МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ
РОССИЙСКОЙ ФЕДЕРАЦИИ

ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ ОБРАЗОВАТЕЛЬНОЕ
УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ

СЕВЕРО-КАВКАЗСКАЯ ГОСУДАРСТВЕННАЯ АКАДЕМИЯ

Л.Г. Темирова

ЗАЩИТА ИНФОРМАЦИИ В КОМПЬЮТЕРНЫХ СИСТЕМАХ

Практикум для обучающихся 4 курса
по специальности 01.03.04 Прикладная математика

Черкесск
2019

УДК 681.3
ББК 32.973.26-018.2
Т32

Рассмотрено на заседании кафедры Математика
Протокол № 2 от «20 » 09 2018 г.
Рекомендовано к изданию редакционно-издательским советом СевКавГГТА
Протокол № 15 от «30» 10 2018 г.

Рецензенты: Кочкаров А.М. – д.ф-м.н., проф. кафедры математики
Бежанова Е.Х. – к.ф-м.н., доц. кафедры математики

Т32 **Темирова, Л.Г.** Защита информации в компьютерных системах: практикум для обучающихся 4 курса по специальности 01.03.04 Прикладная математика / Л.Г. Темирова. – Черкесск: БИЦ СевКавГГТА, 2019. – 64 с.

Пособие содержит перечень лабораторных работ по освоению технологии индивидуальных настроек окон оснасток для целей защиты информации, создание локального профиля пользователя, осуществление проверки событий в операционной системе, имеющие отношение к безопасности файловой системы, аудит локальной системы, также настройка рабочей среды пользователя при помощи сценариев входа и его аутентификация. Все лабораторные задания выполняются в среде виртуальной машины.

УДК 681.3
ББК 32.973.26-018.2

Содержание

Ведение……. 4
Лабораторная работа 1. Консоль управления Microsoft ……. 5
Лабораторная работа 2. Создание локальных учетных записей пользователей и групп ……..... 14
Лабораторная работа 3. Управление рабочей средой пользователя …… 20
Лабораторная работа 4. Настройка рабочей среды пользователя при помощи сценариев входа и его аутентификация …… 32
Лабораторная работа 5. Аудит локальной системы …… 37
Лабораторная работа 6. Управление общими дисковыми ресурсами…… ….. 47
Лабораторная работа 7. Средства мониторинга и оптимизации. Диспетчер задач……. 56
Список литературы …… 63

Введение

Проблема защиты информации: надежное обеспечение ее сохранности и установленного статуса использования – является одной из важнейших проблем современности.

В настоящее время выделяют четыре уровня правового обеспечения информационной безопасности. Первый уровень образуют международные договоры, к которым присоединилась Российская Федерация, и федеральные законы России: международные конвенции об охране промышленной собственности, охране интеллектуальной собственности, авторском праве; Конституция РФ (ст. 23 определяет право граждан на тайну переписки, телефонных, телеграфных и иных сообщений); гражданский кодекс РФ (в ст. 139 устанавливается право на возмещение убытков от утечки с помощью незаконных методов информации, относящейся к служебной и коммерческой тайне). Второй уровень правового обеспечения информационной безопасности составляют подзаконные акты, это указы Президента РФ, постановления РФ, письма Высшего арбитражного суда РФ, постановления пленумов Верховного суда РФ и т.д. Третий уровень правового обеспечения информационной безопасности составляют государственные стандарты (ГОСТы) в области защиты информации, руководящие документы, нормы, методики, и классификаторы, разработанные государственными органами.

Существуют программные средства защиты информации, такие как программы идентификации и аутентификации пользователей компьютерной системы (КС); программы разграничения доступа пользователей к ресурсам КС; программы шифрования информации; программы защиты информационных ресурсов (системного и прикладного программного обеспечения, баз данных, компьютерных средств обучения и т. п.) от несанкционированного изменения, использования и копирования.

Лабораторная работа 1
Тема: Консоль управления Microsoft

Цель работы: Освоить технологию создания консоли управления Microsoft и проведение индивидуальных настроек окон оснасток для целей защиты информации

Общие сведения

Консоль управления Microsoft: Microsoft Management Console (MMC) предназначена для запуска следующих программных модулей:

- администрирования;
- конфигурирования локальных компьютеров и сети в целом;
- мониторинга локальных компьютеров и сети в целом.

Запускаемые программные модули называются оснастками (snap-ins). Консоль управления сама по себе не выполняет никаких функций администрирования, но служит в качестве рабочей среды для запуска оснасток. Оснастки представляют собой управляющие компоненты, которые объединены в среде MMC. Из нескольких оснасток можно создать индивидуальный управляющий инструмент.

MMC обеспечивает возможность индивидуальной настройки и передачи полномочий, интеграцию и унификацию, гибкость в выборе инструментов и продуктов.

В среде MMC можно использовать различные инструменты и оснастки.

Диспетчер оснасток (Snap-in Manager) дает системному администратору или разработчику оснасток возможность добавлять, удалять или изменять оснастки.

Все инструменты MMC состоят из совокупности оснасток. Каждая оснастка представляет собой минимальную единицу управления. Оснастка может вызывать другие элементы управления и динамические библиотеки (DLL) для выполнения своей задачи.

Ряд оснасток могут быть объединены администратором в инструмент (также называется документом), который сохраняется в файле с расширением «*.msc», например, **gpedit.msc** (Management Saved Console). Администратор использует инструменты для управления сетью. Файл *.msc можно затем передать другому администратору по электронной почте, который сможет использовать содержащийся в нем инструмент на своем рабочем месте.

Благодаря возможности индивидуальной настройки MMC, администратор может создать идеальный инструмент на основе доступных оснасток. Кроме того, инструмент MMC, включающий в себя стандартные оснастки, занимает в памяти меньше места, чем эти оснастки, запущенные по отдельности. В MMC поддерживаются два типа оснасток:

1. Изолированная оснастка (stand-alone snap-in) обеспечивает выполнение своих функций даже при отсутствии других оснасток, например, управление компьютером (Computer Management).

2. Оснастка расширения (extension snap-in) может работать только после активизации родительской оснастки. Функция оснастки расширения заключается в увеличении числа типов узлов, поддерживаемых родительской оснасткой. Оснастка расширения является подчиненным элементом узлов определенных типов, и при каждом запуске узлов данных типов консоль автоматически запускает все связанные с ней расширения. В качестве примера можно привести оснастку Диспетчер устройств (Device Manager).Оснастки расширения могут предоставлять различные функциональные возможности. Например, такие оснастки могут расширять пространство имен консоли, увеличивать число пунктов в меню или добавлять определенные мастера.

Создание новой консоли

Лабораторная работа проводится с помощью программы VMware, которая эмулирует работу виртуальной машины. VMware Workstation позволяет работать с высокой эффективностью в безопасных виртуальных машинах с различными операционными системами и их приложения. Каждая виртуальная машина эквивалентна PC с уникальным сетевым адресом и полным дополнением аппаратных средств. Для выполнения лабораторной работы запустите из главного меню программу **VMware Workstation**. Результат запуска программы представлен на рисунке 1.1

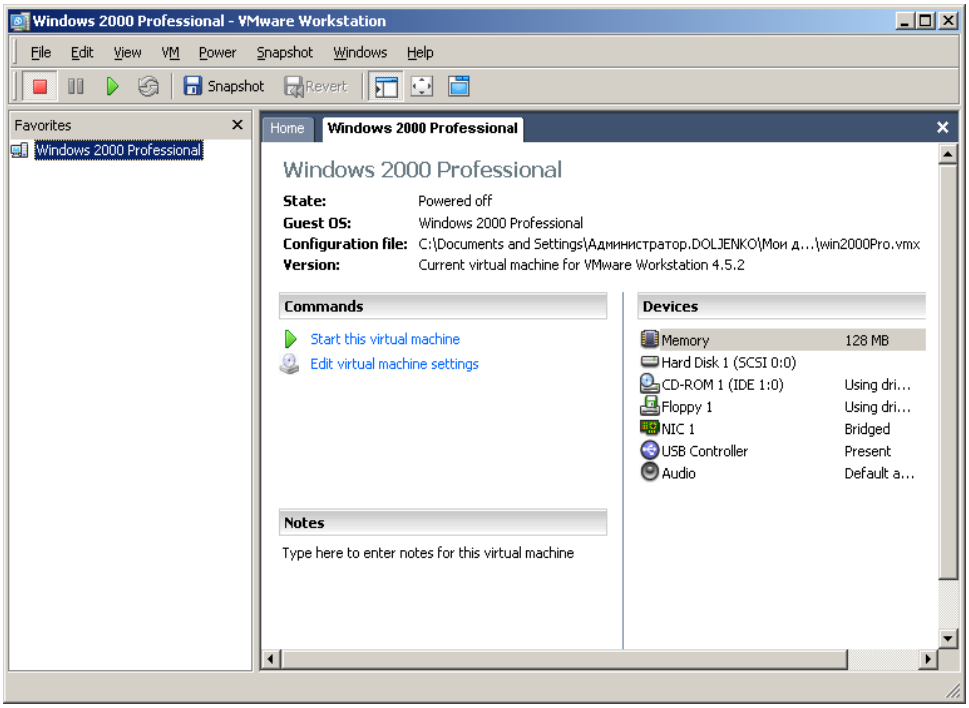

Рисунок 1.1 – Стартовое окно программы VMware Workstation

Для запуска операционной системы Windows выделите в навигаторе пункт Windows/ *Start virtual machine.*

После запуска виртуальной машины работа в ней осуществляется как на обычном компьютере.

Процедура создания новой консоли и добавления к ней оснасток **Управление компьютером** и **Сертификаты** (Certificates) следующая.

1. В меню **Пуск/Выполнить,** введите **mmc** и **ОК**. Откроется окно Консоль1 с пустой консолью или административным инструментом.
2. В меню **Консоль** (Console) выберите пункт **Добавить/Удалить** оснастку. В открывающем окне перечисляются изолированные оснастки и оснастки расширения, которые будут добавлены в консоль или уже включены в нее. Оснастки можно добавлять к корню консоли управления или к уже имеющимся изолированным оснасткам (другим узлам дерева); это указывается в списке **Оснастки** (Snap-ins added to). В нашем случае оставим значение по умолчанию - **Корень консоли** (Console Root).
3. Нажмите кнопку **Добавить** (Add). На экране появится окно **Добавить изолированную оснастку** (Add Stand-alone Snap-in) как на рисунке 1.2. со списком изолированных оснасток, имеющихся в системе.
4. Выполните двойной щелчок на пункте **Управление компьютером и** появится окно с конфигурационными опциями для данной оснастки.
5. Оставьте переключатель в положении **локальным компьютером** (Local computer). Затем кнопку **Готово** (Finish).

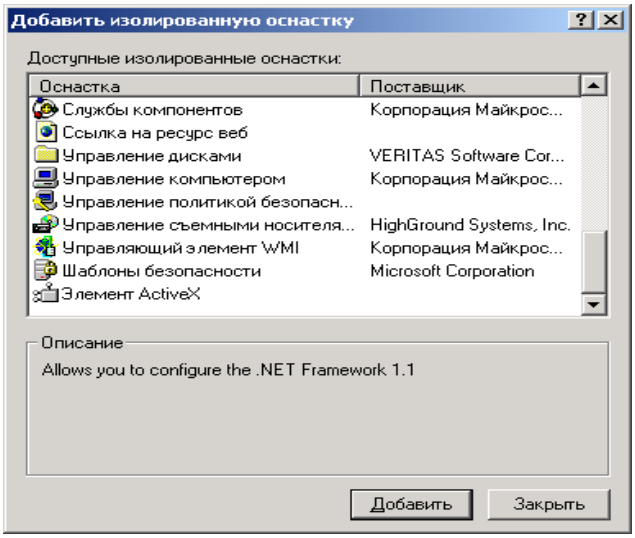

Рисунок 1.2 - Окно со списком имеющихся оснасток

6. В следующем окне выберите соответствующий переключатель. Эта оснастка всегда будет управлять сертификатами для:
   - моей учетной записи пользователя (My user account)
   - учетной записи службы (Service account)
   - учетной записи компьютера (Computer account), затем Готово и Закрыть.
7. В окне **Добавить/Удалить оснастку** (где отображен список подключаемых оснасток) перейдите на вкладку **Расширения** (Extensions) На ней приведен список оснасток расширения, которые поставляются вместе с выбранными изолированными оснастками. Если вы не собираетесь подключать все оснастки расширения, сбросьте флажок

Добавить все расширения (Add all extensions) (который ставится по умолчанию) и снимите флажки с лишних оснасток По окончании процедуры кнопка **ОК.**

8. Закройте окно добавления оснасток, нажав на **ОК**. Теперь окно консоли содержит две оснастки: **Управление компьютером** и **Сертификаты** (см. рисунок 1.3).

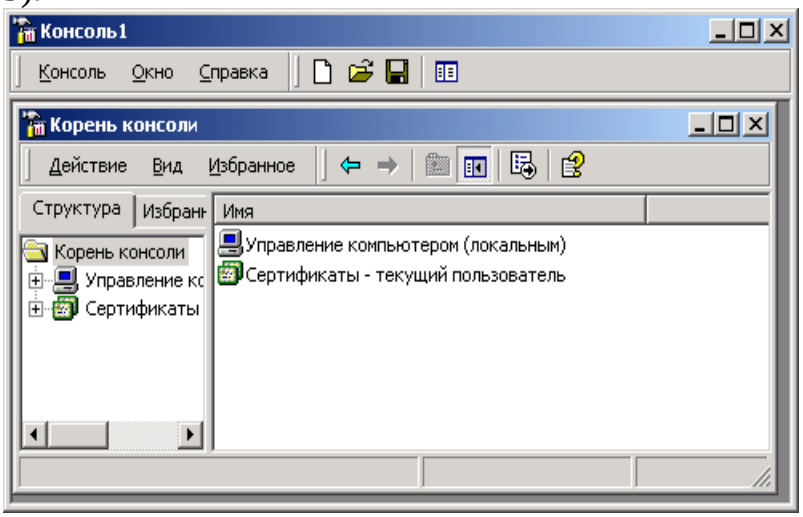

Рисунок 1.3 - Окно консоли после формирования оснасток

9. Для того, чтобы сохранить созданный инструмент, в меню **Консоль** выберите пункт **Сохранить как** и укажите имя файла и папку, в которой будет сохранен файл консоли.

Индивидуальная настройка окон оснасток

После добавления оснасток можно развернуть окна оснасток, чтобы облегчить работу с ними. Для этого выполните следующие действия:

1. В левом подокне (в окне структуры) только что созданной консоли через контекстное меню узла **Управление компьютером** выберите пункт **Новое окно отсюда** (New Window from Here). Будет открыто окно **Управление компьютером**, представляющее одноименную оснастку.
2. Аналогичные действия выполните для узла **Сертификаты**. В новом окне нажмите кнопку **Скрытие или отображение дерева консоли или избранного** (Show/Hide Console tree) на панели инструментов для того, чтобы скрыть панель структуры.
3. Закройте исходное окно, содержащее **Корень консоли**.
4. В меню **Окно** (Window) выберите команду **Сверху вниз**. Консоль будет выглядеть так, как показано на рисунке 1.4.

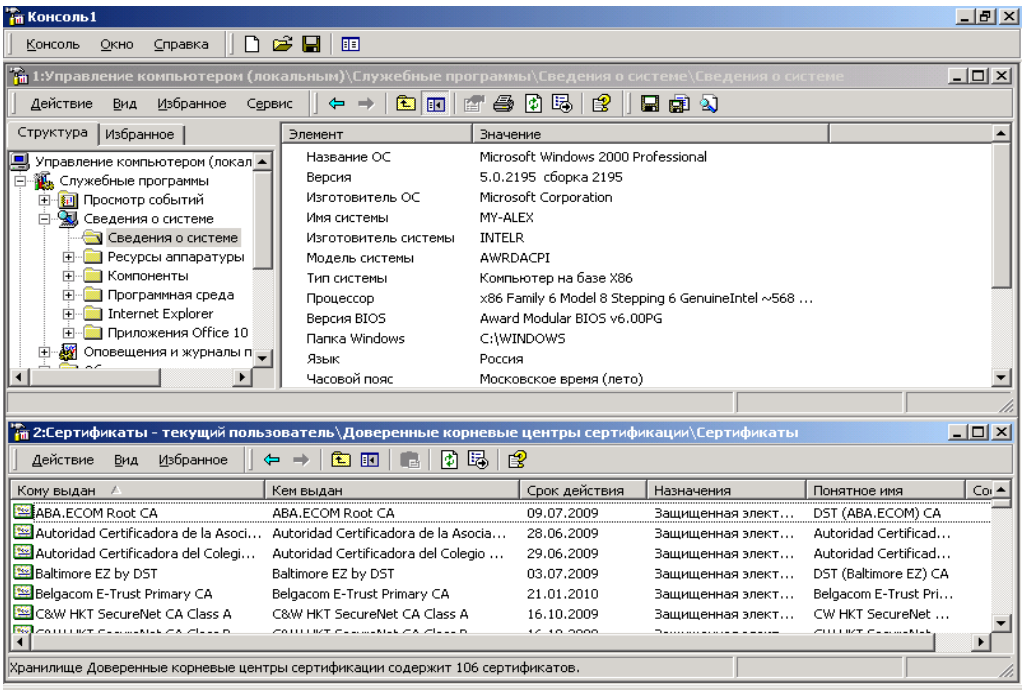

Рисунок 1.4 - Окна консоли с индивидуальной настройкой

Создание панелей задач

Когда требуется создать файл консоли для другого пользователя, полезно предоставить пользователю упрощенный инструмент, позволяющий выполнять только несколько определенных задач. Таким инструментом является панель задач (taskpad). Панель задач является HTML-страницей, на которой могут быть размещены ярлыки, запускающие команды меню и программы или открывающие ссылки на веб-страницы.

Для создания панели задач выполните следующее:

1. В меню Действие (Action) или в контекстном меню любого узла в окне консоли выберите пункт Новый вид панели задач (New Taskpad View).

2. Откроется окно (см.рисунок 1.5) Мастера создания вида панели задач (New Taskpad View Wizard). Затем **Далее**.

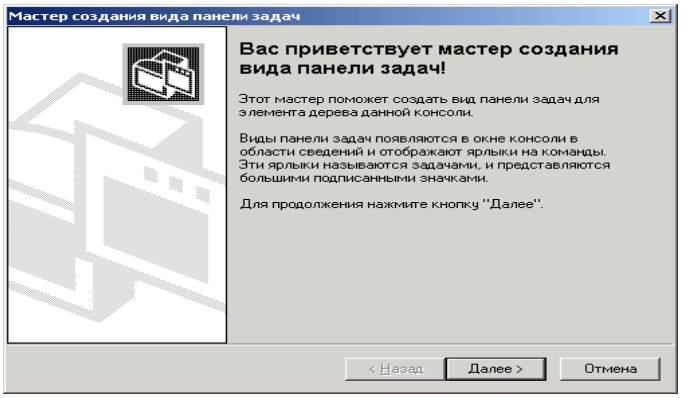

Рисунок 1.5 - Окно Мастера создания вида панели задач

3. В следующем окне мастера вам будет предложено выбрать стиль отображения и размер панели задач (см.рисунок 1.6).

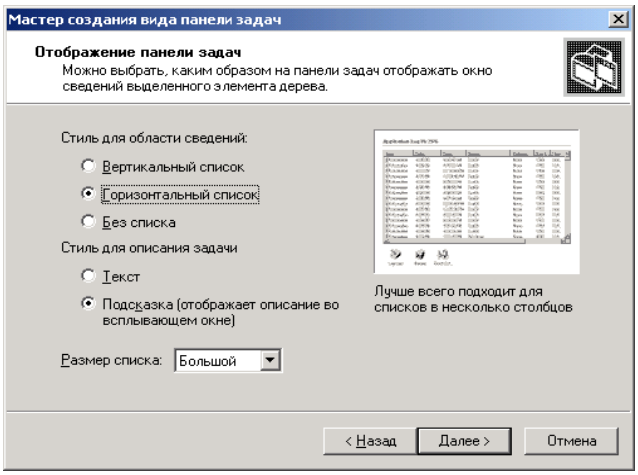

Рисунок 1.6 - Окно мастера создания панелей задач

4. Затем на панели задач вы можете указать использование только тех задач, которые связаны с текущим узлом или со всеми узлами дерева. В следующем окне потребуется ввести имя и описание создаваемой панели задач. Если вы не собираетесь пока добавлять новые задачи на созданную панель, снимите в последнем окне мастера флажок Запустить мастер создания новой задачи (Start New Task Wizard). В противном случае по завершении работы Мастера создания вида панели задач, запускается Мастер создания задач (New Task Wizard). В ходе этой процедуры следует указать функцию задачи: запуск команды меню, программы или ссылка на веб-страницу, ввести путь к исполняемому файлу и параметры запуска.
5. Если новая задача будет запускать команду меню, в следующем окне будет предложено указать элементы в панели результатов, к которым будет применяться выбранная команда. Например, при создании панели задач для Internet Explorer это окно выглядит как на рисунке 1.7.

