Федеральное агентство морского и речного транспорта
Федеральное государственное бюджетное образовательное учреждение высшего образования
«Государственный университет морского и речного флота имени адмирала С.О. Макарова»

Воронежский филиал
Федерального государственного бюджетного образовательного учреждения высшего образования
«Государственный университет морского и речного флота имени адмирала С.О. Макарова»

ФОНД ОЦЕНОЧНЫХ СРЕДСТВ ДЛЯ ПРОВЕДЕНИЯ ТЕКУЩЕЙ И ПРОМЕЖУТОЧНОЙ АТТЕСТАЦИИ ПО ДИСЦИПЛИНЕ
Б1.В.ДВ.6.1 «Администрирование информационных систем»

(Приложение к рабочей программе дисциплины)

Уровень образования:	Высшее образование – бакалавриат	
Направление подготовки:	09.03.02 Информационные системы и технологии	
Язык обучения:	Русский	
Кафедра:	Математики, информационных систем и технологий	
Форма обучения:	Очная	Заочная
Курс:	4	5
Составитель:	Кручинин С.В.	

ВОРОНЕЖ 2019 г.

СОДЕРЖАНИЕ

1. ПАСПОРТ ФОНДА ОЦЕНОЧНЫХ СРЕДСТВ

1.1 Перечень компетенций и этапы их формирования в процессе освоения дисциплины

В результате освоения ОПОП бакалавриата обучающийся должен овладеть следующими результатами обучения по дисциплине:

Код компетенции	Содержание компетенции	Планируемые результаты освоения дисциплины
ОПК-6	способность выбирать и оценивать способ реализации информационных систем и устройств (программно-, аппаратно- или программно-аппаратно) для решения поставленной задачи	**Знать:** теоретические основы способов реализации информационных систем и устройств; способы реализации информационных систем и устройств. **Уметь:** выбирать способы реализации информационных систем и устройств для решения поставленной задачи. **Владеть:** способностью оценивать способ реализации информационных систем и устройств для решения поставленной задачи; инструментами для решения поставленных задач.
ПК-23	готовность участвовать в постановке и проведении экспериментальных исследований	**Знать**: технологии и принципы проведения экспериментальных исследований. **Уметь**: проводить экспериментальные исследования для решения профессиональных задач. **Владеть**: методами экспериментальных исследований с последующей обработкой и представлением результатов.

1.2. Паспорт фонда оценочных средств для проведения текущей и промежуточной аттестации обучающихся

№ п/п	Контролируемые темы дисциплины	Код контролируемой компетенции	Наименование оценочного средства
1.	Раздел 1. Понятие качества информационных систем.	ОПК-6 ПК-23	Вопросы для контроля знаний, курсовая работа, зачет
2.	Раздел 2. Стандарты управления качеством информационной продукции.	ОПК-6 ПК-23	Вопросы для контроля знаний, курсовая работа, зачет
3.	Раздел 3. Многокритериальные оценки качества информа-	ОПК-6 ПК-23	Вопросы для контроля знаний, курсовая работа, зачет

	ционных систем.		
4.	Раздел 4. Функциональность информационных систем.	ОПК-6 ПК-23	Вопросы для контроля знаний, курсовая работа, зачет
5.	Раздел 5. Надежность как показатель качества информационных систем.	ОПК-6 ПК-23	Вопросы для контроля знаний, курсовая работа, зачет
6.	Раздел 6. Математические модели теории надежности.	ОПК-6 ПК-23	Вопросы для контроля знаний, курсовая работа, зачет
7	Раздел 7. Оптимальное резервирование в отказо-устойчивых системах.	ОПК-6 ПК-23	Вопросы для контроля знаний, курсовая работа, зачет
8	Раздел 8. Контроль и диагностика информационных систем.	ОПК-6 ПК-23	Вопросы для контроля знаний, курсовая работа, зачет
9	Раздел 9. Испытания на качество и надежность.	ОПК-6 ПК-23	Вопросы для контроля знаний, курсовая работа, зачет

1.3 Критерии оценивания результата обучения по дисциплине и шкала оценивания

Уровни сформированности компетенции	**Основные признаки уровня**
Пороговый (базовый) уровень (Оценка «3», Зачтено) (обязательный по отношению ко всем выпускникам к моменту завершения ими обучения по ОПОП)	**Знать:** основные способы реализации информационных систем и устройств и критерии оценки этих способов и иногда испытывать некоторые трудности при реализации ИС; теоретические основы постановки и проведения экспериментальных исследований на пороговом уровне. **Уметь:** использовать способы реализации информационных систем и устройств на пороговом уровне, в некоторых случаях испытывать затруднения; проводить экспериментальные исследования на пороговом уровне. **Владеть:** элементарными навыками оценки эффективности способов реализации ин формационных систем и устройств; способностью к постановке и проведению экспериментальных исследований на пороговом уровне.
Повышенный (продвинутый) уровень (Оценка «4», Зачтено) (превосходит пороговый (базовый) уровень по одному	**Знать:** основные способы реализации информационных систем и устройств и критерии оценки этих способов; теоретические основы постановки и проведения экспериментальных исследований на продвинутом уровне. **Уметь:** использовать способы реализации

или нескольким существенным признакам)	информационных систем и устройств на продвинутом уровне; проводить экспериментальные исследования на продвинутом уровне. **Владеть:** навыками оценки эффективности способов реализации информационных систем и устройств; способностью к постановке и проведению экспериментальных исследований на продвинутом уровне.
Высокий (превосходный) уровень (Оценка «5», Зачтено) (превосходит пороговый (базовый) уровень по всем существенным признакам, предполагает максимально возможную выраженность компетенции)	**Знать:** основные способы реализации информационных систем и устройств и критерии оценки этих способов и при этом не испытывать затруднений; теоретические основы постановки и проведения экспериментальных исследова- ний на высоком уровне. **Уметь:** использовать способы реализации информационных систем и устройств на вы- соком уровне; проводить экспериментальные исследования на высоком уровне. **Владеть:** навыками оценки эффективности способов реализации информационных систем и устройств; способностью к постановке и проведению экспериментальных исследований на высоком уровне.

2. ФОНД ОЦЕНОЧНЫХ СРЕДСТВ ДЛЯ ПРОВЕДЕНИЯ ТЕКУЩЕГО КОНТРОЛЯ

2.1 Задания для самостоятельной работы и текущего контроля

Тема 1. ФУНКЦИИ, ПРОЦЕДУРЫ И СЛУЖБЫ АДМИНИСТРИРОВАНИЯ

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 называется гостевой?
5. Каким образом можно изменять конфигурацию созданной виртуальной машины?

Лабораторная работа

Применение технологии виртуализации для решения задач администрирования

ЦЕЛЬ РАБОТЫ: изучение технологии виртуальных машин «Огас1е VirtualBox».

1. Рабочее задание

1. Изучить технологии создания виртуальных машин.
2. Научиться создавать виртуальные жесткие диски, подключать ранее созданные образы виртуальных дисков.
3. Научиться создавать виртуальную машину, изменять ее конфигурацию, устанавливать ОС Windows, создавать снимок состояния и устанавливать расширенный набор инструментов в виртуальной среде.

2. Методические указания к выполнению

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»). На одном физическом устройстве можно создавать и запускать произвольное число виртуальных машин, ограничиваемое лишь физическими ресурсами реального компьютера.

Собственно инструмент для создания ВМ (его также называют приложением виртуальных машин, или ПВМ) - это обычное программное приложение, устанавливаемое, как и любое другое, на конкретную реальную операционную систему. Эта реальная ОС именуется «хозяйской», или «хостовой ОС» (от англ. термина host- «главный», «базовый», «ведущий»). Все задачи по управлению виртуальными машинами решает специальный модуль в составе приложения ВМ

- монитор виртуальных машин (МВМ).

В большинстве программных продуктов ему предоставляется лишь графический интерфейс для создания и настройки виртуальных машин. Этот интерфейс обычно называют консолью виртуальных машин. «Внутри» виртуальной машины пользователь устанавливает, как и на реальном компьютере, нужную ему операционную систему. Такая ОС, принадлежащая конкретной ВМ, называется гостевой (guest OS). Перечень поддерживаемых гостевых ОС является одной из наиболее важных характеристик виртуальной машины.

Алгоритм выполнения работы

Запуск консоли управления виртуальными машинами.

Запустить консоль управления виртуальными машинами можно с помощью соответствующего ярлыка, расположенного на рабочем столе (рис. 1.1) или через «Пуск»/«Меню» из программной группы «Orac1e VirtualBox».

Рис. 1.1. Ярлык программы «Orac1e VirtualBox»

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

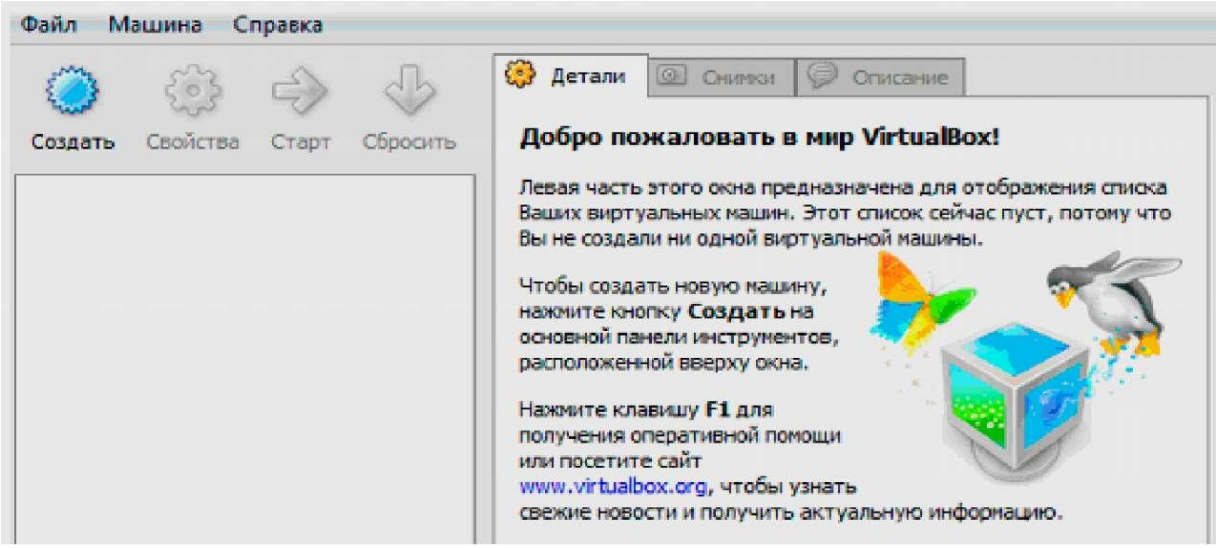


Рис. 1.2. Консоль виртуальных машин «Oracle VirtualBox»

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

Подключение ранее созданных виртуальных дисков к менеджеру виртуальных машин.

Для создания виртуального жесткого диска необходимо выполнить следующие действия.

1. В меню «Файл» выбрать «Менеджер виртуальных носителей...» или воспользоваться сочетанием клавиш «Ctrl + D». В результате откроется окно управления виртуальными носителями (рис. 1.3).
2. 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.
3. В открывшемся окне «Создать новый виртуальный жесткий диск» нажать Next».

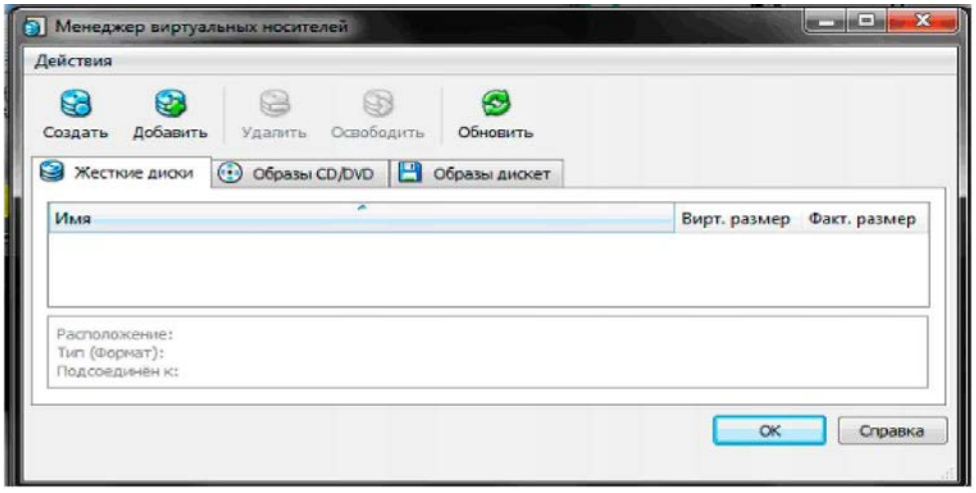


Рис. 1.3. Диалоговое окно «Менеджер виртуальных носителей»

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

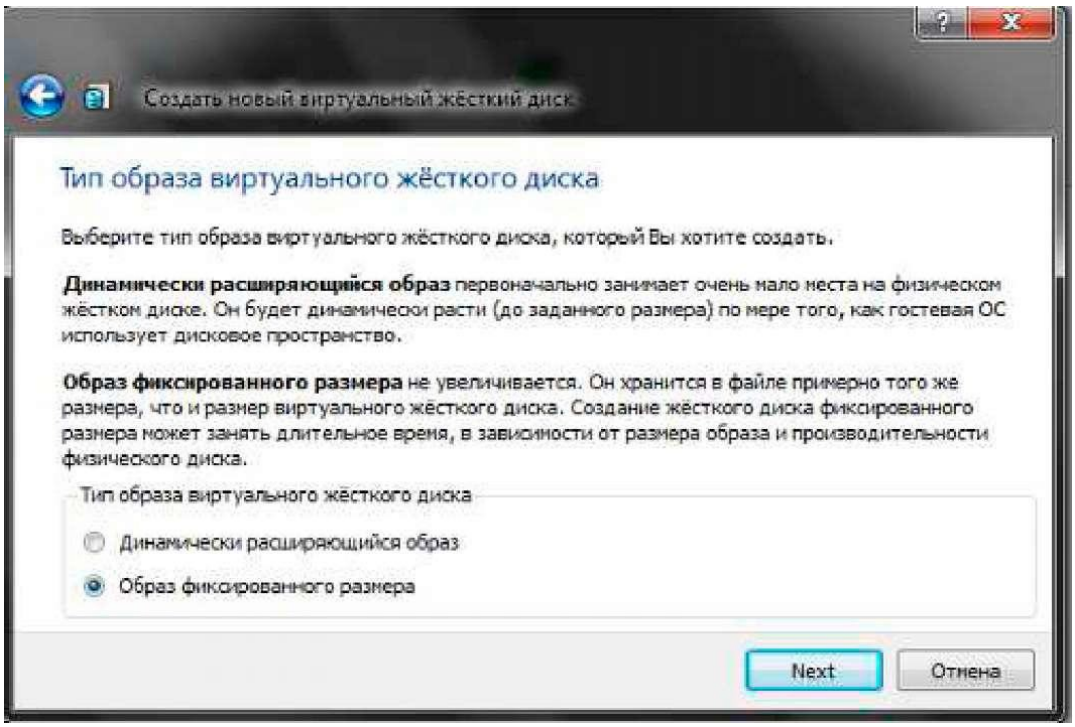


Рис. 1.4. Диалоговое окно «Создать новый виртуальный жесткий диск»

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

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

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

7. 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 (рис. 1.5).

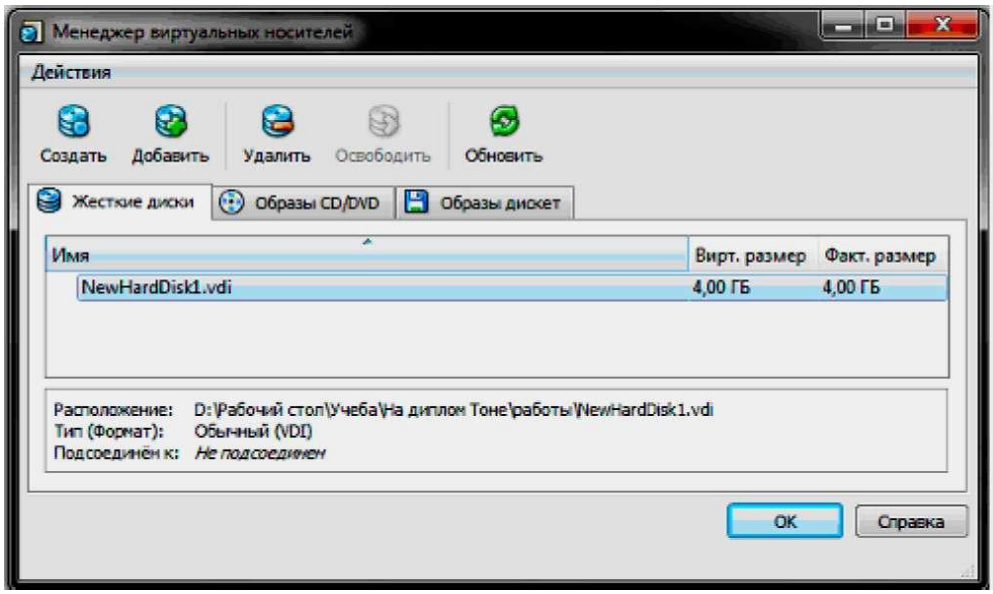


Рис. 1.5. Диалоговое окно «Менеджер виртуальных носителей»

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».

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 (рис. 1.6).

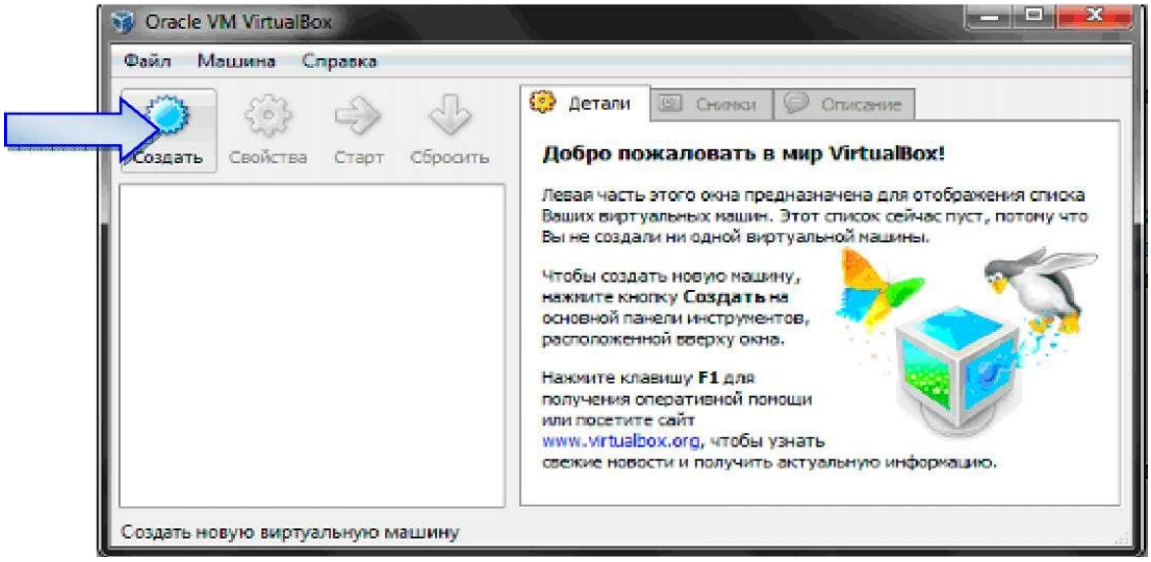


Рис. 1.6. Консоль управления виртуальных машин «0rac1e VirtualBox»

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 мастера создания виртуальной машины, нажав работу кнопку «Финиш» (рис. 1.7).

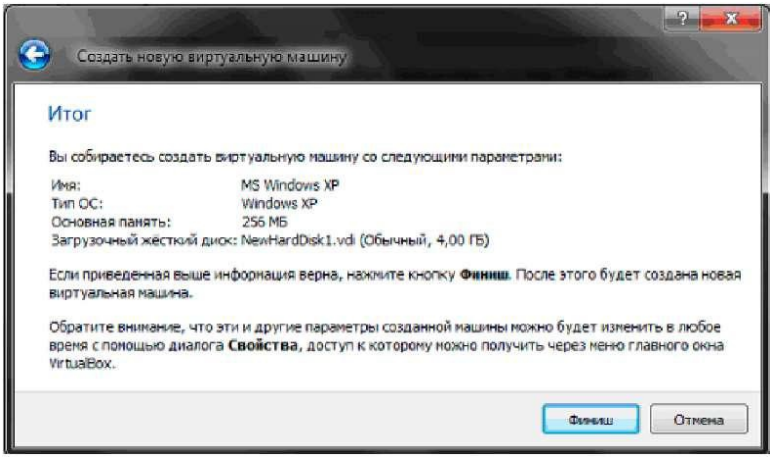


Рис. 1.7. Диалоговое окно «Создать новую виртуальную машину»

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 настранице «Детали» даны сведения об аппаратной конфигурации виртуальной машины (рис. 1.8).

Рис. 1.8 Консоль управления 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.
4. Далее, для организации взаимодействия между гостевой ОС и основной ОС, зададим общую сетевую папку.
5. В разделе настроек «Общие папки» добавить папку (рис. 1.9).

