Государственное областное бюджетное
профессиональное образовательное учреждение
«Усманский многопрофильный колледж»

МЕТОДИЧЕСКИЕ РЕКОМЕНДАЦИИ ПО ОРГАНИЗАЦИИ И ПРОВЕДЕНИЮ ПРАКТИЧЕСКИХ РАБОТ

по учебной дисциплине ОП.02 Операционные системы

Программы подготовки специалистов среднего звена (ППССЗ)

по специальности 09.02.04 Информационные системы (по отраслям)

по программе базовой подготовки

Усмань 2017

Методические рекомендации по организации и проведению практических работ по учебной дисциплине Операционные системы по специальности 09.02.04 Информационные системы (по отраслям).

Организация-разработчик: Государственное областное бюджетное профессиональное образовательное учреждение «Усманский многопрофильный колледж»

Разработчики:
Боев Е.И., преподаватель естественнонаучных дисциплин

Рассмотрены и утверждены на заседании предметно-цикловой комиссии естественнонаучных дисциплин

Протокол № 6 от 30.06.2017 г.

Председатель предметно-цикловой комиссии естественнонаучных дисциплин _____ Коровина Т.В.

УТВЕРЖДАЮ

Заместитель директора
по учебно-методической работе _____ Думма Т.А.

Введение

Практические занятия, как вид учебных занятий, направлены на экспериментальное подтверждение теоретических положений и формирование учебных и профессиональных практических умений и составляют важную часть теоретической и профессиональной практической подготовки.

В процессе практического занятия обучающиеся выполняют одно или несколько практических заданий в соответствии с изучаемым содержанием учебного материала.

Содержание практических занятий по учебной дисциплине ОП.02 Операционные системы должно охватывать весь круг профессиональных умений, на подготовку к которым ориентирована данная дисциплина, а в совокупности охватывать всю профессиональную деятельность, к которой готовится специалист.

При разработке содержания практических занятий следует учитывать, что наряду с формированием умений и навыков в процессе практических занятий обобщаются, систематизируются, углубляются и конкретизируются теоретические знания, вырабатывается способность и готовность использовать теоретические знания на практике, развиваются интеллектуальные умения.

Выполнение обучающимися практических занятий проводится с целью:

- формирования практических умений в соответствии с требованиями к уровню подготовки обучающихся, установленными ФГОС и рабочей программой учебной дисциплины ОП.02 Операционные системы по конкретным разделам и темам дисциплины;
- обобщения, систематизации, углубления, закрепления полученных теоретических знаний;
- совершенствования умений применять полученные знания на практике, реализации единства интеллектуальной и практической деятельности;
- развития интеллектуальных умений у будущих специалистов: аналитических, проектировочных, конструктивных и др.;
- выработки таких профессионально значимых качеств, как самостоятельность, ответственность, точность, творческая инициатива при решении поставленных задач при освоении общих и профессиональных компетенций.

Соответственно в процессе освоения учебной дисциплины Операционные системы обучающиеся должны овладеть:

умениями:

- устанавливать и сопровождать операционные системы;
- учитывать особенности работы в конкретной операционной системе, организовывать поддержку приложений других операционных систем;
- пользоваться инструментальными средствами операционной системы;

знаниями:

- понятие, принципы построения, типы и функции операционных систем;
- операционное окружение;
- машинно-независимые свойства операционных систем;
- защищенность и отказоустойчивость операционных систем;
- принципы построения операционных систем;
- способы организации поддержки устройств, драйверы оборудования, сетевые операционные системы

Выше перечисленные умения и знания направлены на формирование следующих профессиональных и общих компетенций студентов:

Профессиональные компетенции:

ПК 1.2. Взаимодействовать со специалистами смежного профиля при разработке методов, средств и технологий применения объектов профессиональной деятельности.

ПК 1.7. Производить инсталляцию и настройку информационной системы в рамках своей компетенции, документировать результаты работ.

ПК 1.9. Выполнять регламенты по обновлению, техническому сопровождению и восстановлению данных информационной системы, работать с технической документацией.

ПК 1.10. Обеспечивать организацию доступа пользователей информационной системы в рамках своей компетенции.

Общие компетенции:

ОК 1. Понимать сущность и социальную значимость своей будущей профессии, проявлять к ней устойчивый интерес.

ОК 2. Организовывать собственную деятельность, выбирать типовые методы и способы выполнения профессиональных задач, оценивать их эффективность и качество.

ОК 3. Принимать решения в стандартных и нестандартных ситуациях и нести за них ответственность.

ОК 4. Осуществлять поиск и использование информации, необходимой для эффективного выполнения профессиональных задач, профессионального и личностного развития.

ОК 5. Использовать информационно-коммуникационные технологии в профессиональной деятельности.

ОК 6. Работать в коллективе и команде, эффективно общаться с коллегами, руководством, потребителями.

ОК 7. Брать на себя ответственность за работу членов команды (подчиненных), результат выполнения заданий.

ОК 8. Самостоятельно определять задачи профессионального и личностного развития, заниматься самообразованием, осознанно планировать повышение квалификации.

ОК 9. Ориентироваться в условиях частой смены технологий в профессиональной деятельности.

Данные методические указания по организации и проведению практических работ составлены в соответствии с содержанием рабочей программы учебной дисциплины Операционные системы специальности 09.02.04 Информационные системы (по отраслям) по программе базовой подготовки.

Учебная дисциплина Операционные системы изучается в течение двух семестров. Общий объем времени, отведенный на выполнение практической работы по учебной дисциплине Операционные системы, составляет в соответствии с учебным планом и рабочей программой – 32 часа.

Методические рекомендации призваны помочь студентам правильно организовать работу и рационально использовать свое время при овладении содержанием учебной дисциплины Операционные системы, закреплении теоретических знаний и практических умений.

Распределение часов на выполнение практической работы студентов по разделам и темам учебной дисциплины Операционные системы

Наименование раздела, темы	Количество часов
Раздел 1. Основы теории операционных систем	**6**
Тема 1.2. Архитектура операционной системы	4
Тема 1.3. Интерфейс пользователя	2
Раздел 2. Процессы и потоки	**2**
Тема 2.1 Планирование процессов и потоков	2
Раздел 4. Ввод-вывод и файловая система	**6**

Тема 4.1 Базовая система ввода-вывода (BIOS)	2
Тема 4.2 Логическая и физическая организация файловой системы	4
Раздел 5. Управление безопасностью. Защита системы и данных	**8**
Тема 5.1. Основные понятия безопасности	4
Тема 5.2. Защита системы и данных	4
Раздел 6. Работа в операционных системах и средах	**10**
Тема 6.1. Установка и настройка операционной системы	6
Тема 6.2. Администрирование	4
Всего	

Перечень рекомендуемой литературы

1. Т.Л. Партыка, И.И. Попов. Операционные системы, среды и оболоч- ки.Изд. 4-е испр. и доп. - М.:ФОРУМ, 2016
2. Назаров С.В., Гудыно Л.П., Кириченко А.А. Операционные системы. Практикум. Под ред. С.В. Назарова - М.: Кудиц-пресс, 2017. - 464с., илл.
3. Кондратьев В.К. Введение в операционные системы: (Электронный ресурс): Кондратьев В.К. Введение в операционные системы: Учебное пособие//Московский государственный университет экономики, статистики и информатики. - М.:МЭСИ, 2016. - 232с.

Интернет-ресурсы

1. Интернет-Университет Информационных технологий http://www.intuit.ru
2. Каталог библиотеки учебных курсов - http://msdn.microsoft.com/ru-ru/gg638594
3. Мультипортал http://www.km.ru
4. Паскаль – шифрование http://www.cyberforum.ru/pascal/thread33245.html
5. Образовательный портал http://claw.ru

Практическая работа №1 Анализ программного обеспечения персонального компьютера. Сбор сведений о системе.

Цель работы: *изучить состав программного обеспечения компьютера, соотнести его с видами ПО.*

Задание

1. Изучить состав программного обеспечения ПК.
2. Выяснить назначение программ, установленных на ПК.
3. Соотнести ПО, установленное на ПК, с видами.
4. Сделать вывод об установленном ПО, его необходимости и достаточности для реализации целей квалификации «Техник».
5. Ответить на вопросы.

Ход выполнения работы

1. Ознакомиться с программным обеспечением, установленным на ПК, через главное меню.
2. Для анализа ПО и соотнесения его с видами, воспользоваться структурной схемой ПО (составленной по материалам лекции при выполнении самостоятельной работы). Согласно схеме:
   а) выделить виды программного обеспечения,
   б) соотнести имеющиеся программы с видами ПО,
   в) привести примеры программ для каждого вида ПО.
3. Составить структурную схему ПО компьютера, соотнести программы с видами ПО.
4. Заполнить в отчете таблицу:

Таблица 1. Характеристика ПО

№ п/п	Наименование программы	Вид программного обеспечения	Место хранения программы	Объем памяти программы

5. Сделать вывод об имеющемся ПО на компьютере, целесообразности его использования, необходимости и достаточности для достижения цели квалификации «Техник». Отметить необходимость и полезность других программ для решения дополнительных задач.

Вопросы для самопроверки

1. Перечислите виды программного обеспечения.
2. Сформулируйте назначение каждого вида ПО.
3. Приведите примеры программ, обязательных для работы ПК.

Практическая работа №2 Выполнение команд при работе с дисками, каталогами, файлами. Выполнение тестовых заданий по теме «Команды DOS»

Цель работы: *изучить команды DOS при работе с командной строкой.*

Задание

1. Запустить командную строку. Просмотреть версию операционной системы, текущую дату и время.
2. Создать на рабочем диске каталог.

3. Выполнить команды для работы с диском, каталогами и файлами.
4. Ответить на вопросы.

Ход выполнения работы

1. Запустить командную строку Пуск - Программы - Стандартные:

а) С помощью команды (например, D:) выполнить переход к диску пользователя.

б) С помощью команды ver через командную строку просмотреть версию операционной системы, текущую дату и время.

2. Создать на рабочем диске каталог с помощью команды md.

а) В каталоге с номером своей группы создать папку под своей фамилией (команда md). Перейти к своей папке.

б) В своей папке создать два каталога с именами Proba и Zadanie.

в) Просмотреть содержимое своей папки (команда dir).

г) В папке Proba создать 2 текстовых файла (команда copy con) с именами text1.txt, , записав в них следующую информацию: в файл text1.txt - ваши фамилия, имя, отчество, в файл text2.txt - сведения о вашей специальности.

д) Выполнить соединение информации двух текстовых файлов (copy text1.txt+text2.txt) в файл itog.txt в папку Zadanie.

е) Просмотреть содержимое папок Proba и Zadanie.

ж) Просмотреть содержимое файла itog.txt (команда type).

з) Скопировать файл itog.txt в папку Proba, задав ему новое имя new.txt.

и) В папку Zadanie скопировать 4 других файла разного типа, предварительно выполнив их поиск на компьютере. Просмотреть содержимое папки Zadanie.

к) Выполнить сортировку файлов в папке Zadanie по размеру, по дате, типу, имени.

л) Переименовать папку Proba в PRIMER (команда move).

м) Представить работу преподавателю.

н) После проверки удалить свою папку.

Вопросы для самопроверки

1. Каково назначение командной строки?
2. Как произвести запуск командной строки?
3. Назовите команды для работы с дисками (переход к другому диску).
4. Назовите команды для работы с каталогами (переход к каталогу, создание, копирование, переименование, просмотр, удаление).
5. Назовите команды для работы с файлами (создание, копирование, переименование, просмотр, удаление, сортировка).

Практическая работа №3 Просмотр и анализ информации о заданиях, процессах и потоках. Детальное исследование вычислительного процесса.
Запись и представление результатов анализа вычислительного процесса. Создание журнала трассировки.

Цель: изучение возможностей контроля и управления процессами в операционной системе Windows, научиться создавать журнал трассировки.

Заданием данной практической работы является изучение утилит и команд управления процессами в операционной системе Windows:

Ознакомиться с управлением процессами в ОС Windows с помощью утилиты Process Explorer (procexp.exe).

Просмотр и управление процессами под Windows будем выполнять с помощью утилиты Process Explorer фирмы SysInternals.

Утилита показывает не просто список активных процессов, но и файлы динамических библиотек, связанные с процессом, приоритет процесса, нагрузку на процессор отдельно для каждой программы и т.д.

· Возможность запуска и полноценного использования в режиме простого пользователя.

· Полнофункциональное дерево процессов с возможностью полного раскрытия для изучения различных дочерних процессов (ветвей).

· Отличный системный монитор с более богатой и подробной информацией.

· Возможность назначения тем или иным процессам различных приоритетов.

· Интерактивное отображение того или иного процесса в двух режимах – Handle mode (отображение всех системных операций задействованных выделенным в верхнем окне программы процессом) и DLL mode (отображение всех динамических библиотек, так или иначе связанных с выделенным для изучения процессом) и многое другое.

