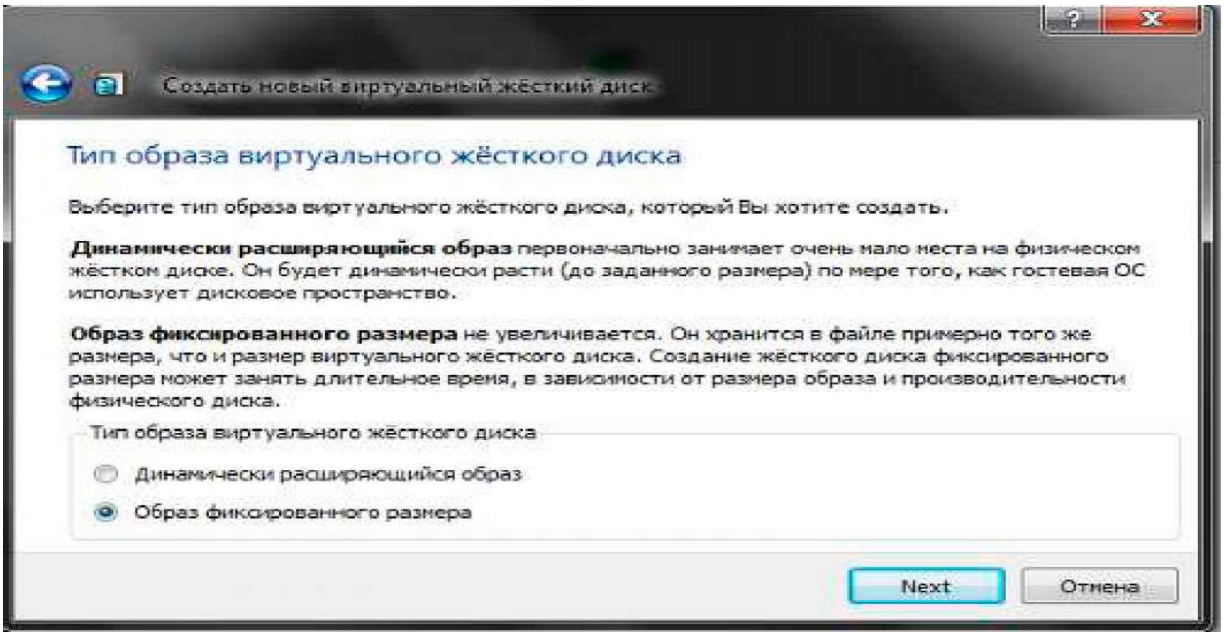

Рисунок 1.4 - Диалоговое окно «Создать новый виртуальный жесткий диск»

6. Выбрать расположение файла виртуального жесткого диска и ввести его название.

7. Установить размер жесткого диска - 4 ГБ и нажать кнопку «Next».

В результате откроется окно, в котором представлены параметры создаваемого виртуального жесткого диска.

8. После проверки введенной информации нажать кнопку «Финиш».

Новый виртуальный жесткий диск создан и его имя отображается в списке жестких дисков в окне управления виртуальными проектами (рисунок 1.5).

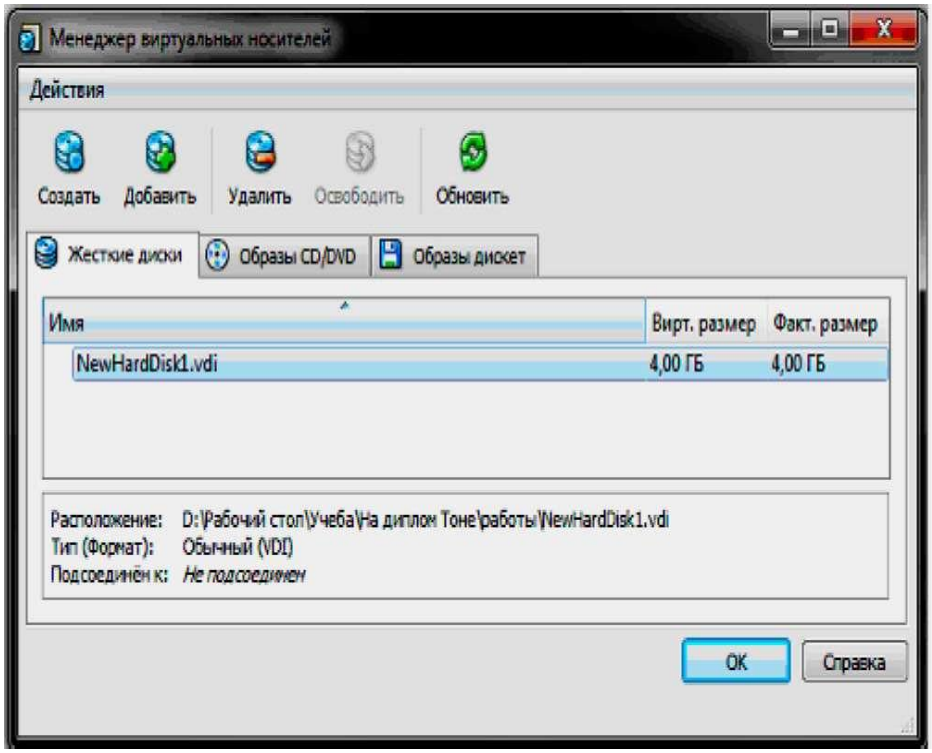

Рисунок 1.5 - Диалоговое окно «Менеджер виртуальных носителей»

Для подключения образа CD/DVD диска выполнить следующие действия:

1. Перейти на вкладку «CD/DVD образы».
2. Нажать кнопку «Добавить» на панели инструментов.
3. Из папки «Администрирование iso» выбрать образ «xp. iso» и подтвердить выбор нажатием кнопки «Открыть».

Результатом проделанных операций будет зарегистрированный образ жесткого и CD/DVD дисков в менеджере виртуальных дисков и, следовательно, в консоли виртуальной машины.

Завершить регистрацию виртуальных дисков закрытием окна «Менеджер виртуальных дисков».

1.2.3 Создание виртуальной машины.

Процесс создания виртуальной машины выполняется с использованием специального мастера, который собирает все необходимые сведения и позволяет установить конфигурацию вновь создаваемой виртуальной машины.

Для запуска мастера необходимо воспользоваться кнопкой «Создать» на панели инструментов консоли управления ВМ (рисунок 1.6).

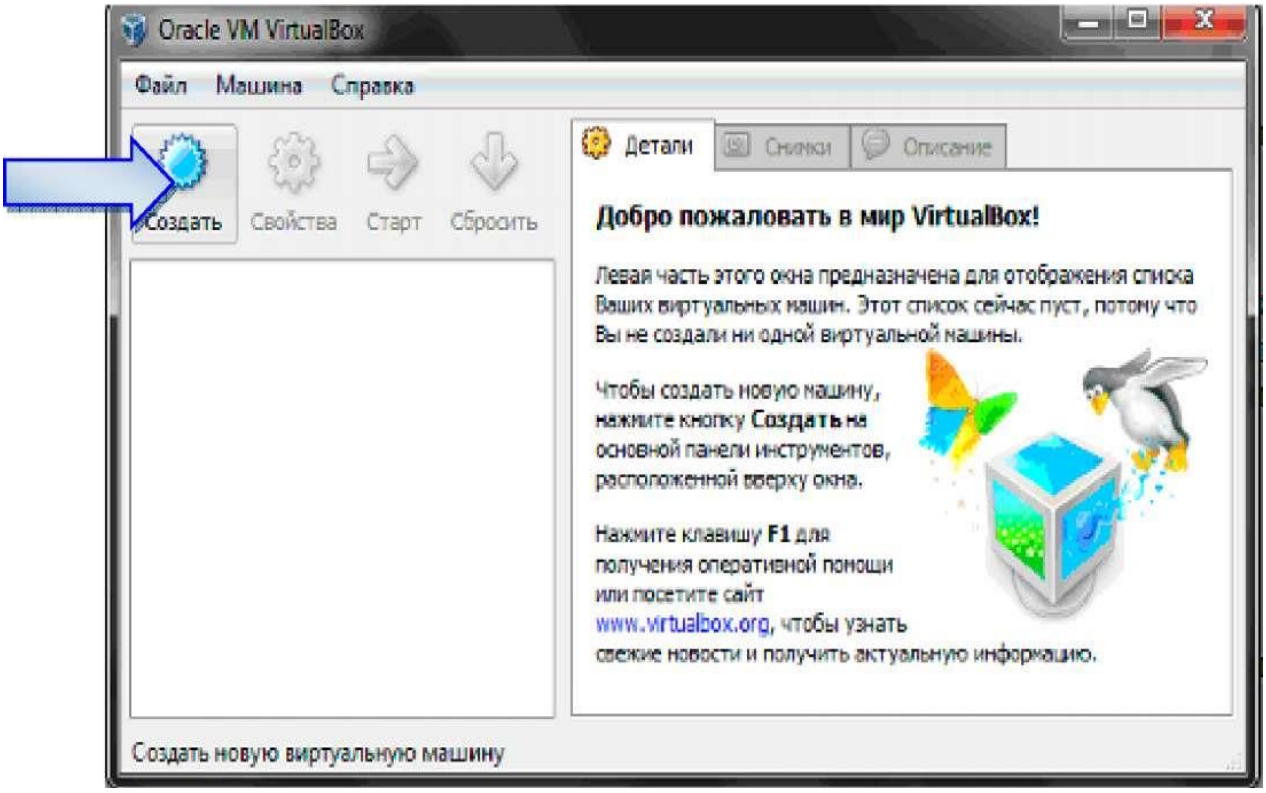

Рисунок 1.6 - Консоль управления виртуальных машин *«Orac1e VirtualBox»*

После запуска мастера нужно выполнить следующие действия:

1. Нажать кнопку «Next» в окне «Мастера создания виртуальной машины».

2. Ввести имя новой виртуальной машины «MS Windows XP» и выбрать тип устанавливаемой гостевой операционной системы Windows XP.

3. Выбрать количество основной памяти - 256 МБ.

4. Выбрать виртуальный жесткий диск. Диск выбирается из списка подключенных в менеджере образов виртуальных дисков или создается с помощью специального мастера. В случае создания образ автоматически регистрируется в менеджере образов.

5. Завершаем работу мастера создания виртуальной машины, нажав кнопку «Финиш» (рисунок 1.7).

После завершения работы мастера в консоли виртуальной машины в списке машин появляется вновь созданная виртуальная машина с названием «MS Windows XP». В правой части окна на странице «Детали» даны сведения об аппаратной конфигурации виртуальной машины (рисунок 1.8).

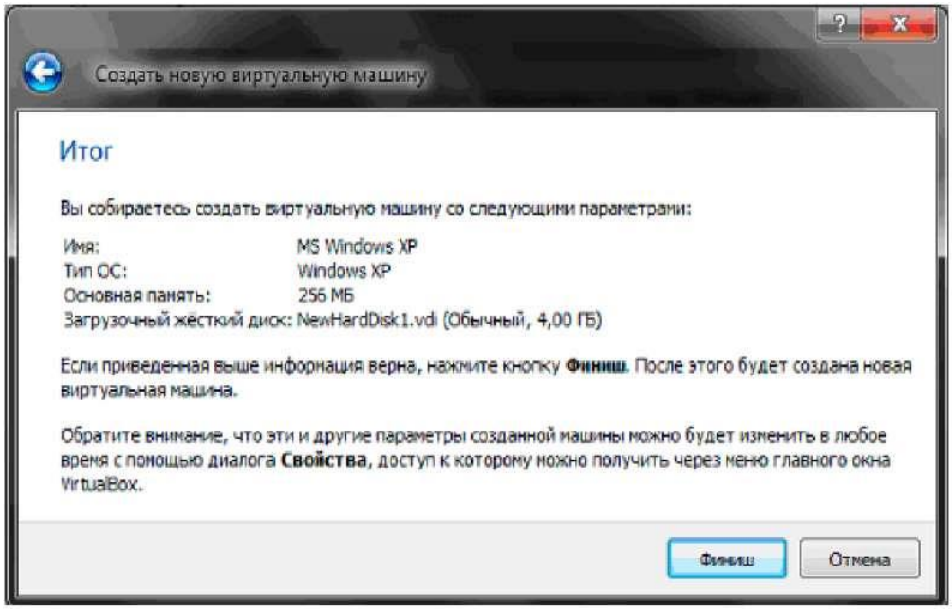

Рисунок 1.7 - Диалоговое окно
«Создать новую виртуальную машину»

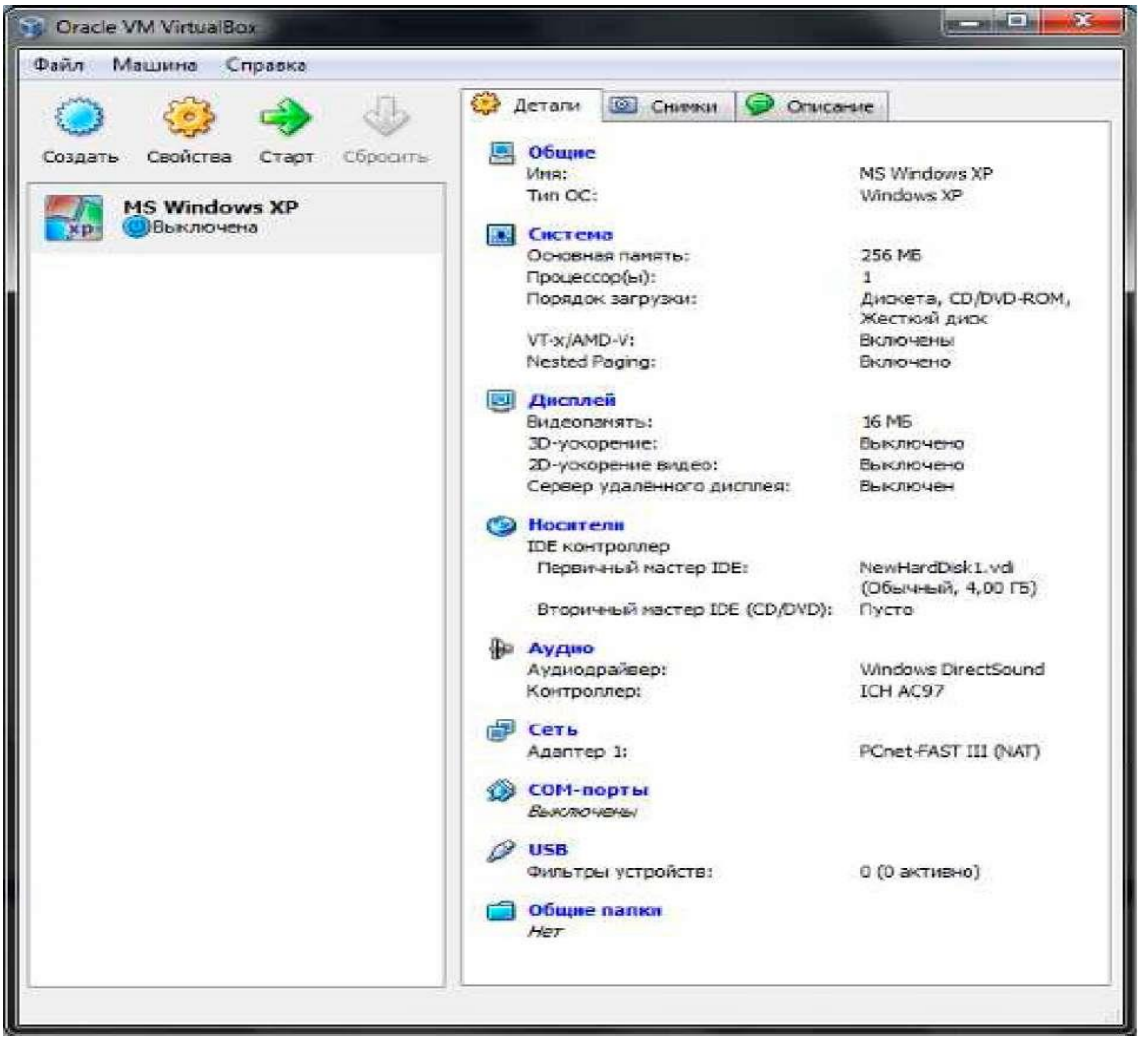

Рисунок 1.8 - Консоль конфигурации виртуальных машин
«Oracle VirtualBox»

Настройка конфигурации виртуальной машины.

Перед первым запуском ВМ необходимо настроить дополнительные параметры аппаратной конфигурации:

1.) С помощью кнопки «Свойства» на панели инструментов консоли управления перейти в окно настройки свойств системы.

2.) В разделе настроек «Система» на вкладке «Материнская плата» установить порядок загрузки: CD/DVD-ROM, жесткий диск.

3.) В разделе настроек «Носители» проверить путь к созданному жесткому диску.

Далее, для организации взаимодействия между гостевой ОС и основной ОС, зададим общую сетевую папку.

4.) В разделе настроек «Общие папки» добавить папку (рисунок 1.9).

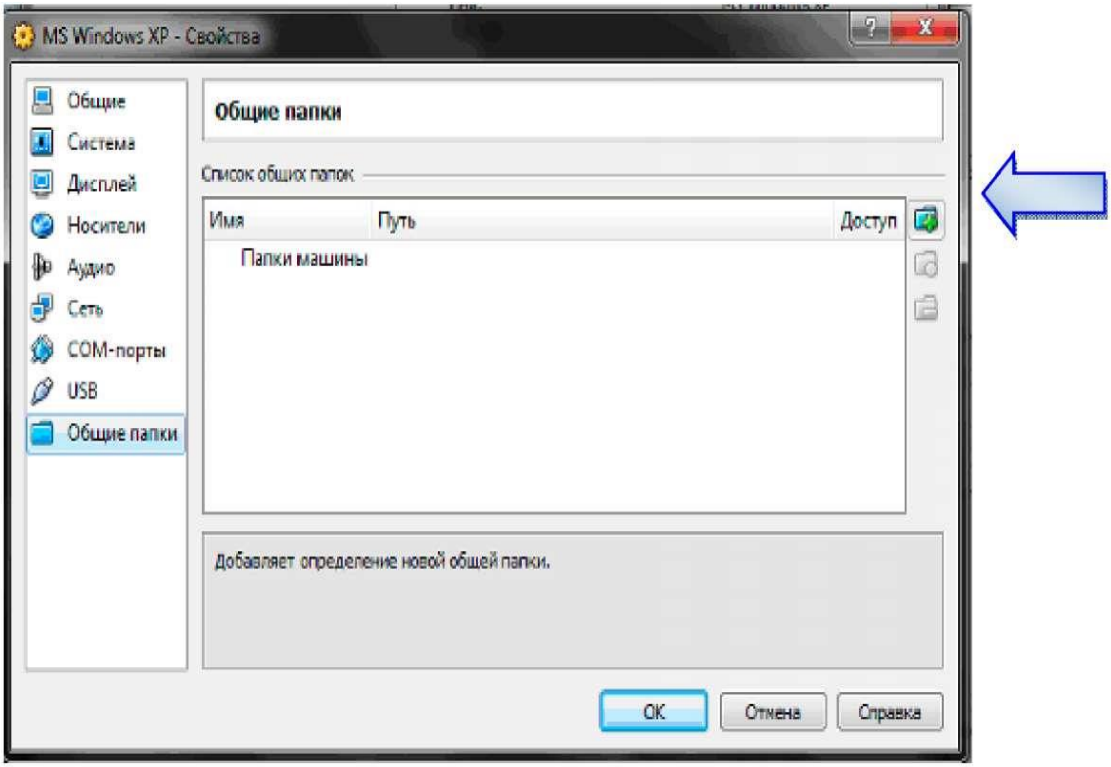

Рисунок 1.9 - Диалоговое окно «Свойства»

5.) В появившемся диалоговом окне «Добавить общую папку» ввести путь и имя папки.

Запустить виртуальную машину.

1.2.4 Установка ОС Windjws XP/

На следующем этапе работы необходимо установить ОС в соответствии с приведенными ниже требованиями.

1) Установить Windows XP в выделенном разделе.

2) Форматировать раздел в системе NTFS.

3) Закончить настройку нажатием кнопки «Готово».

После загрузки гостевой ОС до момента аутентификации необходимо выполнить команду из трех клавиш: «Ctrl + Alt + Del». Однако если их нажать на клавиатуре, то команду перехватит основная ОС и среагирует соответствующим образом. На этот случай предусмотрена специальная команда в виртуальной машине, которая вызывается также виртуально.

4) Выполнить команду «Машина» и «Послать Ctrl + Alt + Del» в меню виртуальной машины (рисунок 1.10).