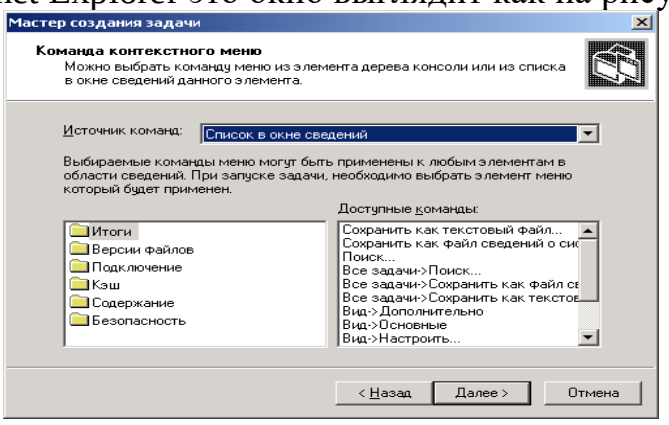

Рисунок 1.7 - Окно выбора элемента узла и команды

6. В остальных окнах мастера примите значения по умолчанию. Если требуется создать несколько задач на одной панели, установите в последнем окне мастера флажок **Запустить этот мастер снова** (Run this wizard again) затем нажмите кнопку **Готово.**

7. На рисунке 1.8 показана созданная панель задач В данном окне консоли панель структуры отключена — аналогично тому, как это было сделано в предыдущем разделе. Для удаления лишних меню и панелей инструментов снимите соответствующие флажки в окне **Настройка вида (**Customize View) (опции **Вид** (View)/ **Настроить** (Customize) на панели инструментов или команда **Вид/ Настроить** в контекстном меню созданной панели задач).

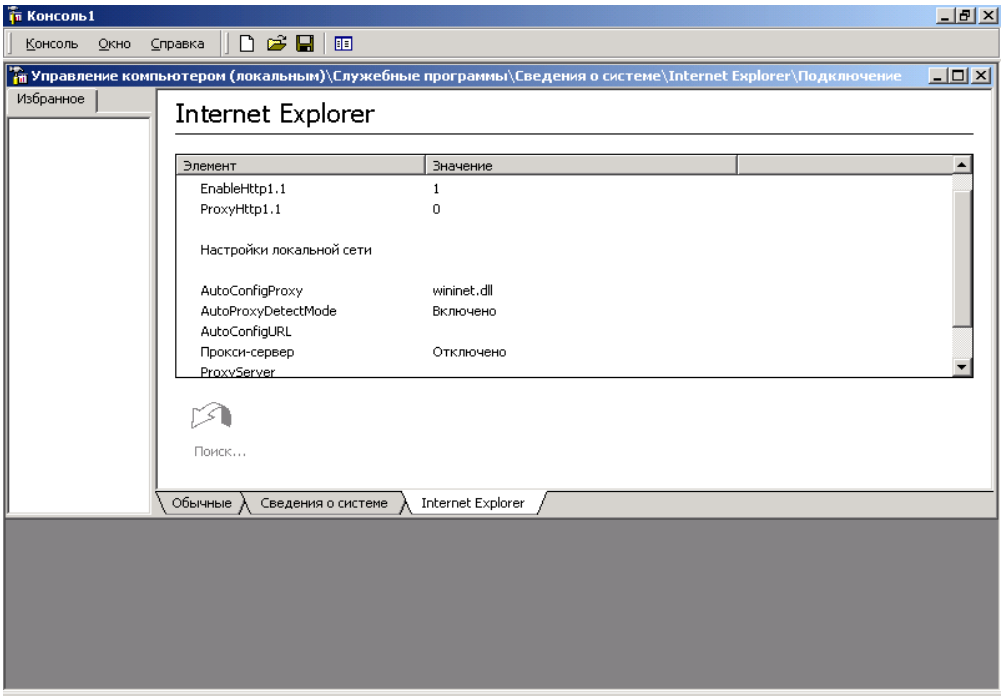

Рисунок 1.8 - Окно консоли с панелью задач

Установка опций консоли

Если консоль создается для другого пользователя, может оказаться полезным установить запрет на изменение консоли. Для этого следует открыть окно **Параметры** (Options).

1. В меню Консоль выберите **Параметры** (Options) (см.рисунок 1.9).
2. Установите в списке **Режим консоли** (Console mode) значение **Пользовательский режим — полный доступ** (User Mode — full access). В этом режиме пользователь не сможет добавлять новые оснастки в инструмент, но будет иметь возможность изменять расположение окон. Новый режим начнет работать при следующем запуске файла консоли.

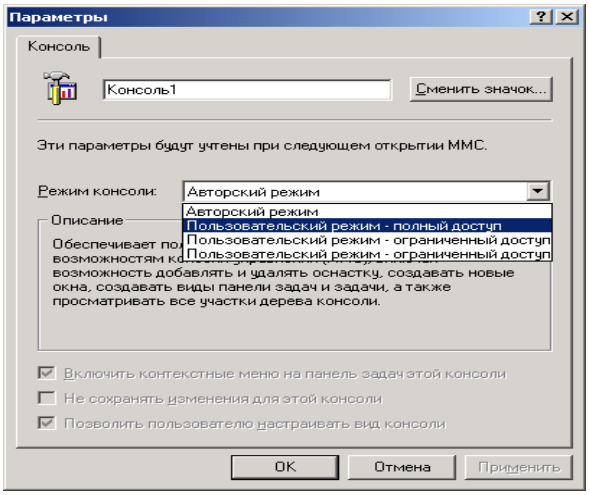

Рисунок 1.9 - Окно установки опций консоли

3. Нажмите **ОК** и сохраните файл.
4. Сохраненный файл консоли можно также открыть с помощью **Проводника**. Для этого двойной щелчок на файле с расширением **msc**. Файл консоли будет открыт в среде MMC.

Запуск инструментов MMC

Для запуска стандартных инструментов MMC, установленных на компьютере, можно использовать один из приведенных ниже способов:

Откройте меню **Пуск/Программы/Администрирование** и выберите необходимый инструмент.

Дважды щелкните на значке **Администрирование** на панели управления. Откроется окно **Администрирование**, содержащее значки всех установленных на компьютере инструментов.

Задания на лабораторную работу

По заданию преподавателя создать консоль и добавить в неё оснастки из таблицы, провести индивидуальную настройку окон оснасток и создать панель задач.

Таблица 1 – Варианты заданий на лабораторную работу

Вариант создания консоли	Оснастка, добавляемая к консоли	Назначение оснастки
1	Анализ и настройка безопасности (Security Configuration and Analysis)	Служит для управления безопасностью системы с помощью шаблонов безопасности

2	Групповая политика (Group Policy)	Служит для назначения сценариев регистрации, групповых политик для компьютера и пользователей некоторого компьютера сети; позволяет просматривать и изменять политику безопасности, политику аудита и права пользователей
3	Диспетчер устройств (Device Manager)	Содержит список всех устройств, подключенных к компьютеру, и позволяет их конфигурировать
4	Локальные пользователи и группы (Local Users and Groups)	Служит для управления локальными учетными записями пользователей и групп
5	Оповещения и журналы производительности (Performance Logs and Alerts)	Конфигурирует журналы данных о работе системы и службу оповещений
6	Просмотр событий (Event Viewer)*	Служит для просмотра и управления системным журналом, журналами безопасности и приложений
7	Сведения о системе (System Information)	Отображает информацию о системе
8	Системный монитор (Performance)*	Используется для сбора и просмотра в реальном времени данных, характеризующих работу памяти, дисков, процессора и других компонентов системы
9	Служба индексирования (Indexing Service)	Служит для индексирования документов различных типов с целью ускорения их поиска
10	Службы (Services)*	Запускает, останавливает и конфигурирует службы (сервисы) Windows
11	Ссылка на ресурс веб (Link to Web Address)	Служит для подключения веб-страниц (html, asp, stml)
12	Управление дисками (Disk Management)	Служит для управления дисками и защитой данных, для разбиения дисков на логические тома, форматирования, управления совместным доступом, квотами и т.д.
13	Управление политикой безопасности IP (IP Security Policy Management)	Служит для управления политиками IPSec для безопасного соединения с другими компьютерами
14	Управление службой факсов (Fax Service Management)	Служит для управления службой и устройствами факсимильной связи
15	Управление съемными носителями (Removable Storage Management)	Служит для управления сменными носителями информации
16	Шаблоны безопасности (Security Templates) Элемент ActiveX (ActiveX Control)	Обеспечивает возможность редактирования файлов-шаблонов безопасности Подключение к дереву консоли различных элементов управления ActiveX

Лабораторная работа 2
Создание локальных учетных записей пользователей и групп

Цель работы: Освоить технологию системного администрирования при создании локальных учетных записей пользователей и групп в операционной системе Windows, для целей защиты информации.

Общие положения

Создание учетных записей и групп занимает важное место в обеспечении безопасности Windows, поскольку, назначая им права доступа, администратор получает возможность ограничить пользователей в доступе к конфиденциальной информации компьютерной сети, разрешить или запретить им выполнение в сети определенного действия, например архивацию данных или завершение работы компьютера. Обычно право доступа ассоциируется с объектом-файлом или папкой. Оно определяет возможность данного пользователя получить доступ к объекту.

Оснастка Локальные пользователи и группы

Оснастка **Локальные пользователи и группы** (Local Users and Groups) – это инструмент MMC, с помощью которого выполняется управление локальными учетными записями пользователей и групп — как на локальном, так и на удаленном компьютерах. С ним можно работать на рабочих станциях и серверах (не контроллерах домена) Windows 2000. Запускать оснастку **Локальные пользователи и группы** может любой пользователь. Выполнять администрирование учетных записей могут только администраторы и члены группы Опытные пользователи (Power Users).

Окно изолированной оснастки **Локальные пользователи и группы** выглядит так, как на рисунке 2.1.

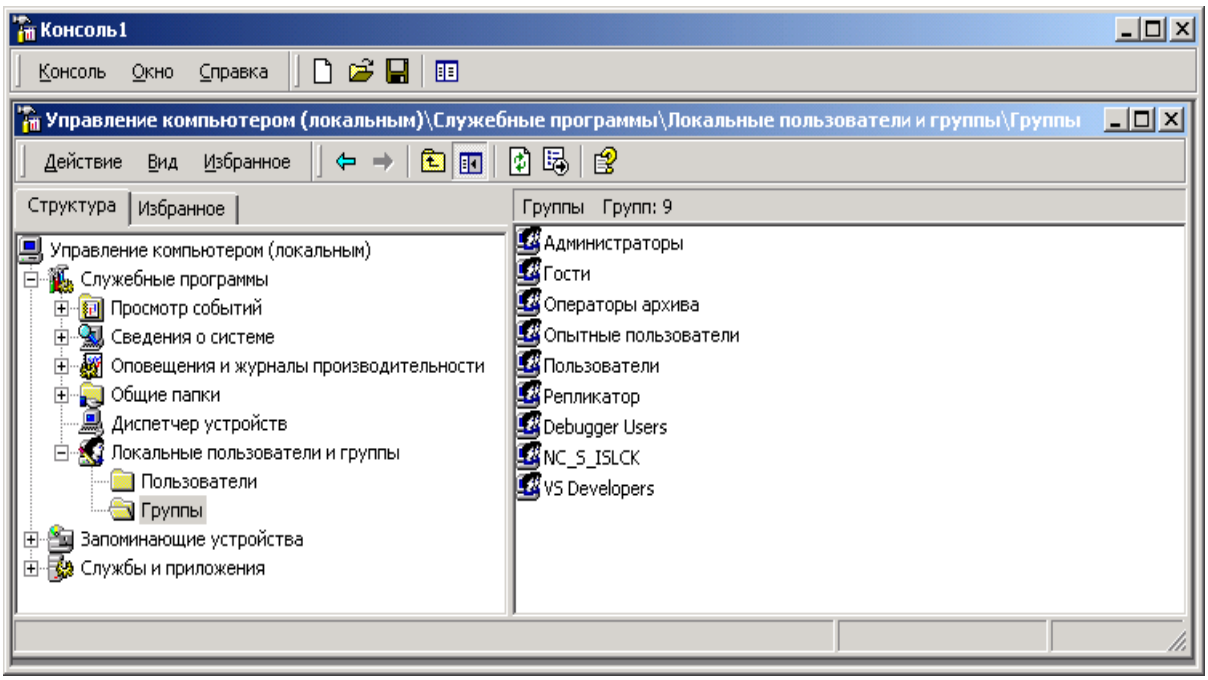

Рисунок 2.1 – Окно оснастки Локальные пользователи и группы

Папка *Пользователи* (Users)

Сразу после установки системы Windows папка **Пользователи** содержит две встроенные учетные записи — Администратор (Administrator) и Гость (Guest). Они создаются автоматически при установке ОС Windows. Ниже даны описания свойств обеих встроенных учетных записей.

Администратор — эту учетную запись используют при установке и настройке рабочей станции или сервера. Она не может быть уничтожена, блокирована или удалена из группы Администраторы (Administrators), ее можно только переименовать.

Гость — эта учетная запись применяется для регистрации в компьютере без использования специально созданной учетной записи. Учетная запись Гость не требует ввода пароля и по умолчанию блокирована (Обычно пользователь, учетная запись которого блокирована, но не удалена, при регистрации получает предупреждение и входить в систему не может.) Она является членом группы Гости (Guests) Ей можно предоставить права доступа к ресурсам системы точно так же, как любой другой учетной записи.

Папка Группы (Groups)

После установки системы Windows (рабочей станции или сервера) папка **Группы** (Groups) содержит шесть встроенных групп. Они создаются автоматически при установке Windows. Ниже описаны свойства всех встроенных групп.

Администраторы (Administiators) — ее члены обладают полным доступом ко всем ресурсам системы. Это единственная встроенная группа, автоматически предоставляющая своим членам весь набор встроенных прав.

Операторы архива (Backup Operators) — члены этой группы могут архивировать и восстанавливать файлы в системе независимо от того, какими правами эти файлы защищены. Кроме того, операторы архива могут входить в систему и завершать ее работу, но они не имеют права изменять настройки безопасности.

Гости (Guests) — эта группа позволяет выполнить регистрацию пользователя с помощью учетной записи Гость и получить ограниченные права на доступ к ресурсам системы. Члены этой группы могут завершать работу системы.

Опытные пользователи (Power Users) — члены этой группы могут создавать учетные записи пользователей, но они имеют право модифицировать настройки безопасности только для созданных ими учетных записей. Кроме того, они могут создавать локальные группы и модифицировать состав членов созданных ими групп. То же самое они могут делать с группами Пользователи, Гости и Опытные пользователи. Члены группы Опытные пользователи не могут модифицировать членство в группах Администраторы и Операторы архива. Они не могут быть владельцами файлов, архивировать или восстанавливать каталоги, загружать и выгружать драйверы устройств и модифицировать настройки безопасности и журнал событий.

Репликатор (Replicator) — членом группы Репликатор должна быть только учетная запись, с помощью которой можно зарегистрироваться в службе репликации контроллера домена. Ее членами не следует делать рабочие учетные записи.

Пользователи (Users) — члены этой группы могут выполнять большинство пользовательских функций, например, запускать приложения, пользоваться локальным или сетевым принтером, завершать работу системы или блокировать рабочую станцию. Они также могут создавать локальные группы и регулировать состав их членов. Они не могут получить доступ к общему каталогу или создать локальный принтер.

Управление учетными записями

В качестве примера использования оснастки **Локальные пользователи и группы** для работы с учетными записями рассмотрим процедуру создания пользовательской учетной записи.

Создание учетной записи

Для создания учетной записи:

1. В оснастке **Локальные пользователи и группы** установите указатель мыши на папку **Пользователи** и нажмите правую кнопку. В появившемся контекстном меню выберите команду **Новый пользователь** (New User) (см. рисунок 2.2).

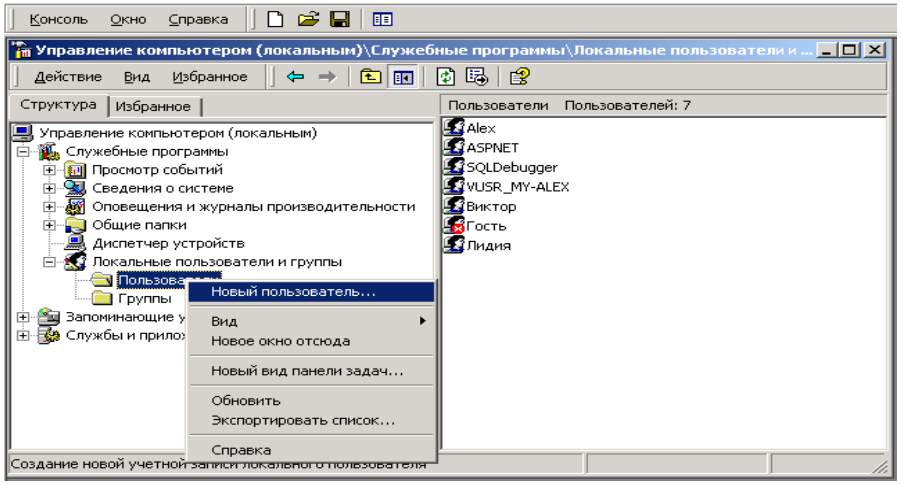

Рисунок 2.2 – Формирование команды **Новый пользователь**

2. Появится окно диалога **Новый пользователь** (New User). В поле **Пользователь** (User name) введите имя создаваемого пользователя. В поле **Полное имя** (Full name) введите полное имя создаваемого пользователя. В поле **Описание** (Description) введите описание создаваемого пользователя или его учетной записи. В поле **Пароль** (Password) введите пароль пользователя и в поле **Подтверждение** (Confirm Password) подтвердите его правильность вторичным вводом. Длина пароля не может превышать 14 символов (см.рисунок 2.3).
3. Установите или снимите флажки **Потребовать смену пароля при следующем входе в систему** (User must change password at next logon), **Запретить смену пароля пользователем** (User cannot change password), **Срок действия пароля не ограничен** (Password never expires) и **Отключить учетную запись** (Account is disabled).
4. Чтобы создать еще одного пользователя (см.рисунок 2.3), нажмите кнопку **Создать** (Create) и повторите шаги с 1 по 3. Для завершения работы нажмите кнопку **Создать** и затем **Закрыть** (Close).

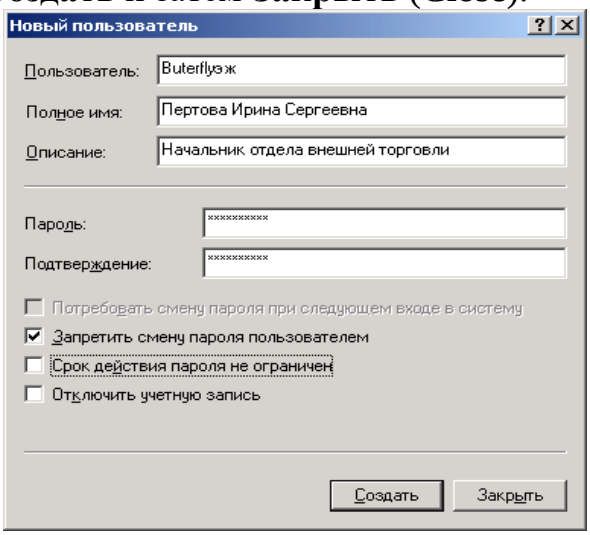

Рисунок 2.3 – Окно Новый пользователь

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.

Изменение и удаление учетных записей

Изменять, переименовывать и удалять учетные записи можно с помощью контекстного меню, вызываемого щелчком правой кнопки мыши на имени пользователя, либо — меню **Действие** (Action) на панели меню оснастки **Локальные пользователи и группы** (при этом в правом подокне оснастки должна быть выбрана модифицируемая или удаляемая учетная запись пользователя).

Поскольку переименованная учетная запись сохраняет *идентификатор безопасности* (Security Identifier, SID), она сохраняет и все свои свойства, например, описание, полное имя пароля, членство в группах и т. д.

Управление локальными группами

Создание локальной группы

Для создания локальной группы:

1. В окне оснастки **Локальные пользователи и группы** установите указатель мыши на папке **Группы** и с помощью контекстного меню на нем выберите команду **Новая группа** (New Group) как на рисунке 2.4.
2. В поле **Имя группы** (Group Name) введите имя новой группы.
3. В поле **Описание** (Description) введите описание новой группы (см. рисунок 2.5).