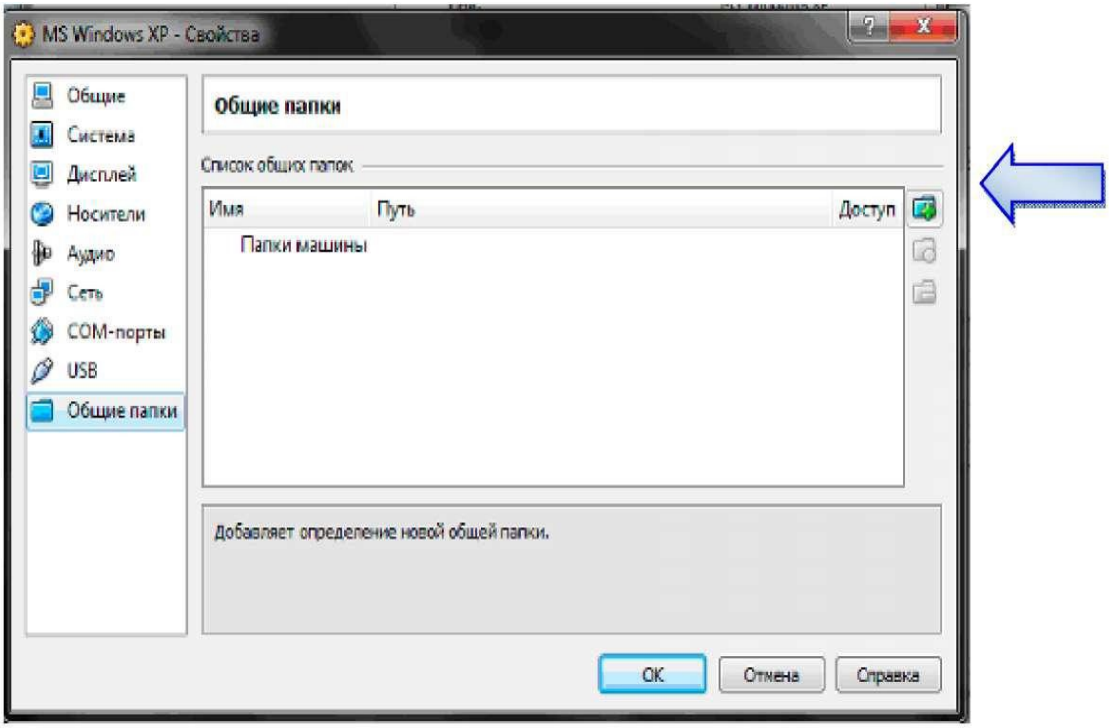


Рис. 1.9. Диалоговое окно «Свойства»

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

Запустить виртуальную машину.

Установка ОС ***Windows 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 (рис. 1.10).

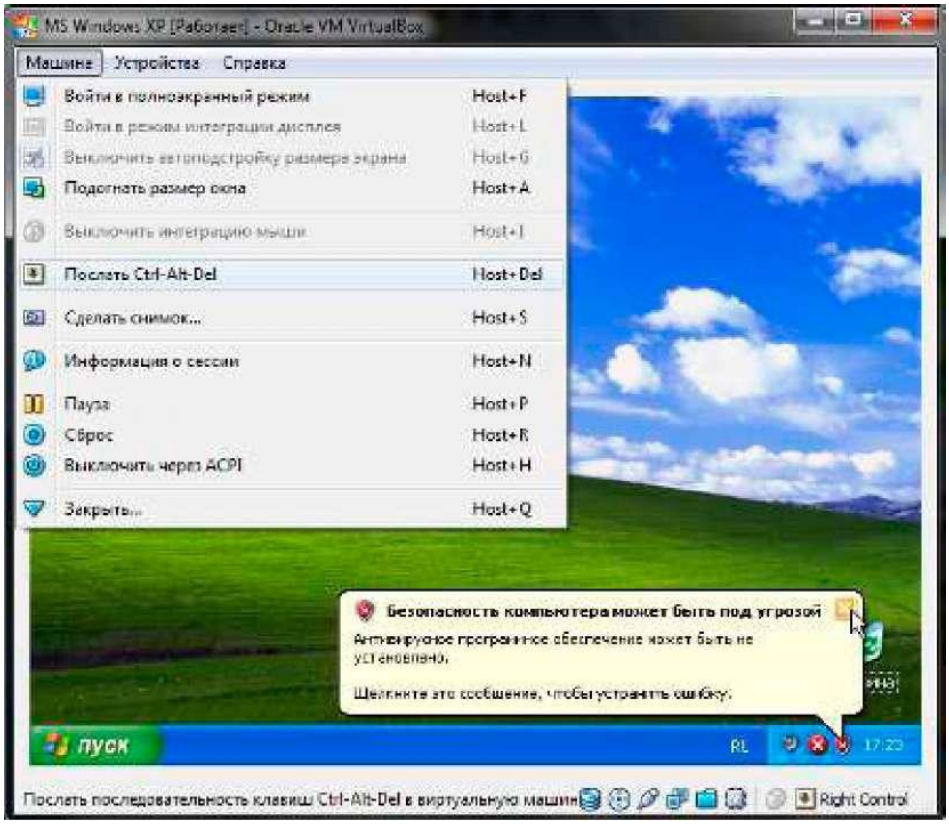


Рис. 1.10. Виртуальная машина

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» (рис. 1.11).

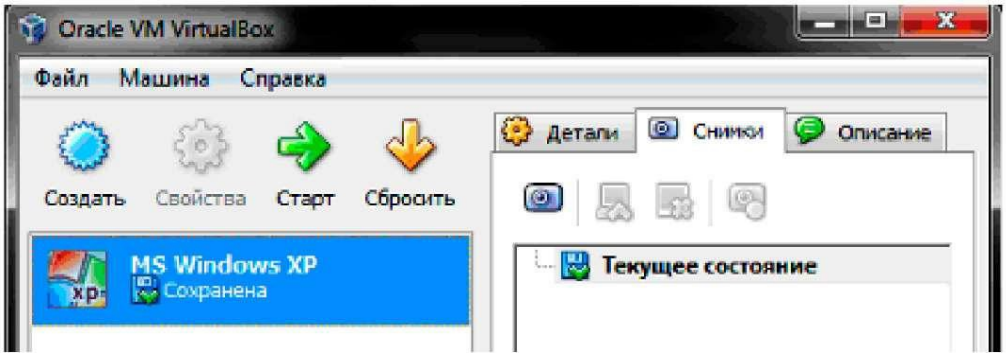


Рис. 1.11. Вкладка «Снимки» консоли управления ВМ

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

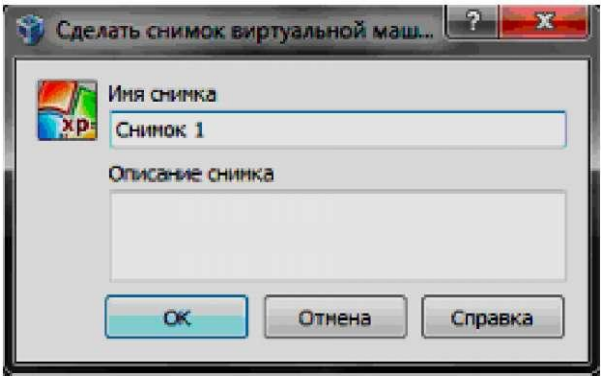


Рис. 1.12. Диалоговое окно «Сделать снимок виртуальной машины»

5. Ввести имя и описание снимка. Нажать «ОК».

Для подключения расширенных инструментов необходимо выполнить следующие действия.

1. Запустить виртуальную машину, используя инструмент «Старт» в консоли управления.
2. Выполнить команды «Устройства» и «Установить Дополнения гостевой ОС».

Вопросы для контроля знаний:

1. Функции администрирования.
2. Процедуры администрирования.
3. Службы администрирования.
4. Категории администраторов.

Тема 2. ОБЪЕКТЫ АДМИНИСТРИРОВАНИЯ

Контрольные вопросы:

1. Какие методы управления доступом Вам известны?
2. Чем отличается мандатное управление доступом от дискретного?

3. Допустимо ли имя пользователя П38/44? Почему?

Лабораторная работа

Назначение прав пользователей при произвольном управлении доступом в Windows XP

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

1. Рабочее задание

Создать учетную запись и локальную группу, изменить принадлежность пользователя к локальной группе и блокировать учетную запись пользователя

2. Методические указания к выполнению

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.

Алгоритм выполнения работы

А. Создание учетной записи.

1. Откройте оснастку Управление компьютером в разделе Администрирование Панели управления (рис. 2.1).

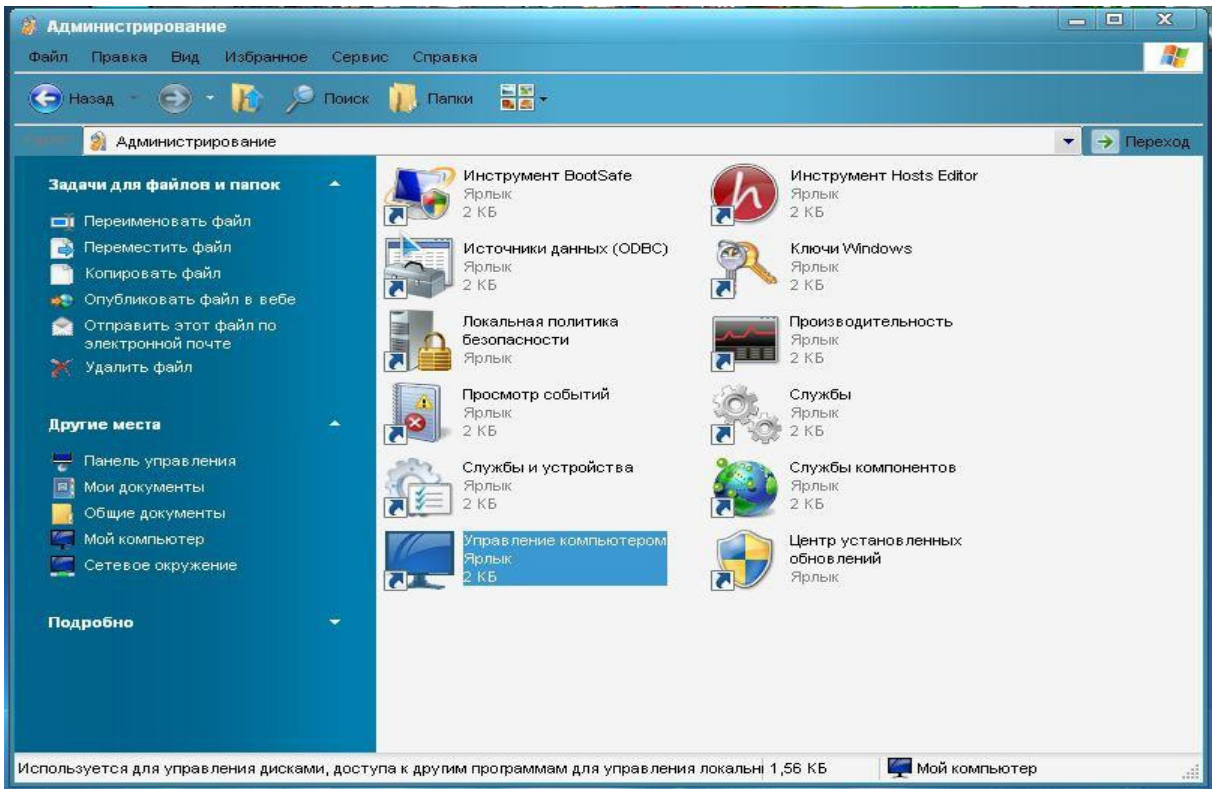


Рис. 2.1

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

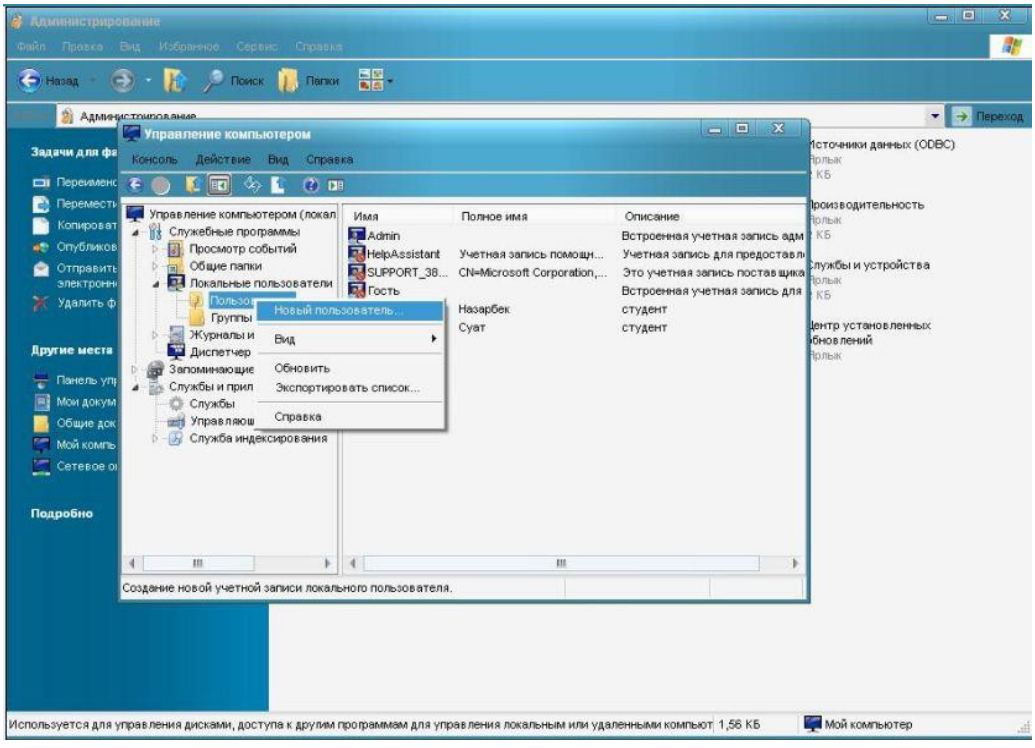


Рис 2.2

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

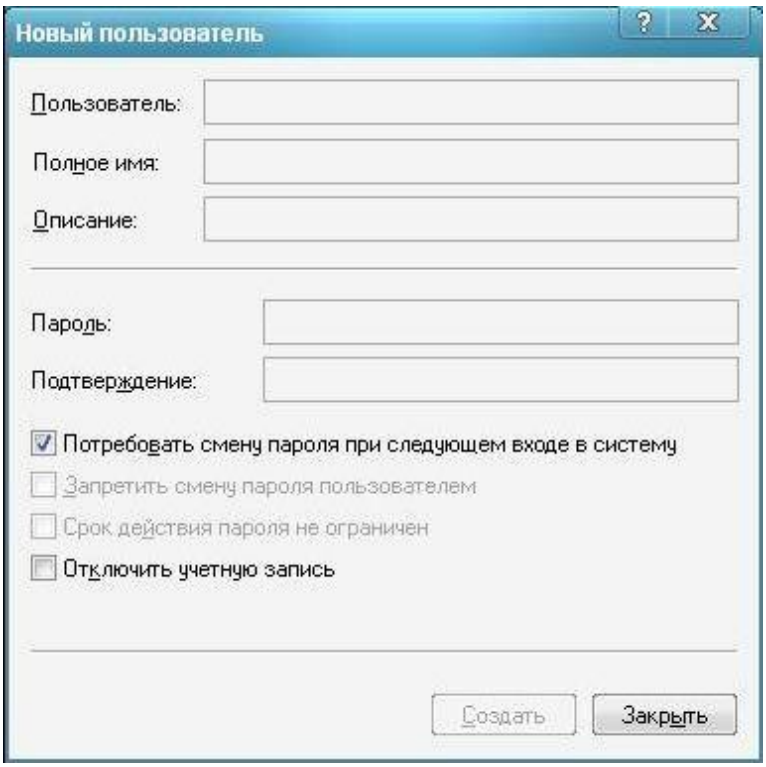


Рис 2.3

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. (рис 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.

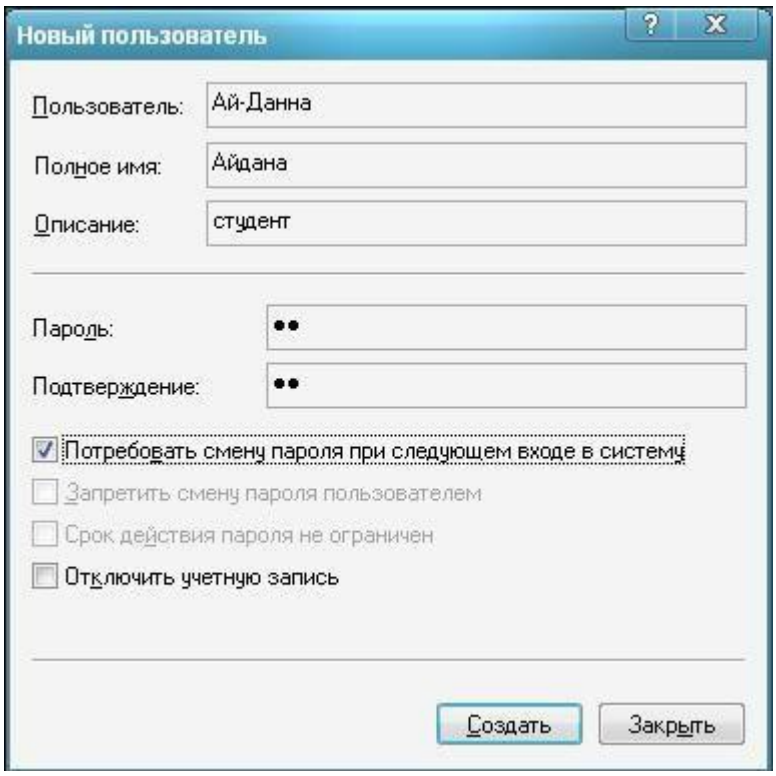


Рис 2.4

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.

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.

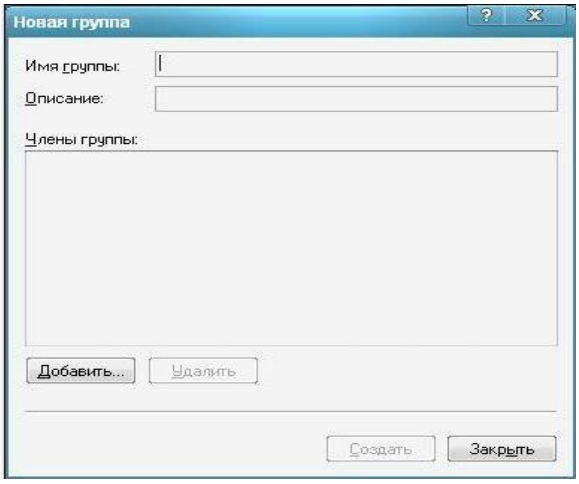


Рис. 2.5

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.

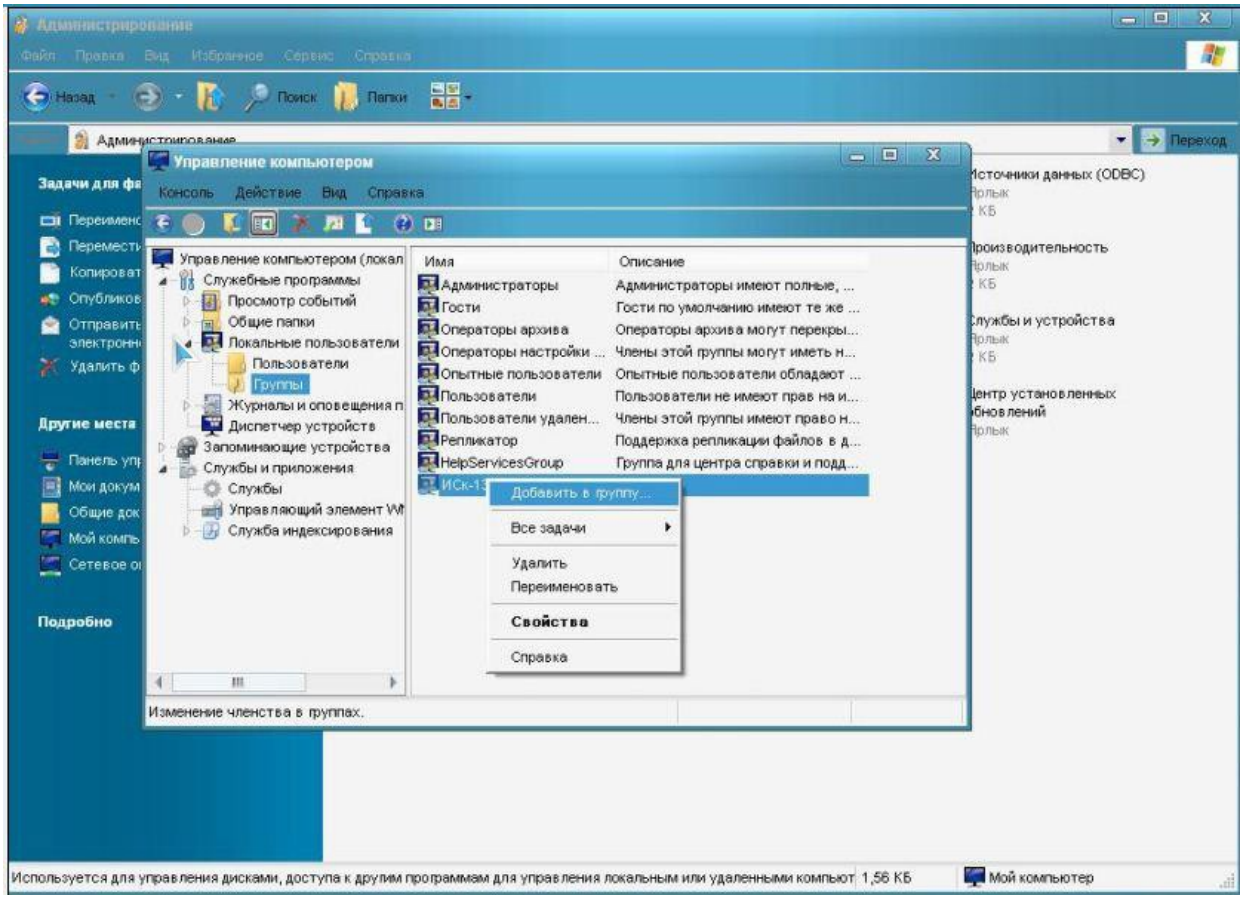


Рис 2.6

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

Рис. 2.7

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(рис 2.9).