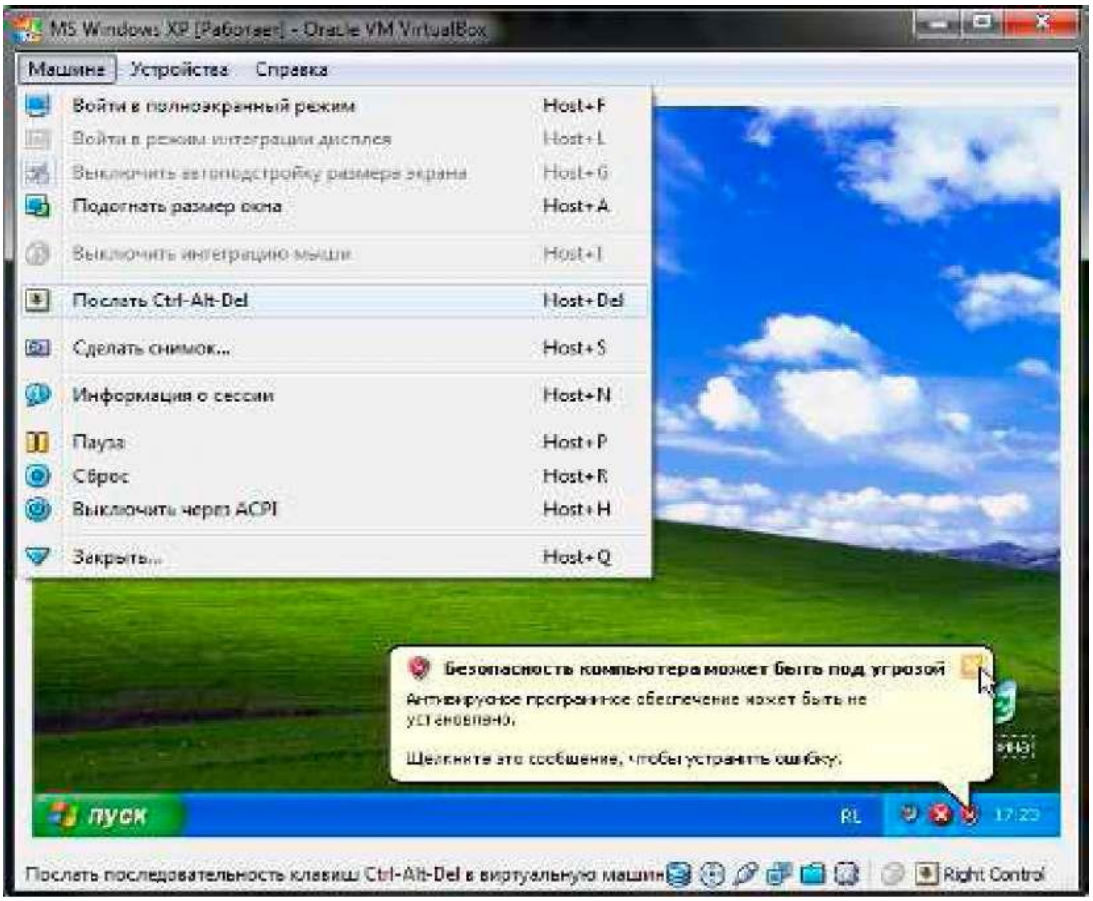

Рисунок 1.10 - Виртуальная машина

После команды «Ctrl + Alt + Del» появляется окно диспетчера задач.

5) Проверить работоспособность гостевой ОС.

Завершение работы виртуальной машины. Создание снимка состояния.

1. В меню «Машина» выбрать пункт «Закрыть», чтобы отобразить диалоговое окно «Закрыть виртуальную машину».

2. Выбрать пункт «Сохранить состояние машины» и нажать ОК.

3. В консоли управления виртуальной машины перейти на вкладку «Снимки» (рисунок 1.11).

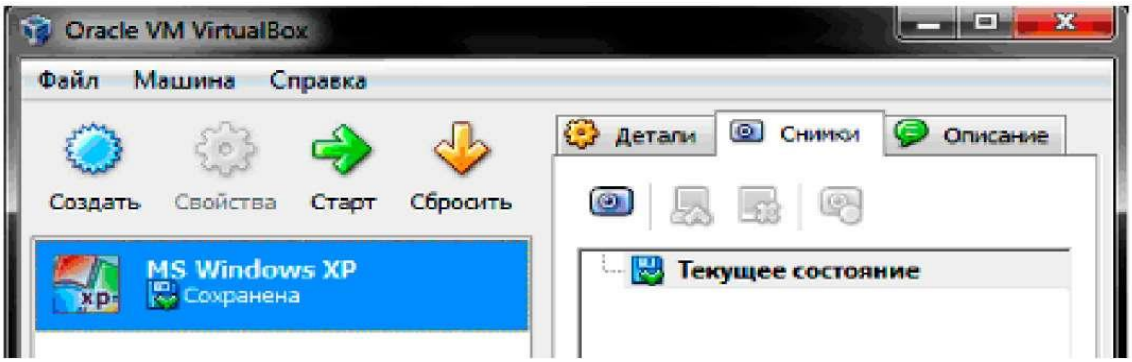

Рисунок 1.11- Вкладка «Снимки» консоли управления ВМ

4. Нажать кнопу «Сделать снимок» или выполнить команду «Ctrl + Shift + S», чтобы вызвать диалоговое окно «Сделать снимок виртуальной машины» (рисунок 1.12).

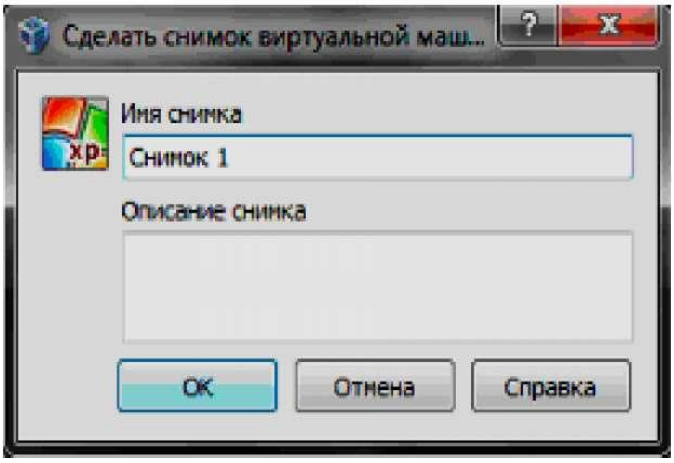

Рисунок 1.12 - Диалоговое окно «Сделать снимок виртуальной машины»

Ввести имя и описание снимка. Нажать «ОК».

1.3 Содержание отчета

Отчет о лабораторной работе должен содержать следующие разделы:
-цель работы;
-задание;
-краткое описание;
-процесс создания виртуальной машины;
-настройку дополнительных параметров аппаратной конфигурации;
-выводы по работе.

1.4 Варианты заданий

Номер варианта	1	2	3	4	5	6	7	8	9	10
установить размер жесткого диска Гб	4	8	16	24	32	48	60	28	36	18
количество основной памяти Мб	256	500	1000	1200	2000	1800	1600	2200	2400	600

1.5 Контрольные вопросы

1. Что представляют собой виртуальные машины?
2. Для каких целей можно использовать виртуальные машины?
3. Какое количество виртуальных машин можно создать на одном физическом устройстве (компьютере)?
4. Какая операционная система именуется хозяйской ОС?
5. Как называется специальный модуль в составе?
6. Приложения ВМ, который решает все задачи по управлению виртуальными машинами.
7. Какая операционная система называется гостевой?
8. Каким образом можно изменять конфигурацию созданной виртуальной машины?
9. Каким образом осуществляется подключение жесткого и CD-ROM дисков**?**

2 Лабораторная работа №2. Назначение прав пользователей при произвольном управлении доступом в Windows 2003 (XP)

Цель работы: изучить операции по созданию учетных записей пользователей и групп пользователей, механизмы по их настройке.

2.1 Задание к лабораторной работе

1. Создайте учетную запись с именем студента, используя команду «Print Screen» клавиатуры, сохраните копию экрана со списком пользователей вашего компьютера (для этого после нажатия клавиши «Print Screen»).
2. Вставить скопированное изображение в новый документ для представления в качестве отчета.
3. Создайте группу «Информационная безопасность» и, как в первом задании сохраните окно со списком групп «Вашего компьютера» для отчета.

4. Заблокируйте учетную запись студента и после этого удалите.

2.2 Порядок выполнения лабораторной работы

После выполнения идентификации и аутентификации подсистема защиты устанавливает полномочия (совокупность прав) субъекта для последующего контроля санкционированного использования объектов информационной системы. Обычно полномочия субъекта представляются списком ресурсов, доступным пользователю и правами по доступу к каждому ресурсу из списка.

При разграничении доступа по спискам задаются соответствия: каждому пользователю - список ресурсов и прав доступа к ним или каждому ресурсу - список пользователей и их прав доступа к данному ресурсу. Списки позволяют установить права с точностью до пользователя. Списки используются в подсистемах безопасности операционных систем и систем управления базами данных.

2.2.1 Создание учетной записи.

1. Откройте оснастку «Управление компьютером» в разделе «Администрирование, панели управления» (рисунок 2.1).

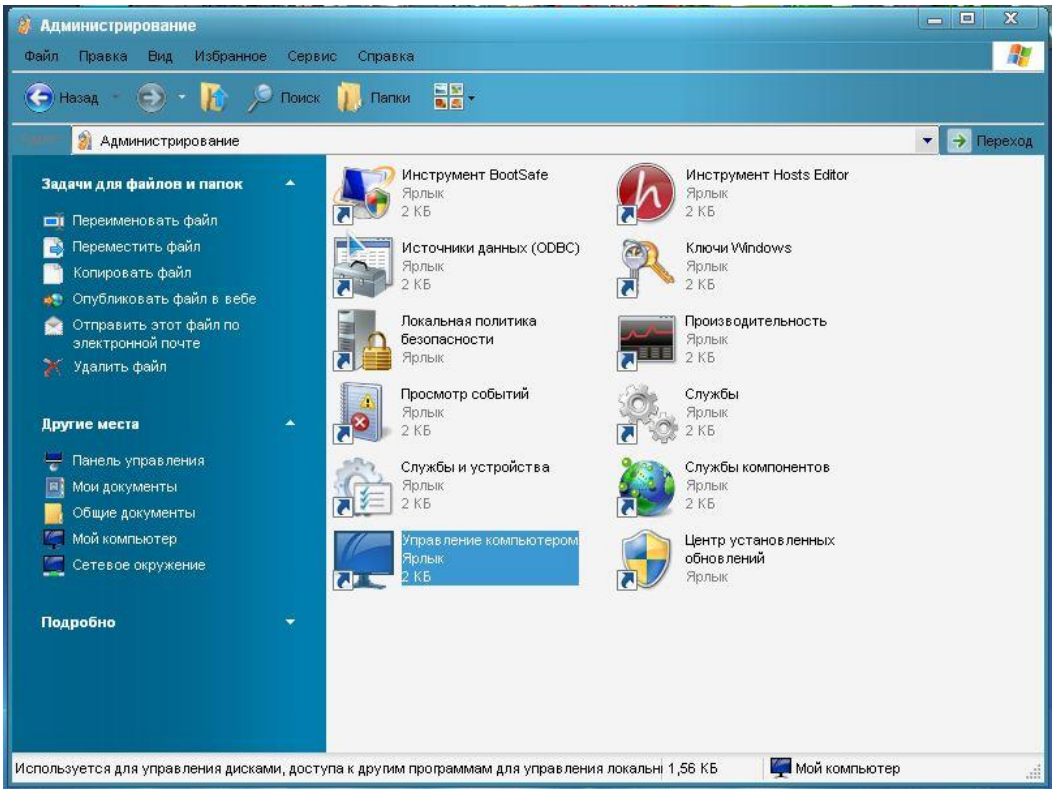

Рисунок 2.1- Администрирование

2. В оснастке «Локальные пользователи и группы» установите указатель мыши на папку «Пользователи» и нажмите правую кнопку.

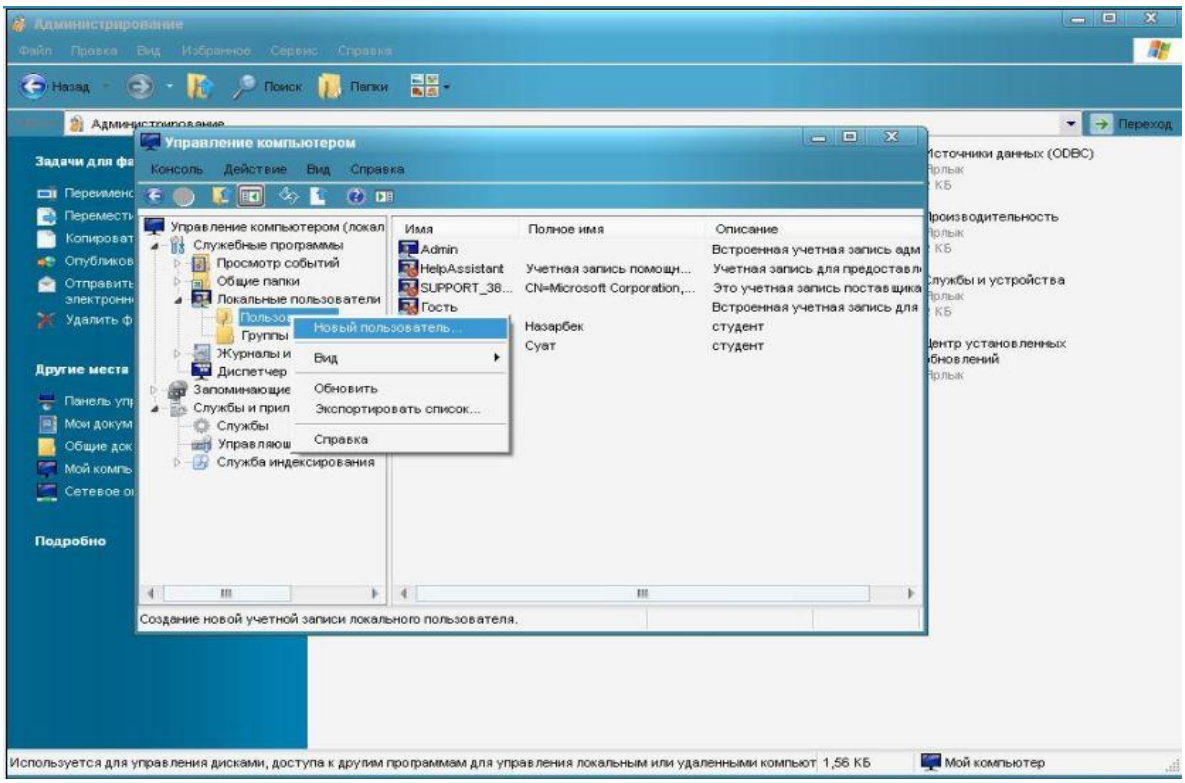

Рисунок 2.2- Новый пользователь

3. В появившемся контекстном меню выберите команду «Новый пользователь» (рисунок 2.2). Появится окно диалога «Новый пользователь» (рисунок 2.3).

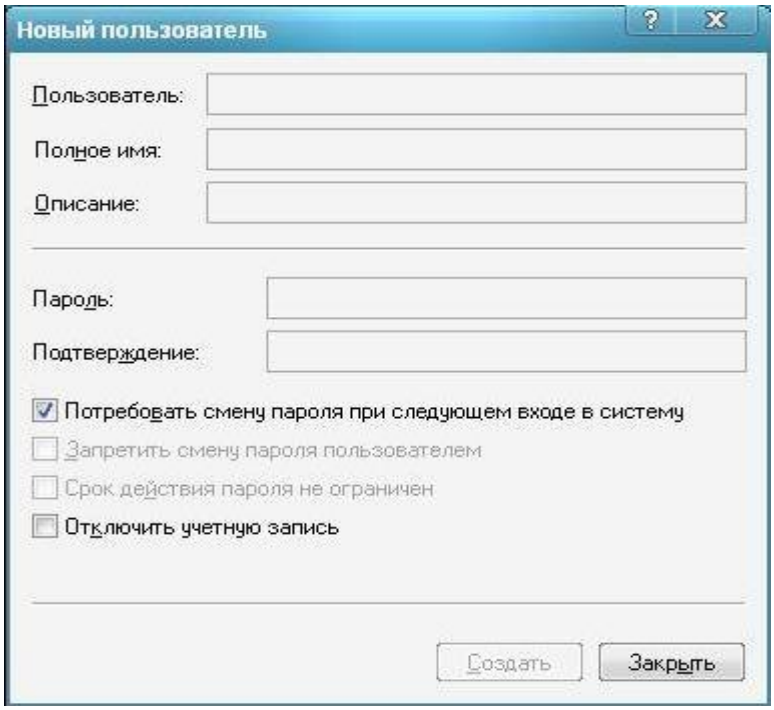

Рисунок 2.3- Окно диалога новый пользователь

4. В поле «Пользователь» введите имя создаваемого пользователя, например, свою фамилию.

Примечание. Имя пользователя должно быть уникальным для компьютера. Оно может содержать до 20 символов верхнего и нижнего регистра. Ниже приведены символы, применение которых в имени пользователя недопустимо:»/ \ []:; =,+*?<> Имя пользователя не может состоять целиком из точек и пробелов.

5. В поле «Полное имя» введите полное имя создаваемого пользователя.

6. В поле «Описание» введите описание создаваемого пользователя или его учетной записи, например, «студент ».

7. В поле «Пароль» введите пароль пользователя и в поле «Подтверждение» подтвердите его правильность вторичным вводом.

Примечание. Длина пароля не может превышать 14 символов (рисунок 2.4).

8.Установите или снимите флажки:

- потребовать смену пароля при следующем входе в систему;
- запретить смену пароля пользователем;
- срок действия пароля не ограничен;
- отключить учетную запись.

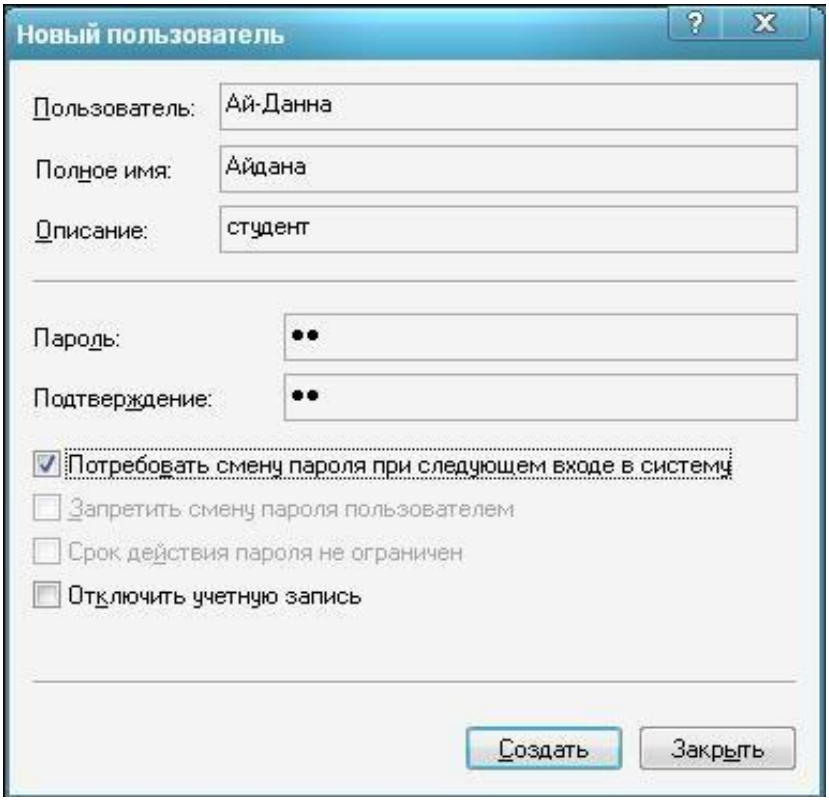

Рисунок 2.4- Окно диалога длина пароля

9. Чтобы создать еще одного пользователя, нажмите кнопку «Создать» и повторите шаги с 1 по 8. Для завершения работы нажмите кнопку «Создать» и затем «Закрыть».

2.2.2 Создание локальной группы.

1. В окне оснастки «Локальные пользователи и группы» установите указатель мыши на папке «Группы» и нажмите правую кнопку.

2. В появившемся контекстном меню выберите команду «Новая группа».

3. В поле «Имя» группы (рисунок 2.5) введите имя новой группы, например, «Студенты».

Примечание. Имя локальной группы должно быть уникальным в пределах компьютера. Оно может содержать до 256 символов в верхнем и нижнем регистрах.

4. В поле «Описание» введите описание новой группы.

5. В поле «Члены группы» можно сразу же добавить пользователей и группы, которые войдут в данную группу: для этого нужно нажать кнопку «Добавить» и выбрать их в списке.

Для завершения нажмите кнопку «Создать» и затем «Закрыть».

