

Учреждение образования  
«Белорусский государственный университет культуры и искусств»  
Факультет культурологии и социокультурной деятельности  
Кафедра информационных технологий в культуре

СОГЛАСОВАНО  
Заведующий кафедрой

СОГЛАСОВАНО  
Декан факультета

\_\_\_\_\_ Т. С. Жилинская  
«\_\_» \_\_\_\_\_ 2020 г.

\_\_\_\_\_ И. Н. Воронович  
«\_\_» \_\_\_\_\_ 2020 г.

УЧЕБНО-МЕТОДИЧЕСКИЙ КОМПЛЕКС  
ПО УЧЕБНОЙ ДИСЦИПЛИНЕ

ПРОГРАММНО-ТЕХНИЧЕСКИЕ СРЕДСТВА

**Раздел 3. СИСТЕМНОЕ ПРОГРАММНОЕ ОБЕСПЕЧЕНИЕ**

по специальности 1-21 04 01 Культурология (по направлениям),  
направление специальности 1-21 04 01-02 Культурология (прикладная),  
специализация 1-21 04 01-02 04 Информационные системы в культуре

1 семестр обучения

Составители:

П. В. Гляков, профессор кафедры информационных технологий в культуре учреждения образования «Белорусский государственный университет культуры и искусств»;

А. К. Демидович, доцент кафедры информационных технологий в культуре учреждения образования «Белорусский государственный университет культуры и искусств»

Рассмотрено и утверждено

на заседании Совета университета 28.01.2020

протокол № 5.

Составители:

Гляков П. В., профессор кафедры информационных технологий в культуре учреждения образования «Белорусский государственный университет культуры и искусств», кандидат физико-математических наук, доцент;

Демидович А. К., доцент кафедры информационных технологий в культуре учреждения образования «Белорусский государственный университет культуры и искусств», кандидат физико-математических наук, доцент

Рецензенты:

*Кафедра* дискретной математики и алгоритмики факультета прикладной математики и информатики Белорусского государственного университета;

*С. А. Гончарова*, доцент кафедры информационных технологий в культуре учреждения образования «Белорусский государственный университет культуры и искусств», кандидат технических наук, доцент

Рассмотрено и рекомендовано к утверждению:

Кафедрой информационных технологий в культуре (протокол от 25.09.2019 г., № 2);

Советом факультета культурологии и социокультурной деятельности (протокол от 27.01.2020 г., № 6)

## Оглавление

1 ПОЯСНИТЕЛЬНАЯ ЗАПИСКА.....	4
2 ТЕОРЕТИЧЕСКИЙ РАЗДЕЛ.....	7
2.1 Учебные издания.....	7
2.2 Конспект лекций.....	7
2.2.1 Темы лекций.....	7
Лекция 1. Принципы организации и функционирования вычислительных систем.....	7
Лекция 2. Этапы развития вычислительных систем.....	7
Лекция 3. Аппаратное обеспечение настольного персонального компьютера.....	8
Лекция 4. Операционные системы и их функции.....	8
Лекция 5. Системы хранения данных, файловые системы операционных систем.....	8
Лекция 6. Инструменты и утилиты конфигурирования операционных систем Windows.....	9
Лекция 7. Системный реестр как иерархическая база данных конфигурации системы Windows.....	9
Лекция 8. Установка операционной системы и обслуживание персонального компьютера.....	9
Лекция 9. Основы администрирования операционных систем Windows.....	10
2.2.2 Материалы лекций.....	10
3 ПРАКТИЧЕСКИЙ РАЗДЕЛ.....	60
3.1 Описание лабораторных работ.....	60
Лабораторная работа 1 Интерфейс командной строки и ее команды (4 ч.)..	60
Лабораторная работа 2 Запуск программы или команды в отдельном окне ..	63
Лабораторная работа 3 Командный процессор и интерпретатор команд.....	65
Лабораторная работа 4 Служебные утилиты командной строки (4 ч.).....	71
Лабораторная работа 5 Аппаратно-программное обеспечение персонального компьютера (4 ч.).....	87
Лабораторная работа 6 Администрирование персонального компьютера.....	88
3.2 Тематика семинарских занятий.....	88
3.3 Тематика практических работ.....	88
4 РАЗДЕЛ КОНТРОЛЯ ЗНАНИЙ.....	90
4.1 Контрольные вопросы.....	90
4.2 Перечень вопросов к экзамену.....	90
4.3 Критерии оценки результатов учебной деятельности студентов.....	92
4.4 Учебная программа.....	92
4.5 Список основной литературы.....	92
4.6 Список дополнительной литературы.....	93

## 1 ПОЯСНИТЕЛЬНАЯ ЗАПИСКА

Массовое распространение настольных персональных компьютеров, переносных сенсорных и мобильных устройств, их участие в локальных сетевых и глобальных сетевых коммуникациях, использование в качестве инструмента платежных систем, применение различных систем хранения данных, поддержка графических процессоров и обеспечение безопасности требуют от рядового пользователя все больших знаний и умений в области аппаратуры и программного обеспечения вычислительных устройств, системного программного обеспечения для поддержки их работоспособности. Работоспособность может рассматриваться локально, без поддержки сетей, с поддержкой локальной сети с выходом в глобальную сеть. На уровне глобальной сети могут рассматриваться вопросы взаимодействия с базовыми службами интернета, сервисами и ресурсами облачных технологий, настройкой обновлений, синхронизацией данных.

*Цель* изучения данной дисциплины – формирование знаний и умений о вычислительных устройствах, их аппаратном и программном обеспечении для оптимального их применения в профессиональной деятельности и повседневном их использовании.

*Основные задачи* изучения дисциплины:

- Ознакомиться с основами аппаратного устройства вычислительных систем;
- Освоить основные функции операционных систем и систем хранения данных;
- Ознакомиться с основными компонентами операционных систем, системными службами и средствами администрирования;
- Повысить компетентность безопасного использования устройств, приемов борьбы со зловредными приложениями, анализом процессов и потоков.

Предметом изучения дисциплины являются современные вычислительные устройства, персональные компьютеры, их архитектура и программное обеспечение.

Изучение учебного материала связано с учебными дисциплинами «Основы информационных технологий», «Информационные технологии в культуре». Основными формами учебной работы являются лекционные, семинарские занятия, лабораторные работы, практические работы и самостоятельное изучение отдельных тем и вопросов.

Требования к компетенциям студента:

АК-1. Уметь использовать базовые научно-теоретические знания для решения теоретических и практических задач.

АК-2. Методологические знания и исследовательские умения, обеспечивающие решение прикладных и инновационных задач.

АК-3. Способность к постоянному самообразованию.

АК-4. Уметь работать самостоятельно.

АК-5. Иметь навыки, связанные с использованием технических устройств, управления данными и работой с компьютером.

АК-6. Владеть междисциплинарным подходом к настройке рабочей среды.

СЛК-1. Учитывать социальные и нравственно-этические нормы в социально-профессиональной деятельности.

СЛК-2. Быть способным к сотрудничеству и работе в команде.

СЛК-3. Владеть коммуникативными способностями для работы в междисциплинарной и межкультурной среде.

СЛК-4. Совершенствовать и развивать свой интеллектуальный уровень.

ПК-1. Квалифицированно использовать современные достижения по цифровой трансформации общества и построению цифровой экономики.

ПК-2. Использовать нормативно-правовую базу отрасли информационных технологий.

ПК-4. Обосновывать выбор приложений и инструментов для эффективного решения задач менеджмента.

ПК-5. Осваивать и реализовывать управленческие инновации в профессиональной деятельности.

В результате изучения дисциплины студент должен *знать*:

- принципы работы вычислительных систем;
- этапы развития, принципы функционирования и основные характеристики современных вычислительных систем и их компонентов;
- общую классификацию программного обеспечения и классификацию информационных технологий;
- функции и особенности различных операционных систем;
- методику и технику определения и решения основных программных и аппаратных проблем;
- правила подготовки системы для дальнейшей установки программных модулей;
- приемы настройки рабочей среды, основы администрирования и программного обслуживания настольного персонального компьютера.


В результате изучения дисциплины студент должен *уметь*:

- выявить и заменить неисправный аппаратный блок, плату расширения;
- выполнить настройки установленной операционной системы;
- восстановить или переустановить необходимую операционную систему;

- установить необходимое программное обеспечение;
- настроить систему безопасности и антивирусную защиту персонального компьютера;
- создавать резервные копии данных и при выходе из строя системы проводить ее восстановление.

Учебным планом на изучение учебной дисциплины предусмотрено всего 150 часов, в том числе 64 часа аудиторных занятий. Из них: лекции – 18, лабораторные занятия – 18, практические занятия – 16, семинары – 12 часов. Для проведения занятий требуется компьютерный класс, наделение пользователей полномочиями администратора и возможность полного управления локальным компьютером. Завершается изучение курса сдачей экзамена.

В учебно-методическом комплексе используются следующие специальные обозначения:

- ▶ – далее следует список команд указанного меню;
-  – задание, которое должно быть выполнено на компьютере;
- + – далее следует команда из указанного меню.

## 2 ТЕОРЕТИЧЕСКИЙ РАЗДЕЛ

### 2.1 Учебные издания

Демидович, А.К. Основы операционной системы Windows 7 : учеб.пособие / А.К. Демидович; ГУО «Академия последипломного образования». – Минск : АПО, 2016. – 70 с.

### 2.2 Конспект лекций

#### 2.2.1 Темы лекций

##### **Лекция 1. Принципы организации и функционирования вычислительных систем**

1. Структурная организация вычислительных систем.
2. Состав, назначение и взаимодействие устройств.
3. Основные характеристики вычислительных систем.
4. Понятие архитектуры вычислительных систем.
5. Схема Фон Неймана вычислительных систем с двоичной системой счисления, произвольным доступом к оперативной памяти, принципом программного управления, с расположением программ в оперативной памяти. Арифметико-логические устройства, регистры и шины.
6. Алгоритм, программа, процесс, поток.

Цель. Провести анализ состояния вычислительных систем, назначения настольных и сетевых систем обработки данных и организации взаимодействия участников управления данными.

*Выводы.* Разработка концепции управления данными – важный этап достижения целей организации или физического лица. От нее зависит четкость и слаженность работы персонала, учет использования данных, взаимодействие с заинтересованными сторонами и внешней средой.

*Ключевые понятия:* вычислительная система, алгоритм, программа, операционная система, программное обеспечение, процесс, поток.

##### **Лекция 2. Этапы развития вычислительных систем**

1. Первое поколение компьютеров 1943-1955 на электронных лампах.
2. Второе поколение 1955-65 – полупроводниковая база, мейнфреймы.
3. Третий этап 1965-80 годы – на интегральных схемах.
4. 4-й этап – элементная база на СБИС.
5. Классификация программного обеспечения: системное, прикладное, инструментальное и встроенное.
6. Краткая история возникновения операционных систем.

7. Технологии облачных вычислений, виртуальные машины, виртуальные сети, виртуальные диски и хранилища. Цифровая трансформация и Индустрия 4.

### **Лекция 3. Аппаратное обеспечение настольного персонального компьютера**

1. Аппаратное устройство персональных компьютеров.
2. Базовая система ввода/вывода BIOS (UEFI) и CMOS.
3. Назначение и программная поддержка устройств компьютера.
4. Устройства ввода/вывода, мультимедиа, сетевые платы и хранение данных.
5. Этапы загрузки операционной системы.
6. Базовая система ввода/вывода BIOS (UEFI) и разбиение жесткого диска на разделы.

### **Лекция 4. Операционные системы и их функции**

1. Современные операционные системы, их назначение и функции, компоненты ОС, основные приложения.
2. Работа в режиме командной строки MS DOS.
3. Архитектура ОС Windows, приложения режима ядра и пользовательские приложения.
4. Диспетчеризация процессов, организация многозадачного их выполнения.
5. Кодовая таблица данных и способы представление данных в операционной системе.
6. Растровое и векторное представление графических изображений, цветовые модели. Аналоговое и цифровое представление аудио данных. Цифровое кодирование видео данных.

### **Лекция 5. Системы хранения данных, файловые системы операционных систем**

1. Система размещения данных в оперативной памяти, хранения на жестких дисках и в сетевом окружении. Совместно используемые ресурсы.
2. Разбиение дисков на разделы, файловые системы, виртуальное хранение.
3. Профиль пользователя на системном диске. Настройка пользовательского интерфейса, настройка рабочей среды проводника в файловой системе.



4. Использование параметров безопасности, дисковых квот и шифрования данных.

5. Настройка персонального компьютера на работу в локальной и глобальной сети.

### **Лекция 6. Инструменты и утилиты конфигурирования операционных систем Windows**

1. Настройка среды ОС с использованием служб, локальной политики безопасности, групповой политики, параметров аудита, диспетчера служб ПС.

2. Настройка учетных записей с использованием групп безопасности, защиты брандмауэром Windows и защитником Windows.

3. Служебные программы и обслуживание компьютера. Обновление операционной системы, приложений и службы телеметрии.

4. Архивация данных, состояния операционной системы и таблицы разделов диска.

### **Лекция 7. Системный реестр как иерархическая база данных конфигурации системы Windows**

1. Структура разделов реестра. Редактор реестра.

2. Типы данных параметров реестра. Экспорт и импорт данных из реестра.

3. Специфические настройки, выполняемые с использованием редактора реестра.

4. Параметры реестра, используемые для автозапуска приложений, служб, библиотек и вредоносных программ.

5. Классификация вредоносных программ, способы защиты и борьбы с ними.

6. Основные утилиты Sysinternals «лицензией на убийство вирусов».

### **Лекция 8. Установка операционной системы и обслуживание персонального компьютера**

1. Загрузочные внешние устройства для установки операционных систем. Настройка BIOS (UEFI) на загрузку с внешнего носителя.

2. Предустановочная среда Windows PE.

3. Выбор способа загрузки операционной системы. Многовариантная загрузка.

4. Приложения защиты от вирусов и вредоносных программ.
5. Способы восстановления работоспособного состояния персонального компьютера.

## **Лекция 9. Основы администрирования операционных систем Windows**

1. Группы безопасности и доменная организация сетей.
2. Службы компонентов ОС, системные службы и телеметрия.
3. Управление компьютером и планировщик заданий.
4. Аудит и просмотр событий.
5. Набор утилит Sysinternals по оптимизации выполнения приложений и защите от вредоносного программного обеспечения.
6. Основные определения и понятия типов памяти.

### **2.2.2 Материалы лекций**

Рассматривается операционная система WindowsXP(ServicePack3). Требования к ее установке можно проверить в процессе установки. Рекомендуется процессор с тактовой частотой 300 МГц, 128 ОЗУ, 1,5 Гб свободного места на ЖД, видеоадаптер с поддержкой разрешения 800×600.

Требования к установке: симметричная многопроцессорность (не более двух), IPSec–защищенныйIP, рекомендация подключения к домену, динамические диски. При установке системы должен учитываться уровень абстрагирования, поддерживаемый BIOS.BIOS, заведомо не совместимые синтерфейсом автоматического управления конфигурацией и питанием(ACPI)уровниперечислены в файле Txtsetup.sif в разделе [NWACL]. Уровню ACPIудовлетворяютBIOS,выпущенные после 1.01.1999. Заведомо совместимыеBIOSперечислены в разделе [GoodACPIBIOS]. В диспетчере устройств смотрите системные устройства на наличиеуровня ACPIв аппаратуре компьютера.

В операционной системе поддерживаются полномочия доступа к файлам и папкам, средство защиты входа в систему, набор средств администрирования пользователей, управляемые списки доступа к объектам, защита важных системных файлов, подключение к удаленному рабочему столу.

Ядро операционной системыобладает защищенной моделью памяти с интегрированной системой защиты и уровнем абстрагирования от оборудования, защищающего ключевые компоненты операционной системы от некорректных программ, имеется набор средств восстановления работоспособности системы, отката драйверов устройств. Операционная система поддерживает беспроводные соединения, дистанционное управление рабочим столом с подключением клиентов.Возможно подключение к доменуAD с

использованием его служб. Динамические диски в WindowsXP на ноутбуках не поддерживаются.

При установке ОС создается ключ установки продукта – 25 алфавитно-цифровых знаков (серийного номера) с установочного компакт-диска Windows. На его основе создается код продукта (ProductID) из 20 знаков. На его основе генерируется ActivationCode. Создается неуникальный идентификатор оборудования. Для создания уникального кода установки используется идентификатор оборудования и код продукта. Каждому компьютеру присваивается уникальный идентификатор безопасности. Защита от копирования ОС осуществляется способом активации.

Механизм защиты от переноса или копирования активированной WindowsXP срабатывает, если заменены более трех из десяти компонентов компьютера в течение 120 дней. Среди них видеоадаптер, жесткий диск, контроллер жесткого диска, привод CDилиDVD, сетевой адаптер, процессор и оперативная память. Установку можно привязать к BIOS, и тогда защита от переноса не срабатывает. Файл System32\wpa.dblсодержит сведения об оборудовании, по которому определяется потребность в активации. При каждой загрузке создается его копия wpa.bak. Возможно его переименование при перезагрузке в безопасном режиме с поддержкой сети.

При установке ОС из среды MS-DOSнадо запуститьпрограмму smartdrive.exe, являющуюсяутилитой кэширования дисков, и при совместимости оборудования с операционной системой Windows XP запуститьпрограмму winnt.exe. На первом этапе установки копируется архив файлов установки в первый FAT-раздел. Затем выполняется перезагрузка с FAT-раздела и осуществляется переход ко второму этапу, на котором выбирается раздел и его файловая система.

Процесс установки из этой среды и последующих выполняетсяпрограммойwinnt32.exe. При этом NTFS-разделы недоступны для просмотра. Загрузка обычно выполняетсяс CDили DVD. Предварительно требуется убрать антивирусные программы,выполнить настройки сети, отключить защиту от вирусов и системные утилиты. Можно выполнить динамическое обновление системы и драйверов устройствчерез Интернет.

Выполняется чистая установка, или если есть установленная ОС Windows, предлагается восстановить ее. Обновление предыдущей версии Windowsнельзя выполнять при загрузке с внешнего носителя. Имеется консультант по обновлению операционной системы,совместимости оборудования и программ. На заключительном этапе выполняется активация WindowsXP, автоматическое обновление и, возможно, установка мультизагрузчика.

Не мультизагрузочное меню установочного CD-диска позволяет выбрать следующее: установку Windows XP, вывод подробных сведений о процессе установки, установку дополнительных компонентов Windows, выполнение иных задач, проверку совместимости системы с аппаратурой.

Выполнение иных задач включает установку удаленного управления рабочим столом, установку домашней или малой сети, перенос файлов и параметров настройки, выполнение обзора этого компакт-диска, выполнение просмотра заметок о выпуске, установку компонента .NETFramework.

На первом этапе установки выполняется копирование файлов системы, установка выполняется в текстовом режиме. По нажатию функциональной клавиши F6 выполняется установка драйверов ATA-66 или SCSI. В это время нажатие функциональной клавиши F5 предлагает выбрать тип компьютера или задать уровень абстрагирования оборудования HAL. Затем можно нажать функциональную клавишу F7, которая отменяет процесс автоматического определения HAL. Уровень абстрагирования оборудования иногда переустанавливается из свойств компьютера в диспетчере устройств при переустановке драйвера.

Затем установка происходит в графическом режиме с заданием языка и региональных параметров, с настройкой компьютера, созданием учетных записей пользователей. При первом запуске операционной системы появляется окно приглашения Windows.

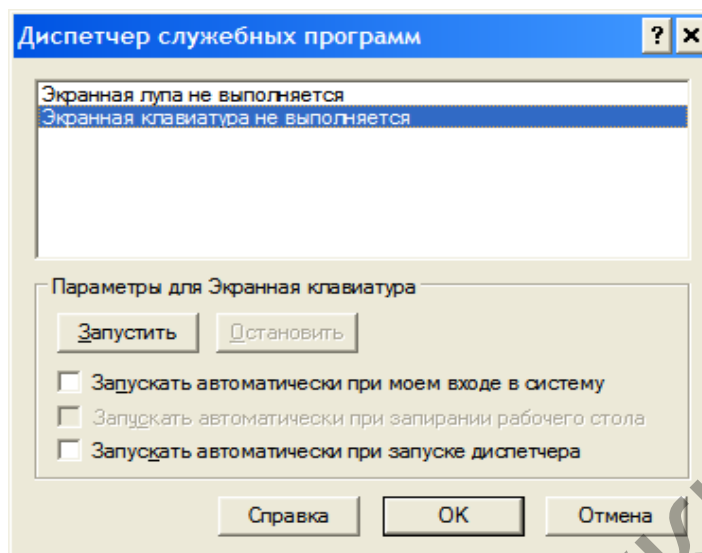
В мастере компонентов Windows XP отображается список компонентов, которые не скрыты в файле Windows\inf\sysoc.inf в информационном файле WindowsManager строкой в виде

IEAccess=ocgen.dll,OcEntry,ieaccess.inf,hide(7—отобразить).

Компонента службы терминалов не может быть удалена.

Перечислим не упомянутые компоненты операционной системы: IE, IIS, MSN Explorer, Outlook Express, Windows Messenger, другие службы доступа к принтерам и файлам сети, компонента обновления корневых сертификатов, очереди сообщений, проигрыватель Windows media, сетевые службы, службы индексирования, факсов, средства управления и наблюдения, стандартные и служебные программы. Не рекомендуется использовать кириллицу в именах доменов и компьютеров.

Компонент специальных возможностей используется для пользователей с ограничениями по подвижности, зрению, слуху. Экранная лупа увеличивает часть экрана. Диктор читает вслух выводимый на экран текст. Экранная клавиатура позволяет изменять раскладку, настроить функционирование клавиатуры. Имеется мастер специальных возможностей для настройки и диспетчер служебных программ (W + U).



К средствам и инструментам поддержки операционных систем относятся: диспетчер устройств, сведения о системе, средство производительности, редактор реестра, средство WindowsUpdate, командный процессор, сетевой монитор.

Возможна установка средств развертывания с использованием файла Deploy.cab для работы администраторов. Средства развертывания располагаются на CDWindowsXP в папке Support\Tools\. Файлом их установки является программasetup.exe. На компакт-диске имеются дополнительные средства поддержки, утилитаDiskProbe для ручного восстановления данных на диске.

Средства развертывания предназначены для установки операционной системы на большое количество компьютеров. При этом требуется установить на эталонном компьютере в папке c:\sysprep файлы: sysprep.exe, setupcl.exe, factory.exe; sysprep.inf, winbom.ini из файла Deploy.cab, systemmgr.exe. Файл Deploy.chm является файлом справки по развертыванию системы.

Файл ref.chm является справочным об утилитах и файлах поддержки при развертывании и по созданию файла ответов. Утилита convert.exe предназначена для конвертирования диска в файловую систему NTFS с использованием программы svtarea.exe, которая создает нефрагментированный файл для системных файлов с обновлением основной таблицы файлов. Утилиты oformat.com и ifactory.exe используются для внесения изменений в стандартную конфигурацию перед ее переносом на другие компьютеры.

Допускается автоматизированная установка операционной системы, не сопровождаемая пользователем с файлом ответов. При этом создается дистрибутивная папка C:\i386 или C:\ia64. В ее корне файл Unattend.txt содержит сведения о настройке файла ответов.

Можно воспользоваться программой WindowsSetupManager, по использованию которой имеются справочные chm-файлы. Менеджер установки WindowsXP позволяет создавать файлы ответов и пакетный файл.

Установку можно выполнять с использованием образов дисков, с предварительной подготовкой к установке с помощью утилиты Sysprep. Вначале подготавливается эталонный образец операционной системы, содержащий полностью сконфигурированную копию ОС Windows. Устанавливаются нужные приложения. Утилита Sysprep.exe используется для подготовки системы к созданию образа диска, удаления с компьютера всех идентификаторов безопасности. Однако это может привести к фатальным последствиям. После включения компьютера с копией диска (или подготовленного к копированию) программа sysprep обнаружит PnP устройства, запустит установку WindowsXP с экрана «Добро пожаловать» с активизацией, удалит папку sysprep и ее содержимое; перезагрузит или запустит утилиту MiniSetup.

Имеется возможность удаленной установки системы с помощью программы RIS на основе образа (клона) ОС, передаваемого по сети с поддержкой PXE сетевых карт и сервера управления системами SystemManagement-Server. Программа RIS создает на сервере каталог со службой и с образами операционной системы, указывается путь к дистрибутиву операционной системы. После этого устанавливаем ОС WindowsXP профессиональную, которую при выборе установочного образа требуется авторизовать в домене AD.

Надо соблюдать ограничения по тиражированию диска: одинаковые контроллеры жесткого диска, уровень HAL и версии BIOS и тип монитора. Для создания копии образа диска рекомендуется использовать утилиту Ghost (Symantec) или утилиту DriveImage (PowerQuest). Для его создания системного образа можно загрузиться с гибкого диска или внешнего носителя. Жесткий диск по объему должен быть не меньше образа. В образах не поддерживаются учетные записи пользователей или их профили, зашифрованные данные, подключения к домену.

Системный раздел EFI форматируется для FAT и содержит в корневом каталоге папку EFI. В версии Windows XP 64-Bit Edition создается подкаталог \Microsoft\Winnt50. Кроме того, в разделе могут присутствовать другие подкаталоги, создаваемые поставщиками операционных систем, поставщиками BIOS. Подкаталог \Mutil содержит программы, используемые микропрограммами EFI и операционной системой. Такие программы и содержимое системного раздела EFI доступны с помощью диспетчера загрузки EFI. Содержимое подкаталога \Microsoft\Winnt50 доступно только для уполномоченных сотрудников служб технической поддержки.