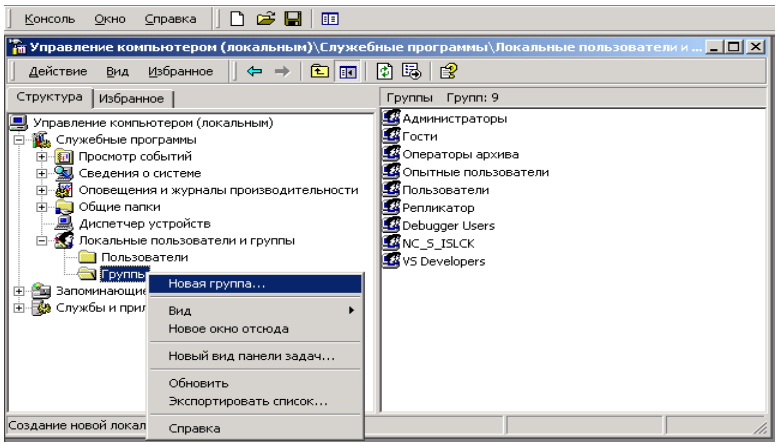

Рисунок 2.4 – Формирование команды **Новая группа**

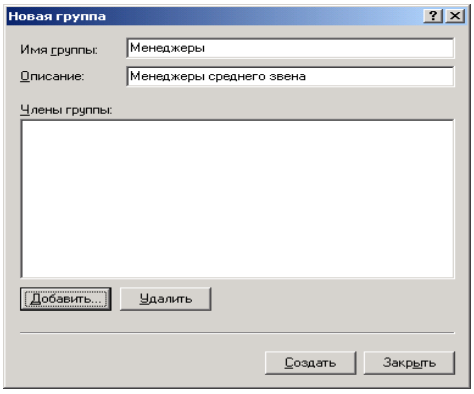

Рисунок 2.5 – Окно Новая группа

4. В поле Члены группы (Members) можно сразу же добавить пользователей и группы, которые войдут в данную группу: для этого нужно нажать кнопку Добавить (Add) и выбрать их в списке (см. рисунок 2.6). Для завершения нажмите кнопку Создать и затем Закрыть.

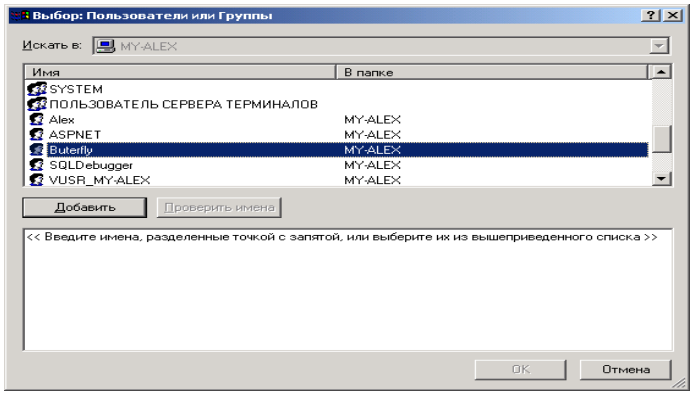

Рисунок 2.6 – Окно выбора пользователя группы

5. Имя локальной группы должно быть уникальным в пределах компьютера. Оно может содержать до 256 символов в верхнем и нижнем регистрах. В имени группы запрещено применение символа обратного слэша (\).

Изменение членства в локальной группе

Чтобы добавить или удалить учетную запись пользователя из группы:

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. В появившемся контекстном меню выберите команду **Добавить в группу** (Add to Group) или **Свойства** (Properties) (см.рисунок 2.7).

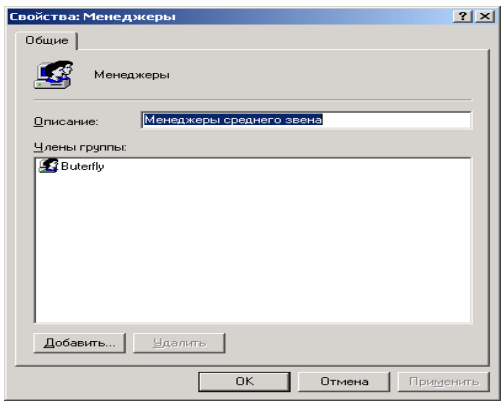

Рисунок 2.7. Окно Свойства группы

3. Для того чтобы добавить новые учетные записи в группу, нажмите кнопку **Добавить.** Далее следуйте указаниям окна диалога **Выбор: Пользователи или Группы** (Select Users or Groups).
4. Для того чтобы удалить из группы некоторых пользователей, в поле **Члены группы** окна свойств группы выберите одну или несколько учетных записей и на кнопку **Удалить** (Remove).

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.

Задание на лабораторную работу

1. В папке Пользователи создать шесть учетных записей.
2. Создать две локальные группы.
3. Созданных пользователей распределить в две локальные группы.
4. По заданию преподавателя произвести изменения в учетных записях и группах.
5. Продемонстрировать преподавателю созданные учетные записи и локальные группы, а также умение управления локальными группами.
6. Удалить созданные в соответствии с п.1 учетные записи.
7. Удалить созданные в соответствии с п.3 локальные группы.

Лабораторная работа 3
Управление рабочей средой пользователя

Цель работы: Освоить технологию системного администрирования при управлении рабочей средой пользователя в операционной системе Windows

Рабочая среда пользователя состоит из настроек рабочего стола, например, цвета экрана, настроек мыши, размера и расположения окон, из настроек процесса обмена информацией по сети и с устройством печати, переменных среды, параметров реестра и набора доступных приложений.

Для управления средой пользователя предназначены следующие средства Windows:

- *Сценарий входа в сеть* (сценарий регистрации) представляет собой командный файл с расширениями bat и cmd, сценарий с расширением vbs и js или исполняемый файл с расширением exe, который выполняется при каждой регистрации пользователя в сети. Сценарий может содержать команды операционной системы, предназначенные, например, для создания соединения с сетью или для запуска приложения. Кроме того, с помощью сценария можно устанавливать значения переменных среды, указывающих пути поиска, каталоги для временных файлов и другую подобную информацию.
- *Профили пользователей.* В профиле пользователя хранятся все настройки рабочей среды компьютера, на котором работает Windows, определенные самим пользователем. Это могут быть, например, настройки экрана и соединения с сетью. Все настройки, выполняемые самим пользователем, автоматически сохраняются в файле, путь к которому выглядит следующим образом: *Имя_устройства\корневой_каталог\Profiles.* Как правило, корневым является каталог *\winnt.*
- *Сервер сценариев Windows* (Windows Scripting Host, WSH). Сервер сценариев независим от языка и предназначен для работы на 32-разрядных платформах Windows. Он включает в себя как ядро сценариев Visual Basic Scripting Edition (VBScript), так и JScript. Сервер сценариев Windows предназначен для выполнения сценариев с использованием графического интерфейса или в командной строке. При этом сценарии не надо встраивать *в* документ HTML.

Профили пользователей

На изолированном компьютере с Windows локальные профили пользователей создаются автоматически. Информация локальных профилей необходима для поддержки настроек рабочего стола локального компьютера, характерных для конкретного пользователя.

Профиль создается для каждого пользователя в процессе его первой регистрации в компьютере, а сохраняется при выходе из системы.

Профиль пользователя обладает следующими преимуществами:

При регистрации пользователя в системе рабочий стол получает те же настройки, какие существовали в момент предыдущего выхода пользователя из системы.

Несколько пользователей могут работать на одном и том же компьютере в индивидуальных средах.

Профили пользователей могут быть сохранены на некотором компьютере в сети. В этом случае пользователь получает возможность работать со своим профилем при регистрации на любом компьютере сети. Такие профили называются *перемещаемыми* (roaming profile).

Пользовательские профили можно применять следующим образом:

Создать несколько типов профилей и назначить их определенным группам пользователей. Это позволит получить несколько типов рабочих сред, соответствующих различным задачам, решаемым пользователями.

Назначать общие групповые настройки всем пользователям.

Назначать обязательные профили, какие-либо настройки которых пользователи изменять не могут.

Настройки, хранящиеся в профиле пользователя

Профиль пользователя хранит настройки конфигурации и параметры, индивидуально назначаемые каждому пользователю и полностью определяющие его рабочую среду (см.таблицу 3.1).

Таблица 3.1 – Настройки профиля пользователя

Объект	Соответствующие ему параметры
Windows NT Explorer	Все настройки, определяемые самим пользователем, касающиеся программы Проводник (Windows NT Explorer)
Панель задач	Все персональные группы программ и их свойства, все программные объекты и их свойства, все настройки панели задач
Настройки принтера	Сетевые соединения принтера
Панель управления	Все настройки, определенные самим пользователем, касающиеся панели управления
Стандартные	Настройки всех стандартных приложений, запускаемых для конкретного пользователя
Приложения, работающие в операционной системе Windows	Любое приложение, специально созданное для работы в среде Windows, может обладать средствами отслеживания своих настроек относительно каждого пользователя. Если такая информация существует, она хранится в профиле пользователя
Объект	Соответствующие ему параметры
Электронная подсказка	Любые закладки, установленные в справочной системе Windows
Консоль управления Microsoft	Индивидуальный файл конфигурации и текущего состояния консоли управления

Структура профиля пользователя

Профиль пользователя создается на основе профиля, назначаемого по умолчанию. Он хранится на каждом компьютере, где работает Windows. Файл NTuser.dat, находящийся в папке **Default User**, содержит настройки конфигурации, хранящиеся в реестре Windows. Кроме того, каждый профиль пользователя использует общие программные группы, находящиеся в папке **All Users**.

Папки профиля пользователя

Как уже говорилось, при создании профиля пользователя используется профиль, назначаемый по умолчанию, находящийся в папке **Default User.** Папка **Default User,** папки профилей индивидуальных пользователей, а также папка **All Users,** находятся в папке **Documents and Settings** корневого каталога. В папке **Default User** находятся файл NTuser.dat и список ссылок на объекты рабочего стола. На рисунке 3.1 показана структура папок *локального* профиля пользователя. В этих папках, в частности, хранятся ссылки на различные объекты рабочего стола. В таблице 3.2 перечислены подпапки, находящиеся внутри папки локального профиля пользователя, и описано их содержимое.

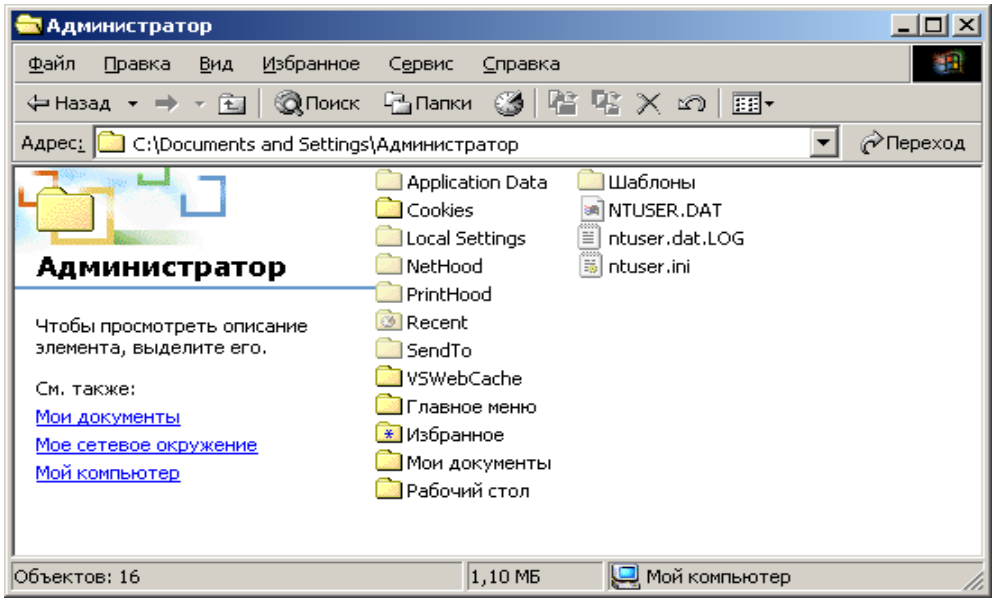

Рисунок 3.1– Структура подпапок профиля пользователя

Таблица 3.2 – Содержимое папки локального профиля пользователя

Подпапка	Содержимое
Application Data	Данные, относящиеся к конкретному приложению. Например, индивидуальный словарь. Разработчики приложений сами принимают решение, какие данные должны быть сохранены в папке профиля пользователя
Cookies	Служебные файлы, получаемые с просматриваемых веб-серверов
Local Settings	Данные о локальных настройках, влияющих на работу программного обеспечения компьютера
NetHood	Ярлыки объектов сетевого окружения

PrintHood	Ярлыки объектов папки принтера
Recent	Ярлыки недавно используемых объектов
SendTo	Ярлыки объектов, куда могут посылаться документы
Главное меню(Start Menu)	Ярлыки программ
Избранное (Favorites)	Ярлыки часто используемых программ и папок
Мои документы (My Documents)	Данные о документах и графических файлах, используемых пользователем
Рабочий стол (Desktop)	Объекты рабочего стола, включая файлы и ярлыки
Шаблоны (Templates)	Ярлыки шаблонов

Папка All Users

Настройки, находящиеся в папке **All Users,** не копируются в папки профиля пользователя, но используются для его создания. Платформы Windows NT поддерживают два типа программных групп:

*Общие программные группы***.** Они всегда доступны на компьютере, независимо от того, кто зарегистрирован на нем в данный момент. Только администратор может добавлять объекты к этим группам, удалять или модифицировать их.

*Персональные программные группы***.** Они доступны только создавшему их пользователю.

Общие программные группы хранятся в папке **All Users,** находящейся в папке **Documents and Settings.** Папка **All Users** также содержит настройки для рабочего стола и меню **Пуск.** Группы этого типа на компьютерах, где работает Windows, могут создавать только члены группы Администраторы.

Создание локального профиля пользователя

Локальный профиль пользователя хранится на компьютере в папке, имя которой совпадает с именем данного пользователя, находящейся в папке **Documents and Settings.** Если для данного пользователя не существует сконфигурированный перемещаемый (находящийся на сервере) профиль, то при **первой регистрации пользователя в компьютере для него создается индивидуальный профиль**. Содержимое папки **Default User** копируется в папку нового профиля пользователя. Информация профиля, вместе с содержимым папки **All Users** используется при конфигурации рабочей среды пользователя. При завершении пользователем работы на компьютере все сделанные им изменения настроек рабочей среды, выбираемых по умолчанию, записываются в его профиль. Содержимое папки **Default User** остается неизменным.

Если пользователь имеет отдельную учетную запись на локальном компьютере и в домене, для каждой из них создается свой профиль

пользователя, поскольку регистрация на компьютере происходит с помощью различных учетных записей. При завершении работы все сделанные изменения также записываются в соответствующий данной учетной записи профиль.

Папка профиля пользователя на локальном компьютере содержит файл NTuser.dat и файл журнала транзакций с именем NTuser.dat.LOG (см.рисунок 3.1). Он нужен для обеспечения отказоустойчивости, позволяя Windows восстанавливать профиль пользователя в случае сбоя при модификации содержимого файла NTuser.dat.

Перемещаемые профили пользователя

Перемещаемые профили пользователя могут быть созданы тремя способами:

- Каждой учетной записи назначается путь к профилю пользователя. В этом случае на сервере происходит автоматическое создание пустой папки профиля пользователя. Затем пользователь может сам создать свой профиль.
- Каждой учетной записи назначается путь к профилю пользователя. Затем в папку, указанную в пути, копируется приготовленный заранее профиль пользователя.
- Каждой учетной записи назначается путь к профилю пользователя. Затем в папку, указанную в пути, копируется приготовленный заранее профиль пользователя. После этого файл NTuser.dat, путь к которому указан в каждой учетной записи, переименовывается в NTuser.man. В этом случае создается обязательный профиль пользователя.

В перемещаемый профиль не входит подпапка **Local Settings,** где хранятся архивы программы Outlook Express, папки **Temporary Internet Files и History** и временные файлы!

Имя сервера (это может быть любой компьютер в сети!), на котором будут находиться перемещаемые профили пользователей, указывается с помощью оснастки **Локальные пользователи и группы** и вкладки **Профиль** окна свойств пользователя. В результате при завершении работы пользователя на компьютере его профиль сохраняется как на локальном компьютере, так и в папке на сервере, в соответствии с путем профиля. При следующей регистрации пользователя в сети дата копии профиля, находящейся на сервере, сравнивается с копией, расположенной локально на компьютере. Если они отличаются, информация берется из более свежей копии.

Перемещаемый профиль находится в централизованном хранилище профилей в масштабах домена. Он может быть доступен только при условии работоспособности хранящего его сервера. В обратном случае используется локальная кэшированная копия профиля пользователя. Если пользователь первый раз зарегистрировался в компьютере, создается новый профиль. В любом случае, если хранящийся централизованно профиль пользователя недоступен, он не обновляется при завершении работы. При следующей

регистрации в компьютере пользователю придется напрямую указать копию профиля - более новую локальную или старую копию, находящуюся на сервере.

Настройка перемещаемых профилей пользователей, являющихся членами домена Windows, выполняется при помощи оснастки **Active Directory -пользователи и компьютеры**, поскольку основная информация о пользователях домена хранится в каталоге. В остальном логика управления профилями остается неизменной: перемещаемый профиль хранится в указанной папке на некотором общем сетевом ресурсе, а в случае его недоступности используется кэшированная копия с локального компьютера.

Для создания перемещаемого профиля вначале необходимо сделать копию профиля на сервере или в любой другой папке. В окне диалога **Свойства системы** перейдите на вкладку **Профили пользователей.** Все профили пользователей, созданные на компьютере, появятся в списке **Профили, хранящиеся на этом компьютере**. На рисунке 3.2 выделен профиль пользователя DOLJENKO\Лидия

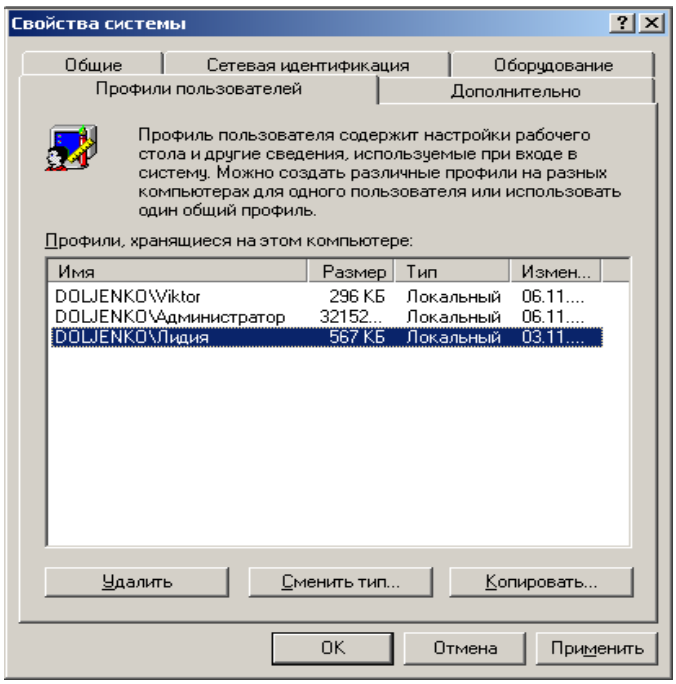

Рисунок 3.2 – Окно **Свойства системы** со списком профилей пользователя

Для копирования определенного профиля пользователя необходимо его выделить и нажать кнопку **Копировать**. В появившемся диалоговом окне необходимо ввести имя целевой папки ((DOLJENKO\D:\Profiles\Лидия)) или выбрать её с помощью службы просмотра – Обзор . . .(см. рисунок 3.3).

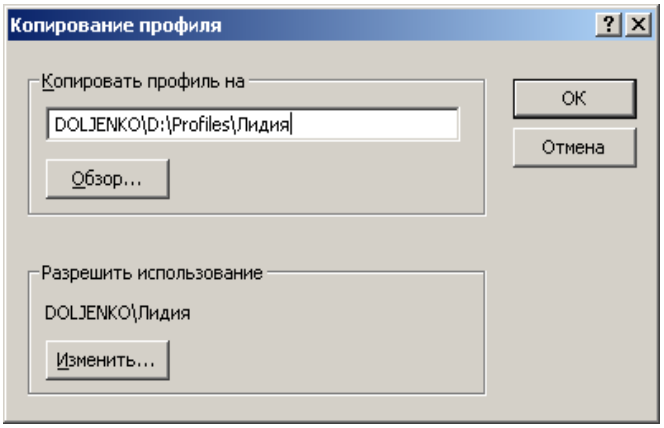

Рисунок 3.3 – Окно диалога Копирование профиля

При последующей регистрации вместо профиля, установленного по умолчанию, пользователь получит копию заранее сконфигурированного профиля с сервера. В дальнейшем этот профиль функционирует так же, как любой стандартный профиль пользователя. Каждый раз, когда пользователь завершает работу, его профиль сохраняется локально и одновременно копируется на сервер.

Для копирования профиля пользователя следует перейти на вкладку **Профили пользователей** окна **Система**. Нельзя для этой цели использовать Проводник или какой-либо другой инструмент управления файлами.