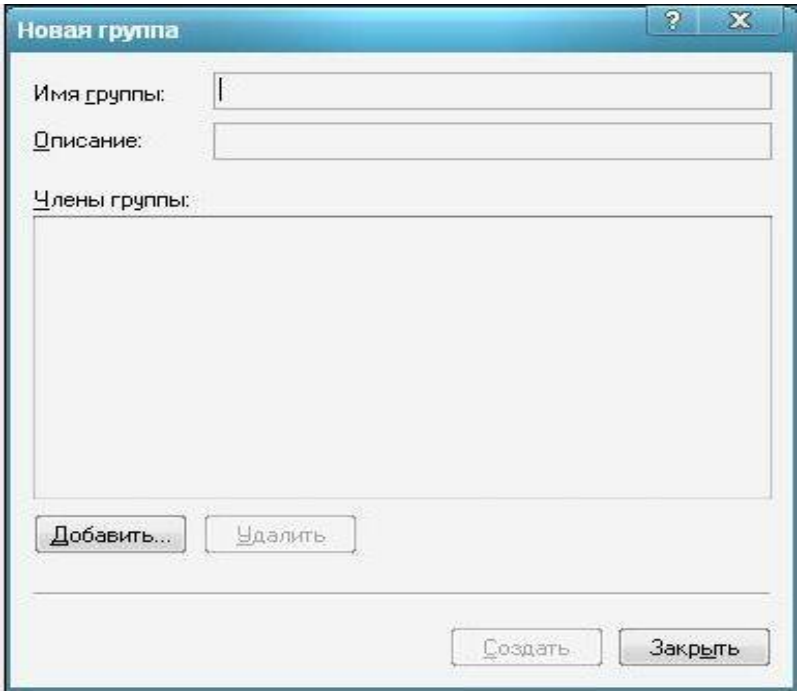

Рисунок 2.5 - Имя группы

2.2.3 Изменение членства в локальной группе.

1. В окне оснастки «Локальные пользователи и группы» щелкните на папке «Группы».

2. В правом подокне установите указатель мыши на модифицируемую группу и нажмите правую кнопку.

3. В появившемся контекстном меню выберите команду «Добавить» в группу или «Свойства».

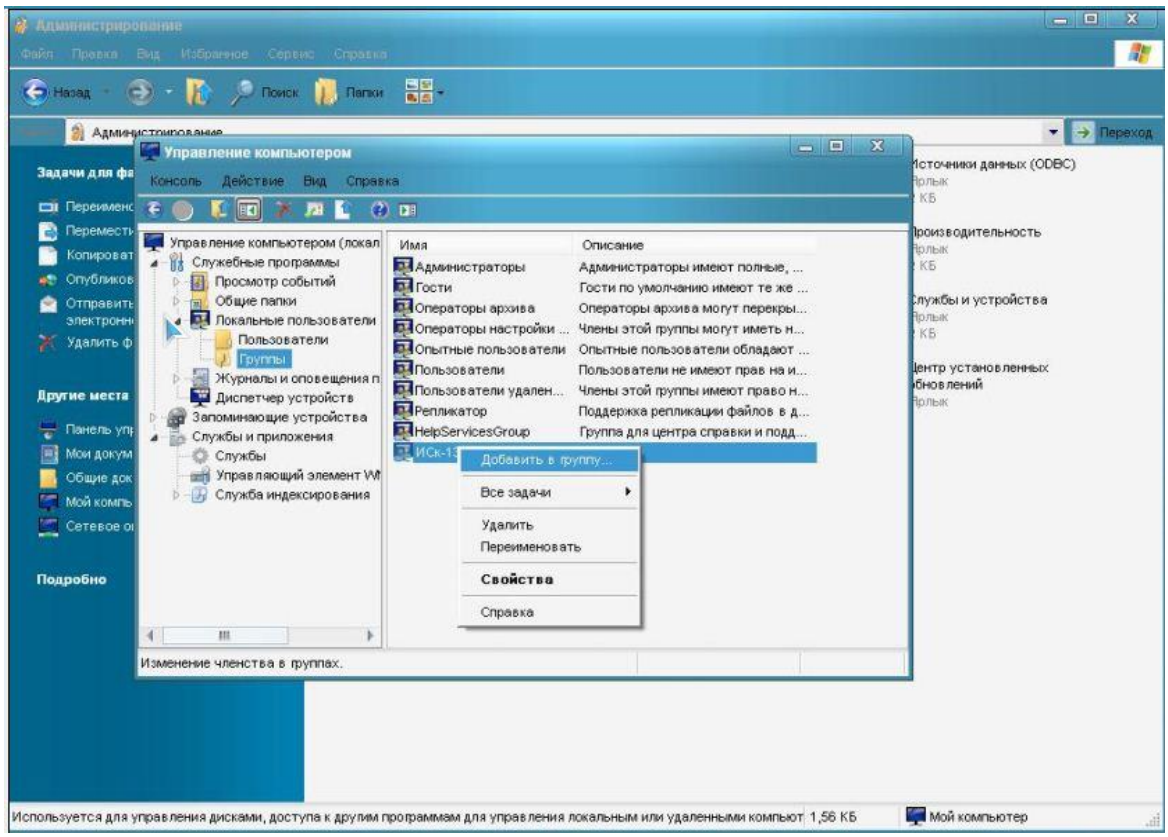

Рисунок 2.6 - Новые учетные записи в группу

4. Для того, чтобы добавить новые учетные записи в группу, нажмите кнопку «Добавить» (рисунок 2.6).

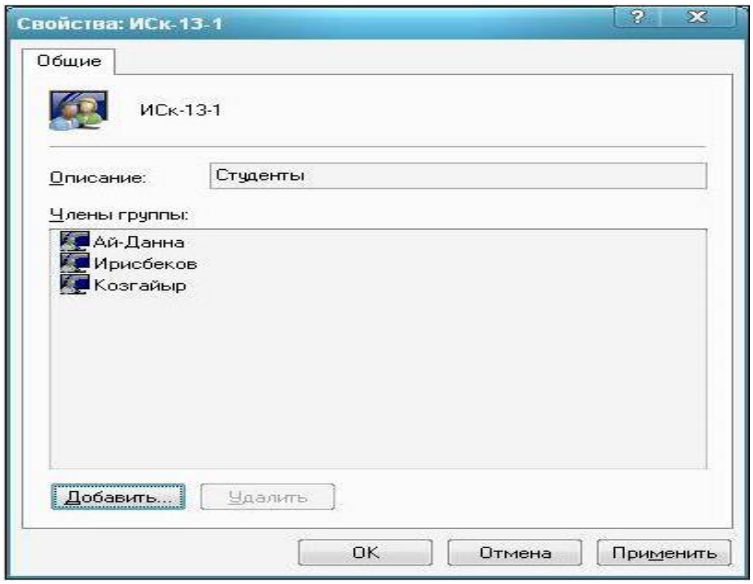

Рисунок 2.7 - Члены группы

5. Далее следуйте указаниям окна диалога «Выбор. Пользователи или Группы».

6. Для того, чтобы удалить из группы некоторых пользователей, в поле «Члены группы» (рисунок 2.7) окна свойств группы выберите одну или несколько учетных записей и нажмите кнопку «Удалить» (рисунок 2.9).

Рисунок 2.8 - Свойства группы

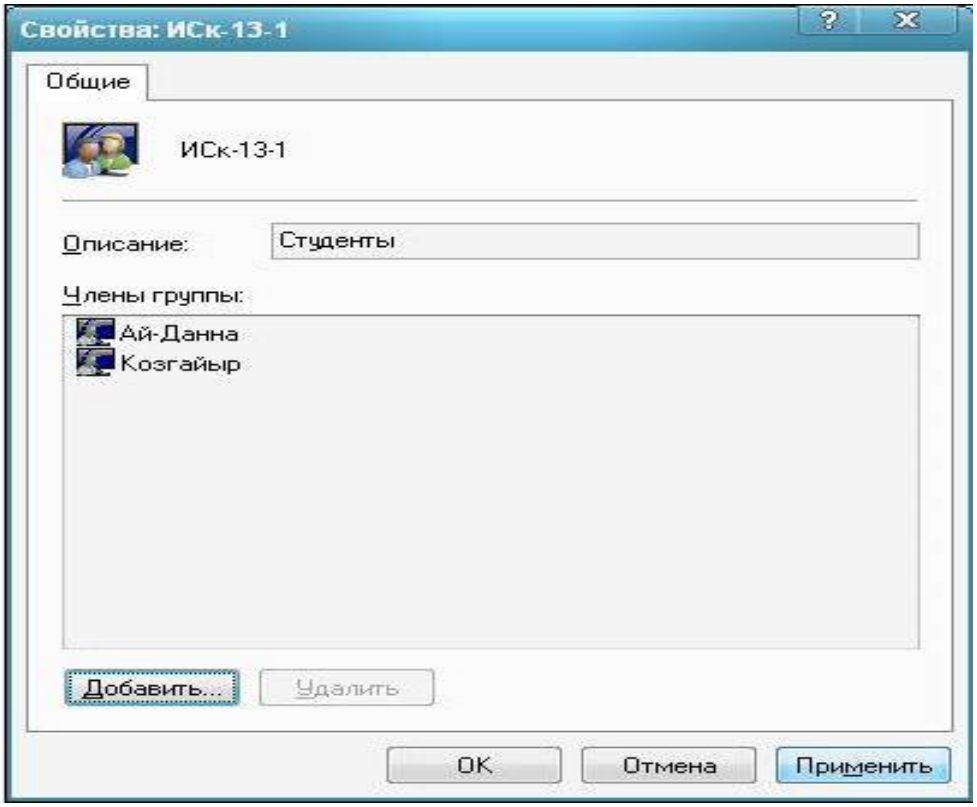

Рисунок 2.9 - Удаление учетных записей

Примечание - в локальную группу можно добавлять как локальных пользователей, созданных на компьютере, так и пользователей и глобальные группы, созданные в домене, к которому принадлежит компьютер, или в доверяемых доменах. Встроенные группы не могут быть удалены. Удаленные группы не могут быть восстановлены. Удаление группы не отражается на входящих в нее пользователей.

2.2.4 Временная блокировка учетной записи.

1. Откройте оснастку «Управление компьютером».

2. Для этого либо выберите на «Рабочем столе» ярлык «Мой компьютер» и нажмите правую клавишу мыши, после чего выберите пункт контекстного меню «Управление», либо воспользуйтесь разделом «Администрирование в Панели управления».

3. В открывшейся оснастке выберите пункты «Служебные программы Локальные пользователи и группы» (рисунок 2.10).

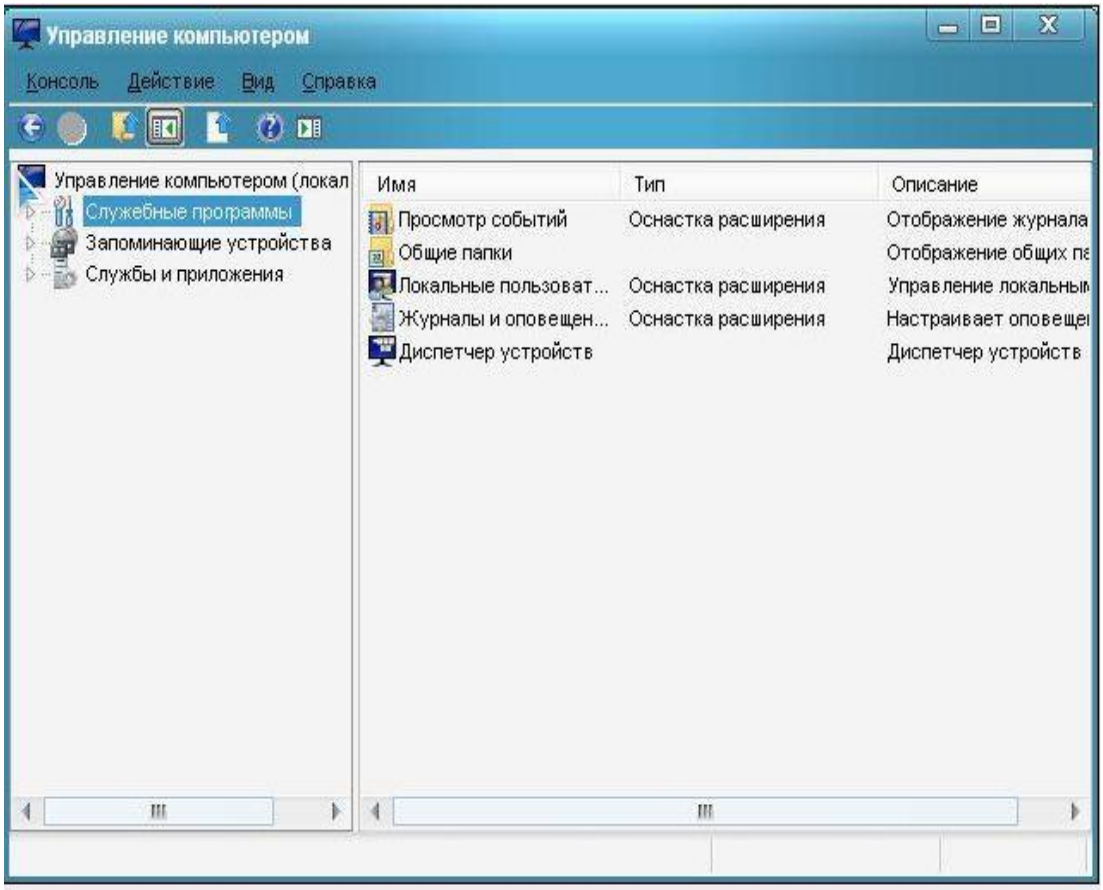

Рисунок 2.10 - Локальные пользователи и группы

4. Откройте папку «Пользователи» и выберите учетную запись «Гость» (рисунок 2.11).

5. Нажмите правую клавишу мыши и выберите пункт «Свойства».

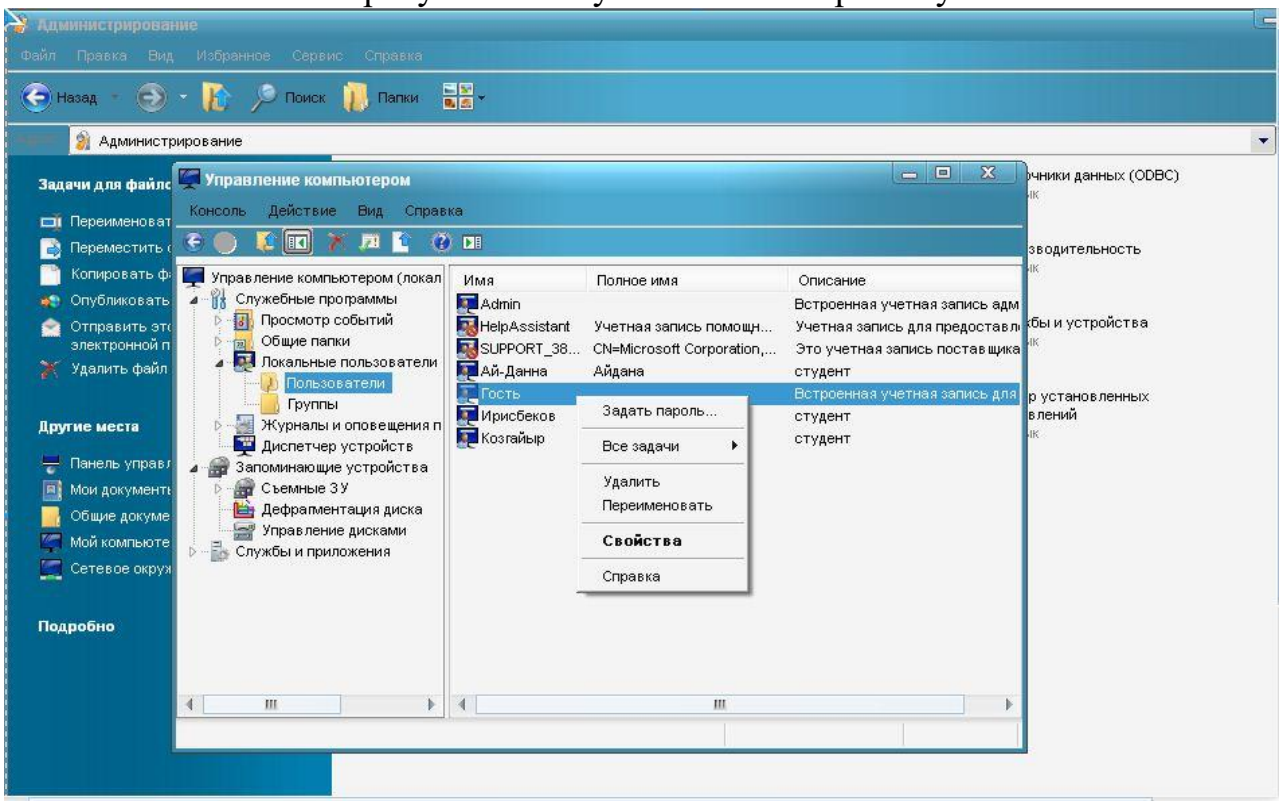

Рисунок 2.11- Папка учетная запись «Гость»

6. В открывшемся окне снимите отметку пункта «Отключить» учетную запись (рисунок 2.12).

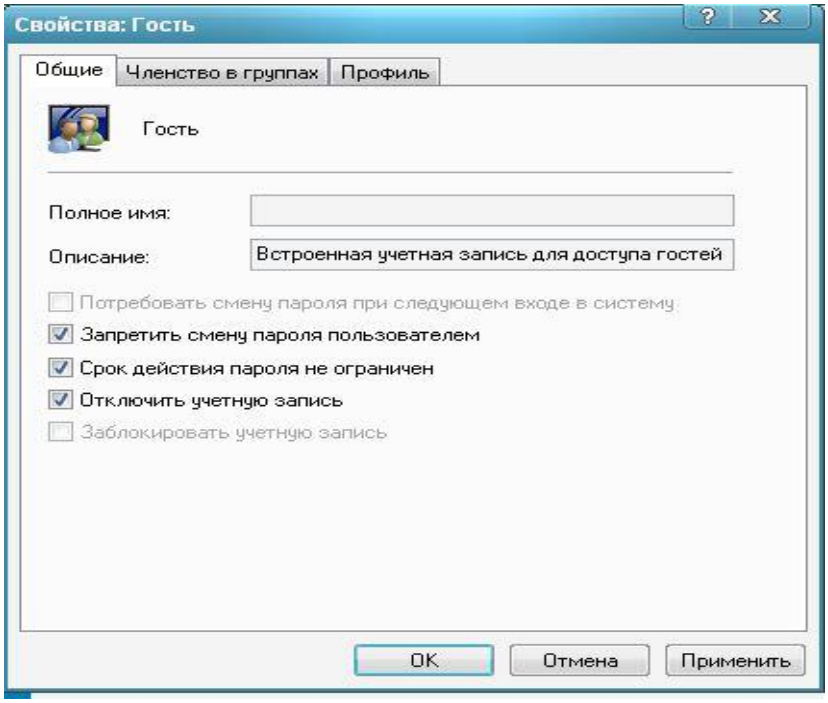

Рисунок 2.12 - Отключение учетной записи

5. Нажмите кнопку «ОК» и сделайте вывод о состоянии учетной записи
8. Выполните пункт 5 и отметьте пункт «Отключить учетную запись».

2.3 Содержание отчета

Отчет о лабораторной работе должен содержать следующие разделы:
-цель работы;
-задание;
-краткое описание;
-создание учетной записи;
-изменение членства в локальной группе;
-временная блокировка учетной записи;
-выводы по работе.

2.4 Варианты заданий

Номер варианта	При создании учетной записи установить или снять флажки	Изменение членства в локальной группе
1	потребовать смену пароля при следующем входе в систему	добавить в группу
2	запретить смену пароля пользователем	пользователи
3	срок действия пароля не ограничен	опытные пользователи
4	срок действия пароля ограничить	пользователи удалённые
5	отключить учетную запись	гости
6	запретить смену пароля пользователем	опытные пользователи
7	потребовать смену пароля при следующем входе в систему	гости
8	отключить учетную запись	опытные пользователи
9	срок действия пароля не ограничен	пользователи удалённые
10	срок действия пароля ограничен	пользователи удалённые

2.5 Контрольные вопросы

1. Что представляет собой учетная запись пользователя?

2. Какие типы учетных записей вам известны?

3. Какую учетную запись рекомендуется использовать после окончания настройки компьютера для повседневной работы?

4. Для чего предназначена учетная запись «Гость»?

5. Какая учетная запись позволяет настраивать ПК и устанавливать любые программы?

6. Для чего создаются группы пользователей?

7. Каким образом можно изменять и настраивать учетные записи пользователей?

8. Как установить безопасный вход в систему?

3 Лабораторная работа №3. Настройка параметров регистрации и аудита в Windows 2003 (XP)

Цель работы: активизировать механизмы регистрации и аудита операционной системы Windows 2003(XP) и настроить параметры просмотра аудита папок и файлов.

3.1 Задание к лабораторной работе

1. Включить аудит успеха и отказа всех параметров;

2. Изучить требования к надежности и информационной безопасности средствами регистрации и аудита;

3. Удалить созданную ранее учетную запись студентов.

3.2 Порядок выполнения лабораторной работы

Регистрация является еще одним механизмом обеспечения защищенности информационной системы. Этот механизм основан на подотчетности системы обеспечения безопасности, фиксирует все события, касающиеся безопасности. Аудит - это анализ накопленной информации, проводимый оперативно, в реальном времени или периодически.

Регистрационный журнал - это хронологически упорядоченная совокупность записей результатов деятельности субъектов системы, достаточная для восстановления, просмотра и анализа последовательности действий, окружающих или приводящих к выполнению операций, процедур или совершению событий при транзакции с целью контроля конечного результата.

3.2.1 Активизация механизма регистрации и аудита с помощью оснастки «Локальные политики безопасности».

1. Выберите кнопку «Пуск» панели задач.

2. Откройте меню «Настроить/Панель управления».