Перечислим специальные файлы, создаваемые при установке и загрузке ОС: nbtlog.txt – протокол загрузки ОС, setupact.log – журнал регистрации

операций, netsetup.log–используемые сети установки, repair\setup.log–журнал для консоли восстановления, scesetup.log– журнал по безопасности пользователей, setuperr.log–журнал сбоев при установке, MSBATCH.TXT– файл автоматизации установки, LMHOSTS(.sam) – задает соответствие NETBIOS имен и IP-адресов. Возможно создание файлов заставки входа или выхода.


Поддерживается защита важных системных файлов от замены другими их версиями и поддержка версий библиотек динамической компоновки. Защита файлов Windows выполняется в фоновом режиме и защищает все файлы, установленные программой установки Windows. Она предотвращает замещение защищенных системных файлов следующих типов: SYS, DLL, OCX, TTF, FON и EXE. Защита файлов Windows проверяет цифровую подпись файла. Подписанные файлы распространяются следующими способами:

- в пакетах обновления Windows;
- в пакетах исправлений;
- в составе обновлений операционной системы;
- в обновлениях, полученных с помощью средства WindowsUpdate;
- устанавливаются диспетчером устройств и установщиком классов Windows.

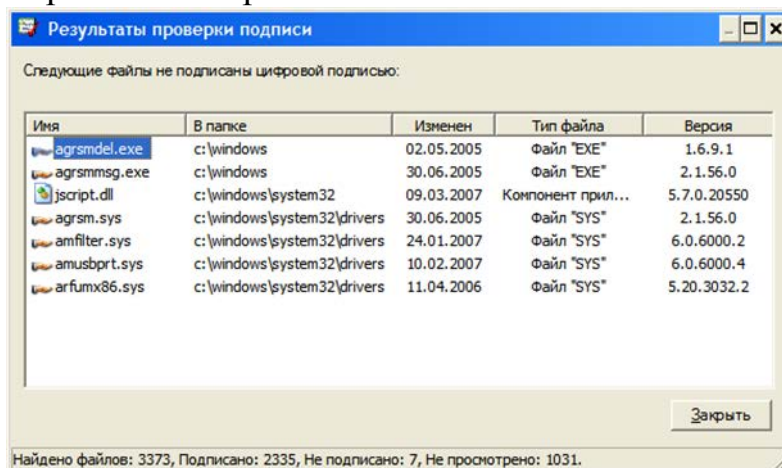
Служба SFP (SystemFileProtection) регистрирует попытку подменить системный файл и далее восстанавливает его исходную копию из папки Windows/system32\dllcache или из места установки ОС.

 Выполните программу SystemFileChecker(Sfc.exe), являющуюся утилитой командной строки отслеживания и разрешения проблем с подписью драйверов.

Кэш WindowsFileProtection(WFP) хранит системные файлы для их восстановления. Данная служба приостанавливает работу при загрузке в режиме защиты от боев.

 Используйте программы проверки подписи файла. Выполните программу sigverif (SIGVERIF.TXT).

Результаты ее работы отображены ниже:



Консоль восстановления обеспечивает режим загрузки и работы администратора в безопасной системной подсказке с ограничениями для устранения неполадок путем замены файлов, удаления драйвера, остановки службы. Для запуска консоли загружают ОС с установочного диска, затем начинают устанавливать ОС. На странице WelcometoSetupнажимаютклавишу R(еstore) и вводят номер раздела, содержащегоWindowsXP. Нельзя нажимать клавишу ввода, так как произойдет перезагрузка. При вводе номера раздела с иной ОС можно повредить системные файлы этой ОС. Для восстановления их надо войти в их консоль восстановления.

При работе в консоли восстановленияможно осуществить доступ только к корневым папкам дисков, доступ к %SystemRoot% и вложенным в нее папкам выбранной версии WindowsXP, доступ к папке Cmdcons и всем в нее вложенным, ко всем съемным дискам без полномочий копированияна них. Имеются особенности работы с динамическими дисками. Запрещен доступ к другим разделамОС, системным папкам, запрещена запись на съемные носители, нельзя изменять пароль администратора, отсутствуют программы редактирования. В этом режиме контрольные точки восстановления не сохраняются.

Команда Fixbootиспользуется для восстановлениязагрузчикantldr, запрещенного установкой другой (ранней) версии ОС Windows. Утилита Systemrootиспользуется для проверки правильности раздела. Может потребоваться исправление загрузочного сектора и главной загрузочной записи MBR, проверка диска на целостность данных утилитой CheckDisk. Для исправления поддержки устройств можно воспользоваться специальным файломExpandDriver.cab.

Для добавления консоли в меню загрузки выполняют командуd:\i386\winnt32.exe /cmdcons. При этом создается папка C:\cmdcons и файл cmdldr загрузки, дописывается пункт меню в файл boot.ini конфигурации загрузки.

Исправление системы после загрузки с CD-диск выполняется следующим образом.После начала установки нельзя выбирать команду исправления текущей версииWindowsc помощью консоли восстановления. Только после принятия лицензионного соглашенияпросканируйте диски на наличие версий Windows, выберите нужную ОС и нажмитеклавишу R. После этого выполняется чистая установка с заменой системных файлов и сохранением данных и настроек. Для замены библиотеки поддержки уровня абстрагирования оборудования можно обновить WindowsXP, либо найти существующий раздел с WindowsXP, загрузившись с CD-диска.

Ниже описано назначение служебных программ администратора:

bootcfg /scan– выдаетсписок доступных версий Windowsна всех дисках;



bootcfg/rebuild–заменяет файл boot.ini новым;

bootcfg/add– добавляет строку загрузки текущей версии Windows в boot.ini без замены других строк.

ListSvc– выдает полный список служб и драйверов с их текущим состоянием и комментариями; она доступна только в консоли восстановления.

Загрузка в режиме отладки запускает ядро ОС при подключении данного компьютера к другому компьютеру через последовательный порт COM2 и запускает на нем совместимый отладчик.

Существуют следующие уровни ОС:

1. Системная виртуальная машина состоит из трех основных элементов: 32-разрядного приложения Windows, программы-оболочки проводника и диспетчера программ, 16-разрядного приложения Windows, виртуальной машины MS-DOS. Все 32-разрядные приложения используют индивидуальное адресное пространство. ОС использует режим вытесняющей многозадачности для того, что бы гарантировать выделение необходимых системных ресурсов каждому приложению. 16-разрядное приложение выполняется как независимый процесс, для повышения надежности системы применяется режим кооперативной многозадачности.

2. Уровень прикладного интерфейса WinAPI обеспечивает 16-разрядная подсистема Windows, 32-разрядная подсистема Windows.

3. Сервисами режима ядра являются базовая система, подсистема управления файлами, подсистема сети, сервисы операционной системы, подсистема диспетчера виртуальной машины, драйверы аппаратных средств, диспетчер управления объектами.


4. Сервисы пользовательского режима.

5. Виртуальная машина Microsoft для Java (Microsoft VM) теперь доступна только в Интернете, откуда ее можно загрузить на компьютер.

Рассмотрим элементы экранного интерфейса. Интерфейс это есть схема взаимодействия приложения и пользователя. Объект– все, что может располагаться на рабочем столе и имеет свойства (папка, ярлык, панель, окно). Рабочий стол всегда имеет активный объект. Панорамирование выполняется с помощью технологии IntelliMouse. Можно использовать колесико мыши Microsoft IntelliMouse для панорамирования, изменения масштаба.

На рабочем столе имеются панель задач, кнопка меню пуск, кнопки задач (сгруппированные), в правой части панели располагается область уведомлений (можно использовать команды: настроить, скрыть неиспользуемые значки). Возможно расширение рабочего стола на два монитора при помощи технологии Dualview. Элементами интерфейса являются экран приветствия для входа в систему, окно быстрого переключения пользователей, диалоговое окно входа в систему.

Папка является электронным эквивалентом обычной папки, контейнером для хранения компьютеров, дисков, очереди заданий на печать, файлов и других папок, ссылок на объекты. В графическом интерфейсе пользователя она отображается в виде значка с именем. Системными папками являются папки: мой компьютер, принтеры и факсы, шрифты, панель управления, мои документы, избранное, портфель, корзина (у каждого пользователя своя или общая папка), сетевое кружение, рабочая группа, вся сеть, удаленный доступ к сети, веб-папки, общие документы, последние документы, автономные файлы, неиспользуемые ярлыки. Для системных папок имеется специальный идентификатор GUID (32-разрядная строка 16-ричных чисел). В корзину не попадают файлы, удаленные из 16-разрядных приложений Windows и MS-DOS. Папка моих документов содержит папки: мои веб-узлы, мои видеозаписи, мои рисунки, моя музыка.

 Выполните настройку рабочего стола компьютера.


Выполните очистку рабочего стола. Скрывая неиспользуемые значки в области индикаторов, отобразите один дополнительно, например, громкость.

Ярлыки – это указатели, ссылки на объекты: программы, папки, документы, принтеры, жесткие диски, сетевые узлы, элементы панели управления, веб-страницы. Существуют способы создания ярлыков: перетаскиванием правой кнопкой мыши, щелчком на объекте правой кнопкой мыши, щелчком правой в папке или по рабочему столу. Ярлыкам соответствуют файлы с расширением .lnk. Значок это есть графическое представление объекта. В отличие от ярлыка для него нельзя изменить параметры командной строки. Ярлыкам папки рабочего стола можно назначать сочетания клавиш для выполнения действий.

Перечислим существующие типы окон: окна приложений, документов, диалоговые окна, окна папок, окно быстрого переключения пользователей. Особые окна – открыть, сохранить, окно свойств, окно всплывающей подсказки.

Перечислим элементы окна. Заголовок окна имеет системное меню; кнопки в правой части заголовка; границу; строку меню (перечень заголовков меню и пункты меню после выбора заголовка и команды и подменю); панели инструментов; строку состояния; область содержимого. Рабочая область может содержать координатные линейки с индикаторами текущих табулстопов, панель просмотра свойств, указатели отступов абзаца и отступа первой строки; полосы прокрутки со слайдерами, разделитель рабочей области, кнопки перехода на полосе прокрутки (предыдущий или последующий объект, меню выбора объектов перехода). К элементам окна относят контекстное или всплывающее меню, шевроны (двойные стрелки), указывающие на наличие скрытых кнопок или команд, а также служебные элементы.

Диалоговые окна имеют кнопки команд и некоторые из элементов: текстовое поле ввода, списки, текстовое поле со списком, раскрывающиеся списки, раздел, группа переключателей, поля-флажки, счетчики, ползунки, набор вкладок, надпись. Кнопка сведений об элементах может располагаться в заголовке окна. Диалоговые окна могут быть модальными, которые не предоставляют доступа к родительскому окну, и немодальными.

 Рассмотрите управление диалоговыми окнами без использования мыши, только с помощью клавиатуры, используя клавиши Tab, Shift + Tab, Ctrl + Tab, пробел и другие.

Стиль интерфейса Windows Aero обеспечивает прозрачность окон, их эскизы и трехмерные эффекты или эргономическое пролистывание Flash3D. Для поддержки данного стиля требуется видеоадаптер с Windows Aero.

Панель задач имеет кнопки задач, область уведомлений, языковую панель. На панели задач могут отображаться закрепленные панели инструментов, сгруппированные кнопки приложений, область уведомлений с шевроном или двойной стрелкой. Вертикальная черта в левой части панели инструментов или рукоятка используется для перемещения панели инструментов. Параметр TaskbarGroupSize= 3 задает количество родственных кнопок на панели задач, открытых до начала их группировки. Кнопки панели могут быть только для чтения или для показа заголовков кнопок. Контекстное меню панели задач используется для ее настройки.

На панели задач могут находиться следующие панели инструментов: адрес, избранное, рабочий стол, быстрый запуск.

На диске имеется специальная папка панели быстрого запуска – C:\Documents and Settings\Administrator\Application Data\Microsoft\Internet Explorer\Quick Launch.

Панель инструментов может быть закрепленной на панели задач, плавающей или пристыкованной к одной из границ экрана.

Панель быстрого запуска содержит значки для быстрого доступа к программам, отображения рабочего стола, переключения между окнами или выполнения других задач.

 Создайте свою панель инструментов на панели задач.

Панель адреса позволяет выполнять команды, открывать документы, отображать содержимое папки в проводнике, открывать содержимое ресурса в окне обозревателя Интернета. Эквивалентное действие – команда выполнения из главного меню, из адресной строки проводника и обозревателя Internet Explorer.

Меню пуск может быть классическим либо двух панельным. Левая панель состоит из четырех частей: значка и имени пользователя, верхних закрепленных пунктов меню, расположенных выше разделительной линии, ярлы-

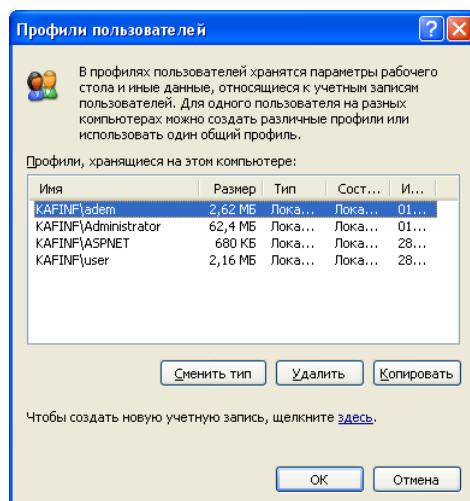
ков наиболее часто (недавно) использовавшихся программ, папки всех программ, которая отображает ярлыки из профиля пользователя и профиля AllUsers. В список часто используемых программ могут попадать ярлыки исполняемых файлов с запретом на некоторые. Правая панель меню с фиксированным списком программ неизменна. Она содержит важные программы и системные средства, а также пункт для работы с недавними документами.

При настройке меню пуска можно указывать количество закрепленных на ней программ (0-30), очищать меню, использовать сокращенное меню, устанавливать прокрутку программ, удалять программы из списка закрепленных, группировать кнопки на панели задач, задать выделение недавно установленных программ. Папка на диске с именем меню пуска отвечает папке меню всех программ.

Для классического меню можно использовать сокращенное меню, прокрутку программ в окне элементов меню пуска. Некоторые элементы главного меню можно отображать в виде папок или раскрывающихся меню. Ярлык установленной программы выделяется на несколько дней после ее установки ярким цветом (оранжевым).

Главное меню содержит следующие папки: программы, избранное (каналы, обновление приложений, ссылки, мои документы), папка документов, содержащую 15 последних использовавшихся документов, строку поиска, справку и поддержку, команды выполнения и выключения компьютера (завершение работы), выхода из системы и завершения сеанса.

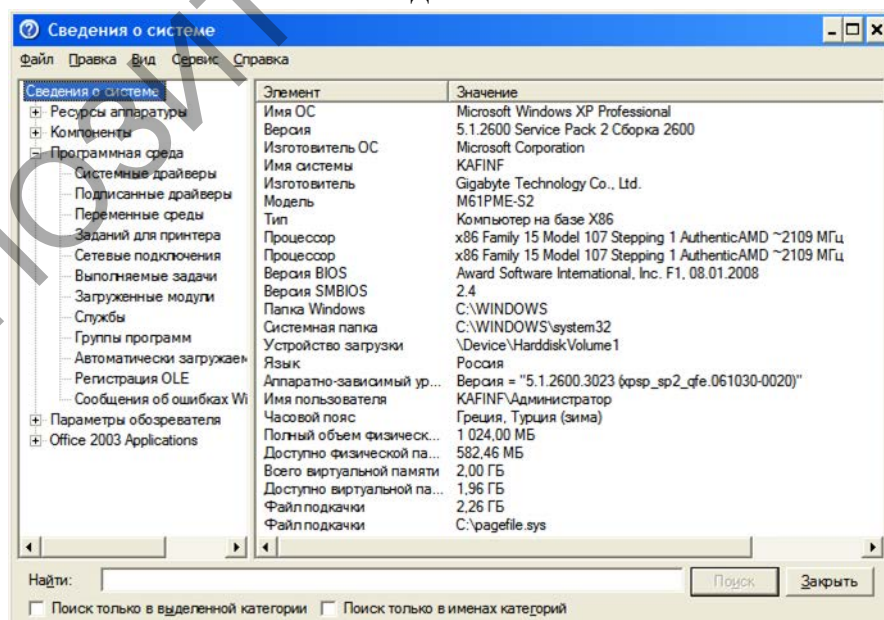
Рассмотрим стандартные профили пользователей. Профиль AllUsers влияет на меню пуска всех пользователей. Его папки рабочий стол, главное меню, документы, общие документы влияют на интерфейс всех пользователей. Папка избранного каждого пользователя своя. Папка DefaultUser копируется в профиль впервые создаваемой учетной записи. В профиле пользователя в папке Recent хранятся ярлыки всех ранее открытых документов, но только 15 последних отображаются в папке недавних документов главного меню. Очистка меню удаляет содержимое из папки Recent. Автоматически при выходе из системы для всех пользователей это можно делать через групповую политику, ветвь Меню Пуск и панель задач. Окно для управления профилями пользователей приведено ниже.



Настройка главного меню осуществляется командами: добавить, удалить, переместить, скопировать, сортировать (выполняется через редактор реестра), переименовать.


Существует три типа пользовательского интерфейса: в стиле веб-обозревателя, классический и смешанный.

Перечислим и кратко опишем назначение служебных программ. Проверка файловой системы диска (флэш-карты) определяет наличие ошибок и поврежденных секторов, файлов, индексов, дескрипторов безопасности, файловых данных, свободного пространства. Дефрагментация дисков устраняет разрывы в последовательности записи кластеров. Очистка дисков оценивает объем диска, который можно освободить, и удаляет указанные по категориям и папкам вспомогательные данные.

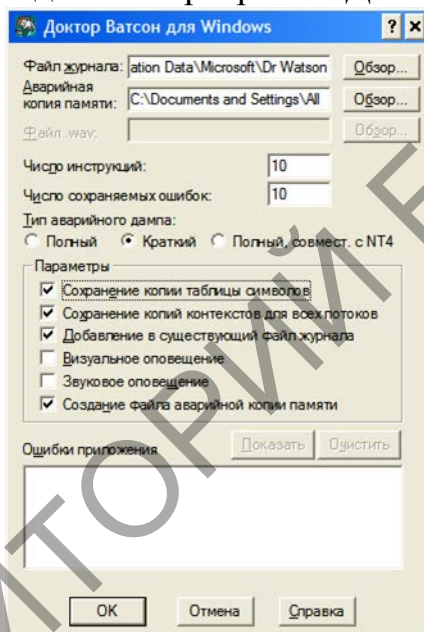


Программа сведений о системе отображает информацию о ресурсах аппаратуры, компонентах, программной среде, параметрах обозревателя и офисных приложениях. Для обслуживания компьютера можно использовать сервисные команды: диагностика сети, восстановление системы, проверка подписи файлов, средства диагностики DirectX, доктор Ватсон, регистрация

OLE, центр обеспечения безопасности, сжатие в системе NTFS, архивация данных, восстановление системы, мастер переноса файлов и параметров, назначенные задания, таблица символов.

 Создайте и запустите автоматическое задание на архивацию. Архивация может быть обычной (без учета атрибутов архивации). Она снимает атрибут А, означающий, что требуется архивация, и ускоряет процесс восстановления. Добавочная архивация используется только для тех данных, у которых установлен атрибут А. Разностная архивация используется также как добавочная, но она не снимает атрибут А. Часто используется ежедневная архивация.

Рассмотрим общие сведения о программе Доктор Ватсон.



Программа Доктор Ватсон для Windows представляет собой отладчик программных ошибок. Сведения, обнаруживаемые и записываемые программой Доктор Ватсон, используются группами технической поддержки при диагностике программных ошибок на компьютерах, работающих под управлением Windows. Текстовый файл журнала (Drwtsn32.log) создается в папке C:\Documents and Settings\AllUsers\ApplicationData\Microsoft\DrWatson. При обнаружении ошибки файл может быть передан сотрудникам группы технической поддержки. Кроме того, имеется возможность создания двоичного файла аварийной копии памяти, который может быть загружен в отладчик.

При возникновении программных ошибок программа Доктор Ватсон запускается автоматически. Самостоятельный запуск программы осуществляется командой drwtsn32.

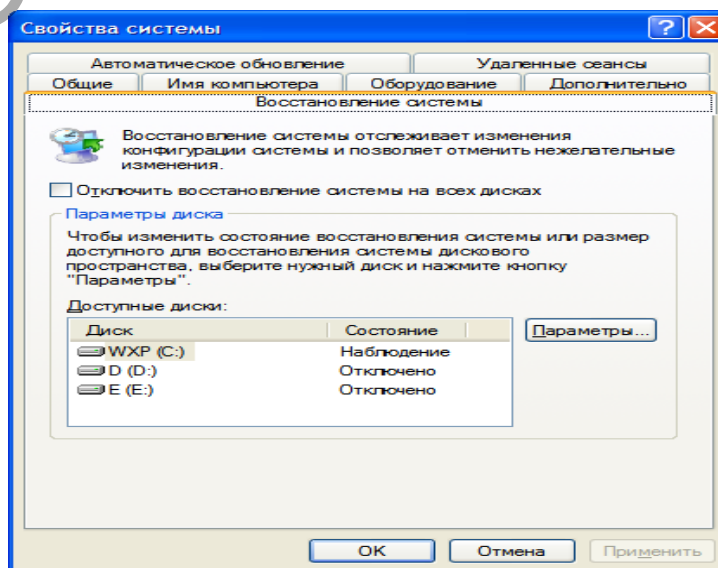
Система ASR предназначена для автоматизированного восстановления системного раздела в случае глобального сбоя. При этом надо предварительно выполнить архивирование данных, запомнить состояние разделов диска, системных файлов и оборудования, как правило, на внешнем носителе. Вос-

становление системы выполняется при загрузке с диска CD Windows XP нажимается функциональной клавиши F2. Далее поступаем согласно указаниям мастера.

Система аварийного восстановления состоит из двух частей: архивации и восстановления. Доступ к восстановлению выполняется нажатием клавиши F2 в ответ на соответствующее приглашение на текстовом этапе процесса установки. Средство аварийного восстановления системы считывает конфигурацию дисков из созданного ей файла и восстанавливает все подписи дисков, тома и разделы. Выполняется попытка восстановления конфигураций всех дисков. Затем средство аварийного восстановления системы производит простую установку Windows и автоматически запускает процесс восстановления с использованием архива, созданного мастером аварийного восстановления системы.

Служба восстановления предыдущего состояния системы является службой фонового режима, ведущей журнал изменений файлов определенных типов. Служба ведет журнал изменений файлов, типы которых заданы в файле %SystemRoot%\System32\Restore\Filelist.xml. Восстановление системы автоматически сохраняет каждые 24 часа точки восстановления в специальной папке restoreGUID, имеющей 32-символьный идентификатор, системных файлов и параметров в защищенной папке. Она создает на дисках папку SystemVolumeInformation объемом около 12 % от диска. Параметры настройки службы восстановления системы хранятся в разделе реестра HK\_LM\Software\MS\WindowsNT\CurrentVersion\SystemRestore. После восстановления в контрольную точку выполняется перезагрузка компьютера.

Настройка параметров загрузки и восстановления системы выполняется с использованием элемента система из панели управления заданием наблюдаемых дисков.





Служба автоматически отключается при менее чем 200 МБ свободного пространства на системном диске. В этом случае после освобождения пространства на нем надо перезапустить службу.

При успешной загрузке операционная система сохраняет в разделе реестра HK\_LM\System\CurrentControleSet список всех установленных драйверов и всех записей. В компоненте справки и поддержки имеются разделы выбора задания и отмены изменений.

После загрузки операционной системы в обычном или защищенном режиме состояние системы можно вернуть в предыдущее состояние. При восстановлении возвращаются системные файлы операционной системы и все содержимое реестра из папки SystemVolumeInformation. Рекомендуется отключить восстановление для не системных дисков. Доступ к папке SystemVolumeInformation разрешен только для учетной записи System. После восстановления предыдущего состояния удаляются все исполняемые файлы, \*.dll, сценарии, шрифты ТТ и \*.vls с датой изменения позднее точки восстановления. Точки восстановления автоматически удаляются службой через 90 дней.

При загрузке последней удачной версии восстанавливается последняя рабочая версия содержимого реестра, отменяются параметры оборудования и могут измениться драйверы в разделе реестра HK\_LM\System\CurrentControleSet.

Назначенные задания – это служба запуска в назначенное время программ, пакетных файлов, запуская ярлыка, сценария или документа по расписанию. Задания могут выполняться при загрузке операционной, при входе в систему. Задания выполняются под некоторой учетной записью, для которой установлен пароль. Журнал запуска располагается в файле C:\WINDOWS\Tasks\shedlgu.txt.

Имеется мастер переноса файлов и параметров пользователя из любой 32-разрядной версии Windows. Для переноса данных по сети запускают мастер на новом компьютере, на исходном компьютере из установочного диска операционной системы стартуют установку WindowsXP, выбираем другие задачи и затем перенос файлов и параметров. При «ручном» способе сохраняем либо только параметры, либо только файлы, или параметры и файлы для физического переноса. При этом переносятся пользовательские установки, свойства обозревателя Internet Explorer, электронной почты, а также параметры приложений из реестра и файлы профиля.