Обязательный профиль представляет собой сконфигурированный заранее перемещаемый профиль, который недоступен пользователю для модификации. Пользователь может изменять настройки рабочего стола, но при завершении работы на компьютере изменения не заносятся в профиль. При следующей регистрации на компьютере загружается обязательный профиль пользователя, в котором не произошло никаких изменений. Профиль пользователя становится обязательным, когда вы переименовываете файл NTuser.dat в NTuser.man. В этом случае файл становится доступен только для чтения. Один обязательный профиль может быть использован большим количеством пользователей. Когда для обеспечения безопасности или приведения рабочей среды пользователя в соответствии с его уровнем подготовки для работы на компьютере необходимо контролировать набор доступных функций, лучше использовать групповые политики. С их помощью вы можете выбрать подмножество настроек, а также контролировать как параметры среды *пользователя,* так и настройки *компьютера.* При копировании профиля на сервер необходимо в учетной записи указать полный путь к профилю пользователя: \\сервер*имя_общего_ресурса**имя_профиля.*

В качестве общего ресурса может выступать любая папка, к которой следует организовать общий доступ для группы **Все** (Everyone). В качестве имени профиля следует указать имя папки профиля данного пользователя (это может быть любая папка на общем ресурсе, в которой будет храниться профиль) Путь профиля пользователя может указывать на любой компьютер, не обязательно это должен быть сервер или контроллер домена.

В лабораторной работе перемещаемый профиль устанавливается на локальном компьютере в папке D:\Profiles\Лидия (см.рисунок 3.4). Когда пользователь регистрируется в сети, система Windows проверяет, указан ли в его учетной записи путь профиля. Если путь указан, система находит соответствующий профиль.

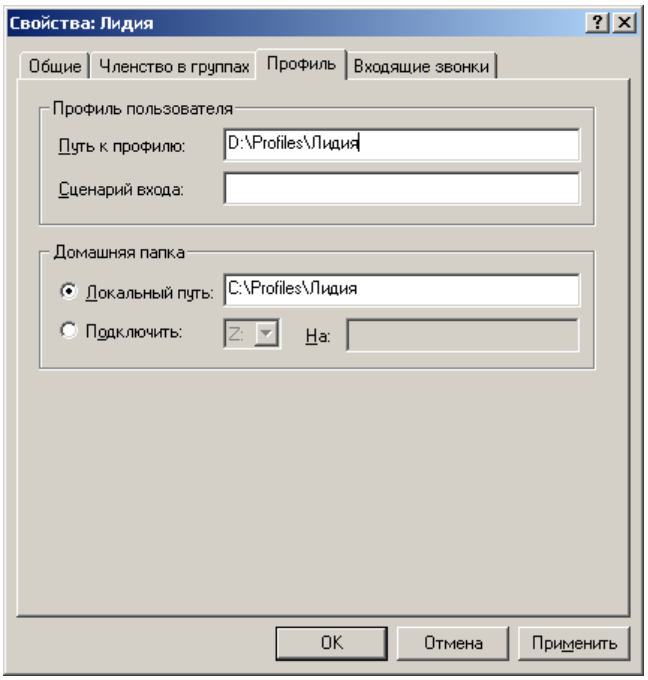

Рисунок 3.4 – Вкладка **Профиль** (Profile) окна свойств учетной записи

Копирование профиля пользователя на сервер

Для того чтобы сделать определенный профиль доступным для нескольких пользователей, необходимо скопировать его на сервер с помощью вкладки **Профили пользователей** окна **Система,** вызываемого из панели управления. На рис 3.4 показан пример окна **Свойства системы** со списком созданных на компьютере профилей пользователя.

Место, куда скопирован профиль, должно совпадать с путем профиля, указанным в учетных записях пользователей

В окне диалога **Свойства системы** (System Properties) перейдите на вкладку **Профили пользователей.** Все профили пользователей, созданные на компьютере, появятся в списке **Профили, хранящиеся на этом компьютере** (Profiles stored on this computer).

Для копирования определенного профиля пользователя перейдите на вкладку **Копировать** и введите имя целевой папки (см.рисунок 3.5). В качестве альтернативы можно выбрать целевую папку с помощью службы просмотра.

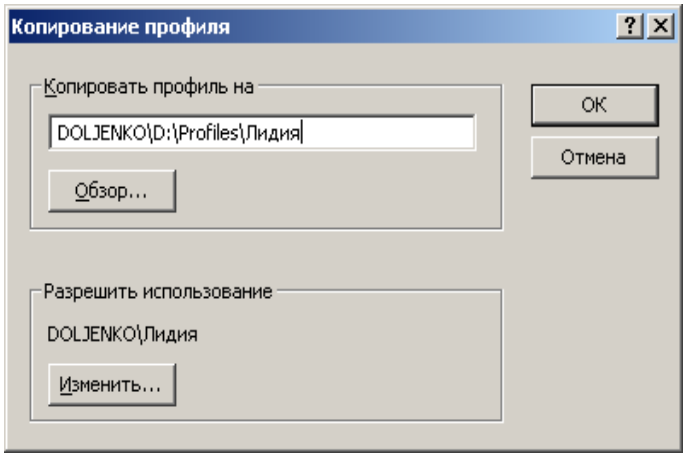

Рисунок 3.5 – Окно диалога Копирование профиля

Завершите сеанс пользователя с правами администратора и войдите в систему под именем пользователя, для которого был создан перемещаемый профиль (в нашем случае учетная запись с именем пользователя: Лидия). В свойствах системы для профиля пользователя Лилия будет указан тип перемещаемого профиля (см.рисунок 3.6).

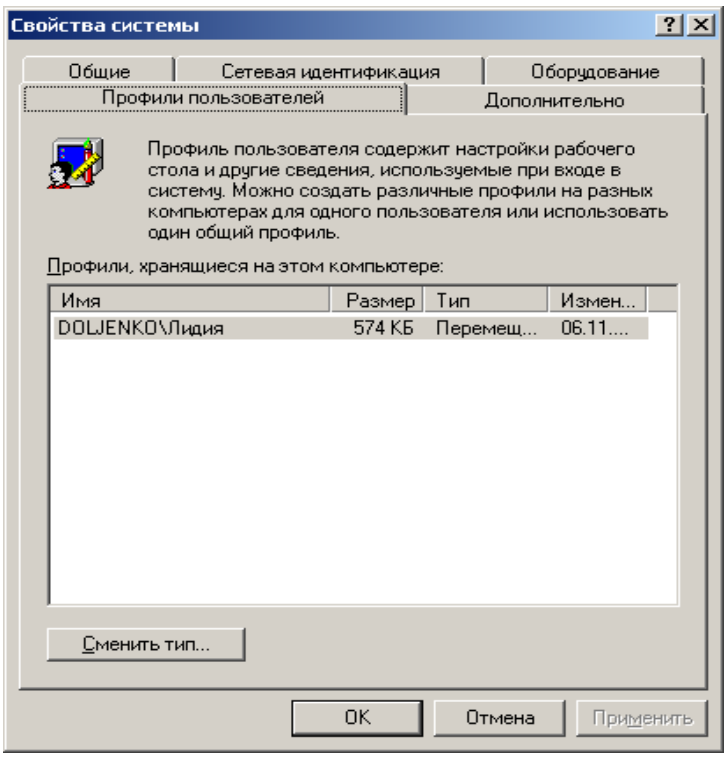

Рисунок 3.6 – Окно Свойство системы с указанием перемещаемого профиля

Добавление пользователей и групп к списку разрешений перемещаемого профиля пользователя

Данная функция может выполняться пользователем с правами администратора. С помощью окна **Система** вместе с профилем пользователя копируются и соответствующие разрешения. Поэтому пользователь

автоматически получает доступ к своему профилю. Однако если вы хотите, чтобы к профилю получили доступ другие пользователи и группы, необходимо добавить их в список объектов, которым разрешено использовать данный профиль. Для этого в списке **Профили, хранящиеся на этом компьютере** выберите интересующий вас профиль и нажмите кнопку **Копировать.** Появится окно диалога **Копирование профиля** (Copy To) (см.рисунок 3.5*)*. В группе **Разрешить использование** (Permitted to use) показано, кто имеет разрешение на использование данного профиля (DOLJENLO\Лидия). Для того чтобы добавить нового пользователя или группу к списку разрешений профиля пользователя, нажмите кнопку **Изменить** (Change). В результате выводится окно **Выбор: Пользователь или Группа** (см.рисунок 3.7).

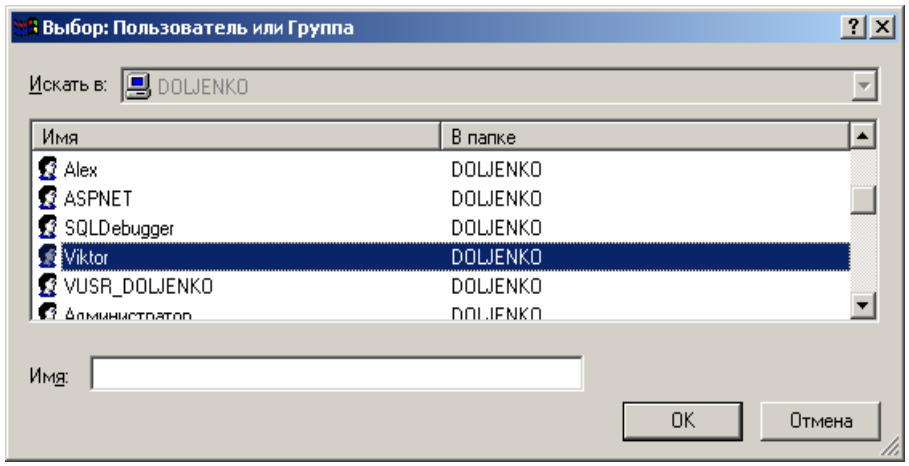

Рисунок 3.7– Окно выбора пользователя или группы

После выбора нового пользователя необходимо указать имя целевой папки для данного пользователя и произвести копирование профиля (см.рисунок 3.8)

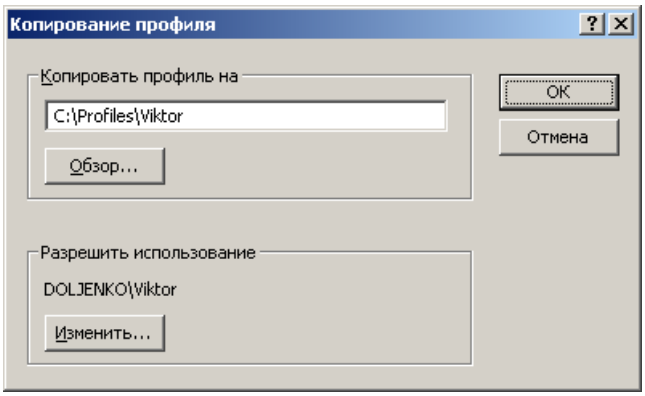

Рисунок 3.8 – Добавление нового пользователя к списку разрешений перемещаемого профиля

Если вы назначаете путь перемещаемого профиля пользователя группе, то при каждом завершении работы кого-либо из членов группы его настройки записываются в хранящийся централизованно профиль. По этой

причине рекомендуется делать такие профили пользователя обязательными или устанавливать различные настройки разным группам с помощью системных политик.

Изменение типа профиля пользователя для подключения по медленной линии

Пользователи, присоединяющиеся к сети по медленной линии, например, при использовании службы удаленного доступа, могут работать со своим локальным профилем, а не загружать его с сервера по сети, что значительно ускоряет процесс регистрации. В таком случае при регистрации появляется окно, в котором пользователь может указать, какой профиль должен быть загружен

Если вы уже зарегистрировались в сети, с помощью кнопки **Сменить тип** (Change Type) на вкладке **Профиль** окна свойств системы можно изменить тип профиля пользователя с перемещаемого на локальный и наоборот (см.рисунок 3.9).

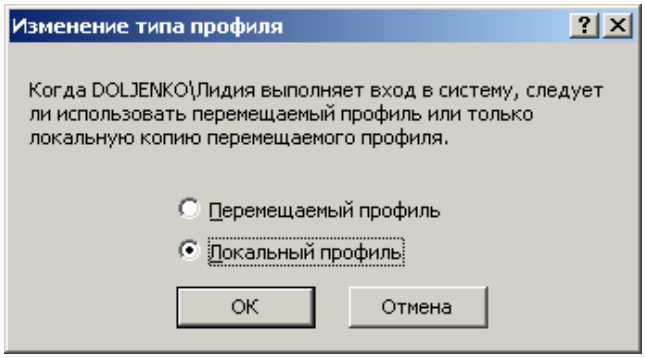

Рисунок 3.9 – Изменение типа профиля

Новые настройки останутся неизменными до их следующей модификации При изменении профиля пользователя с перемещаемого на локальный кэшированная локально копия вашего профиля будет загружаться при каждой регистрации в компьютере При каждом завершении работы все изменения также будут записываться в локальную копию профиля

Если клиент работает по медленной линии, то для ускорения входа в систему можно установить на компьютере групповую политику, при которой будет использоваться кэшированный профиль, а не загружаемый с сервера Имеется также групповая политика, с помощью которой можно определить, какая линия будет считаться "медленной".

Подготовка заранее настроенных перемещаемых и обязательных профилей пользователя

Хотя для создания заранее сконфигурированного перемещаемого или обязательного профиля можно использовать любую учетную запись, часто удобнее иной подход Например, если вы хотите создать три различных заранее настроенных перемещаемых или обязательных профиля для трех

отделов предприятия, сначала следует создать и настроить три различные базовые учетные записи Затем необходимо зарегистрироваться с помощью каждой из созданных учетных записей и тем самым создать три профиля пользователя для трех отделов. После этого опять зарегистрироваться с помощью учетной записи администратора и, используя оснастку **Локальные пользователи и группы,** назначить созданные профили индивидуальным пользователям или группам. Затем с помощью вкладки **Профили пользователей** окна **Система** панели управления скопируйте созданные профили на соответствующий сервер.

Работа пользователей с различными конфигурациями оборудования

Следует помнить, что профили могут применяться на компьютерах, отличающихся по конфигурации оборудования, особенно типами мониторов и видеоадаптеров.

Профиль пользователя может определять положение и размер окон, поэтому тип оборудования экрана в значительной степени влияет на качество работы профиля. Например, параметры окна, выводимого на экране типа Super VGA, могут быть неверны при выводе того же изображения на экране с типом VGA. Для предотвращения подобных проблем:

- Создавайте и редактируйте профиль пользователя на компьютере, тип экрана которого совпадает с типом экрана компьютера пользователя.
- При создании обязательного профиля для нескольких пользователей создавайте один профиль для группы пользователей только в случае, если все члены группы работают на компьютерах с одинаковым типом экранов.

Удаление профиля пользователя

Если вы больше не хотите использовать перемещаемый или обязательный профиль, назначенный пользователям, с помощью оснастки **Локальные пользователи и группы** удалите путь к нему в учетных записях соответствующих пользователей. Сам профиль пользователя, находящийся на сервере, можно удалить с помощью кнопки **Удалить** на вкладке **Профили пользователей** окна **Система.**

Задание на лабораторную работу

1. Создайте три учетные записи.
2. Зарегистрироваться с помощью каждой из созданных учетных записей.
3. Создать локальный профиль для 1 – го, 2 –го и 3 – го пользователей (зарегистрировать пользователей в системе).
4. Создать перемещаемый профиль для 1 - го пользователя.
5. Добавить пользователей 2 и 3 к списку разрешений перемещаемого профиля 1- го пользователя.
6. Для 2 – го пользователя изменить тип профиля на локальный.
7. Продемонстрировать результаты выполнения лабораторной работы преподавателю.

8. Удалить профили пользователей и созданные учетные записи.

Лабораторная работа 4
Настройка рабочей среды пользователя при помощи сценариев входа и его аутентификация

Цель работы: Научиться настраивать рабочую среду пользователя с помощью специальных сценариев и установкой пароля входа

Сценарии входа выполняются автоматически в процессе каждой регистрации пользователя на компьютере, работающем с программным обеспечением Windows. Хотя чаще всего сценарий входа представляет собой командный файл с расширением *bat* или *cmd*, в качестве сценария может быть использован и исполняемый файл (**.exe*). Сценарии входа не являются обязательными. Они могут применяться для:

- настройки рабочей среды пользователя;
- создания сетевых соединений;
- запуска приложений.

Сценарии входа очень удобны, если необходимо изменить некоторые параметры рабочей среды пользователя без выполнения ее полной настройки.

Примечание. Профили пользователя могут в процессе регистрации восстанавливать существовавшие ранее соединения с сетью, но они не могут быть использованы для создания новых соединений

Создание сценариев входа

Для создания сценариев входа может быть использован обыкновенный текстовый редактор. Затем с помощью оснастки **Локальные пользователи и группы** (Local Users and Groups) сценарии входа назначаются соответствующим пользователям. Кроме того, один сценарий может быть назначен нескольким пользователям. В таблице 4.1 приведены параметры, значения которых можно устанавливать с помощью сценария входа и их описания.

Таблица 4.3 – Параметры, устанавливаемые с помощью сценария входа

Параметр	Описание
%HOMEDRIVE%	Имя устройства локального компьютера, связанного с домашним каталогом пользователя
%HOMEPATH%	Полный путь к домашнему каталогу пользователя
%HOMESHARE%	Имя общего ресурса, где находится домашний каталог пользователя
%OS%	Операционная система компьютера пользователя

%PROCESSOR_ARCHITECTURE%	Тип процессора (например, Pentium) компьютера пользователя
% PROCESSOR_LEVEL%	Уровень процессора компьютера пользователя
%USERDOMAIN%	Домен, в котором находится учетная запись пользователя
%USERNAME%	Имя пользователя

Назначение сценариев входа учетным записям пользователей и групп

Для того, чтобы назначить сценарий входа учетным записям пользователей и групп, с помощью оснастки **Локальные пользователи и группы** (или **Active Directory** - пользователи и компьютеры – если компьютер входит в домен) указывается путь к сценарию. Если при регистрации пользователя с помощью определенной учетной записи среди ее параметров указан путь к сценарию входа, соответствующий файл сценария открывается и выполняется. На вкладке **Профиль** окна свойств учетной записи вы можете назначить сценарий входа, введя в поле **Сценарий входа** (Logon Script) имя файла и, возможно, относительный путь к нему.

При регистрации сервер, аутентифицирующий пользователя, находит файл сценария (если таковой существует) с помощью указанного в учетной записи имени и пути (на контроллерах домена сценарии хранятся в общей папке NETLOGON — *%SystemRoot% \SYSVOL\sysvol\DSN-имя-домена\cripts*; на изолированных компьютерах — в локальной папке ***%SystemRoot% \System32\Repl\Import\Scripts***). Например, по сценарию необходимо при регистрации пользователя «Лидия» открыть текстовый редактор Word. Для этого в любом текстовом редакторе создаем файл *Profstart.bat,* содержащий следующий текст: ***start winword.exe.*** Далее необходимо запомнить файл *Profstart.bat* в папке *C:\Winnt\System32\Repl\Import\Scripts.* Во вкладке **Профиль** (см.рисунок 4.1) окна свойств учетной записи назначаем сценарий входа, введя в поле **Сценарий входа** имя файла *Profstart.bat.*

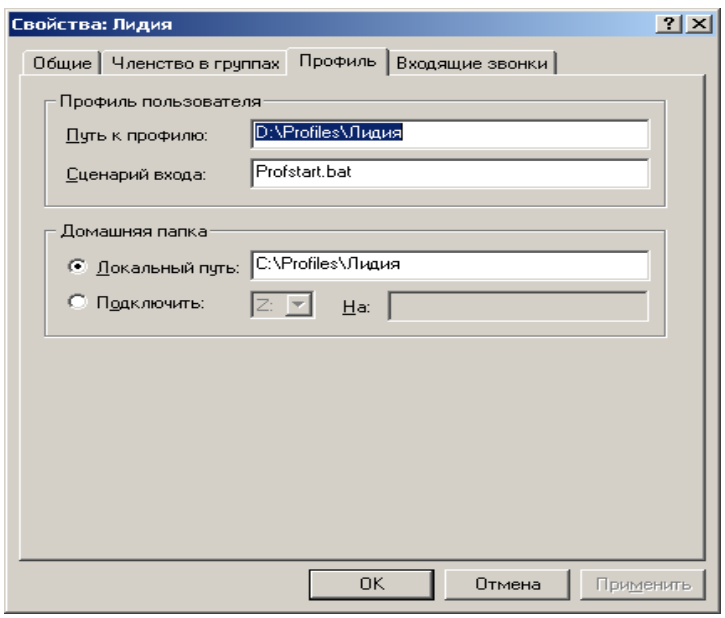

Рисунок 4.1– Вкладке **Профиль** окна свойств учетной записи

Если перед именем файла указан относительный путь, сервер ищет сценарий входа в подкаталоге основного локального пути сценариев. Данные поля **Сценарий входа** определяют только имя файла и относительный путь, но не содержат сам сценарий входа. После создания файл сценария с определенным именем помещается в соответствующий реплицируемый (если компьютеры объединены в домен) каталог.