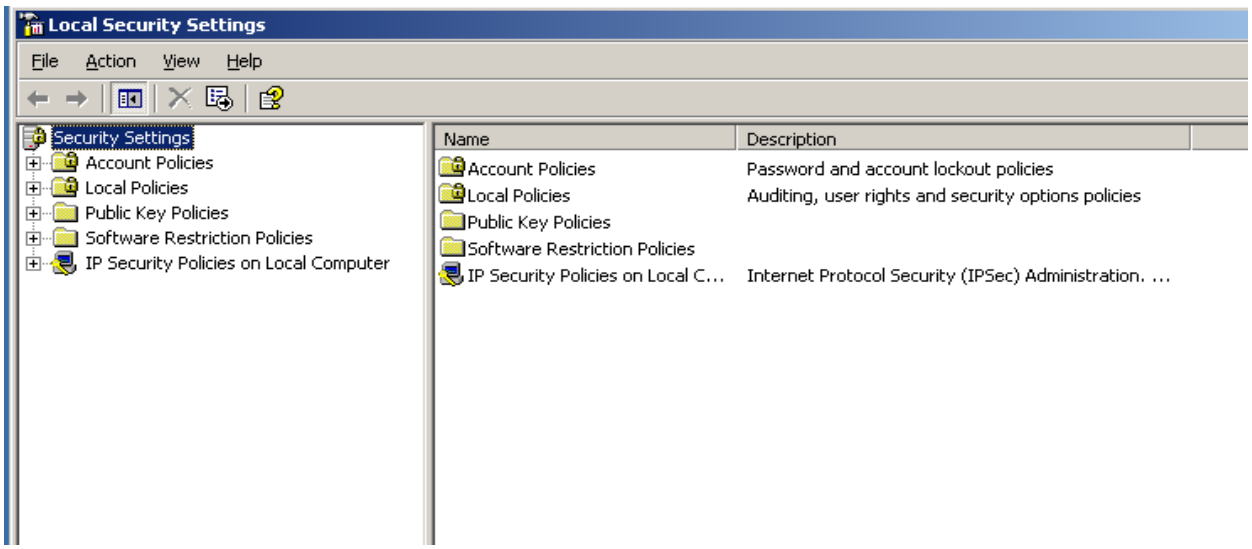

Рисунок 3.1- Локальная политика безопасности

В открывшемся окне выберите ярлык «Администрирование/ Локальная политика безопасности» (рисунок 3.1).

3. Выберите пункт «Политика аудита» (рисунок 3.2).

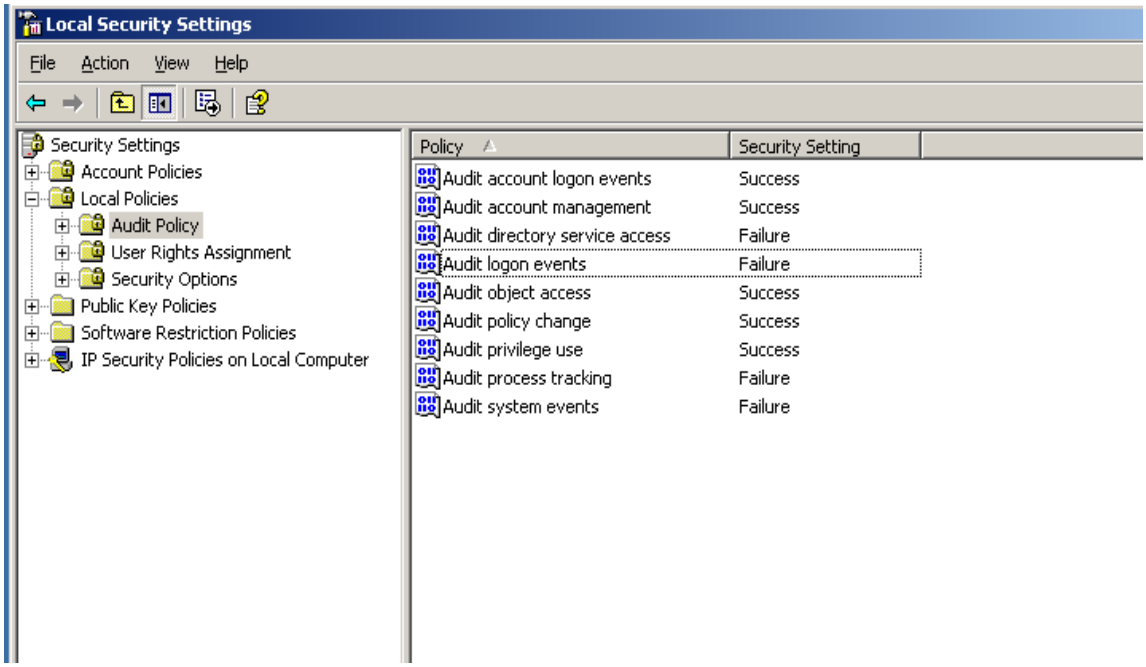

Рисунок 3.2 - Пункт «Политика аудита»

4. Для включения или отключения параметров аудита выберите требуемый параметр и дважды щелкните левой клавишей мыши.

Рисунок 3.3 - Аудит событий данного типа

5. Для каждого параметра можно задать аудит успехов или отказов, либо вообще отключить аудит событий данного типа (рисунок 3.3).

6. Значения параметров политики аудита приведены на лекциях.

7. По умолчанию все параметры политики аудита выключены.

8. Включите аудит успеха и отказа для всех параметров.

9. Для этого включить параметры политики аудита (рисунок 3.4).

10. Нажмите кнопку «ОК».

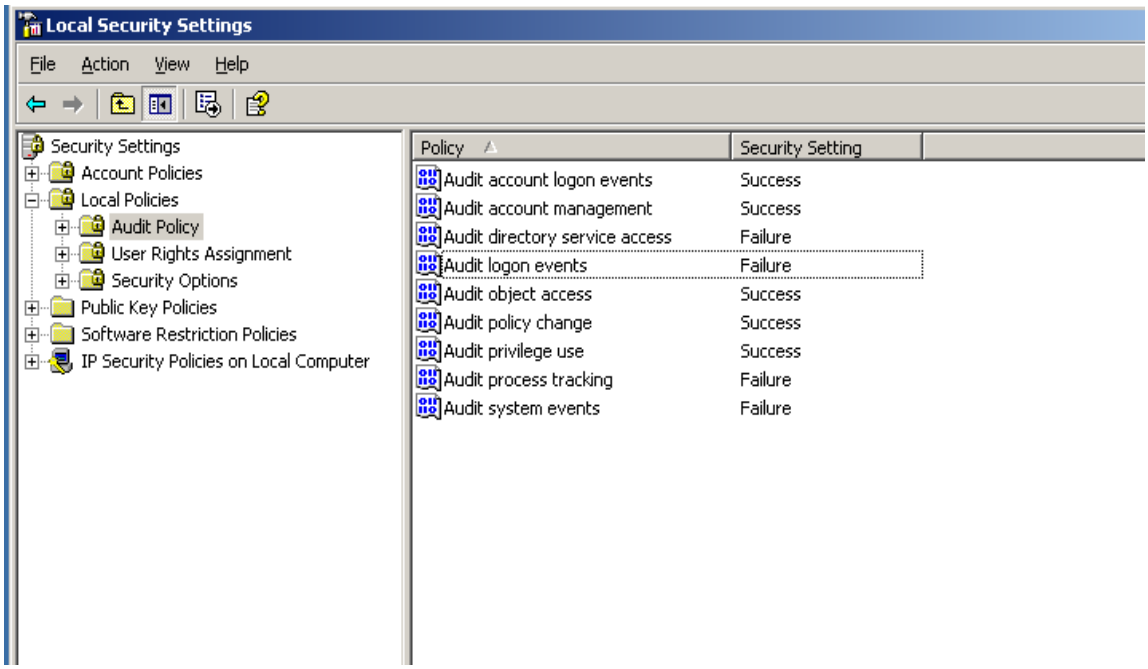

Рисунок 3.4 - Включение политики аудита

3.2.2 Настройка и просмотр аудита папок и файлов (Доступно только на томах NTFS).

1. Установите указатель мыши на файл или папку, для которой следует выполнить аудит, и нажмите правую кнопку.

2. В появившемся контекстном меню выберите команду «Свойства» (рисунок 3.5).

3. В окне свойств папки или файла перейдите на вкладку «Безопасность».

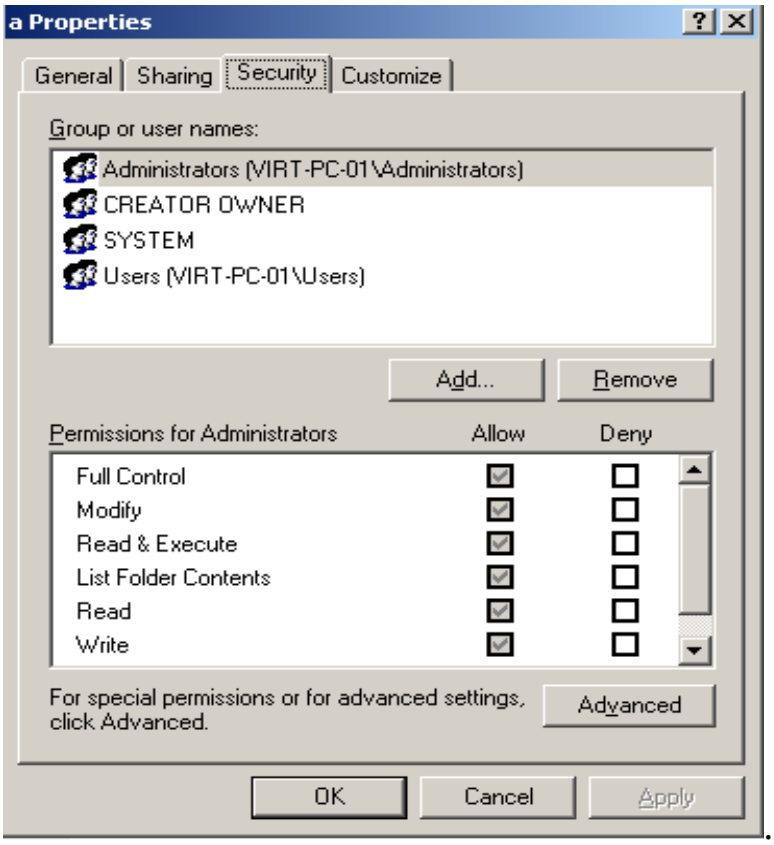

Рисунок 3.5 - Свойства контекстного меню

4. На вкладке «Безопасность» нажмите кнопку «Дополнительно» и затем перейдите на вкладку «Аудит».

5. Если Вы хотите настроить аудит для нового пользователя или группы на вкладке «Аудит» нажмите кнопку «Добавить».

6. Появится диалоговое окно «Выбор: Пользователь, Компьютер или Группа» (рисунок 3.6).

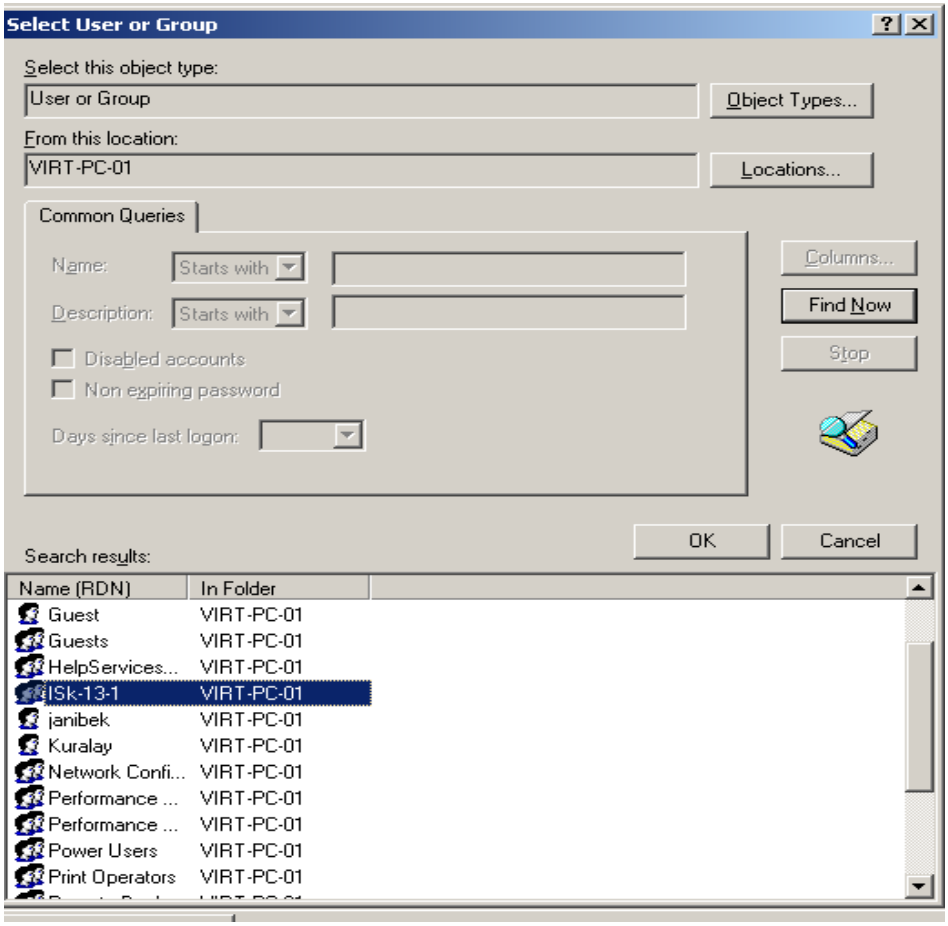

Рисунок 3.6 - Диалоговое окно «Выбор»

7. Выберите имя нужного пользователя или группы и нажмите кнопку «ОК». Откроется окно диалога «Элемент» аудита для. Здесь Вы сможете ввести все необходимые параметры аудита.

8. В списке «Применять» укажите, где следует выполнять аудит (это поле ввода доступно только для папок).

9. В группе «Доступ» следует указать, какие события следует отслеживать: окончившиеся успешно («Успех»), неудачно («Отказ») или оба типа событий.

10. Применять этот аудит к объектам и контейнерам только внутри этого контейнера - определяет, распространяются ли введенные Вами настройки аудита на файлы и папки, находящиеся ниже по дереву каталогов файловой системы (флажок не установлен). В обратном случае, установите флажок (или выберите в списке) Применять опцию «Только для этой папки». Это позволит не выполнять аудит для тех объектов файловой системы, которые не представляют интереса.

11. После завершения настройки аудита для папки или файла нажмите несколько раз кнопку «ОК», чтобы закрыть все окна диалога (рисунок 3.7).

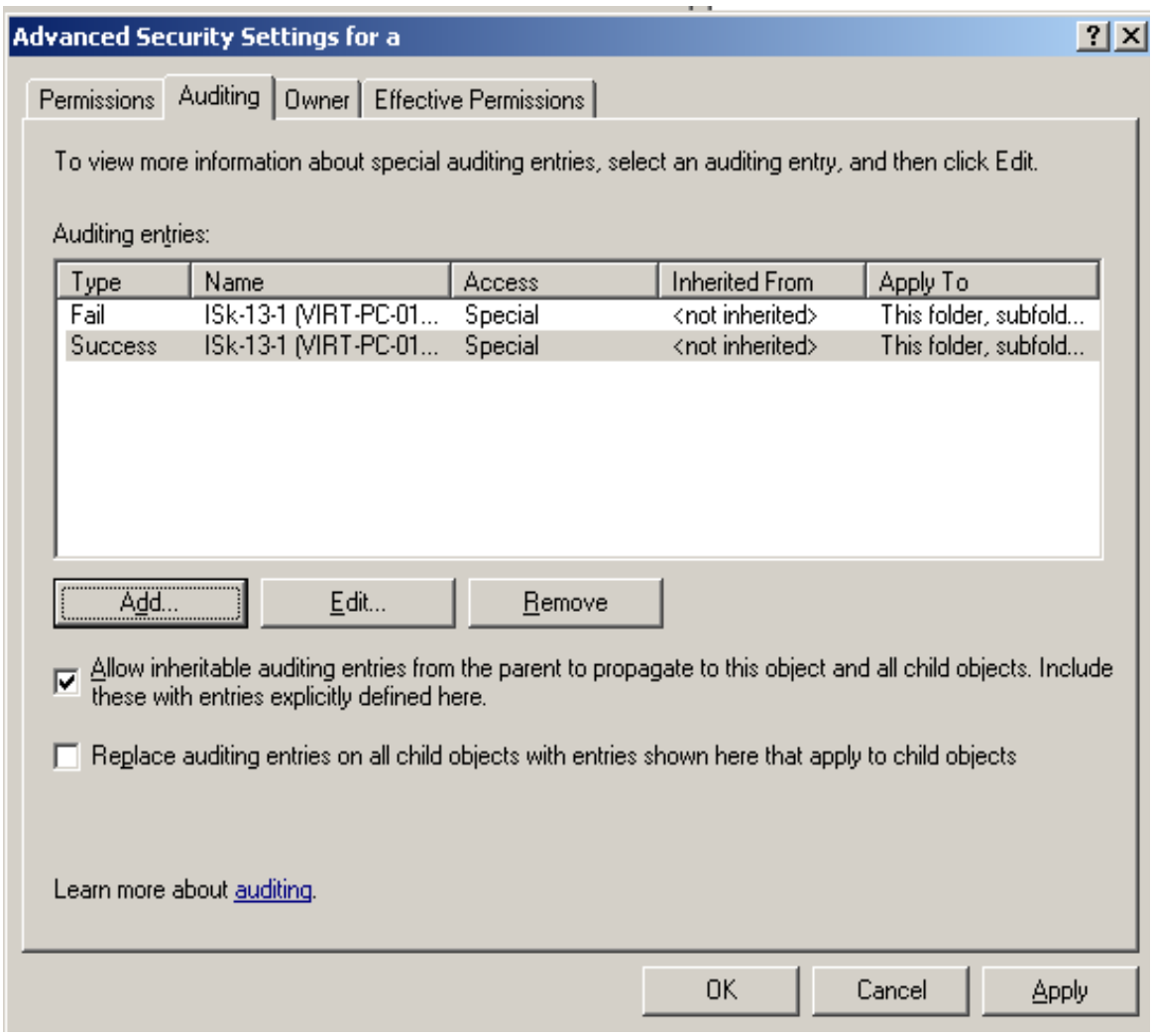

Рисунок 3.7 - Закрытие всех окон диалога

12. Если Вы хотите просмотреть или изменить настройки аудита для уже существующего пользователя или труппы, нажмите кнопку «Показать/Изменить». Появится окно диалога «Элемент аудита для». Здесь Вы сможете выполнить все необходимые изменения параметров аудита для выбранного Вами пользователя или группы. По окончании внесения изменений нажмите кнопку «ОК».

3.2.3 Просмотр событий в журнале событий.

1. Выберите кнопку «Пуск» панели задач.
2. Откройте меню «Настроить/Панель управления».
3. В открывшемся окне выберите ярлык «Администрирование» и далее «Просмотр событий» (рисунок 3.8).
4. В открывшемся окне выберите пункт «Безопасность».

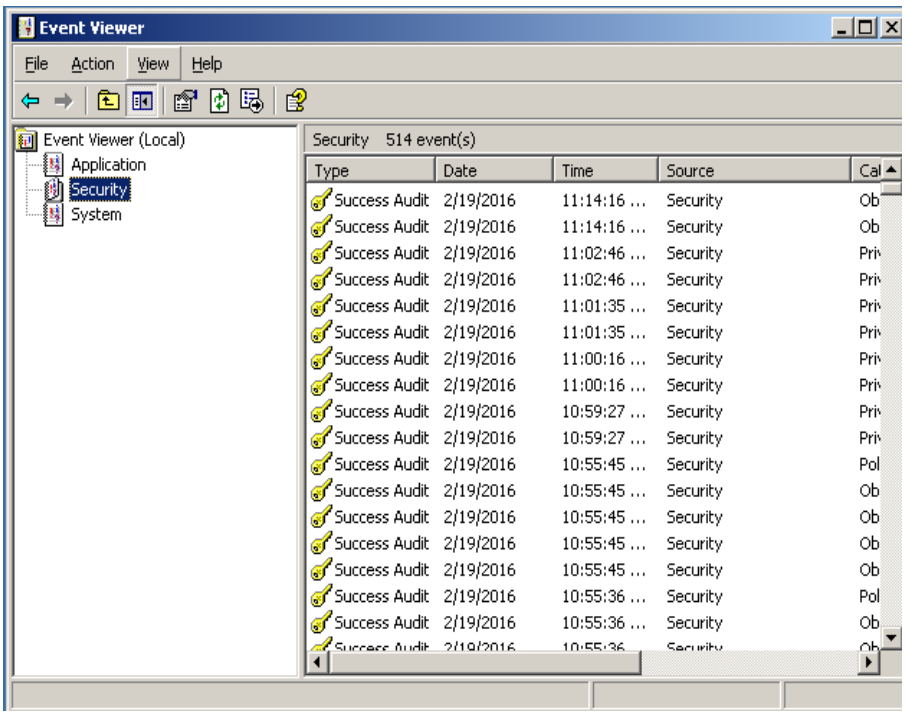

Рисунок 3.8 - Администрирование. Просмотр событий

5. В правой половине открытого окна появится список всех зарегистрированных событий.