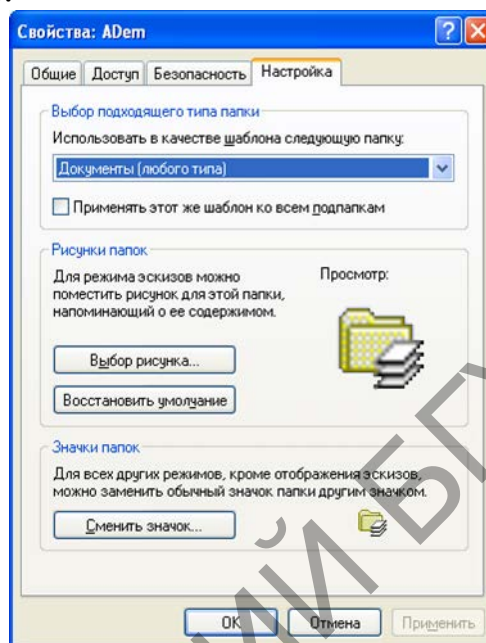
Рассмотрим способы настройки среды проводника. Проводник имеет: панель инструментов обычные кнопки, адресную строку. В проводнике левую панель со списком папок можно заменить панелью задач со списком



системных задач, других мест и миниатюрным окном свойств выделенных объектов (подробно).

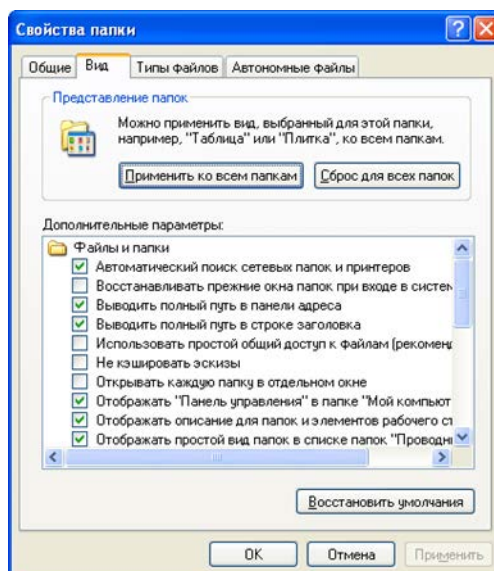
 Настройка панели обычных кнопок.

Существует режим просмотра эскизов страниц, в котором объекты представляются в виде эскизов.




На эскизе папки могут отображаться картинки из альбома, первые 4 изображения, первые кадры видео файла. Значки всех вложенных папок с изображениями представляют эскизы четырех изображений из этой папки, которые в ней были изменены последними. При просмотре папки в режиме плитки может использоваться замощение. Имеются режимы таблицы, списка и значков. Можно упорядочивать значки, используя имя, размер, тип и другие параметры. Группировка объектов отсутствует в режиме списка и диафильма.


В панели задач доступна группировка по задачам для изображений (слайд шоу), для файлов и папок и других задач. Нажатие функциональной клавиши F11 используется для просмотра всего экрана. Возможно групповое переименование с автоматической нумерацией нового имени.

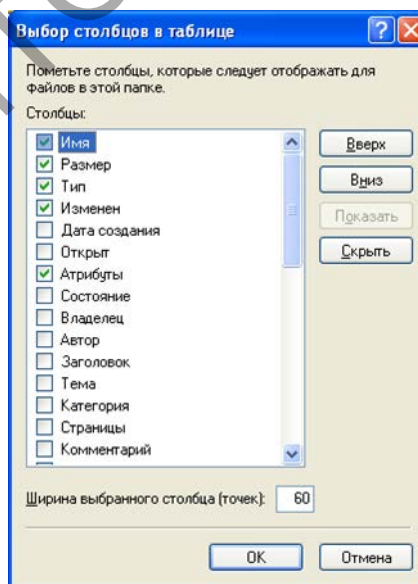



Для настройки способа отображения содержимого папок выполняем команду Сервис + Свойства папок с выбором вкладки вида.

Сетевое окружение обслуживается службой обозревателя компьютеров, которая автоматически осуществляет поиск сетевых ресурсов.

 Добавьте новый элемент в сетевое окружение (ярлыки общих папок и ресурсов, расположенных на серверах локальной сети, веб-серверах и серверах FTP).

 Задайте и просмотрите общие и особые свойства файлов и сводку. Выбор отображаемых столбцов в режиме таблица выполняется в следующем окне.



 Установите действие по умолчанию для указанного типа файлов (открыть, напечатать, слить). Настройте отображения расширения имени для данного типа файла при скрытых расширениях для зарегистрированных типов. Настройте действия при загрузке файла.

Представление шаблона может иметь следующие типы: документы, изображения, фотоальбом (фотографий), музыка (аудиозаписи и списки воспроиз-

изведения), артист (исполнитель или композитор), музыкальный альбом и видео. Значки папок задаются bmp-изображением размера 32×32 с расширением .ico. Шаблон может задавать для папки список задач, режим просмотра по умолчанию, значок папки в режиме эскизов, фоновый рисунок.

Для папки, настроенной как папка изображений (Вид + Диафильм), эскизы располагаются в полоске, а выбранный эскиз отображается в увеличенном виде. Вид сочетает предварительный показ одного изображения и эскизов остальных с тремя строками названия объекта. Панель предварительного просмотра и лента с изображением располагаются в нижней части. Под выделенным объектом располагаются кнопки: предыдущий, следующий, поворот поилипротив часовой стрелки с автоматическим сохранением нового изображения в оригинале. Этот режим можно установить только для папок с картинками, которые используют в качестве шаблона папки изображений или фотоальбома.


Для работы с CD и DVD накопителями используется файловая система Live(UDF). Ранее использовалась система хранения Mastered. Существуют аудио CD в формате RedBook для обычных проигрывателей и CD-диски с данными в объединенном формате 9660 и Joliet. При записи на CD-диск используется встроенное средство записи EasyCD Creator (Roxio). Если установлено приложение от иных фирм, например Nero, то требуется отключить встроенную запись CD-дисков на этом дисковом устройстве и автоизвлечение после записи данных. Копируемые файлы предварительно помещаются в папку


User\LocalSetting\ApplicationData\MS\CD Burning\CD Burning\stash-files.bin.

Чтобы отключить автозапуск, надо в разделе реестра HK\_LM\SYSTEM\CurrentControlSet\Services\CDRom присвоить параметру "Autorun" значение 0 (1 – для включения). В результате могут утратиться возможность записывать и очищать CD-диски встроенными средствами Windows. На работу внешних программ для записи это не окажет никакого влияния.

 Отформатируйте флэш-диск в файловой системе NTFS.

В свойствах устройства выбирается вкладка оборудование и кнопка свойств, вкладка политики. Включите оптимизацию для выполнения, тогда доступно форматирование в файловой системе NTFS, затем включите оптимизацию для быстрого удаления (без указания безопасного извлечения).

 Освойте установку параметров автозапуска для съемных накопителей.

 Освойте команды в файле автоисполнения Autorun.inf, синтаксис которых приведен ниже:

Icon= источник [,index] – файл значков для текущего каталога;

Defaulticon= путь к файлу [,index];  
Label = MySystem – метка диска для файла Autorun.inf в проводнике;  
Open = [полное имя] [параметры];  
Shellexecute= readme.txt – автоматическое открытие файлов зарегистрированного типа;

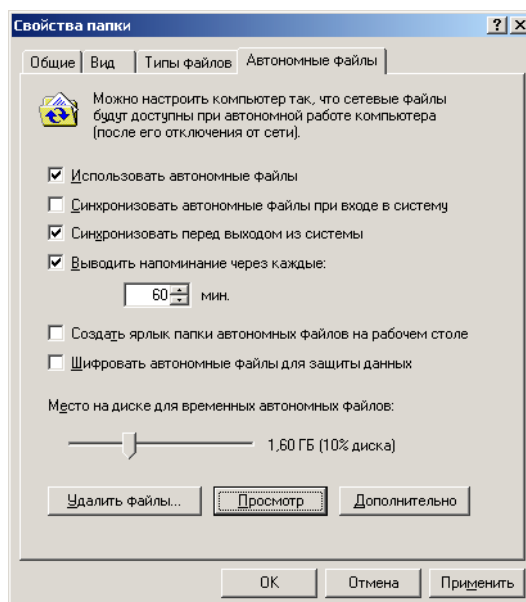
Shell\play\command= msplayer.exe – команда контекстного меню данного диска. По умолчанию выполняется команда AutoPlay.

Рассмотрим сжатие в файловой системе NTFS и Zip-папки. Включение или выключение встроенного сжатия NTFS файлов либо папок задается через общие свойства в окне дополнительных атрибутов и используется для экономии места на диске. Для обеспечения эффективности и надежности работы с дисками запрещено одновременное сжатие и шифрование NTFS. Не рекомендуется сжимать системные папки и регулярно используемые журналы.

Работа с Zip-папками доступна из проводника. Такие папки создаются командой Отправить + Создать Zip-папку. Вновь добавленные в нее файлы не защищаются, список содержимого всегда доступен. В сравнении с программой архивации, например, WinRAR встроенная архивация не налагает ограничений на интерфейс взаимодействия, использует меньше ресурсов. Zip-папки работают только при отключенной связи расширения файлов .zip со сторонними программами архивации.

В отличие от встроенной архивации Zip-архив или RAR-архив – это один файл, в котором упакованы несколько файлов или папок. Архивы можно защищать паролем, однако архиватор не защищает от удаления, удаленные из архива данные не попадают в корзину. Во время работы с архивом создаются временные папки с разархивированными элементами, которые удаляются после успешного завершения работы архиватора. Могут возникать трудности со поиском данных по содержимому архива.

Папка автономных файлов упрощает работу в локальной сети путем синхронизации, аналогичной папке портфеля, настраивая компьютер так, что сетевые папки или файлы будут локально доступны при отключении компьютера от сети. Чтобы включить работу с этой папкой требуется отключить быстрое переключение пользователей. Данное отключение выполняется через элемент учетных записей пользователей, расположенный в панели управления. Затем используем изменение входа пользователей в систему.



Для включения папки автономных файлов в свойствах папки вкладки автономных файлов включают флажки использования, синхронизации при входе в систему, перед выходом из системы, выводом напоминания каждые 60 минут. Данную папку нельзя использовать для удаленного рабочего стола на компьютере. Синхронизация содержимого папки возможна из среды проводника.

После настройки папки автономных файлов в нее добавляем любые файлы и папки из сетевого окружения. Они становятся доступными автономно, значки имеют двойную стрелку, в области уведомлений отображается значок автономной работы.

Настройка кэширования на файловом сервере выполняется консолью ShareFolders по команде разрешения кэша файлов в этой общей папке. Доступно ручное или автоматическое кэширование документов, автоматическое кэширование программ.

Для синхронизации из среды проводника используется команда Сервис + Синхронизировать. Если автоматическая синхронизация невозможна вследствие изменения обоих объектов, можно сохранить одну версию либо две.

Для поиска данных может использоваться их тип: изображение, музыка или видео, документы, все файлы и папки. Дополнительно можно задать различные сведения о файле, поддерживаются булевские операторы, словоформы, сохранение параметров поиска. Ускорение поиска обеспечивает служба индексирования, которая использует дополнительно до 30 % объема индексируемых файлов. Она следует правилам безопасности NTFS, индексирует офисные документы и файлы следующих типов – \*.txt, \*.rtf, \*.htm, при этом не учитывается регистр символов. Индексирование игнорирует словесный шум, который задается в текстовом файле

system32\noise.eng (rus). При изменении пространства индексирования можно удалить старый индексный файл и создать новый.


Если служба индексирования не готова, то происходит обычный поиск. Текстовые запросы имеют две формы: фразы по умолчанию и простой текст. Возможно использование шаблонов имен, атрибутов поиска, операторов Equals, Contains. Настройка службы индексирования выполняется через средство администрирования служб и приложений. Поиск без использования службы индексирования занимает много времени.

Поиск файлов является средством текстового поиска. Имя файла не может содержать специальные символы: \ / : \* ? " < > ; |, его длина до 255 символов.


При открытии в NTFS-разделе папки, содержащей большое количество файлов, операционная система каждый раз обновляет метку последнего доступа к файлам, что может замедлять работу. Чтобы отключить использование данной функции, создают в реестре по адресу


HK\_LM\System\CurrentControlSet\Control\FileSystem параметр типа DWord с именем NtfsDisableLastAccessUpdate и присваивают ему значение 1.

Настройка рабочего пространства может выполняться с помощью параметров панели задач: ее расположением, настройкой области индикаторов со значками и уведомлениями, расположением поверх всех окон, автоматическим скрыванием с экрана и размером значков.

 Выполните добавление панелей инструментов на панель задач и их настройку.

Настройка главного меню выполняется путем создания папок и ярлыков, их добавлением, удалением, очисткой меню документов, перетаскиванием из окна проводника на кнопку пуска. Имя документа заносится в папку главного меню недавних документов щелчком по его ярлыку, двойным щелчком по иконке в папке или в окне проводника и после его сохранения.

 Создайте эргономическое меню пуска. Выполните настройку контекстного меню отправления, воспользовавшись папкой SendTo.

 Выполните настройку среды на пользователя заданием пароля для входа в систему, созданием учетной записи пользователя или файлового профиля.

Перечень элементов панели управления задается в папке Windows\system32\\*.cpl с перечнем файлов, конфигурация окна панели управления задается в файле control.ini (system.cpl=no).

Редактор блокнота поддерживает кодировки ANSI, Юникод, Юникод BigIndian, UTF-8. Уникальные символы присутствуют в кодировке Unicode, в формате ANSI поддерживается усеченный набор символов. ANSI-кодировка

является однобайтовой. В ней коды от 0 до 127 совпадают с кодами ASCII, коды от 128 до 255 могут задавать символы различных языков в зависимости от выбранной кодовой страницы.

Редактор личных символов позволяет создать уникальные символы, например, специальные буквы и эмблемы для использования в имеющейся библиотеке шрифтов. Он содержит основные инструменты для создания и изменения символов, а также дополнительные возможности.

Настройку экрана можно выполнить заданием фона, который состоит из рисунка (обоев) и узора под ним. Обои могут задаваться веб-страницами из папки Windows\Web или растровым изображением. Допускается использование файлов фона со следующими расширениями: .bmp, .gif, .jpg, .dib, .png, .htm.

Технология ClearType программно утраивает горизонтальную разрешающую способность отображения очертаний символов шрифтов на экране для жидко-кристаллических мониторов с цифровым интерфейсом.

Экранная заставка может появляться, если некоторое время нет действий с мышью и клавиатурой. Задается заставка вызовом программы-заставки, расположенной в папке Windows\system/\*.scr.


 Создайте ярлык быстрого вызова заставки с указанием его свойств.


В системе с несколькими мониторами используется PCI-видеоадаптер (Peripheral Component Interconnect) или AGP (Accelerated Graphics Port). Адаптер, располагаемый на материнской плате, становится дополнительным, если совместим с режимом работы с несколькими мониторами. При установке операционной системы Windows основным монитором становится внешний, при этом может отключиться встроенный адаптер монитора на материнской плате. Через BIOS можно отменить полное отключение встроенного адаптера.


Активный рабочий стол имеет:

- уровень пиктограмм рабочего стола;
- уровень компонентов (веб-контейнер) или HTML-уровень;
- уровень HTML-фона (обои задаются HTML-файлом или рисунком).

В панели управления имеются элементы: используемый язык и национальные стандарты, почта, настройка мыши, настройка клавиатуры, назначение событиям звука, установка даты и времени.

 Настройте работу проводника в стиле веб. Создайте панель инструментов на панели задач, настройте видимость панелей. Настройте параметры системной папки корзина (размер, отключение корзины, отключение запросов на удаление). Воспользуйтесь мастером очистки рабочего стола в папку неиспользуемых ярлыков (настройка экрана), отобразите или скройте элементы рабочего стола.

 Используйте удаленный рабочий стол для подключения к серверу терминалов или к сеансу консоли удаленного компьютера. Если нужно применить сочетание клавиш Ctrl+Alt+Del к удаленному компьютеру, используйте сочетание Ctrl+Alt+End. Для переключения между полноэкранным и оконным режимом в сеансе служб терминалов следует использовать сочетание клавиш Ctrl+Alt+Break.

 Отобразите на рабочем столе версию операционной системы. С этой целью в ветви реестра HK\_CU\ControlPanel\Desktop создайте параметр типа DWordc именем PaintDesktopVersion=1, который позволяет вывести на рабочий стол номер версии операционной системы. Присвоение параметру нуля скрывает его отображение.

В файловом профиле пользователя на диске располагаются специальные папки:

\Favorites (избранное), которая содержит закладки обозревателя;

\Desktop (рабочий стол) – содержит объекты рабочего стола;

Папка C:\Windows\inf\ – содержит файлы с расширением \*.inf с информацией об установленных устройствах и сведениями о доступных для установки устройствах;

Папка C:\...\Главное меню\Программы\Стандартные – соответствует структуре соответствующих папок меню пуска.


Брандмауэр Windows предоставляет компьютерам, имеющим доступ к Интернету, дополнительную безопасность с помощью специальной защиты. Брандмауэр включен по умолчанию для защиты всех сетевых подключений. Его журнал располагается в файле C:\WINDOWS\pfirewall.log. Можно также загрузить и установить брандмауэр от независимого разработчика.

Брандмауэр поддерживает службы трансляции адресов, адресации и разрешения имен, блокирует подключение внешних источников к компьютеру, кроме выбранных на вкладке исключений. Он обеспечивает общий доступ к файлам и принтерам. На вкладке Дополнительно указываем, для каких подключений он предназначен, необходимость ведение журнала безопасности, настраиваем протокол ICPM, параметры по умолчанию.

Файл Svchost.exe (*GenericHostProcessforWin32 Services*) – системный процесс операционной системы, который обрабатывает 32-битные DLL и поддерживает системные службы. В процессе загрузки операционной на основании записей в реестре исполняемый файл Svchost.exe составляет список служб, которые необходимо запустить. Одновременно могут быть запущены несколько экземпляров процесса Svchost.exe. Каждый сеанс Svchost.exe содержит группировку служб, следовательно, отдельные службы могут выполняться в зависимости от того, как и когда был запущен Svchost.exe. Таким



образом, улучшается контроль и упрощается отладка. Файл Svchost.exe расположен в папке %SystemRoot%\System32.

 Включите или отключите удаленный рабочий стол, удаленный помощник. Пригласите помощника (эксперта). Освойте работу удаленным помощником, установите срок действия приглашения. С помощью сетевого мессенджера или Outlook разошлите приглашение на сеанс удаленного помощника. При этом используется билет удаленного помощника в формате XML в качестве вложения письма. Если соединение выполняется по Интернету, требуется указать свой публичный IP-адрес и уточнить настройки брандмауэра.


Центр справки и поддержки обслуживается исполняемым модулем helpctr.exe и службой helpsvc.exe. В обеспечение ее содержимого включены обычные обучающие и справочные материалы.

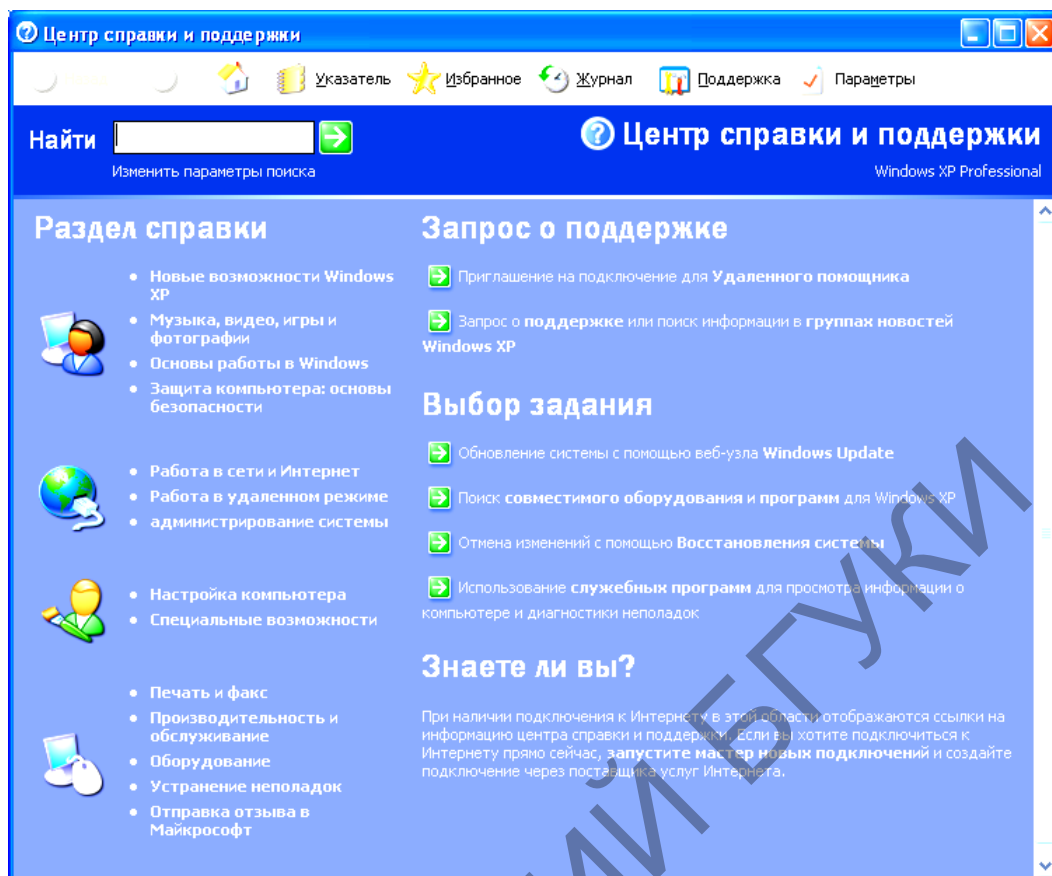
Синтаксис обращения к справке следующий:

```
%systemroot%\PCHealth\HelpCtr\Binaries\helpctr [/url [адрес_URL]]  
[/mode [адрес_URL]] [/hidden] [/fromstarthelp]
```

Настройка центра справки и поддержки выполняется выбором поля параметров: Результаты поиска и советы справки могут указывать рекомендуемые разделы. Полнотекстовый поиск и база знаний MS указывают на статьи материалов.

 Выполните настройку параметров поиска. Задайте установку и совместное использование справки.

 Настройте справку без поиска в базе знаний Microsoft, если компьютер не подключен к Интернету.



Поиск разделов справки возможен по содержанию, указателю и поиску. При поиске точного названия или термина можно использовать указатель. На панели справки доступны команды:домой, избранное, журнал, поддержка. В тексте раздела справки могут присутствовать:

Ссылки на системные средства и утилиты;

Описание команд командной строки в алфавитном порядке;

Ссылки на сведения о системе и ее текущей конфигурации, аппаратном и программном обеспечении и системных службах;

Доступ к журналам регистрации ошибок, параметрам групповой политики, дополнительные сведения о системе;


Ссылки на внешние источники (базу данных Microsoft) и программу улучшения справки;


Доступ к удаленному помощнику.

Домашняя страница центра справки и поддержки содержит разделы справки, запрос о поддержке, выбора задания и подсказкузнаете ли вы.

В процессе взаимодействия со справкой создается список избранного с темами разделов.

Результаты поиска выдаются в трех группах:рекомендуемых разделах по ключевым словам, в полнотекстовомпоиске по словам и фразам и в базе знаний.

 Изучите мастер Windowsc пошаговыми инструкциями по их применению. Создайтезакладки избранногов центре справки и поддержки.

 Выполните установку и совместное использование справки, в частности установите справку с другого компьютера. После этого освоите переключение между версиями справки.

Расширенные сведения о системе можно получить при запуске мастера результирующей политики, компонента производительности и обслуживания.

Стандартная программа мастера совместимости программ предыдущих версий используется для задания свойств их исполнения. С этой целью выполняем для ее файла команду Свойства + Совместимость. Для выполнения 16-разрядных приложений запускается виртуальная машина, имитирующая защищенный режим 386 процессора и среду Windows 3. Такие приложения ограничены одним потоком. Операционная система рассматривает каждое 16-разрядное приложение как поток в одной виртуальной машине. На ней не запускается несколько копий одной программы.

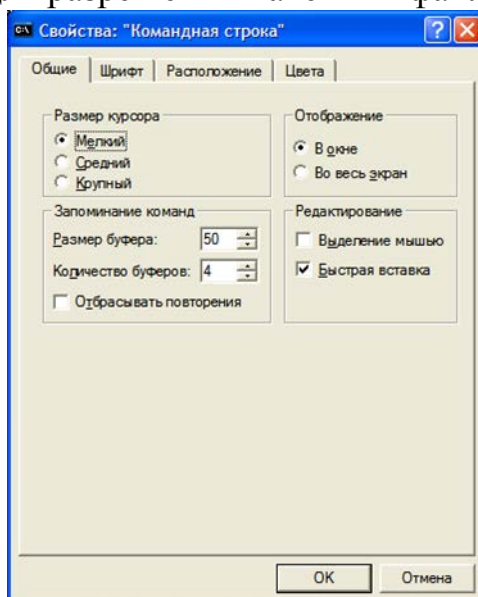
В 64-разрядной версии ОС 16-битные приложения не поддерживаются. Установка 32-разрядных приложений 16-битными программами установки, как правило, не поддерживается. Не поддерживаются 32-битные драйвера устройств и антивирусные программы.


Переменные среды окружения операционная система читает из следующих разделов реестра:


HK\_LM\System\CurrentControlSet\Control\SessionManager\Environment  
HK\_LM\Environment


Командная строка предоставляет среду, в которой выполняются приложения и служебные программы с текстовым интерфейсом, обеспечивается прямая связь между пользователем и операционной системой. Адресная строка IЕ также является командным интерпретатором.

Специальная учетная запись пакетных файлов управляется операционной системой и используется для разрешений пакетных файлов.



 Выполните команду `Cmd /U`, которая запускает процессор в кодировке Unicode. Флажок быстрой вставки позволяет вставлять текст, начиная с позиции курсора, причем последующие символы сдвигаются вправо, а не замещаются.