Сценарий входа можно поместить в локальный каталог компьютера пользователя. Но подобный подход, как правило, применяется только при администрировании учетных записей, существующих на одиночном компьютере, а не в домене. В этом случае вы должны поместить файл сценария в соответствии с локальным путем к сценариям входа в компьютер.

Помимо оснастки **Локальные пользователи и группы,** сценарии входа могут быть назначены пользователям или компьютерам и с помощью оснастки **Групповая политика** (Group Policy).

Переменные среды

Изменение системных и пользовательских переменных среды

Для конфигурирования, поиска, выделения памяти определенным программам и управления приложениями операционная система Windows и прикладные программы требуют определенной информации, называемой *переменными среды* системы и пользователя. Их можно просмотреть на вкладке **Дополнительно** (Advanced) окна **Система** (см. рисунок 4.2), нажав кнопку **Переменные среды** (Environment Variables) (см. рисунок 4.3). Эти переменные похожи на переменные, которые устанавливались в операционной системе MS-DOS, например *PATH* и *TEMP*.

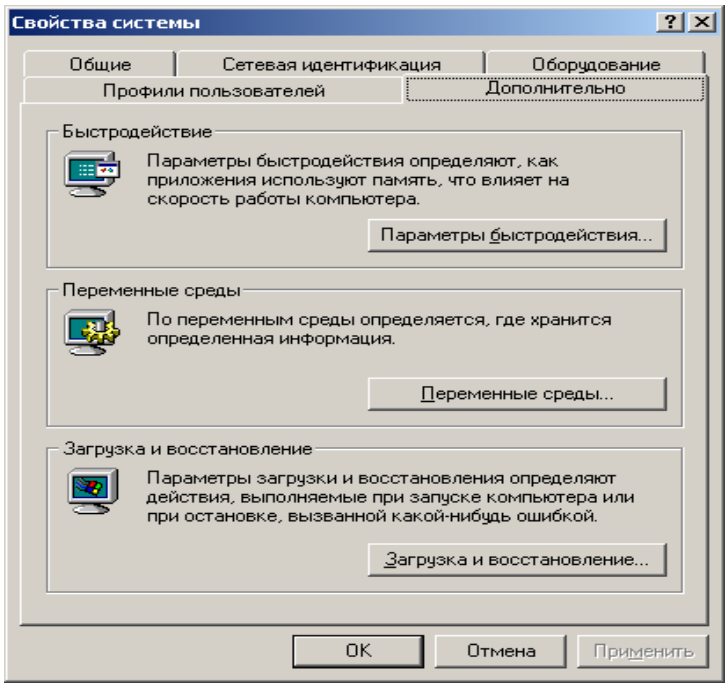

Рисунок 4.2 – Окно свойства системы

Системные переменные среды определяются в Windows независимо от того, кто зарегистрировался на компьютере. Если вы зарегистрировались как член группы Администраторы, то можете добавить новые переменные или изменить их значения.

Переменные среды *пользователя* устанавливаются индивидуально для каждого пользователя одного и того же компьютера. Сюда включаются любые переменные среды, которые вы хотите определить, или переменные, определенные вашим приложением, например путь к файлам приложения.

После изменения переменных среды их новые величины сохранятся в реестре, после чего они становятся доступны ("видны") при закрытии окна **Переменные среды.**

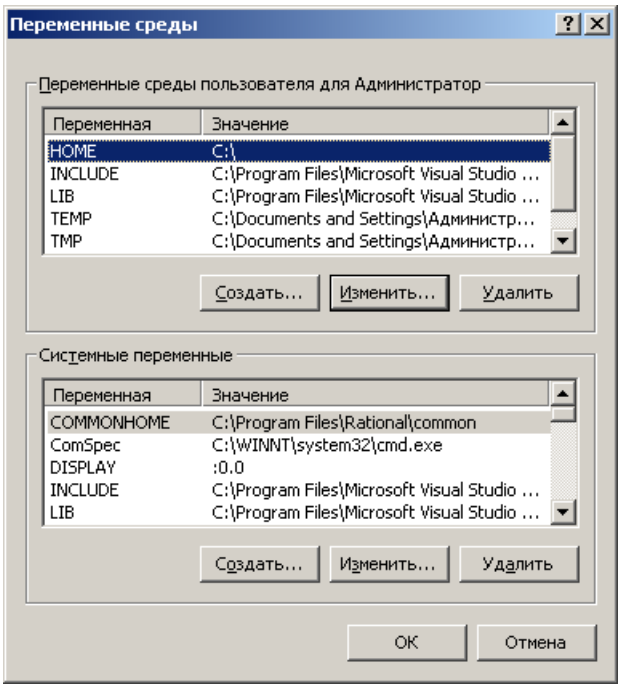

Рисунок 4.3 – Окно Переменные среды

Если между переменными среды возникает конфликт, он разрешается следующим способом:

1. Устанавливаются системные переменные среды.
2. Устанавливаются переменные, определенные в файле *Autoexec.bat* (за исключением переменных *PATH*). Они перезаписывают системные переменные.
3. Устанавливаются переменные среды пользователя, определенные в окне **Система.** Они перезаписывают как системные переменные, так и переменные файла *Autoexec.bat.*
4. Устанавливаются переменные *PATH* файла *Autoexec.bat.*

Примечание. Настройки пути (*PATH*), в отличие от других переменных среды, кумулятивно. Полный путь (который вы видите как результат выполнения в командной

строке команды *path*) создается присоединением путей, устанавливаемых в файле *Autoexec.bat*, к путям, определенным в окне **Система**

Использование переменных среды в профилях пользователей, именах домашних каталогах и сценариев входа

При управлении множеством учетных записей пользователей и групп часто возникает необходимость одновременно выполнить одинаковые изменения в нескольких учетных записях. Вместо конкретных имен или меток в сценарий входа вводится одна общая переменная среды, замещаемая реальными данными в процессе выполнения сценария.

Значение любой переменной среды компьютера клиента, где работает программное обеспечение Windows, может быть подставлено в путь профиля, задаваемого в учетной записи пользователя, путь сценария входа, путь домашнего каталога и в сам сценарий входа. Для этого системную переменную среды следует заключить в знаки процента (%). Например, для того чтобы использовать в пути профиля пользователя переменную среды *servername*, в поле **Путь к профилю** (Profile Path) окна учетной записи следует ввести *\\%servername%\scnpts*.

Подобный подход очень удобен при работе с профилями пользователя в сетях, включающих каналы WAN. Особенно, если ваши пользователи работают с обеих сторон этого канала. Предположим, что сеть состоит из двух площадок, разделенных глобальным каналом. На каждом из компьютеров, работающих на одной стороне канала, переменная *servername* устанавливается в соответствии с именем контроллера домена данной площадки. На другой стороне канала переменная *servername* устанавливается аналогичным образом, но ее значение соответствует имени контроллера домена этой площадки. Теперь в пути сценария входа каждой учетной записи пользователя домена используется *%servername%.* Когда пользователь регистрируется в сети, его сценарий входа загружается с сервера, определяемого переменной среды и расположенного локально относительно глобального канала.

Задание на лабораторную работу

1. Создать три учетные записи.
2. Создать файл для сценария пользователя.
3. Скопировать файл сценария в стандартную папку сценариев.
4. Задать в профиле первого пользователя сценарий входа.
5. Проверить выполнение сценария при регистрации пользователя в системе.
6. Задать в профиле второго пользователя сценарий входа.
7. Проверить выполнение сценария при регистрации пользователя в системе.
8. Для третьего пользователя задать сценарий первого пользователя

9. Проверить выполнение сценария при регистрации пользователя в системе.
10. Продемонстрировать результаты выполненной лабораторной работы преподавателю.
11. Удалить профили пользователей и созданные учетные записи.

Лабораторная работа 5
Аудит локальной системы

***Цель работы*: Научиться осуществлять проверку событий в ОС, имеющие отношение к безопасности файловой системы**

Аудит – это процесс, позволяющий фиксировать события, происходящие в операционной системе и имеющие отношение к безопасности. Например, попытки создать объекты файловой системы или Active Directory, получить к ним доступ или удалить их. Информация о подобных событиях заносится в файл журнала событий операционной системы.

После включения аудита операционная система Windows начинает отслеживать события, связанные с безопасностью. Полученную в результате информацию можно просмотреть с помощью оснастки Просмотр событий (Event Viewer). В процессе настройки аудита необходимо указать, какие события должны быть отслежены. Информация о них помещается в журнал событий. Каждая запись журнала хранит данные о типе выполненного действия, пользователе, выполнившем его, а также о дате и моменте времени выполнения данного действия. Аудит позволяет отслеживать как успешные, так и неудачные попытки выполнения определенного действия, поэтому при просмотре журнала событий можно выяснить, кто предпринял попытку выполнения неразрешенного ему действия.

Аудит представляет собой многошаговый процесс. Сначала его следует активизировать с помощью оснастки Групповая политика (Group Policy). (По умолчанию аудит отключен, поскольку он несколько снижает производительность системы.) После включения аудита необходимо определить набор отслеживаемых событий. Это могут быть, например, вход и выход из системы, попытки получить доступ к объектам файловой системы и т. д. Затем следует указать, какие конкретно объекты необходимо подвергнуть аудиту и включить его с помощью Редактора списков управления доступом, ACL.

Для того чтобы иметь возможность настраивать аудит для файлов и папок, необходимо иметь права администратора

Аудит, установленный для родительской папки, автоматически наследуется всеми вновь созданными дочерними папками и файлами. Этого можно избежать, если при создании файла или папки вызвать окно свойств и на вкладке **Аудит** (Auditing) снять флажок **Переносить наследуемый от родительского объекта аудит на этот объект** (Allow inheritable auditing en-

tries from parent to propagate to this object). Если же этот флажок отображен серым цветом или кнопка **Удалить** недоступна, это значит, что настройки аудита уже унаследованы. В этом случае для изменения настроек аудита дочерних объектов нужно изменить настройки аудита родительской папки, и они будут наследоваться всеми дочерними объектами.

Активизация аудита с помощью оснастки Групповая политика (Group Policy)

Для активизации аудита на изолированном компьютере:
Запустите оснастку **Групповая политика** (это изолированная оснастка, которую можно использовать как самостоятельный инструмент). Можно выполнить команду **Пуск/Программы/Администрирование/Локальная политика безопасности** (см.рисунок 5.1 и 5.2) или подключите к консоли оснастку **Групповая политика** (Group Policy)

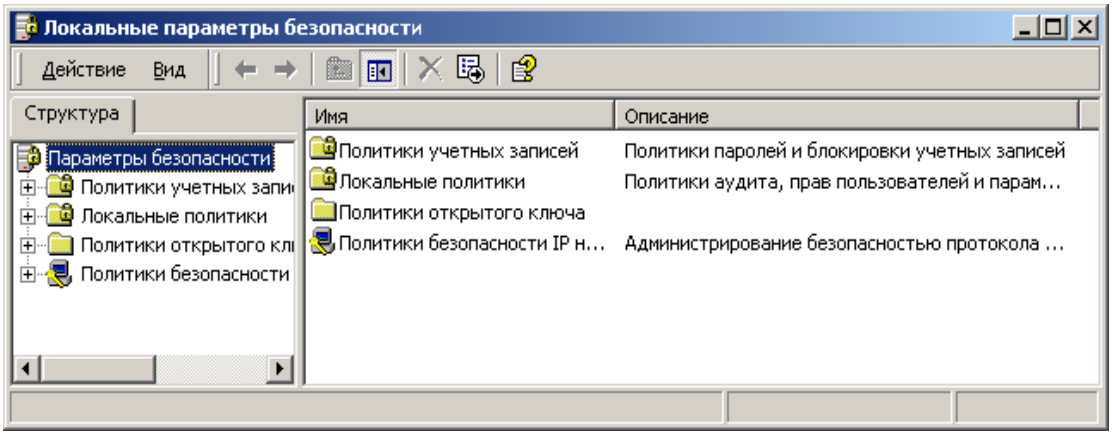

Рисунок 5.1– Папка Локальные параметры безопасности

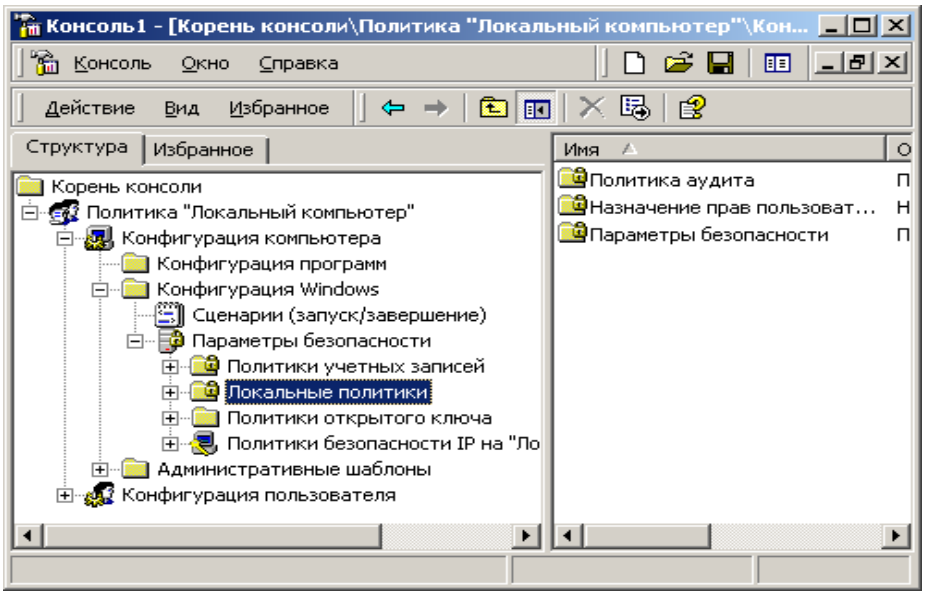

Рисунок 5.2 – Оснастка групповая политика

1. Откройте папку **Локальные политики** (Computei Configuration) и раскройте узлы **Конфигурация Windows** (Windows Setting), **Параметры**

безопасности (Secuiity Settings), **Локальные политики** (Local Policies), **Политика аудита** (Audit Policy) (см.рисунок 5.3).

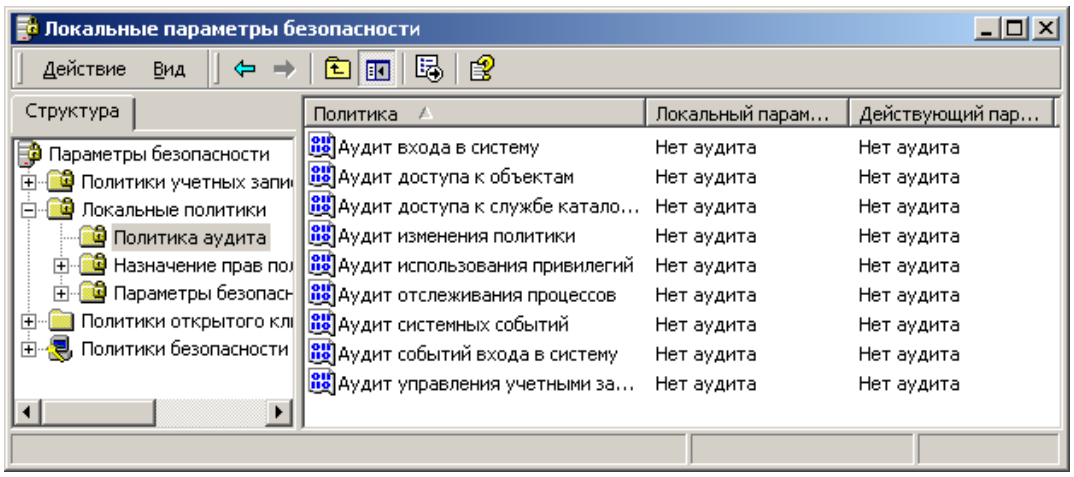

Рисунок 5.3 – Узел **Политика аудита**

2. На правой панели появится список политик аудита. По умолчанию все они имеют значение Нет аудита (No Auditing). Для включения аудита следует изменить значения нужных параметров.

3. Выполните двойной щелчок на устанавливаемой политике аудита. Появится окно диалога, с помощью которого можно разрешить аудит. В группе Вести аудит следующих попыток доступа (Audit these attempts) установите флажки Успех (Success) или Отказ (Failure), или оба (см.рисунок 5.4). Аналогично можно установить аудит управления учетными записями.

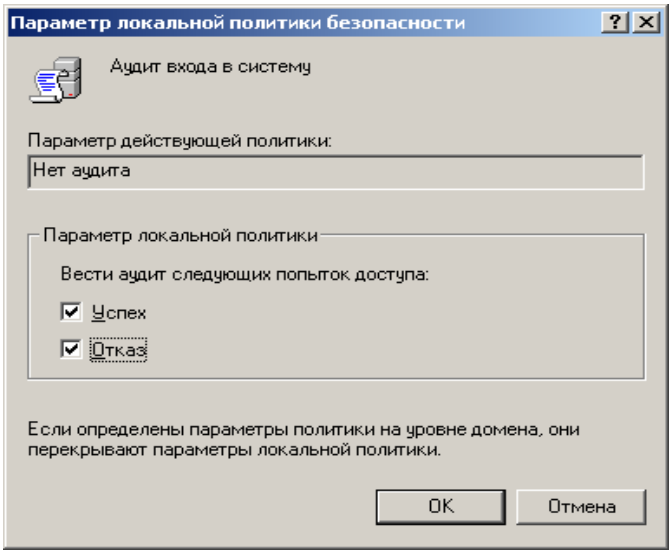

Рисунок 5.4 - Окно **Параметры локальной политики**

4. Нажмите кнопку ОК. В результате проведенных действий на правой панели окна Локальные параметры безопасности для политик Аудит входа в систему и Аудит управления учетными записями изменятся локальные параметры на значение Успех, Отказ (см.рисунок 5.5). Подобную операцию

следует повторить для политик аудита, которые вы хотите активизировать. Для того чтобы отключить аудит, следует снять флажки **Успех и Отказ.**

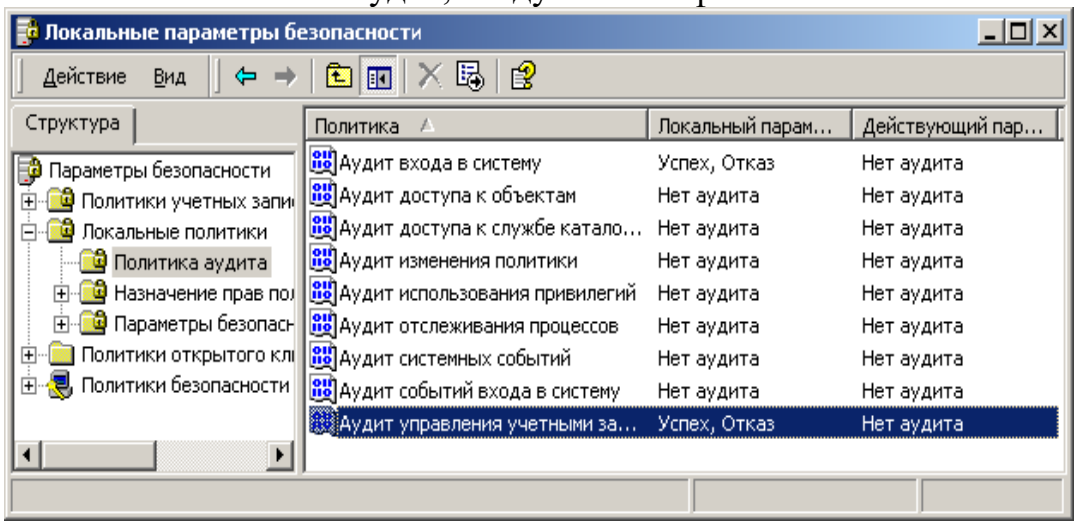

Рисунок 5.5 – Узел Политика аудита с измененными Локальными параметрами

Настройка и просмотр аудита папок и файлов

Чтобы настроить, просмотреть или изменить настройки аудита файлов и папок:

1. Установите указатель мыши на файл или папку, для которой следует выполнить аудит (например, папка Аналитика), и нажмите правую кнопку. В появившемся контекстном меню выберите команду Свойства, что приведет к открытию окна Свойства (см.рисунок 5.6).