6. Для просмотра требуемого события вызовите его свойства из контекстного меню или дважды щелкните по его названию левой клавишей мыши.

7. В результате появится окно, как показано на рисунке 3.9.

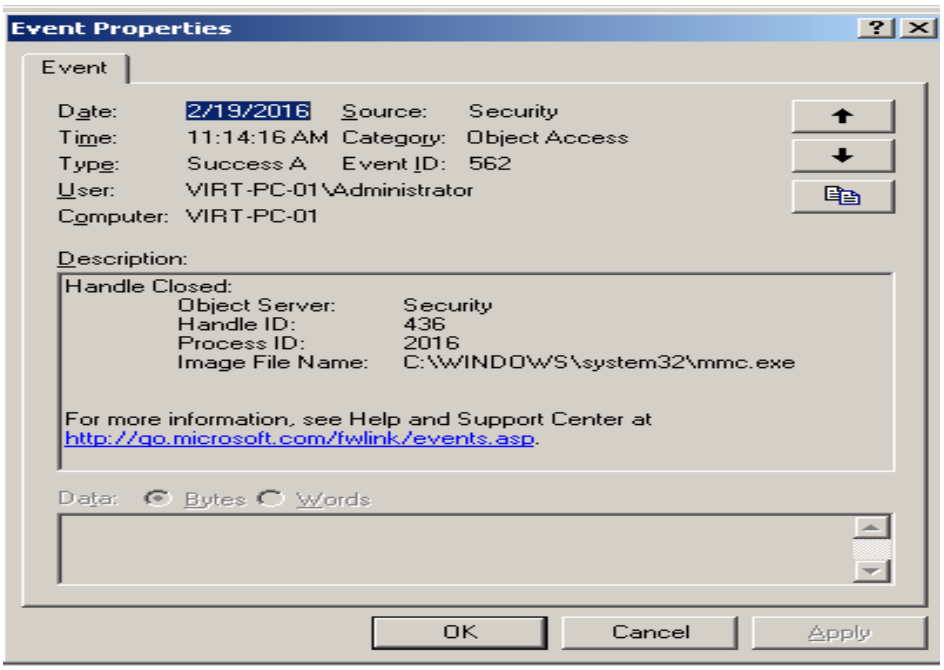

Рисунок 3.9 - Отключение учетной записи «Гость»

8. В показанном примере зафиксирован успех отключения учетной записи «Гость» пользователем «Admin» 8.05.04 в 18.28.31».

9. В примере, показанном на рисунке 3.10., зафиксирован отказ входа в систему пользователю NT AUTHORITY\SYSTEM (системная учетная запись) 08.05.04 в 17:39:58 по причине «неизвестное имя пользователя или неверный пароль».

10. Таким образом, просмотр журнала событий позволяет в полной мере проанализировать действия пользователей и процессов.

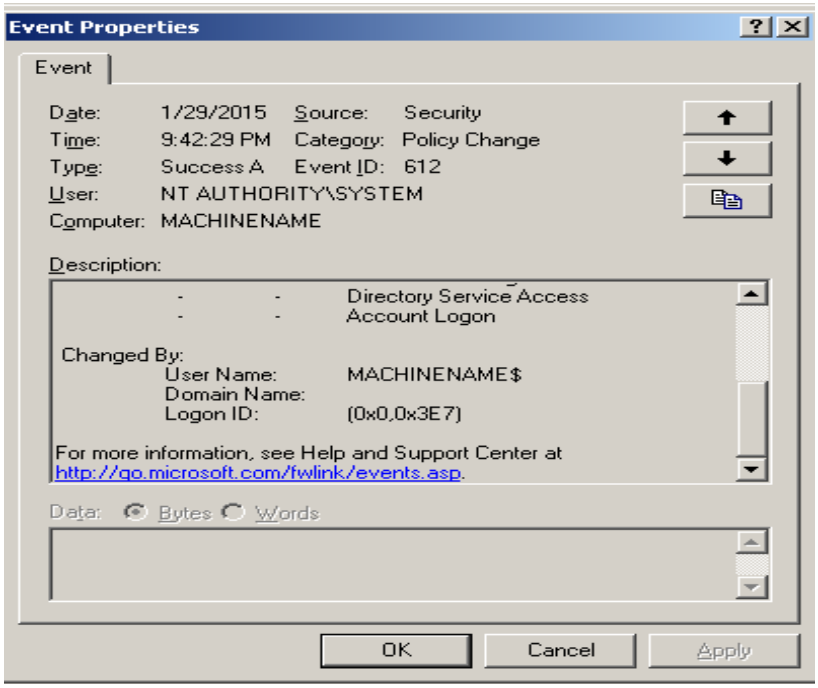

Рисунок 3.10 - Отказ входа в систему пользователя

3.3 Содержание отчета

Отчет о лабораторной работе должен содержать следующие разделы:
-цель работы;
-задание;
-краткое описание;
-создание учетной записи;
-изменение членства в локальной группе;
-временная блокировка учетной записи;
-выводы по работе.

3.4 Варианты заданий

Номер варианта	Параметры аудита	Значение аудита системы
1	событий входа в систему	успех
2	событий входа в систему	отказ
3	доступ к службе каталогов	доступа пользователя к AD
4	вход в систему	подключиться через сеть
5	доступ к объектам	раздел реестра
6	изменения политики	доверительные отношений
7	использования привилегий	право пользователя
8	отслеживания процессов	активизация программы
9	системных событий	журнал безопасности
10	управления учетными записями	удаление учетной записи

2.5 Контрольные вопросы

1. Чем отличаются регистрация и аудит?
2. Что является средствами регистрации и аудита?
3. Какие события фиксируются в системном журнале?
4. Что фиксирует система при регистрации событий?
5. Что такое надежность и безопасность ИС?
6. По каким трем основным уровням распределяются специальные методы и средства обеспечения надежности и информационной безопасности?
7. Какие средства обеспечения защиты информации вы знаете?
8. Что должен включать комплекс программно-технических средств и административных мер по обеспечению надежности информационной безопасности компьютерной сети предприятия?

4 Лабораторная работа№ 4. Управление шаблонами безопасности в Windows 2003(XP)

Цель работы: создания и редактирования текстовых файлов конфигурации безопасности операционной системы Windows 2003 (XP).

4.1 Задание к лабораторной работе

1. Создайте на базе существующего шаблона безопасности новый шаблон и дайте ему имя;

2. Зафиксировать список шаблонов;

3. Скопировать изображение экрана в буфер и далее в файл для отчета.

4.2 Порядок выполнения лабораторной работы

Управление шаблонами безопасности в Windows 2003 (XP) осуществляется с помощью «Редактора шаблонов безопасности», реализованного в виде оснастки MMC.

Он предназначен для создания и редактирования текстовых файлов конфигурации безопасности операционной системы Windows 2003 (XP). Такие файлы значительно легче переносятся с одной системы на другую, чем соответствующие им базы данных безопасности. Созданные при помощи оснастки «Шаблоны безопасности» текстовые файлы хранятся на жестком диске и при необходимости могут быть импортированы в базу данных безопасности. В этом случае все хранимые настройки безопасности начнут действовать.

Значения параметров обеспечения безопасности заносятся в текстовые файлы с расширением inf, называемые «Шаблонами безопасности».

4.2.1 Загрузка оснастки «Шаблоны безопасности».

1. Выберите кнопку «Пуск» в панели задач.
2. Перейдите к пункту «Выполнить».
3. В открывшемся окне в поле ввода введите команду «mmc».
4. В результате откроется консоль управления «mmc» (рисунок 4.1).

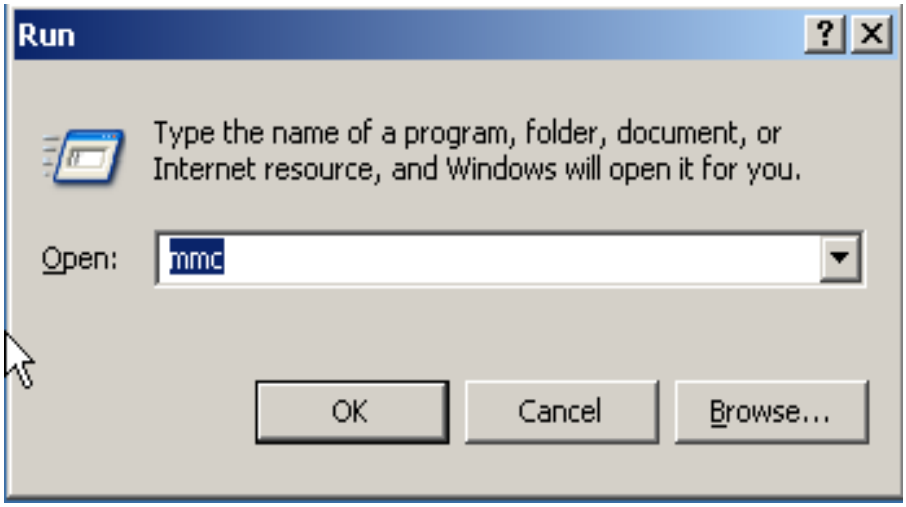

Рисунок 4.1- Консоль управления «mmc»

5. В меню «Консоль» выберите команду «Добавить» или удалить оснастку (рисунок 4.2) и нажмите кнопку «Добавить».

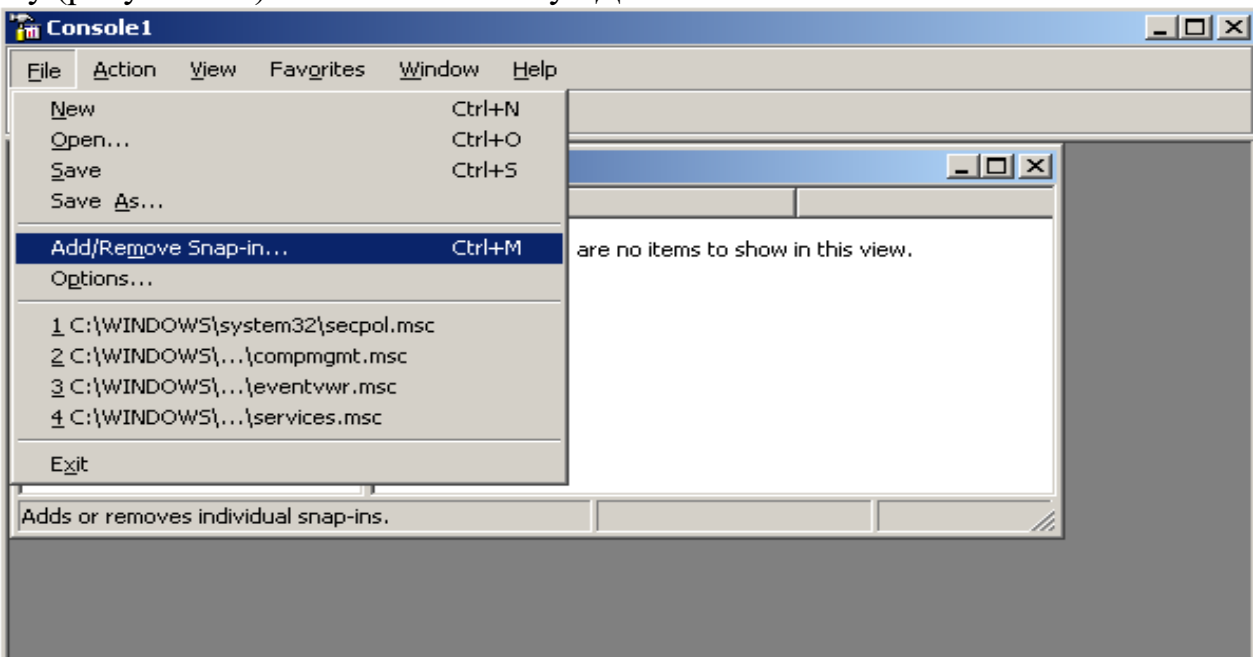

Рисунок 4.2 - Добавить или удалить оснастку

6. В поле «Оснастка» дважды щелкните «Шаблоны безопасности» (рисунок 4.3).

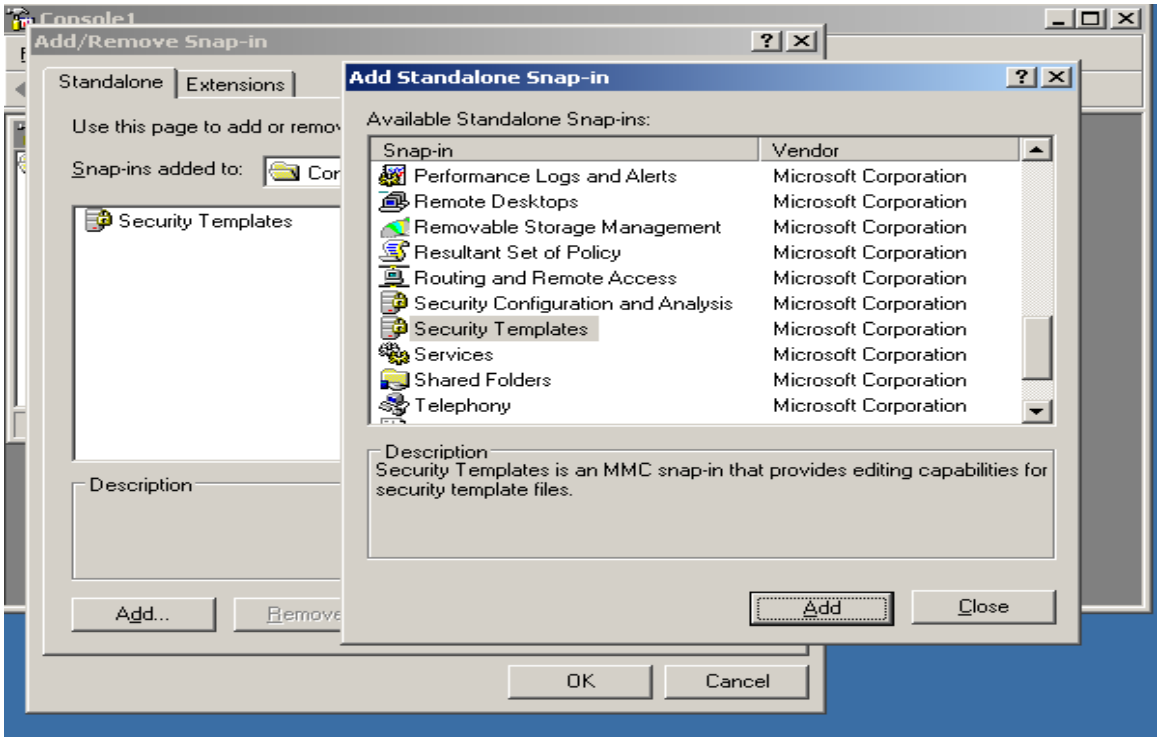

Рисунок 4.3- Шаблоны безопасности

7. Нажмите кнопку «Закрыть».

8. В списке выбранных оснасток для новой консоли появится элемент «Шаблоны безопасности».

9. Если на консоль не нужно добавлять другие оснастки, нажмите кнопку «ОК».

10. Чтобы сохранить эту консоль, в меню «Консоль» выберите команду «Сохранить» и укажите имя оснастки «Шаблоны безопасности».

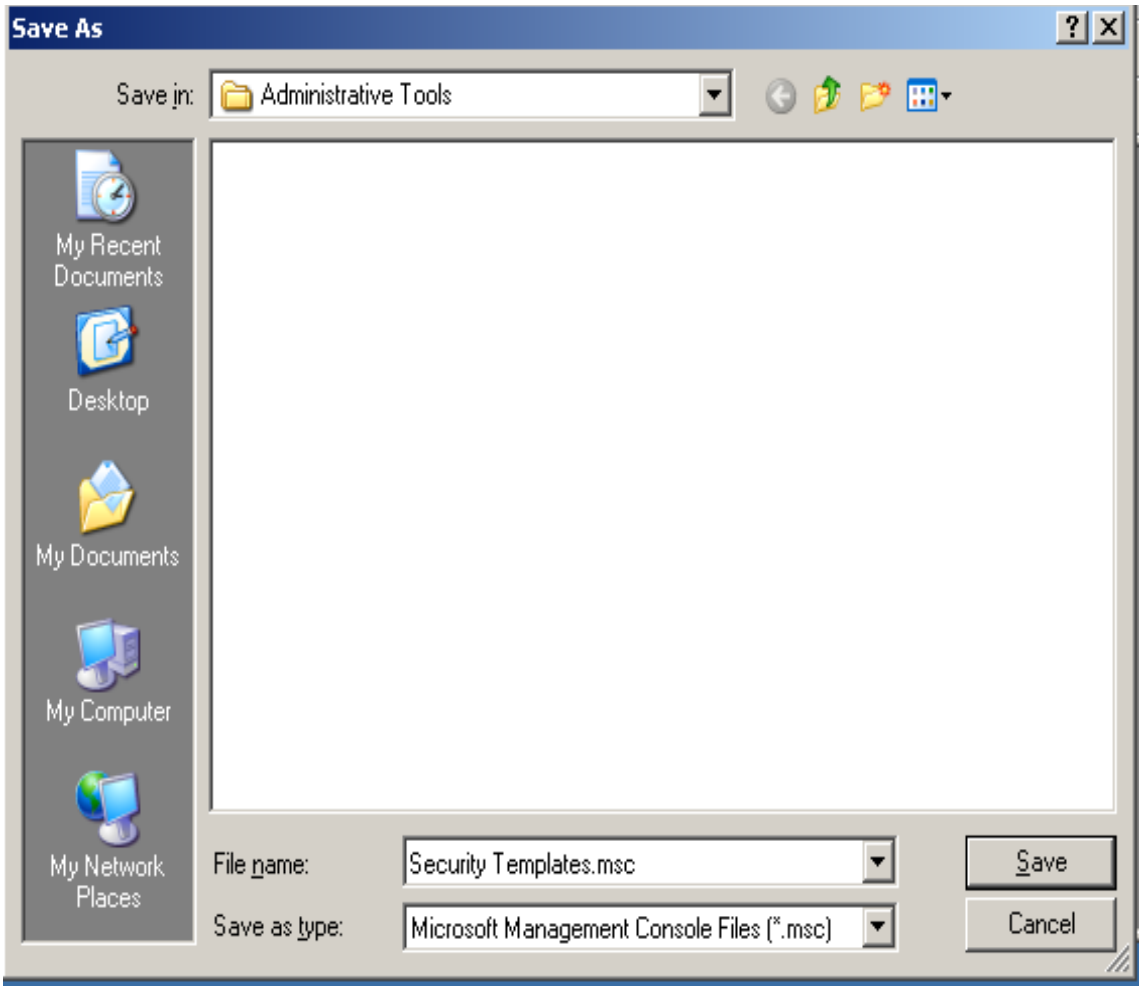

Рисунок 4.4 - Администрирование «Шаблона безопасности»

11. Закройте окно «Консоли» и выберите команду «Пуск» и далее «Все программы».

12. Найдите пункт «Администрирование» и выберите подпункт «Шаблоны безопасности» (Теперь оснастка с «Шаблоны безопасности» доступна в меню «Пуск» рисунок 4.4).

13. Для просмотра значений имеющихся шаблонов в окне оснастки откройте, например, узел «Шаблоны безопасности», щелчком выберите шаблон безопасности compatws и просмотрите его папки «Политика учетных записей», «Локальная политика» и др.

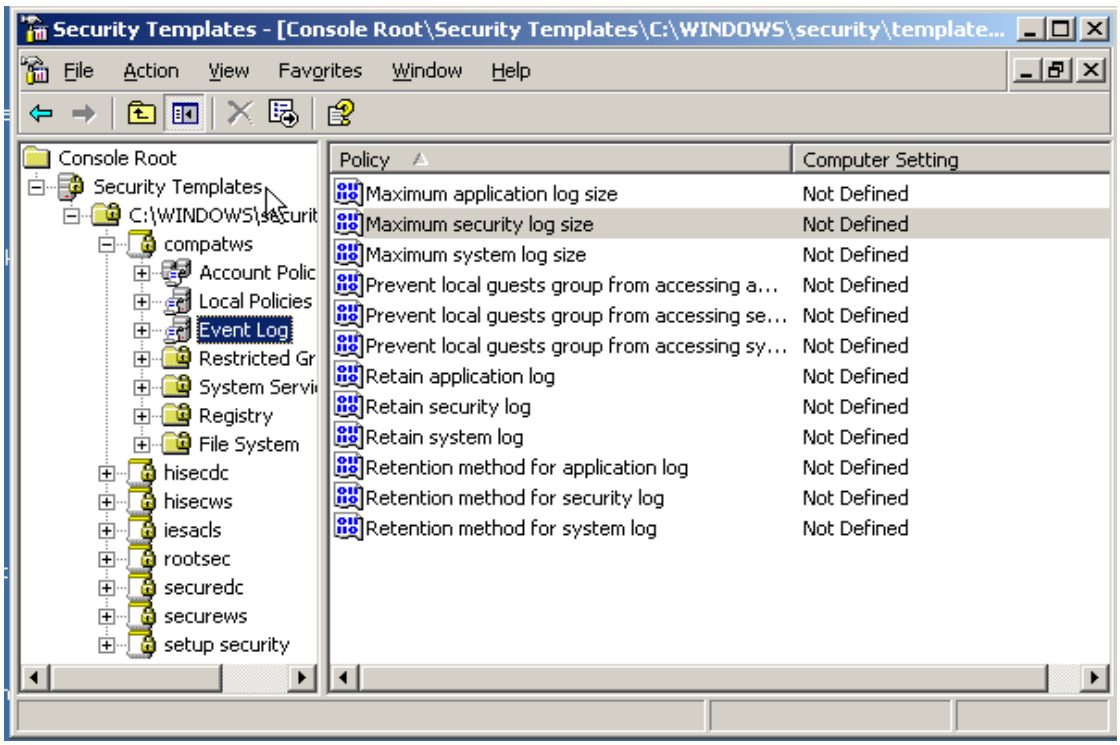

Рисунок 4.5- Оснастка «Шаблона безопасности»

4.2.2 Редактирование и сохранение шаблона безопасности.