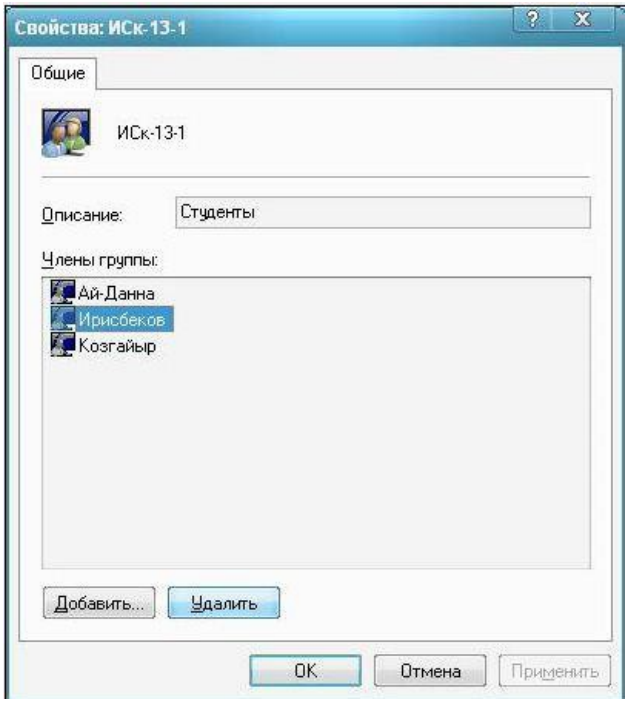


Рис 2.8

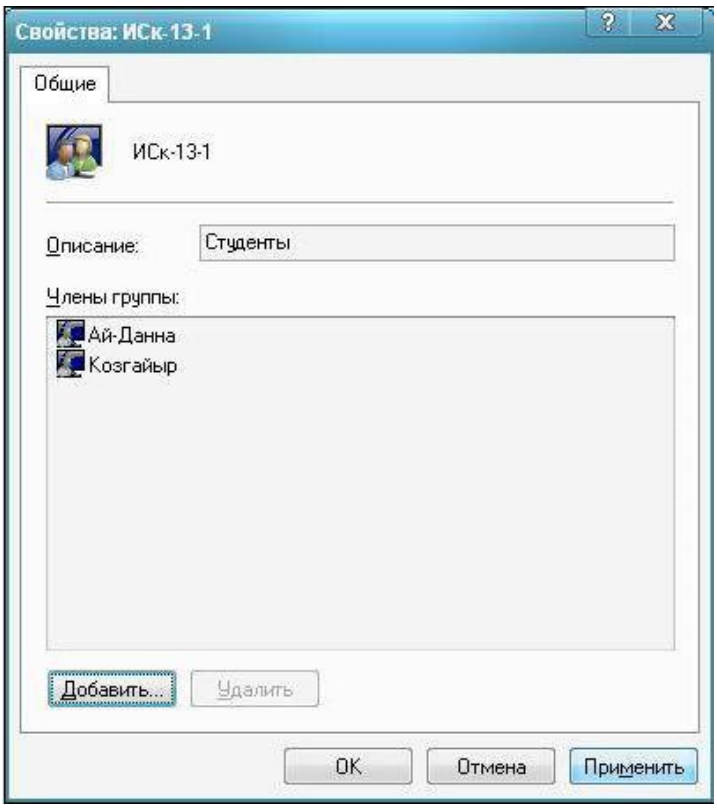


Рис 2.9

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.

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 (рис. 2.10).

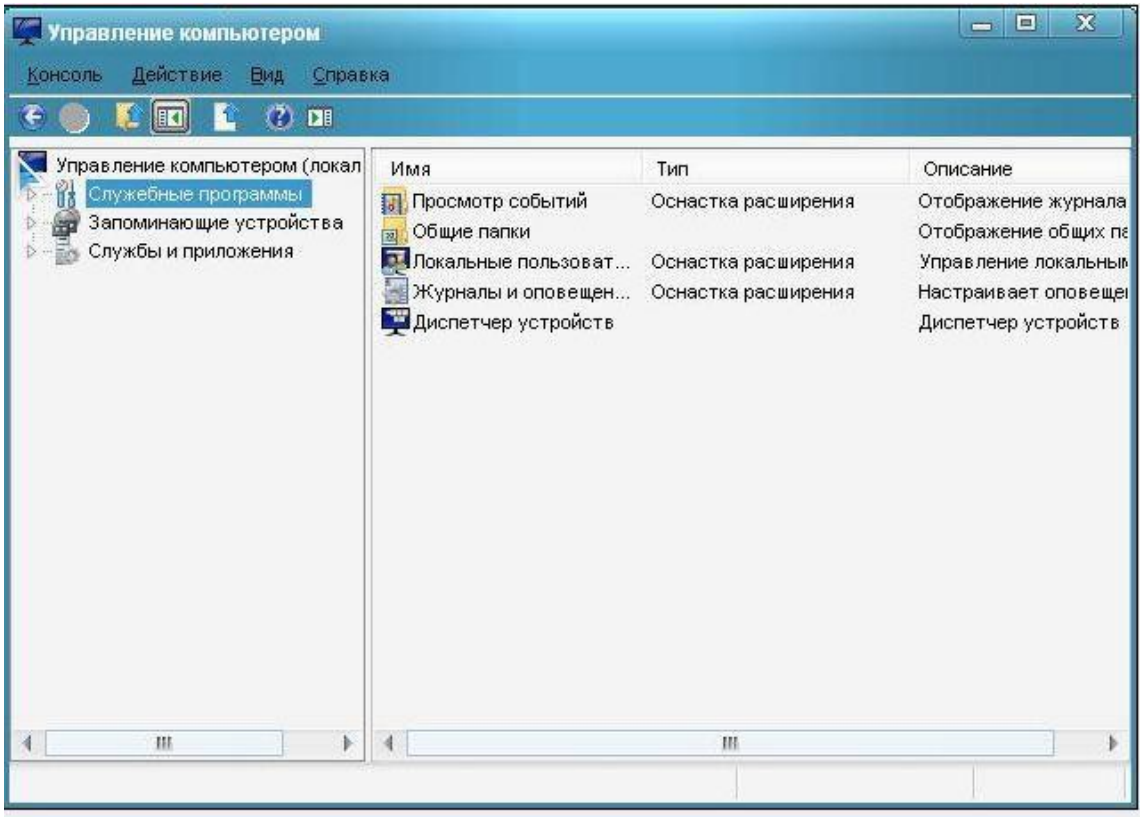


Рис 2.10

4. Откройте папку Пользователи и выберите учетную запись Гость(2.11).
5. Нажмите правую клавишу мыши и выберите пункт Свойства.

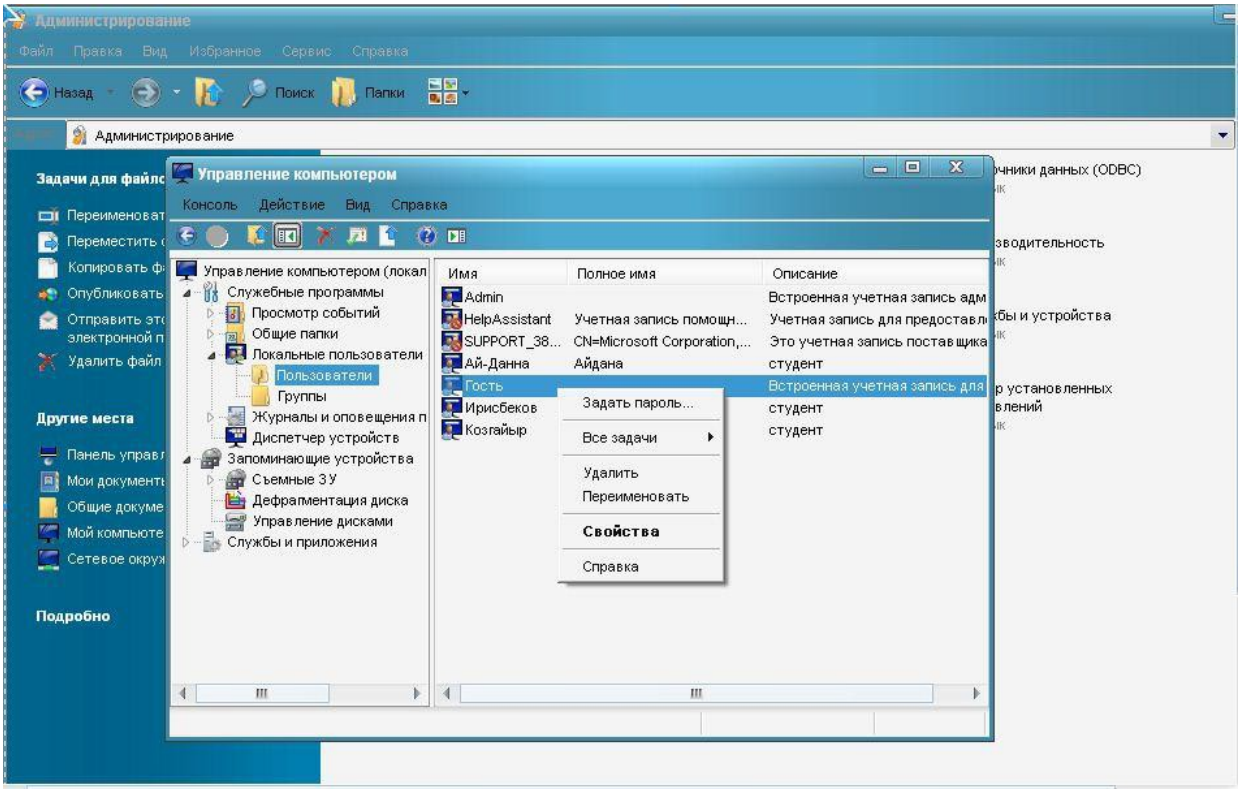


Рис. 2.11

6. В открывшемся окне снимите отметку пункта Отключить учетную запись (рис. 2.12).

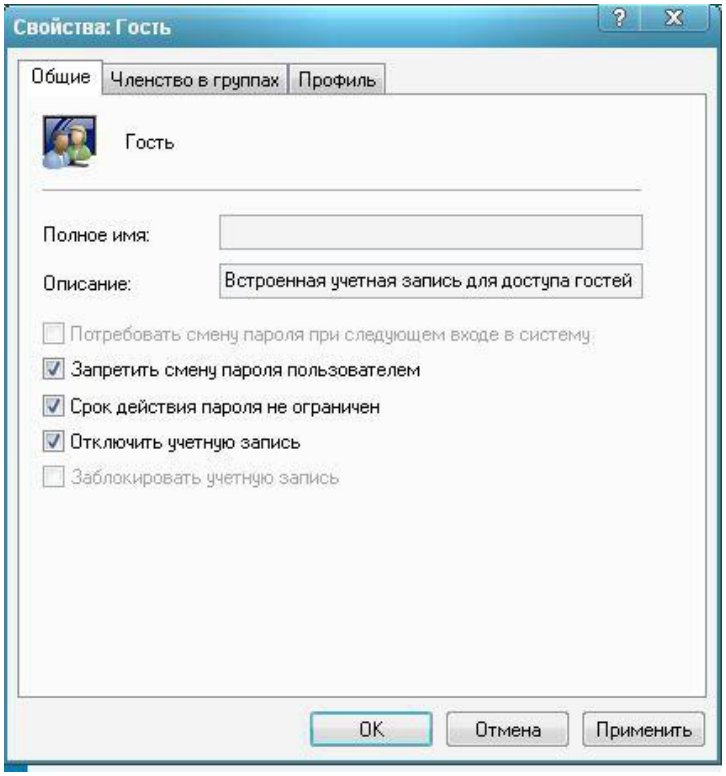


Рис. 2.12

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

Задания для самостоятельной работы

1. Создайте учетную запись с именем ПЗ-б, используя команду Print Screen клавиатуры, сохраните копию экрана со списком пользователей Вашего компьютера (для этого после нажатия клавиши Print Screen вставьте скопированное изображение в новый документ \Vorc1) для представления в качестве отчета.
2. Создайте группу Информационная безопасность и, как в первом задании, сохраните окно со списком групп Вашего компьютера для отчета.
3. Заблокируйте учетную запись ПЗ-6 и после этого удалите.

Вопросы для контроля знаний:

1. Объекты администрирования.
2. Компоненты в ведении администратора информационных систем. Разработчики приложений и служба безопасности.
3. Реализация служб каталогов.

Тема 3. ПРОГРАММНАЯ СТРУКТУРА

Контрольные вопросы:

1. Что подразумеваем под выражением резервная копия сертификата?
2. Что входит в обязанности системного администратора?
3. Что подразумеваем под понятием консоль?
4. Что такое mms?

Лабораторная работа

Создание резервной копии Сертификата средствами Windows XP

Цель работы: изучение основ создания скрытого раздела системы при помощи резервной копии сертификата.

1. Рабочее задание

1. Изучение основ создания скрытого раздела системы.

2. Освоить методы создания скрытого раздела с помощью

2. Методические указания к выполнению

Резервная копия сертификата необходима для расшифровки данных после переустановки операционной системы или для просмотра зашифрованной информации на другой ПЭВМ.

Внимание! Перед переустановкой операционной системы обязательно создайте копии Сертификатов, так как после переустановки Вы не сможете расшифровать информацию. Примечание. **Консоль ММС — это средство для создания, сохранения и открытия наборов средств администрирования, называемых консолями**. Консоли содержат такие элементы, как **оснастки**, расширения оснасток, элементы управления, задачи, мастера и документацию, необходимую для управления многими аппаратными, программными и сетевыми компонентами системы Windows. Можно добавлять элементы в существующую консоль ММС, а можно создавать новые консоли и настраивать их для управления конкретными компонентами системы.

Создаваемые программой резервные копии надежно защищаются от повреждения или уничтожения. Для этого используется так называемая зона безопасности (Acronis Secure Zone). Она представляет собой скрытый служебный раздел, который можно разместить на локальном жестком диске. Зона безопасности имеет особую файловую систему, и поэтому доступна только программам компании Acronis. Все остальное ПО, использующее стандартные возможности ОС, считает этот раздел просто неразмеченным пространством и не может работать с сохраненными в нем резервными копиями и образами. Это защищает последние от повреждения вирусами, удаления легитимными пользователями и т. д. Помимо этого резервные копии можно создавать просто в существующих разделах локального жесткого диска, на сетевых дисках, удаленных FTP-серверах, сменных (в том числе и ленточных) носителях.

Алгоритм выполнения работы

Для создания резервной копии сертификата выполните следующие действия.

1. Выберите кнопку Пуск в панели задач.
2. Перейдите к пункту Выполнить.(3.1)

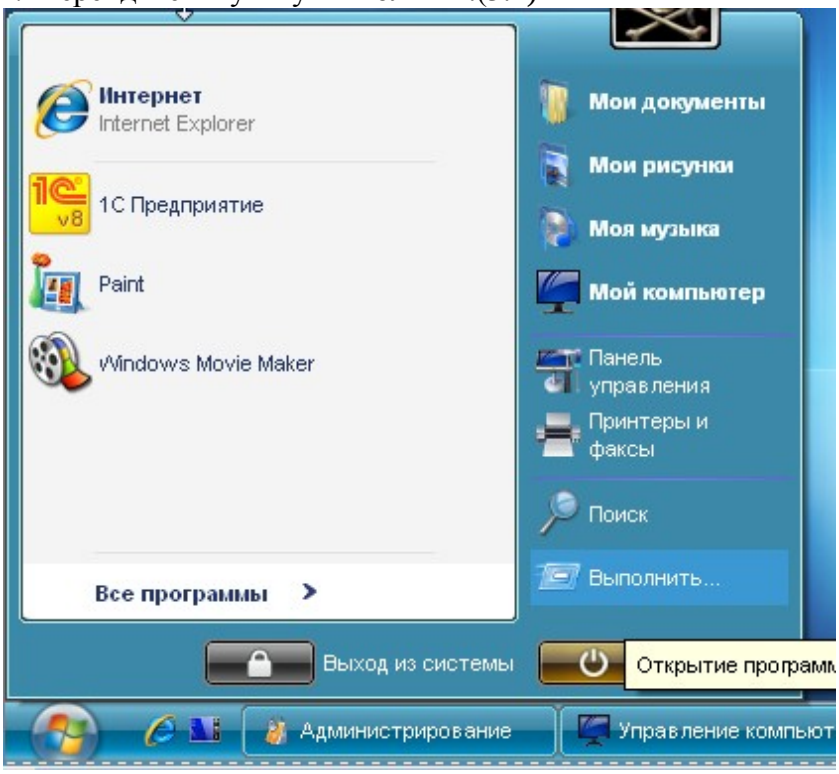


Рис. 3.1

3. В открывшемся окне в поле ввода введите команду mmc.(рис3.2)

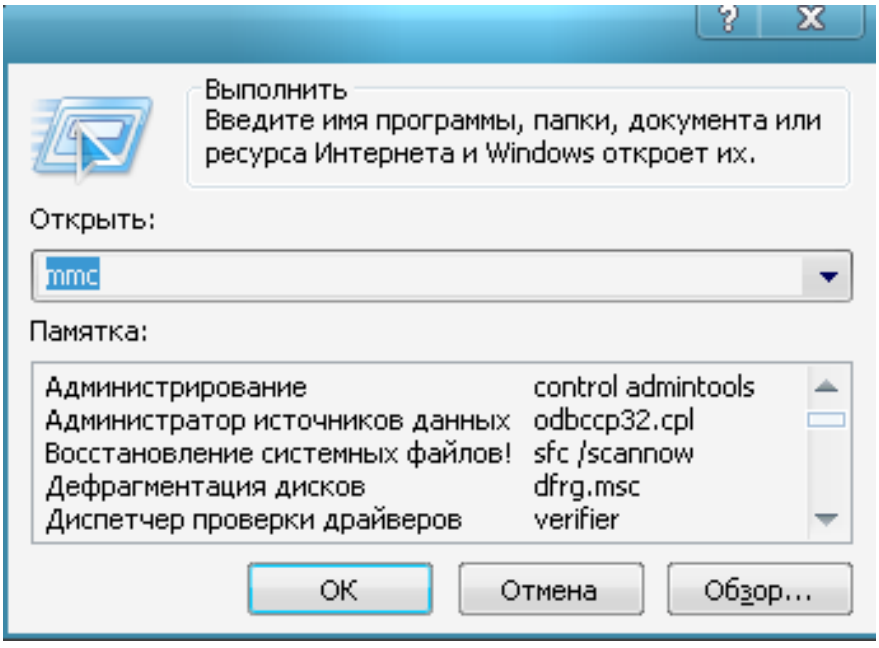


Рис. 3.2

4. В результате откроется консоль управления mmc.(рис 3.3)

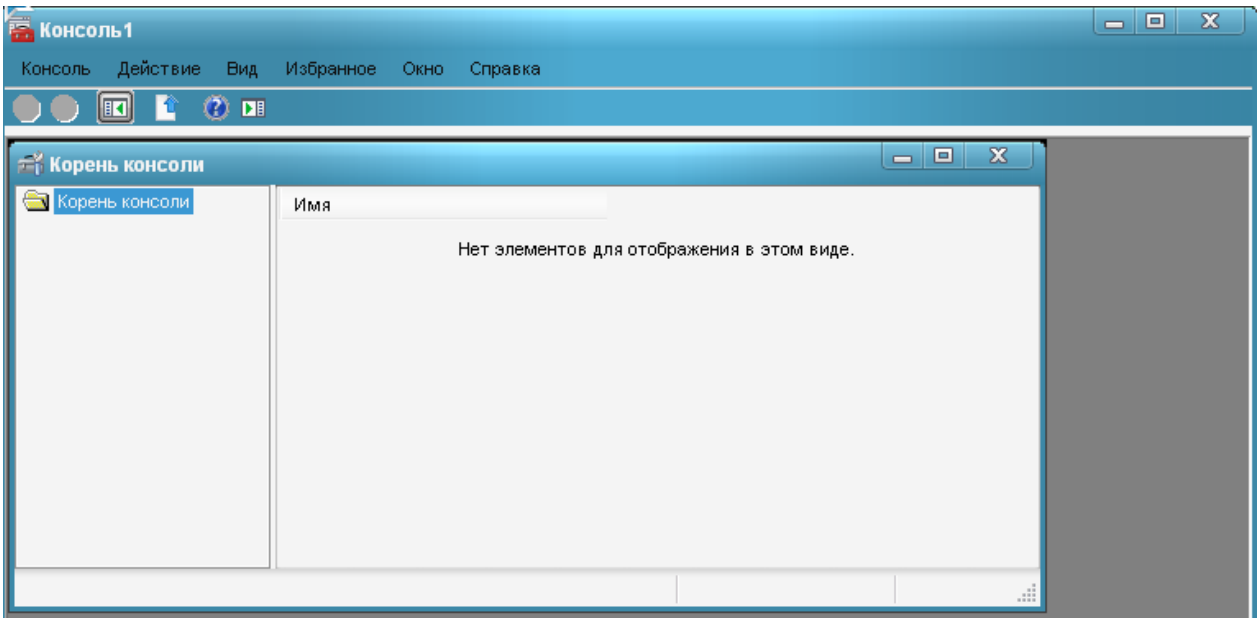


Рис 3.3

5. В меню Консоль выберите команду Добавить или удалить оснастку (рис. 3.4) и нажмите кнопку Добавить.