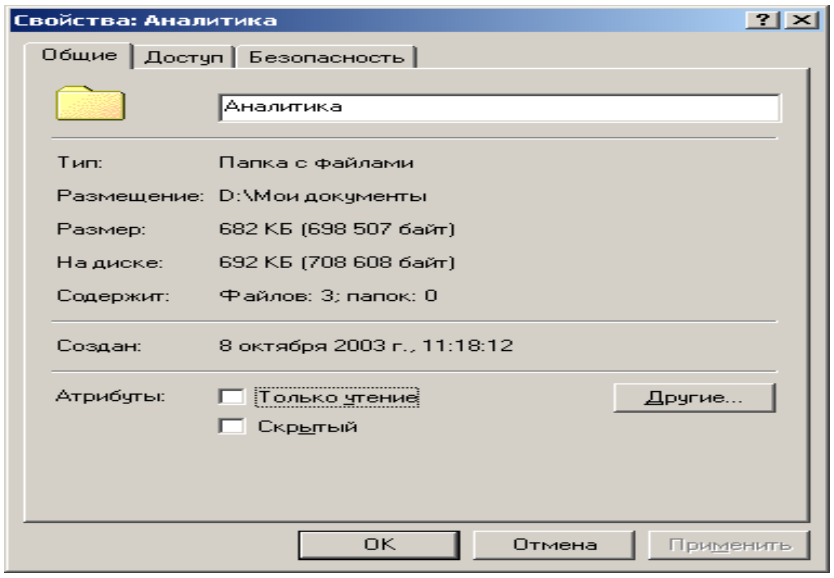

Рисунок 5.6 - Окно **Свойство** вкладка **Общие**

В окне свойств папки или файла перейдите на вкладку **Безопасность** (Security) (см.рисунок 5.7).

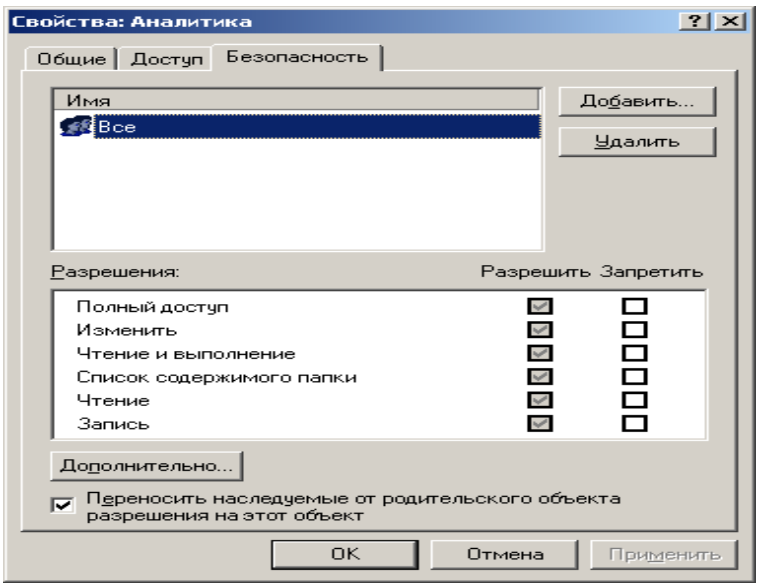

Рисунок 5.7 – Окно **Свойство** вкладка Безопасность

2. На вкладке Безопасность нажмите кнопку Дополнительно (Advanced) и перейдите на вкладку Аудит (см.рисунок 5.8).

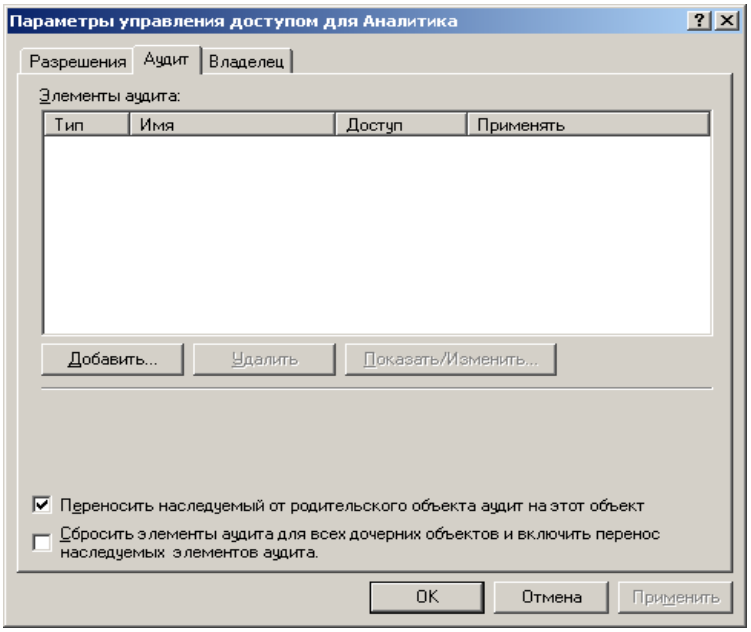

Рисунок 5.8 - Окно Параметры управления доступом вкладка Аудит

3. Если вы хотите настроить аудит для нового пользователя или группы, на вкладке Аудит нажмите кнопку Добавить. Появится диалоговое окно Выбор: Пользователь, Компьютер или Группа (Select User, Computer, or Group). Выберите имя нужного пользователя или группы и нажмите кнопку ОК (на см.рисунок 5.9 выбран пользователь Viktor).

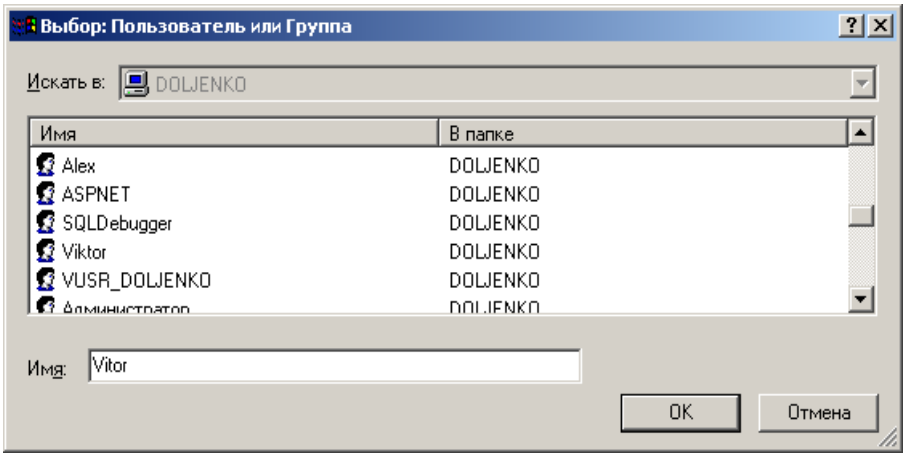

Рисунок 5.9. Окно **Выбор: Пользователь или Группа**

4. Откроется окно диалога Элемент аудита для (Audit Entry for). Здесь вы сможете ввести все необходимые параметры аудита. В списке Применять (Apply onto) укажите, где следует выполнять аудит (это поле ввода доступно только для папок). В группе Доступ (Access) следует указать, какие события следует отслеживать: окончившиеся успешно (Успех, Successfull), неудачно (Отказ, Failed) или оба типа событий. Флажок Применять этот аудит к объектам и контейнерам только внутри этого контейнера (Apply these audit entries to objects and/or containers within this container only) 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 (см.рисунок 5.10).

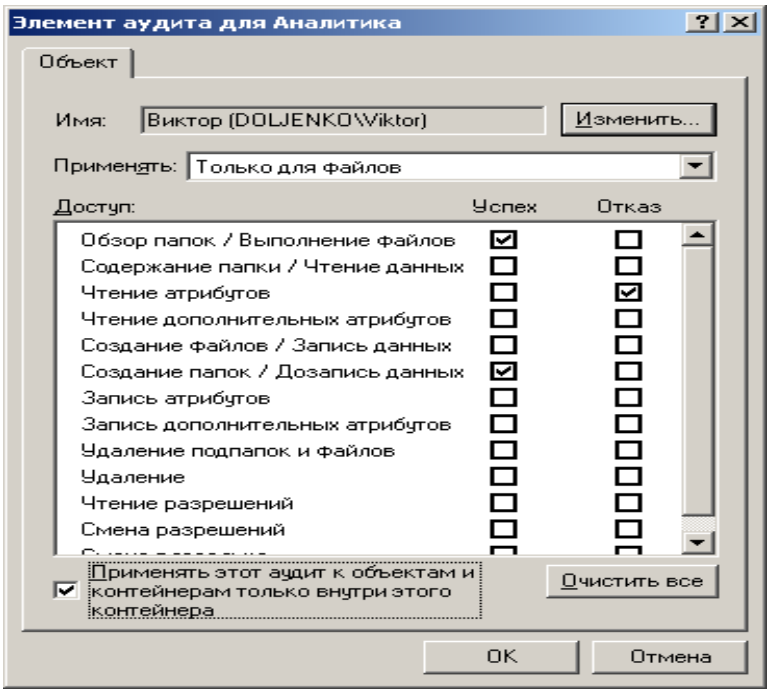

Рисунок 5.10 – Окно **Элементы аудита**

После завершения настройки аудита для папки или файла нажмите кнопку **ОК**. В окне **Параметры управления** доступом будут отображены установленные элементы аудита (см. рисунок 5.11).

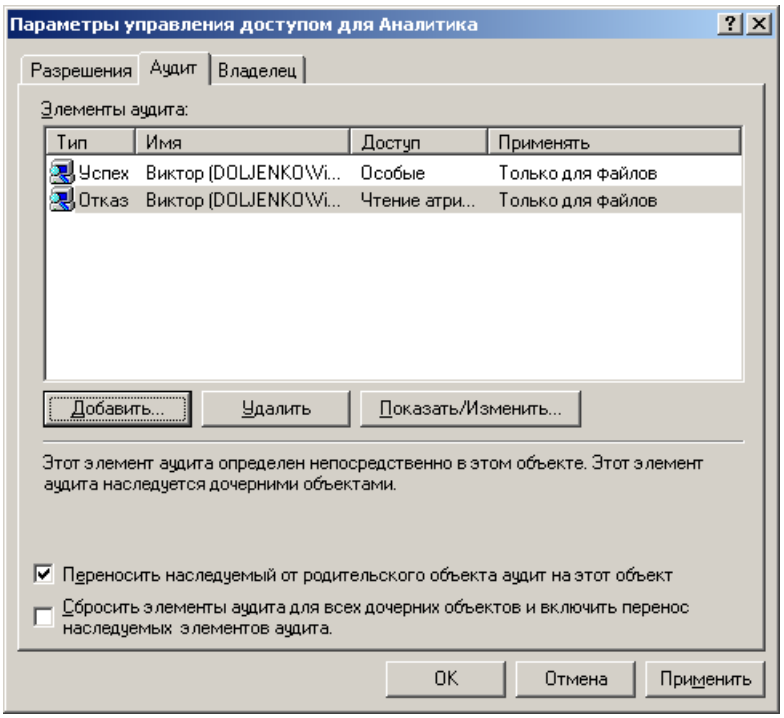

Рисунок 5.11 - Окно **Параметры управления доступом**

5. Если вы хотите просмотреть или изменить настройки аудита для уже существующего пользователя или группы, нажмите кнопку Показать/Изменить (View/Edit). 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.

Область действия настроек аудита

Настройка аудита выполняется с помощью окна диалога **Элемент аудита для**, где с помощью поля **Применять** можно определить область распространения настроек аудита. Результирующее действие значения, введенного в этом поле, зависит от того, установлен ли флажок **Применять этот аудит к объектам и контейнерам только внутри этого контейнера**. По умолчанию этот флажок снят. В табл. 5.1 и 5.2 показано, как настройки аудита действуют в случае, когда этот флажок соответственно снят и установлен.

Таблица 5.1 - Действие настроек аудита при снятом флажке

Значения в поле Применять	Выполняется аудит текущей папки	Выполняется аудит дочерних папок текущей папки	Выполняется аудит файлов в текущей папке	Выполняется аудит всех дочерних папок	Выполняется аудит файлов во всех дочерних папках
Только для этой папки (This folder only)	X				
Для этой папки, ее под папок и файлов (The folder, subfolders and files)	X	X	X	X	X
Для этой папки и ее подпапок (This folder and subfold-ers)	X	X		X	
Для этой папки и ее файлов (This folder and files)	X		X		X
Только для подпапок и файлов (Subfolders and files only)		X	X	X	X
Только для подпапок (Subfolders only)		X		X	
Только для файлов (Files only)			X		X

Примечание: применять этот аудит к объектам и контейнерам только для этого контейнера

Таблица 5.2. Действие настроек аудита при установленном флажке

Значения в поле Применять	Выполняется аудит текущей папки	Выполняется аудит дочерних папок текущей папки	Выполняется аудит файлов в текущей папке	Выполняется аудит всех дочерних папок	Выполняется аудит файлов во всех дочерних папках
Только для этой папки (This folder only)	X				
Для этой папки, ее под папок и файлов (The folder, subfolders and files)	X	X	X		
Для этой папки и ее подпапок (This folder and subfolders)	X	X			
Для этой папки и ее файлов (This folder and files)	X		X		

Только для подпапок и файлов (Subfolders and files only)		X	X		
Только для подпапок (Subfolders only)		X			
Только для файлов (Files only)			X		

Примечание: Применять этот аудит к объектам и контейнерам только внутри этого контейнера

Просмотр журналов безопасности

Аудит системы фиксируется в журнале безопасности. Для просмотра журнала безопасности Запустите оснастку **Просмотр событий** и откройте папку Журнал безопасности (можно выполнить команду **Пуск/ Программы/ Администрирование/Просмотр событий.**) (см.рисунок 5.12). В журнале зафиксированы параметры событий, аудит которых осуществляется в системе.

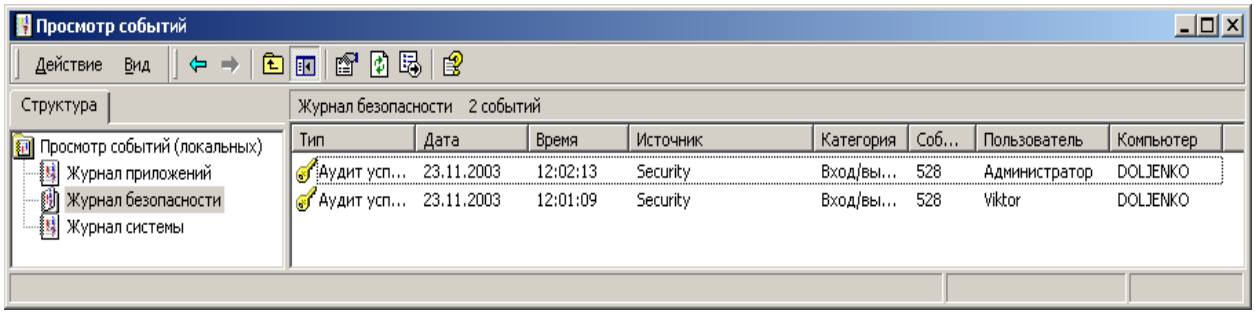

Рисунок 5.12 - Окно **Просмотр событий**

Для просмотра событий по папке, аудит которой проводится, необходимо:

1. Установить указатель мыши на файл или папку, для которой проводится аудит, и нажать правую кнопку. В появившемся контекстном меню выберите команду **Свойства** .

В окне свойств папки или файла перейдите на вкладку **Безопасность** (Security). На вкладке **Безопасность** нажмите кнопку **Дополнительно** (Advanced) и перейдите на вкладку Аудит (см.рисунок 5.13).

В таблице **Элементы аудита** окна **Параметры управления доступом** зафиксированы события осуществляемые с папкой Аналитика.

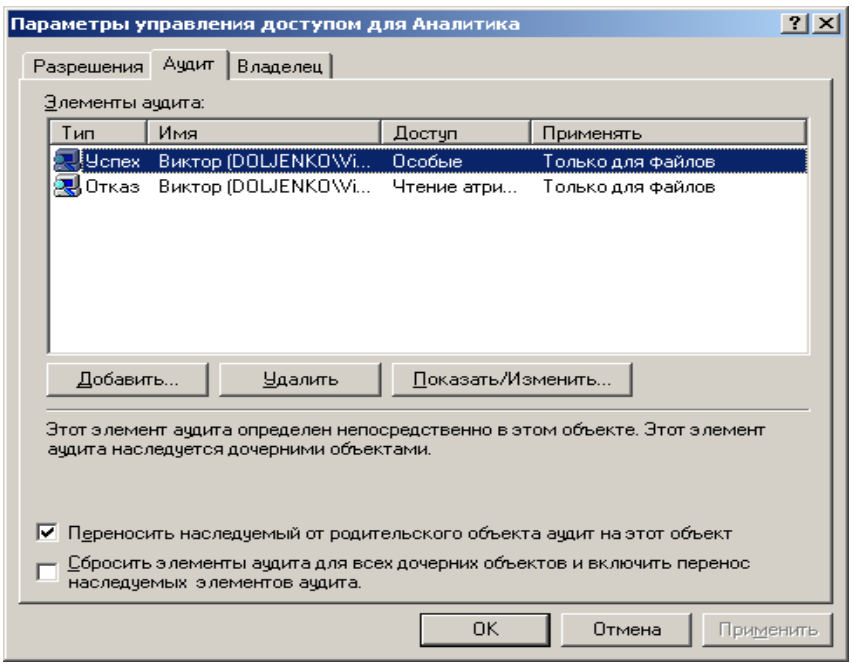

Рисунок 5.13 – Окно **Параметры управления доступом**

Отключение аудита файлов и папок

Для отключения аудита файла или папки:

1. Установите указатель мыши на файл или папку, где необходимо отключить аудит, и нажмите правую кнопку. В появившемся меню выберите команду **Свойства**. Появится окно свойств файла или папки Перейдите на вкладку **Безопасность** (см. рисунок 5.7).
2. На вкладке **Безопасность** нажмите кнопку **Дополнительно**. В появившемся окне диалога выберите вкладку **Аудит (**см.рисунок 5.11**).**
3. В поле Элементы аудита выберите нужную запись и нажмите кнопку **Удалить**. Соответствующая запись будет удалена.

Если кнопка Удалить недоступна, это значит, что настройки аудита наследуются от родительской папки

Задание на лабораторную работу

1. Создать три учетные записи. Учетные записи включить в две группы
2. Для системы установить аудит входа в систему и аудит событий входа в систему.
3. Для каждого пользователя и группы 1 установить аудит для двух папок (создать две любые папки по усмотрению обучающегося).
4. Для пользователей провести регистрацию в системе
5. Для каждого пользователя выполнить ряд манипуляций с созданной папкой (например создать в папке файл).
6. Просмотреть журнал безопасности системы.
7. Просмотреть параметры доступа для папки, аудит которой проводится

8. Отменить аудит одной из папок, отменить аудит для группы 1 и установить аудит для группы 2.
9. Выполнить ряд манипуляций с папками, дл которых установлен аудит.
10. Продемонстрировать выполненную работу преподавателю.
11. Просмотреть журнал безопасности системы.
12. Просмотреть параметры доступа для папки, аудит которой проводится
13. Отключить аудит системы и папок, удалить созданные папки и учетные записи пользователей.

Лабораторная работа 6
Управление общими дисковыми ресурсами

Цель лабораторной работы: Освоить технологию управления общими дисковыми ресурсами в Windows, использование средства «Автономные файлы» и процессы синхронизации автономных папок и общего ресурса.

Общие сведения

Локальное и удаленное администрирование общих ресурсов в Windows осуществляется с помощью оснастки **Общие папки** (Shared Folders).

Она входит в стандартный инструмент администрирования – **Управление компьютером** (Computer Management). Рассмотрим, как с помощью оснастки **Общие папки** можно создать общий ресурс.

Для запуска изолированной оснастки **Общие папки** как самостоятельного инструмента:

1. Нажмите кнопку **Пуск** (Start), выберите команду **Выполнить** (Run), введите с клавиатуры ***mmc*** и нажмите кнопку **ОК.**

2. В появившемся окне в меню **Консоль** (Console) выберите команду **Добавить/удалить оснастку** (Add/Remove Snap-in).

3. В следующем окне нажмите кнопку **Добавить** (Add).

4. В окне **Добавить изолированную оснастку** (Add Stand-alone Snap-in) выделите оснастку **Общие папки** и нажмите кнопку **Добавить.**

5. В окне **Общие папки (**см.рисунок 6.1**)** в группе **Эта оснастка всегда управляет** (This snap-in will always manage) выберите положение переключателя **локальным компьютером** (Local Computer) или **другом компьютером** (Another Computer), если вы хотите работать с другим компьютером сети. В последнем случае в поле ввода следует указать имя компьютера (или можно воспользоваться кнопкой **Обзор** (Browse)). В группе параметров **Просмотр** (View) укажите, какую информацию (общие ресурсы, сеансы, открытые файлы или все перечисленное) можно будет просматривать с помощью оснастки.