1. Щелкните на одном из стандартных шаблонов безопасности (например, compatws) (рисунок 4.5), которые Вы видите в окне оснастки «Шаблоны безопасности».

2. Если Вы хотите модифицировать какую-либо настройку безопасности, дважды щелкните на ней и отредактируйте значения параметров (рисунок 4.6).

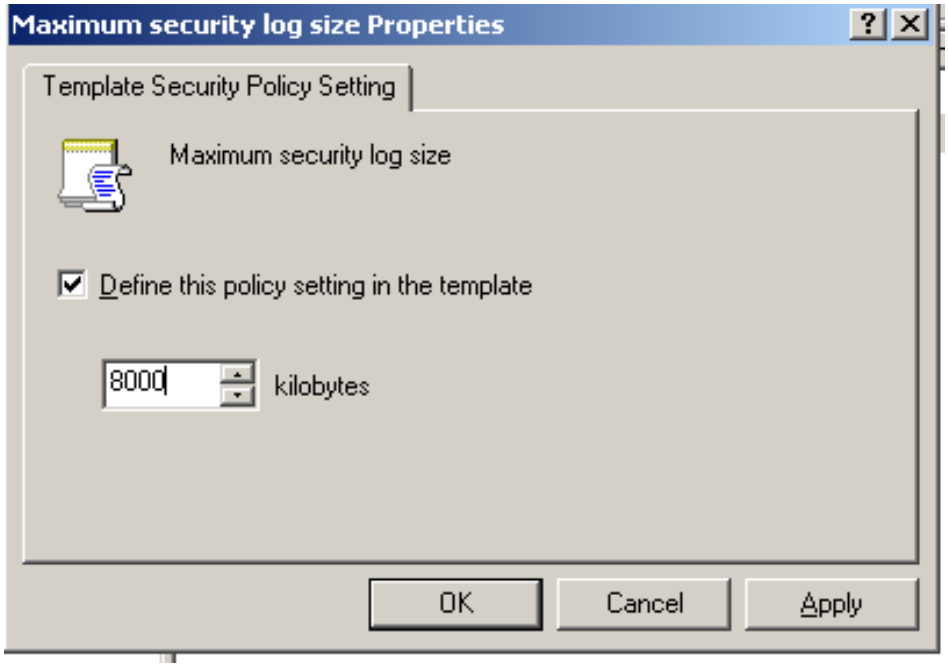

Рисунок 4.6 - Редакция значения параметров

3. Для сохранения откорректированного стандартного шаблона безопасности под другим именем выполните следующие действия.

4. Укажите откорректированный стандартный шаблон (например, compatws), и нажмите правую кнопку мыши.

5. В появившемся контекстном меню выберите команду «Сохранить как».

6. Введите с клавиатуры новое имя файла (например, custom). По умолчанию шаблоны безопасности располагаются в каталоге *Templates*. (рисунок 4.7.)

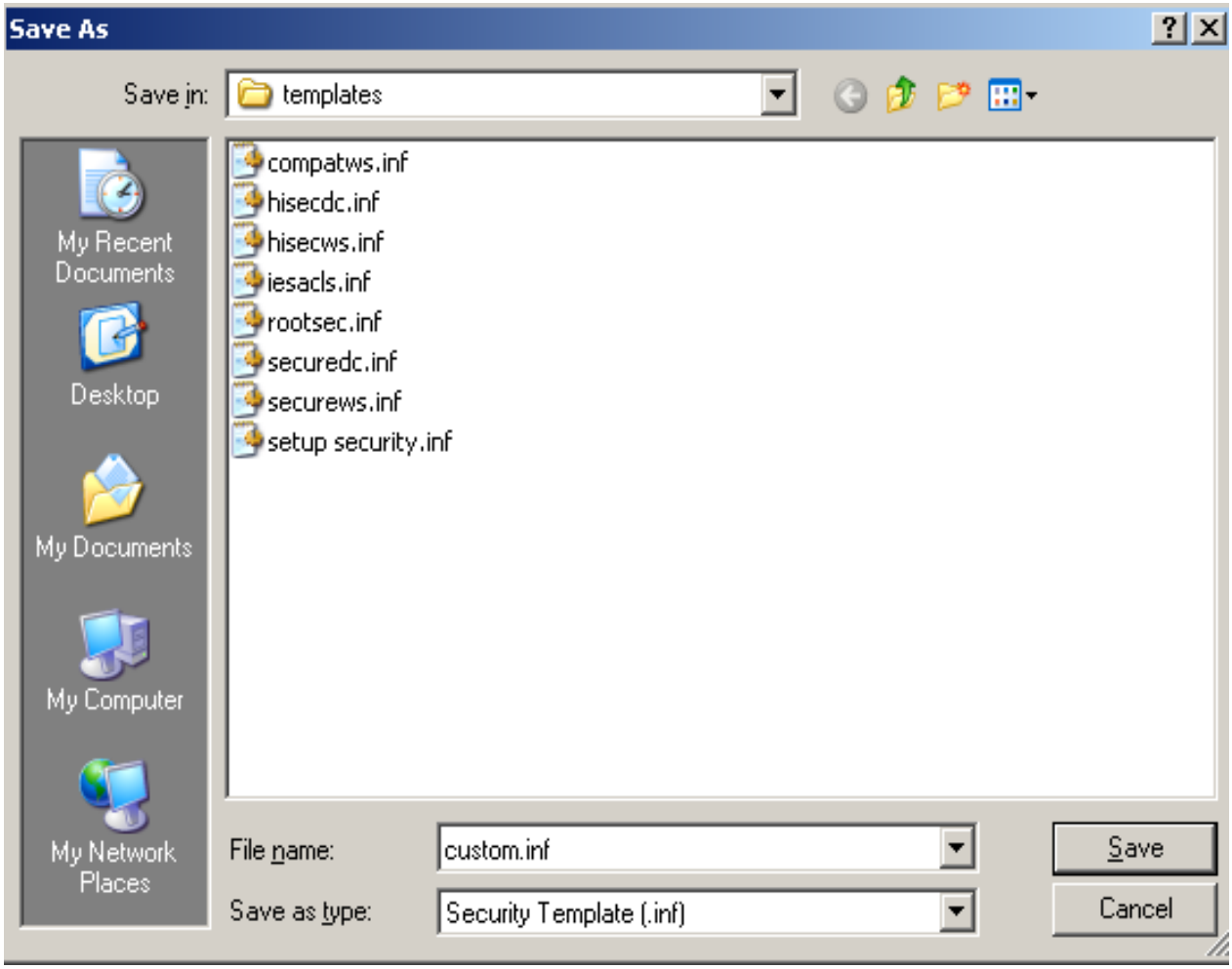

Рисунок 4.7 - Каталог шаблона безопасности

7. Пользовательский шаблон будет добавлен в определенную заранее конфигурацию безопасности и сохранен под введенным Вами именем.

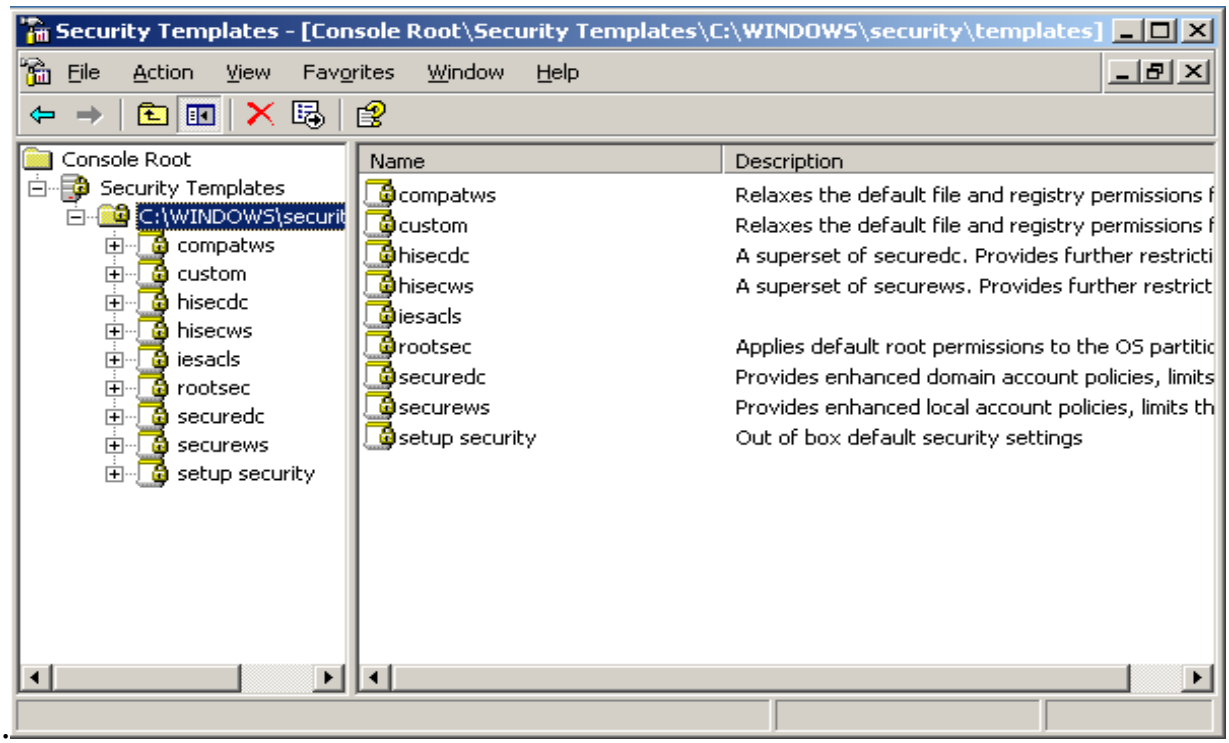

Рисунок 4.8 – Настройка шаблона безопасности

Настроив «Шаблон безопасности» для одной ПЭВМ, Вы можете перенести его и на другие ПЭВМ Вашей рабочей группы. Шаблоны безопасности являются гибким и удобным инструментом по настройке системы безопасности операционной системы.

4.3 Содержание отчета

Отчет о лабораторной работе должен содержать следующие разделы:
-цель работы;
-задание;
-краткое описание;
-загрузка оснастки шаблоны безопасности;
-редактирование и сохранение шаблона безопасности;
-настройка шаблона безопасности;
-выводы по работе.

4.4 Варианты заданий

Номер варианта	В текстовые файлы с расширением inf,внесите команды и выберите правильную оснастку	В шаблоне безопасности «compatws» выберите имя файла
1	добавить оснастку	custom
2	удалить оснастку	caste
3	закрыть оснастку	compare
4	другие оснастки	game
5	сохранить оснастку	rubber
6	удалить оснастку	custom
7	другие оснастки	caste
8	добавить оснастку	compare
9	сохранить оснастку	rubber
10	закрыть оснастку	game

4.5 Контрольные вопросы

1. Для чего используются «Шаблоны безопасности»?
2. В каком месте на диске хранятся (по умолчанию) шаблоны безопасности?
3. Какие разделы включает стандартный «Шаблон безопасности»?
4. В каком случае увеличивается степень защищенности компьютера?
5. Где в каталоге располагаются по умолчанию шаблоны безопасности?
6. Предназначение оснастки ММС?
7. Где хранятся текстовые файлы оснастки «Шаблоны безопасности»?

5 Лабораторная работа№ 5. Конфигурации системы реестра операционной системы Windows 2003 (XP)

Цель работы: изучить работу в реестре.

5.1 Задание к лабораторной работе

1. Проверьте содержимое ключа HKEY_LOCAL_MACHINE\Software\Microsoft\WindowsNT\CurrentVersion\Winlogon\System(REG.SZ).

2. Зафиксируйте этапы работы, используя команду PrintScreen клавиатуры.

3. Составьте отчет о результатах проверки.

5.2 Порядок выполнения лабораторной работы

Основным средством для просмотра и редактирования записей реестра служит специализированная утилита «Редактор реестра».

Файл редактора реестра находится в папке Windows. Называется он regedit.exe. После запуска появится окно редактора реестра. Вы увидите список из 5 разделов (рисунок 5.1):

HKEY_CLASSES_ROOT
HKEY_CURRENT_USER
HKEY_LOCAL_MACHINE
HKEY_USERS
HKEY_CURRENT_CONFIG

Работа с разделами реестра аналогична работе с папками в «Проводнике». Конечным элементом дерева реестра являются ключи или параметры, делящиеся на три типа (рисунок 5. 2):

- строковые (напр. «C:\\Windows»);
- двоичные (напр. 10 82 AO 8F).

DWORD — этот тип ключа занимает 4 байта и отображается в шестнадцатеричном и в десятичном виде (например, 0x00000020 (32)).

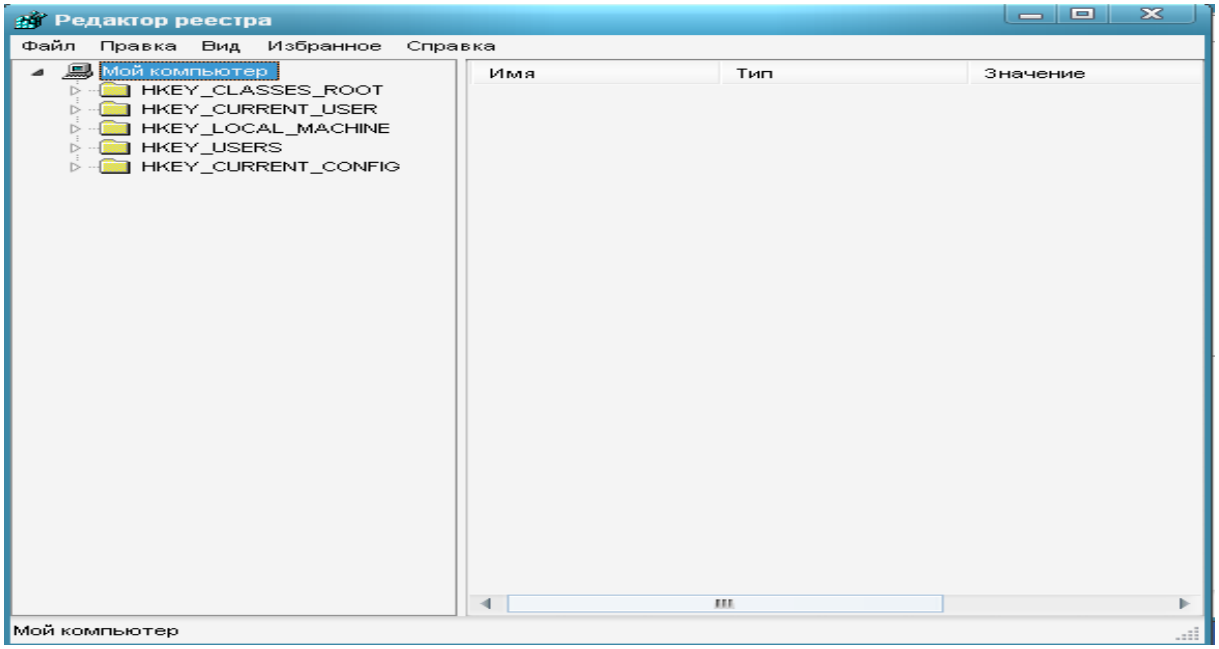

Рисунок 5.1- Разделы реестра

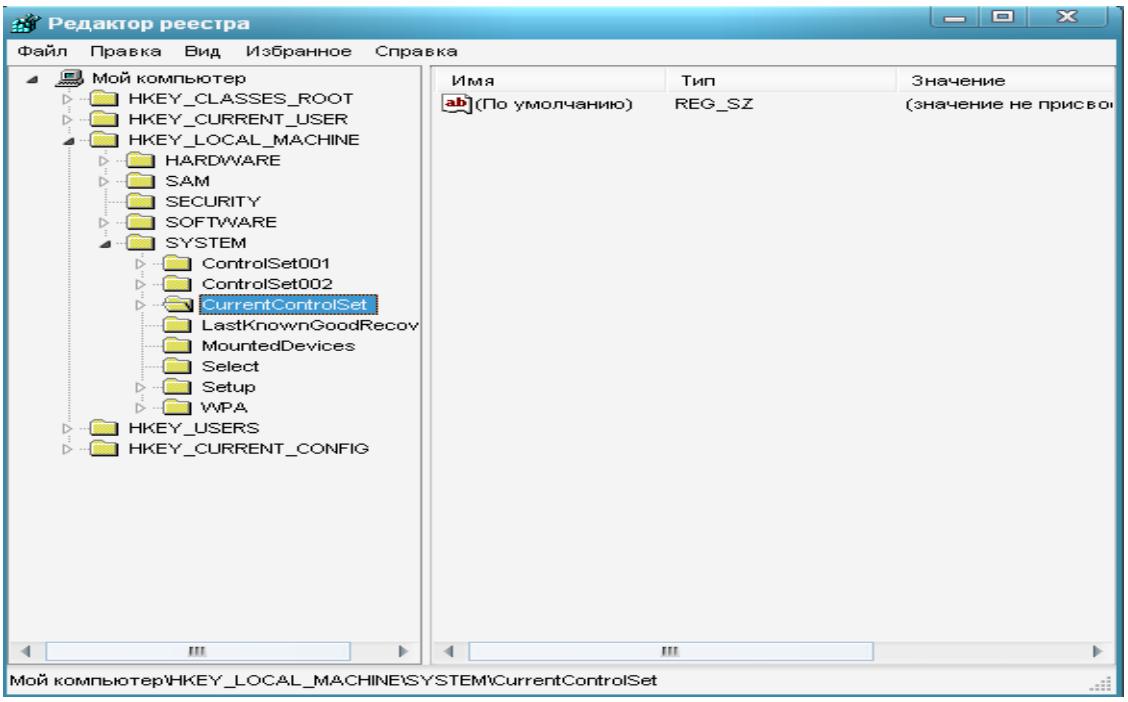

Рисунок 5.2 - Параметры реестра

В Windows системная информация разбита на так называемые ульи (hive), Это обусловлено принципиальным отличием концепции безопасности этих операционных систем. Имена файлов ульев и пути к каталогам, в которых они хранятся, расположены в разделе «Редактор реестра» HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\hivelist (рисунок 5.3).

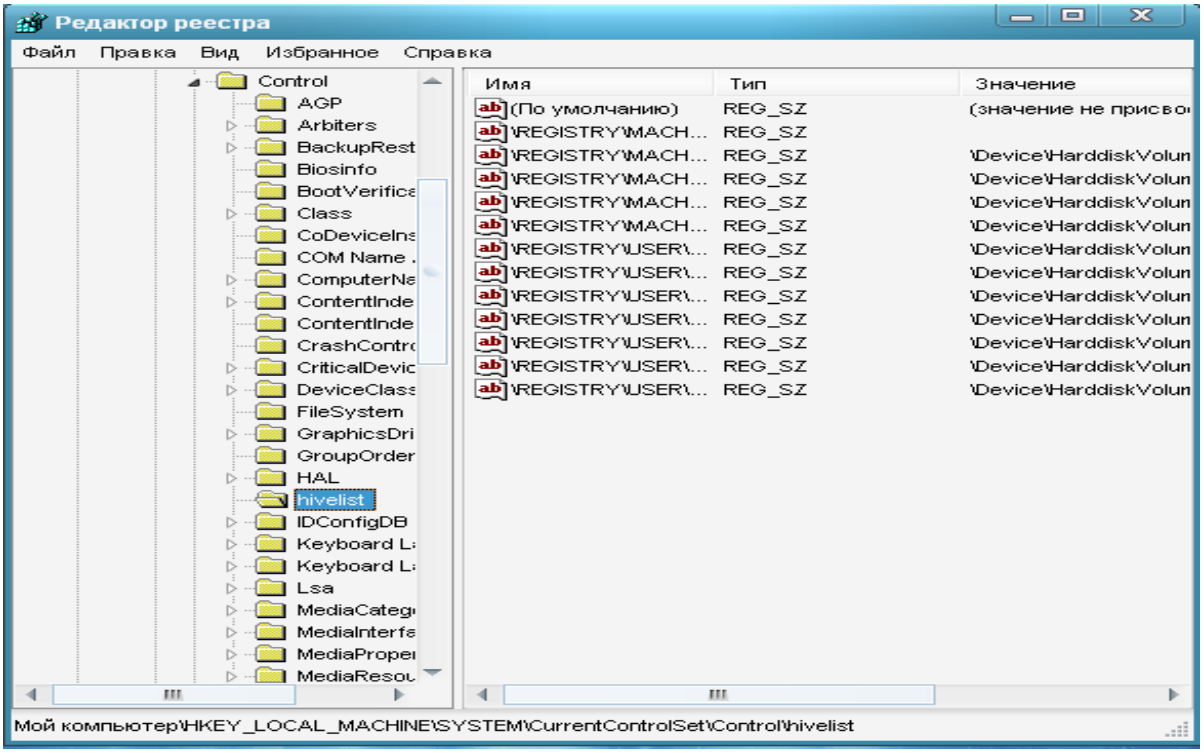

Рисунок 5.3 – Редактор реестра

Краткие описания ульев реестра и файлов, в которых хранятся параметры безопасности и технические характеристики.