 Выполните команду `helpcmd` для описания параметров запуска командного процессора. Имеются специальные символы условной обработки при передаче нескольких команд.

 Изучите использование операторов перенаправления вывода команд. Создайте файлы со справочными сведениями, например, по командам `Ipconfig`, `Tracert`.

Просмотрите переменные среды окружения. Отобразите перечень папок автоматического просмотра.

Когда требуется оставить окно открытым после завершения выполнения команды, используют параметры запуска командного процессора, например, `cmd.com /Kping192.168.15.14` – для вывода окна запроса параметров программы.

При запуске любого приложения командой `Start` оно выполняется в новом командном процессоре.

 Отключите автоматическое выполнение команд при запуске командного процессора. Задайте автозапуск одной команды при вызове интерпретатора команд:

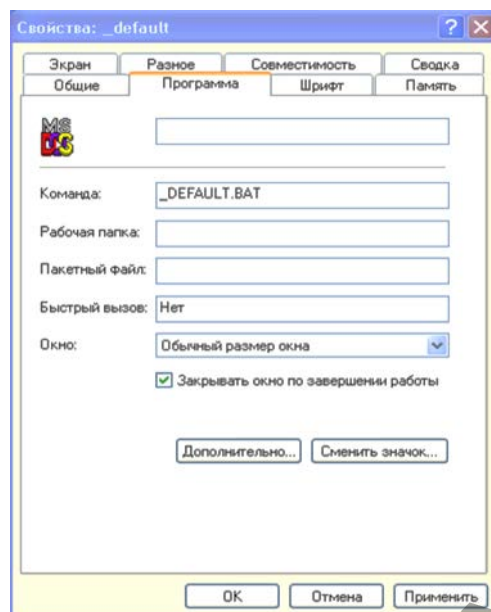
```
HK_LM\Software\MS\Command Processor\AutoRun=C:\bp\keyrus.com
```

```
HK_CU\AutoRun= C:\bp\keyrus.com
```

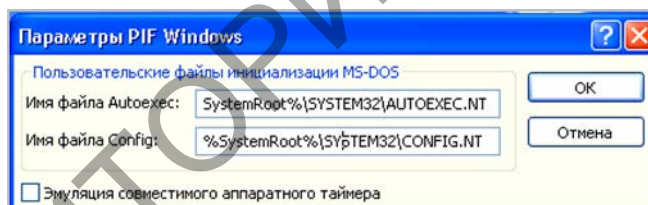
При работе в командной строке завершение имен файлов и папок (по нажатию `Ctrl + D`, `Ctrl + F`) не включено. Командное автозаполнение работает после запуска командного процессора с параметрами `cmd /f:on`.

Оконный режим (по нажатию `Alt+Enter`) командного процессора имеет панель инструментов для совместного использования данных.

Все 16-разрядные приложения выполняются в одном пространстве памяти. Ярлык программы можно настроить на ее запуск в отдельной области памяти. По умолчанию параметры среды DOS-программ содержатся в `Windows\_default.pif`, они копируются в создаваемые `pif` – файлы программ.



Если требуется при запуске DOS-программ запускать пакетный файл, сохраните его в `Windows\_default.bat`. Файлы конфигурации виртуальных DOS-машин задаются в файлах `system32\autoexec.nt`, `config.nt`. Можно для программ задать другие пути к файлам конфигурации с такими именами, используя контекстное меню файла программы и выбрать команду дополнительно.



В них нельзя задавать устаревшие и неподдерживаемые драйверы (памяти, `ansy.sys`, `country.sys`, `smartdrive.sys`). Графические DOS-программы работают только в полноэкранном режиме. Из командной строки можно запускать приложения WindowsXP и предыдущих версий Windows. Приложения текстового режима выполняются в этом же окне командной строки, графического режима – в отдельном. Предлагается использование оконного интерфейса WindowsXP в устаревших программах путем задания файла манифеста `pn.manifest`.

Приведем пример расширенного синтаксиса команд, когда перенаправление вывода в файлы выполняется с учетом наличия ошибок в выполнении:

```
Type Autoexec.bat 2>err.out 1>std.out
```

Стандартный поток ошибок    Стандартный поток вывода

Пакетные файлы имеют расширение `*.bat` и `*.cmd`, выполняются 32-разрядным интерпретатором команд (командным процессором) `cmd.exe`. Он использует кодировку ANSI для текста, направляемого в файл или на устройство. В пакетных файлах комментарии, начинающиеся с двух двоеточий `::`, не выводятся на экран.

Промежуток между командами setlocalendlocal– место объявления локальных переменных окружения.

setpath= %path%;c:\bp\bin – команда добавления папки в число автоматически просматриваемых.

В пакетных файлах могут использоваться строки, содержащие несколько команд. В этом случае используются специальные символы, которые могут влиять на выполнение перечисляемых команд:

& – отделять команды в строке запроса;

&& – выполнять команду, если предыдущая завершена успешно;

|| – выполнять команду, если предыдущая завершилась с ошибкой;

^&– за вставкой символ-буква, а не специальный символ.

Скобки( ), [...] используется для группировки или вложения команд.

Типы переменных среды в порядке убывания приоритета:

1. Встроенные системные переменные;
2. Системные переменные куста HKEY\_LOCAL\_MACHINE;
3. Локальные переменные куста HKEY\_CURRENT\_USER;
4. Все переменные среды и пути указаны в файле Autoexec.bat;
5. Все переменные среды и пути указаны в сценарии входа в систему (если он имеется);
6. Переменные, используемые интерактивно в сценарии или пакетном файле

В командной оболочке каждый экземпляр Cmd.exe наследует среду своего родительского приложения. Поэтому можно изменять переменные в новой среде Cmd.exe, что не повлияет на среду родительского приложения.

Command.com– 16-разрядный командный процессор, подуправлением которого выполняются 16-разрядные программы MS-DOS.

Протокол FTP не полностью поддерживает кириллицу, поскольку основывается на 7-битной кодовой странице. Поэтому не рекомендуется использовать кириллические названия папок и файлов для использования их в FTP.

Сервер сценариев\*.vbsи сценарии решают более сложные задачи, чем пакетные файлы. С их помощью можно управлять большинством компонентов Windowsи ее приложениями. Сервер сценариев Windowsимеет имяCScript.exe и используется для выполнения в командной оболочке сложных сценариев. Для включения сценариев используют групповую политику: разделыКонфигурация пользователя, Конфигурация компьютера.

Имеется четыре вида локальных сценариев WindowsXP: сценарии при входе пользователя в систему, при выходе пользователя, при загрузке операционной системы, при выключении компьютера. Они располагаются соответственно в папках:

system32\GroupPolicy\User\Scripts\Logon (Logoff);

system32\GroupPolicy\Machine\ Scripts\StartUp(Shutdown).

### Основные разрешения доступа

Разрешения определяют правила доступа к объектам файловой системы и системы хранения данных. Разрешение Read (чтение) предоставляет просмотр имен файлов, атрибутов файлов, чтение разрешений и синхронизацию файлов, Read&Execute – чтение или просмотр содержимого папок и файлов, запуск программ и просмотр списка содержимого папки (ССП). Разрешение ССП предоставляет предыдущие действия только для папок. Разрешение Запись предоставляет создание файлов, запись данных, считывание атрибутов и разрешений, синхронизацию файлов. Разрешение Изменить (Change) действует без изменения разрешений, не разрешает создавать новые файлы и папки, становится владельцем (чтение + выполнение + запись). Разрешение Полный доступ (Full) предоставляет изменять, изменять разрешения, становится владельцем файла. В связи разрешениями вводятся характеристики пользователей – создатель-владелец, интерактивный – это вошедший в систему локально или с помощью удаленного рабочего стола. При разрешении ССП наследование разрешений осуществляется вложенными папками, а при R&E – также и файлами.

Разрешения для объектов назначаются в окне его свойств и могут назначаться группам безопасности и пользователям. Особые разрешения назначаются при выборе кнопки Дополнительно. Аутентификация в домене выполняется по протоколу Kerberosv5 и требует согласования времени клиента со временем на сервере домена.

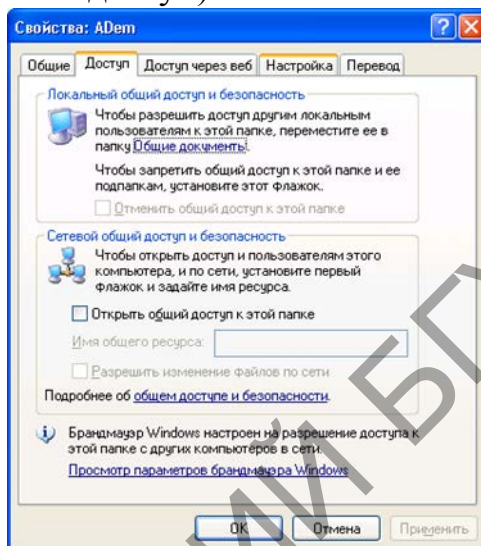
Маркер доступа (securityaccessstoken) содержит имя пользователя, его SID и сведения о группах безопасности, к которым принадлежит учетная запись этого пользователя. Имеются заведомо известные SID, например, S-1-5-18 для встроенной учетной записи System.

Изначально после установки ОС в среде существует полное доверие пользователей, профиль каждого пользователя полностью доступен администраторам и учетной записи System, пользователи с ограниченными правами не могут просматривать файлы из других профилей. Отменить общий доступ можно только для папок, входящих в профиль. Полномочие Отменить общий доступ наследуется безусловно всеми вложенными файлами и папками. Этот запрет безопасности наследуют все файлы и вложенные папки. При копировании из профиля файлы и папки получают разрешения новой папки.

Пользователи с ограниченными учетными записями могут устанавливать приложения лишь в профиле пользователя на диске, создают свои ярлыки, изменяют в реестре содержимое раздела HK\_CU. При нарушении хотя бы одного условия выдается сообщение об ошибке. Данные, расположенные вне профиля нельзя защитить от неавторизованного доступа.

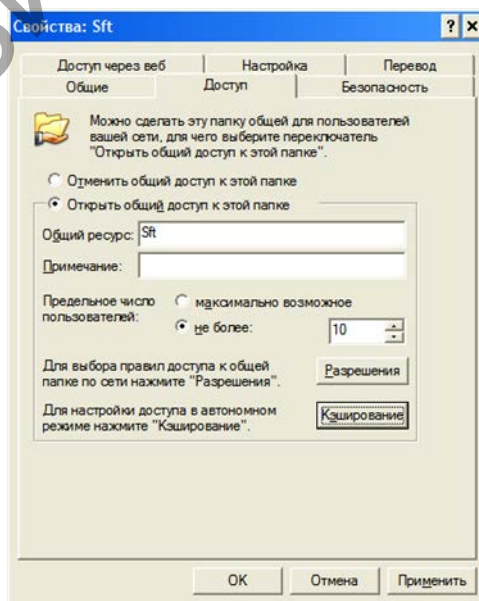
Папка *Общие документы* (SharedDocuments\$) совпадает с папкой AllUsers\Документы. Она доступна ограниченному локальным учетным записям на чтение и открытие с запретом на изменение и создание. Для компьютера в составе домена Windows *Общие документы* не создаются.

Создание общего ресурса выполняется в проводнике: папка может быть выделена в совместное использование на чтение и выполнение либо Изменить (запись Все имеет полный доступ).



Параметр выделения в общий доступ запрещен для системных папок Documents and Settings, Program Files и Windows. Кроме того, нельзя предоставлять общий доступ к папкам из профилей других пользователей.

Простой общий доступ (ПОД) к сетевым ресурсам Windows XP осуществляется под учетной записью Гость (точнее группой Все), которая по умолчанию отключена.



ВПОД разрешения устанавливаются только на уровне папок, можно запретить просмотр другим личных папок пользователя, меньше параметров безопасности, отсутствует вкладка безопасность. В свойствах сетевого под-



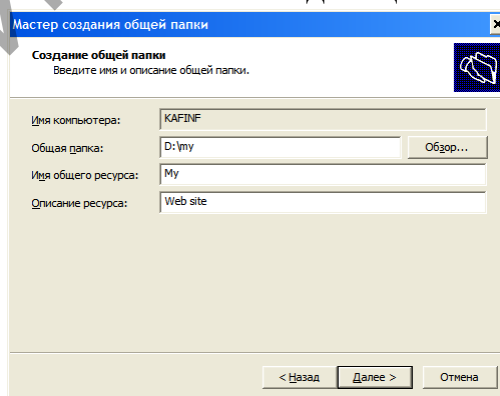
ключения устанавливается служба доступа к файлам и принтерам сетей MS. В системных службах требуется запустить службу сервера, от которой зависит обозреватель компьютеров. Папка Общие документы (SharedDocs) при выделении в совместное использование становится доступной в сети на изменение. В такой модели нельзя предоставить доступ к папкам ProgramFiles, Windows (только к вложенным в них папкам).

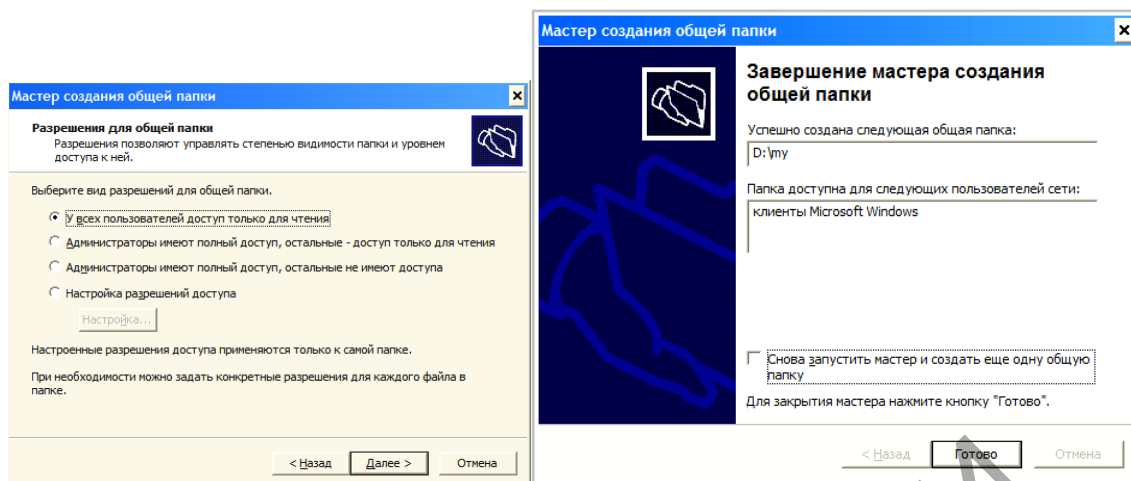
Имя совместного ресурса со знаком \$ в конце скрывается на клиентских узлах под управлением ОС Windows, из среды операционных систем Linux и MacOS просматриваются. Мастер настройки сети позволяет включить простой общий доступ, активизирует учетную запись Гость, разрешает гостю доступ к компьютеру по локальной сети. Под этой записью все пользователи сети имеют доступ. В этом режиме нельзя просматривать списки управления доступом. При использовании брандмауэра Windows просмотр общих ресурсов может ограничиваться.

При включенном классическом общем доступе полномочия доступа можно уточнить путем задания разрешений на уровне пользователей или групп и настройки доступа в автономном режиме.

После переключения с простого общего доступа к папке на классический, все гости продолжают работу с ней как владельцы. В этом случае для запрета группе Все разрешения владельца нужно стать владельцем папки и ее содержимого и удалить группу Все из списка управления доступом для папки и ее содержимого.


Перемещение файлов или папок в пределах одного диска сохраняет разрешения, но пользователь становится их владельцем.






### Окна мастера создания общей папки

Второй способ создания общих папок выполняется из менеджера управления компьютером. В ветви Общие папки ► Общие ресурсы выбирают создание нового общего ресурса с запуском мастера создания общей папки. Требуется разрешить изменение файлов по сети, иначе их нельзя создавать или сохранять. В менеджере можно просмотреть перечень всех выделенных ресурсов, существующие сеансы подключения к ресурсам, открытые документы. Для отключения сеансов или открытых файлов можно удалить пользователя, предварительно пошлав ему из меню консольное сообщение: Все задачи ► Отправка сообщения консоли. Предварительно требуется включить службу сообщений Alerter (оповещателя) и Messenger.

 Выделите в совместное использование ресурсы с учетной записью рядового пользователя, администратора. Выделите сетевой ресурс на доступ в сети на чтение и изменение.

Включите использование автономных файлов на компьютере, предварительно отключив быстрое переключение пользователей.

 Добавьте сетевые файлы для кэширования в папке автономных файлов. Просмотрите содержимое папки автономных файлов.

Отключите использование папки автономных файлов.

Выделение ресурсов в совместное использование можно выполнять из командной строки:

Netshare имя ресурса=диск:путь.

Можно добавить следующие ключи:

/GRANT:admin, Read|CHANGE|full;

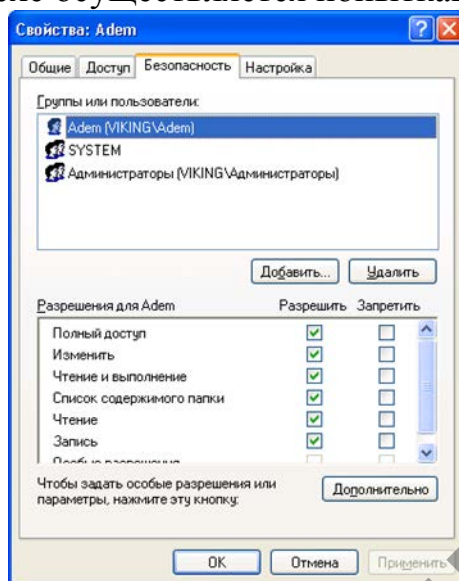
/unlimited|/user:10 /|/remark:"Для всех" /delete;

/CASHE:Manual| Document | Programs | None;

Net use \\503-15-14\work пароль /user:student.

Настройка локального классического общего доступа выполняется через свойства папки вкладки безопасности. Он всегда включен, если компьютер подключен к домену. В современных системах он включен по умолчанию.

нию. Попытка подключения сначала осуществляется с представленной учетной записью, при неуспехе осуществляется попытка входа в качестве гостя.



Разрешения для совместного используемых ресурсов по сети и разрешения NTFS работают на разных уровнях. Соответственно используются вкладки доступа и безопасности. Если применяются оба этих типа разрешений, то сначала применяются разрешения сетевого ресурса, затем разрешения NTFS могут только сузить (не расширить) сетевые разрешения.

Принтеры также могут выделяться в совместное использование. Для них не поддерживаются разрешения ресурса и разрешений NTFS. Единый набор разрешений по сети и локально. Папки очереди печати располагаются локально в Print\Printers\DefaultSpoolDirectory.

Папка очереди печати задается для всех локальных принтеров в реестре HK\_LM\Software\MS\WindowsNT\CurrentVersion\Print\Printers\DefaultSpoolDirectory\EpsonLx 300\SpoolDirectory.

Настройка порта для 16-разрядного драйвера печати из командного процессора можно выполнить командой

```
Net use lpt1: \\123-ПК\EpsonLx 300.
```

Приведем правила для применения полномочий NTFS:

1. Скопированные файлы или папки получают полномочия папки назначения, пользователь становится владельцем (может изменять разрешения доступа к ФП).
2. Перемещение файлов или папок в пределах одного диска с NTFS сохраняет исходный список доступа, пользователь становится владельцем.
3. Перемещение файлов или папок на другой диск с NTFS приобретает разрешения папки назначения, пользователь – владелец.
4. Копирование или перемещение файлов или папок с диска с файловой системой FAT32 на диск с системой NTFS изменяет разрешения на разрешения папки назначения, пользователь становится владельцем.

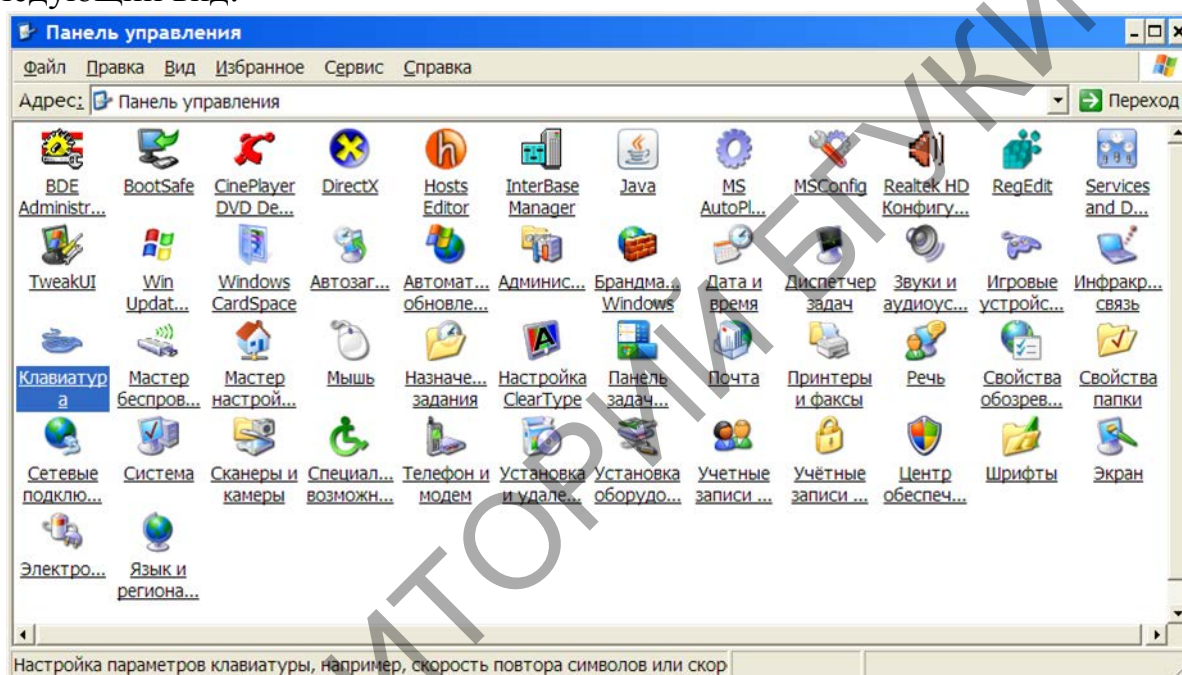
5. Копирование или перемещение файлов или папок на диск FAT32 требует исходные списки доступа.

6. Полномочие запрета имеет приоритет перед любыми разрешениями.

7. После преобразования диска в NTFS группа Все имеет к нему полный доступ.

#### Элементы панели управления

Панель управления используется для настройки среды операционной системы и оборудования компьютера. В кратком виде панели отображаются несколько категории элементов. В подробном представлении ее окно имеет следующий вид:



В ее составе: оформление и темы, сетевые подключения, установка и удаление программ, звуки и аудиоустройства, производительность и обслуживание, принтеры и факсы, учетные записи.

Ограниченные пользователи могут управлять лишь своей учетной записью, задавать свой паспорт .NET. Панель используется при настройке доступа к электронной почте и доступе к сайтам с номерами кредитных карт.


Включите быстрое переключение пользователей. Требуется около 64 Мбайт ОЗУ на каждого пользователя.

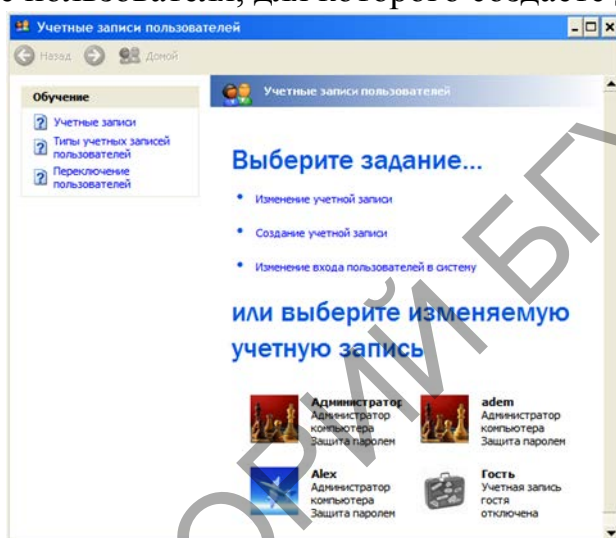
В окне Добро пожаловать в Windows требуется нажать сочетание клавиш Ctrl+ Alt+ Del для вызова окна Входа в систему. Имеется окно безопасности Windows, диспетчера задач Windows (Ctrl+ shift+ Esc). Включение учетной записи позволяет от ее имени выполнять приложения. Для добавления ее на экран приветствия отмените для нее запрет на локальный вход в систему.


Учетные записи пользователей отображаются на экране приветствия, в главном меню и в папке пользователей. Имя пользователя отображается в окне входа, командах и диалоговых окнах разрешений. Учетные записи могут


иметь пароль и подсказку для пароля. Имеется изображение приветствия, указывается тип учетной записи при задании пароля обращения к сетевым ресурсам, при создании диска сброса пароля.

Скрытые учетные записи не отображаются на экране приветствия. Для хранения паролей используется функция хеширования. Пароли служебных записей, кроме System, в незашифрованном виде присутствуют в разделе реестра LSASecrets. В связи с этим рекомендуется групповой политикой запретить интерактивный вход в систему со служебной учетной записью.

 Создайте дискету сброса пароля. Войдите в учетные записи пользователей, выберите пользователя, для которого создаете дискету (флешку).




 Воспользуйтесь дискетой сброса пароля для смены пароля пользователя. Смену пароля можно выполнить через экран входа в систему или экран приветствия.

 Смените визуальные эффекты с помощью элементов панели управления экран и система.

Имеются элементы Дата и время, Язык и региональные стандарты, Специальные возможности.