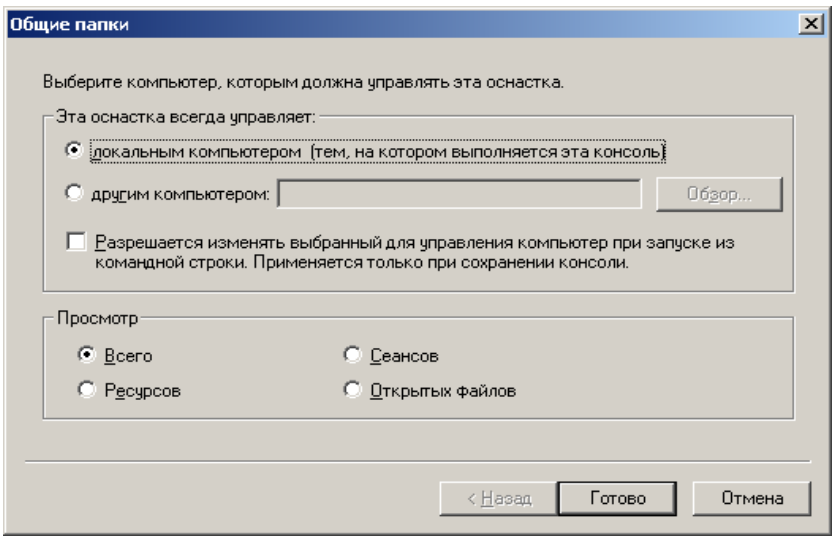

Рисунок 6.1 Окно Общие папки

6. Нажмите кнопку **Готово** (Finish).

7. В окне **Добавить изолированную оснастку** нажмите кнопку **Закрыть** (Close).

8. В окне **Добавить/удалить оснастку** нажмите кнопку ОК — окно будет закрыто. Пример окна оснастки **Общие папки** для локального компьютера показан на рисунке 6.2.

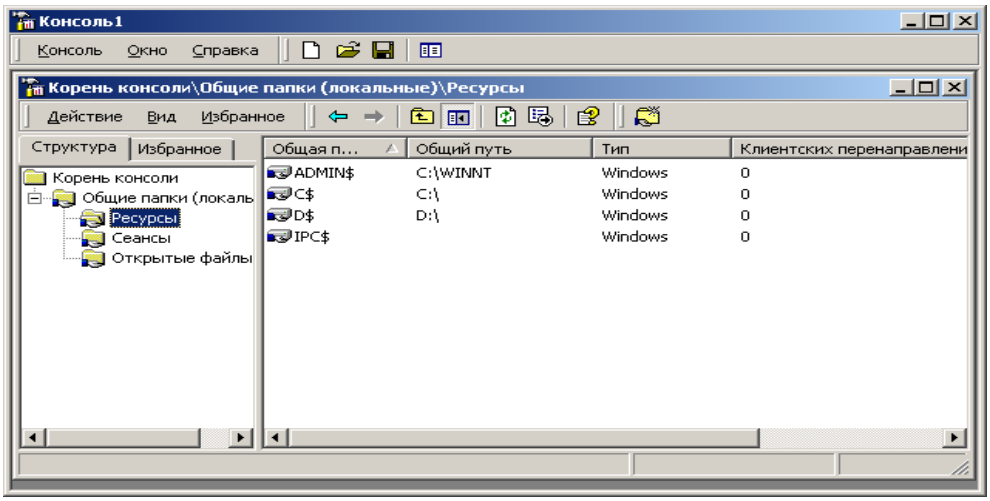

Рисунок 6.2 – Окно оснастки Общие папки

Для создания общего ресурса:

1. В окне структуры оснастки **Общие папки** установите указатель мыши на папку **Ресурсы** (Shares) и нажмите правую кнопку.

2. В появившемся контекстном меню выберите команду **Новый общий файл** (New File Share).

3. В полях ввода окна **Создание общей папки** (Create Shared Folder), показанных на рисунке 6.3, следует указать имя каталога (это может быть уже существующий каталог или вновь создаваемый), который должен стать общим ресурсом, сетевое имя общего ресурса и описание общего ресурса. Имена каталога и общего ресурса являются обязательными для ввода. Существующий каталог можно выбрать с помощью кнопки **Обзор.** Нажмите кнопку Далее (Next).

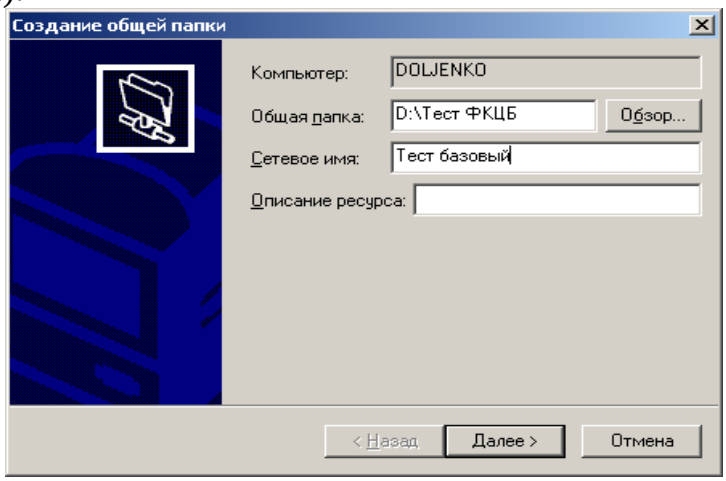

Рисунок 6.3 Окно диалога программы создания общих ресурсов

4. Появится окно (см.рисунок 6.4), в котором можно выбрать разрешения доступа к создаваемому общему ресурсу (по умолчанию — доступ для всех пользователей разрешен). Выполните все необходимые настройки и нажмите кнопку **Готово.** В появившемся окне нажмите кнопку **Да**, если необходимо создать еще один общий ресурс, или Нет – для возврата в основное меню оснастки **Общие папки.**

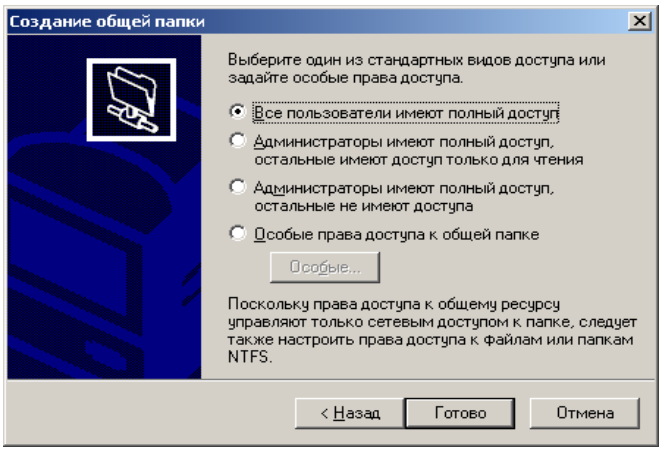

Рисунок 6.4. Настройка разрешений доступа к создаваемому общему ресурсу

Примечание. Рекомендуется на уровне прав доступа к общему ресурсу задавать наиболее *"широкие"* права (если позволяют требования безопасности — полный доступ для всех), а затем настраивать более *"узкие"* права доступа к файлам и папкам на уровне файловой системы NTFS. Такой подход упрощает администрирование прав пользователей.

Хотя Windows и поддерживает файловую систему FAT, для более высокой безопасности, надежности и легкости в администрировании, рекомендуется использовать файловую систему NTFS. Посмотреть, какая файловая система используется в настоящий момент, можно в окне свойств диска или с помощью оснастки **Управление дисками** (Disk Management).

Свойства уже созданного общего ресурса могут быть модифицированы следующим образом

1. Установите указатель мыши на общий ресурс, свойства которого вы хотите модифицировать, и нажмите правую кнопку (см. рисунок 6.5).

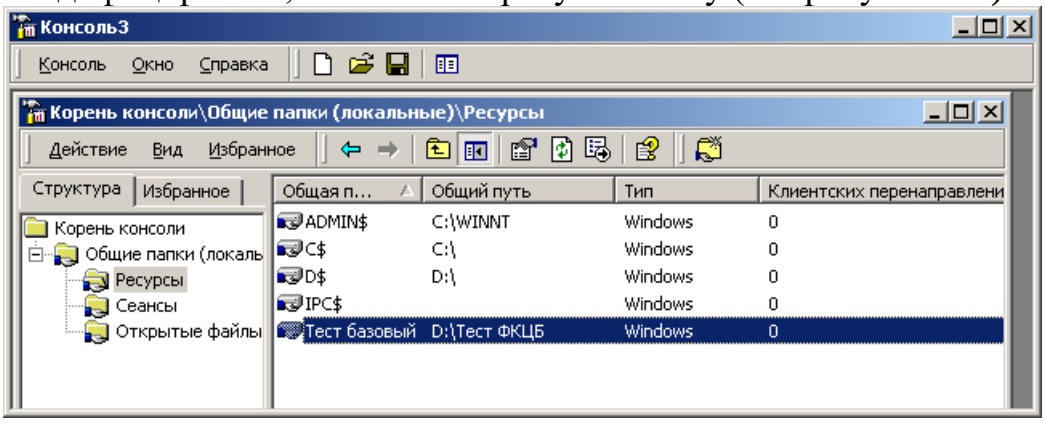

Рисунок 6.5 – Окно **Консоль 3** с общими ресурсами

2. В появившемся контекстном меню выберите команду **Свойства** (Properties). Появится окно свойств общего ресурса (см. рисунок 6.6), в котором можно менять его существующие параметры.

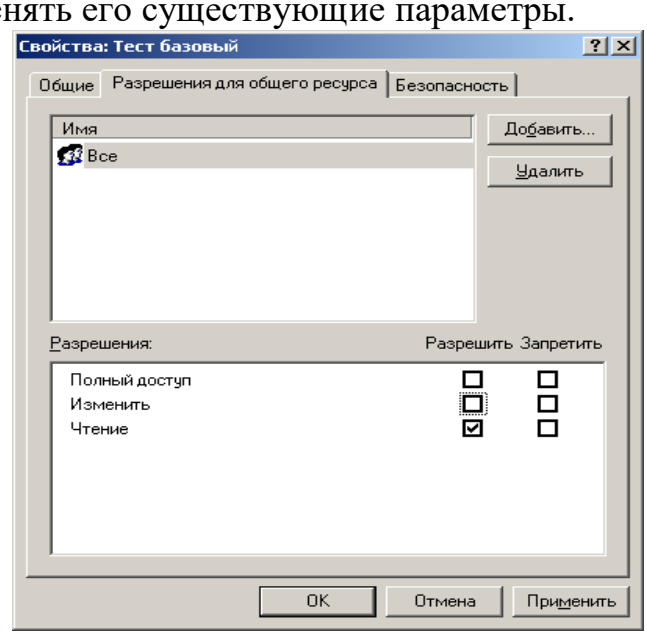

Рисунок 6.6 – Окно свойств общего ресурса

Автономные файлы

Операционная система Windows располагает средством ***Автономные файлы*** (Offline Files), позволяющим работать с документами, находящимися в общем каталоге, в условиях отсутствия соединения с сетью. С помощью этого средства пользователи могут открывать и корректировать файлы, находящиеся в общих папках, даже отключившись от сети.

При отключении от сети автономные файлы извещают об этом пользователя. В панели задач появляется специальный значок, а на рабочем столе – сообщение, сигнализирующее о том, что сетевое соединение исчезло, и началась автономная работа. При конфигурировании автономных файлов пользователь может сам выбрать, как они должны реагировать на отключение от сети. После подключения к сети *Диспетчер синхронизации* (Synchronization Manager) переносит все изменения, сделанные пользователем в сетевых файлах в процессе автономной работы, на общий сетевой ресурс.

При автономной работе, не имея соединения с сетью, пользователь не теряет способности просматривать сетевые устройства и работать со своими файлами. На значках отключенных сетевых общих ресурсов появляется красный крестик. Просматривая эти ресурсы, пользователи смогут увидеть только те файлы, которые были заранее указаны или которые были открыты ими недавно, до разрыва соединения.

Права доступа в автономном режиме работы остаются такими же, какие они были при наличии соединения с сетью. Например, документ,

доступный на сетевом общем ресурсе только для чтения, будет доступен только для чтения и при автономной работе.

Для того чтобы сделать доступными для пользователей, отключенных от сети, файлы общих ресурсов, нужно поместить их в кэш компьютера. Кэш компьютера – это часть пространства диска, доступ к которому возможен в любом состоянии соединения с сетью. Автономные файлы позволяют применять три варианта кэширования (это задается на вкладке **Доступ** (Sharing) в окне свойств общего ресурса — кнопка **Кэширование** (Caching)):

1. *Ручное* кэширование для документов (Manual Caching for Documents)
2. *Автоматическое* кэширование для документов (Automatic Caching for Documents)
3. Автоматическое кэширование для *программ* (Automatic Caching for Programs)

Ручное кэширование для документов

Ручное кэширование предполагает, что, отключившись от сети, пользователь сможет открывать только те файлы общего сетевого ресурса, которые он *предварительно указал.* Такой тип кэширования идеален для работы с общим ресурсом, на котором находятся документы или рисунки. Этот вариант кэширования устанавливается по умолчанию.

Автоматическое кэширование для документов

Автоматическое кэширование позволяет данному пользователю работать автономно с теми файлами, которые он *открывал* на общем сетевом ресурсе. Нет гарантии, что для автономной работы будут доступны *все* файлы, находящиеся в общей папке.

Автоматическое кэширование для программ

Автоматическое кэширование для программ позволяет автономно работать только с теми программами, которые пользователь *запускал,* работая в сети, из общей папки. Рекомендуется для работы с ресурсами, доступными только для чтения.

Настройка компьютера для работы с автономными папками

Для создания автономных папок на компьютере:

1. В окне Проводника или в окне **Мой компьютер** (My Computer) в меню **Сервис** (Tools) выберите команду **Свойства папки** (Folder Options).

2. В появившемся окне перейдите на вкладку **Автономные файлы** (Offline Files) (рис 6.6) и установите флажок **Использовать автономные файлы** (Enable Offline Files).

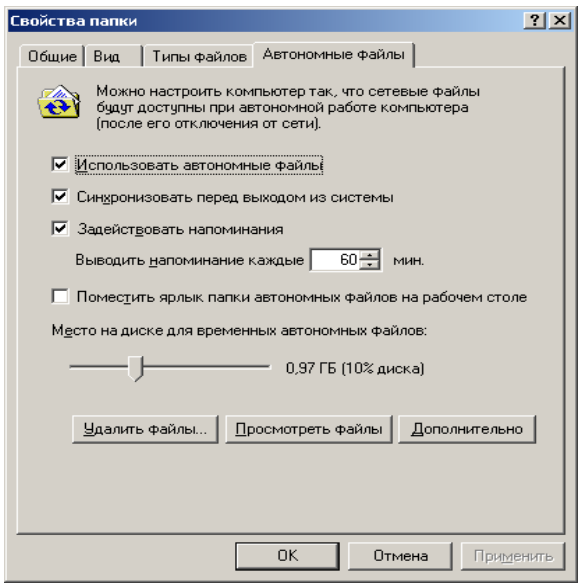

Рисунок 6.6 – Вкладка Автономные файлы (Offline Files) окна Свойства папки(Folder Options)

3. Установив или сняв флажок **Синхронизировать перед выходом из системы** (Synchronize all offline files before logging off), можно указать на необходимость осуществления синхронизации при выходе

По умолчанию в Windows Professional флажок **Использовать автономные файлы** установлен. После настройки компьютера для работы с автономными папками следует указать конкретные файлы и папки, с которыми необходимо работать автономно. Для выполнения быстрой синхронизации нужно сформировать расписание диспетчера синхронизации, который осуществляет синхронизацию файлов и папок перед завершением работы компьютера.

Для просмотра списка сетевых файлов и папок, с которыми можно работать автономно, следует нажать кнопку **Просмотреть файлы** (View Files) на вкладке **Автономные файлы.**

Выбор файлов для автономной работы

Для того чтобы обозначить, с какими файлами и папками необходимо работать автономно:

1. Щелкните на значке **Мой компьютер или Мое сетевое окружение** (My Network Places). В появившемся окне выделите файлы, находящиеся на сетевых устройствах, с которыми будет выполняться автономная работа.

2. В контекстном меню выберите команду **Сделать доступным в автономном режиме** (Make Available Offline) — запустится Мастер автономных файлов Следуйте указаниям этой программы. После ввода всей необходимой для создания автономных файлов информации начнется процесс синхронизации. Появится окно синхронизации. Когда оно закроется, указанные файлы и папки будут доступны для автономной работы.

Доступные для автономной работы файлы и папки можно изменять после отключения от сети. Команда **Сделать доступным в автономном режиме** доступна в меню **Файл** только после того, как на вкладке **Автономные файлы** установлен флажок **Использовать автономные файлы.**

Настройка реакции автономных файлов на отключение компьютера от сети

Чтобы определить, как автономные папки будут реагировать на отключение от сети:

1. В окне Проводника или в окне **Мой компьютер** в меню **Сервис** выберите команду **Параметры папки.**

2. В появившемся окне диалога на вкладке **Автономные файлы** нажмите кнопку **Дополнительно.**

3. Появится окно Автономные файлы — дополнительная настройка (Offline Files — Advanced Settings) (см.рисунок 6.7). С его помощью можно настроить реакцию компьютера на потерю сетевого соединения, для чего в группе **Когда теряется сетевое подключение** (When a network connection is lost) следует установить соответствующий переключатель.

4. В поле **Список исключений** (Exception list) можно определить список компьютеров, при потере соединения с которыми должны выполняться индивидуальные настройки реакции автономных файлов. Добавить компьютер в список исключений можно, нажав кнопку **Добавить.** В появившемся диалоговом окне следует указать имя компьютера, обладающего индивидуальными настройками реакции автономных папок, и действие при отключении от сети.

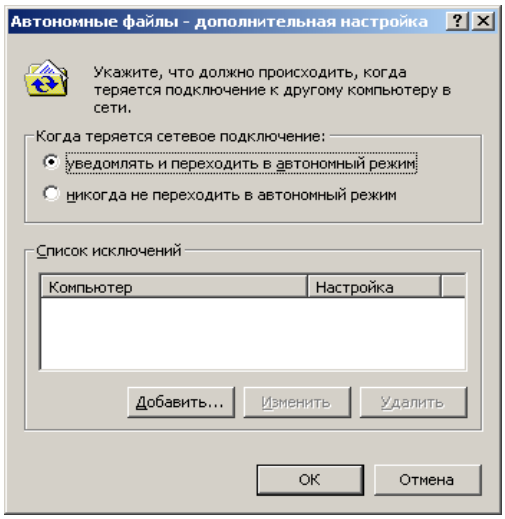

Рисунок 6.7. Окно диалога, предназначенное для настройки реакции автономных файлов на отключение от сети

Синхронизация информации автономных папок и общего ресурса

Поскольку отключение компьютера от сети дает возможность пользователю продолжать корректировать свои файлы в автономных папках,

а все пользователи, компьютеры которых не потеряли соединения с сетью, продолжают работать с файлами общего ресурса сети, содержимое одних и тех же файлов становится различным. Поэтому после восстановления соединения с сетью необходимо выполнить синхронизацию автономных папок и общего сетевого ресурса. Синхронизация информации может быть выполнена тремя способами:

-Принудительная синхронизация

- Синхронизация в процессе регистрации на компьютере или завершения работы компьютера

- Синхронизация в момент бездействия компьютера.

Для принудительной синхронизации:

1. Запустите диспетчер синхронизации. Для этого в меню **Сервис** следует выбрать команду **Синхронизировать** (Synchronize).

2. Установите флажки, соответствующие автономным файлам, которые следует синхронизировать (см. рисунок 6.8).

3. Нажмите кнопку **Синхронизация.** В процессе синхронизации возможны конфликты версий одноименных файлов, располагающихся на локальном компьютере и на общем ресурсе. При этом система выдает сообщения, содержащие информацию о времени корректировки каждого из файлов и запрос на последующие действия. В этих случаях пользователь может выбрать одну из трех возможностей:

- Оставить только ту копию файла, которая хранится на локальном компьютере.

- Оставить только ту копию файла, которая находится на общем ресурсе.

- Сохранить более позднюю версию файла под новым именем (по умолчанию- к имени файла добавляется имя компьютера, откуда берется эта версия).

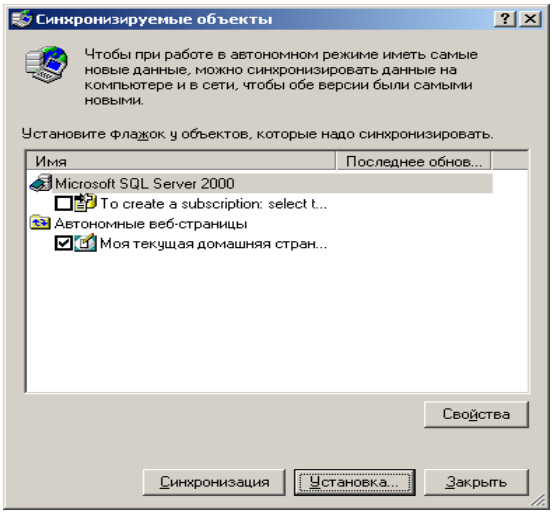

Рисунок 6.8 – Выбор синхронизируемых папок и файлов

При возникновении конфликтов пользователь может обрабатывать каждую ситуацию *отдельно, а* может указать *общее* действие (из трех перечисленных выше возможностей) для всех дублирующихся имен.