Помимо этого, с помощью программы можно изменить приоритет процесса, просмотреть информацию о DLL-файле и принудительно завершить безнадежно зависшую программу.

Process Explorer 8.34 может быть очень полезна как системным администраторам, так и программистам (например, позволяет отыскивать утечки памяти в приложениях), так как обладает следующими интересными преимуществами по сравнению хотя бы со встроенным в Windows NT/2000/XP диспетчером задач:

Утилита содержит 2 окна. В верхнем отображается список активных процессов (в т.ч. идентификатор процесса - **PID**, процент загрузки процессора - **CPU**, описание - **Description,** наименование аккаунта владельца - **Owner**, приоритет процесса - **Priority**, **Handles, Windows Title**). Информация, показываемая в нижнем окне, зависит от режима **Process Explorer** - если он находится в режиме **handle mode**, Вы можете

видеть **handles**(файлы для Windows 9x/Me), которые открыл процесс, выбранный в верхнем окне; если это режим **DLL (DLL mode**) - Вы можете видеть **DLL**, которые загрузил данный процесс.

Переключение между режимами осуществляется "горячими клавишами" или с помощью соответствующих пунктов меню: Вы можете сортировать процессы по любому критерию, щелкая мышкой на соответствующей колонке; либо представить процессы в виде дерева процессов (**process tree**) путем выбора пункта меню **View - Show Process Tree.**

Щелкнув правой кнопкой мыши по выбранному процессу, с помощью появившегося контекстного меню Вы можете изменить базовый приоритет процесса (Set Priority), принудительно завершить процесс (**Kill Process**) и просмотреть дополнительные параметры процесса (**Properties):**

С помощью пункта меню **Options - Highlight Services** можно выделить процессы, которые обслуживают хост. Для выделения процессов текущего пользователя выберите пункт меню **Options - Highlight Own Processes**.

Практическое задание №1. Запустив утилиту, запустите восемь приложений (например Word, Paint, Notepad и т.д.), обратите внимание на изменения в окне процессов. Прокомментируйте их. Приведите копии экрана и опишите процессы, порожденные запущенными приложениями.

Практическое задание №2. Выполните следующие действия. Отсортируйте процессы по заданному критерию. Опишите один из системных процессов. Запустите указанное приложение. Опишите возникший процесс по заданным характеристикам. Принудительно завершите указанный процесс. Выполняемые действия иллюстрируйте копиями экранов.

Критерий	Приложение	Характеристики
Показать дерево системных процессов	Far Manager	Определить используемые DLL
Отсортировать по PID	Блокнот	Просмотреть доп. свойства процесса
Отсортировать по загрузке процессора	Wordpad	Определить используемые handles
Отсортировать по приоритету	Калькулятор	Просмотреть доп. свойства процесса
Отсортировать по владельцу	Paint	Изменить приоритет пользовательского процесса
Показать дерево пользовательских процессов	Проводник	Просмотреть доп. свойства процесса
Отсортировать по наименованию	Редактор реестра	Определить используемые DLL
Отсортировать по приоритету	Web-браузер	Изменить приоритет пользовательского процесса
Отсортировать по загрузке процессора	Сетевое окружение	Определить используемые handles
Показать дерево пользовательских процессов	Дефрагментация диска	Определить используемые DLL

Копии экрана с выполненным заданием и описание выполненных действий привести в отчете.

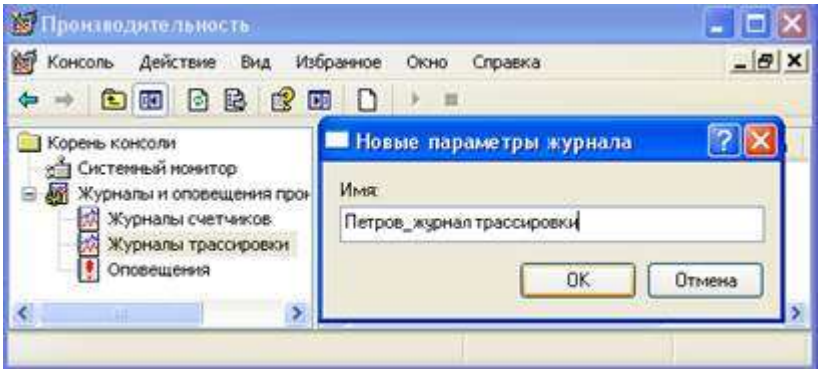
Создание журнала трассировки.

В отличие от журналов счетчиков, журналы трассировки находятся в ожидании определенных событий. Для интерпретации содержимого журнала трассировки необходимо использовать *специальный анализатор*.

Для создания журнала трассировки необходимо выполнить следующие действия:

1. запустить оснастку Производительность;
2. щелкнуть по значку Журналы трассировки;
3. щелкнуть правой кнопкой мыши в панели результатов и выбрать в контекстном меню пункт Новые параметры журнала;

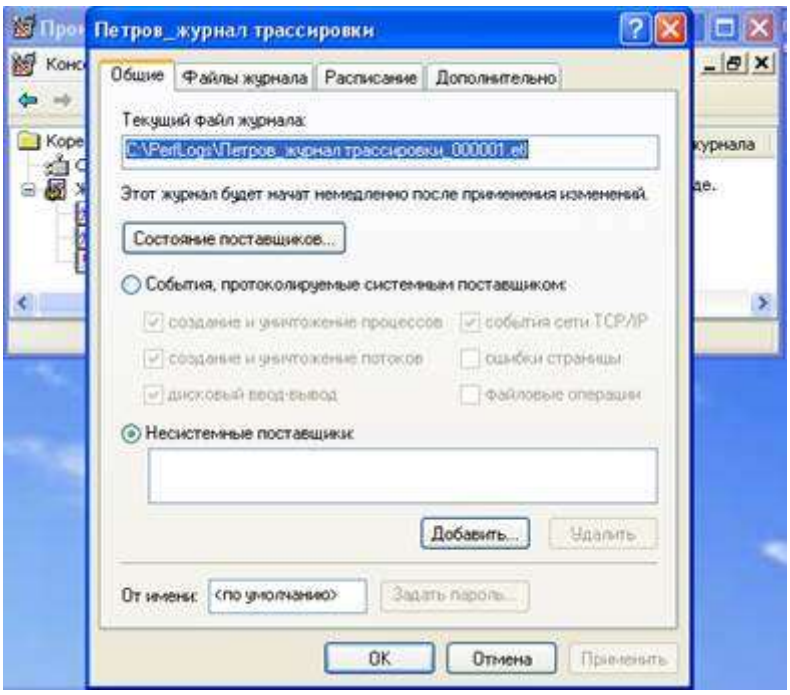
4. в открывшемся окне ввести произвольное имя журнала и нажать кнопку ОК;



5. по умолчанию файл журнала создается в папке PerfLogs в корневом каталоге и к имени журнала присоединяется серийный номер;

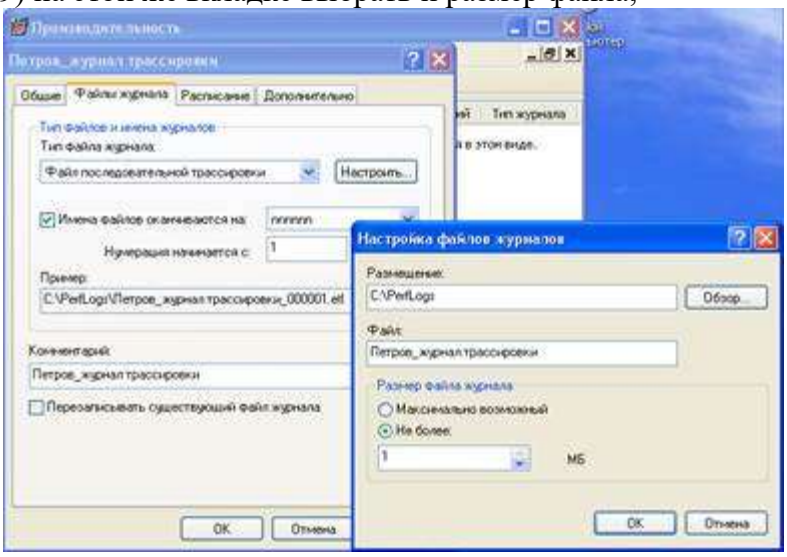
6. на вкладке Общие указать путь и имя созданного журнала (по умолчанию оно уже есть);

7. на этой же вкладке выбрать События, протоколируемые системным поставщиком или указать другого поставщика;

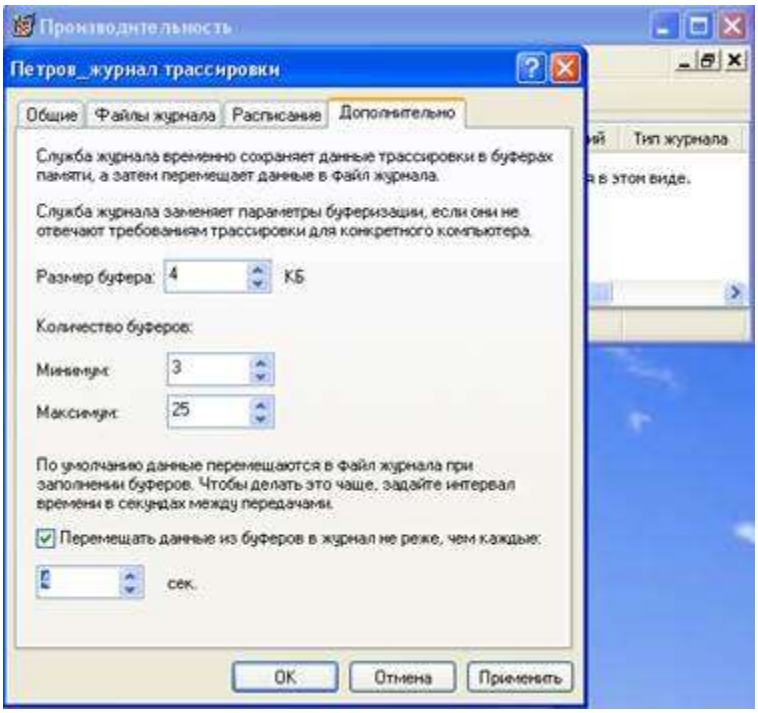


8. на вкладке Файлы журналов выбрать тип журнала:

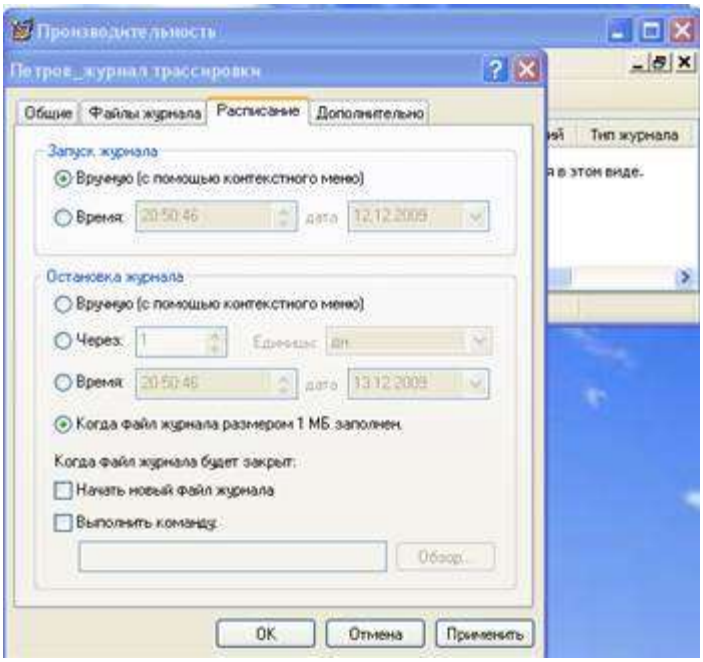
· файл циклической трассировки (журнал с перезаписью событий, расширение etl);
· файл последовательной трассировки (данные записываются, пока журнал не достигнет предельного размера, расширение etl);
9) на этой же вкладке выбрать и размер файла;



10) на вкладке Дополнительно можно указать размер буфера журнала;



11) на вкладке Расписание выбрать режим запуска и остановки журнала (вручную или по времени).



Создание оповещений.