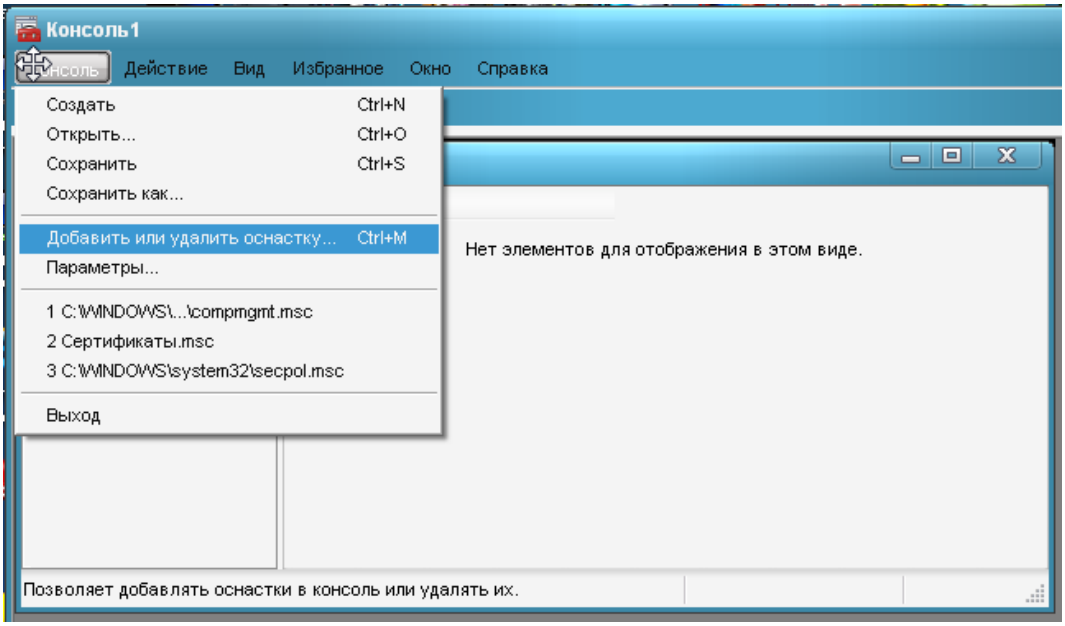


Рис. 3.4

6. В поле Оснастка дважды щелкните Сертификаты, (рис. 3.5), установите переключатель в положение учетной записи компьютера и нажмите кнопку Далее.

7. Выполните одно из следующих действий.

- Чтобы управлять сертификатами локального компьютера, установите переключатель в положение локальным компьютером и нажмите кнопку Готово.

Чтобы управлять сертификатами удаленного компьютера, установите переключатель в положение другим компьютером и введите имя компьютера или нажмите кнопку Обзор для выбора компьютера, затем нажмите кнопку Готово.

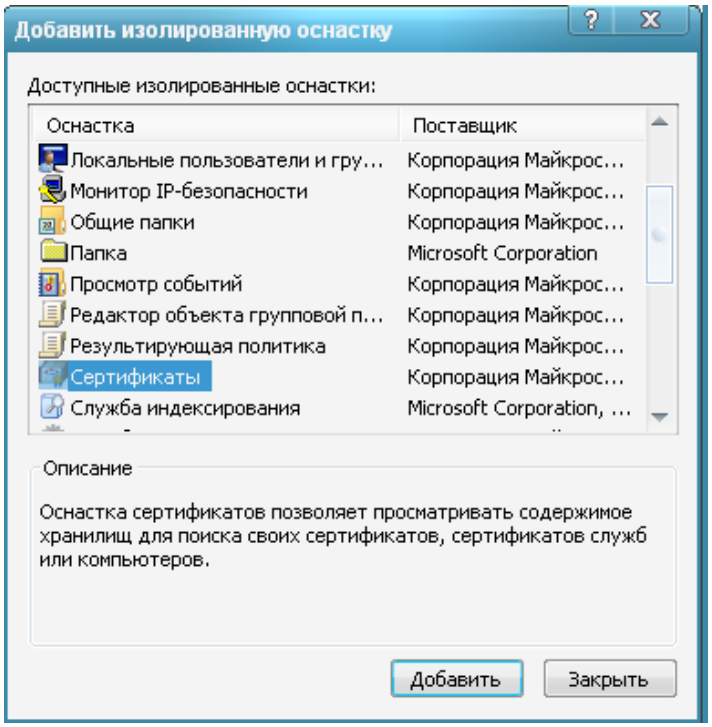


Рис. 3.5

8. Нажмите кнопку Закрыть.

9. В списке выбранных оснасток для новой консоли появится элемент Сертификаты (имя компьютера).

10. Если на консоль не нужно добавлять другие оснастки, нажмите кнопку ОК(рис.3.6).

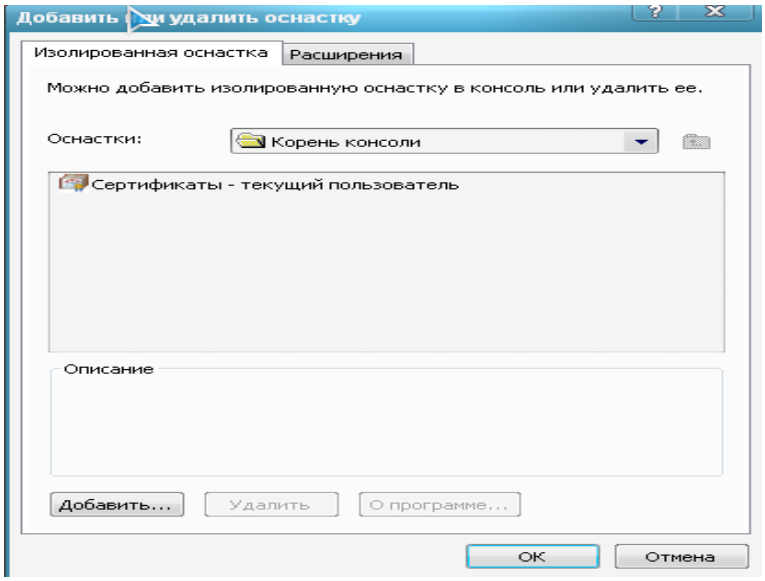


Рис. 3.6

Чтобы сохранить эту консоль, в меню Консоль выберите команду Сохранить и укажите имя оснастки Сертификаты.

11. Закроите окно Консоли и выберите команду Пуск и далее Все программы.

12. Найдите пункт Администрирование и выберите подпункт Сертификаты (теперь оснастка с Сертификатами доступна в меню Пуск)(рис.3.7).

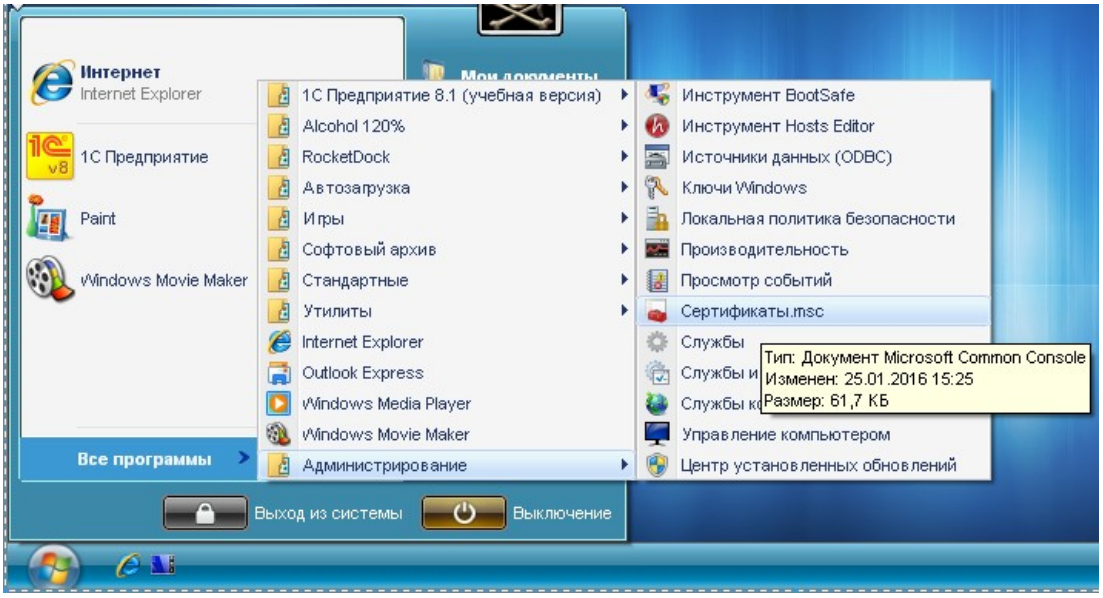


Рис. 3.7

13. В левом подокне оснастки Сертификаты откройте папку Доверенные корневые сертификаты, а затем папку Сертификаты. В правом подокне появится список сертификатов(рис 3.8).

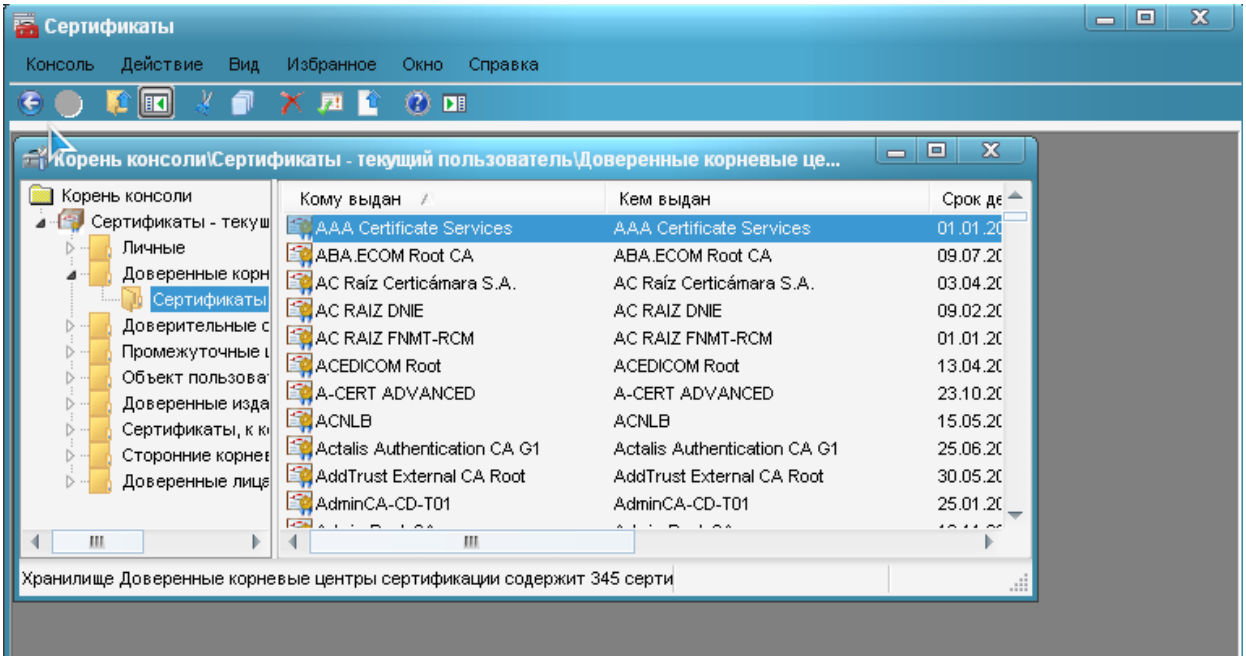


Рис. 3.8

Укажите переносимый сертификат (например, первый в списке, рис. 3.9) и щелкните правой кнопкой мыши. В появившемся контекстном меню выберите команду Все задачи и далее выберите команду Экспорт.

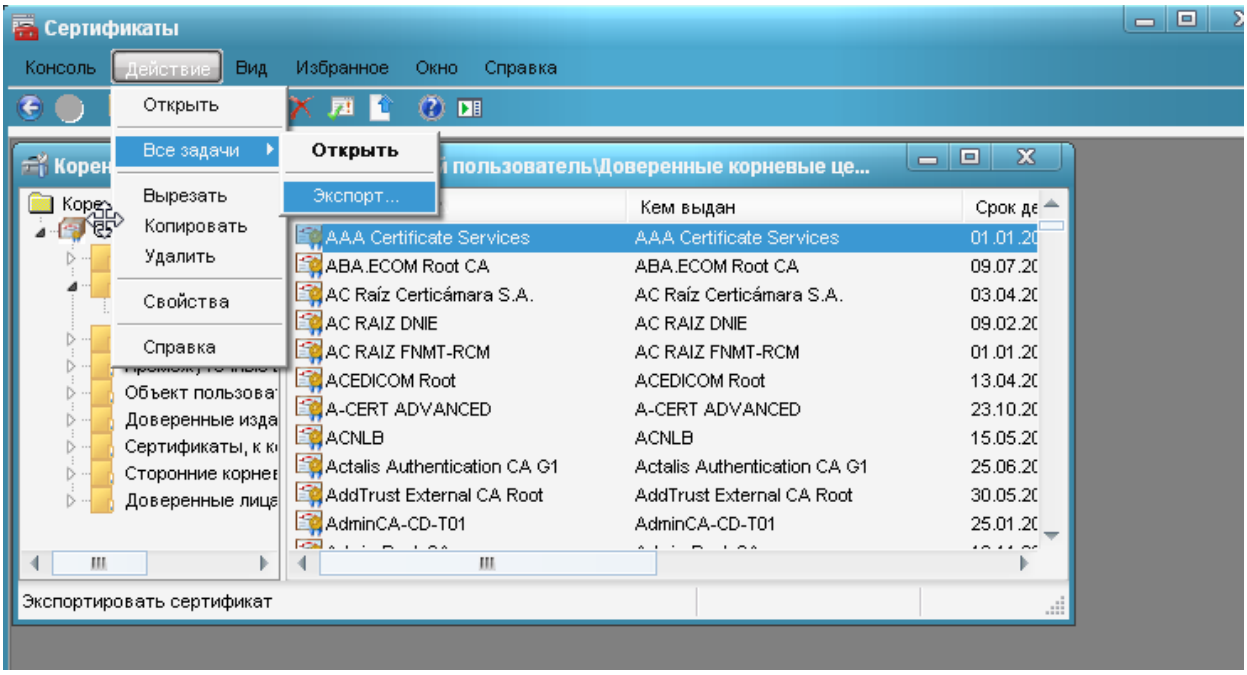


Рис. 3.9

14. В результате запустится Мастер экспорта сертификатов.

15. Нажмите кнопку Далее.

16. В следующем окне мастера выберите опцию Да, экспортировать закрытый ключ.

17. Затем нажмите кнопку Далее.

18. В следующем окне мастера доступен только один формат (PFX), предназначенный для персонального обмена информацией. Нажмите кнопку Далее.

19. В следующих окнах сообщите пароль (например, 11), защищающий данные файла сертификат.pfx, а также путь сохранения файла (запишите путь к папке, в которой Вы сохранили копию Сертификата) сертификатах.

20. Нажмите кнопку Далее.

21. Отобразится список экспортируемых сертификатов и ключей. Нажмите кнопку Готово.

22. Завершите работу Мастера экспорта сертификата нажатием кнопки ОК в окне диалога, сообщающем об успешном выполнении процедуры экспорта(рис 3. 10).

В результате сертификат и секретный ключ будут экспортированы в файл с расширением сертификат.pfx, который может быть скопирован на гибкий диск и перенесен на другой компьютер или использован после переустановки операционной системы.

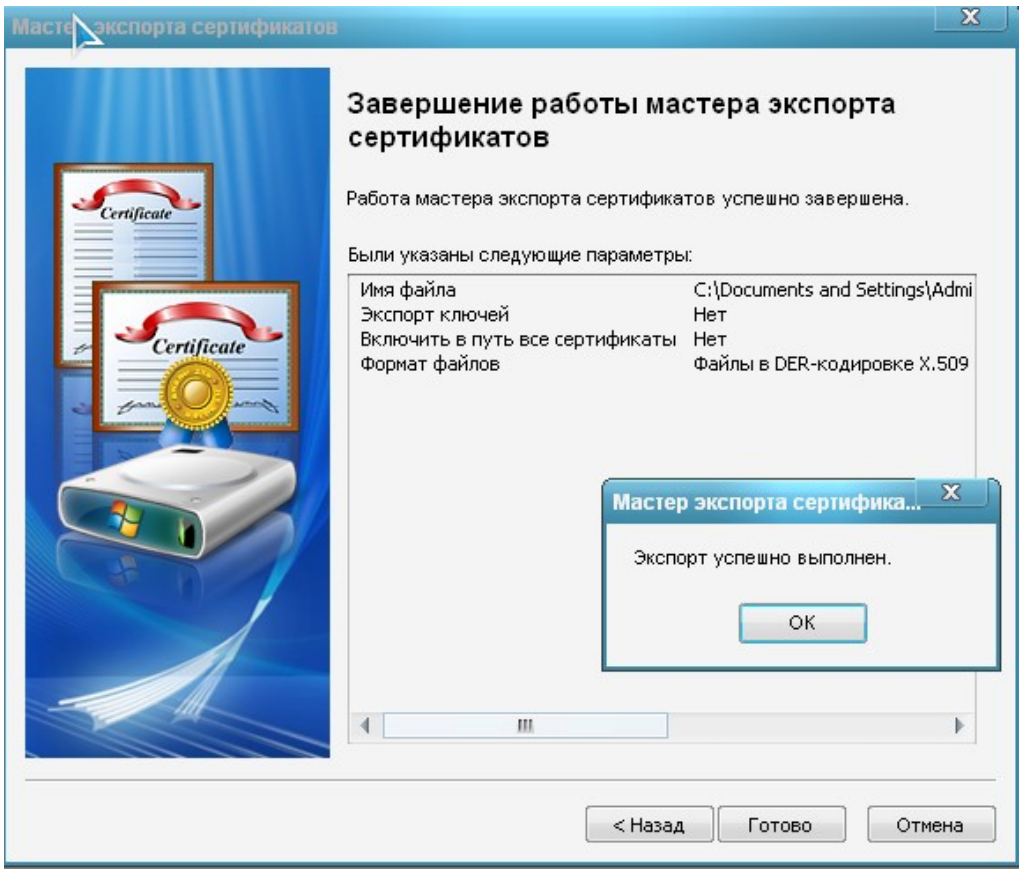


Рис. 3.10

D. Для восстановления сертификата из резервной копии выполните следующие действия.

1. Перенесите созданный на предыдущем этапе файл с расширением сертификат.pfx на компьютер (Вам необходимо вспомнить путь к копии Сертификата).
2. Запустите оснастку Сертификаты, для этого выберите кнопку Пуск панели задач и далее Все программы/Администрирование/Сертификаты.
3. В окне структуры оснастки Сертификаты откройте папку Доверенные корневые сертификаты, затем папку Сертификаты. В правом подокне появится список Ваших сертификатов.
4. Щелкните правой кнопкой мыши на пустом месте правого подокна.
5. В появившемся контекстном меню выберите команду Все задачи.
6. В ее подменю выберите команду Импорт (Import)(рис 3.11).

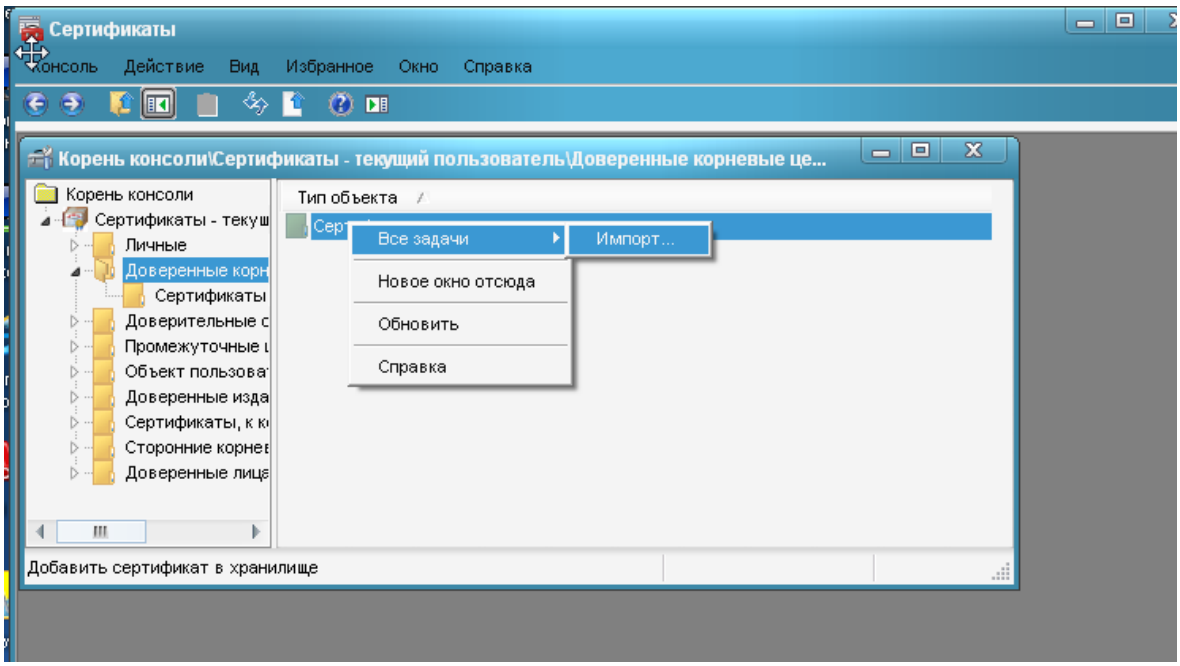


Рис. 3.11

7. Запустится Мастер импорта сертификатов(3.12).