Управление пользовательскими профилями выполняется через элемент панели управления с названием система. Выбирают вкладку дополнительно и затем кнопку параметров. Каждому профилю отвечает раздел реестра

HK\_LM\Software\MS\WindowsNT\CurrentVersion\Profilelist.

 Отключите автоматическую перезагрузку компьютера при отказе системы.

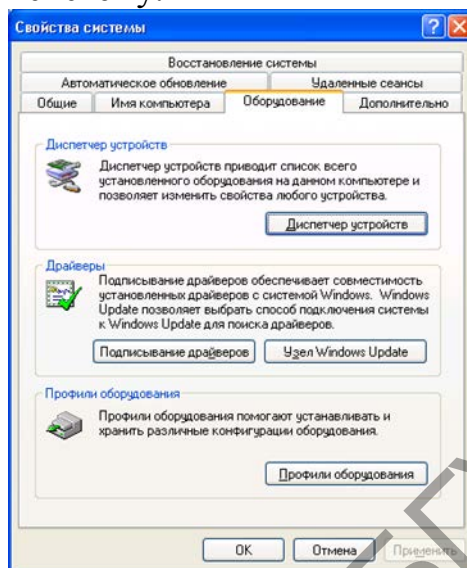
Через реестр включение экрана приветствия доступно только в составе рабочей группы, например, следующим заданием параметра:

HK\_LM\Software\Windows NT\CurrentVersion\WinLogon\LogonType = 1 (=0).

Экран приветствия можно включить через групповую политику (Административные шаблоны\Система\Вход в систему), и задать Всегда использо-




вать классический вход в систему. Чтобы добавить запись на экранприветствия нужно в панели управления включить ее, что удаляет запрет для учетной записи на локальный вход в систему.





Доступ к управлению аппаратным обеспечением компьютера выполняется через элемент панели управления Система, вкладка Оборудование. Здесь доступна установка драйверов и их обновление. После обнаружения нового устройства и считывания его идентификатора PnP он сравнивается с содержимым основного списка идентификаторов всех информационных файлов \*.inf из папки inf и устанавливается подписанный драйвер. В нем сведения об устройстве, название файлов драйвера, их размещение после установки, параметры реестра и подобное. В противном случае запускается мастер нового оборудования. Возможны проблемы подключения звуковой карты, сетевого адаптера или устройств, подключаемых через ISA шину.

Драйвер – управляющая программа, подключающаяся к ядру ОС и выполняющая основные задачи по взаимодействию с оборудованием – передаче данных от пользователя к устройству и обратно. Все драйверы устройств для установки в Windows должны обладать информационным установочным файлом Windows\Inf\\*.inf именами файлов драйверов, их расположением после установки, требуемыми настройками реестра и номером версии. Драйвер с цифровой подписью выделен зеленой галочкой.

В диспетчере устройств в пункте меню видается команда показать скрытые устройства (не удовлетворяющие стандарту Plug and Play).

 Задайте профили оборудования с выбором в процессе загрузки ОС для переносных компьютеров. Выведите список всех драйверов системы с использованием команды

 `driverquery /v /focsv>dwlist.csv` (в Excel формате).  
Файлы драйверов располагаются в папке Windows\system32\drivers.

 Настройте автоматический вход в систему. В разделе реестра HK\_LM\Software\MS\WindowsNT\CurrentVersion\Winlogon задайте параметры:


```
AutoAdminLogon=1;  
DefaultUserName= student;  
DefaultPassword=*****
```

Можно выполнить команду Controluserpasswords2 (пользователь, требовать ввод имени пользователя).

Управление электропитанием актуально выполнять для ноутбуков и систем, работающих без подключения к силовым сетям. В свойствах электропитания настраивают запрос пароля при пробуждении, действие кнопок питания, настраивают план электропитания, отключение дисплея и сохранение данных при переходе в спящий режим:

????.

Для того чтобы управление электропитанием работало, требуется согласование его функций в BIOS и наличие ACPI BIOS. Стандартом работы BIOS является интерфейс автоматического управления конфигурацией и питанием (ACPI). При наличии APM BIOS (Advanced Power Management) управление электропитанием осуществляется совместно средствами операционной системы и BIOS. В ждущем режиме может отключаться питание жесткого диска, вентиляторов, процессора, подача питания на ОЗУ. В спящем режиме содержимое ОЗУ, в том числе часть таблицы размещения файлов, сохраняется на жестком диске, питание всех устройств отключается. При выходе из спящего режима содержимое ОЗУ считывается с жесткого диска в память и можно продолжить работу. Нельзя загружаться из спящего режима в другую операционную систему.

 Выполните принудительный переход в состояние сна или гибернации через главное меню, в ждущий режим (Shift спящий режим), в режим гибернации.

Системные службы выполняют важную роль в настройке возможностей компьютера на выполнение практических задач пользователя. Они могут взаимодействовать с разработчиками программного обеспечения, сетями и сервисами. Служба – программа или процесс, выполняющий конкретную системную функцию по поддержке других программ, особенно на низком, близком к аппаратному уровню. Для управления ими используется инструмент администрирования с названием службы. В его окне для службы отображается имя, описание, состояние службы и вход от имени.

Администратору нередко требуются дополнительные имена, связываемые со службой: отображаемое имя в средстве администрирования, основное имя в окне свойств службы при выбранной вкладке Общие (используется в

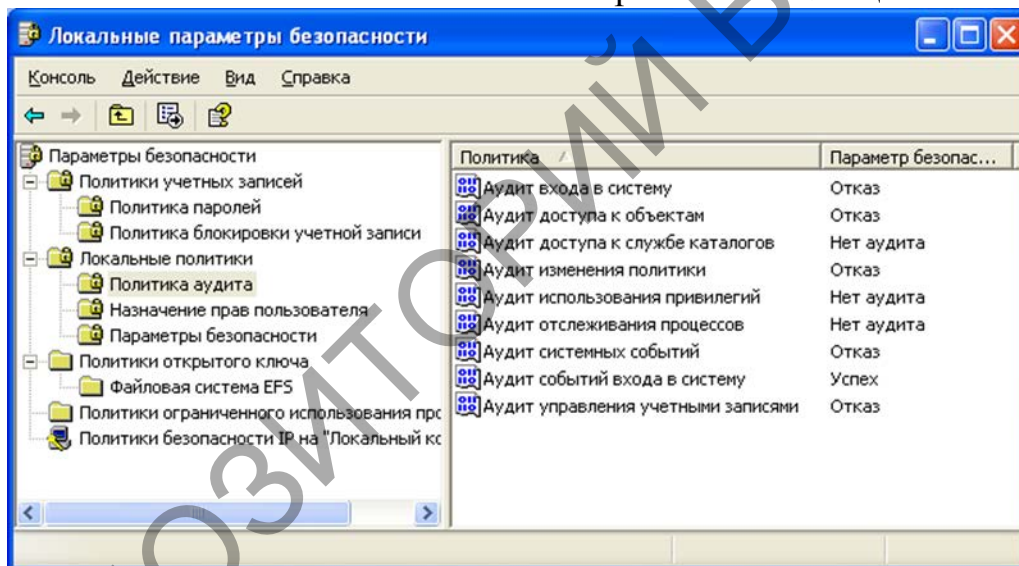
строке подсказки), имя исполняемого файла (отображается в окне диспетчера задач Windows). Параметры реестра для службы отображаются в подразделе HK\_LM\System\CurrentControlSet(001)\Services\имяслужбы.

HK\_LM\System\ControlSet001\Services\ имяслужбы, где задаются параметры системных служб. Параметр Dwordstart =2 (automatic), =3 (Manual), =4 (Disable).

Служба времени Windows синхронизирует время и дату компьютеров сети с выбранным сервером времени. Общее время контролируется протоколом Kerberos при проверке подлинности. Она использует простой сетевой протокол времени SNTP :132 (SimpleNetworkTimeProtocol). В домене сервером времени является контроллер домена, последние согласуют время с вышестоящими серверами в дереве доменов, корневой сервер – с сервером Морской обсерватории США.

Приведем команду синхронизации времени: `nettime\sv-bguki /y/set`

Локальная политика безопасности настраивается в специальном окне:



Оснастка локальной политики безопасности применяется для прямого изменения политик учетных записей и локальных политик, политик открытого ключа, а также политик безопасности IP локального компьютера. Для отслеживания и просмотра журнала событий необходимо задать политику аудита, которая определяет типы событий, которые заносятся в журналы.

По умолчанию готовые шаблоны безопасности сохранены в папке: `Windows\Security\Templates\*.inf`

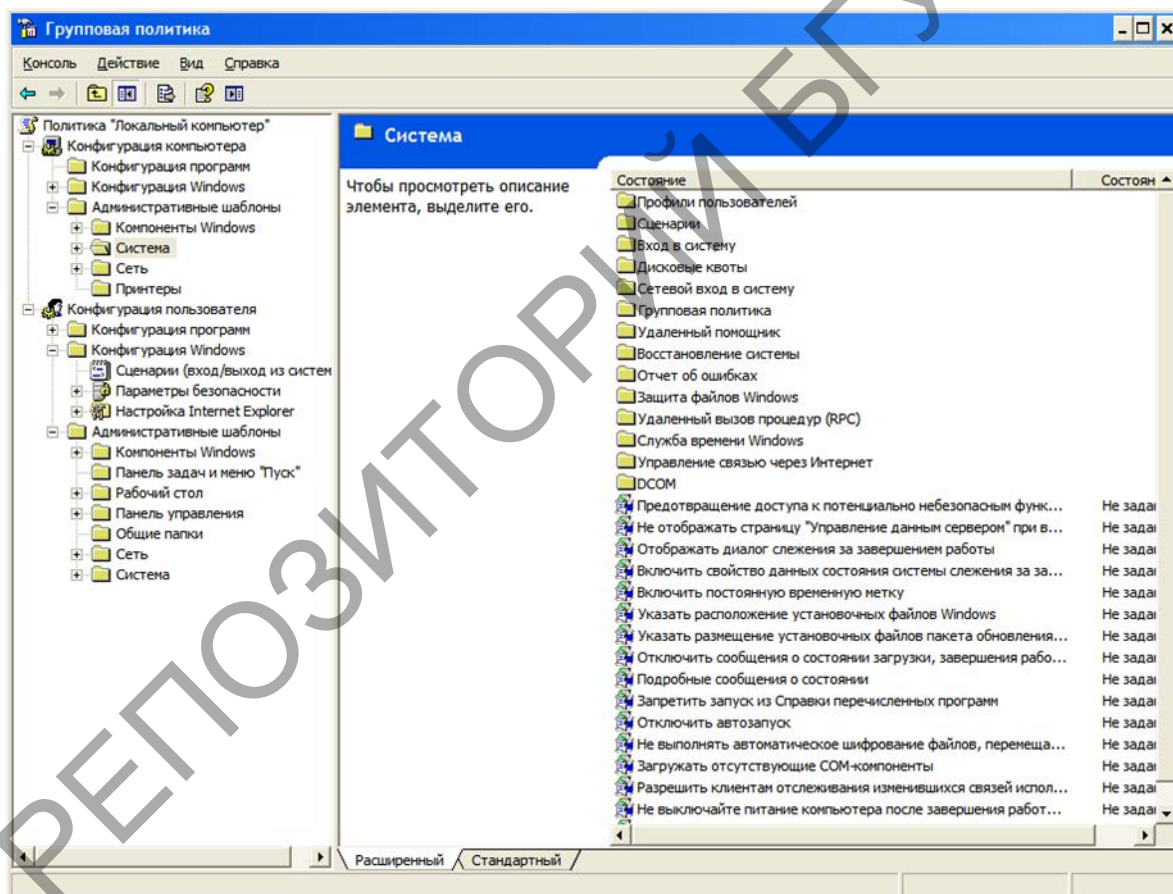
Файл шаблона `Setupsecurity.inf` задает параметры безопасности, используемые по умолчанию, которые применяются во время установки операционной системы, включая разрешения для файлов корневого каталога системного диска. В шаблоне `Secure*.inf` определяются параметры повышенной безопасности.



Файлы hisec\*.inf задают повышенную защиту, налагающую дополнительные ограничения на уровни кодировки и подписи, необходимые для проверки подлинности и для данных, передаваемых по безопасным каналам между клиентами SMB и серверами. Безопасность системного корневого каталога задается файлом Rootsec.inf.


Оснастка групповой политики отсутствует в папке администрирования из меню пуска. Она запускается на выполнение командой gpedit.msc и политику конфигурации компьютера и пользователя.

Существует два типа объектов групповой политики. *Нелокальные объекты* групповой политики хранятся на контроллере домена и доступны только в среде ActiveDirectory. Они применяются к пользователям или компьютерам в сайте, домене или подразделении, связанном с объектом групповой политики.




Локальные объекты групповой политики хранятся на локальном компьютере. На компьютере существует только один локальный объект групповой политики, содержащий набор параметров, доступных в нелокальном объекте групповой политики. В случае конфликта, параметры локального объекта будут перезаписаны нелокальными параметрами или применены совместно. В локальных объектах групповой политики не поддерживается политика перенаправления папок и установки программного обеспечения. Локальный

объект групповой политики расположен по адресу *Windows\System32\GroupPolicy\*, где имеются папки *Machine* и *User*.

 Запретите использование редактора реестра. Задайте в ветви Административные шаблоны + Система ► Сделать недоступными средства реестра.

Групповая политика дает возможность ограничить пользователей по внесению изменений, централизованно устанавливать программное обеспечение, настраивать, обновлять, удалять программы. Она может управлять автоматическим выполнением сценариев, перенаправлять папки пользователей, например, мои документы в сетевые папки. Эти действия можно выполнять локально на компьютере для групп пользователей, в домене – на уровне групп, организационных подразделений и сайтов, компьютеров. По сравнению с редактированием реестра это проще в использовании и обеспечивает периодическое автоматическое обновление политик. Параметры групповой политики имеют приоритет перед параметрами пользователей из их профилей. При инициализации операционной системы и периодическом обновлении компьютера параметры групповой политики компьютера копируются в раздел реестра *HK\_LM*, при входе в среду пользователя – в раздел *HK\_CU*.

Файл системной политики для пользователя *ntuser.pol* хранится на контроллере домена. По умолчанию файлы *register.pol* копируются в реестр каждые 90 минут + 0-30 минут, чтобы при доменной политике не перегружать сеть. Результирующий набор политик получаем применением: параметров локального объекта групповой политики; параметров объектов групповой политики сайта в последовательности, указанной администратором; параметров групповой политики домена в своей последовательности; параметров групповой политики подразделений от родительских к дочерним.

 Планировщик пакетов службы контроля допуска QoS сети резервирует для своих нужд 20% пропускной способности канала. Если просто удалить, то канал не освобождается. Нужно это выполнить через групповую политику: Выбираем ветвь Сеть ► Диспетчер пакетов QoS и указываем Ограничить резервную пропускную способность 0% (по умолчанию 20%). Команда *Groupdate* используется для обновления групповых политик немедленно:

```
GPUpdate [/Target:{Computer | User}] [/Force] [/Wait:<значение>]
[/Logoff] [/Boot] [/Sync].
```

Команда *GPresult.exe* выдает эффективные параметры групповой политики для конкретного пользователя или компьютера:

```
GPRESULT [/S <система> [/U <пользователь> [/P <пароль>]
[/USER <имя_конечного_пользователя>]
[/R | /V | /Z] [(/X | /H) <имя_файла> [/F]]
```

 Выполните программу формирования отчета групповой политики операционной системы: `GPRESULT /R`.

Запуск редактора групповой политики удаленного компьютера выполняется командой:

`gpedit.msc/gpcomputer:"503-15-14"`.

Папка `GroupPolicy\Userc Registry.pol`– содержит параметры реестра для всех пользователей (компьютера). Файлы *административных шаблонов* хранятся в папке `System32\GroupPolicy\Admi` влияют на отображение политик в окне редактора GP, но не на значения этих политик. Операционная система включает следующий набор файлов в папке шаблонов администрирования:

`conf.adm`;

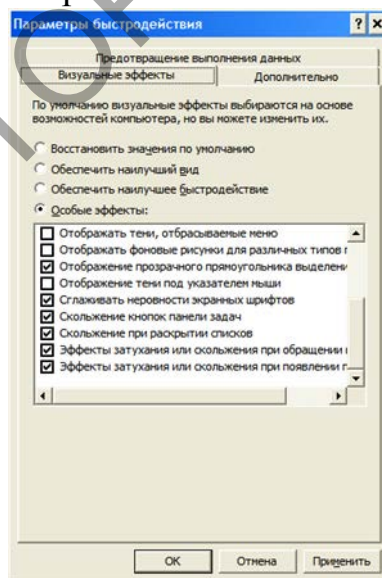
`Inetcorp.adm`, `Inetset.adm`– параметры IE, используемые IE Administration Kit;

`inetres.adm`– параметры IE групповой политики;

`system.adm`– параметры Windows XP из групповой политики;

`Wmplayer.adm`– параметры пользователя для Windows Media.

Производительность системы и быстродействие компьютера может зависеть от его настроек через элемент Свойства системы + Дополнительно, Быстродействие, кнопка Параметры:

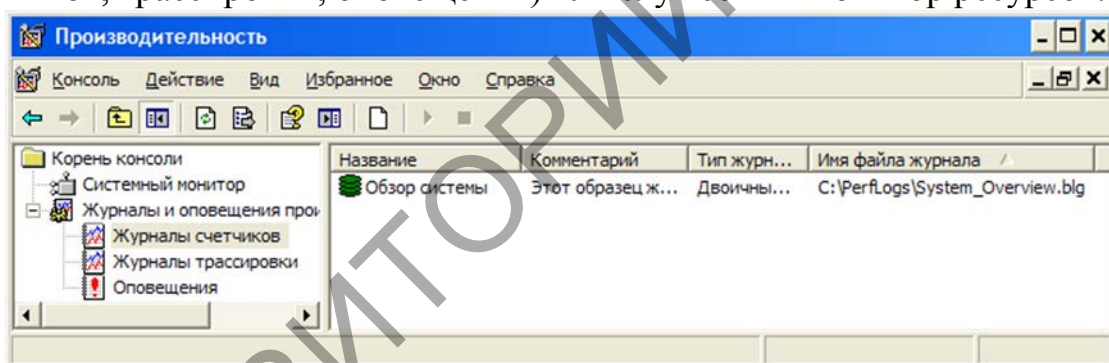


Диспетчер задач операционной системы отображает сведения о ресурсах: приложения, процессы, быстродействие, сети, пользователи. Просмотр доступен в сжатом и полном представлении окна. Процессы инициируются программами, службами и подсистемами. Для отображения списка пользователей включаем быстрое переключение пользователей и запускаем службу терминалов.

Просмотр параметров производительности можно выполнить через диспетчер задач, на вкладке быстродействия. Он предназначен для сбора сведе-

ний о производительности системы с вкладками: память, процессор, автозагрузка, службы. Память разделяется на физическую и виртуальную на жестком диске, которая занимает 1,5-3 объема физической памяти. Системный кэш – часть физической памяти для кэширования часто вызываемых программ и данных. Память ядра – часть ОЗУ, занимаемая основными компонентами операционной системы и драйверами. Выгружаемая (paged) – часть памяти ядра, отображенная в виртуальную. Невыгружаемая – часть памяти ядра, которая не может быть перенесена в виртуальную. Файл подкачки может иметь параметры минимальный или максимальный размер, может располагаться на нескольких физических, но не логических дисках. Файл hiberfil.sys используется для сохранения ОЗУ на случай переключения электропитания компьютера в спящий режим, совпадает по размеру с ОЗУ. Приоритеты процессов изменяются от реального времени до низкого, команда SetAffinity назначает выполнение процесса только одному процессору.

Более подробные сведения о производительности выдает инструмент администрирования ► Производительность (системный монитор, журналы счетчиков, трассировки, оповещения) или служебный монитор ресурсов.



Инструмент администрирования управление диском позволяет назначить буквы томам жесткого диска, съемным устройствам и приводам CD, DVD, изменять активный раздел, чтобы с него загрузить операционную систему, например, ОС Linux. Буквы назначаются в порядке их подключения, в том числе и CD, DVD дисководом. Букву системного и загрузочного диска можно изменять лишь через реестр непосредственно. Можно к диску подключить том, который отображается как папка NTFS. Для увеличения их объема разрешено расширять только простые тома и составные на динамических дисках. Не доступно объединение чередующихся томов или разделов на базовых дисках. Нельзя расширять системный или загрузочный том. Для этих целей используются *утилиты* командной строки fsutil, diskpart. Нужно учитывать наличие системных файлов WindowsXP Safeboot.fs, \*.csv, \*.rsv, Memory.dmp


#### Аудит событий

В среде операционной системы ведутся журналы событий приложений C:\WINDOWS\system32\config\AppEvent.Evt, событий-

безопасности (SecEvent.Evt), событий системы (SysEvent.Evt), которые регистрируются в журналах службой журналов событий (event.log). Управление и просмотр выполняется административным инструментом просмотра событий.

В разделе HK\_LM\System\CurrentControlSet\Services\Eventlog\Application (Security, System) имеется перечень всех объектов, способных породить события (ошибка, предупреждение, уведомление). Возможна установка размера журнала, времени сохранения событий, их архивация и очистка.

Аудит доступа к файлам и папкам можно устанавливать в проводнике после отключения простого общего доступа на компьютере, вкладка Безопасность (кнопка дополнительно). В аудит можно включить пользователя или группу с регистрацией успехов, отказов. Аналогично выполняется аудит событий для конкретного принтера. Обычные события принтеров (завершение печати, удаление задания) фиксируются в журнале Система.

 Выполните архивацию журнала событий, обработку заполненных журналов. Профильтруйте события в журналах для поиска ошибок, предупреждений, критических событий и сведений.

### Реестр

Реестр – это двоичная иерархическая база данных, в которой хранятся все настройки конфигурации системы в иерархической структуре. Это данные о компьютере, оборудовании, периферийных устройствах, установленном программном обеспечении и пользователях, имеющих вход. Приложения, компоненты ОС, драйверы устройств и ядро ОС пользуются реестром, чтобы хранить свои настройки, читать их, получать информацию о конфигурации аппаратных средств. Здесь хранится база данных защиты и конфигурационные настройки на каждого пользователя, стандартные настройки по умолчанию. Реестр хранится в памяти, имеет динамические данные, формируемые при каждой загрузке, и долговременные, которые хранятся на диске в нескольких файлах.

Имеются особенности использования редактора реестра в 64-разрядной версии Windows XP. Реестр в 64-разрядной версии Windows XP поделен на 32-разрядный и 64-разрядный разделы. Большинство 32-разрядных разделов имеют те же имена, что и их аналоги в 64-разрядном разделе, и наоборот. По умолчанию в 64-разрядной версии редактора реестра, поставляемой в 64-разрядной версии Windows XP, отображаются только 64-разрядные разделы.

Чтобы запустить 32-разрядную версию редактора реестра для просмотра 32-разрядных разделов выполните команду REGEDT32.EXE. Его 64-разрядная версия запускается по команде %systemroot%\syswow64\regedit.


Перед запуском 32-разрядной версии редактора реестра необходимо закрыть 64-разрядную версию программы, и наоборот. Работа с 64-разрядной и 32-разрядной версиями редактора реестра не различается.

Экспорт реестра или его раздела из редактора выполняется в файл реестра в формате Unicode\*.reg, файлы кустов реестра могут быть в двоичном формате, текстовые файлы.

В следующей таблице представлен список разделов реестра:

Папка/стандартный раздел	Описание
HKEY_CURRENT_USER	Данный раздел является корневым для данных настройки пользователя, вошедшего в систему в настоящий момент. Здесь хранятся папки пользователя, цвета экрана и настройки панели управления. Эти данные называются профилем пользователя.
HKEY_USERS	Данный раздел содержит все профили пользователей компьютера. HKEY_CURRENT_USER является подразделом HKEY_USERS.
HKEY_LOCAL_MACHINE	Раздел содержит данные настройки, относящиеся к данному компьютеру (для всех пользователей).
HKEY_CLASSES_ROOT	Данный раздел является подразделом HKEY_LOCAL_MACHINE\Software. Хранящиеся здесь сведения обеспечивают открытие необходимой программы при открытии файла с помощью проводника.
HKEY_CURRENT_CONFIG	Данный раздел содержит сведения о профиле оборудования, используемом локальным компьютером при запуске системы.

С использованием редактора реестра выполняется множество тонких настроек параметров системы. Приведем некоторые из них, наиболее часто используемые.

 Поддержка русской кодировки в DOS-приложениях выполняется следующим образом. Открываем реестр, находим ключ HKEY\_LOCAL\_MACHINE\SYSTEM\CurrentControlSet\Control\KeyboardLayout\DosKeybCodes и изменяем его значение 00000409 на "ru".

После этого открываем файл `autoexec.nt` в папке `%SystemRoot%\system32` и добавляем строку

```
lh %SystemRoot%\system32\kb16.com ru
```

Перезгружаем компьютер и убеждаемся, что теперь в DOS-приложениях переключение на русскую раскладку происходит по нажатию `Ctrl + Right Shift`, на английскую – `Ctrl + Left Shift`.

 Задайте свойства клавиатуры при входе в систему:

[HKEY\_USERS\DEFAULT\KeyboardLayout\Preload]и для изменения языка ввода по умолчанию измените значения параметров:

"1"="00000409" –Английская (США), основная

"2"="00000419" – Русская, дополнительнаяLogonUserName.

Приведем описание некоторые типов файлов при работе с реестром: `*.alt`–резервная копия куста, `*.log`– хранит изменения в кусте в течение последнего сеанса работы, `*.sav`– копия данных куста на момент завершения запуска Windows.