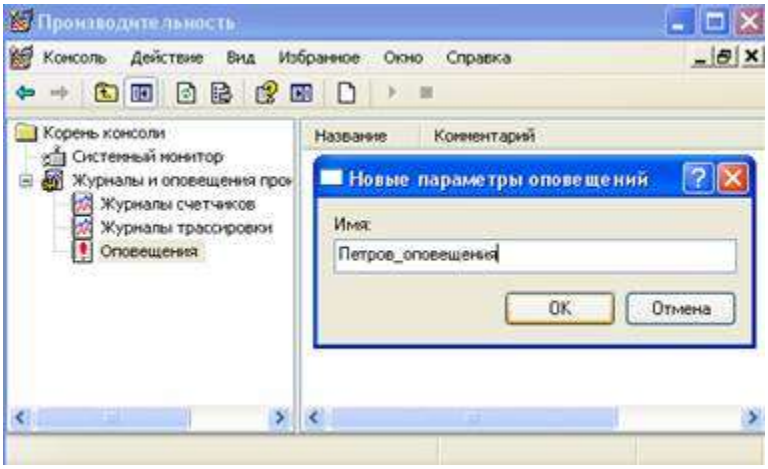
Для обнаружения неполадок в организации вычислительного процесса удобно использовать оповещения. С помощью этого компонента можно установить оповещения для выбранных счетчиков. При превышении или снижении относительно заданного значения выбранными счетчиками оснастка посредством сервиса Messenger оповещает пользователя.

Для создания оповещений необходимо выполнить следующие действия:

1) щелкнуть по значку Оповещения;

2) щелкнуть правой кнопкой мыши в панели результатов и выбрать в контекстном меню пункт Новые параметры оповещений;

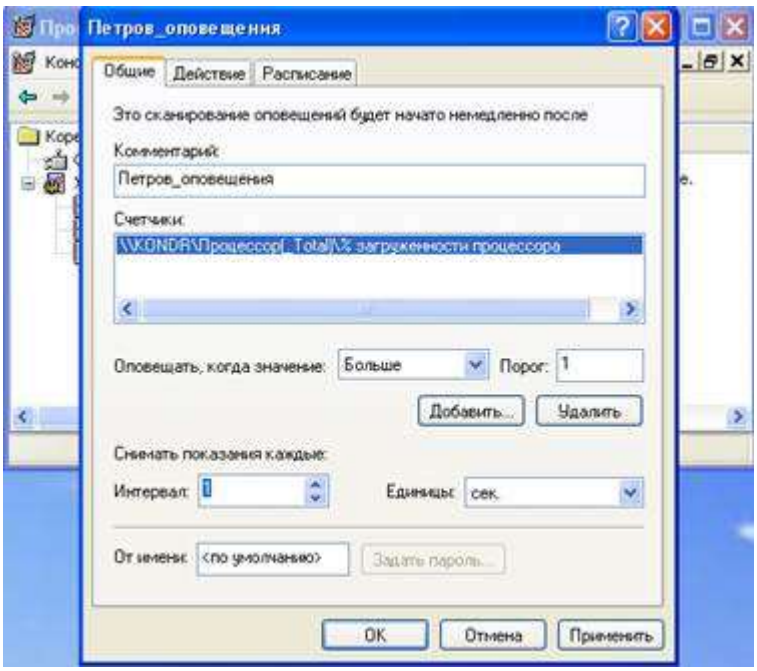
3) в открывшемся окне ввести произвольное имя оповещения и нажать кнопку ОК;



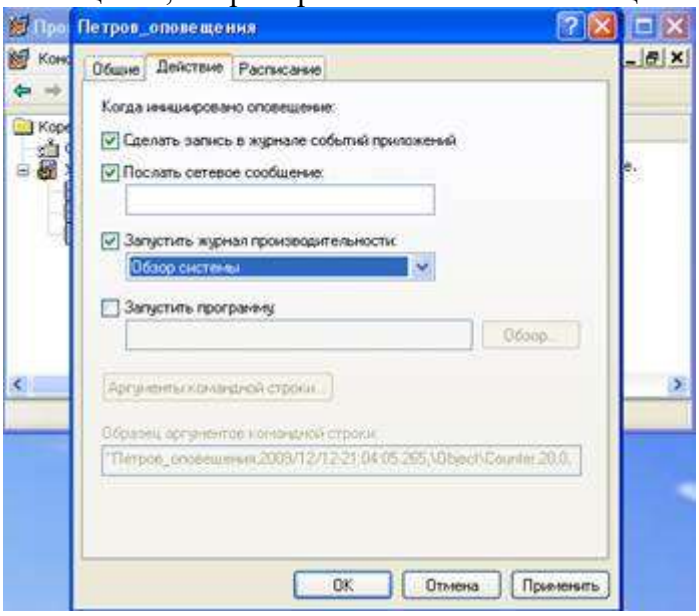
4) в появившемся окне на вкладке Общие можно задать комментарий к оповещению и выбрать нужные счетчики;

5) в поле Оповещать выбрать предельные значения для счетчиков;

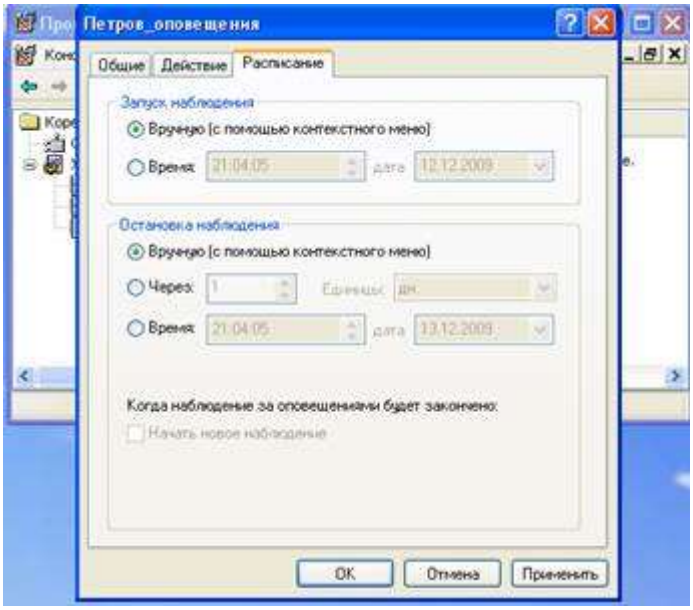
6) в поле Снимать показания выбрать период опроса счетчиков;



7) на вкладке Действие можно выбрать действие, которое будет происходить при запуске оповещения, например Послать сетевое сообщение и указать имя компьютера;



8) на вкладке Расписание выбрать режим запуска и остановки наблюдения.



Если в компьютере произойдет событие, предусмотренное в Оповещениях, в журнал событий Приложение будет сделана соответствующая запись. Для ее просмотра нужно зайти в оснастку Просмотр событий, где и можно увидеть сведения о событии.

ЗАДАНИЕ 4.
Создать журнал трассировки для исследования своего приложения.
1. Создать Оповещения по выбранным счетчикам для своего приложения.
2. Просмотреть журнал событий.
3. Объяснить полученные результаты.

Практическая работа № 4 Оптимизация работы компьютера. Изучение настроек BIOS.

Тема: «Оптимизация работы компьютера. Изучение настроек BIOS».

Цель: Изучить основные настройки BIOS. Работа в симуляторе BIOS. Выполнить настройки по оптимизации работы компьютера.

Оборудование: автоматизированное рабочее место студента с установленной операционной системой Windows. Программа симулятора BIOS

Краткие теоретические сведения

Основное назначение, принципы работы и классификация

BIOS (Basic Input-Output System) - базовая система ввода/вывода. Все системные платы содержат небольшой блок постоянного запоминающего устройства (ROM), который отделен от основной системной памяти, используемой для загрузки и выполнения программного обеспечения. ROM содержит BIOS ПК. Это дает два преимущества: программы и данные в ROM BIOS не должны перезагружаться каждый раз при запуске компьютера, и они не могут быть разрушены ошибками в приложениях, которые пытаются записать информацию в «неправильную» часть памяти. По существу, BIOS является неким промежуточным слоем (интерфейсом) между программной и аппаратной частями компьютерной системы.

BIOS включает несколько отдельных подпрограмм, обслуживая различные функции. Первая часть выполняется при включении машины. Компьютер инспектируется, чтобы определить, какие аппаратные средства присоединены, и затем проводятся некоторые простые тесты, чтобы зафиксировать, что все функционирует. Когда все тесты пройдены, ROM пытается определять, с какого устройства будет загружаться ОС машины.

BIOS имеют различные контроллеры, видеоплаты, дисководы, модемы, сканеры и другие

внутренние и периферийные устройства компьютера. Это так называемые BIOS адаптеров, которые загружаются при запуске системы. Но наиболее важной в компьютере является системная BIOS, в которой находится всё основное системное программное обеспечение компьютера и в функции которой входят:

- тестирование компьютера при включении питания с помощью специальных тестовых программ;
- поиск и подключение к системе других BIOS, расположенных на платах расширения;
- распределение ресурсов между компонентами компьютера.

Схемотехническое воплощение:

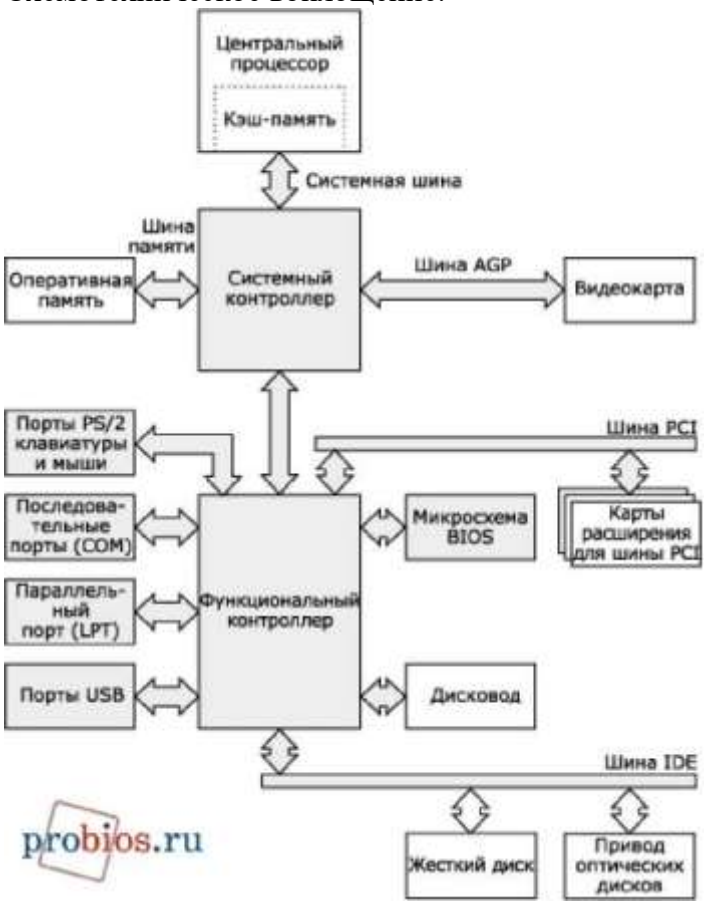


Рис. 1 Схема

История развития BIOS

Микросхем BIOS существует всего четыре типа: ROM (Read Only Memory) или ПЗУ, PROM (Programmable ROM) или ППЗУ (программируемое ПЗУ), EPROM (Erasable PROM) или СППЗУ (Стираемое ППЗУ), EEPROM (Electrically EPROM) или ЭСППЗУ (электронно-стираемое НИЗУ), второе название - flash ROM. Именно в таком порядке, как перечислено, они и были разработаны. Самые первые ПЗУ, как понятно из названия, были неперезаписываемые и представляли собой матрицу с выжженным программным кодом. Такой тип BIOS просуществовал очень недолго. Первое ППЗУ было создано в конце 1970-х годов фирмой Texas Instruments. Его емкость составляла 2 Мбит и оно было выполнено в виде микросхемы с возможностью лишь однократной записи. Несколько позже на смену ППЗУ пришла EPROM и код Базовой Системы Ввода/Вывода стали записывать в перезаписываемую EPROM (Erasable PROM, стираемую программируемую память только для чтения). Достаточно привычный тип микросхем BIOS'cnk а именно EEPROM получили широкое распространение только в 1994 году. Такие микросхемы могут быть перезаписаны с

помощью специальных программ прямо на компьютере. Запись новой версии BIOS обычно называется «перепрошивкой». Эта операция может понадобиться, чтобы добавить в код BIOS новые функции, исправить ошибки или заменить поврежденный код BIOS.

В настоящее время среди разработчиков BIOS для персональных компьютеров наиболее известны три фирмы. Во-первых, это **American Megatrends, Inc**. Было время, когда BIOS разработки этой фирмы (AMI BIOS) стояли практически на всех компьютерах. Затем постепенно их вытеснили BIOS производства **Award Software, Inc**. Но в последнее время ситуация изменилась и AMI BIOS снова завоевал заслуженную популярность у производителей. Его используют такие известные производители материнских плат, как ASUS, Gigabyte, MSI, ESC и другие. Второй по алфавиту идет фирма Intel. Некоторое время назад на своих материнских платах она использовала модифицированный BIOS производства American Megatrends, Inc. — он так и назывался Intel/AMI BIOS. Сейчас, после существенной переработки, упоминание о American Megatrends, Inc. исчезло и на современных материнских платах используется уже собственный Intel BIOS, но в отличие от других компаний-разработчиков BIOS, Intel использует свои наработки только на собственных материнских платах. И, наконец, третий весьма влиятельный производитель этого рынка - **Phoenix Technologies**. До поглощения Award Software, Inc. (во времена процессоров Pentium — Pentium II) Phoenix BIOS не был особо популярен у производителей материнских плат, а вот Award BIOS самостоятельной тогда Award Software, Inc. использовался на подавляющем большинстве компьютеров. Так что приобретение Award Software, Inc. позволило Phoenix Technologies существенно расширить занимаемую долю рынка, и сейчас BIOS Phoenix Technologies (торговые марки — Award BIOS, Phoenix Award BIOS, Phoenix Award Workstation BIOS) используются практически всеми производителями материнских плат. Он даже более популярен, чем AMI BIOS.