Для установки синхронизации автономных папок при входе в систему или выходе из системы:

1. Запустите диспетчер синхронизации и нажмите кнопку **Установка** (Setup). Появится окно диалога **Параметры синхронизации** (Synchronization Settings) (см. рисунок 6.9).

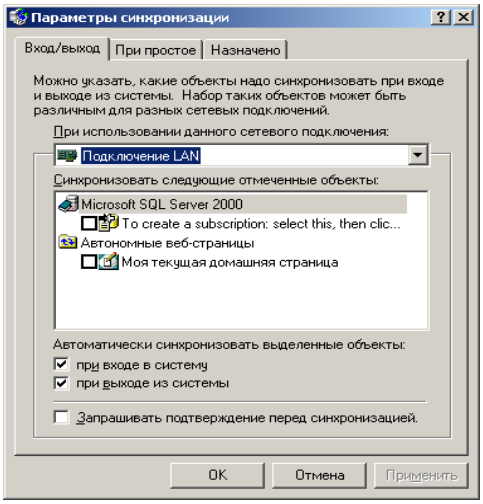

Рисунок 6.9. Настройка параметров синхронизации

2. Перейдите на вкладку **Вход/выход** (Logon/Logoff). В поле **При использовании данного сетевого подключения** (When I am using this network connection) выберите сетевое соединение, которое вы хотите использовать.

3. В поле **Синхронизовать следующие отмеченные объекты** (Synchronize the following checked items) установите флажки, соответствующие синхронизируемым объектам.

4. В поле **Автоматически синхронизовать выделенные объекты** (Automatically synchronize the selected items) выберите положение переключателя **при входе в систему** (When I log on to my computer) или **при выходе из системы** (When I log off my computer) — если вы хотите синхронизировать информацию по завершению работы с системой.

5. Если вы хотите, чтобы диспетчер синхронизации запрашивал у вас разрешения на автоматическую синхронизацию, установите флажок **Запрашивать подтверждение перед синхронизацией** (Ask me before synchronizing the items)

6. После установки параметров закройте окно диспетчера синхронизации Для синхронизации информации автономных папок в момент бездействия компьютера нужно в окне **Параметры синхронизации** перейти на вкладку **При простое** (On Idle), выбрать нужное сетевое подключение и установить флажки около синхронизируемых файлов. По умолчанию синхронизация отмеченных файлов начинается, если компьютер не используется 15 минут, и повторяется каждый час.

Задание на лабораторную работу

1. Изучить теоретический материал.
2. С помощью оснастки **Общие папки** создать папку общего использования.
3. В созданной папке сформировать общий ресурс - задать каталог и файл, который должен стать общим ресурсом.
4. Задать для общего ресурса вид доступа и права доступа.
5. Создать автономную папку режим синхронизации.
6. Создать файл для автономной работы.
7. Установить режим синхронизации папки и файлов.
8. Продемонстрировать результаты выполненной работы преподавателю.

Лабораторная работа 7
Средства мониторинга и оптимизации. Диспетчер задач

Цель работы: Получить навыки работы с «Диспетчером задач» операционной системы Windows для анализа информации о программах и процессах, запущенных на компьютере, а также анализа общих показателей производительности процессов.

Общие сведения

Для мониторинга и оптимизации работы компьютера в системе Windows доступны следующие три инструмента:

1. Производительность (Performance) — обновленный инструмент в системе Windows. Оснастка Производительность включает в себя две оснастки: **System Monitor** и **Оповещения и журналы** безопасности (Performance Logs and Alerts). Графические средства **System Monitor** позволяют визуально отслеживать изменение производительности системы. С помощью **System Monitor** можно одновременно просматривать данные с нескольких компьютеров в виде динамических диаграмм, на которых отображается текущее состояние системы и показания счетчиков. Оснастка **Оповещения и журналы безопасности** позволяет создавать отчеты на основе текущих данных производительности или информации из журналов. При превышении счетчиками заданного значения или уменьшения ниже указанного уровня данная оснастка посредством службы сообщений (Messenger) посылает оповещения пользователю.

2. Диспетчер задач (Task Manager) служит для просмотра текущих данных о производительности системы. В этой утилите основными являются три индикатора: использование процессора, использование виртуальной памяти и запущенные процессы и программы.

3. Оснастка Просмотр событий (Event Viewer) позволяет просматривать журналы событий, генерируемых приложениями, службой безопасности и системой.

Диспетчер задач (Task Manager)

В системе Windows средством мониторинга производительности является ***Диспетчер задач***, который предоставляет информацию о программах и процессах, запущенных на компьютере, и отображает наиболее общие показатели производительности процессов.

Диспетчер задач можно использовать для отслеживания ключевых индикаторов производительности вашего компьютера. Вы можете быстро отслеживать статус запущенных программ и завершать приложения, которые перестали отвечать на запросы системы. С помощью диспетчера задач можно

отслеживать активность запущенных процессов по 15 параметрам и просматривать графики использования процессора и памяти.

Запуск диспетчера задач

Для запуска диспетчера задач можно выбрать один из следующих методов:

Щелкнуть правой кнопкой мыши на свободном пространстве панели задач и выбрать в контекстном меню пункт **Диспетчер задач**.

Нажать комбинацию клавиш <Ctrl>+<Alt>+<Del> и нажать в появляющемся окне кнопку **Диспетчер задач**. Вызвать команду **Выполнить** (Run) и ввести ***taskmgr***. Если диспетчер задач запущен, то в правой части панели задач (на *systray)* появляется индикатор загрузки процессора. Если подвести указатель мыши к этому индикатору, то будет показана степень загруженности процессора в процентах. Окно диспетчера задач можно открыть двойным щелчком на значке индикатора загрузки на панели задач. Если вы не хотите, чтобы свернутое окно диспетчера оставалось на панели задач среди других запущенных программ, то в окне диспетчера в меню **Параметры** (Options) установите флажок **Скрывать свернутое** (Hide When Minimized).

Мониторинг процессов

Для просмотра запущенных процессов и показателей их производительности выберите вкладку **Процессы** (Processes) в окне **Диспетчер задач** Windows (см.рисунок 7.1). Таблица процессов содержит все процессы, запущенные в собственном адресном пространстве, включая все приложения и системные сервисы. Если требуется просмотреть 16-разрядные процессы, то в меню **Параметры** выберите команду **Отображать 16-разрядные задачи** (Show 16-bit tasks).С помощью команды **Выбрать столбцы** (Select Columns) меню **Вид** (View) можно добавить на экран новые столбцы показателей. В открывшемся диалоговом окне **Выбор столбцов** установите флажки рядом с теми показателями, которые должны быть отображены в таблице. В табл. 6.1 кратко описаны основные столбцы таблицы и соответствующие им счетчики.

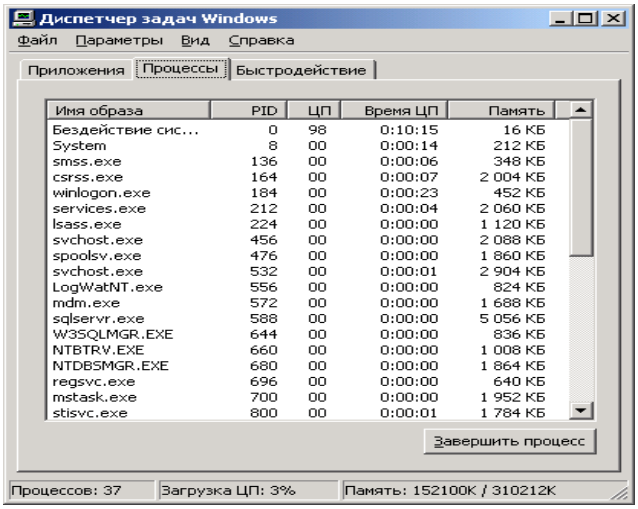

Рисунок 7.1 – Вкладка Процессы (Processes) в окне диспетчера задач

Таблица 7.1– Основные счетчики диспетчера задач

Счетчик	Описание
Имя образа (Image Name)	Имя процесса
Идентификатор процесса (PID) (Process Identifier)	Числовое значение, которое уникальным образом определяет процесс во время его работы
Загрузка ЦП (CPU Usage)	Выраженное в процентах время, в течение которого процесс использовал время процессора с момента последнего обновления
Время ЦП (CPU Time)	Суммарное время процессора, использованное процессом со времени его запуска (в секундах)
Память— использование (Memory Usage)	Объем виртуальной памяти, используемой процессом (в килобайтах)
Память— изменение (Memory Usage Delta)	Изменение объема памяти с момента последнего обновления. Диспетчер задач отображает отрицательные значения
Память— максимум (Peak Memory Usage)	Максимальный объем выделенной памяти, использованной процессом с момента запуска. Выделенной памятью является память, которую процесс использует на физическом носителе (например, в ОЗУ) или в файле подкачки
Ошибки страницы (Page Faults)	Число прерываний, которые возникают, когда приложение пытается прочитать или записать данные в несуществующую виртуальную память
Объекты USER (USER Objects)	Число объектов USER, которые используются в данное время определенным процессом
Число чтений (I/O Reads)	Число операций ввода/вывода, сгенерированных процессом чтения, включая операции для файлов, сети и устройств
Прочитано байт (I/O Read Bytes)	Число байт, прочитанных в ходе операций ввода/вывода, сгенерированных процессом чтения, включая операции для файлов, сети и устройств
Ошибки страницы— изменение (Page Faults Delta)	Изменение числа ошибок страниц с момента последнего обновления

Объем виртуальной памяти (Virtual Memory Size)	Объем виртуальной памяти или адресного пространства, выделенного процессу
Выгружаемый пул (Paged Pool)	Виртуальная память, доступная для кэширования на диск, которая включает в себя всю пользовательскую память и часть системной памяти. Кэширование представляет собой перемещение редко используемых компонентов рабочей памяти из ОЗУ на другой носитель, обычно на жесткий диск
Невыгружаемый пул (Non-Paged Pool)	Объем памяти операционной системы, используемой процессом (в килобайтах). Данная память никогда не выгружается на диск
Базовый приоритет (Base Priority)	Определяет порядок диспетчеризации потоков процесса для обработки процессором. В Службах очереди сообщений (Microsoft Message Queuing Services, MSMQ) базовый приоритет (или приоритет очереди) определяет proxy-приоритет очереди в общей очереди Базовый приоритет может быть установлен в диапазоне от -32 768 до 32 767 (значение по умолчанию равно 0) любым приложением MSMQ с разрешениями на запись для очереди. Частные очереди не поддерживают базовый приоритет. MSMQ маршрутизирует и передает сообщения на основе комбинации базового приоритета и приоритета сообщения
Счетчик дескрипторов (Handle Count)	Число дескрипторов объектов в таблице объектов процесса
Счетчик потоков (Thread Count)	Число потоков, запущенных в процессе
Объекты GDI (GDI Objects)	Число объектов GDI, используемых в данный момент процессом. Объекты из библиотеки графического пользовательского интерфейса (Graphics Device Interface, GDI), входящей в интерфейс прикладного программирования (API) для устройств вывода графики
Число записей (I/O Writes)	Число операций ввода/вывода, сгенерированных процессом записи, включая операции для файлов, сети и устройств
Записано байт (I/O Write Bytes)	Число байт, записанных в ходе операций ввода/вывода, сгенерированных процессом записи, включая операции для файлов, сети и устройств
Прочий ввод/вывод (I/O Other)	Число операций ввода/вывода, сгенерированных процессом, который не является ни чтением, ни записью, включая операции для файлов, сети и устройств. Примером такого типа операции является функция управления
Прочих байт при вводе/выводе (I/O Other Bytes)	Число байт, переданных в ходе операций ввода/вывода, сгенерированных процессом, который не является ни чтением, ни записью, включая операции для файлов, сети и устройств

Изменение приоритета запущенной программы

Базовый приоритет задается, как правило, кодом приложения. С помощью диспетчера задач можно изменить базовый приоритет процесса. Внесенное изменение будет действительно только в течение времени работы процесса. При следующем запуске процесс будет выполняться с базовым значением приоритета. Для изменения приоритета процесса выделите имя процесса на вкладке **Процессы** и щелкните на нем правой кнопкой мыши. Затем в контекстном меню выберите пункт **Приоритет** (Set Priority) и укажите новый уровень приоритета (см.рисунок 7.2).

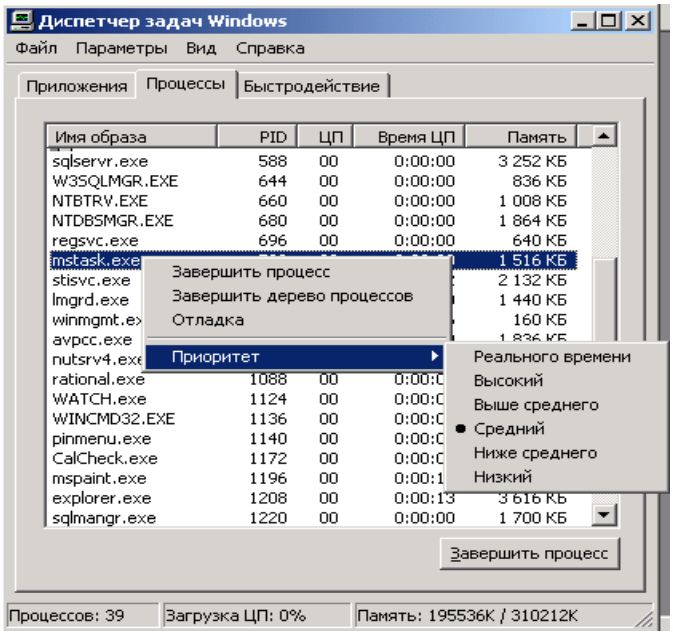

Рисунок 7.2 – Изменение базового приоритета процесса в диспетчере задач

Выбор процессора

В диспетчере задач можно назначить выполнение определенного процесса одному или нескольким процессорам. Для этого на вкладке **Процессы** щелкните правой кнопкой мыши на названии процессора, укажите пункт **Установить связь** (Set Affinity) и затем выберите один или несколько процессоров.

Скорость обновления

Вы можете регулировать скорость, с которой обновляются показания счетчиков в диспетчере задач. Это позволяет снизить процент использования ресурсов, но при этом данные могут оказаться слишком приближенными. Для выполнения принудительного обновления выберите команду **Обновить** (Refresh Now) меню **Вид** или нажмите клавишу <F5>.

В диспетчере задач можно задать следующие скорости обновления:

- высокая (High) – обновление проводится каждые полсекунды;

- обычная (Normal) – обновление выполняется каждую секунду;
- низкая (Low) – показания обновляются каждые 4 секунды;
- приостановить (Paused) – автоматическое обновление не производится.

Для запуска обновления нажмите клавишу <F5>

Мониторинг производительности системы

Для отслеживания производительности системы откройте вкладку **Быстродействие** (Performance) (см.рисунок 7.3.). Для вывода на экран числового значения (в процентах) процессорного времени, в течение которого процессор работал в режиме ядра, выберите команду **Вывод времени ядра** (Show Kernel Times) в меню **Вид**. Данное значение равно периоду времени, в течение которого приложения пользовались сервисами операционной системы. Остальную часть времени процессор работал в режиме пользователя, выполняя потоки в режиме работы приложений. Пользователи многопроцессорных систем могут выбрать команду **Загрузка ЦП** (CPU History) меню Вид, чтобы вывести график занятости для каждого процессора.

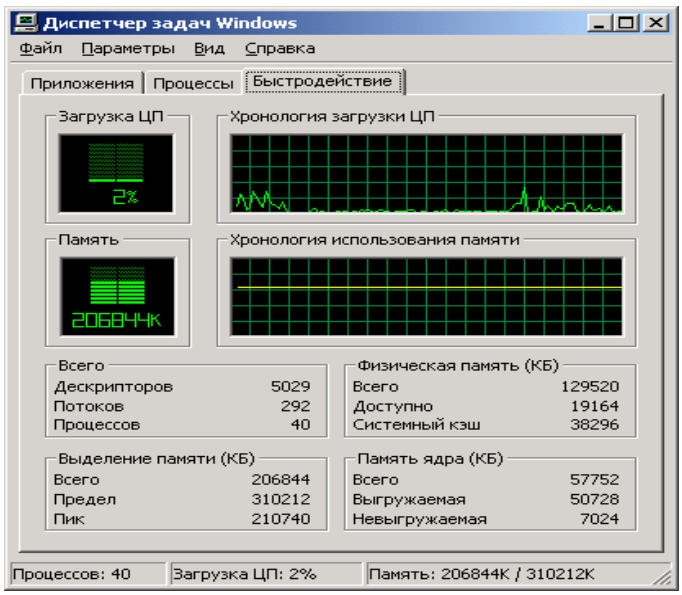

Рисунок 7.3 – Вкладка Быстродействие (Performance)

Задание на лабораторную работу

1. Изучить теоретический материал.
2. Запустите какое-либо приложение (текстовый редактор, графический редактор или что-либо другое).
3. Запустите диспетчер задач.
4. На вкладке «Приложения» просмотрите отображаемые приложения, которые запущены.
5. Перейдите на вкладку «Процессы»

6. Сделайте изменения в столбцах, которые появляются на странице процессов диспетчера задач.
7. Поясните Назначение установленных Вами столбцов страницы процессов диспетчера задач в соответствии с табл. 6.1.
8. Измените скорость обновления показаний счетчиков в диспетчере задач (по Вашему усмотрению).
9. Перейдите на вкладку «Быстродействие»
10. Установите режим «Вывод времени ядра».
11. Для активного клиентского приложения проведите несколько операций обработки информации.
12. Прокомментируйте результаты отображаемые на вкладке «Быстродействие» диспетчер задач
13. Продемонстрируйте сделанную работу преподавателю.

Список литературы

1. Башлы, П.Н. Информационная безопасность [Электронный ресурс]: учебное пособие/ Башлы П.Н., Бабаш А.В., Баранова Е.К.— Электрон. текстовые данные.— М.: Евразийский открытый институт, 2012.— 311 с.— Режим доступа: http://www.iprbookshop.ru/10677.— ЭБС «IPRbooks», по паролю
2. Аверченков, В.И. Организационная защита информации [Электронный ресурс]: учебное пособие/ Аверченков В.И., Рытов М.Ю.— Электрон. текстовые данные.— Брянск: БГТУ, 2012.— 184 с.— Режим доступа: http://www.iprbookshop.ru/7002.— ЭБС «IPRbooks», по паролю
3. Гафнер, В.В. Информационная безопасность [Текст] : учеб. пособие/ В.В. Гафнер.– Ростов н/Д.: Феникс, 2010.- 324 с.
4. Корнеев, И.К. Защита информации в офисе [Текст]: учеб. пособие/ И.К. Куприянов, Е.А. Степанов.- М.: ТК Велби, Проспект, 2010.- 336 с.
5. Куприянов, А.И. Основы защиты информации [Текст]: учеб. пособие для студ. высш. учеб. заведений/ А.И. Куприянов, А.В. Сахаров, В.А. Шевцов.- М.: Академия, 2008.- 256 с.
6. Мельников, В.П. Информационная безопасность и защита информации [Текст]: учеб. пособие для студ. высш. учеб. заведений/ В.П. Мельников, С.А. Клейменов, А.М. Петраков; под ред. С.А. Клейменова. – М.: Академия, 2008.- 336 с.
7. Титов, А.А. Инженерно-техническая защита информации [Электронный ресурс]: учебное пособие/ Титов А.А.— Электрон. текстовые данные.— Томск: Томский государственный университет систем управления и радиоэлектроники, 2010.— 197 с.— Режим доступа: http://www.iprbookshop.ru/13931.— ЭБС «IPRbooks», по паролю
8. Хорев, П.Б. Методы и средства защиты информации в компьютерных системах [Текст]: учеб. пособие для студ. высш. учеб. заведений/ П.Б. Хорев - М.: Академия, 2008.- 256 с.
9. Шаньгин, В.Ф. Защита компьютерной информации [Электронный ресурс]: учебное пособие/ Шаньгин В.Ф.— Электрон. текстовые

данные.— М.: ДМК Пресс, 2010.— 544 с.— Режим доступа: http://www.iprbookshop.ru/7943.— ЭБС «IPRbooks», по паролю

ТЕМИРОВА Лилия Гумаровна

ЗАЩИТА ИНФОРМАЦИИ В КОМПЬЮТЕРНЫХ СИСТЕМАХ

Практикум для обучающихся 4 курса
по специальности 01.03.04 Прикладная математика

Печатается в редакции автора

Корректор Темирлиева Р.М.
Редактор Темирлиева Р.М.

Сдано в набор 17.01 2098 г.
Формат 60х84/16
Бумага офсетная.
Печать офсетная.
Усл. печ. л. 3,7
Заказ № 3588
Тираж 100 экз.

Оригинал-макет подготовлен
в Библиотечно-издательском центре СКГА
369000, г. Черкесск, ул. Ставропольская, 36