Папка `%systemroot%\prefetch`используется для ускорения запуска недавно использовавшихся программ.Это тормозит загрузку системы. Если важнее скорость загрузки системы, выполните следующее. Чтобы отключить эту функцию, находим путь

HK\_LM\SYSTEM\CurrentControlSet\Control\SessionManager\MemoryManagement\PrefetchParameters,создаемпараметрEnablePrefetchегиприсваиваемему значение0.

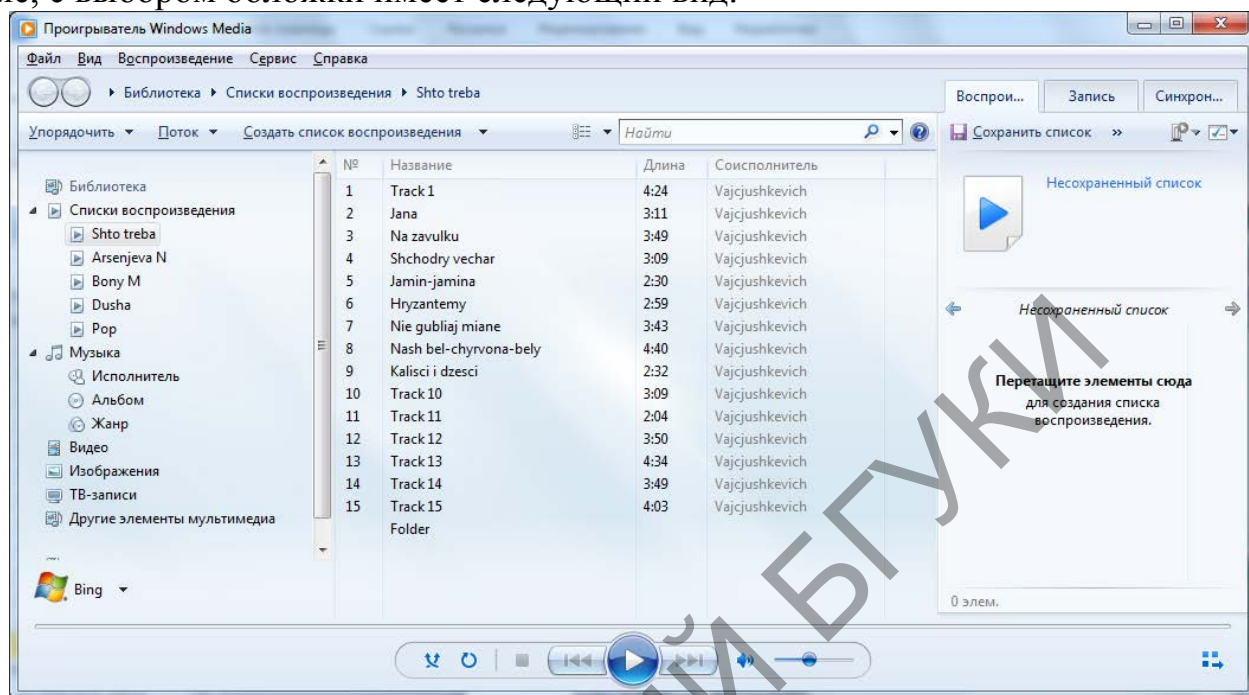
Опишем кратко схему загрузкиоперационной системы после включения компьютера. После тестирования оборудования, выбора раздела загрузки системы, ядро и HAL запускают *исполнительную систему* ОС Windows, основная часть которой содержится в `win.com`. Используемая система читает из реестра конфигурацию оборудования и запускает драйверы и службы. Ядро запускает программу `SessionManager(smss.exe)`, которая переключает операционную систему из текстового режима в графический. Запускается менеджер входа в систему (`winlogon.exe`), создается файл подкачки. Менеджер входа в систему запускает подсистему сервисов (`services.exe`) и локальную систему безопасности (`lsass.exe`), выводит экран приветствия или окно входа в систему. После входа пользователя в систему загружается оболочка операционной системы (`explorer.exe`)и выполняется автоматический запуск дополнительных программ.

### Проигрыватель WindowsMedia

Проигрыватель воспроизводит цифровое мультимедиа, звуковые файлы различных форматов, видео с DVD, принимает звуковые и видео потоки из Интернета. Он позволяет прослушивать Интернет-радиостанции, копировать дорожки с CD/DVD на диск в формате `wma64` Кбит/с, в формате MP3, запи-



сывать на DVD-диски, загружать звуковые файлы на MP3-плеер, прослушивать в заданной или случайной последовательности. Его окно в полном режиме, с выбором обложки имеет следующий вид:



Элементы окна проигрывателя:

- панель задач с видом – библиотека, списки воспроизведения, музыка, видео, изображения, ТВ-записи, другие изображения.
- список воспроизведения для выбранного списка,
- панель с вкладками записи, воспроизведения и синхронизации, которая может использоваться для создания списков воспроизведения,

Имеется набор видов: режим библиотеки, обложки, текущего списка воспроизведения, Интернет-магазины.

Имеются элементы управления воспроизведением. Видео и зрительные образы – цветовые анимации, изменяющиеся согласованно с частотой и амплитудой звука, выбор обложки. Дополнительные возможности – выбор цвета, плавный переход и автовыравнивание громкости, графический эквалайзер, ссылки мультимедиа для электронной почты, настройка скорости воспроизведения, тихий режим, эффекты и настройка видео.

Создайте пользовательский список воспроизведения, выполните его экспорт в файл \*.asf, импорт в библиотеку мультимедиа (\*.wav, \*.m3u, \*.wvx, \*.wmx). Файл Folder.jpg используется в качестве обложки альбома для проигрывателя.

При задании параметров проигрывателя имеются вкладки проигрывателя, копирования музыки, устройств, записи, конфиденциальности, безопасности, DVD, сети, быстрого действия, библиотеки и подключаемых модулей.



Обычно устанавливаются дополнительные кодеки, которые используются для сжатия и распаковки цифрового мультимедиа в процессе его обработки.

#### Составные документы

OLE технология – способ обмена и совместного использования данных приложениями посредством вставки объекта из одного приложения в другое. Связанные объекты содержат только поле и обрабатываются в окне приложения–сервера, состоят из своих базовых данных, содержат объекты, созданные другими приложениями. Объект – не только данные, но и действие по созданию, доступу и использованию. Имеется приложение сервера, приложение контейнера, статическое перемещение и копирование. При связывании объекта в составном документе хранятся сведения о приложении сервера. Связанный объект содержит:

- Ключ реестра для вызова приложения сервера объекта;
- Метафайл GDI – инструкций образа объекта;
- Указатель на файл источник и приложение сервера.

Технология позволяет обновлять изменения из источника при открытии документа либо открытом, поддерживает отключение режима автоматического обновления. Изменение выполняется в исходном приложении.

Внедренные объекты хранятся в приемнике, содержат ту же информацию, обрабатываются на месте, то есть в окне клиента с переопределением меню и панелей. Они увеличивают размер документа, но не зависят от перемещения источника и контейнера. Внедрение путем выполняется перетаскивания, через буфер обмена.

Механизм динамического обмена данными DDE не хранит информацию в объекте–приемнике, а только имя приложения источника, имя документа и его конкретной части (поле). Документ, управляемый и обрабатываемый приложением–контейнером, содержит несколько внедренных объектов.

#### Команды связывания

В офисных приложениях имеется Специальная вставка + Связь. Нельзя вставлять часть BMP–файла в качестве связанного объекта.

Команда вставки объекта имеет варианты: поверх текста, в виде значка, создание из файла. Управление связями документа контейнера осуществляется командой правки Связь.

Имеются режимы обновления: автоматический или ручной, обновить теперь, изменить источник, прервать связь.

Технология OLE1 использует абсолютные адреса объектов, объекты обрабатываются в окне сервера, нет вложенных объектов. Технология OLE2 использует относительные адреса, обрабатывает объекты на месте, приложение–сервер изменяет меню и панели инструментов приложения–клиента, по-

зволяет внедрять объекты внутрь других объектов, поддерживает операции перетаскивания мышью, связи могут быть глобальными и (сетевыми) с записью на языке VBA, механизм обновления связей для версий приложений, функции конвертирования объектов.

#### Внедренный объект

Представление вставленных в документ данных, созданных в другом приложении без установления связи. Механизм внедрения позволяет изменять внедренные данные с помощью меню и панелей инструментов программы, в которой они были созданы.

Чтобы изменить внедренные данные, укажите на них и выполните двойной щелчок. На экране появятся меню и панели инструментов программы, в которой они были созданы. При внедрении данных из одного документа в другой связь между документами не устанавливается. Это означает, что изменения данных в исходном документе не отображаются автоматически в новом документе. Внедренные данные необходимо обновлять вручную.

#### Упакованный объект

Значок, представляющий внедренный или связанный объект. Эти данные могут состоять как из документа целиком, например, точечного рисунка, так и его части, например, диапазона ячеек Excel. Когда пользователь выбирает упакованный объект, приложение, в котором был создан объект, либо воспроизводит объект, либо открывает и отображает его на экране.

#### Связанный объект

Связанный объект – вставленный в документ, но остающийся в исходном файле. Связанные данные автоматически обновляются при их изменении в исходном документе. Если требуется изменить связанные данные, дважды щелкните их. На экране появятся меню и панели инструментов программы, в которой эти данные были созданы. Если оба документа находятся на одном компьютере, то изменения, вносимые в связанные данные, будут также отражаться в документе назначения. При изменении исходных данных автоматически обновляются связанные данные.

#### Общее представление о предотвращении выполнения данных

Предотвращение выполнения данных (DEP) используется для предотвращения проникновения на компьютер вирусов и других угроз безопасности, которые выполняют вредоносный код из областей памяти, которые должны использоваться только операционной системой Windows и другими программами. Такой тип угроз безопасности наносит ущерб, занимая по очереди все области памяти, используемые программой. Затем вирус распространяется и повреждает другие программы, файлы и даже контакты электронной почты.

В отличие от брандмауэра или антивирусной программы средство DEP не препятствует установке потенциально опасных программ на компьютер. Вместо этого выполняется наблюдение, чтобы программы использовали системную память безопасным образом. Для этого DEP работает отдельно или вместе с совместимыми микропроцессорами и помечает некоторые области как «невыполняемые». Если программа пытается запустить код (любой код) из защищенной области, DEP закрывает программу и отображает уведомление.

DEP может использовать поддержку программного и аппаратного обеспечения. Для использования DEP на компьютере должна быть установлена операционная система. Для Microsoft Windows XP (SP2) или Windows Server 2003 с пакетом обновления 1 (SP1), или более поздняя версия одной из этих программ. Программное обеспечение DEP используется для защиты от некоторых типов атак вредоносного кода, но для использования возможностей DEP в полном объеме процессор должен поддерживать «защиту от выполнения». Это аппаратная технология, разработанная для обозначения некоторых областей памяти как невыполняемых. Если процессор не поддерживает аппаратную версию DEP, рекомендуется обновить процессор, чтобы использовать возможности защиты от выполнения.

## 3 ПРАКТИЧЕСКИЙ РАЗДЕЛ

### 3.1 Описание лабораторных работ

#### Лабораторная работа 1

#### Интерфейс командной строки и ее команды (4 ч.)

Создайте документ краткой справки по командам командной строки.

Для получения сведений об определенной команде наберите HELP<имя команды>. Ниже приведен список имеющихся команд.

ASSOC – вывод либо изменение сопоставлений по расширениям имен файлов;

ATTRIB – отображение и изменение атрибутов файлов;

BREAK – включение и выключение режима обработки комбинации клавиш CTRL+C;

BOOTCFG – настройка параметров в файле управления загрузкой boot.ini;

CACLS – отображение и редактирование списков управления доступом (ACL) к файлам;

CALL – вызов одного пакетного файла из другого;

CD – вывод имени либо смена текущей папки;

CHCP – вывод либо установка активной кодовой страницы;

CHDIR – вывод имени либо смена текущей папки;

CHKDSK – проверка диска и вывод статистики;

CHKNTFS – отображение или изменение выполнения проверки диска во время загрузки;

CLS – очистка экрана;

CMD – запуск еще одного интерпретатора командных строк Windows;

COLOR – установка цвета текста и фона, используемых по умолчанию;

COMP – сравнение содержимого двух файлов или двух наборов файлов;

COMPACT – отображение и изменение сжатия файлов в разделах NTFS;

CONVERT – преобразование дисковых томов FAT в NTFS. Нельзя выполнить преобразование текущего активного диска;

COPY – копирование одного или нескольких файлов в другое место;

DATE – вывод либо установка текущей даты;

DEL – удаление одного или нескольких файлов;

DIR – вывод списка файлов и подпапок из указанной папки;

DISKCOMP – сравнение содержимого двух гибких дисков;

DISKCOPY – копирование содержимого одного гибкого диска на другой;

DISKPART – отображение и настройка свойств раздела диска;

DOSKEY – редактирование и повторный вызов командных строк; создание макросов;

DRIVERQUERY – отображение текущего состояния и свойств драйвера устройства;

ECHO – вывод сообщений и переключение режима отображения команд на экране;

ENDLOCAL – конец локальных изменений среды для пакетного файла;

ERASE – удаление одного или нескольких файлов;

EVENTQUERY – отображение записей журнала событий, отвечающих заданному критерию;

EXIT – завершение работы программы CMD.EXE (интерпретатора командных строк);

FC – сравнение двух файлов или двух наборов файлов и вывод различий между ними;

FIND – поиск текстовой строки в одном или нескольких файлах;

FINDSTR – Поиск строк в файлах.

FOR – запуск указанной команды для каждого из файлов в наборе;

FORMAT – форматирование диска для работы с Windows;

FSUTIL – отображение и настройка свойств файловой системы;

FTYPE – вывод либо изменение типов файлов, используемых при сопоставлении по расширениям имен файлов;

GOTO – передача управления в отмеченную строку пакетного файла;

GPRESULT – отображение информации о групповой политике для компьютера или пользователя;

GRAFTABL – позволяет Windows отображать расширенный набор символов в графическом режиме;

HELP – выводит справочную информацию о командах Windows;

IF – оператор условного выполнения команд в пакетном файле;

LABEL – создание, изменение и удаление меток тома для дисков;

MD – создание папки;

MKDIR – создание папки;

MODE – конфигурирование системных устройств;

MORE – последовательный вывод данных по частям размером в один экран;

MOVE – перемещение одного или нескольких файлов из одной папки в другую;

OPENFILES – отображение файлов, открытых на общей папке удаленным пользователем;

PAGEFILECONFIG – отображение и настройка свойств файла подкачки;

PATH – вывод либо установка пути поиска исполняемых файлов;

PAUSE – приостановка выполнения пакетного файла и вывод сообщения;

POPD – восстановление предыдущего значения текущей активной папки, сохраненного с помощью команды PUSHD;

PRINT – вывод на печать содержимого текстовых файлов;

PROMPT – изменение приглашения в командной строке Windows;

PUSHD – сохранение значения текущей активной папки и переход к другой папке;

RD – удаление папки;

RECOVER – Восстановление читаемых данных с плохого или поврежденного диска;

REM – помещение комментариев в пакетные файлы и файл CONFIG.SYS;

REN – переименование файлов и папок;

RENAME – переименование файлов и папок;

REPLACE – замещение файлов;

RMDIR – удаление папки;

SET – вывод, установка и удаление переменных среды Windows;

SETLOCAL – начало локальных изменений среды для пакетного файла;

SC – отображение и настройка служб (фоновые процессы);

SCHTASKS – выполнение команд и запуск программ по расписанию;

SHIFT – изменение содержимого (сдвиг) подставляемых параметров для пакетного файла;

SHUTDOWN – локальное или удаленное выключение компьютера;

SORT – сортировка ввода;

SUBST – сопоставляет заданному пути имя диска;

SYSTEMINFO – выводит сведения о системе и конфигурации компьютера;

TASKLIST – отображение всех выполняемых задач, включая службы;

TASKKILL – прекращение или остановка процессов или приложений;

TIME – вывод и установка системного времени;

TITLE – назначение заголовка окна для текущего сеанса интерпретатора командных строк CMD.EXE;

TREE – графическое отображение структуры папок заданного диска или заданной папки;

TYPE – вывод на экран содержимого текстовых файлов;

VER – вывод сведений о версии Windows;

VERIFY – установка режима проверки правильности записи файлов на диск;

VOL – вывод метки и серийного номера тома для диска;

XCOPY – копирование файлов и дерева папок;

WMIC – отображение информации WMI в интерактивной среде.

Воспользуйтесь приведенным списком команд для выполнения операций копирования, удаления, переименования и вывода на печать.

## Лабораторная работа 2

### Запуск программы или команды в отдельном окне

Освойте запуск команд с использованием команды START.

Запуск указанной программы или команды в отдельном окне. Команда START имеет следующий синтаксис:

```
START ["заголовок"] [/Dпуть] [/I] [/MIN] [/MAX] [/SEPARATE |  
/SHARED][/LOW | /NORMAL | /HIGH | /REALTIME| /ABOVENORMAL |  
/BELOWNORMAL][/WAIT] [/B]
```

[команда/программа] [параметры]

Параметры означают следующее:

"заголовок" – заголовок окна;

путь – рабочий каталог;

B–запуск приложения без создания нового окна с отключением обработки сочетания клавиш ^C. Если приложение не обрабатывает сочетание клавиш ^C самостоятельно, единственным способом его прерывания является использование сочетания клавиш ^Break;

I – новой средой станет исходная среда, переданная cmd.exe, а не текущая среда;

MIN – запуск команды/программы в свернутом окне;

MAX – запуск команды/программы в развернутом окне;

SEPARATE – запуск 16-разрядной программы Windows в отдельной области памяти;

SHARED – запуск 16-разрядной программы Windows в общей области памяти;

LOW–запуск приложения с приоритетом IDLE;

NORMAL–запуск приложения с приоритетом NORMAL;

HIGH–запуск приложения с приоритетом HIGH;

REALTIME–запуск приложения с приоритетом REALTIME;

WAIT–запуск приложения с ожиданием его завершения;

ABOVENORMAL– запуск приложения с классом приоритета ABOVE-NORMAL;

BELOWNORMAL– запуск приложения с классом приоритета;

BELOWNORMAL – команда/программа.

Если это внутренняя команда `cmd.exe` или пакетный файл, обработчик команд (`cmd.exe`) запускается с ключом /K. Это означает, что окно не будет закрыто после завершения команды.

Если это не внутренняя команда `cmd.exe` и не пакетный файл, значит это программа, которая будет запущена в графическом или текстовом окне. параметры – Параметры, передаваемые команде/программе.

Изменения вызова внешних команд из командной строки или с помощью команды `START` при включении расширенной обработки команд:

Для вызова неисполняемых файлов через механизм сопоставления типов файлов достаточно просто ввести имя файла в командной строке. Например, команда `WORD.DOC` запускает приложение, сопоставленное расширению имени файла `.DOC`.

Сведения о создании подобных сопоставлений из пакетных файлов приведены в описаниях команд `ASSOC` и `FTYPE`.

При запуске 32-разрядного приложения с графическим интерфейсом пользователя обработчик команд `CMD.EXE` не ожидает завершения работы приложения перед возвратом к приглашению командной строки. Подобное новое поведение не относится к запуску приложений из пакетных файлов.

При выполнении командной строки, первым элементом которой является текстовая строка "CMD" без расширения имени файла или указания пути, она заменяется значением переменной `COMSPEC`. Это предотвращает запуск `CMD.EXE` из текущей активной папки, если таковая программа там имеется.

Если первый элемент командной строки не содержит расширения имени файла, обработчик команд `CMD.EXE` использует значение переменной среды `PATHEXT`, чтобы определить расширения имен исполняемых файлов и порядок поиска нужного файла. По умолчанию для переменной `PATHEXT` задается значение: `.COM;.EXE;.BAT;.CMD`. Обратите внимание, что этот синтаксис подобен синтаксису для переменной `PATH`, то есть отдельные элементы разделяются точкой с запятой. Если при поиске исполняемого файла нет соответствия ни одному из расширений, выполняется проверка соответствия указанного имени папки. Если имя папки соответствует указанному, то команда `START` запускает `EXPLORER` для этого пути. Если такое действие выполняется из командной строки, то оно эквивалентно выполнению команды `CD /D` для указанного пути.



## Лабораторная работа 3

### Командный процессор и интерпретатор команд

Создайте документ расширенной справки по командной строке с использованием bat-файлов и синтаксиса команд командной строки. Освойте различные способы запуска командного процессора.

Запуск новой копии интерпретатора команд Windows выполняется командой:

`CMD [/A | /U] [/Q] [/D] [/E:ON | /E:OFF] [/F:ON | /F:OFF] [/V:ON | /V:OFF] [[/S] [/C | /K] строка]`, в которой параметры означают следующее:

`/C` – выполнение указанной команды (строки) с последующим завершением;

`/K` – выполнение указанной команды (строки) без последующего завершения;

`/S` – изменение поведения после `/C` или `/K` (см. ниже);

`/Q` – отключение режима вывода команд на экран (ECHO);

`/D` – отключение выполнения команд AutoRun из реестра (см. ниже);

`/A` – вывод результатов выполнения команд в формате ANSI;

`/U` – вывод результатов выполнения команд в формате UNICODE;

`/T:цвет` – выбор цвета текста/фона (более подробно см. COLOR /?);

`/E:ON` – разрешение расширений команд (см. ниже);

`/E:OFF` – запрет расширений команд (см. ниже);

`/F:ON` – разрешение символов завершения имен файлов и папок (см. ниже);

`/F:OFF` – запрет символов завершения имен файлов и папок (см. ниже);

`/V:ON` – разрешение отложенного расширения переменных среды с применением символа `!` в качестве разделителя. Например, `/V:ON` разрешает использовать `!var!` в качестве расширения переменной `var` во время выполнения. Синтаксис `var` служит для расширения переменных при вводе, что приводит к совсем другим результатам внутри цикла FOR;

`/V:OFF` – запрет отложенного расширения переменных среды.

Чтобы указать в одной строке несколько команд, следует разделить их символами `&&` и заключить в кавычки. Кроме того, из соображений совместимости, `/X` означает то же, что и `/E:ON`, `/Y` то же, что и `/E:OFF` и `/R` то же, что и `/C`. Все прочие ключи командной строки игнорируются.

Если указаны ключи `/C` или `/K`, то остальная часть командной строки после такого ключа обрабатывается как командная строка, а обработка символов кавычек (") ведется по следующим правилам:

1. Если выполняются все перечисленные ниже условия, то символы кавычек в командной строке сохраняются:

- ключ /S отсутствует
- есть ровно два символа кавычек
- между ними нет других специальных символов, как то: &<>()@^|
- между ними имеются один или несколько пробелов
- строка, заключенная в кавычки, является именем исполнимого файла.

2. В противном случае, проверяется первый символ, и если он является символом кавычек, то он удаляется, также удаляется последний символ кавычек в командной строке, а весь текст после этого последнего символа кавычек сохраняется.

Если ключ /D НЕ УКАЗАН в командной строке, то при запуске CMD.EXE выполняется проверка значений переменных REG\_SZ или REG\_EXPAND\_SZ для следующих разделов системного реестра:

HKEY\_LOCAL\_MACHINE\Software\Microsoft\Command Processor\AutoRun

и/или

HKEY\_CURRENT\_USER\Software\Microsoft\Command Processor\AutoRun

и если одна из них или обе они присутствуют, то сначала выполняются они. По умолчанию расширенная обработка команд включена. Чтобы запретить расширенную обработку для конкретного вызова, используется ключ /E:OFF. Можно включить или отключить расширенную обработку команд для всех вызовов CMD.EXE на данном компьютере или для данного пользователя, с помощью REGEDT32.EXE задав значения REG\_DWORD в системном реестре для следующих разделов:

HKEY\_LOCAL\_MACHINE\Software\Microsoft\Command Processor\EnableExtensions

и/или

HKEY\_CURRENT\_USER\Software\Microsoft\Command Processor\EnableExtensions

равными 0x1 или 0x0. Параметры пользователя перекрывают параметры компьютера.

Ключи командной строки, в свою очередь, перекрывают параметры реестра.

При расширенной обработке команд изменения и/или добавления затрагивают следующие команды: DEL или ERASE; COLOR; CD или CHDIR; MD или MKDIR; PROMPT; PUSHD; POPD; SET; SETLOCAL; ENDLOCAL; IF; FOR; CALL; SHIFT; GOTO; START (изменен также вызов внешних команд); ASSOC; FTYPE.

Для получения более подробных сведений введите "имяКоманды /?".

Отложенное расширение переменных среды НЕ ВКЛЮЧЕНО по умолчанию. Можно включить или отключить отложенное расширение перемен-

ных среды для конкретного вызова CMD.EXE с помощью ключей /V:ON или /V:OFF. Можно включить или отключить отложенное расширение переменных среды для всех вызовов CMD.EXE на данном компьютере или для данного пользователя, с помощью REGEDT32.EXE задав значения REG\_DWORD в системном реестре для следующих разделов:

HKEY\_LOCAL\_MACHINE\Software\Microsoft\Command Processor\DelayedExpansion

и/или

HKEY\_CURRENT\_USER\Software\Microsoft\Command Processor\DelayedExpansion

равными 0x1 или 0x0. Параметры пользователя перекрывают параметры компьютера.

Ключи командной строки, в свою очередь, перекрывают параметры реестра.

Если отложенное расширение переменных среды включено, то символ '!' (восклицательный знак) может использоваться для замены текущего значения переменной среды во время выполнения.

Завершение имен файлов и папок НЕ ВКЛЮЧЕНО по умолчанию. Можно включить или отключить завершение имен файлов и папок для конкретного вызова CMD.EXE с помощью ключей /F:ON или /F:OFF.