8. Следуйте указаниям мастера — укажите местоположение файла сертификатах и сообщите пароль защиты данного файла.

9. Для начала операции импорта нажмите кнопки Готово и ОК.

10. После завершения процедуры импорта нажмите кнопку ОК и закройте окно Мастера импорта.

В результате Ваших действий текущий пользователь или Вы сами получите возможность работать с зашифрованными данными на этом компьютере.

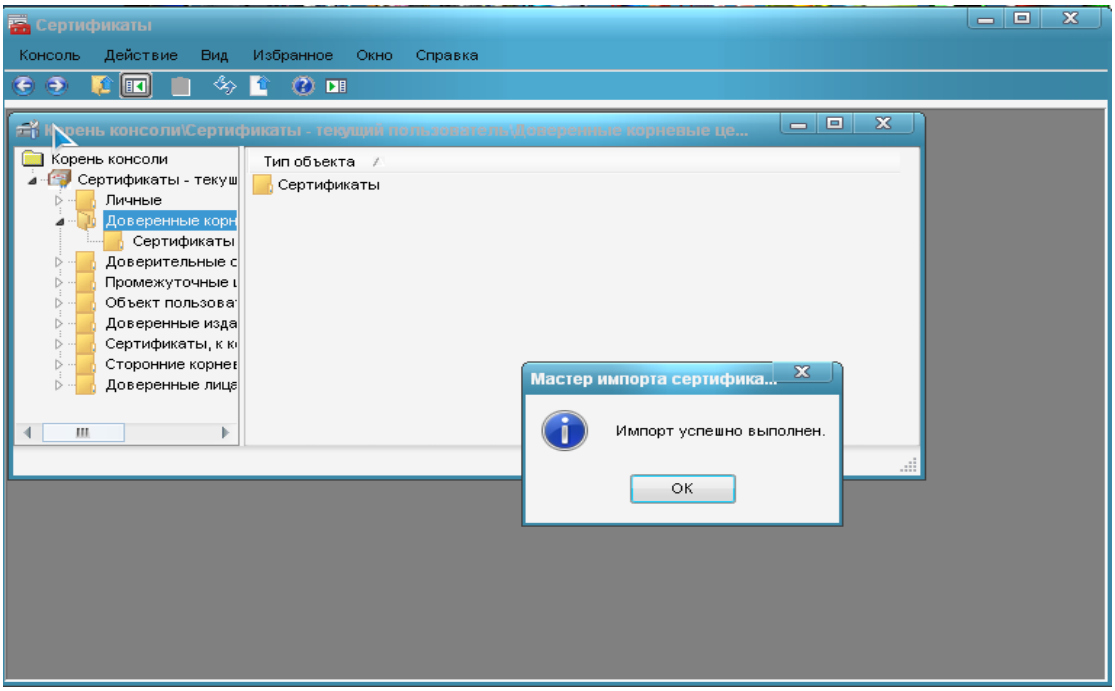


Рис. 3.12

Задания для самостоятельной работы

1. Экспортируйте сертификат № 2 из папки Промежуточные центры сертификации Root Agency (сохраните иллюстрации для отчета).

2. Импортируйте экспортированный сертификат в папку Личные (сохраните иллюстрации для отчета).

Вопросы для контроля знаний:

1. Система администрирования Webmin.
2. Анализатор полномочий.
3. Обзор анализатора связей.
4. Ориентированный метод.
5. Archie. ARP протокол решения.
6. DNS. Управляющий список.

Тема 4. МЕТОДЫ АДМИНИСТРИРОВАНИЯ

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?

Лабораторная работа

Настройка параметров регистрации и аудита в Windows XP

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

1. Рабочее задание

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

Изучить принципы организации комплексной защиты информации средствами регистрации и аудита.

2. Методические указания к выполнению

Регистрация является еще одним механизмом обеспечения защищенности информационной системы. Этот механизм основан на подотчетности системы обеспечения безопасности, фиксирует все события, касающиеся безопасности. Эффективность системы безопасности принципиально повышается в случае дополнения механизма регистрации механизмом аудита. Это позволяет оперативно выявлять нарушения, определять слабые места в системе защиты, анализировать закономерности системы, оценивать работу пользователей и т. д.

Аудит — это анализ накопленной информации, проводимый оперативно, в реальном времени или периодически (например, раз в день). Оперативный аудит с автоматическим реагированием на выявленные нештатные ситуации называется активным.

Практическими средствами регистрации и аудита являются:

- различные системные утилиты и прикладные программы;
- регистрационный (системный или контрольный) журнал.

Первое средство является обычно дополнением к мониторингу, осуществляемому администратором системы. Комплексный подход к протоколированию и аудиту обеспечивается при использовании регистрационного журнала.

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.

Алгоритм выполнения работы

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

1. Выберите кнопку **Пуск** панели задач.
2. Откройте меню **Настроить/Панель управления**.

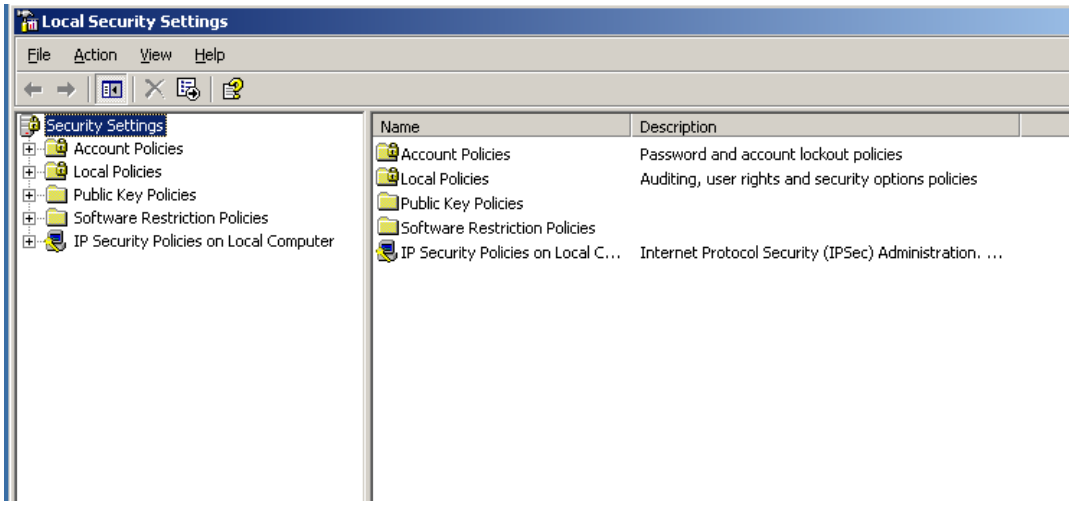
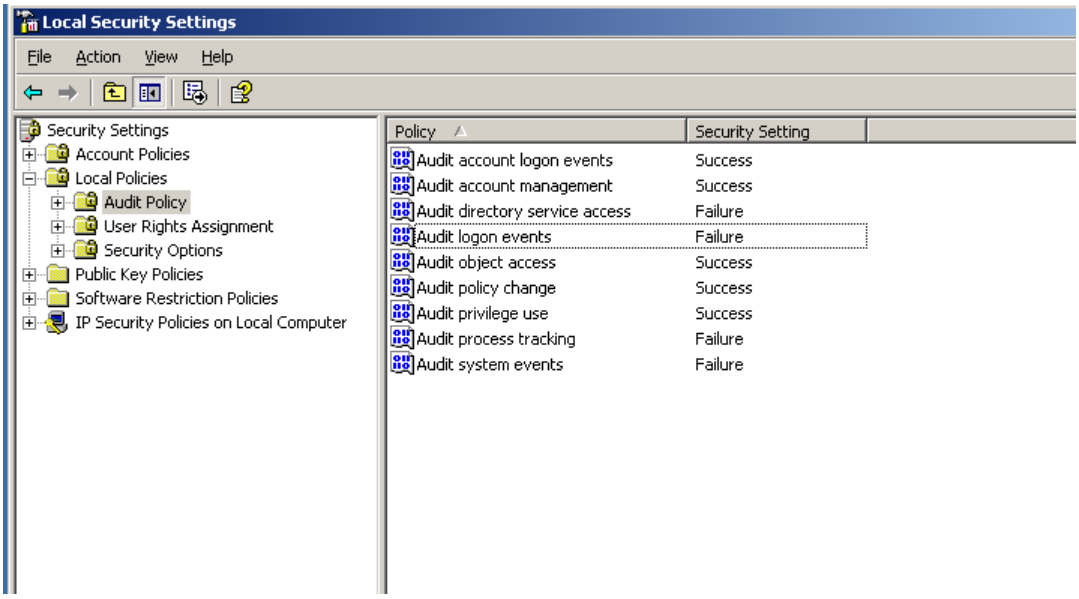


Рис. 4.1

1. В открывшемся окне выберите ярлык

2.Администрирование/ Локальная политика безопасности (рис. 4.1).

3. Выберите пункт Политика аудита(рис 4.2).



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

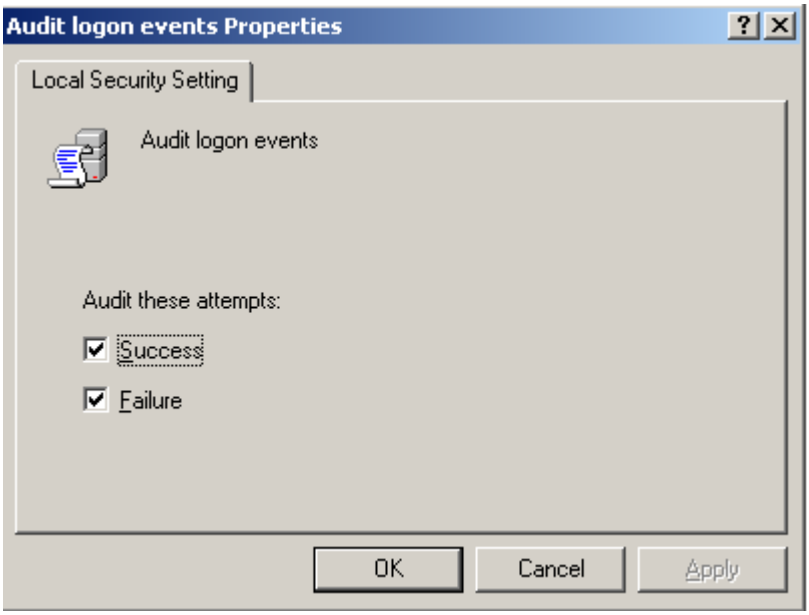


Рис. 4.3

4. Для каждого параметра можно задать аудит успехов или отказов, либо вообще отключить аудит событий данного типа(рис 4.3).
5. Значения параметров политики аудита приведены на лекциях.
6. По умолчанию все параметры политики аудита выключены.
7. Включите аудит успеха и отказа для всех параметров.

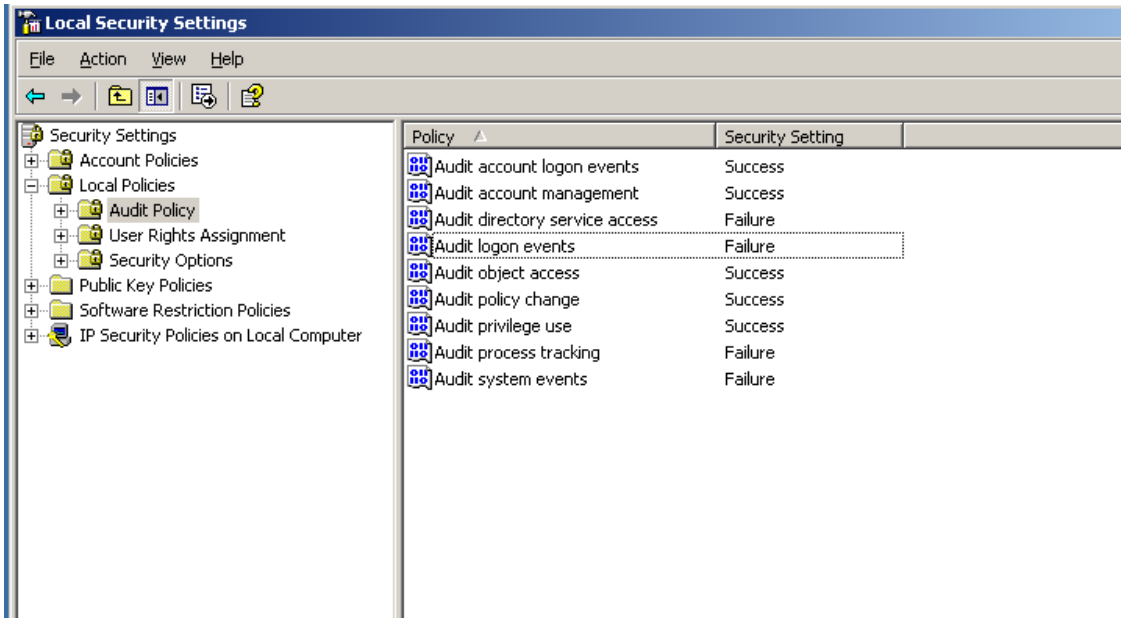


Рис. 4.4

8. Для этого выполните (рис. 4.4).
9. Нажмите кнопку ОК.

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(рис.4.5)**.
3. В окне свойств папки или файла перейдите на вкладку **Безопасность.**

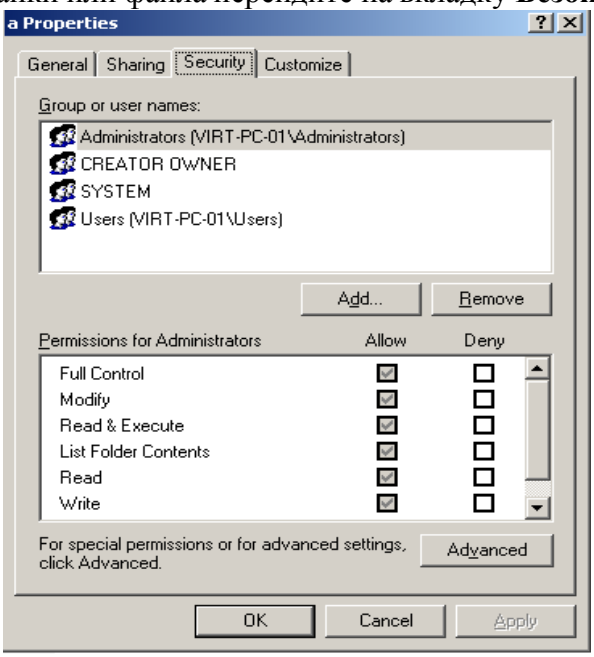


Рис. 4.5

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(рис. 4.6).

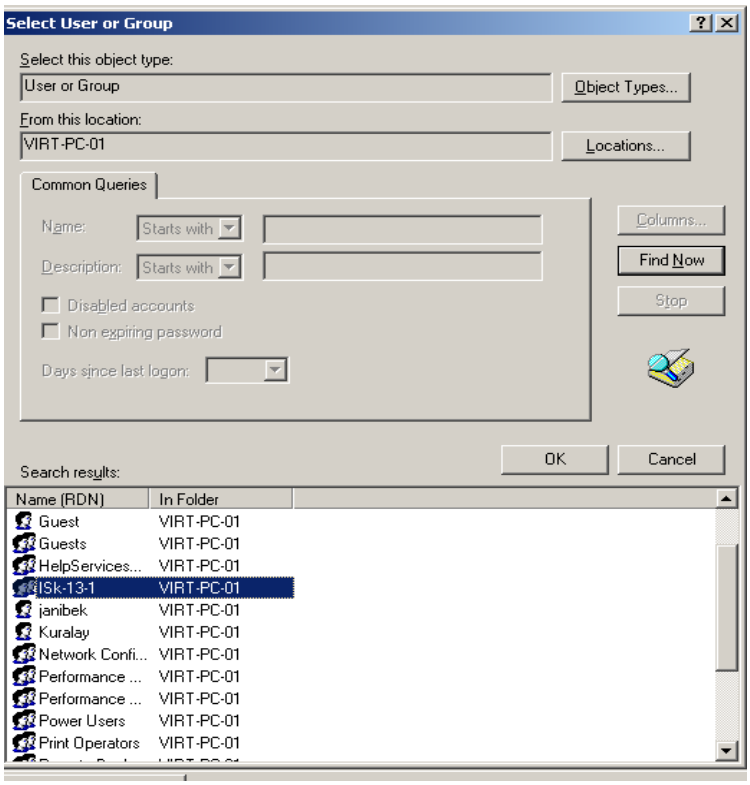


Рис. 4.6

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(рис.4.7).

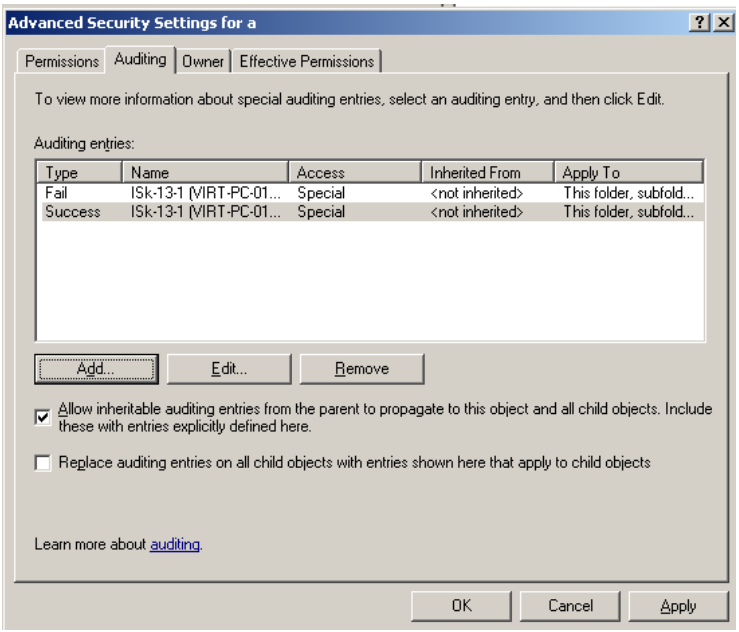


Рис. 4.7

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.

С. 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(рис. 4.8).
4. В открывшемся окне выберите пункт Безопасность.

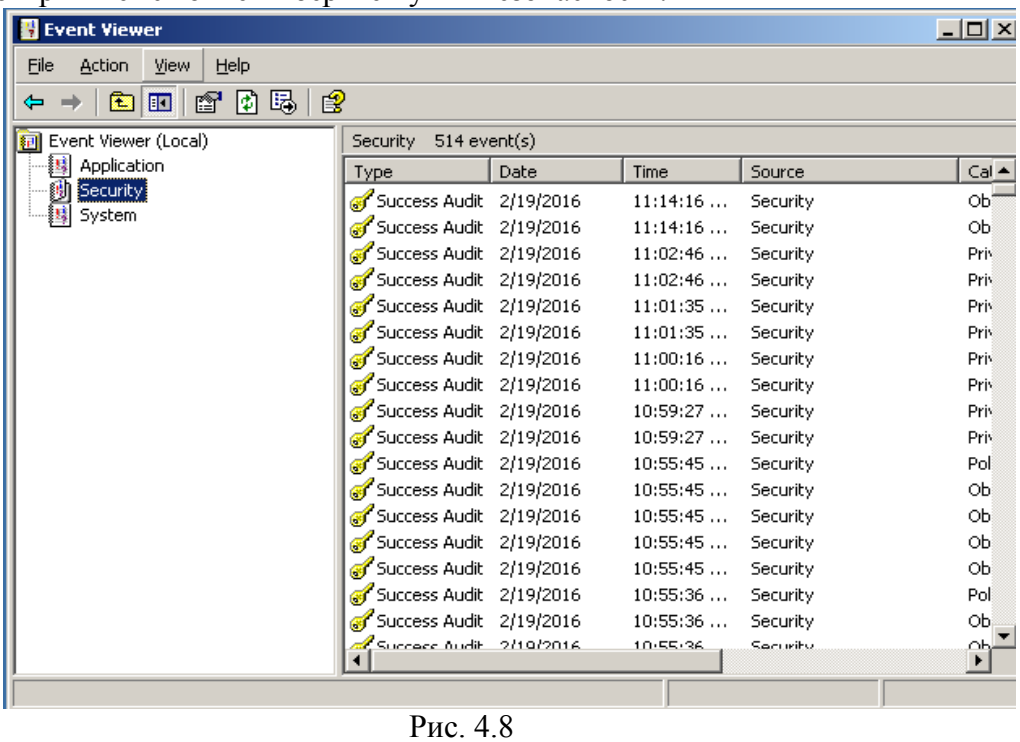


Рис. 4.8

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 рис. 4.9

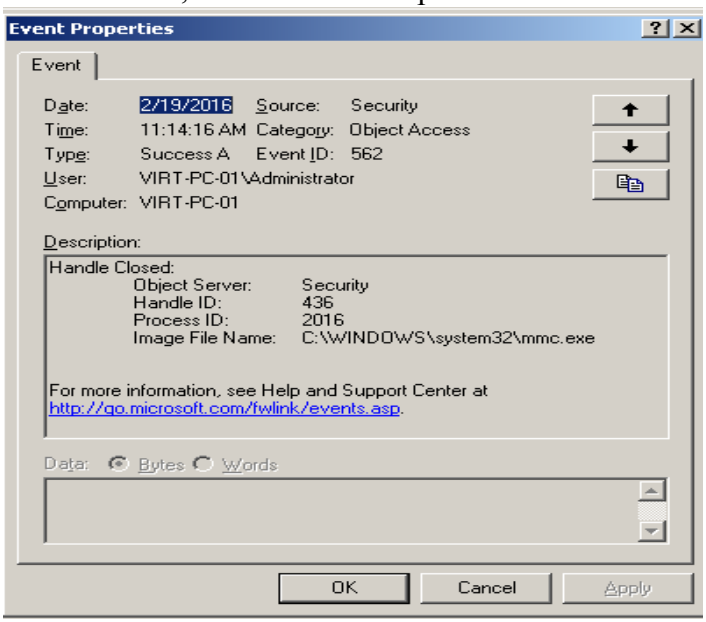


Рис. 4.9

8.В показанном примере зафиксирован успех отключения учетной записи Гость пользователем Админ 8.05.04 в 18.28.31.