В начале 2000г. компания Intel объявила, что собирается заменить BIOS выпуском первой версии EFI (extensible firmware interface). В сущности, EFI - «мини-ОС» с собственными правами, способная работать с сетями, графикой, клавиатурой и памятью. Эта система предусматривает загрузку с Flash ROM, как и BIOS, но, загрузившись в EFI, можно будет протестировать систему на работоспособность, зайти в Интернет без загрузки основной операционной системы. Это новый стандарт для архитектуры, интерфейса и услуг марки встроенного программного обеспечения ПК, но на данный момент у этой системы еще много недостатков и недоработок.

Понятие CMOS

Системные платы включают отдельный блок оперативной памяти, основанный на схеме малой мощности CMOS RAM (Complementary Metal- Oxide Semiconductor RAM), который сохраняется действующим с помощью батареи даже после отключения питания ПК и располагается в контроллере периферии. Он используется, чтобы сохранять основную информацию о конфигурации ПК: номера и тип жестких дисков, объем памяти, какой вид и т. д. Это можно вводить вручную, но современные BIOS автоконфигурирования делают многое из этой работы, и в CMOS сохраняются более важные параметры настройки типа выбора периода регенерации динамической оперативной памяти. В момент запуска компьютера BIOS считывает содержимое памяти CMOS в оперативную память компьютера, а также содержит программу настройки параметров системы (CMOS Setup), посредством которой можно изменить содержимое памяти CMOS. Другие важные данные, сохраняемые в CMOS, - время и дата, которые модифицируются часами реального времени (RTC - real time clock).

Понятие интерфейса BIOS

Чтобы войти в BIOS Setup. Нужно вовремя процедуры первоначального тестирования компьютера нажать определенную клавишу или их комбинацию. Наиболее часто используется Delete, реже F1 или F2; есть и другие варианты.

Интерфейс - совокупность средств и методов взаимодействия между элементами

системы. BIOS представляет собой интерфейс между аппаратным обеспечением и операционной системой.

Как правило, программа BIOS Setup имеет текстовый интерфейс и управляется с помощью клавиатуры. В главном окне BIOS Setup присутствует меню со списком основных разделов программы Setup. Главное меню BIOS Setup обычно расположено в два столбца, этот вариант используется в различных версиях AwardBIOS и AMIBIOS. Подобный интерфейс применяется в системных платах большинства производителей: Gigabyte, MSI, Foxconn, ECS, Abit и многих других. Другой распространенный вариант интерфейса BIOS Setup - со строкой меню в верхней части экрана. Такой интерфейс используется в PhoenixBIOS, Intel BIOS, а также в некоторых версиях Award BIOS и AMIBIOS . Этот вариант интерфейса используется в системных платах производства ASUS, AsRock, Intel и некоторых других.

Назначение POST

POST (Power On Self Test) - самотестирование процессора, модулей оперативной памяти, набора микросхем, дисководов, клавиатуры и других жизненно важных компонентов компьютерной системы при включении её электропитания.

POST - программа, расположенная в микросхеме BIOS, загружается первой после включения питания компьютера. Она детектирует и проверяет установленное оборудование, настраивает устройства и готовит их к работе. Если во время самотестирования будет обнаружена неисправность оборудования, то процедура POST будет остановлена с выводом соответствующего сообщения или звукового сигнала. Если же все проверки прошли успешно, самотестирование завершается вызовом встроенной подпрограммы для загрузки операционной системы.

Процесс самопроверки включает:

- проверка программы BIOS;
- обнаружение и инициализацию основных системных шин и устройств, а также выполнение программ заложенных в устройства и обеспечивающих их самоинициализацию;
- определение размера оперативной памяти и тестирования первых 64 килобайт.

Конфигурация главного меню интерфейса BIOS

В нижней части окна находится информация о производителе и программе, в верхней части расположено строковое меню, основные разделы программы (см. Рис. 3 Конфигурация главного меню BIOS):

- Main (раздел основной информации, дата и время);
- Advanced (в разделе собраны параметры дисковых накопителей, настройки для работы процессора, памяти, чипсета, периферийных устройств);
- Security (данный раздел собирает параметры для управления паролями);
- Power (в разделе устанавливаются параметры электропитания);
- Boot (здесь находятся параметры, определяющие порядок опроса загрузочных устройств, и другие настройки загрузки);
- Exit (выход из программы, возможность сохранения внесенных изменений);

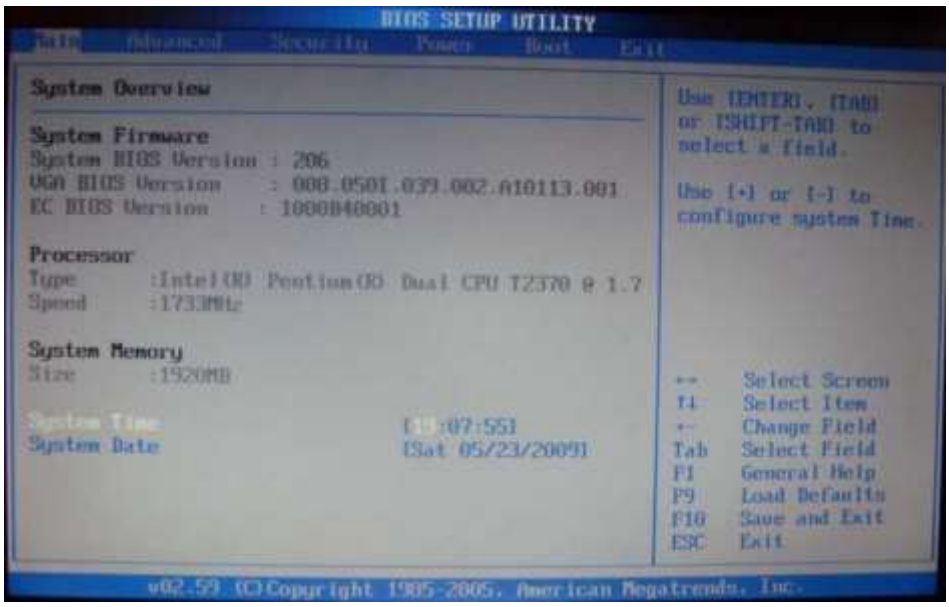


Рис. 3 Конфигурация главного меню BIOS

Перевод и трактовка терминов BIOS

Primary-первичный
Secondary-вторичный
Master-главный узел
Slave-подчиненный узел
Dev^e - устройство
IRQ - прерывание
IDE-контроллер
Bus Mastering- пересылка данных по шине без участия ЦП

Primary IDE Master (см. Рис. 4 Advanced)

Здесь указываются характеристики или тип накопителя (жесткого диска), подключенного как основной, к первичному (или единственному) IDE- каналу стандартного IDE/SATA-контроллера чипсета материнской платы.

Primary IDE Slave (см. Рис. 4 Advanced)

Здесь указываются характеристики или тип накопителя (жесткого диска), подключенного как ведомый, к первичному (или единственному) IDE- каналу стандартного IDE/SATA-контроллера чипсета материнской платы.

Secondary IDE Master (см. Рис. 4 Advanced)

Здесь указываются характеристики или тип накопителя (жесткого диска), подключенного как основной, к вторичному (если он есть) IDE-каналу стандартного IDE/SATA-контроллера чипсета материнской платы.

Secondary IDE Slave (см. Рис. 4 Advanced)

Здесь указываются характеристики или тип накопителя (жесткого диска), подключенного как ведомый, к вторичному (если он есть) IDE-каналу стандартного IDE/SATA-контроллера чипсета материнской платы.

IDE Configuration (см. Рис. 4 Advanced)

Опция дает возможность сконфигурировать современный IDE/SATA- контроллер чипсета.

Рис. 4 Advanced

Boot Device (см. Рис. 5 Boot Device Priority)

Параметр определяет носитель для загрузки системы. First Boot Device - параметр для первоочередной загрузки системы, если с этого устройства загрузиться невозможно, компьютер обратится к тем, которые указаны в параметрах Second Boot Device и Third Boot Device.

Рис. 5 Boot Device Priority

Bus Mastering (см. Рис. 6 Virtual Machine)

Опция дает возможность управления (пересылки данных) шиной устройством, без участия центрального процессора.

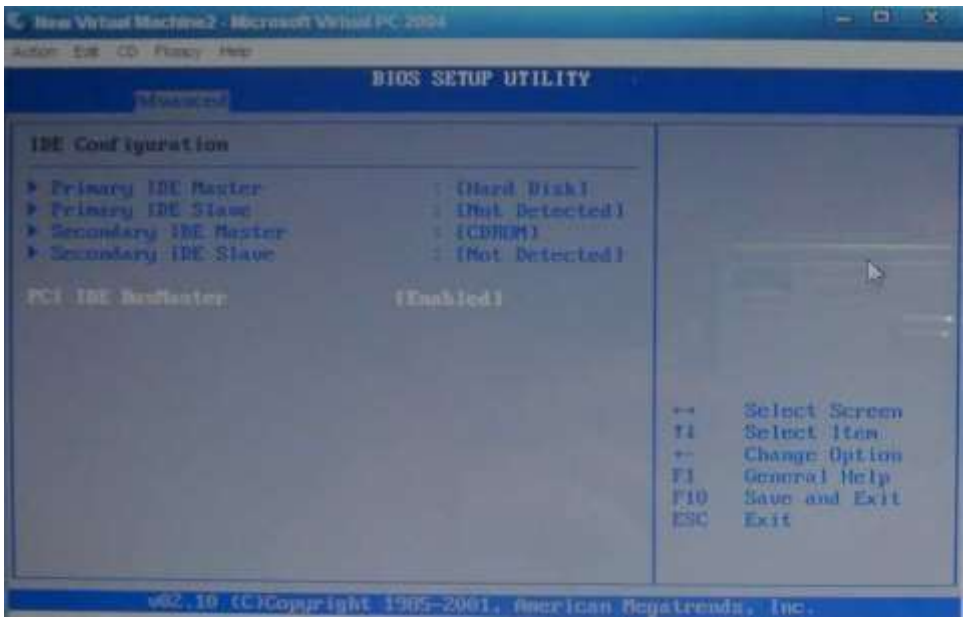


Рис. 6 Virtual Machine

IRQ

Прерывание - это приостановка процессором выполнения основной программы для обработки события, поступившего от внешнего устройства, когда возникает ситуация, требующая вмешательства процессора (например, была нажата клавиша), устройство посылает специальный сигнал - запрос на прерывание (lRQ)

Группировка параметров подменю интерфейса настроек BIOS Future Setup

Группировка параметров подменю раздела:

1. Обеспечение безопасности системы и настроек (осуществляется в разделе Security)

- Supervisor Password
- User Password
- Boot Sector Virus Protection
- I/O Interface Security
- Hard Disk Password

2. Управление процессом загрузки (осуществляется в разделе BooWBoot Device Priority)

- 1st Boot Device - Removable Device
- 2nd Boot Device - Hard Drive
- 3rd Boot Device - CD/DVD

Поведение ПК при различных вариантах установки параметров: Virus Warning, Quick Power On Self Test, Boot Sequence, Security Option

Virus Warning (см. Рис. 7 Security и Virus Warning).

Включив этот параметр, можно оградить загрузочный сектор жесткого диска от изменений на уровне BIOS: любые попытки вторгнуться в загрузочные области будут блокироваться. Это неплохая защита от типов вирусов, которые записываются в указанные области. Блокируя, система может выводить на экран соответствующее предупреждение. В таком случае пользователь выбирает, разрешить или запретить запись в загрузочный сектор. Если сообщение отображается, программа, обратившаяся к загрузочной области, может зависнуть

или вызвать сбой операционной системы.
Enabled (On) - защита загрузочного сектора включена, и все способы его изменить будут п ресекаться;
Disabled (Off) - запись в загрузочный сектор разрешена.

Quick Power On Self Test (см. Рис. 8 Quick Boot).

Параметр разрешает более быструю процедуру первоначального тестирования (POST) и существенно ускоряет загрузку в целом. При этом пропускаются некоторые тесты, наиболее важный из которых - полный тест оперативной памяти. Он обычно выполняется за несколько проходов и продолжается до нескольких десятков секунд.
Возможные значения:
Enabled (On) - выполняется ускоренный тест;
Disabled (Off) - выполняется полный тест.