Можно включить или отключить отложенное расширение переменных среды для всех вызовов CMD.EXE на данном компьютере или для данного пользователя, с помощью REGEDT32.EXE задав значения REG\_DWORD в системном реестре для следующих разделов:

HKEY\_LOCAL\_MACHINE\Software\Microsoft\Command Processor\CompletionChar

HKEY\_LOCAL\_MACHINE\Software\Microsoft\Command Processor\PathCompletionChar

и/или

HKEY\_CURRENT\_USER\Software\Microsoft\Command Processor\CompletionChar

HKEY\_CURRENT\_USER\Software\Microsoft\Command Processor\PathCompletionChar

установив их шестнадцатеричные значения равными коду управляющего символа, используемого для конкретной функции (например, 0x4 для Ctrl-D или 0x6 для Ctrl-F). Параметры пользователя перекрывают параметры компьютера.

Ключи командной строки, в свою очередь, перекрывают параметры реестра.

Если завершение включено с помощью ключа командной строки /F:ON, то используются два управляющих символа: Ctrl-D для имен папок и Ctrl-

Для имен файлов. Чтобы отключить конкретный символ завершения в системном реестре, в качестве кода специального символа используется шестнадцатеричное значение символа пробела (0x20).


Завершение вызывается при вводе одного из этих двух специальных символов. Функция завершения берет строку пути слева от точки ввода, дописывает к ней символ шаблона, если таковой отсутствует, а затем строит список путей, которые соответствуют полученному определению. После этого выводится первый элемент этого списка соответствующих путей. Если же список пуст, то подается звуковой сигнал и ничего не выводится.

После этого повторный ввод того же самого специального символа приводит к циклическому перебору всех соответствующих путей. Нажатие клавиши <Shift> при вводе управляющего символа позволяет просматривать список путей в обратном порядке. Если изменить выведенный путь, а затем снова ввести управляющий символ, сохраненный список очищается и строится новый список путей. То же самое происходит, если переключиться с одного символа завершения на другой. Единственное отличие при использовании символа завершения файла состоит в том, что при этом для построения списка соответствия берется и путь, и имя файла, а при использовании символа завершения папки берется только путь. Если символ завершения используется в одной из встроенных команд манипулирования папками (CD, MD или RD), то всегда подразумевается символ завершения папок.

Символ завершения правильно работает и с именами файлов, содержащими пробелы или иные специальные символы, если при этом строка соответствия заключена в кавычки. Кроме того, если сместить точку ввода влево, а затем использовать символ завершения внутри строки, оставшийся справа от точки ввода текст будет отброшен.

Специальные символы, которые требуют обязательного заключения в кавычки:

<пробел>  
&()[]{}^=;!'+,`~

 Создайте документ справки по команде sc и выполните простейшие действия.

```
C:\Users\Администратор>sc /?
```

Описание:

SC представляет собой программу командной строки, используемую для связи со службами и диспетчером управления службами.

Использование:

```
sc<сервер> [команда] [имя службы] <параметр1><параметр2>...
```

Параметр <сервер> задается в формате "\\Имя\_сервера".

Для получения справки о командах введите "sc [команда]"

Команды:

query – Запрос состояния службы или перечисление состояний типов служб.

queryex – Запрос расширенного состояния службы или перечисление состояний типов служб.

start – Запуск службы.

pause – Отправка службе управляющего запроса PAUSE.

interrogate – Отправка службе управляющего запроса INTERROGATE.

continue – Отправка службе управляющего запроса CONTINUE.

stop – Отправка службе запроса STOP.

config – Изменение конфигурации службы (постоянное).

description – Изменение описания службы.

failure – Изменение действия, выполняемого службой при сбое.

failureflag – Изменение флага действия, выполняемого службой при сбое.

sidtype – Изменение типа SID службы.

privs – Изменение привилегий, требуемых для службы.

qc – Запрос данных конфигурации для службы.

qdescription – Запрос описания службы.

qfailure – Запрос действия, выполняемого службой при сбое.

qfailureflag – Запрос флага действия, выполняемого службой при сбое

qsidtype – Запрос типа SID службы.

qprivs – Запрос привилегий, требуемых для службы.

qtriggerinfo – Запрос параметров службы.

qpreferrednode – Запрос предпочтительного узла NUMA службы.

delete – Удаление службы (из реестра).

create – Создание службы (добавление ее в реестр).

control – Отправка службе управляющего сигнала.

sdshow – Отображение дескриптора безопасности службы.

sdset – Установка дескриптора безопасности службы.

showsid – Отображение строки SID службы, соответствующей произвольному имени.

triggerinfo – Настройка параметров триггеров службы.

preferrednode – Задание предпочтительного узла NUMA службы.

GetDisplayName – Получение параметра DisplayName для службы.

GetKeyName – Получение имени раздела для службы (ServiceKeyName).

EnumDepend – Перечисление зависимостей службы.

Следующие команды не требуют имени службы:

sc<сервер><команда><параметры>

boot– (ok| bad) Показывает, требуется ли сохранить последнюю загрузку в качестве последней удачной конфигурации загрузки

Lock– Блокировка базы данных служб.

QueryLock-----Запрос состояния блокировки (LockStatus) базы данных диспетчера управления службами (SCManager).

Пример:

scstartMyService

Показать справку для команд QUERY и QUERYEX? [Y(да)/N(нет)]:

Параметры QUERY и QUERYEX:

Если после команды query указано имя службы, будет возвращено состояние этой службы. В этом случае дополнительные параметры не используются. Если после команды запроса указаны следующие параметры либо ничего не указано, выполняется перечисление служб.

type= Тип служб для перечисления (driver, service, all) (по умолчанию = service);

state= Состояние служб для перечисления (inactive, all) (по умолчанию = active);

bufsize= Размер (в байтах) буфера перечисления (по умолчанию = 4096);

ri= Номер индекса возобновления для начала перечисления (по умолчанию = 0);

group= Группа служб для перечисления (по умолчанию = все группы).

Примеры использования:

scquery– Перечисление состояний активных служб и драйверов;

scqueryeventlog– Отображение состояния службы eventlog;

scqueryexeventlog– Отображение расширенного состояния службы eventlog;

scquerytype= driver– Перечисление только активных драйверов;

scquerytype= service– Перечисление только служб Win32;

scquerystate= all– Перечисление всех служб и драйверов;

scquerybufsize= 50 – Перечисление с буфером размером 50 байт;

scqueryri= 14 – Перечисление с индексом возобновления = 14;

scqueryexgroup= "" – Перечисление активных служб, не входящих в группу;

scquerytype= interact– Перечисление всех интерактивных служб;

scquerytype= drivergroup= NDIS – Перечисление всех драйверов NDIS.

Дополнительные сведения о программах приведены в описании программ командной строки в справке.

## Лабораторная работа 4 Служебные утилиты командной строки (4 ч.)

Воспользуйтесь следующими командами для управления сетевыми настройками компьютера. Особое внимание уделить команде NET. Создайте расширенные сведения по командам работы в сети и командам администрирования.

ARP /?

Отображение и изменение используемой протоколом ARP таблицы соответствия адресов IP и физических адресов.

ARP -s inet\_addr eth\_addr [if\_addr]

ARP -d inet\_addr [if\_addr]

ARP -a [inet\_addr] [-N if\_addr],

где

-a – вывод текущих записей таблицы ARP путем опроса текущих данных протокола. Если указан адрес inet\_addr, то адреса IP и физические выводятся только для указанного компьютера. Если протокол ARP используется несколькими сетевыми интерфейсами, то выводятся записи из каждой таблицы ARP.

-g Аналог -a.

inet\_addr– задание адреса IP.

-N if\_addr – вывод текущих записей таблицы ARP для сетевого интерфейса, определяемого параметром if\_addr.

-d – удаление узла, определяемого параметром inet\_addr.

-s – добавление узла и связывание адреса IP inet\_addr с физическим адресом eth\_addr. Физический адрес задается с помощью 6 шестнадцатеричных чисел, разделяемых дефисами. Запись является постоянной.

eth\_addr– задание физического адреса.

if\_addr– необязательный параметр, указывающий адрес IP интерфейса, для которого следует изменить таблицу адресов. Если параметр не задан, используется первый доступный интерфейс.

Образец: >arp -s 157.55.85.212 00-aa-00-62-c6-09 .... – добавляет статическую запись.

>arp -a . – выводит таблицу arp.

Диагностика состояния контроллера домена и репликаций Active Directory или DC диагностика

dcdiag /?

dcdiag.exe /s:<Domain Controller> [/u:<Domain>\<Username>

/p:\*\<Password>|"]

[/hqv] [/n:<Naming Context>] [/f:<Log>] [/ferr:<Errlog>] [/skip:<Test >]

[/test:<Test>]

/h: Показать этот экран справки

/s:<server> - Использует<Domain Controller>как Home Server. Это обязательный параметр.

/n:<naming context> - Использует<Naming Context>как контекст именованья для тестирования

Домены могут быть указаны в Netbios, DNS или DN форме.

/u:<domain>\<username> - Использовать учетные данные домена\имя пользователя для привязки.

Также необходимо использовать параметр / p

/p:<password> - Использует<Password>как пароль. Также необходимо использовать параметр / u

/a: Протестировать все серверы на этом сайте

/e: Протестировать все серверы на всем предприятии. Переопределяет /a

/q: Quiet - Печатать только сообщения об ошибках

/v: Verbose - Распечатать расширенную информацию

/i: ignore - игнорировать лишние сообщения об ошибках.

/fix: fix - Сделать безопасный восстановление.

/f: Перенаправить весь вывод в файл <Log>, /ferg перенаправит вывод ошибок отдельно.

/ferr:<ErrLog>Перенаправить вывод фатальной ошибки в отдельный файл <ErrLog>

/c: Comprehensive, запускает ВСЕ тесты, включая тесты не по умолчанию.

Можно использовать со / skip / test: <TestName> - тестировать только этот тест. Не пропускаемые тесты по-прежнему будут проводиться. Не смешивайте со / skip. Допустимые тесты:

Connectivity - Проверить, зарегистрированы ли контроллеры домена DNS, пингуются ли они и имеют ли LDAP / RPC-подключение.

Replications - Проверить своевременную репликацию между контроллерами домена.

Topology - Проверить, что сгенерированная топология полностью подключена для всех контроллеров домена.

CutoffServers - Проверить серверы, которые не будут получать репликации, потому что его партнеры не работают

NCSecDesc - Проверить, что дескрипторы безопасности на заголовках контекста именованья имеют соответствующие разрешения для репликации.

NetLogons - Проверить, что соответствующие привилегии входа в систему позволяют репликации продолжиться.

Advertising - Проверить, рекламирует ли каждый DC сам себя, и рекламирует ли он себя как имеющего возможности DC.



KnowsOfRoleHolders - Проверить, полагает ли DC, что он знает владельцев ролей, и распечатывает эти роли в подробном режиме.

Intersite - Проверить наличие сбоев, которые могут предотвратить или временно приостановить межсайтовую репликацию.

FsmoCheck - Проверить, что глобальные держатели ролей известны, могут быть найдены и отвечают.

RidManager - Проверить, доступен ли мастер RID, и проверьте, содержит ли он правильную информацию.

MachineAccount - Проверить, правильно ли указана учетная запись машины.

Services - Проверить, работают ли соответствующие службы DC.

OutboundSecureChannels - Посмотреть, есть ли у нас безопасные каналы от всех контроллеров домена в доменах, указанных в / testdomain :. / nitherrestrict будет препятствовать тому, чтобы тест был ограничен DC's на сайте

ObjectsReplicated - Убедиться, что учетная запись компьютера и объекты DSA реплицированы.

Используйте /objectdn:<dn>c /n:<nc> для указания дополнительного объекта для проверки.

frssysvol - Этот тест проверяет готовность системы репликации файлов (FRS) SYSVOL

kcsevent - Этот тест проверяет, что Проверка согласованности знаний завершается без ошибок.

systemlog - Этот тест проверяет, что система работает без ошибок.

/skip:<TestName> - Пропустить названный тест. Не пропускаемые тесты по-прежнему будут проводиться. Не смешивать с / test. Допустимые тесты следующие:

Replications - Проверить своевременную репликацию между контроллерами домена.

Topology - Проверить, что сгенерированная топология полностью подключена для всех контроллеров домена

CutoffServers - Проверить серверы, которые не будут получать репликации, потому что его партнеры не работают

NCSecDesc - Проверить, что дескрипторы безопасности на заголовках контекста именования имеют соответствующие разрешения для репликации.

NetLogons - Проверить, что соответствующие привилегии входа в систему позволяют репликации продолжиться.

Advertising - Проверить, рекламирует ли каждый DC сам себя, и рекламирует ли он себя как имеющего возможности DC.

KnowsOfRoleHolders - Проверить, полагает ли DC, что он знает владельцев ролей, и распечатывает эти роли в подробном режиме.

Intersite - Проверить наличие сбоев, которые могут предотвратить или временно приостановить межсайтовую репликацию.

FsmoCheck - Проверить, что глобальные держатели ролей известны, могут быть найдены и отвечают.

RidManager - Проверить, доступен ли мастер RID, и проверьте, содержит ли он правильную информацию.

MachineAccount - Проверить, правильно ли указана учетная запись машины.

Services - Проверить, работают ли соответствующие службы DC.

OutboundSecureChannels - Посмотреть, есть ли у нас безопасные каналы от всех контроллеров домена в доменах, указанных в / testdomain :: / nitherrestrict будет препятствовать тому, чтобы тест был ограничен DC's на сайте.

ObjectsReplicated - Убедиться, что учетная запись компьютера и объекты DSA реплицированы.

Используйте /objectdn:<dn>c /n:<nc> для указания дополнительного объекта для проверки

frssysvol - Этот тест проверяет готовность системы репликации файлов (FRS) SYSVOL

kcsevent - Этот тест проверяет, что Проверка согласованности знаний завершается без ошибок.

systemlog - Этот тест проверяет, что система работает без ошибок.

Следующие тесты не запускаются по умолчанию: Topology, CutoffServers, OutboundSecureChannels.

Команда ipconfig используется для конфигурирования сетевых протоколов в следующем виде:

```
ipconfig [/? | /all | /release [адаптер] | /renew [адаптер] | /flushdns | /displaydns /registerdns | /showclassидаптер | /setclassидаптер [устанавливаемый_код_класса_dhcp] ],
```

гдеадаптер – полное имя или имя, содержащие подстановочные знаки "\*" и "?" (\* –означает любое количество знаков, ? – один любой знак).

Ключи позволяют выполнить следующие действия:

/? –отобразить это справочное сообщение;

/all–отобразить полную информацию о настройке параметров;

/release–освободить IP-адрес для указанного адаптера;

/renew–обновить IP-адрес для указанного адаптера;

/flushdns–очистить кэш разрешений DNS;

/registerdns— обновить все DHCP-аренды и перерегистрировать DNS-имена;

/displaydns—отобразить содержимое кэша разрешений DNS.

/showclassid— отобразить все допустимые для этого адаптера коды (IDs) и DHCP-классов;

/setclassid—изменить код (ID) DHCP-класса.

По умолчанию отображается только IP-адрес, маска подсети и стандартный шлюз для каждого подключенного адаптера, для которого выполнена привязка с TCP/IP.

Для ключей /releaseи /renew, если не указано имя адаптера, то будет освобожден или обновлен IP-адрес, выданный для всех адаптеров, для которых существуют привязки с TCP/IP.

Для ключа setclassid, если не указан код класса (ID),то существующий код класса будет удален.

Примеры:

>ipconfig—отображает краткую информацию;

>ipconfig /all—отображает полную информацию;

>ipconfig /renew—обновляет сведения для всех адаптеров;

> ipconfig /renewEL\* —обновляет сведения для адаптеров, начинающихся с EL;

>ipconfig /release\*ELINK?21\* —освобождает IP-адреса для всех адаптеров, имена которых удовлетворяют запросу:ELINK-21 или myELELINKi21adapter и т.п.

 Обмен файлами с FTP-сервером в командной строке Windows

Для локального использования рекомендуется предварительно установить компонент информационных служб интернета и FTP-сервер. Приведем синтаксис выполнения команды:

C:\Users\Администратор>ftp /?

Обмен файлами с компьютером, на котором запущена служба сервера FTP. FTP может использоваться интерактивно.

FTP [-v] [-d] [-i] [-n] [-g] [-s:имя\_файла] [-a] [-A] [-x:sendbuffer] [-r:recvbuffer] [-b:asyncbuffers] [-w:window size] [узел]

-v Отключение вывода на экран ответов с удаленного сервера.

-n Отключение автоматического входа при начальном подключении.

-i Отключение интерактивных запросов при передаче нескольких айлов.

-d Включение отладочного режима.

-g Отключение глобализации имен файлов (см. команду GLOB).

-s:имя\_файла Задание текстового файла, содержащего команды FTP, которые будут выполняться автоматически при запуске FTP.

- a Использование локального интерфейса для привязки соединения.
  - A Анонимный вход в службу.
  - x:sendsockbuf Переопределение стандартного размера буфера SO\_SNDBUF (8192).
  - r:recvsockbuf Переопределение стандартного размера буфера SO\_RCVBUF (8192).
  - b:asynccount Переопределение стандартного размера счетчика async
- (3)
- w:windowsize Переопределение стандартного размера буфера передачи (65535).
  - узел Задание имени или адреса IP удаленного узла, к которому необходимо выполнить подключение.

#### Команда FTP

```
ftp>open<имя_сервера>
```

```
Пользователь :администратор
```

```
Пароль: *****
```

```
ftp>help
```

Допускается сокращение команд при вводе. Наборкоманд:

```
!      delete      literal      prompt      send
?      debugs      put          status
appenddirmdirdeletepwd  trace
asciidisconnect  mdirquit    type
bell            get          mget         quote        user
binary          glob         mkdirrecv    verbose
bye             hash         mlsremotehelp
cd help         mput         rename
closelcd       open         rmdir
ftp>
```

#### Отображение сетевой статистики

Отображение статистики протокола и текущих сетевых подключений TCP/IP выполняется командой NETSTAT, которая имеет следующий синтаксис:

```
NETSTAT [-a] [-e] [-n] [-s] [-p имя] [-r] [интервал].
```

В ней параметры означают следующее:

- a – отображение всех подключений и ожидающих портов(Подключения со стороны сервера обычно не отображаются);
- e – отображение статистики Ethernet. Этот ключ может применяться вместе с ключом -s;
- n – отображение адресов и номеров портов в числовом формате;

-r имя – отображение подключений для протокола "имя": tcp или udp. Используется вместе с ключом -s для отображения статистики по протоколам. Допустимые значения "имя": tcp, udp или ip;

-r – отображение содержимого таблицы маршрутов;

-s – отображение статистики по протоколам. По умолчанию выводятся данные для TCP, UDP и IP. Ключ -r позволяет указать подмножество выводимых данных;

интервал– повторный вывод статистических данных через указанный интервал в секундах. Для прекращения вывода данных нажмите клавиши CTRL+C. Если параметр не задан, сведения о текущей конфигурации выводятся один раз.

Команда NET /?

Синтаксис этой команды:

NET[ ACCOUNTS | COMPUTER | CONFIG | CONTINUE | FILE | GROUP | HELP | HELPMMSG | LOCALGROUP | NAME | PAUSE | PRINT | SEND | SESSION | SHARE | START | STATISTICS | STOP | TIME | USE | USER | VIEW ]

Команда NET help

Синтаксис этой команды: NET HELP command или NET command /HELP

Доступны следующие команды:

NET ACCOUNTS	NET HELP	NET SHARE
NET COMPUTER	NET HELPMMSG	NET START
NET CONFIG	NET LOCALGROUP	NET STATISTICS
NET CONFIG SERVER	NET NAME	NET STOP
NET CONFIG WORKSTATION	NET PAUSE	NET TIME
NET CONTINUE	NET PRINT	NET USE
NET FILE	NET SEND	NET USER
NET GROUP	NET SESSION	NET VIEW

Команда NETHELPSERVICES перечисляет некоторые из служб, которые вы можете запустить.

Команда NETHELPSYNTAX объясняет, как читать строки синтаксиса NETHELP.

Команда NETHELP command | MORE отображает справку по одному экрану за раз.

Команда NETHELPSHARE

Синтаксис этой команды:

NET SHARE sharename sharename=drive:path [/GRANT:user,[READ | CHANGE | FULL]] [/USERS:number | /UNLIMITED] [/REMARK:"text"]

[/CACHE:Manual | Documents | Programs | None ] sharename[/USERS:number | /UNLIMITED] [/REMARK:"text"] [/CACHE:Manual | Documents | Programs | None] {sharename | devicename | drive:path} /DELETE.

Указанные в команде параметры означают следующее:

NETSHARE делает ресурсы сервера доступными для пользователей сети. При использовании без параметров в нем отображается информация обо всех ресурсах, используемых на компьютере. Для каждого ресурса Windows сообщает имя (имена) устройства или путь (и) пути и связанный с ним описательный комментарий;

sharename—имя сети общего ресурса. Введите NETSHARE только с общим именем, чтобы отобразить информацию об этом ресурсе;

drive:path— определяет абсолютный путь к каталогу для общего доступа;

/GRANT:user,perm— создает общий ресурс с дескриптором безопасности, который дает запрошенные разрешения указанному пользователю. Этот параметр можно использовать более одного раза, чтобы предоставить разрешения на доступ к нескольким пользователям;

/USERS:number—устанавливает максимальное количество пользователей, которые могут одновременно получить доступ к общему ресурсу;

/UNLIMITED—указывает, что неограниченное количество пользователей может одновременно получить доступ к общему ресурсу.

/REMARK:"text" — добавляет описательный комментарий о ресурсе. Заключите текст в скобки;

devicename—если общий доступ предоставляется одному или нескольким принтерам (LPT1: через LPT9 :) имени;

/DELETE—прекращает деление ресурсом.

/CACHE:Manual—включает ручное клиентское кэширование программ и документов из этой папки

/CACHE:Documents— включает автоматическое кэширование документов из этой папки;

/CACHE:Programs—включает автоматическое кэширование документов и программ из этой папки;

/CACHE:None—отключает кэширование из этой части общего ресурса

Команда NETHELP command | MORE отображает справку по одному экрану за 1 раз.

Чтобы получить дополнительные сведения о конкретной команде Microsoft NET, поместите вслед за именем команды ключ /? (например NETVIEW /?).

Команда NETCONFIG выводит сведения о рабочей группе.

Команда NETDIAG запускает программы MicrosoftNetworkDiagnostics для получения данных о сети.

Запуск программы MicrosoftNetworkDiagnostics для проверки аппаратного соединения между компьютерами и вывода сведений о компьютере.

Команда NETDIAGNOSTICS [/NAMES | /STATUS]

Параметры этой команды означают следующее:

/NAMES– Имя сервера диагностики, необходимое для устранения конфликтов при использовании NETDIAG одновременно несколькими пользователями. Этот параметр применим лишь при использовании протокола NetBIOS.

/STATUS– Компьютер, о котором следует получить сведения.

Команда NETHELP– выводит сведения о командах и сообщения об ошибках. Она используется в двух формах: NETHELP [суффикс] и NETHELPкод\_ошибки, где

суффикс –определяет второе слово интересующей команды. Например, суффикс команды NETVIEW– слово VIEW;

код\_ошибки–задает номер интересующего сообщения об ошибке.

Команда NETINIT– загружает протокол и драйверы сетевой платы без привязки их к диспетчеру протоколов. Эта команда может понадобиться при использовании драйверов сторонних поставщиков. Привязка драйверов в данном случае производится командой NETSTARTNETBIND.

Команда NETINITIALIZE [/DYNAMIC] осуществляет динамическую загрузку диспетчера протоколов. Она удобна при работе с сетями сторонних поставщиков, например Banyan(R) и VINES(R), и служит для устранения неполадок с памятью.

Команда NETLOGOFFотключает все используемые компьютером общие ресурсы.

Команда NETLOGONидентифицирует пользователя как члена рабочей группы.

Команда NETPASSWORDизменяет пароль для входа в сеть.

Команда NETPRINTвыводит сведения об очередях печати и управляет заданиями по выводу на печать.

Команда NETSTARTзапускает службы. Службы нельзя запускать из сеанса MS-DOS в Windows.

Команда NETSENDиспользуется для сообщений, в ней параметры означают следующее: получатель – имя компьютера либо пользователя, /users–

все пользователи, подключенные к общим ресурсам данного компьютера, \* – все пользователи рабочей группы или домена.

Команда NETSTART имеет следующий синтаксис:

NET START [BASIC | NWREDIR | WORKSTATION | NETBIND | NETBEUI | NWLINK] [/LIST] [/YES] [/VERBOSE], где

BASIC–запуск базовой системы переадресации;

NWREDIR– запуск системы переадресации Microsoft, совместимой с Novell(R);

WORKSTATION–запуск стандартной системы переадресации;

NETBIND–привязка протоколов к драйверам сетевых плат;

NETBEUI–запуск интерфейса NetBIOS;

NWLINK–запуск IPX/SPX-совместимого интерфейса;

/LIST–вывод списка запущенных служб;

/YES–выполнение команды NETSTART без предварительного запроса данных или подтверждения;

/VERBOSE–вывод сведений о драйверах устройств и службах по мере загрузки.

Для запуска системы переадресации, выбранной при установке, используется команда NETSTART без параметров. В большинстве случаев использование параметров не потребуется.

NETSTOP Остановка работы служб.

NETTIME Вывод времени с другого компьютера или синхронизация часов с часами на сервере времени Microsoft Windows для рабочих групп, Windows NT, Windows 95 или NetWare.

NETUSE Подключение и отключение сетевых ресурсов и вывод сведений о подключениях.