9. В примере, показанном на рисунке 4.10., 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.

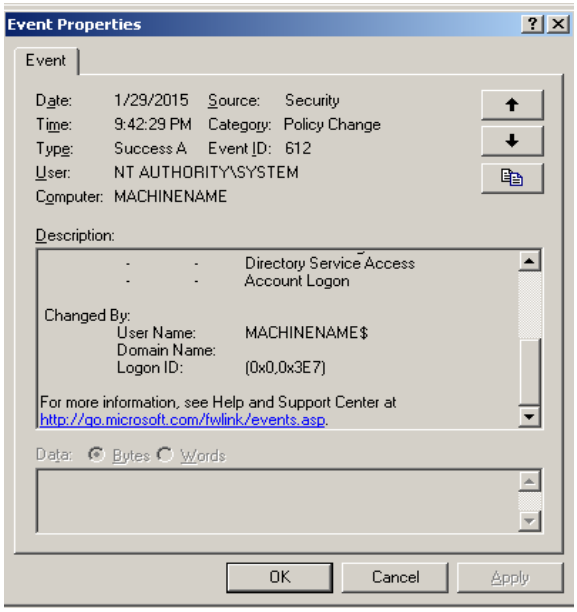


Рис. 4.10

Задания для самостоятельной работы

1. Включите аудит успеха и отказа всех параметров (используйте задание А).

2. Выйдите из системы и предпримите попытку входа в операционную систему с неверным паролем. Откройте журнал событий, найдите соответствующую запись и скопируйте экран в буфер (Print Screen) для отчета.

3. Удалите созданную ранее учетную запись ПЗ-6 и зафиксируйте все события системного журнала, связанные с этим действием для отчета.

Вопросы для контроля знаний:

1. Сканирование портов.
2. Анализаторы полномочий.
3. Сетевой мониторинг.
4. Анализаторы связей.
5. Мониторинги процессов.
6. Системные информаторы.
7. Телекс ресурсов.
8. Работа с системой от имени Администратора.

Тема 5. СЛУЖБЫ УПРАВЛЕНИЯ И КОНТРОЛЯ

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?

Лабораторная работа

Управление шаблонами безопасности в Windows XP

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

1. Рабочее задание загрузить редактор Шаблона безопасности, редактировать шаблон безопасности и сохранить его с новым именем.

2. Методические указания к выполнению

Управление шаблонами безопасности в Windows 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 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 на- стройки безопасности начнут действовать.

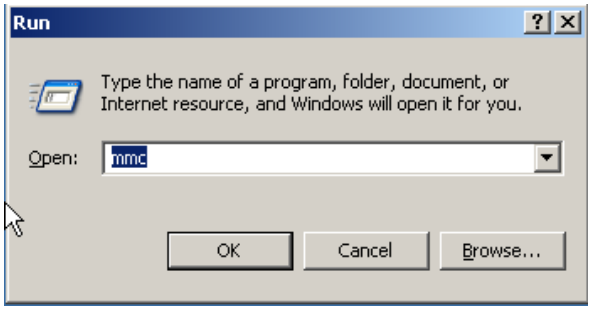
Значения параметров обеспечения безопасности заносятся в текстовые файлы с расширением inf, называемые Шаблонами безопасности.

Примечание. Новые Шаблоны безопасности не изменяют все старые настройки параметров системы безопасности, они лишь дополняют их, увеличивая (инкрементируя) степень защищенности компьютера..

Алгоритм выполнения работы

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(рис 5.1).



Рим. 5.1

5. В меню Консоль выберите команду Добавить или удалить оснастку (рис. 5.2) и нажмите кнопку Добавить.

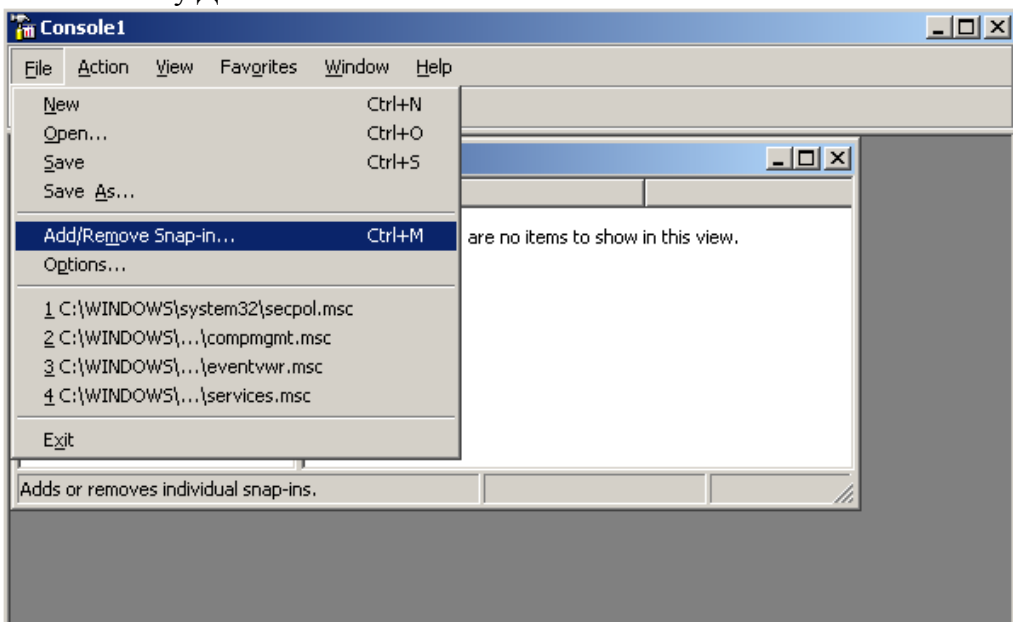


Рис. 5.2

6. В поле Оснастка дважды щелкните Шаблоны безопасности.

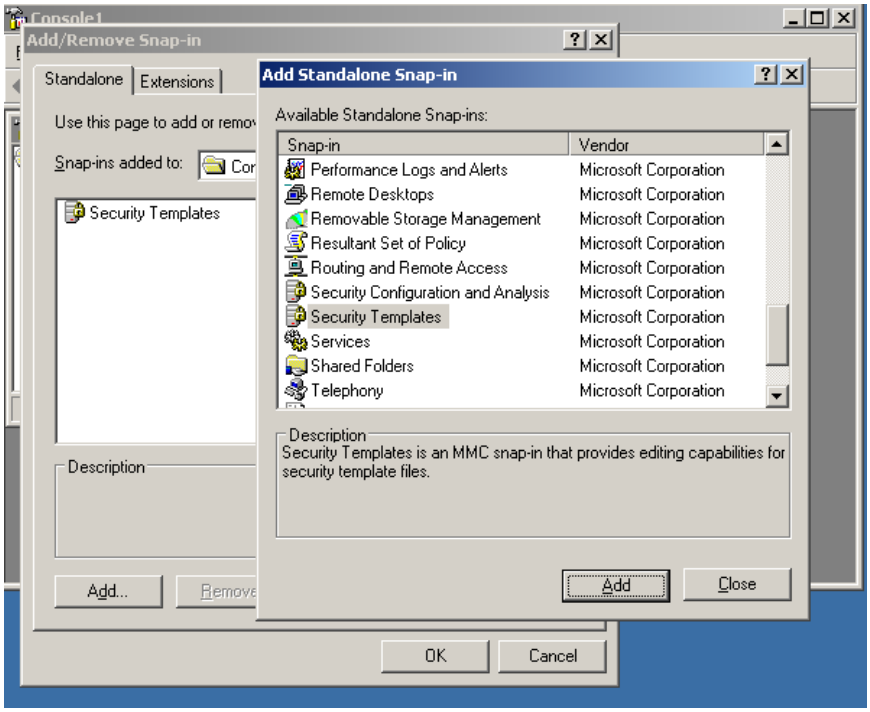


Рис. 5.3

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.

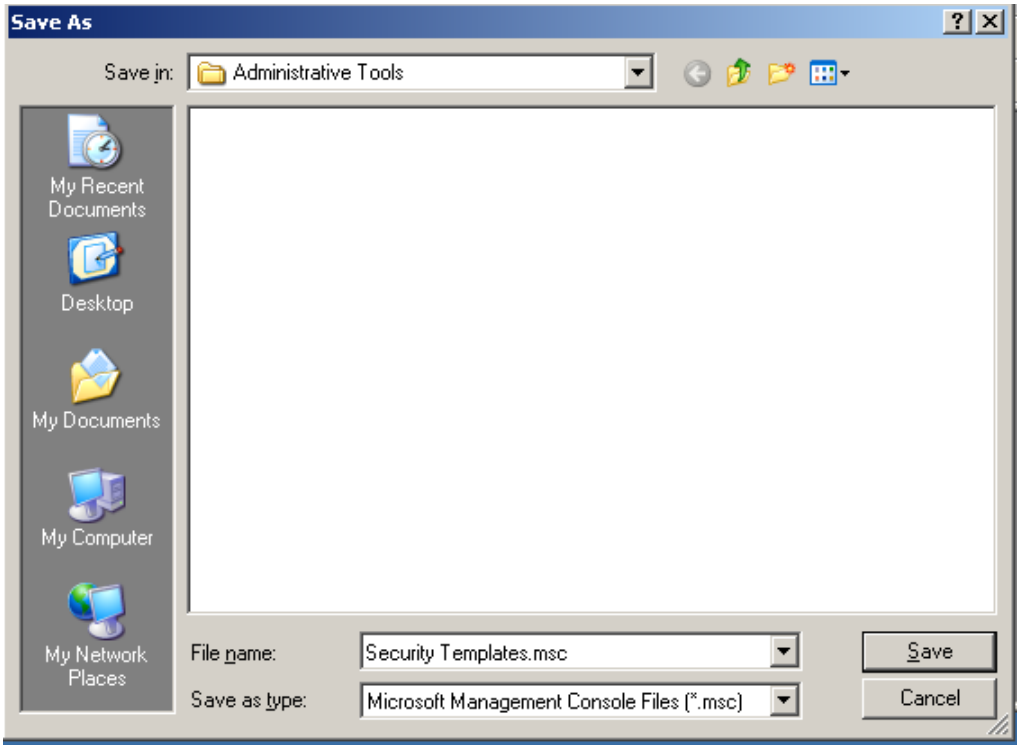


Рис. 5.4

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).

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.

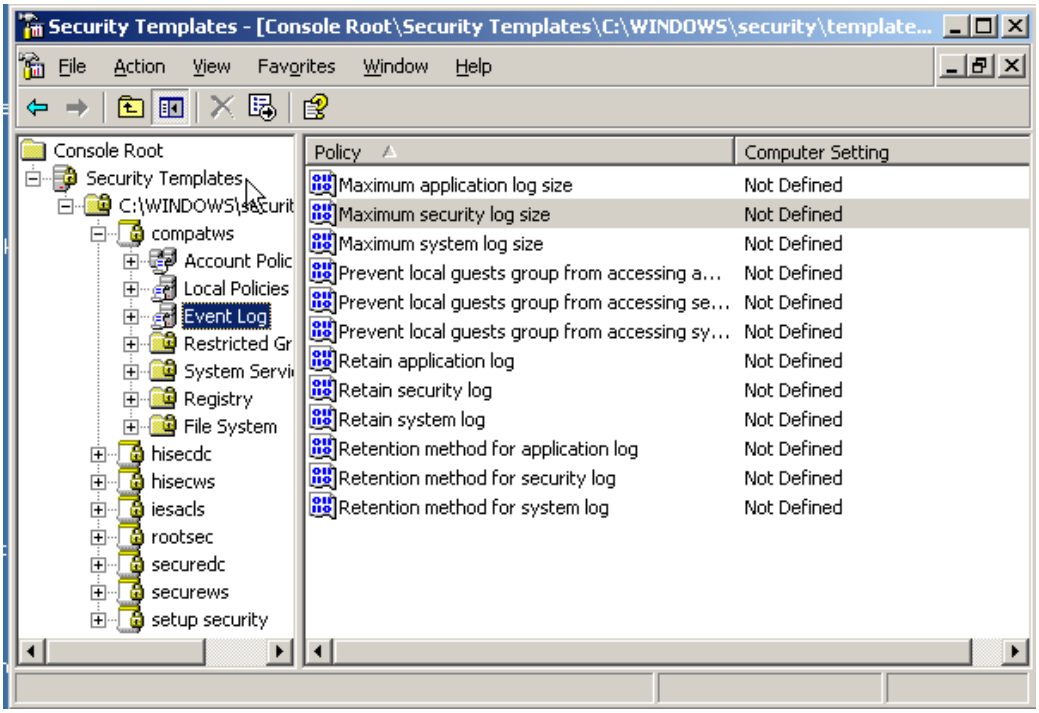


Рис. 5.5

Редактирование и сохранение шаблона безопасности.

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

2. Если Вы хотите модифицировать какую-либо на стройку безопасности, дважды щелкните на ней и отредактируйте значения параметров.

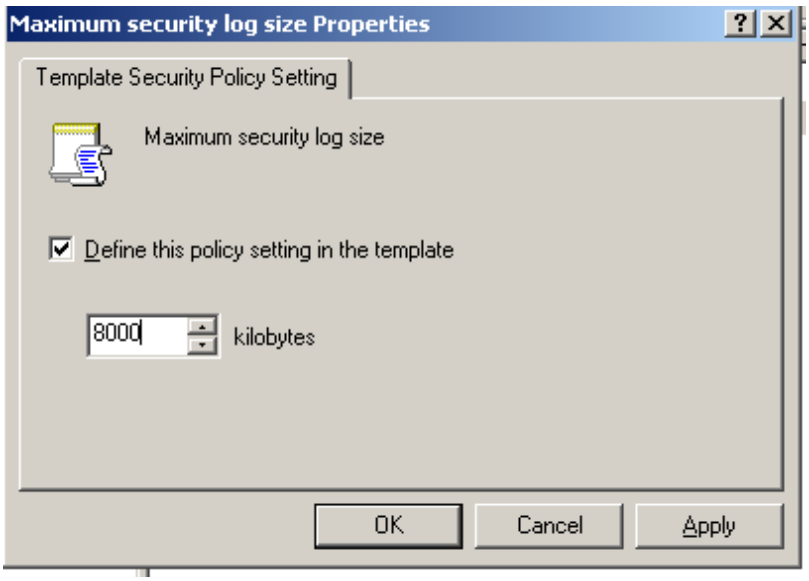


Рис. 5.6

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

%System%\Secunfy \Templates.

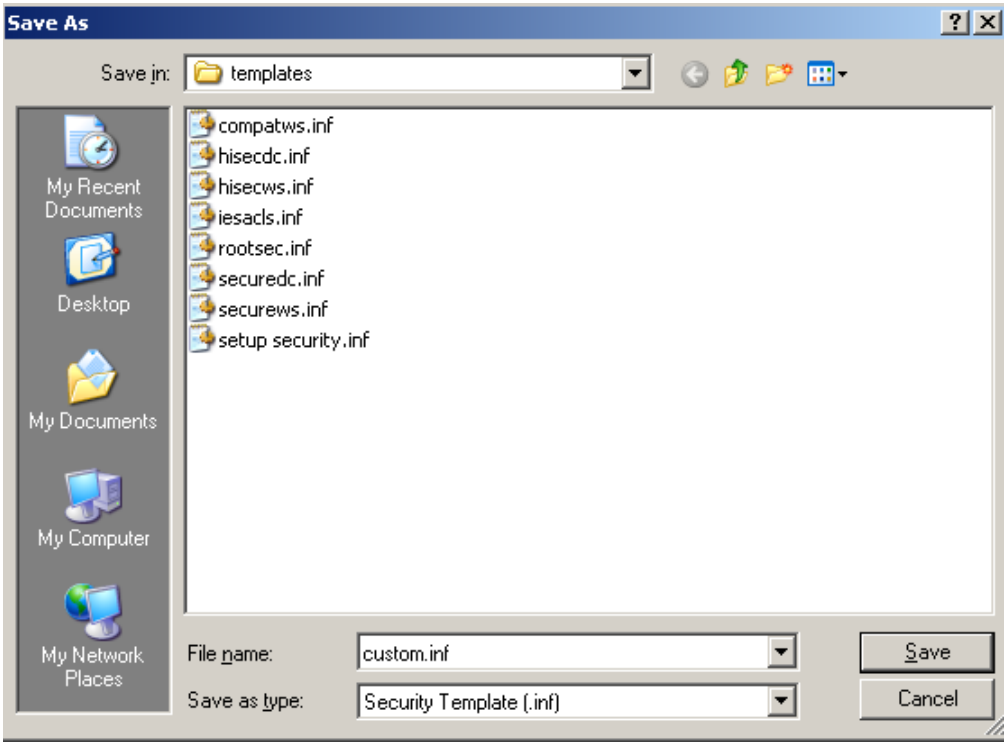


Рис. 5.7

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

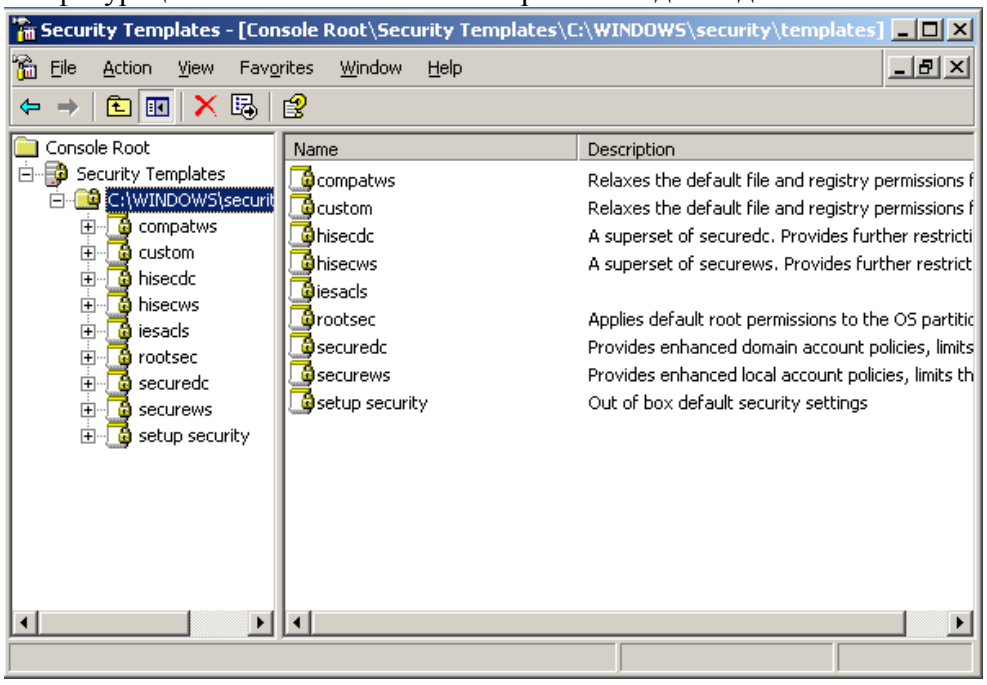


Рис. 5.8

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.

Задания для самостоятельной работы

Создайте на базе существующего Шаблона безопасности новый шаблон и дайте ему имя ПЗ-8. После этого зафиксируйте список шаблонов, ско- пировав изображение экрана в буфер и далее в файл для отчета.

Вопросы для контроля знаний:

1. Службы управления конфигурацией.
2. Службы контроля характеристик.
3. Службы управления ошибочными ситуациями.
4. Службы учета и безопасности систем.
5. Службы управления общего пользования.

Тема 6. ИНФОРМАЦИОННЫЕ И ИНТЕЛЛЕКТУАЛЬНЫЕ СЛУЖБЫ

Контрольные вопросы:

1. Что такое реестр?
2. Поясните особенности «троянских программ».
3. Почему профилактика «троянских программ» связана с системным реестром?

Лабораторная работа

Конфигурации системы реестра операционной системы Windows XP

Цель работы: изучение работы в реестре.

1. Рабочее задание проверить потенциальные места записей «троянских программ» в системном реестре операционной системы Windows 2003 (XP).

Изучить стандартные средства просмотра и редактирования реестра Windows.