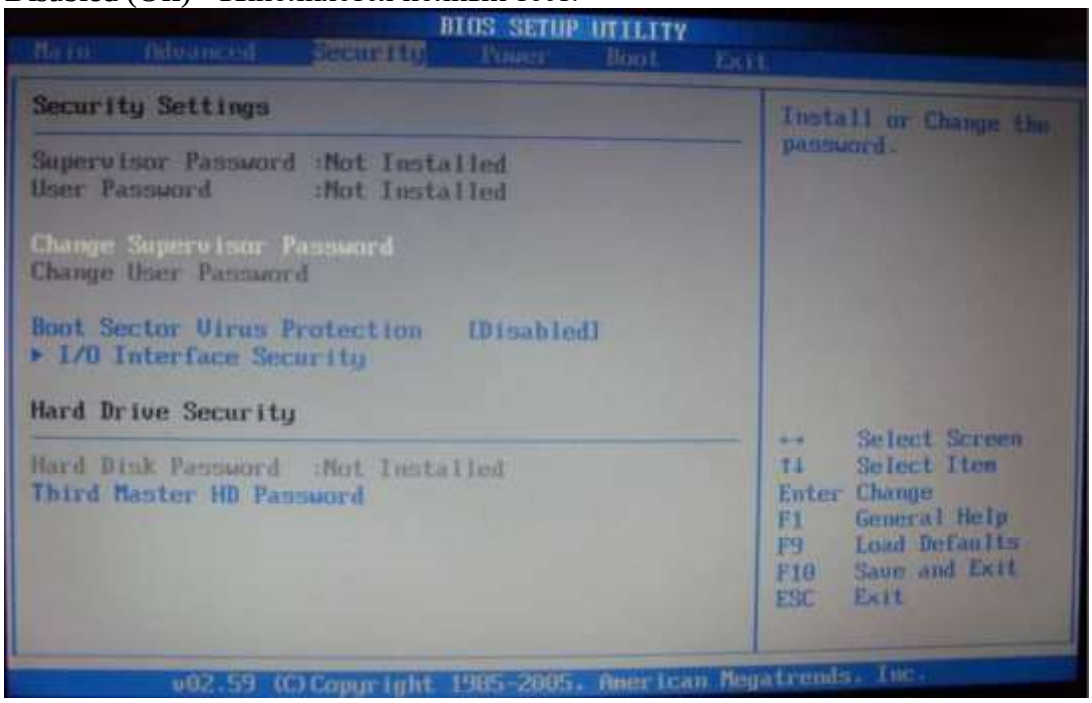


Рис. 7 Security и Virus Warning

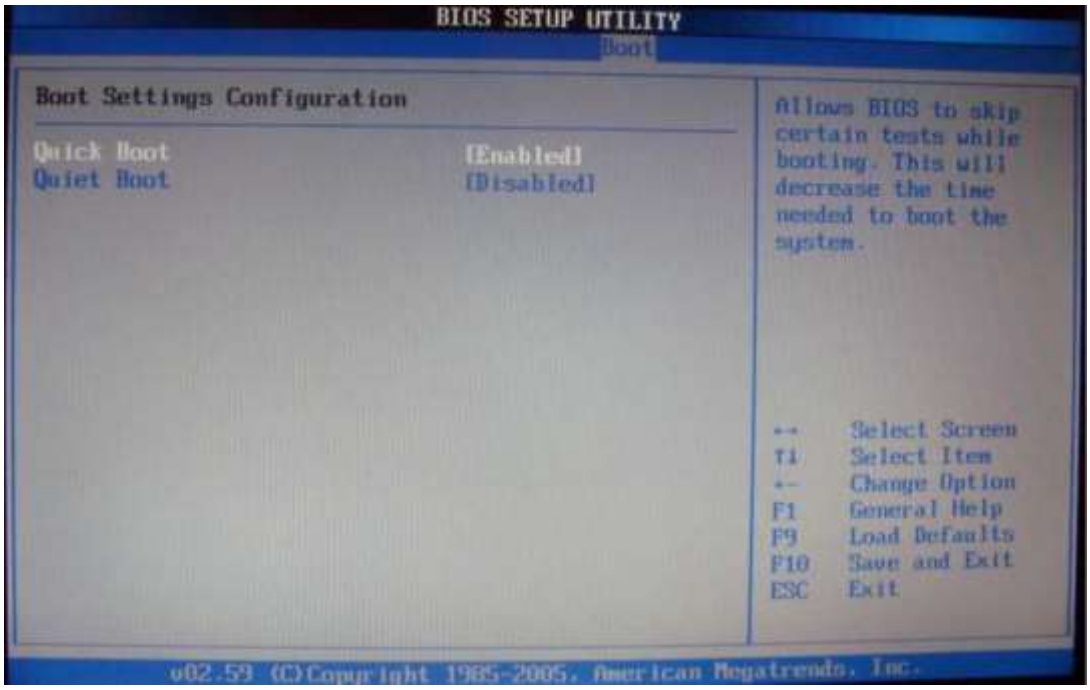


Рис. 8 Quick Boot

Boot Sequence (см. Рис. 5 Boot Device Priority) - последовательность начальной загрузки системы. Определяется последовательность опроса различных накопителей для загрузки операционной системы. Эти устройства обозначаются либо буквами, для физических жестких дисков и обычных дисководов, либо названием устройства. В некоторых версиях BIOS опция Boot Sequence трансформировалась в несколько самостоятельных опций, например: First Boot Device, Second Boot Device.

Security Option (см. Рис. 7 Security и Virus Warning) - опция, позволяющая ограничить доступ к системе и к BIOS Setup, или только к BIOS Setup. Выбор «System» блокирует загрузку компьютера и доступ к BIOS Setup. Вход в систему возможен только при вводе правильного пароля. Выбор «Setup» не ведет к блокировке загрузки ПК, но блокирует вход в BIOS Setup. По умолчанию - «Setup».

Общая характеристика разделов BIOS - Chipset Features Setup, Power Management Setup.

Chipset Features Setup

Данный раздел описывает настройки чипсета, а значит, его содержимое зависит от типа чипсета, на котором построена системная плата. Если быть более точным, то здесь присутствуют параметры, относящиеся к северному мосту чипсета и определяющие работу оперативной памяти, процессора, видеосистемы, шин AGP, PC1 и некоторых других устройств.

Power Management Setup (см. Рис. 9 Power Management Settings) - опция управления энергосбережением, осуществляющая основной контроль за функциями энергосбережения, включая снижение энергопотребления жесткого диска, режимы резервирования, приостанавливающие режимы, включение таймеров устройств и др., которые все вместе составляют аппаратную схему консервации.

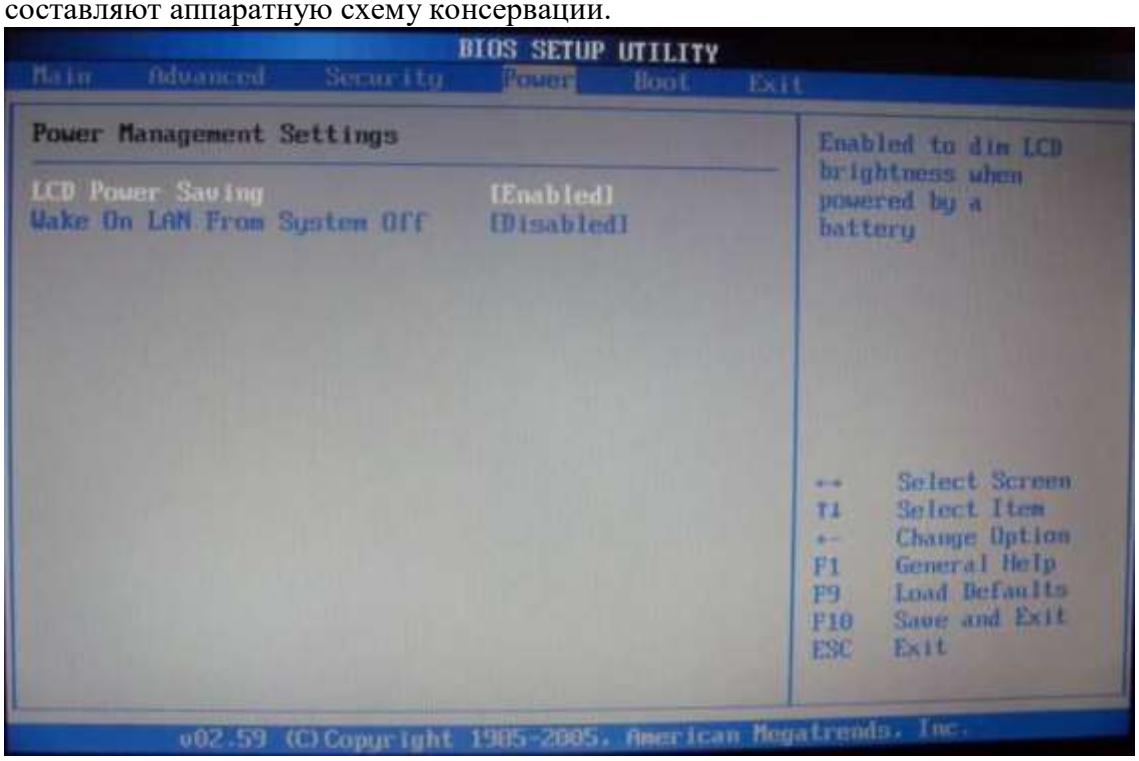


Рис. 9 Power Management Settings

Возможности управления настройками периферийных устройств в BIOS

Управление настройками периферийных устройств осуществляется в разделе I/O Interface Security (см. Рис. 10 I/O Interface Security).

BTOS SETUPUTILITY
I/O Interface Security
Express Card Interface LAN Network Interface Wireless Network Interfa USB Interface
[UNLOCKED! [UNLOCKED] [UNLOCKED] [UNLOCKED]

В данном разделе реализуется поддержка USB-устройств на уровне BIOS, использование интегрированного на материнской плате аудиочипа, управление режимами обмена данными стандартного IDE-контроллера чипсета, контроллером дисковода, последовательными портами и другим интегрированными компонентами.

USB Controllers (контроллеры USB): функция позволяет ограничить функциональность контроллеров Universal Serial Bus (USB).

USB Keyboard Support (USB Keyboard Legacy Suppor): поддержка USB - клавиатуры.

USB Mouse Support -поддержка USB-мыши.

OnBoard LAN Boot ROM: опция позволяет разрешить (значение Enabled) или запретить (Disabled) сетевую загрузку компьютера посредством интегрированного сетевого адаптера.

Onboard Serial Port 1- встроенный последовательный порт.

Onboard Parallel Port (встроенный параллельный порт): эта функция позволяет выбрать режим параллельного порта или вообще его отключить.

Onboard H/W LAN: опция отвечает за интегрированный сетевой контроллер. Это может быть как стандартный сетевой интерфейс чипсета, так и полноценная сетевая карта с интерфейсом PCI или PCI Express, распаянная на материнской плате.

Audio Controller (Onboard Audio Chip): параметр управляет работой интегрированного звукового адаптера.

HD Audio, HDA Controller, High Definition Audio, Azalia Codec: новые модели системных плат могут быть оснащены интегрированным звуковым контроллером с возможностью многоканального высококачественного воспроизведения звука (High Definition Audio). Рассматриваемый параметр позволяет включать или выключать этот адаптер.

Настройка жестких Дисков. Возможности S.M.A.R. T. - Диагностики.

Настройками жестких дисков можно управлять из следующих разделов BIOS:

- Boot Settings - определяется последовательность опроса различных накопителей для загрузки операционной системы, указывается жесткий диск.
- Advanced Settings (IDE Configuration) - указываются характеристики или тип накопителя (жесткого диска), подключенного как основной, к третичному (если он есть) IDE-каналу стандартного IDE/SATA- контроллера чипсета материнской платы.

S.M.A.R.T. for Hard Disks или функция HDD S.M.A.R.T. Capability (Self-Monitoring, Analysis And Reporting Technology - «Самоконтроль, анализ и отчетность»). S.M.A.R.T. позволяет контролировать множество параметров накопителя, осуществляя раннюю диагностику и профилактику сбоев, формировать прогноз, предупреждать о возможных проблемах накопителя и т.д. К контролируемым параметрам можно отнести, например, высоту полета головок над поверхностью диска, скорость передачи данных, количество перенесенных (передвинутых в другие области) секторов и неудачных попыток чтения и записи и т.п.

Для анализа надежности жесткого диска используются две группы параметров. Первая характеризует параметры естественного старения жесткого диска (количество циклов включения/выключения, количество оборотов двигателя за время работы, количество

перемещений головок). Вторая группа параметров информирует о текущем состоянии накопителя (расстояние между головкой и поверхностью диска, скорость обмена данными между поверхностью носителя и дисковой кэш-памятью, количество переназначений плохих секторов, количество ошибок поиска, скорость поиска данных на диске).