NETUSE [диск: | \*] [\\компьютер\папка [пароль | ?]] [/SAVEPW:NO] [/YES] [/NO]

NET USE [порт:] [\\компьютер\принтер [пароль| ?]] [/SAVEPW:NO] [/YES] [/NO]

NET USE диск: | \\компьютер\папка /DELETE [/YES]

NET USE порт: | \\компьютер\принтер /DELETE [/YES]

NET USE \* /DELETE [/YES]

NET USE диск: | \* /HOME

диск – Имя диска, назначаемое общей папке.

\* – Эквивалент следующего свободного имени диска.



При использовании совместно с ключом /DELETE производится отключение сразу всех ресурсов.

порт – Имя параллельного (LPT) порта, назначаемое общему принтеру.

компьютер – Имя компьютера, на котором расположен общий ресурс.

папка Сетевое имя общей папки.

принтер Сетевое имя общего принтера.

пароль Пароль для доступа к общему ресурсу (если он имеется).

? Пароль для доступа к ресурсу запрашивается интерактивно. Этот режим может понадобиться лишь в том случае, когда ввод пароля необязателен.

/SAVEPW:NO Использование этого ключа позволяет предотвратить запись пароля в файл со списком паролей. В этом случае при каждом подключении к ресурсу пароль надо будет вводить заново.

/YES Выполнение команды NETUSE без предварительного запроса данных или подтверждения.

/DELETE Отключение общего ресурса.

/NO– Выполнение команды NETUSE с автоматической выдачей отрицательных (NO) ответов на все запросы, относящиеся к подтверждению действий.

/HOME– Подключение к основному каталогу, если сведения о нем имеются в учетной записи LANManager или WindowsNT.

Команда NETUSE без параметров выводит список всех подключенных ресурсов. Для просмотра выводимых сведений с паузами между отдельными экранами используются команды

```
NET USE /? | MORE
```

```
NET HELP USE | MORE
```

## NETSHARE

Синтаксис этой команды следующий:

```
sharename
```

```
sharename=drive:path [/GRANT:user,[READ | CHANGE | FULL]]
```

```
[/USERS:number | /UNLIMITED]
```

```
[/REMARK:"text"]
```

```
[/CACHE:Manual | Documents | Programs | None ]
```

```
sharename [/USERS:number | /UNLIMITED]
```

```
[/REMARK:"text"]
```

```
[/CACHE:Manual | Documents | Programs | None]
```

```
{sharename | devicename | drive:path} /DELETE
```

NET VER – Выводит тип и версию используемой системы переедресации.

NETVIEW– Вывод списка компьютеров, обеспечивающих совместный доступ к ресурсам, или общих ресурсов конкретного компьютера.

NET VIEW [\\компьютер] [/YES]

NET VIEW [/WORKGROUP:группа] [/YES]

компьютер – Имя компьютера, список общих ресурсов которого следует вывести.

/WORKGROUP– Этот ключ указывает необходимость вывода списка компьютеров из другой рабочей группы, имеющих общие ресурсы.

группа – Имя рабочей группы, список компьютеров которой следует вывести.

/YES– Выполнение команды NETVIEW без предварительного запроса данных или подтверждения.

Для вывода полного списка имеющих общие ресурсы компьютеров из рабочей группы, в которой зарегистрирован данный компьютер, используется команда NET VIEW без параметров.

The syntax of this command is:

NET SHARE sharename

sharename=drive:path [/USERS:number | /UNLIMITED]

[/REMARK:"text"]

[/CACHE:Manual | Automatic | No ]

sharename [/USERS:number | /UNLIMITED]

[/REMARK:"text"]

[/CACHE:Manual | Automatic | No ]

{sharename | devicename | drive:path} /DELETE

Получить список контроллеров домена, состояние безопасных каналов, отношений доверия с использованием nlttest

Использование: nlttest [/OPTIONS]

/SERVER:<имя\_сервера> - указать <имя\_сервера>

/QUERY - запросить службу входа в сеть <имя\_сервера>

/REPL - принудительно выполнить частичную синхронизацию на BDC  
<имя\_сервера>

/SYNC - принудительно выполнить полную синхронизацию на BDC

<имя\_сервера>

/PDC\_REPL - принудительно выполнить сообщение смены UAS из PDC

<имя\_сервера>

/SC\_QUERY:<имя\_домена> - запросить безопасный канал для <домен> на  
<имя\_сервера>

/SC\_RESET:<имя\_домена>[\<имя\_DC>] - переустановить безопасный канал для <домен> на <имя\_сервера>к<имя\_DC>  
 /SC\_VERIFY:<имя\_домена> - проверить безопасный канал для <домен> на <имя\_сервера>  
 /SC\_CHANGE\_PWD:<имя\_домена> - сменить пароль безопасного канала для <домен>на <имя\_сервера>  
 /DCLIST:<имя\_домена> - получить список контроллеров домена для<имя\_домена>  
 /DCNAME:<имя\_домена> - получить имя PDC для<имя\_домена>  
 /DSGETDC:<имя\_домена> - вызвать DsGetDcName /PDC /DS /DSP /GC /KDC /TIMESERV /GTIMESERV /WS /NETBIOS /DNS /IP /FORCE /WRITABLE /AVOIDSELF /LDAPONLY /BACKG /DS\_6 /TRY\_NEXT\_CLOSEST\_SITE /SITE:<имя\_сайта>  
 /ACCOUNT:<имя\_учетной\_записи> /RET\_DNS /RET\_NETBIOS  
 /DNSGETDC:<имя\_домена> - вызватьDsGetDcOpen/Next/Close /PDC /GC /KDC /WRITABLE /LDAPONLY /FORCE /SITESPEC  
 /DSGETFTI:<имя\_домена> - вызватьDsGetForestTrustInformation  
 /UPDATE\_TDO /DSGETSITE - вызватьDsGetSiteName  
 /DSGETSITECOV - вызватьDsGetDcSiteCoverage  
 /DSADDRESSSTOSITE:[имя\_компьютера] - вызватьDsAddressToSiteNamesEx  
 /ADDRESSES:<адрес1,адрес2,...>  
 /PARENTDOMAIN - получить имя родительского домена этого компьютера  
 /WHOWILL:<домен>\* <пользователь> [<итерация>] - определить, выполнит ли <домен> вход для<пользователь>  
 /FINDUSER:<пользователь> - посмотреть, какой доверенный домен выполнит вход для<пользователь>  
 /TRANSPORT\_NOTIFY - уведомить службу входа в сеть о новом порте  
 /DBFLAG:<шестнадцатеричные флаги> - новый флаг отладки  
 /USER:<имя\_пользователя> - запросить сведения о пользователе на <имя\_сервера>  
 /TIME:<шестнадцатеричный LSL><шестнадцатеричный MSL> - преобразовать время NT по Гринвичу в формат ASCII  
 /LOGON\_QUERY - запросить количество совокупных попыток входа  
 /DOMAIN\_TRUSTS - запросить доверия домена на <имя\_сервера>  
 /PRIMARY /FOREST /DIRECT\_OUT /DIRECT\_IN /ALL\_TRUSTS /V  
 /DSREGDNS - принудительно выполнить регистрацию всех относящихся к контроллеру домена записей DNS

/DSDEREGDNS:<DNS\_имя\_узла> - отменить регистрацию относящихся к контроллеру домена записей DNS для указанного контроллера домена

/DOM:<DNS\_имя\_домена> /DOMGUID:<GUID\_домена>

/DSAGUID:<GUID\_DSA>

/DSQUERYDNS - запросить состояние последнего обновления для всех относящихся к контроллеру домена записей DNS

/BDC\_QUERY:<имя\_домена> - запросить состояние репликации BDC для <имя\_домена>

/LIST\_DELTAS:<имя\_файла> - отобразить содержимое данного файла журнала изменений

/CDIGEST:<сообщение> /DOMAIN:<имя\_домена> - получить дайджест клиента

/SDIGEST:<сообщение> /RID:<RID в шестнадцатеричном формате> - получить дайджест сервера

/SHUTDOWN:<причина> [<секунд>] - завершить работу <имя\_сервера> вследствие <причина>

/SHUTDOWN\_ABORT - прервать завершение работы системы

Утилита для отслеживания сетевого пути Pathping

Использование: сочетает возможности ping и tracer и обладает дополнительными возможностями

pathping [-g<список\_узлов>] [-h<число\_прыжков>] [-i<адрес>] [-n] [-p<пауза>] [-q<число\_запросов>] [-w<таймаут>] [-4] [-6] <конечный\_узел>

Параметры:

- g<список\_узлов> Свободный выбор маршрута по списку узлов.
- h<число\_прыжков> Максимальное число прыжков при поиске узла.
- i<адрес> Использовать указанный адрес источника.
- n Не определять имена узлов по адресам.
- p<пауза> Пауза между отправками пакетов (мсек).
- q<число\_запросов> Число запросов при каждом прыжке.
- w<таймаут> Время ожидания каждого ответа (мсек).
- 4 Обязательное использование протокола IPv4.
- 6 Обязательное использование протокола IPv6.

Проверка качества передачи пакетов по TCP/IP сети

Использование:

ping [-t] [-a] [-n<число>] [-l<размер>] [-f] [-i<TTL>] [-v<TOS>] [-r<число>] [-s<число>] [[-j<список\_узлов>] | [-k<список\_узлов>]]

`[-w<таймаут>] [-R] [-S<источник>] [-4] [-6] <конечный_узел>`

Параметры:

`-t` Отправка пакетов на указанный узел, пока вы не прекратите опрос узла вручную. Для вывода статистики и продолжения опроса нажмите `<Ctrl>+<Break>`, для прекращения опроса нажмите `<Ctrl>+<C>`.

`-a` Определение имени узла по адресу.

`-n<число>` Число отправляемых запросов.

`-l<размер>` Размер буфера отправки.

`-f` Установка флага, запрещающего фрагментацию пакета (только IPv4).

`-i<TTL>` Задание срока жизни пакета ("TimeToLive").

`-v<TOS>` Задание типа службы ("TypeOfService") (только IPv4).

`-r<число>` Запись маршрута для указанного числа прыжков (только IPv4).

`-s<число>` Штамп времени для указанного числа прыжков (только IPv4).

`-j<список_узлов>` Свободный выбор маршрута по списку узлов (только IPv4).

`-k<список_узлов>` Жесткий выбор маршрута по списку узлов (только IPv4).

`-w<таймаут>` Таймаут для каждого ответа в миллисекундах.

`-R` Трассировка кругового пути (только IPv6).

`-S<источник>` Используемый адрес источника (только IPv6).

`-4` Обязательное использование протокола IPv4.

`-6` Обязательное использование протокола IPv6.

Отображение состояния портов TCP и UDP..

`portqry /?`

PortQry Usage:

`portqry -n server [-p protocol] [-e || -r || -o endpoint(s)] [-l logfile] [-s] [-i] [-q]`

Где:

`-n [server]` IPадрес или имя сервера для запроса

`-p [protocol]` TCPилиUDPилиBOTH (по умолчанию используетсяTCP)

`-e [endpoint]` один порт для запроса (правильный диапазон: 1-65535)

`-r [endpointrange]` диапазон портов для запроса (начальный:конечный)

`-o [endpointorder]` диапазон портов для запроса в порядке(x,y,z)

`-l [logfile]` имя файла журнала для создания

`-s`«медленная задержка связи»дольше ожидатьUDP-ответов от удаленных систем

`-i`обход по умолчанию поиска IP-адресов в именах игнорируется, если IP-адрес не указан после `-n`

`-q 'quiet'` операция выполняется без вывода

возвращает 0, если порт прослушивает  
возвращает 1, если порт не прослушивает  
возвращает 2, если порт прослушивает или фильтрует

Замечания:

PortQry работает на Windows 2000 и выше

Умолчания: TCP, порт 80, без журнала, медленная ссылка отключена

Нажмите Ctrl-c для досрочного прекращения

Примеры:

```
portqry -n myserver.com -e 25
```

```
portqry -n 10.0.0.1 -e 53 -p UDP -i
```

```
portqry -n host1.dev.reskit.com -r 21:445
```

```
portqry -n 10.0.0.1 -o 25,445,1024 -p both
```

### Обработка таблиц сетевых маршрутов

route /?

ROUTE [-f] [команда [узел] [MASK маска] [шлюз] [METRIC метрика]]

-f- Очистка таблиц маршрутов от записей для всех шлюзов. При указании одной из команд, таблицы очищаются до выполнения команды.

команда – Одна из четырех команд

PRINT Печать маршрута

ADD Добавление маршрута

DELETE Удаление маршрута

CHANGE Изменение существующего маршрута

узел – Адресуемый узел.

MASK– Если вводится ключевое слово MASK, то следующий параметр интерпретируется как параметр "маска".

маска – Значение маски подсети, связываемое с записью для данного маршрута. Если этот параметр не задан, по умолчанию подразумевается 255.255.255.255.

шлюз – Шлюз.

METRIC– Определение параметра метрика/цена для адресуемого узла.

Поиск всех символических имен узлов проводится в файле сетевой базы данных NETWORKS. Поиск символических имен шлюза проводится в файле базы данных имен узлов HOSTS. Для команд PRINT и DELETE можно указать узел и шлюз с помощью подстановочных знаков или опустить параметр "шлюз".

Сведения диагностики:

неправильное значение MASK приводит к ошибке, (DEST&MASK) != DEST.

Например>routeADD 157.0.0.0 MASK 155.0.0.0 157.55.80.1

## Сбой добавления маршрута: 87

Примеры:

```
>routePRINT
```

```
>routeADD 157.0.0.0 MASK 255.0.0.0 157.55.80.1 METRIC 3  
          ^назначение ^маска ^шлюз ^метрика
```

```
>route PRINT
```

```
>route DELETE 157.0.0.0
```

```
>route PRINT
```

Отслеживание маршрута пакета, посланного текущим хостом удаленному хосту

```
tracert [name|address]
```

Использование:

```
tracert [-d] [-hмаксЧисло] [-jсписокУзлов] [-w таймаут]  
        [-R] [-SадресИсточника] [-4] [-6] конечноеИмя
```

Параметры:

- d Без разрешения в имена узлов.
- hмаксЧисло Максимальное число прыжков при поиске узла.
- jсписокУзлов Свободный выбор маршрута по списку узлов (только IPv4).
- w таймаут Таймаут каждого ответа в миллисекундах.
- R Трассировка пути (только IPv6).
- SадресИсточника Используемый адрес источника (только IPv6).
- 4 Принудительное использование IPv4.
- 6 Принудительное использование IPv6.

## Лабораторная работа 5 Аппаратно-программное обеспечение персонального компьютера (4 ч.)

Воспользуйтесь служебной программой сведений о системе для экспорта подробных сведений о рабочем компьютере и элементом панели управления Система для сбора сведений об оборудовании. На его основании создайте документ об аппаратно-программном обеспечении конкретного компьютера в классе. Образец документа предлагается.

Создайте сведения по сетевым настройкам рабочего компьютера (TCP/IP, шлюз выхода в интернет, DNS-сервер, межсетевой экран, ISP-оператор, домен).

## **Лабораторная работа 6 Администрирование персонального компьютера**

Создайте документ с перечнем установленных служб (выводимое имя, имя и т.д.), определите службы телеметрии. Отключите запуск неиспользуемых служб. Убедитесь, что зависимые от них службы можно не использовать. Для сомнительно нужных служб установите ручную загрузку.

Включите аудит событий и соберите из журналов как можно больше сведений об ошибках и предупреждениях ПК. Установите причины событий и предложите способ их устранения.

Создайте файл с ошибками по журналу событий.

Воспользуйтесь утилитами Sysinternals для управления процессами, определения их свойств, проверки цифровой подписи, отправки на сайт проверки на наличие вирусов. Настройте параметры автозапуска процессов и драйверов, определите способ запуска процессов. Изучите действия планировщика заданий, изучите свойства запланированных заданий. Выявите прослушивание портов, открытые и взаимодействующие порты.

### **3.2 Тематика семинарских занятий**

1. Общие принципы организации и функционирования вычислительных систем.
2. Аппаратное обеспечение настольного персонального компьютера
3. Общая классификация программного обеспечения и место системного программного обеспечения персонального компьютера.
4. Операционные системы и их функции.
5. Интерфейсы встроенного программного обеспечения для компьютеров: базовая система ввода-вывода (BIOS) и унифицированный расширяемый интерфейс UnifiedExtensibleFirmwareInterface(UEFI).
6. Разбиение физического диска на разделы по схеме MBR, GPT и виртуальные жесткие диски. Файловые системы и система хранения данных.
7. Программы и компоненты операционной системы.
8. Элементы настройки параметров операционной системы
9. Инструменты администрирования и служба аудита событий.
10. Системный реестр как иерархическая база данных конфигурации системы Windows.

### **3.3 Тематика практических работ**

1. Преобразование данных из одной кодировки в другую.
2. Преобразование чисел в другую систему счисления с основанием



равным степени двойки.

3. Настройка рабочей среды пользовательского интерфейса системы.

4. Настройка рабочей среды пользователя для взаимодействия в локальной и глобальной сети.

5. Работа с виртуальными жесткими дисками и виртуальными машинами.

6. Диспетчер загрузки, системное хранилище базы данных загрузочной конфигурации и редактор файлов хранилища.

7. Создание загрузочного виртуального жесткого диска.

8. Особенности установки и восстановления операционных систем Windows.

9. Структура разделов реестра MS Windows, типы данных его параметров и редактор реестра.

10. Настройка рабочей среды с использованием утилит Sysinternals.

## 4 РАЗДЕЛ КОНТРОЛЯ ЗНАНИЙ

### 4.1 Контрольные вопросы

1. Охарактеризуйте место операционной системы в программном обеспечении компьютеров, компьютерных систем и сетей.
2. В чем заключается основное назначение операционной системы?
3. Перечислите основные функции операционной системы.
4. Дайте понятие компьютерных ресурсов.
5. Дайте определение архитектуры операционных систем.
6. Перечислите поколения операционных систем.
7. Перечислите классификационные признаки операционной системы.
8. Охарактеризуйте виды интерфейсов операционных систем.
9. Опишите особенности эволюционных этапов развития операционных систем.
10. В чем заключается эффективность операционной системы?
11. Опишите особенности операционной системы MSDOS
12. Охарактеризуйте многопользовательские операционные системы.
13. Охарактеризуйте многопроцессорные операционные системы.
14. Опишите этапы процесса загрузки ОС.
15. В чем заключается работа загрузчика при установке ОС?

### 4.2 Перечень вопросов к экзамену

1. Общие принципы организации и функционирования вычислительных систем.
2. Этапы развития вычислительных систем.
3. Аппаратное обеспечение настольного персонального компьютера
4. Общая классификация программного обеспечения и место системного программного обеспечения персонального компьютера.
5. Командная строка, ее интерфейс, встроенные команды и дисковая операционная система MS-DOS.
6. Операционные системы и их функции.
7. Организация оперативной памяти ОС Windows: физическая память, уровни кэширования, виртуальная память и страничная организация памяти.
8. Предустановочная среда Windows PE как современная среда установки ОС.
9. BIOS постоянного запоминающего устройства и настройка ее параметров, сохранение параметров в CMOS.
10. Особенности настройки параметров безопасности в BIOS UEFI.


11. Разбиение физического диска на разделы по схеме MBR.
12. Разбиение физического диска на разделы по схеме GPT.
13. Система хранения данных ОС, файловые системы.
14. Понятие профиля пользователя, папки профиля пользователя.
15. Пути автоматического поиска, задание переменных среды окружения.
16. Аутентификация учетных записей, авторизация и разрешения доступа.
17. Основные разрешения доступа.
18. Наделение полномочиями через локальную политику безопасности.
19. Наделение полномочиями через групповую политику.
20. Служебные программы ОС Windows.
21. Средства администрирования ОС Windows.
22. Параметры настройки системных служб.
23. Программы и компоненты операционной системы.
24. Группы безопасности и учетные записи.
25. Настройка локальной политик безопасности.
26. Элементы групповой политики.
27. Системные службы и их настройка.
28. Журналы событий аудита: приложений, безопасности, установки, системы.
29. Планировщик заданий, параметры электропитания.
30. Оснастки администрирования.
31. Установка ОС Windows и ее компонент.
32. Установка дополнительных программ в среду ОС.
33. Элементы настройки компьютера: драйвера устройств, локальная сеть, глобальная сеть интернет.
34. Системный реестр как иерархическая база конфигурации системы.
35. Настройка отдельных параметров ОС с использованием редактора реестра.
36. Способы загрузки системы, многовариантная загрузка.
37. Замораживание состояния системы с использованием специальных приемов.
38. Классификация вредоносных программ.
39. Способы восстановления работоспособного состояния персонального компьютера.
40. Возможности Windows Sysinternals по оптимизации выполнения приложений и защите от вредоносного программного обеспечения

41. Утилита Process Explorer для управления процессами операционной системы.

42. Утилита Autoruns для контроля выполнения приложений через реестр

43. Утилита TCPView просмотра конечных точек вашей системы, включая имя владеющего процесса, удаленный адрес и состояние TCP соединения.

#### **4.3 Критерии оценки результатов учебной деятельности студентов**

 Для выявления и исключения пробелов в знаниях студентов рекомендуется использовать следующие средства:

1) фронтальный опрос на лекциях, лабораторных и семинарских занятиях;

2) критериально-ориентированные тесты для контроля теоретических знаний современных информационных настольных издательских систем, основных определений, терминологии и правил набора, редактирования, форматирования и верстки текстовой и графической информации;

3) выполнение тестовых заданий с произвольной формой ответа для контроля умения анализировать и грамотно излагать и формулировать свои соображения и выводы в данной предметной области;

4) выполнение творческих заданий, которые предполагают эвристическую деятельность и поиск неформальных решений.

#### **4.4 Учебная программа**

Программно-технические средства. Раздел 3. Системное программное обеспечение. Учебная программа по специальности 1-21 04 01 Культурология (по направлениям), направление специальности 1-21 04 01-02 Культурология (прикладная), специализация 1-21 01-02 04 Информационные системы в культуре / П. В. Гляков, А.К. Демидович. – Минск : БГУКИ, 2019. – 16 с.

#### **4.5 Список основной литературы**

1. Артемьев, А. Работаем на ноутбуке в Windows 7 / А. Артемьев. – СПб. : Самоучитель, 2012. – 394 с.

2. Ботт, Э. Windows 10 для IT-специалистов / Э. Ботт; пер. с англ. – М. : Эком, 2016. – 173 с.

3. Ватаманюк, А. И. Установка, настройка и восстановление Windows 7 / А. И. Ватаманюк. – СПб. : Питер, 2010. – 160 с.
4. Гралла, П. Windows8. Трюки / П. Гралла. – СПб. : Питер Пресс, 2013. – 415 с.
5. Дейтел, Х. М. Операционные системы / Х. М. Дейтел. – М. : Бинном-Пресс, 2006. – 1024 с.
6. Матвеев, М. Д. Windows7 с обновлениями 2012: все об использовании и настройках: самоучитель / М. Д. Матвеев, М. В. Юдин, Р. Г. Прокди. – СПб. : Наука и техника, 2012. – 640 с.
7. Степаненко, О. С. Установка и настройка MicrosoftWindows XP. Самоучитель/ Степаненко О. С. – СПб. : Вильямс, 2005.
8. Харви, Д. В. Реестр Windows 7. Книга готовых рецептов. Самоучитель / Д. В. Харви, И. И. Антипов, Р. Г.Прокди. – СПб. : Наука и техника, 2011. – 224 с.
9. Безопасность корпоративных данных и управление рисками[Электронный ресурс]. – Режим доступа: <https://www.microsoft.com/ru-ru/security>. – Дата доступа: 10.10.2018.
10. Новости и обзоры операционной системы Windos 10 [Электронный ресурс]. – Режим доступа:<http://microsoftportal.net/windows-9/>. – Дата доступа: 10.10.2018.
11. Демидович, А. К. Основы операционной системы Windows 7 : учеб.пособие / А. К. Демидович. – Минск : АПО, 2016. – 70 с.

#### **4.6Список дополнительной литературы**

1. Ботт, Э. Эффективная работа: WindowsXP / Э. Ботт, К. Зихерт. – СПб. : БХВ-Петербург, 2006. – 1068 с.
2. Демидович, А. К. Расширяемые узлы на базе информационных служб Интернета: учеб.пособие / А. К. Демидович. – ГУО «Академия последипломого образования». – Минск : АПО, 2008. – 108 с.
3. Коваль, А. С. Архитектура ЭВМ и систем : учеб.-метод. пособие/ Коваль А. С., Сычев А. В. Воронеж : ИПЦ ВГУ, 2007. – 160 с.
4. Меженный, О. А. Microsoft Windows XP SP2. Самоучитель 2-е издание/ О. А.Меженный. – М. : Диалектика, 2007. – 310 с.
5. Симонович, С. В. Информатика. Базовый курс : учебник для вузов / С. В. Симонович. – СПб. : Питер:Лидер, 2012. – 640 с.
6. Стоцкий, Ю. А. MicrosoftOffice2010 / Ю. А.Стоцкий, А. Васильев, И.Телина. – СПб. : Питер:Лидер, 2011. – 425 с.
7. Таненбаум, Э. Архитектура компьютера / Э. Таненбаум. – М.:Питер, 2007. – 848 с.

8. Основы компьютерных технологий в образовании. В 4-х ч. Ч. 1.: Аппаратные средства и системное программное обеспечение персонального компьютера : учеб.пособие / Г. М. Троян[и др.] – Под ред. Г. М. Троян. – Минск : РИВШ БГУ, 2002. –180 с.

9. Hard DiskManager™ 15 Professional. Руководство пользователя. – ParagonSoftwareGmbH, 2017. – 311 с.

10. Таненбаум, Э. Современные операционные системы / Э. Таненбаум. – СПб. : Питер, 2010. – 1120 с.

РЕПОЗИТОРИЙ БГУКИ