2. Методические указания к выполнению

Реестр операционной системы Windows — это большая база данных, где хранится информация о конфигурации системы. Этой информацией пользуются как операционная система Windows, так и другие программы. В некоторых случаях восстановить работоспособность системы после сбоя можно, загрузив работоспособную версию реестра, но для этого, естественно, необходимо иметь копию реестра. 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 6.1):

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 (рис.6. 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)).

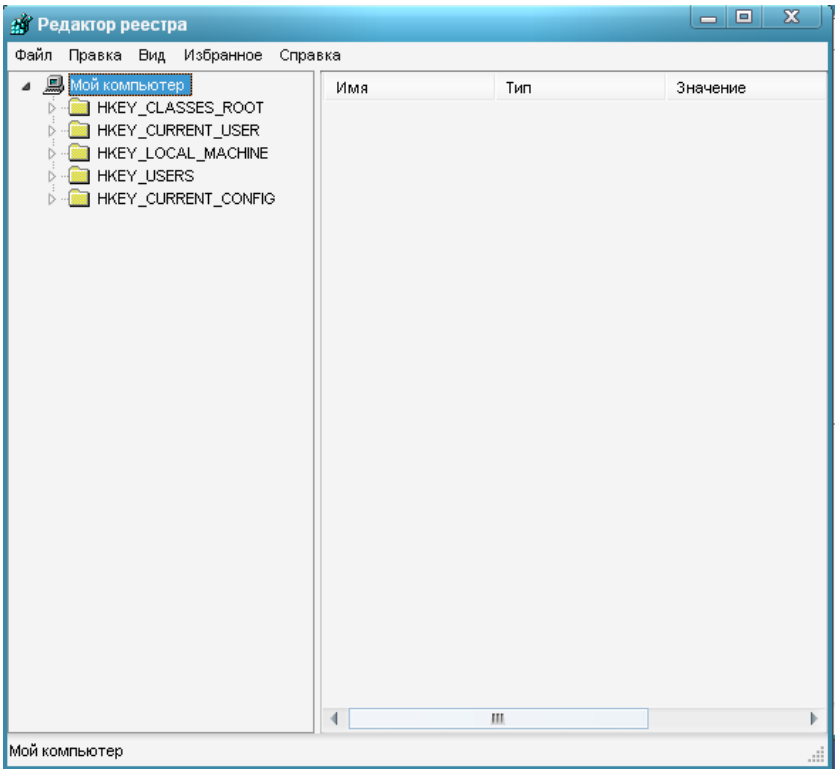


Рис. 6.1

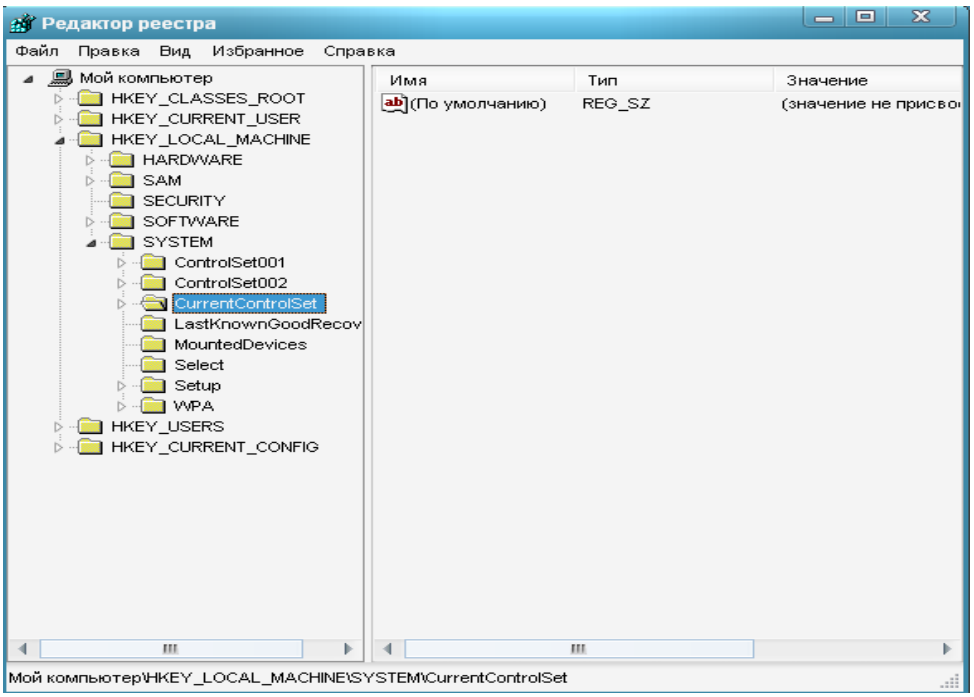


Рис. 6.2

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 HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\hivel ist (рис.6.3).

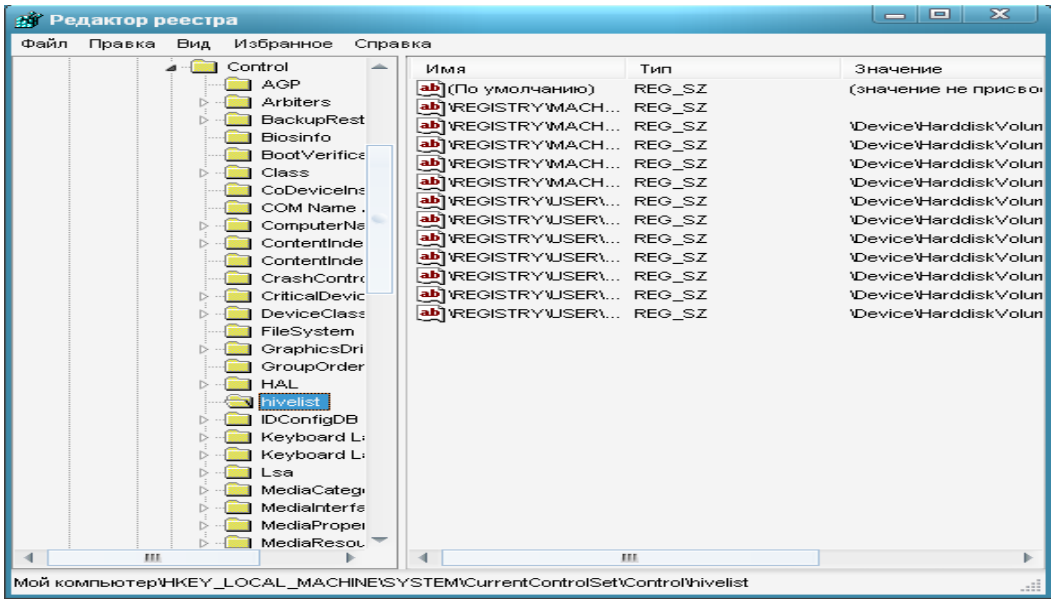


Рис. 6.3

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

Алгоритм выполнения работы

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.

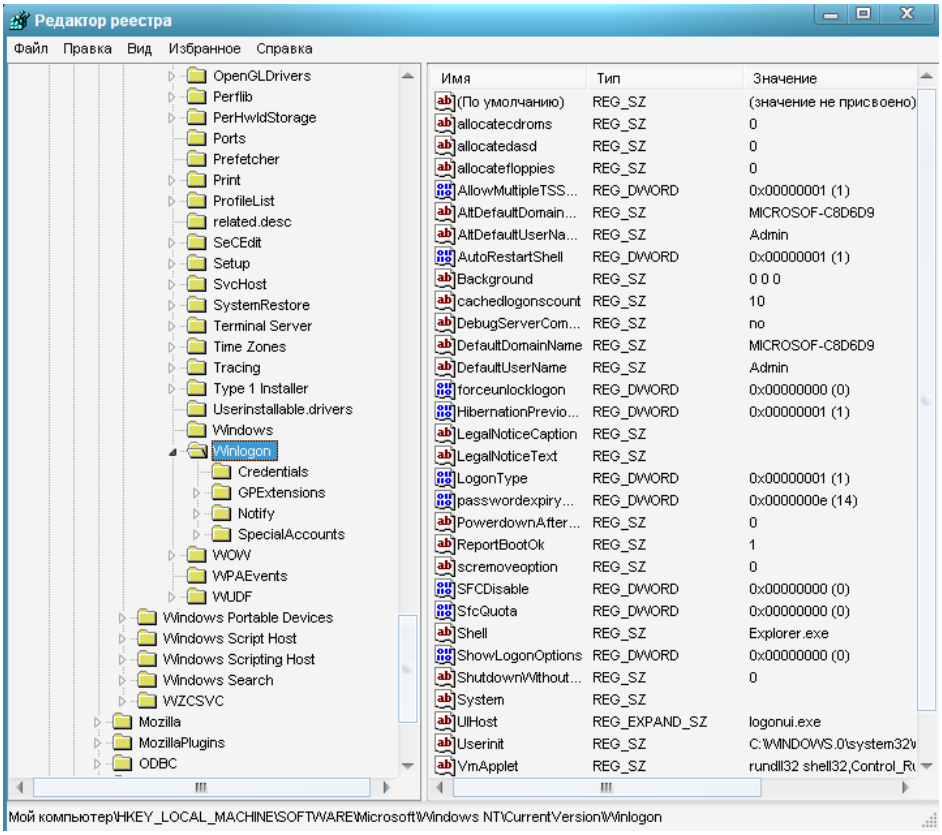


Рис. 6.4

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 (рис.6.4).

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 6.5) удалите ссылку на подозрительный файл.

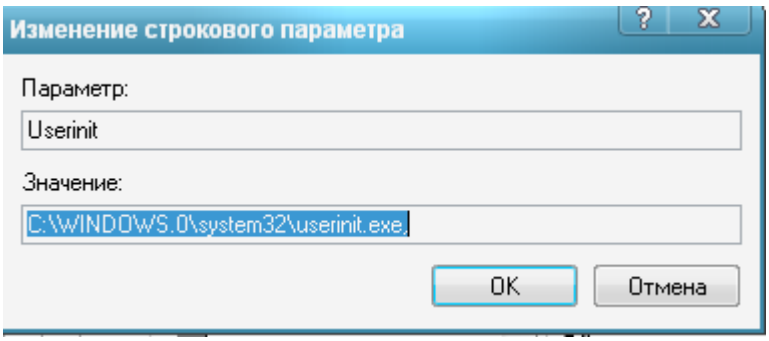


Рис. 6.5

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) (рис. 6.6).

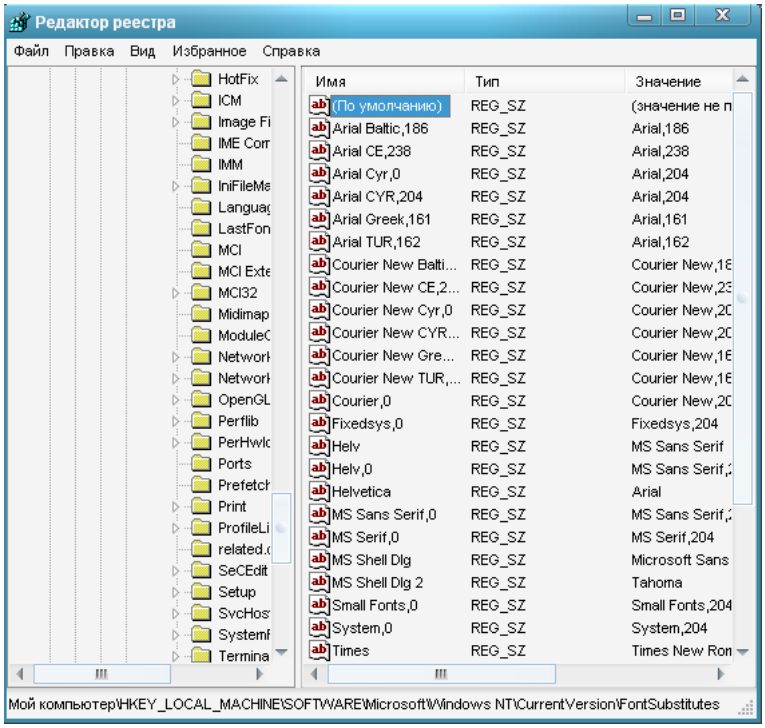


Рис. 6.6

3. В рассматриваемом примере автоматически запускается резидентный антивирус и его планировщик заданий, а также утилита, относящаяся к программе Nero (запись на CD).
4. Если в указанном разделе есть записи вызывающие подозрения, то выполните пункты 6-14 предыдущего задания.

Задания для самостоятельной работы

1. Проверьте содержимое ключа HKEY_LOCAL_MACHINE\Software\Microsoft\WindowsNT\Current Version\Winlogon\System(REG.SZ).
2. Зафиксируйте этапы работы, используя командуь PrintScreen клавиатуры.
3. Составьте отчет о результатах проверки.

Вопросы для контроля знаний:

1. Информационные службы.
2. Интеллектуальные службы.
3. Диспетчер служебных программ.
4. Определенные задания. Служба AT.

Тема 7. СЛУЖБЫ РЕГИСТРАЦИИ, СБОРА И ОБРАБОТКИ ИНФОРМАЦИИ

Контрольные вопросы:

1. Какие существуют основными приемы управления с помощью мыши?
2. Как создать новый текстовый файл?
3. Как создать архив файла?
4. Как осуществляется поиск файла?

Лабораторная работа

Knoppix 3.8 - знакомство с интерфейсом, файловой системой

1. Цель работы

1.1 Получение базовых навыков работы в ОС Knoppix 3.8, знакомство с интерфейсом и файловой системой.

2. Пояснение к работе

2.1 Краткие теоретические сведения

Текстовый процессор OpenOffice – это бесплатная программа, позволяющая полноценно работать с текстовыми документами. По интерфейсу и возможностям она весьма похожа на Microsoft Word, что позволяет работать в ней без долгого переучивания. Управление мышью аналогично интерфейсу Windows Основными приемами управления с помощью мыши являются:

- одинарный щелчок левой кнопкой (для выделения объекта);
- двойной щелчок левой кнопкой (для запуска программ на исполнение)
- одинарный щелчок правой кнопкой (для вызова *контекстного* меню, при этом у каждого объекта свое *контекстное* меню);
- перетаскивание (drag-and-drop) объекта левой кнопкой (перемещение выделенного экранного объекта с цель его копирования, переноса, удаления);
- протягивание левой или правой кнопкой мыши (drag) (выделение объектов или изменение размеров объекта);
- зависание — наведение указателя мыши на значок объекта или на элемент управления и задержка его на некоторое время (при этом обычно на экране появляется всплывающая подсказка, кратко характеризующая свойства объекта).

2.2 Перечень используемого оборудования

Персональный компьютер

3. Задание

3.1. Через меню-приложений выберите несколько мини-приложений, расположите их по своему усмотрению

3.2. Модифицирую панель инструментов менеджера Dolphin, добавив к кнопкам «назад» и « вперед» кнопку « вверх»

3.3. Создайте новый текстовый файл в вашей домашней папке

3.4. Скопируйте этот файл в другую папку Документы и создайте ссылку на него в папке tmp

3.5. Посмотрите свойства трех полученных файлов, чем появившееся окно отличается от окна свойств документа Windows?

3.6. Создайте новую папку, посмотрите ее свойства

3.7. Запустите поиск файлов с расширением .jmp во всех папках

3.8. Запустите файл в архив и распакуйте файл в вашу домашнюю папку

3.9. Наберите команду Help. Появится список внутренних комкнд. Запросите информацию по нескольким указанным командам (help имя команды_команда). Что они делают?

3.10. Представьте все процессы в виде дерева. Отследите хранение информации о идентификаторах процесса. Посмотрите диаграммы работы системы

4. Работа в кабинете

4.1 Ознакомиться с теоретическим материалом по лабораторной работе.

4.2 Выполнить предложенные задания.

4.3 Продемонстрировать результаты выполнения предложенных заданий.

Вопросы для контроля знаний:

1. Службы регистрации.
2. Службы сбора и обработки информации.
3. Программа «Сведения о системе».

Тема 8. СЛУЖБЫ ПЛАНИРОВАНИЯ И РАЗВИТИЯ ИНФОРМАЦИОННЫХ СИСТЕМ

Контрольные вопросы:

1. Как настроить параметры страницы в OpenOffice?
2. Как создать список?
3. Как настроить табуляцию в OpenOffice?
4. Как настроить параметры автозамены?

Лабораторная работа

Встроенное ПО в Knoppix 3.8: электронный офис - OpenOffice, KOffice

1. Цель работы

1.1. Получить практические навыки работы в электронном офисе- OpenOffice, KOffice

2. Пояснение к работе

2.1 Краткие теоретические сведения

Текстовый процессор OpenOffice – это бесплатная программа, позволяющая полноценно работать с текстовыми документами. По интерфейсу и возможностям она весьма похожа на Microsoft Word, что позволяет работать в ней без долгого переучивания.

Запустите текстовый процессор Open Office (Menu -> Офис -> Текстовый процессор OpenOffice)

1. Первичные настройки текстового процессора

Первичные настройки производятся в меню Сервис-> Параметры

2. Настройки параметров страницы документ рисунок 2.1

Она производится в меню Формат -> Страница

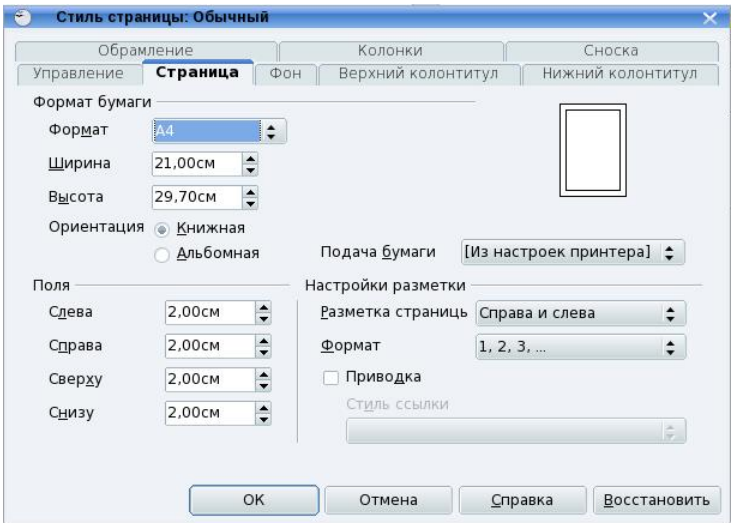


Рисунок 2.1 - Настройки параметров страницы документа

3. Настройка свойств шрифта рисунок 2.2

Она производится в меню формат -> символы

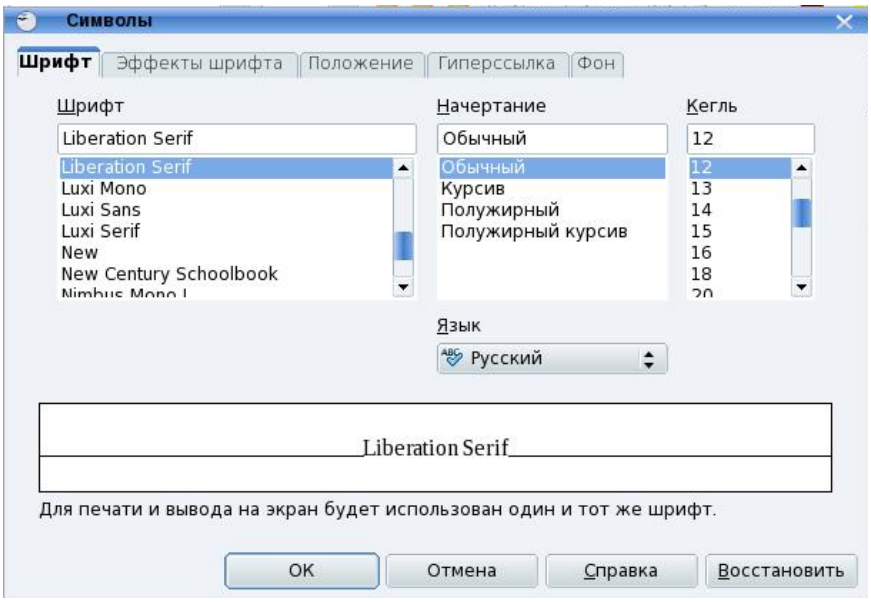


Рисунок 2.2 - Настройка свойств шрифта

1.4. Настройка свойств абзаца

Она производится в меню формат -> абзац

1.5. Списки

Списки создаются в меню Формат -> Маркеры и нумерация

Удобное средство задания уровня списка – Tab – сдвинуть на уровень вниз, Backspace – на уровень вверх.

1.6. Табуляция

Табуляция настраивается в меню Формат -> Абзац ->Табуляция. Позиция табуляции указывается на линейке документа. Для задания табуляции используется клавиша Tab.

1.7. Настройка параметров автозамены

Настройка параметров автозамены производится в меню Сервис -> автозамена.

1.8. Вставка специальных символов.

Она производится в меню Вставка -> Символы

1.9. Колонки

Колонки настраиваются в меню Формат -> Колонки

2.2 Перечень используемого оборудования

Персональный компьютер

3. Задание

3.1. Настройте следующие параметры текстового процессора

- Единицы измерения для настройки параметров документа – см;
- Автосохранение каждые 10 минут;
- Запретите автоматическую проверку орфографии и грамматики
- Включите автоматическую замену «прямых» кавычек парными;
- Отключите Помощника.

3.2 Установите в созданном документе следующие параметры:

- Размер бумаги А4 (это стандартный размер листа бумаги 210 на 297 мм);
- Ориентацию бумаги – книжная
- Размеры полей листа – левое – 2,75 см; правое 1,25 см; Верхнее – 2 см; Нижнее – 2,25 см.