Потенциальными местами записей «троянских программ» в системном реестре являются разделы, описывающие программы, запускаемые автоматически при загрузке операционной системы от имени пользователей и системы.

1. Запустите программу regedit.exe.

2. В открывшемся окне выберите ветвь HKEY_LOCAL_MACHINE и далее Software\Microsoft\ WindowsNT\CurrentVersion\Vinlogon.

3. В правой половине открытого окна программы regedit.exe появится список ключей.

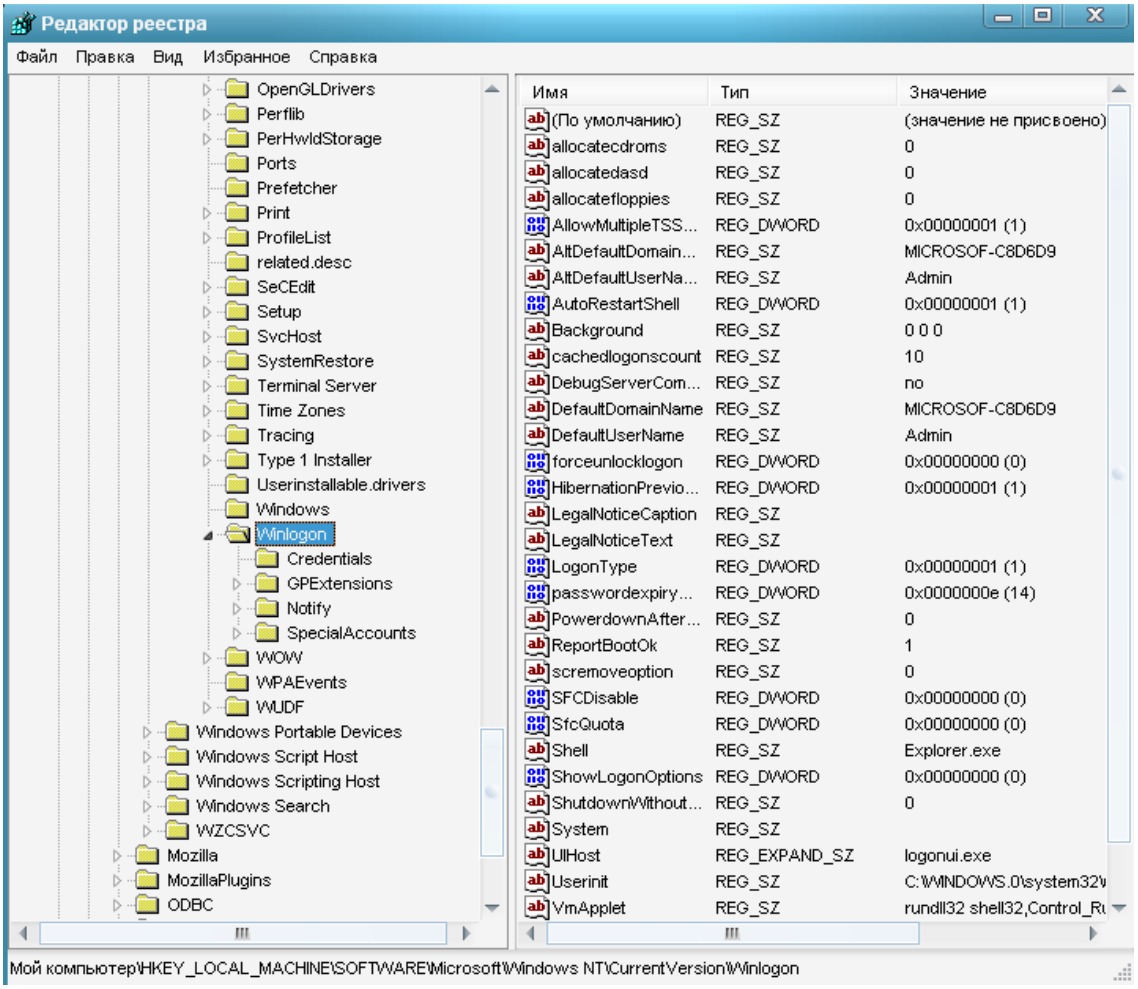

Рисунок 5.4 - C:\WINDOWS\system32\usernit.exe

4. Найдите ключ Userinit (REG_SZ) и проверьте его содержимое.

5. По умолчанию (исходное состояние) 151 этот ключ содержит, следующую запись C:\WINDOWS\system32\usernit.exe (рисунок 5.4).

6. Если в указанном ключе содержатся дополнительные записи, то это могут быть «троянские программы».

7. В этом случае проанализируйте место расположения программы, обратите внимание на время создания файла и сопоставьте с Вашими действиями в это время.

8. Если время создания файла совпадает со временем Вашей работы в Интернете, то возможно, что в это время Ваш компьютер был заражен «троянским конем».

9. Для удаления этой записи необходимо дважды щелкнуть на названии ключа (или при выделенном ключе выбрать команду «Изменить» из меню «Правка» программы regedit.exe).

10. В открывшемся окне в поле «Значение» (рисунок 5.5) удалите ссылку на подозрительный файл.

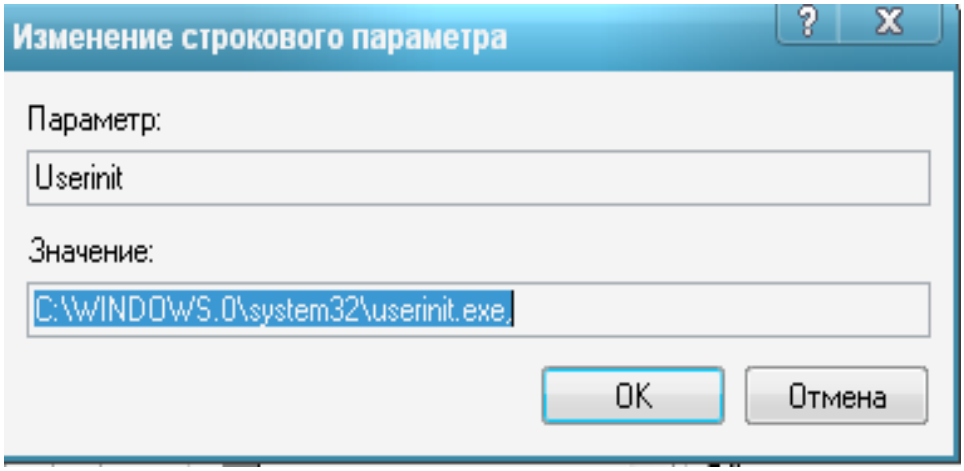

Рисунок 5.5 - Удаление ссылки на подозрительный файл.

11. Закройте программу regedit.exe.

12. Перейдите в папку с подозрительным файлом и удалите его.

13. Перезагрузите операционную систему и выполните пункты задания 1-4.

14. Если содержимое рассматриваемого ключа не изменилось, то предполагаемый «троянский конь» удален из Вашей системы.

Еще одним потенциальным местом записей на запуск «троянских программ» является раздел автозапуска RUN.

Для его проверки выполните следующее:

1) Запустите программу regedit.exe.

2) В открывшемся окне выберите ветвь HKEY_LOCAL_MACHINE и далее Software\Microsoft\ WindowsNT\CurrentVersion\Run\... (REG_82) (рисунок 5.6).

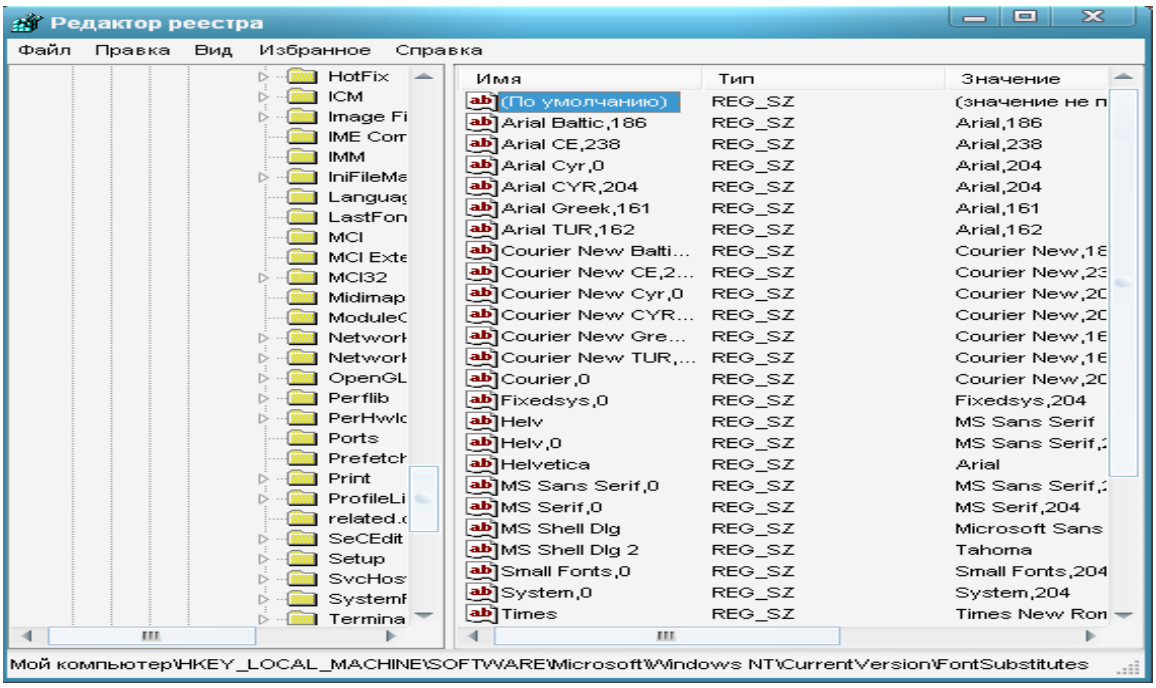

Рисунок 5.6 - Редактор реестра

15. В рассматриваемом примере автоматически запускается резидентный антивирус и его планировщик заданий, а также утилита, относящаяся к программе Nero (запись на CD).

16. Если в указанном разделе есть записи вызывающие подозрения, то выполните пункты 6-14 предыдущего задания.

5.3 Содержание отчета

Отчет о лабораторной работе должен содержать следующие разделы:
-цель работы;
-задание;
-краткое описание;
-запустите программу regedit.exe;
-выбрать ветвь безопасности;
-перезагрузить операционную систему;
выводы по работе.

5.4 Варианты заданий

Номер варианта	Основные разделы системного реестра	Улья реестра, в которых хранятся параметры безопасности
1	Hkey_local_machine\ System	System.log,
2	Hkey_current_config	System.sav
3	Hkey_users\.default	Default.log
4	Hkey_current_user	Ntuser.dat
5	Hkey_local_machine\ Sam	Sam
6	Hkey_local_machine\ System	System.log,
7	Hkey_users\.default	Default.log
8	Hkey_current_config	System.sav
9	Hkey_local_machine\ Sam	Sam
10	Hkey_current_user	Ntuser.dat

5.5 Контрольные вопросы

1. Что представляет собой реестр?
2. Возможна ли работа операционной системы без реестра?
3. В чем проявляется динамичность реестра?
4. Какую структуру имеет реестр?
5. Что означает защищенность реестра?
6. Из чего состоит реестр WindowsXP ?
7. Какие разделы (ключи) содержат поддеревья реестра?
8. Какие возможности предоставляет редактор реестра?

6 Лабораторная работа № 6. Инструменты администрирования и управления серверной системой

Цель работы: изучить основные инструментальные средства Windows Server 2003, предназначенные для управления системой и контроля над действиями пользователей.

6.1 Задание к лабораторной работе

1. Изучить теоретический материал по данной теме.

2. Установить домен Active Directory (сделать сервер контроллером домена).

3. Проверить правильность установки контроллера домена.

6.2 Порядок выполнения лабораторной работы

При построении и настройке компьютерных сетей учитывается их физическая и логическая топология. Физическая топология определяет набор сетевого оборудования, включая кабельные системы и коммуникационное оборудование, который необходим для физического объединения компьютеров в сеть. Логическая топология определяется настройками сетевых протоколов и программ, позволяющими конфигурировать информационные потоки между компьютерами сети. Рабочая группа - это средство поддержки сетевого окружения, входящее в состав Microsoft Windows.

Компьютеры рабочей группы совместно используют общие ресурсы, такие как файлы и принтеры. Для упрощения администрирования любые компьютеры сети и разделяемые ресурсы можно объединять в группы, называемые доменами. Домен - это логическая группировка любых компьютеров сети под одним именем. Домен может объединять любые компьютеры, расположенные в локальной сети или находящиеся в разных городах, странах. Физическое соединение компьютеров домена может быть любым, включая телефонные линии, оптоволоконные линии, спутниковую связь и другие. Служба каталога «Active Directory» разворачивается на любом сервере, входящем в состав сети. Такой сервер получает дополнительно статус *«контроллера домена».* Администрирование сети и управление политиками безопасности осуществляется на контроллере домена. Доменов в сети может быть несколько, и каждый домен обязательно имеет один или несколько контроллеров домена.

Если контроллеров домена несколько, то база данных «Active Directory» копируется на каждый. Это повышает отказоустойчивость и делает администрирование более удобным, так как все изменения, проведенные на одном контроллере домена, отображаются на других. Этот процесс называется *репликацией.*

6.2.1 Установка домена Active Directory.

1. Запустить виртуальную машину.

2. Запустить программу «Управление данным сервером», если она не запустилась автоматически: «Пуск» – «Администрирование» – «Управление данным сервером» (рисунок 6.1).

3. В открывшемся окне «Управление данным сервером» запустить мастер настройки сервера, выбрав «Добавить или удалить роль».

Рисунок 6.1 - Запуск программы «Управление данным сервером»

5. В диалоговом окне выбрать «Параметры настройки», отметить пункт «Особая конфигурация» и нажать кнопку «Далее».

6. Выбрать роль «Контроллер домена (Active Directory)», после чего посмотреть и подтвердить выбранные параметры.

7. Запустится «Мастер установки Active Directory». Нажать кнопку «Далее».

8. Прочитать сведения, приведенные в диалоговом окне «Совместимость с операционными системами», и нажать кнопку «Далее».

9. В диалоговом окне «Тип контроллера домена» выбрать переключателем пункт «Контроллер домена в новом домене» и нажать кнопку «Далее» (рисунок 6.2).

10. В диалоговом окне «Создать новый домен» оставить переключатель в положении «Новый домен в новом лесу».

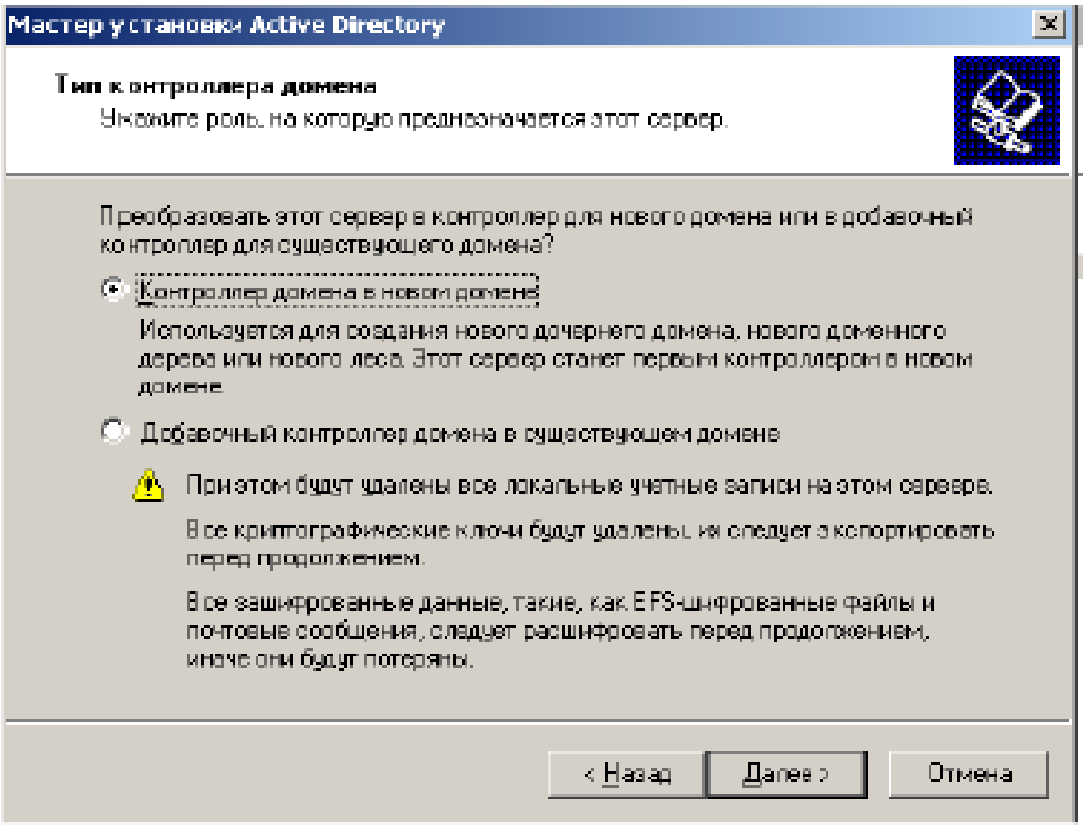

Рисунок 6.2 - Окно «Тип контроллера домена»

11. В диалоговом окне «Новое имя домена» в поле «Полное DNS-имя нового домена» введите: *имя.is4.local* (вместо слова «*имя*» подставить уникальное имя, состоящее из латинских букв и цифр не длиннее 63 байт).

12. В диалоговом окне «NetBIOS-имя домена» оставить имя по умолчанию.

13. В диалоговом окне «Папки базы данных и журналов» оставить предложенный путь C:\WINDOWS\NTDS для базы данных и C:\WINDOWS\NTDS для журнала. С точки зрения оптимизации работы контроллера домена, выгоднее помещать файлы базы данных и журнала на разные физические диски.

14. В диалоговом окне «Общий доступ к системному тому» оставить предложенный путь C:\WINDOWS\SYSVOL.

15. Внимательно ознакомиться с содержимым диалогового окна «Диагностика регистрации DNS» и, установив переключатель в положение

«Проблема будет решена позже ручной настройкой DNS», продолжить работу «Мастера установки Active Directory».

16. В появившемся диалоговом окне «Разрешения» отметить пункт

«Разрешения, совместимые только с Windows 2000 или Server Windows Server 2003».

17. В диалоговом окне «Пароль администратора для режима восстановления» задайте в поле «Пароль режима восстановления» и в поле

«Подтверждение» пароль «*vo$t@nD#1*», который будет использоваться при восстановлении базы данных Active Directory. При установке дополнительного контроллера домена следует выбрать для него другой пароль восстановления, например «*vo$t@nD#2*».

18. В диалоговом окне «Сводка» проверить исправность настроек всех параметров домена Active Directory. При выявлении ошибок вернуться к диалоговому окну и исправить необходимые параметры. Нажать кнопку «Далее» для запуска дальнейшего процесса установки контроллера домена.

19. Завершить установку нажатием кнопки «Готово».

20. По окончании работы «Мастера установки Active Directory» перезагрузить компьютер.

6.2.2 Проверка правильности установки контроллера домена.

1. Поочередно открыть добавленные консоли и изучить их содержимое.

2. Открыть консоль «Просмотр событий» и убедиться в добавлении пунктов «Служба каталогов» и «Служба репликации файлов».

3. Выбрать пункт «Служба репликации файлов», найти событие «13516» и вывести на экран диалоговое окно «Свойства: Уведомление» (рисунок 6.3), в котором сообщается, что контроллер домена выполняет свои функции.