Технология S.M.A.R.T. прошла в своем развитии через 3 стадии: от мониторинга совокупности определенных параметров диска и обеспечения предсказания ошибок через выполнение ряда профилактических операций в состоянии ожидания до определенных сбойных секторов с попытками их восстановления. Все эти алгоритмы уже реализованы в электронике современных дисков.

Практическая часть.

Задание 1. Запустили симулятор BIOS. Выбрав раздел «Demo» изучите конфигурацию главного интерфейса в симуляторе и на примере теоретического раздела опишите основные составляющие.

Задание 2. Выполните практическое задание по настройке BIOS. Для этого в симуляторе выберите «Тест». Не закрывайте окно с результатом тестирования до проверки преподавателем.

Замечание: Рабочая (внутренняя) частота процессора получается в результате умножения коэффициента (Frequency Ratio/Multiplier), на частоту системной шины.

Список источников и литературы

Литература

1. Зозуля Ю. Н. BIOS на 100%. - СПб.: Питер,2015. - 336с.: ил. -

(Серия «На 100%»)

2. Максимов Н. В., Партыка Т. Л., Попов И. И. Технические средства информатизации: учебник. - 2-е изд., перераб. и доп. - М.: ФОРУМ: ИНФАРА-М, 2008. - 592 с.: ил.

Электронные ресурсы

3. Александр Микляев. Сайт, посвященный настройкам BIOS. Web: http://www.probios.ru

Практическая работа №5. Тестирование HDD и приводов (RW, DVD).

Теоретическая часть HDD диски

Во всех современных компьютерах имеется жесткий диск, который предназначен для хранения данных, а также для загрузки операционной системы.

Жесткий диск (Hard Disk Drive, HDD, винчестер, накопитель на жестких магнитных дисках-НЖМД), является прямым потомком дисковода для гибких дисков.

Основное предназначение жесткого диска — он должен предоставить пользователю дисковое пространство, нужное для хранения файлов операционной системы и всех необходимых программ.

Особенностью жесткого диска в отличие от дисковода для гибких дисков является высокая надежность хранения данных.

Корпус винчестера

Корпус винчестера защищает жесткий диск от повреждений. Воздух, которым заполнен корпус, обязательно должен быть очищен от пыли, иначе даже самая маленькая частица при попадании внутрь может привести в негодность все устройство. Поэтому практически все модели винчестеров имеют фильтр, который представляет собой небольшое окошко, закрытое прочным материалом, пропускающим незначительное количество воздуха.

Внутри корпуса размещаются практически все элементы, необходимые для работы винчестера: носитель информации, который представляет собой жесткие диски, а также устройство считывания/записи информации (магнитные головки и устройство позиционирования).

Габаритные размеры современных жестких дисков характеризуются так называемым форм-фактором, который указывает горизонтальный и вертикальный размеры корпуса. Возможны следующие горизонтальные размеры: 1,8; 2,5; 3,5 или 5,25", из них наиболее распространены два последних (хотя самый последний встречается все реже и реже).

Носитель информации

Винчестер содержит один или несколько дисков (platters), то есть это носитель, который смонтирован на оси-шпинделе, приводимом в движение специальным двигателем (часть привода). Скорость вращения современных винчестеров может быть 5400, 7200, 10000 об/мин. Достигнуты скорости вплоть до 15 000 об/мин., но такие винчестеры пока что слишком дороги для среднего пользователя. Понятно, что чем выше скорость вращения, тем быстрее считывается информация с диска. Следует иметь в виду, что чем выше скорость вращения, тем выше уровень шума, издаваемый винчестером. Это является довольно неприятной платой за высокую скорость работы.

Сами диски представляют собой обработанные с высокой точностью керамические или алюминиевые пластины, на которые и нанесен специальный магнитный слой (покрытие). С обеих сторон диски покрыты тончайшим слоем ферромагнитного материала (окисью какого-нибудь металла), подобного тому, что применяется для производства, например, дискет. От прочности покрытия зависят некоторые эксплуатационные характеристики, к примеру, ударопрочность винчестеров. В качестве рабочей поверхности обычно используют обе стороны каждого диска, кроме дисков, расположенных по краям пакета
— у этих дисков внешние поверхности, повернутые в сторону корпуса, для хранения информации не используются. Они являются защитными.

Количество дисков может быть различным - от одного до пяти и выше, число рабочих поверхностей при этом соответственно в два раза больше, правда, не всегда. Иногда наружные поверхности крайних дисков или одного из них не используются для хранения данных, при этом число рабочих поверхностей уменьшается и может оказаться нечетным.

Магнитные головки

Наиболее важной частью любого накопителя являются головки чтения-записи (read- write head). Головки представляют собой магнитные управляемые контуры с сердечниками, на обмотки которых подается переменное напряжение. Принцип действия очень похож на принцип работы головок обычного магнитофона, только требования к ним предъявляются значительно более жесткие.

Количество магнитных головок всегда равно количеству физических поверхностей, используемых для хранения данных. Каждая пара головок одета на своеобразную "вилку", обхватывающую диск с обеих сторон. Данная "вилка" имеет очень длинный "хвост", который заканчивает массивным хвостовиком, составляющим противовес головкам и их несущим. Когда винчестер не работает, головки благодаря упругости "вилки" прижимаются к поверхности диска, что позволяет исключить их "дребезг" во время транспортировки. Все магнитные головки объединены в единый блок, что позволяет организовать их синхронное перемещение.

Практически все современные жесткие диски имеют функцию автоматической "парковки" головок. ***Парковкой*** называется процесс перемещения магнитных головок в специальную зону диска, которая называется ***парковочной зоной"*** (от англ. ***Landing Zone).*** Эта зона не содержит абсолютно никакой полезной информации, кроме специальной сервисной метки, указывающей на местоположение места "парковки". В "запаркованном" состоянии жесткий диск можно транспортировать при достаточно плохих физических условиях — вибрация, легкие удары, сотрясения.

Функция "парковки" реализована достаточно просто. В нерабочем состоянии хвостовик блока головок "приклеивается" к небольшому магниту, расположенному в устройстве позиционирования. При поступлении напряжения питания на жесткий диск генерируется достаточно мощный электромагнитный импульс, который "отрывает" хвостовик от посадочного места. Пока жесткий диск работает, постоянно удерживаемое электромагнитное

поле не дает хвостовику "прилипнуть" к магниту. Когда же напряжение питания исчезает, то головки за счет притяжения постоянного магнита практически мгновенно перемещаются в зону парковки, где они благополучно приземляются на поверхность дисков.

Заметим, что в современных винчестерах головки как бы «летят» на расстоянии доли микрона от поверхности дисков, не касаясь их.

Устройство позиционирования

Устройство позиционирования, которое перемещает магнитные головки, внешне очень похоже на башенный кран. С одной стороны находятся длинные тонкие несущие магнитных головок, а с другой — короткий и значительно более массивный хвостовик с обмоткой электромагнитного привода. Обмотку позиционера окружает статор, представляющий собой постоянный магнит. При подаче в обмотку электромагнита тока определенной величины и полярности хвостовик начинает поворачиваться в соответствующую сторону с ускорением, пропорциональным силе тока. При изменении полярности тока хвостовик начинает движение в обратную сторону. Динамически изменяя уровень и полярность тока, можно устанавливать магнитные головки в любое

возможное положение (от центра до края дисков). Такую систему иногда называют Voice Coil (звуковая катушка) — по аналогии с диффузором громкоговорителя. Данное устройство позиционирования еще называют ***линейным двигателем.*** Применение в качестве движущей силы электромагнитного поля придает головкам равномерное ли - нейное перемещение, чего так не хватает шаговым двигателям, которые используются в дисководах для гибких дисков.

Для определения необходимого положения головок служат специальные сервисные метки, записанные на носитель при изготовлении винчестера и считываемые при позиционировании. В некоторых моделях винчестеров под сервисную информацию отводят отдельную поверхность и специализированную магнитную головку, позволяющую с высокой скоростью определить точное местоположение остальных головок, двигающихся синхронно с ней. Если сервисные метки записаны на тех же дорожках, что и данные, то для них выделяется специальный сектор, а чтение производится теми же головками, что и чтение данных. Благодаря использованию линейного двигателя появилась возможность "тонкой настройки" головок путем их незначительного перемещения относительно дорожки, что помогает более точно отследить центр окружности сервисной метки. В результате повышается достоверность считываемых данных и исключается необходимость временных затрат на процедуры коррекции положения головок, как это происходит в дисководах.

Плата электроники

Внутри любого винчестера обязательно находится печатная плата с электронными компонентами. Печатная плата, на которой расположены электронные компоненты системы управления жестким диском, обычно прикрепляется к нижней плоскости корпуса при помощи обычных винтов. В зависимости от модели электроника может быть либо закрыта металлической пластиной, либо открыта для любых механических воздействий — производители по-разному представляют реальные условия эксплуатации жесткого диска. С внутренней частью винчестера плата соединяется при помощи специального разъема.

Плата электроники предназначена для управления работой механических подвижных частей устройства и формирования электрических импульсов при чтении/записи. Она содержит:

- микропроцессор, управляющий всей остальной электроникой жесткого диска;
- буферную память, предназначенную для временного хранения данных, которые записываются на диск или считываются с него;
- микросхему ПЗУ, используемую для хранения алгоритмов работы, как основного микропроцессора, гак и всех остальных электронных компонентов;
- генератор, питающий переменным током двигатель дисков;
- сложную сервисную систему, которая управляет устройством позиционирования блока головок на требуемую дорожку (цилиндр) в соответствии с поступающими сигналами;

- усилители записи, формирующие электрические импульсы, которые подаются на магнитные головки при записи данных;
- усилители считывания и формирователи выходных сигналов при считывании информации.

Микропроцессор представляет собой специализированную микросхему, внутренняя структура которой направлена на обработку массивов данных, поступающих в схему электроники, как со стороны магнитных головок, так и со стороны компьютера. Основной задачей этой микросхемы является преобразование цифровых потоков
данных, поступающих из компьютера в электромагнитные импульсы, записываемые на диск, а также обратная операция: преобразования считываемых импульсов в поток цифровых данных. Помимо этого микропроцессор занимается постоянным наблюдением за состоянием всех функций винчестера, чтобы можно было прогнозировать возможный выход его из строя.

Буферная память необходима жесткому диску, чтобы немного согласовать разницу в скорости работы интерфейса с реальной скоростью чтения/записи с дисков. При записи информации она сначала сохраняется в буфере, а уже затем записывается на поверхность дисков. При чтении информации используется немного другой режим: данные передаются сразу же на интерфейс и параллельно записываются в буферную память. При повторном обращении к этим же данным чтение производится уже из буфера. На современных жестких дисках объем буферной памяти (иногда встречается название кэш-память винчестера) может достигать 2 Мбайт и более, что является оптимальным для большинства выполняемых компьютером задач.

Микросхема ПЗУ предназначена для хранения алгоритмов работы микропроцессора, а также технической информации, которую можно прочитать при помощи различных тестовых утилит (модель винчестера, серийный номер и т. д.). Некоторые дешевые модели жестких дисков хранят всю служебную информацию на дисках и при каждом включении загружают ее в обыкновенный модуль оперативной памяти.

Интерфейсная логика представляет целый набор электронных компонентов, задача которых сводится к организации соединения с компьютером, т. е. создании физического соединения интерфейса жесткого диска с контроллером компьютера.

Важным компонентом электронной платы являются разъемы для подключения соединительного кабеля и напряжения питания (рис. 10.3). Между этими разъемами, как правило, располагается набор перемычек, при помощи которых изменяется конфигурация жесткого диска (Master, Slave). Описание всех возможных вариантов вы, скорее всего, найдете на наклейке, которая имеется на верхней плоскости корпуса.

Плата интерфейсной электроники современного винчестера, представляет собой самостоятельное устройство с собственным процессором, памятью, устройствами ввода/вывода и прочими атрибутами, присущими любому компьютеру. По сути, жесткий диск это компьютер в компьютере.

Многие винчестеры имеют на плате электроники специальный технологический интерфейс с разъемом, через который при помощи стендового оборудования можно выполнять различные сервисные операции с накопителем — тестирование, форматирование, поиск и "фиксацию" дефектных участков.

SSD диски

SSD - это твердотельный накопитель (англ. ***SSD, Solid State Drive или Solid State Disk),*** энергонезависимое, перезаписываемое запоминающее устройство без движущихся механических частей с использованием флэш-памяти. SSD полностью эмулирует работу жёсткого диска

По сути SSD - это большая флэшка. В отличие от флэшек, в SSD используется микросхема DDR DRAM кеш-памяти, в связи со спецификой работы и возросшей в несколько раз скоростью обмена данными между контроллером и интерфейсом SATA.