3.3. Наберите следующий текст:

Текстовый·редактор·OpenOffice·позволяет·использовать·различные·шрифты·(ACTiONiS,·Times, Courier)·менять·их·размер·(размер·шрифта·10,··размер·шрифта·18),·использовать шрифт·различного·типа·(**жирный**,·*курсив*,·подчеркнутый,·**и·их·различные**·*сочетания*, подчеркнутый·линиями·разного·типа,·использовать·~~зачеркнутый~~·шрифт,·скрытый·шрифт·(скрытый·шрифт·),·^{верхние}·и·$_{нижние}$·индексы,·изменять·цвет·шрифта,·применять·различные эффекты·(мигающий·))¶

3.4 Наберите следующий текст

Пример абзаца с выравниванием по левому краю, красная строка 1,2 см. Межстрочный интервал одинарный, автоматический перенос слов запрещен.

Пример абзаца с выравниванием по правому краю, красной строки нет. Межстрочный интервал одинарный, автоматический перенос слов разрешен.

Пример абзаца с выравниванием по центру, без красной строки. Межстрочный интервал полуторный, автоматический перенос слов запрещен.

Пример абзаца с выравниванием по ширине, красная строка 1,2 см. Межстрочный интервал одинарный, автоматический перенос слов разрешен, интервал перед абзацем 0,8 см, после — 0,6 см.

3.5 Наберите следующий текст

1. Пункт первого уровня
   1.1. Пункт второго уровня
   1.2. Ещё один пункт второго уровня
      a) третий уровень
         - четвертый
      b) снова третий
2. Первый уровень

3.6 Наберите следующий текст, используя выравнивание по символу

Номер элемента	Величина
Первый элемент	13,45678
Второй элемент	456,788
Третий элемент	12,678

3.7 Настройте автозамену аббревиатуры УПЭК на полное название.

3.8 Наберите следующий текст (греческое слово «человек»)

ἄνθρωπος

3.9 Наберите следующий текст:

Текстовый процессор OpenOffice позволяет использовать форматирование в виде многоколоночного текста	(в том числе с колонками различной ширины — в данном случае 6, 4 и 5	сантиметров соответственно, интервал между колонками— 1 см.)

4 Работа в кабинете

4.1 Ознакомиться с теоретическим материалом по лабораторной работе.

4.2 Выполнить предложенные задания.

4.3 Продемонстрировать результаты выполнения предложенных заданий.

Вопросы для контроля знаний:

1. Службы планирования.
2. Службы развития.
3. Службы планирования синхронизации автономных элементов.

Тема 9. ЭКСПЛУАТАЦИЯ И СОПРОВОЖДЕНИЕ ИНФОРМАЦИОННЫХ СИСТЕМ

Контрольные вопросы:

1. Как запустить служебное приложение «Системный монитор»?

2. Для чего предназначено это приложение?

3. Какие показатели можно проанализировать с помощью программы «Системный монитор»?

4. В каком виде возможно отобразить параметры?

Лабораторная работа

СИСТЕМНЫЙ МОНИТОР

Цель: Изучить процессы, происходящие в оперативной памяти и процессоре, во время исполнения прикладной программы.

Ход работы:

1. Изучить *Рекомендации к выполнению работ*.
2. Пользуясь рекомендациями, запустить, изучить и настроить для выполнения работы Системный монитор.
3. Изучить *Порядок выполнения работ*.
4. Выполнить лабораторную работу
5. Подготовить отчёт о проделанной работе в формате MS Word.
6. Ответить на контрольные вопросы

Рекомендации к выполнению работ:

1. В состав операционной системы Windows XP входит программа **Системный монитор**, с помощью которой можно наблюдать за изменением различных показателей во время работы компьютера, а также измерять производительность компьютера.

Запустите эту программу из меню программ: **Пуск/Панель управления/Производительность и обслуживание/Администрирование** и дважды щелкните по значку **Производительность.** Данный инструмент включает системный монитор (реализованный в виде элемента управления Active X) и Журналы и оповещения производительности (автономная оснастка для конфигурирования журналов производительности).

2. Система Windows XP получает информацию о производительности от компонентов операционной системы. Различные системные компоненты в ходе своей работы генерируют данные о производительности. Такие компоненты называются *объектами производительности*. В операционной системе имеется ряд объектов производительности, обычно соответствующих главным аппаратным компонентам, таким как *память, процессоры* и т. д. Приложения могут также инсталлировать свои объекты производительности. Каждый объект производительности предоставляет *счетчики*, которые собирают данные производительности. Например, счетчик Обмен страниц в сек(Pages/sec) объекта Память (Memory) отслеживает степень кэширования страниц.

Для просмотра данных, которые предоставляет конкретный счетчик, нажмите кнопку **Объяснение** (Explain) в диалоговом окне добавления счетчиков **Добавить счетчики.**

Если в системе установлено несколько процессоров, то объект Процессор (Processor) будет иметь множество экземпляров. Более того, если объект поддерживает множество экземпляров, то при объединении экземпляров в группу появятся родительский экземпляр и дочерние экземпляры, которые будут принадлежать данному родительскому экземпляру.

Настроим программу так, чтобы видеть нужные нам характеристики.

Настройка счетчиков.

В окне **Системный монитор** на панели результатов в виде диаграмм отображаются показания счетчиков. В системе Windows XP это окно изначально содержит три счетчика: *Обмен страниц в сек* (Pages/sec) (объект Память), *Средняя длина очереди диска* (Avg. Disk Queue Length) (объект Физический диск) и *% загруженности процессора* (Processor Time) (объект Процессор). Для добавления других счетчиков выполните следующие действия:

a) На панели результатов щелкните правой кнопкой мыши и в контекстном меню выберите команду **Добавить счетчики**, Другой подход — нажать кнопку **Добавить** на панели инструментов или сочетание клавиш **<Ctrl>+<!>.**

b) В открывшемся окне выберите переключатель **Использовать локальные счетчики** для мониторинга компьютера, на котором запущена консоль мониторинга. Если вы собираетесь проводить мониторинг определенного компьютера, независимо от того, где запущена консоль мониторинга, установите переключатель **Выбрать счетчики с компьютера** и укажите имя компьютера (по умолчанию установлено имя локального компьютера).

c) В списке **Объект** выберите объект для мониторинга.

d) В списке **Выбрать счетчики из списка** укажите счетчики, которые вы собираетесь использовать.

e) Для мониторинга всех выбранных экземпляров нажмите переключатель **Все вхождения**. Для мониторинга только определенных экземпляров установите переключатель **Выбрать вхождения из списка** и выберите экземпляры, которые вы собираетесь отслеживать.

f) Нажмите кнопку **Добавить** и затем кнопку **Закрыть.**

Нам нужны две диаграммы, показывающие, как загружен работой процессор и насколько занята оперативная память. Добавьте счетчики *% загруженности процессора* и *Диспетчер памяти*.

Настройка способов представления информации.

Компонент Системный монитор предоставляет три средства просмотра информации о производительности системы: два графических **(График** и **Гистограмма**) и одно текстовое **(Отчет).** Для настройки внешнего вида окна мониторинга щелкните правой кнопкой мыши в окне диаграмм и выберите пункт **Свойства**. В открывшемся окне для диаграммы и гистограммы можно задать ряд дополнительных параметров отображения:

- название диаграммы или гистограммы и дать название осям координат;
- диапазон вывода значений;
- характеристики кривой на диаграмме или колонок на гистограмме, такие как цвет, толщина, стиль и др. Для выбора способа просмотра информации производительности на вкладке **Общие** установите флажок для одной из опций **График**, **Гистограмма** или**Отчет.**

Вы увидите две диаграммы. Диаграммы "двигаются" влево, самая правая часть диаграммы - это то, что происходит в текущий момент. Первая диаграмма показывает, на сколько процентов загружен работой процессор, вторая - сколько памяти занято для работы всех программ.

Примечание. Объем используемой памяти может оказаться больше, чем реальный размер оперативной памяти. Тут нет никаких чудес - часть информации временно хранится на диске в специальном файле. Когда эти данные понадобятся, то будут загружены в оперативную память, а другие, давно не использовавшиеся, «сброшены» на диск.

Запустите процесс построения диаграмм заново.

3. Операционная система Windows многозадачная, т.е. мы можем запускать несколько программ, переходить из окна одной программы в окно другой. Не закрывая

Системный монитор, откройте графический редактор **Paint**, подождите немного, затем закройте.

4. На нижней диаграмме вы увидите (по колебаниям графика), как операционная система загрузила Paint в оперативную память, а затем выгрузила. На верхней диаграмме видна работа процессора по запуску редактора и затем - по закрытию.

Возможно, вам придется отрегулировать скорость построения диаграмм (**Диаграмма**) и масштаб диаграммы загрузки памяти (**Изменить представление**).

Ваша задача: с помощью Системного монитора выяснить, как изменяется загрузка процессора и объем занятой оперативной памяти в ходе обычной работы с прикладной программой. Результаты

лабораторной работы нужно будет оформить в виде отчета. Получившаяся в окне Системного монитора диаграмма должна быть «сфотографирована» и помещена в отчет с помощью, например, клавиши **PrintScreen.**

Порядок выполнения работы

1. Загрузите MS Word, откройте новый лист для отчета. Наберите заголовок, сохраните файл.

2. Запустите Системный монитор.

3. Раскройте на весь экран окно программы Системный Монитор и запустите графики заново.

4. После каждого из следующих действий переходите к окну с диаграммами, замечайте, что изменилось (между действиями выдерживайте небольшую паузу, чтобы отделить на диаграмме одно

действие от другого):

• завершите работу программы MS Word;

• запустите Paint;

• перейдите к окну Системного монитора и нажмите клавишу Print Screen, чтобы поместить картинку с экрана в буфер обмена;

• вставьте картинку из буфера обмена в документ программы Paint;

• сохраните файл с картинкой;

• завершите работу программы Paint.

5. Сделайте еще один "снимок" диаграмм и поместите именно его в ваш отчет.

6. Подпишите на диаграммах (на тех участках, где происходят изменения), какие действия вы выполняли.

7. Отметьте на картинке, какой объем памяти занимают операционная система, MS Word, Paint.

8. Создайте на листе вашего отчета таблицу и заполните ее: поставьте плюс, если устройство участвует в операции.

9. Поместите в отчет ответ на следующий вопрос: почему изменения на диаграмме памяти выглядят такими незначительными по сравнению с изменениями на диаграмме процессора?

Действие	Процессор	Оперативная память	Внешняя память
Запуск программы			
Открытие документа			
Редактирование документа			
Сохранение документа			
Завершение			

работы программы			

Вопросы для контроля знаний:

1. Инструменты настройки параметров безопасности.
2. Аудит.
3. Программа Event Viewer.
4. Дисковые квоты.
5. Технология Intellimirror.

Тематика курсовых работ

1. Сетевое администрирование. Установка, настройка и сопровождение DNS сервера.
2. Сетевое администрирование. Установка, настройка и сопровождение DHCP сервера.
3. Службы каталогов. Установка, настройка и сопровождение Active Directory.
4. Удаленный доступ. Установка, настройка и управление службами удаленного доступа.
5. Многопользовательская вычислительная среда. Службы терминалов. Установка, настройка и управление службами терминалов.
6. Администрирование пользователей. Политики безопасностей, их реализация в операционных системах.
7. Сетевое администрирование. Установка, настройка и сопровождение служб совместного доступа в Интернет.
8. Сетевое администрирование. Мониторинг и поддержка сетевой инфрастукрутры.
9. Сетевое администрирование. Инструменты безопасности в сети. Управление безопасностью.
10. Обеспечение целостности данных. Резервное копирование и восстановление данных. Стратегии резервного копирования.
11. Установка, настройка и сопровождение SQL-сервера.
12. Администрирование сервера БД. Стратегии резервного копирования.
13. Администрирование сервера БД. Управление пользователями сервера БД.
14. Администрирование сервера БД. Инструменты информационной безопасности.
15. Инсталяция, настройка и сопровождение SMTP- POP3(1MAP4)-сервера. Linux/FreeBSD.
16. Инсталяция, настройка и сопровождение SQL- сервера. Linux/FreeBSD.
17. Инсталяция, настройка и сопровождение Router-a. Linux/FreeBSD.
18. Инсталяция, настройка и сопровождение FTP- сервера. Linux/FreeBSD.
19. Инсталяция, настройка и сопровождение VPN сервера. Linux/FreeBSD.
20. Работа с удаленных терминалов. Citrix и т.д.. Инсталяция, настройка и сопровождение.
21. Инсталяция, настройка и сопровождение Proxy- сервера. Linux/FreeBSD.
22. Инсталяция, настройка и сопровождение Firewall-a. Linux/FreeBSD.
23. Инсталяция, настройка и сопровождение систем анализа сетевого трафика. Linux/FreeBSD.
24. Системы доступа к Internet через один компьютер (используя NAT). Инсталяция, настройка, сопровождение. Linux/FreeBSD.
25. Системы удаленного управления.
26. Инсталяция, настройка и сопровождение сервера IP-телефонии. Linux/FreeBSD.
27. Инсталяция, настройка и сопровождение LDAP- сервера Linux/FreeBSD.

2.2 Критерии оценки качества освоения дисциплины

Качество освоения дисциплины оценивается по степени успешности выполнения лабораторных практикумов и результатов ответов на предложенные по темам вопросы.

Критерии оценки знаний обучающихся при выполнении лабораторных практикумов:

Оценка «5» ставится в том случае, если:

– лабораторная работа подготовлена к выполнению, обучаемый знает цель лабораторной работы;

– задания решены без ошибок с первого раза, правильно выбраны решения заданий;

– правильно выполнены расчёты, обучающийся понимает, что они значат;

– полно даны ответы на письменные и устные контрольные вопросы;

– отчёт оформлен аккуратно, сделаны выводы.

Оценка «4» ставится в том случае, если

– лабораторная работа подготовлена к выполнению, обучаемый знает цель практической и лабораторной работы;

– задания решены с ошибками, потребовалась дополнительная помощь преподавателя, правильно выбраны методики решения заданий;

– расчёты выполнены с консультацией преподавателя;

– полно даны ответы на письменные и устные контрольные вопросы;

– отчёт оформлен аккуратно, сделаны выводы.

Оценка «3» ставится в том случае, если

– лабораторная работа подготовлена к выполнению, обучаемый знает цель лабораторной работы;

– задания выполнены с ошибками, потребовалась дополнительная помощь преподавателя, правильно выбраны методики решения заданий;

– с ошибками выполнены расчёты, даже с консультацией преподавателя или обучающийся не может объяснить, как выполнялись расчеты;

– даны ответы на письменные и устные контрольные вопросы.

– отчёт оформлен небрежно, сделаны выводы.

Оценка «2» ставится в том случае, если

– лабораторная работа подготовлена к выполнению, обучаемый не знает цель лабораторной работы;

– задачи решены с ошибками, потребовалась дополнительная помощь преподавателя, неверно выбраны методы решения задач;

– не выполнены расчёты;

– не даны ответы на устные контрольные вопросы;

– отчёт оформлен небрежно, выводы не сделаны.

Критерии оценки знаний обучающихся при выполнении курсовых работ:

Оценка «отлично» – ставиться, если студент демонстрирует знание теоретического и практического материала при написании курсовой работы, определяет взаимосвязи между основными понятиями и методами, даёт правильный алгоритм решения, определяет междисциплинарные связи по условию задания. А также, если студент имеет глубокие знания учебного материала по теме курсовой работы.

Оценка «хорошо» – ставится, если студент демонстрирует знание теоретического и практического материала по теме курсовой работы, допуская незначительные неточности при изложении материала по теме, имея неполное понимание междисциплинарных связей при правильном выборе алгоритма написания работы. А

также, если студент показал знание учебного материала, усвоил основную литературу, смог ответить почти полно на сформулированные по теме курсовой задания.

Оценка «удовлетворительно» – ставится, если студент затрудняется с правильной оценкой темы курсовой, написание носит не полный характер, требующий наводящих вопросов преподавателя. А также, если студент в целом освоил материал по курсовой работе, ответил не на все уточняющие и дополнительные вопросы.

Оценка «неудовлетворительно» – ставится, если студент дает неверную оценку ситуации, неправильно выбирает алгоритм написания курсовой работы. А также, если он имеет существенные пробелы в знаниях основного учебного материала темы курсовой, который полностью не раскрыл содержания работы, не смог ответить на уточняющие и дополнительные вопросы.

3. ФОНД ОЦЕНОЧНЫХ СРЕДСТВ ДЛЯ промежуточной аттестации по дисциплине

3.1 Теоретические вопросы для проведения зачета

1. Администратор ИВС. Функции администратора ИВС.
2. Основные механизмы службы безопасности : наследование и т.д. Типы прав доступа. Права на ресурсы
3. Ресурсы ИВС. Права доступа и проверка прав доступа. Совместное использование ресурсов.
4. Пользователь ИВС. Бюджет пользователя. Регистрация, аутентификация, авторизация.
5. Служба безопасности : действительные права. Права на ресурсы файловой системы. Атрибуты ресурсов файловой системы.
6. Файловые системы FAT, FAT32, NTFS.
7. Администрирование сетей на базе протокола TCP/IP.
8. Маршрутизация TCP/IP.
9. Windows. Файловая система : логическая и физическая структура. Механизмы для оптимизации, обеспечения гибкости и надежности.
10. Windows: функции и требования к современной СОС.
11. Windows: служба справочника, служба безопасности, служба контроля/аудита.
12. Windows Server. Версии ОС. Особенности архитектуры.
13. Windows Server. Служба справочника на базе Active Directory. Доверительные отношения, отличие от Windows NT. Варианты построения сети на базе доменов. Иерархия доменов и организационных единиц.
14. Служба каталога Active Directory. Протоколы аутентификации NTLM и Kerberos в нормальном (native) и смешанном (mixed) режимах.
15. Механизмы Microsoft Windows Server: WMI, MMC, оснастки, WSH.
16. Клиентская ОС : Функции и требования к клиентской ОС.
17. Серверная ОС: Файловая служба, служба печати, служба архивирования и резервного копирования.
18. Серверная ОС: Функции администратора. Клиентская ОС: Функции администратора.
19. Определения леса и дерева Active Directory, схемы каталога, пространства имен. Сплошное и разделенное пространства имен.
20. Домен Windows: определение и основные встроенные объекты. Глобальные и локальные группы домена, контроллеров домена, отдельно стоящего сервера и рабочей станции, область действия, подходы к распределению доступа на основе групп.
21. Групповая политика: определение и составные части (GPT и GPC). Объекты применения групповых политик. Варианты конфликтов политик и их решение в Windows.

22. Варианты проведения резервного копирования, достоинства и недостатки каждого из них.
23. WINS сервер.
24. DHCP сервер.
25. DNS сервер.
26. Файлы Hosts и LMHosts.
27. Оперативное управление и регламентные работы.
28. Управление и обслуживание технических средств.
29. Аппаратно-программные платформы администрирования.
30. Информационные системы администрирования.

3.2 Показатели, критерии и шкала оценивания письменных ответов на зачете

Зачет			
Оценка «зачтено» (отлично)	**Оценка «зачтено» (хорошо)**	**Оценка «зачтено» (удовлетворительно)**	**Оценка «не зачтено» (неудовлетворительно)**
– систематизированные, глубокие и полные знания по всем разделам дисциплины, а также по основным вопросам, выходящим за пределы учебной программы; – точное использование научной терминологии систематически грамотное и логически правильное изложение ответа на вопросы; – безупречное владение инструментарием учебной дисциплины, умение его эффективно использовать в постановке научных и практических задач; – выраженная способность самостоятельно и творчески решать сложные проблемы и нестандартные ситуации; – полное и глубокое усвоение основной и дополнительной литературы, рекомендованной учебной программой по	– достаточно полные и систематизированные знания по дисциплине; – умение ориентироваться в основном теориях, концепциях и направлениях дисциплины и давать им критическую оценку; – использование научной терминологии, лингвистически и логически правильное изложение ответа на вопросы, умение делать обоснованные выводы; – владение инструментарием по дисциплине, умение его использовать в постановке и решении научных и профессиональных задач;	– Достаточный минимальный объем знаний по дисциплине; – усвоение основной литературы, рекомендованной учебной программой; – умение ориентироваться в основных теориях, концепциях и направлениях по дисциплине и давать им оценку; – использование научной терминологии, стилистическое и логическое изложение ответа на вопросы, умение делать выводы без существенных ошибок; – владение инструментари	фрагментарные знания по дисциплине; – отказ от ответа (выполнения письменной работы); – знание отдельных источников, рекомендованных учебной программой по дисциплине; – неумение использовать научную терминологию; – наличие грубых ошибок; – низкий уровень культуры исполнения заданий; – низкий уровень сформированности

дисциплине; – умение ориентироваться в теориях, концепциях и направлениях дисциплины и давать им критическую оценку, используя научные достижения других дисциплин; – творческая самостоятельная работа на практических/семинарских/лабораторных занятиях, активное участие в групповых обсуждениях, высокий уровень культуры исполнения заданий; – высокий уровень сформированности заявленных в рабочей программе компетенций.	– усвоение основной и дополнительной литературы, рекомендованной учебной программой по дисциплине; – самостоятельная работа на практических занятиях, участие в групповых обсуждениях, высокий уровень культуры исполнения заданий; – средний уровень сформированности заявленных в рабочей программе компетенций.	ем учебной дисциплины, умение его использовать в решении типовых задач; – умение под руководством преподавателя решать стандартные задачи; – работа под руководством преподавателя на практических занятиях, допустимый уровень культуры исполнения заданий; достаточный минимальный уровень сформированности заявленных в рабочей программе компетенций.	заявленных в рабочей программе компетенций.