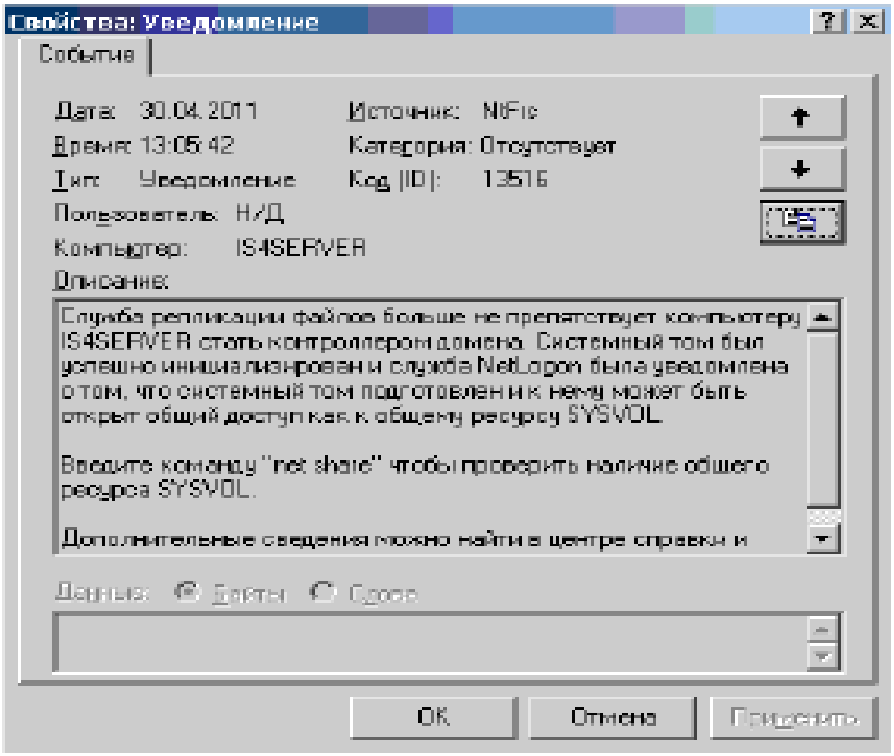

Рисунок 6.3 - Событие «13516» в журнале службы репликации файлов

6.3 Содержание отчета

Отчет о лабораторной работе должен содержать следующие разделы:

-цель работы;

-задание;
-краткое описание;
-установка домена Active Directory;
-проверка правильности установки контроллера домена;
-открыть консоль «просмотр событий» и убедиться в добавлениях;
-выводы по работе.

6.4 Варианты заданий

Номер варианта	Пароль режима восстановления	Пароль дополнительного контроллера домена
1	vo$t@nD#1	vo$t@uD#8
2	vo$t@nf#2	vo$t@yD#9
3	vo$t@nD#3	vo$t@tD#6
4	vo$t@nh#4	vo$t@kD#7
5	vo$t@na#5	vo$t@rD#11
6	vo$t@nh#6	vo$t@yD#9
7	vo$t@nD#7	vo$t@uD#8
8	vo$t@nD#9	vo$t@tD#6
9	vo$t@nf#8	vo$t@rD#11
10	vo$t@na#11	vo$t@kD#7

6.5 Контрольные вопросы

1. Какие топологии логических связей можно использовать при создании компьютерных сетей?
2. Назовите достоинства и недостатки одноранговых сетей и сетей с выделенным сервером.
3. Что такое «Рабочая группа» (*workgroup)* и для чего она используется?
4. Какие функции (роли) выполняет выделенный сервер?
5. Что такое домен?
6. Как называется база данных для домена в Windows Server 2003?
7. Какой статус получает сервер, на котором разворачивается служба каталога «Active Directory»?
8. Почему выгоднее помещать файлы базы данных и журнала на разные физические диски?

7 Лабораторная работа №7. Создание учетных записей пользователей и групп в среде ОС Linux. Организация рабочей среды пользователя

Цель работы: изучить команды, связанные с пользователями и группами при установке ОС Linux.

7.1 Задание к лабораторной работе

1. Создать каталог «Группа» и перейти в новый каталог.
2. В каталоге «Группа» создать текстовый файл *работа_1.txt*, в котором введите дату выполнения работы.
3. Выведите на экран содержимое созданного файла.
4. В том же каталоге создать каталог «Номер подгруппы». Скопировать файл *работа_1.txt* в каталог «Номер подгруппы».

4.2 Порядок выполнения лабораторной работы

Линукс позволяет одновременно работать различным пользователям. Для обеспечения такой возможности используется концепция терминалов. Лабораторная работа выполняется в командной строке (часто используются термины «терминал» или «консоль»), результат работы с объектами можно проверить в любом установленном оконном менеджере. Командная строка начинается приглашением - подсказка, свидетельствующая о том, что система готова принимать команды пользователя от какого-либо пользователя. Приглашение чаще всего оно заканчивается символом “$”(права обычного пользователя) или “#”(супер пользователь). Например, в приглашении root@kate-desktop:/home/kate#до ”@” - имя пользователя; между “@” и “:” - имя домена; после “:” - путь к папке, где находится текущий пользователь. Команды в терминале выводят информацию на экран, в файл, можно использовать метасимволы для формирования сложных команд: а) > - запись в файл.б >> - до запись в конец существующего файла; з) && - при объединении команд: последующая команда выполняется только при нормальном завершении предыдущей; иногда возникает необходимость выполнить некоторые действия от имени другого пользователя (например, от имени root). Это можно сделать, открыв новый терминальный сеанс, но можно и иначе, в текущем сеансе. Для этого используется команда su. Эта команда по умолчанию (без параметров) открывает сеанс супер пользователя, выполняющийся *внутри сеанса* непривилегированного пользователя. Пример выполнения команды su:

```
[aag@localhost ~]$ su
Password:
[root@localhost aag]#
```

Дополнительная информация об указанных командах доступна в справочном руководстве формата man или info. Для того, чтобы создать каталог «Группа», нужно перейти в новый каталог. В каталоге «Группа» создайте текстовый файл *работа_1.txt*, в котором введите дату выполнения работы. Выведите на экран содержимое созданного файла. В том же каталоге создать каталог «Номер подгруппы». Скопировать файл *работа_1.txt*в каталог «Номер подгруппы». В каталоге «Группа» создать текстовый файл *имя студента.txt*, который будет содержать ФИО студентов, выполняющих работу. Объединить содержимое файлов *имя студента.txt* и *работа_1.txt* и сохранить в файл *ФИО студента. txt*. В каталоге «Группа» создать каталог \command. В каталоге command создать командный файл, который бы выводил на экран количество работающих пользователей.

7.2.1 Создание учетной записи.

Введите команду whoami. Залогиниться в терминале под суперпользователем (root). Для создания каталогов пользуются командой mkdir . Откройте новый терминальный сеанс с паролем.

Sudo su, password (пароль):123456789

Mkdir: Создание папки

Cd Название папки: Вход в папку

Cd ..: Выход с папки

Cat >: Добавить текст

После ввода текста Ctrl+C (копировать) (рисунок 7.1).

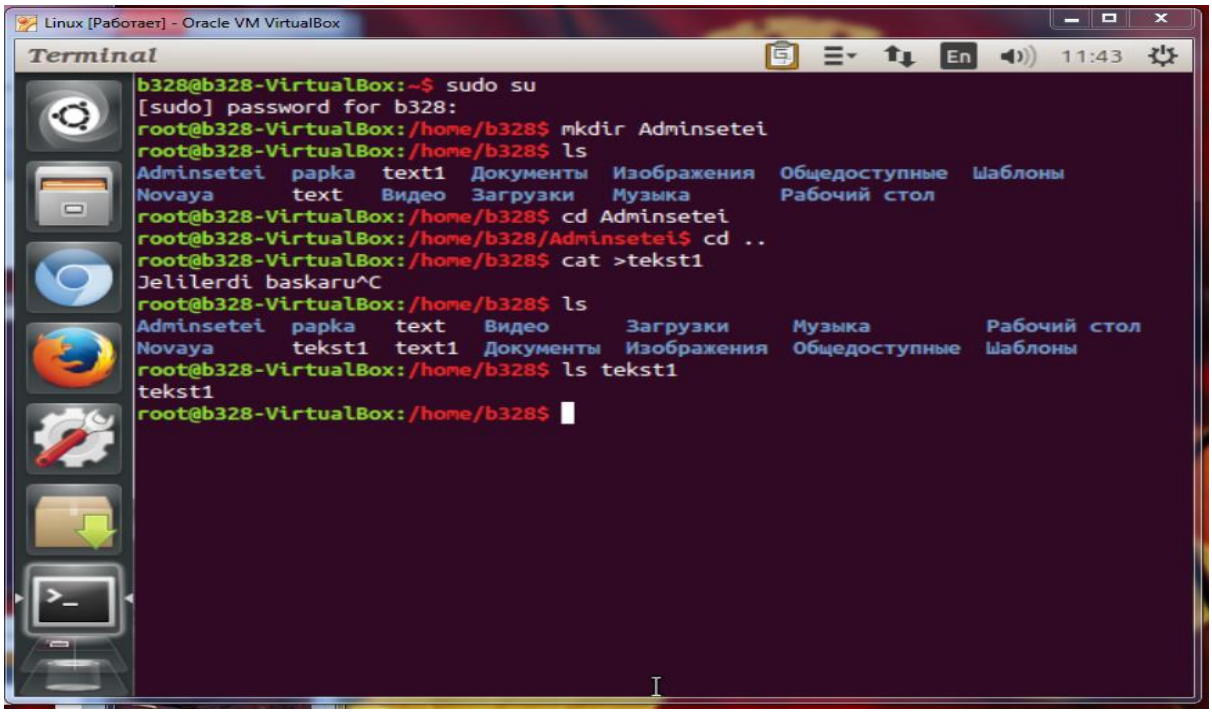

Рисунок 7.1- Терминал ввода текста

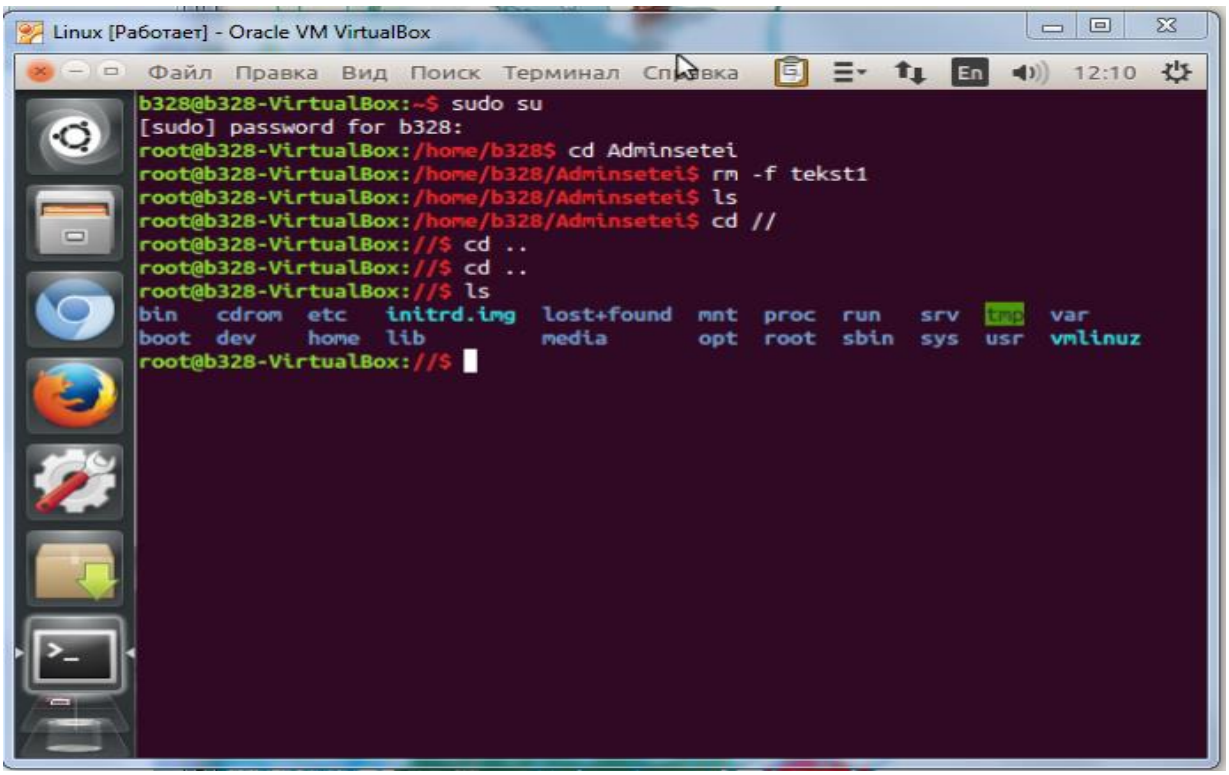

Рисунок 7.2 - Удаление текста с терминала

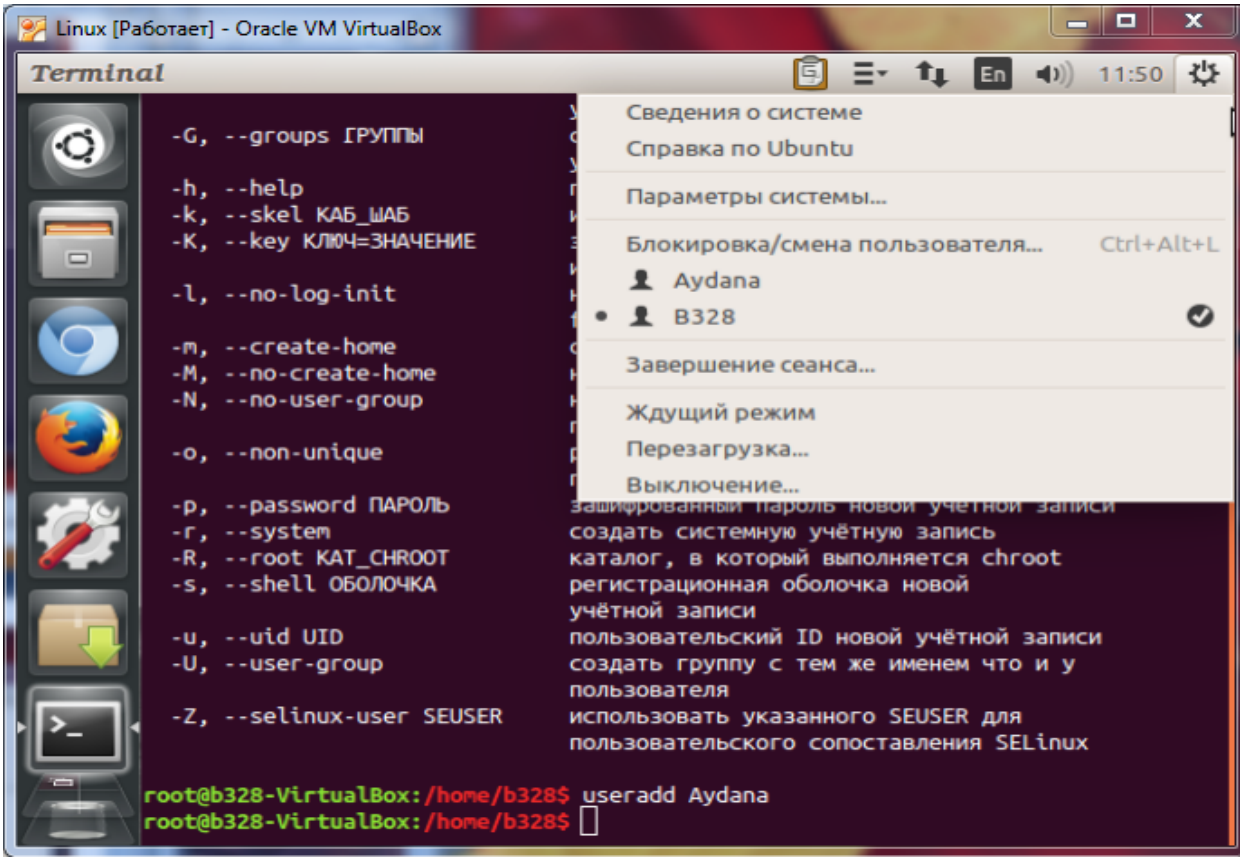

Рисунок 7.3 - Добавление пользователей

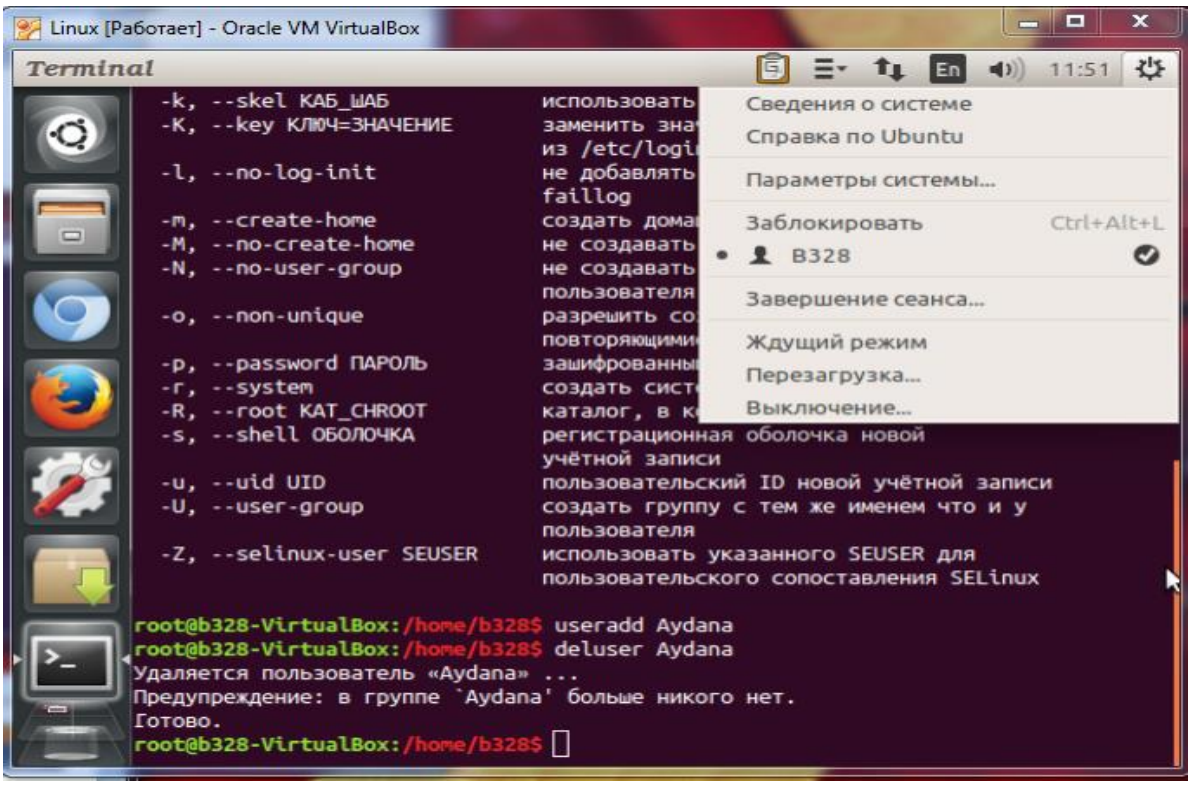

Рисунок 7.4 - Удаление пользователей

7.3 Содержание отчета

Отчет о лабораторной работе должен содержать следующие разделы:
-цель работы;
-задание;
-краткое описание;
-создание учетной записи;
-изменение членства в локальной группе;
-временная блокировка учетной записи;
-выводы по работе.

7.4 Варианты заданий выбираются из лабораторной работы № 2

7.5 Контрольные вопросы

1. Что такое ”командная строка”?
2. Что такое “терминал”?
3. Перечислить состояния процессов в Linux. Как их можно отследить?
4. Зачем используются алиасы в системе?
5. Какие папки есть в корневом каталоге и каково их содержимое?
6. Как создать каталог «Группа»?
7. Как создать каталог «Номер подгруппы»?
8. Как создать в каталоге «Группа» текстовый файл?

Список литературы

1 Станек У.Р. Microsoft Windows Server 2012 R2.-СПб.:БХВ-Петербург, 2015.-416 с.

2 Беленькая М.М. Администрирование в информационных системах.- М.: Горячая линия-Телеком, 2014.

3 Кенин А.М. Практическое руководство системного администратора.- СПб.: БХВ- Петербург, 2013.-544 с.

4 Сатимова Е.Г. Операционные системы: LINUX. Решение задач структурной и функциональной организации: Учебное пособие. - Алматы: АИЭС, 2009. - 100 с.

5 Чекмарёв А.Н. Windows Server 2008. -СПб.:БХВ-Петербург, 2009.-512 с.

6 Самойленко А. Виртуальные машины на платформе Microsoft Virtual PC 2007 [Электронный ресурс]. – Режим доступа:

http://www.windowsfaq.ru/content/view/566/92/.

7 Шетка П. Microsoft Windows Server 2003 [Текст]: практ. руководство по настройке сети. – СПб.: Наука и Техника, 2006. – 608 с.

Сводный план 2016г. поз.156

Галымжан Саруарович Нурмагамбетов.

АДМИНИСТРИРОВАНИЕ ИНФОРМАЦИОННЫХ СИСТЕМ И СЕТЕЙ

Методические указания по выполнению лабораторных работ для студентов специальностей 5В070300 -Информационные системы, 5В060200-Информатика

Редактор Н.М.Голева
Специалист по стандартизации Н.К. Молдабекова

Подписано в печать__.__.__.
Тираж 80экз.
Объем 3,5 уч.-изд. л.

Формат 60Х84 1/16
Бумага типографская №1
Заказ ____ Цена 1750 тг.

Копировально-множительное бюро
некоммерческого акционерного общества
«Алматинский университет энергетики и связи»
050013 Алматы, Байтурсынова, 126