Преимущество SSD дисков по сравнению с традиционными накопителями на жёстких дисках на первый взгляд очевидны. Это высокая механическая надёжность, отсутствие движущихся частей, высокая скорость чтения/записи, низкий вес, меньшее энергопотребление.

Контроллер SSD.

Главной задачей контроллера является обеспечение операций чтения/записи, и управление структурой размещения данных. Основываясь на матрице размещения блоков, в какие ячейки уже проводилась запись, а в какие еще нет, контроллер должен оптимизировать скорость записи и обеспечить максимально длительный срок службы SSD-диска. Вследствие особенностей построения NAND-памяти, работать с ее каждой ячейкой отдельно нельзя. Ячейки объединены в страницы объемом по 4 Кбайта, и записать информацию можно только полностью заняв страницу. Стирать данные можно по блокам, которые равны 512 Кбайт. Все эти ограничения накладывают определенные обязанности на правильный интеллектуальный алгоритм работы контроллера. Поэтому, правильно настроенные и оптимизированные алгоритмы контролера могут существенно повысить производительность и долговечность работы SSD-диска.

Flash память.

В SSD как и в USB Flash используются три типа памяти NAND: SLC (Single Level Cell), MLC (Multi Level Cell) и TLC (Three Level Cell). Отличие только в том, что SLC позволяет хранить в каждой ячейке только один бит информации, MLC - два, а TLC - три ячейки (использование разных уровней электрического заряда на плавающем затворе транзистора), что делает память MLC и TLC более дешёвой относительно ёмкости.

Как работает SSD накопитель.

Для чтения блока данных в винчестере сначала нужно вычислить, где он находится, потом переместить блок магнитных головок на нужную дорожку, подождать пока нужный сектор окажется под головкой и произвести считывание. Причем хаотические запросы к разным областям жесткого диска еще больше сказываются на времени доступа. При таких запросах HDD вынуждены постоянно «гонять» головки по всей поверхности «блинов» и даже переупорядочивание очереди команд спасает не всегда. А в SSD все просто — вычисляем адрес нужного блока и сразу же получаем к нему доступ на чтение/запись. Никаких механических операций — всё время уходит на трансляцию адреса и передачу блока. Чем быстрее флэш-память, контроллер и внешний интерфейс, тем быстрее доступ к данным.

А вот при изменении/стирании данных в SSD накопителе не так все просто. Микросхемы NAND флэш-памяти оптимизированы для секторного выполнения операций. Флеш-память пишется блоками по 4 Кб, а стирается по 512 Кб. При модификации нескольких байт внутри некоторого блока контроллер выполняет следующую последовательность действий:

S считывает блок, содержащий модифицируемый блок во внутренний буфер/кеш;

S модифицирует необходимые байты;

S выполняет стирание блока в микросхеме флэш-памяти;

S вычисляет новое местоположение блока в соответствии с требованиями алгоритма перемешивания;

S записывает блок на новое место.

Но как только вы записали информацию, она не может быть перезаписана до тех пор, пока не будет очищена. Проблема заключается в том, что минимальный размер записываемой информации не может быть меньше 4 Кб, а стереть данные можно минимум блоками по 512 Кб. Для этого контроллер группирует и переносит данные для освобождения целого блока.

Вот тут и сказывается оптимизация ОС для работы с HDD. При удалении файлов операционная система не производит физическую очистку секторов на диске, а только помечает файлы как удаленные, и знает, что занятое ими место можно заново использовать. Работе самого накопителя это никак не мешает и разработчиков

интерфейсов этот вопрос раньше не волновал. Если такой метод удаления помогает повысить производительность при работе с HDD, то при использовании SSD становится проблемой. В SSD, как и в традиционных жестких дисках, данные все еще хранятся на диске после того, как они были удалены операционной системой. Но дело в том, что твердотельный накопитель не знает, какие из хранящихся данных являются полезными, а какие уже не нужны и вынужден все занятые блоки обрабатывать по длинному алгоритму.

Прочитать, модифицировать и снова записать на место, после очистки затронутых операцией ячеек памяти, которые с точки зрения ОС уже удалены. Следовательно, чем больше блоков на SSD содержит полезные данные, тем чаще приходится прибегать к процедуре чтение->модификация->очистка->запись, вместо прямой записи. Вот здесь пользователи SSD сталкиваются с тем, что быстродействие диска заметно снижается по мере их заполнения файлами. Накопителю просто не хватает заранее стёртых блоков. Максимум производительности демонстрируют чистые накопители, а вот в ходе их эксплуатации реальная скорость понемногу начинает снижаться.

Раньше в интерфейсе ATA просто не было команд для физической очистки блоков данных после удаления файлов на уровне ОС. Для HDD они просто не требовались, но появление SSD заставило пересмотреть отношение к данному вопросу. В результате в спецификации ATA появилась новая команда **DATA SET MANAGEMENT**, более известная как **Trim**. Она позволяет ОС на уровне драйвера собирать сведения об удаленных файлах и передавать их контроллеру накопителя.

В периоды простоя, SSD самостоятельно осуществляет очистку и дефрагментацию блоков отмеченных как удаленные в ОС. Контроллер перемещает данные так, чтобы получить больше предварительно стертых ячеек памяти, освобождая место для последующей записи. Это дает возможность сократить задержки, возникающие в ходе работы. Но для реализации **Trim** необходима поддержка этой команды прошивкой накопителя и установленным в ОС драйвером. На данный момент только самые последние модели SSD «понимают» TRIM, а для старых накопителей нужно прошить контроллер для включения поддержки этой команды. Среди операционных систем команду Trim поддерживают: Windows 7, Windows Server 2008 R2, Linux 2.6.33, FreeBSD 9.0. Для остальных ОС необходимо инсталлировать дополнительные драйвера и утилиты. Например, для SSD от Intel существует специальная утилита **SSD Toolbox**, которая может выполнять процедуру синхронизации с ОС по расписанию. Кроме оптимизации, утилита позволяет выполнять диагностику SSD.

О надёжности SSD.

Самый большой источник проблем - контроллер и его прошивка. По причине того, что контроллер физически расположен между интерфейсом и микросхемами памяти, вероятность его повреждения в результате сбоя или проблем с питанием очень велика. При этом сами данные, в большинстве случаев сохраняются. Помимо физических повреждений, при которых доступ к данным пользователя невозможен, существуют логические повреждения, при которых также нарушается доступ к содержимому микросхем памяти. Любая, даже незначительная ошибка, может привести к полной потере данных. Структуры данных очень сложные. Информация «размазывается» по нескольким чипам, плюс чередование, делают восстановление данных довольно сложной задачей.

В таких случаях восстановить накопитель помогает прошивка контроллера с низкоуровневым форматированием, когда заново создаются служебные структуры данных. Производители стараются постоянно дорабатывать микропрограмму,

исправлять ошибки, оптимизировать работу контроллера. По этому, рекомендуется периодически обновлять прошивку накопителя для исключения возможных сбоев.

Безопасность SSD.

В SSD накопителе, как и в HDD, данные не удаляются сразу после того, как файл был стёрт из ОС. Даже если переписать файл по верху нулями - физически данные еще остаются, и если чипы флеш-памяти достать, и считать на программаторе - можно найти 4кб

фрагменты файлов. Полное стирание данных стоит ждать тогда, когда на диск будет записано данных равное количеству свободного места + объем резерва (примерно 4 Гб для 60Гб SSD). Если файл попадёт на «изношенную» ячейку, контроллер ещё не скоро перезапишет её новыми данными.

Основные принципы, особенности, отличия в восстановлении данных с SSD и USB Flash нак

опителей.

Восстановление данных с SSD накопителей достаточно трудоёмкий и долгий процесс по сравнению с портативными flash накопителями. Процесс поиска правильного порядка, объединения результатов и выбора необходимого сборщика (алгоритм/программа полностью эмулирующая работу контроллера SSD накопителя) для создания образа диска не

Связанно это в первую очередь с увеличением числа микросхем в составе SSD накопителя, что во много раз увеличивает число возможных вариантов действий на каждом этапе восстановления данных, каждое из которых требует проверки и специализированных знаний. Так же, в силу того, что к SSD предъявляются значительно более жесткие требования по всем характеристикам (надёжность, быстродействие и т.д.), чем к мобильным флеш накопителям, технологии и методики работы с данными, применяемые в них, достаточно сложны, что требует индивидуального подхода к каждому решению и наличию специализированных инструментов и знаний.

Преимущества SSD.

- высокая скорость чтения любого блока данных не зависимо физического от расположения (более 200 Мб/с);
- низкое энергопотребление при чтении данных с накопителя (приблизительно на 1 Ват ниже, чем у HDD);
- пониженное тепловыделение (внутреннее тестирование в компании Intel показало, что ноутбуки с SSD; нагреваются на 12.2° меньше чем аналогичные с HDD);
- бесшумность и высокая механическая надёжность.

Недостатки SSD.

- высокое энергопотребление при записи блоков данных, энергопотребление растёт с ростом объёма накопителя и интенсивностью изменения данных;
- низкая ёмкость и высокая стоимость за гигабайт по сравнению с HDD;
- ограниченное число циклов записи.

В связи с высокой стоимостью SSD дисков и небольшим объёмом памяти использовать их для хранения данных нецелесообразно. Зато они отлично подойдут в качестве системного раздела, на который инсталлируется ОС и на серверах для кэширования статичных данных.

Практическая часть

1. Изучите теоретическую часть.
2. Заполните таблицу:

Характеристика	**HDD**	**SSD**
Модель накопителя (согласно варианта)		
Кратко сформулируйте принцип работы накопителя		
Форм-фактор		
Г абариты		
Вес		

Стоимость		
Устойчивость к вибрации и ударам		
Скорость чтения		
Скорость записи		

3. Ответьте на контрольные вопросы.

Вопросы для контроля

1. Какую функцию выполняет плата электроники в ЖМД?
2. От чего зависит скорость считывания информации с жесткого диска?
3. Каково назначение устройства позиционирования в ЖМД?
4. В чем причина устойчивости к ударам SSD?
5. Почему ограничено количество циклов чтения-записи в твердотельных носителях?

Список заданий по вариантам

Вариант	**HDD**	**SSD**
Вариант 1	Seagate ST500DM002	Samsung MZ-7TD500KW
Вариант 2	Western Digital WD5000AAKX	Samsung MZ-7TE500BW
Вариант 3	Seagate ST500LT012	Samsung MZ-7TE500LW
Вариант 4	Western Digital WD2503ABYX	Plextor PX-256M5S
Вариант 5	Seagate ST250DM000	ADATA Premier Pro SP900
Вариант 6	Toshiba DT01ACA050	Samsung MZ-7TD500BW

Практическая работа №6. Тестирование flash и USB-накопителей.

Цель работы: научиться работать с программами по тестированию жестких дисков и приводов. Изучить устройство и характеристики флэш-памяти, её особенности и продиагностировать скорость передачи данных флэш-памяти; научиться работать с программами по тестированию флэш- карт и флэш-накопителей. Научиться разбираться в основных характеристиках накопителей.

Время выполнения: 2 часа

Оборудование: учебный персональный компьютер.

Программное обеспечение: операционная система, презентация, тестовые программы.

Теоретические основы

Тестирование жестких дисков используют если возникло подозрение на нехорошее поведение жесткого диска, то ниже представлены **программы для подробного тестирования дисков** по многим параметрам. Но для начала лучше использовать параметры SMART. Если они показывают, что есть проблемы, то нужно скопировать информацию на другой носитель и дальше тестировать другими тестами не нужно.

ПРОГРАММЫ ПО ТЕСТИРОВАНИЮ ЖЕСТКИХ ДИСКОВ

VICTORIA

ОСНОВНЫЕ ВОЗМОЖНОСТИ ПРОГРАММЫ

- Чтение паспорта диска и вывод на экран полной технической информации о накопителе.
- Определение установленных в системе ATA/SATA контроллеров (включая дополнительные).
- Управление уровнем акустического шума.
- Просмотр S.M.A.R.T. параметров накопителя. Быстрая оценка его состояния по псевдографическим шкалам и по регистру статуса.
- Работа с Host Protected Area: изменение и восстановление физического объема диска.
- 5 режимов тестирования поверхности: верификацией, чтением и записью, с подсчетом и отображением адресов дефектных блоков.
- 2 режима построения графика поверхности: полный и оценочный (аналогично тому, как сделано в программе HD Tach).
- Дефектоскоп: анализ состояния поверхности 3-мя видами тестов, с подсчетом и отображением нестабильных участков, с указанием точных адресов каждого нестабильного сектора и автоматическим занесением их в текстовый файл.
- Тестирование буферной памяти и интерфейса на наличие «глюков» и искажения информации при приеме и передаче.
- Измерение частоты вращения вала HDD, в том числе на новых дисках без поля INDEX.

- Скрытие дефектов поверхности методом переназначения секторов из резерва (remap) на любом из 3-х тестов.
- Измерение производительности жесткого диска (бенчмарк функции):
- измерение скорости линейного, нелинейного и случайного чтения с HDD.
- измерение скорости позиционирования головок HDD и времени доступа к секторам.
- Измерение скорости чтения графическими методами.
- Очистка диска (или его части) от информации – «низкоуровневое форматирование».
- Управление опциями безопасности: установка пароля на HDD, снятие пароля, быстрое стирание информации без возможности её восстановления и т.п.
- Возможность остановки и запуска шпиндельного двигателя HDD.
- Тест позиционирования головок HDD (аналогично тому, как это делает ОС при интенсивной работе), с целью выявления надежности и термоустойчивости дисковой подсистемы ПК (приводит к разогреву HDD).
- Посекторное копирование произвольной области HDD в файл, с пропуском дефектных участков (может быть полезно для спасения информации с поврежденного диска).
- Посекторное копирование файлов на HDD.
- Просмотр информации о логических разделах HDD с указанием границ разделов (без определения HDD в BIOS).
- Индикация режимов работы HDD, содержимого регистров, и визуализация кодов ошибок по индикаторным лампочкам.
- Встроенная контекстно-зависимая система помощи.
- Существует 2 версии программы для DOS и для Windows.

MHDD

Одной из лучших программ для тестирования жестких дисков по праву считается **MHDD**. Тест **MHDD** позволяет протестировать поверхность жестких дисков на наличие, так называемых, **bad-секторов** или **bad-блоков**, проверить и управлять системой **SMART** и многое другое.

Тестовая программа жестких дисков **MHDD** распространяется в виде образа ISO, для последующей записи и загрузки с компакт-диска и в виде распаковывающегося на флоппи-дисковод FDD архива. Обе версии являются загрузочными и не требуют наличия установленной операционной системы на ПК, поэтому являются очень удобными в использовании тестами.

Тестовая программа **MHDD** состоит всего из двух файлов: **mhdd.exe** – исполнительный файл теста, и **mhdd.hlp** – файл справки для **MHDD**. После первого запуска программы создается специальный лог-файл, собирающий информацию обо всех действиях и результатах тестов.

Главное отличие теста **MHDD** от многих других тестов винчестера заключается в том, что **MHDD** не использует функции BIOS и прерывания, поэтому не обращает внимание на наличие разделов, типы файловых систем и ограничения BIOS. Благодаря встроенной справке, использование теста винчестеров **MHDD** не должно вызвать сложностей, для доступа к разделу помощи просто нажмите **F1**.

Для сканирования и проверки жесткого диска на **bad-блоки** просто выберите необходимый винчестер, нажав **SHIFT+F3** и номер жесткого диска. Далее выполните команду **SCAN** и нажмите **F4** для тестирования жесткого диска по умолчанию.

Итак, вы можете наблюдать за процессом тестирования. Обратите внимание, что серые блоки на экране обозначают нормально читающиеся блоки жесткого диска. Зеленые, желтые, красные и коричневые секторы обозначают завышенное время чтения/записи на винчестер. Значение **UNC –x** обозначает наличие нечитаемого блока (bad-сектора). В правой части экрана вы можете видеть таблицу со значениями всех секторов жесткого диска. Последние версии программы позволяют тестировать жесткие диски форматов не только IDE, но и SATA (Serial ATA), что позволяет использовать **MHDD** для тестирования современной продукции накопителей. Скачать программу можно бесплатно с сайта производителя. Там же можно скачать и документацию к программе.

УТИЛИТЫ ПРОИЗВОДИТЕЛЕЙ ЖЕСТКИХ ДИСКОВ

Программы диагностики дисков можно найти на сайтах их производителей

Western Digital: Data Lifeguard Tools (необходимо выбрать модель диска).

Seagate: SeaTools

Hitachi: Drive Fitness Test

HDDSCAN

Это очень простая и бесплатная программа для низкоуровневой диагностики накопителей HDD в операционной системе Windows. Программа поддерживает диски IDE/SATA/SCSI, RAID массивы, внешние накопители USB/Firewire, флеш-карты. В программе реализован механизм проверки дисков и отправки отчётов по e-mail по расписанию. Также программа умеет сканировать поверхность, строить график скорости чтения, просматривать атрибуты SMART, настраивать AAM, APM (Power Management).

Флеш-память

Флеш-память (англ. Flash-Memory) — разновидность твердотельной полупроводниковой энергонезависимой перезаписываемой памяти. Она может быть прочитана сколько угодно раз, но писать в такую память можно лишь ограниченное число раз (максимально — около миллиона циклов). Распространена флеш-память, выдерживающая около 100 тысяч циклов перезаписи — намного больше, чем способна выдержать дискета или CD-RW. Не содержит подвижных частей, так что, в отличие от жёстких дисков, более надёжна и компактна. Благодаря своей компактности, дешевизне и низкому энергопотреблению флеш-память широко используется в цифровых портативных устройствах — фото- и видеокамерах, диктофонах, MP3-плеерах, КПК, мобильных телефонах, а также смартфонах и коммуникаторах. Кроме того, она используется для хранения встроенного программного обеспечения в различных устройствах (маршрутизаторах, мини-АТС, принтерах, сканерах, модемах), различных контроллерах. Также в последнее время широкое распространение получили USB флеш-накопители («флешка», USB-драйв, USB-диск), практически вытеснившие дискеты и CD. Одним из первых флешки JetFlash в 2002 году начал выпускать тайваньский концерн Transcend.

На конец 2008 года основным недостатком, не позволяющим устройствам на базе флеш-памяти вытеснить с рынка жёсткие диски, является высокое соотношение цена/объём, превышающее этот параметр у жестких дисков в 2—3 раза. В

связи с этим и объёмы флеш-накопителей не так велики. Хотя работы в этих направлениях ведутся. Удешевляется технологический процесс, усиливается конкуренция. Многие фирмы уже заявили о выпуске SSD-накопителей объёмом 256 Гб и более. Например в ноябре 2009 года компания OCZ предложила SSD-накопитель ёмкостью 1 Тб и 1,5 млн циклов перезаписи. Ещё один недостаток устройств на базе флеш-памяти по сравнению с жёсткими дисками — как ни странно, меньшая скорость. Несмотря на то, что производители SSD-накопителей заверяют, что скорость этих устройств выше скорости винчестеров, в реальности она оказывается ощутимо ниже. Конечно, SSD-накопитель не тратит подобно винчестеру время на разгон, позиционирование головок и т. п. Но время чтения, а тем более записи, ячеек флеш-памяти, используемой в современных SSD-накопителях, больше. Что и приводит к значительному снижению общей производительности. Справедливости ради следует отметить, что последние модели SSD-накопителей и по этому параметру уже вплотную приблизились к винчестерам. Однако, эти модели пока слишком дороги.

Принцип действия

Флеш-память хранит информацию в массиве транзисторов с плавающим затвором, называемых ячейками (англ. cell). В традиционных устройствах с одноуровневыми ячейками (англ. single-level cell, SLC), каждая из них может хранить только один бит. Некоторые новые устройства с многоуровневыми ячейками (англ. multi-level cell, MLC) могут хранить больше одного бита, используя разный уровень электрического заряда на плавающем затворе транзистора.

NOR

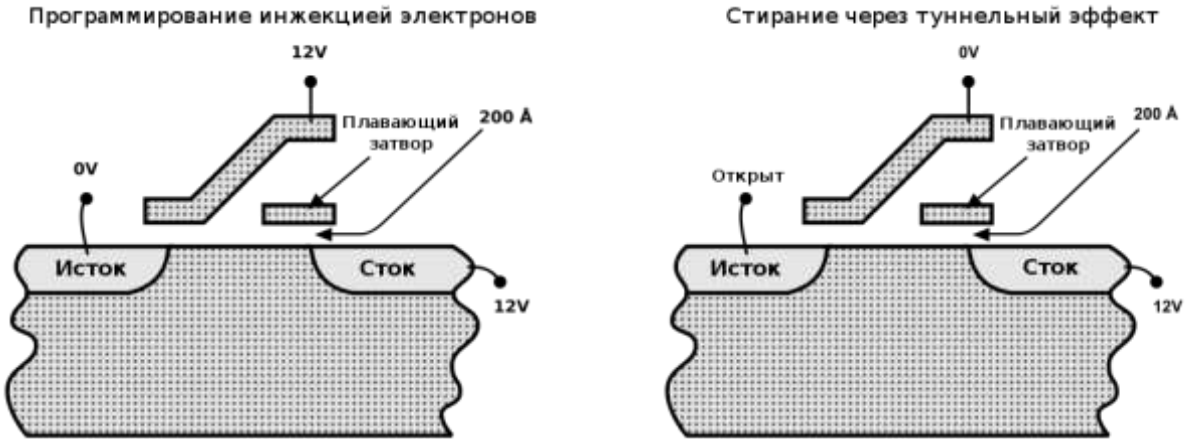
В основе этого типа флеш-памяти лежит ИЛИ-НЕ элемент (англ. NOR), потому что в транзисторе с плавающим затвором низкое напряжение на затворе обозначает единицу.

Транзистор имеет два затвора: управляющий и плавающий. Последний полностью изолирован и способен удерживать электроны до 10 лет. В ячейке имеются также сток и исток. При программировании напряжением на управляющем затворе создаётся электрическое поле и возникает туннельный эффект. Некоторые электроны туннелируют через слой изолятора и попадают на плавающий затвор, где и будут пребывать. Заряд на плавающем затворе изменяет «ширину» канала сток-исток и его проводимость, что используется при чтении.

Программирование и чтение ячеек сильно различаются в энергопотреблении: устройства флеш-памяти потребляют достаточно большой ток при записи, тогда как при чтении затраты энергии малы.

Для стирания информации на управляющий затвор подаётся высокое отрицательное напряжение, и электроны с плавающего затвора переходят (туннелируют) на исток.

В NOR-архитектуре к каждому транзистору необходимо подвести индивидуальный контакт, что увеличивает размеры схемы. Эта проблема решается с помощью NAND-архитектуры.



NAND

В основе NAND-типа лежит И-НЕ элемент (англ. NAND). Принцип работы такой же, от NOR-типа отличается только размещением ячеек и их контактами. В результате уже не требуется подводить индивидуальный контакт к каждой ячейке, так что размер и стоимость NAND-чипа может быть существенно меньше. Также запись и стирание происходит быстрее. Однако эта архитектура не позволяет обращаться к произвольной ячейке.

NAND и NOR-архитектуры сейчас существуют параллельно и не конкурируют друг с другом, поскольку находят применение в разных областях хранения данных.

История

Флеш-память была изобретена инженером компании Toshiba Фудзио Масуокой в 1984 году. Название «флеш» было придумано также в Toshiba коллегой Фудзио, Сёдзи Ариидзуми, потому что процесс стирания содержимого памяти ему напомнил фотовспышку (англ. flash). Масуока представил свою разработку на IEEE 1984 International Electron Devices Meeting (IEDM), проходившей в Сан-Франциско, Калифорния. Intel увидела большой потенциал в изобретении и в 1988 году выпустила первый коммерческий флеш-чип NOR-типа.

NAND-тип флеш-памяти был анонсирован Toshiba в 1989 году на International Solid-State Circuits Conference. У него была больше скорость записи и меньше площадь чипа.

На конец 2008 года, лидерами по производству флеш-памяти являются Samsung (31 % рынка) и Toshiba (19 % рынка, включая совместные заводы с Sandisk). (Данные согласно iSupply на Q4’2008).

Стандартизацией чипов флеш-памяти типа NAND занимается Open NAND Flash Interface Working Group (ONFI). Текущим стандартом считается спецификация ONFI версии

1.0, выпущенная 28 декабря 2006 года. Группа ONFI поддерживается конкурентами Samsung и Toshiba в производстве NAND-чипов: Intel, Hynix и Micron Technology.

Характеристики

Скорость некоторых устройств с флеш-памятью может доходить до 100 Мб/с. В основном флеш-карты имеют большой разброс скоростей и обычно маркируются в скоростях стандартного CD-привода (150 килобайт/с). Так, указанная скорость в 100× означает 100 × 150 килобайт/с = 14,65 мегабайт/с.

В основном объём чипа флеш-памяти измеряется от килобайт до нескольких гигабайт.

В 2005 году Toshiba и SanDisk представили NAND-чипы объёмом 1 Гб, выполненные по технологии многоуровневых ячеек, где один транзистор может хранить несколько бит, используя разный уровень электрического заряда на плавающем затворе.

Компания Samsung в сентябре 2006 года представила 8-гигабайтный чип, выполненный по 40-нм технологическому процессу.

В конце 2007 года Samsung сообщила о создании первого в мире MLC (multi-level cell) чипа флеш-памяти типа NAND, выполненного по 30-нм технологическому процессу с ёмкостью чипа 8 Гб. В декабре 2009 году компанией начато производство этой памяти, но объёмом 4 Гб (32 Гбит).

В то же время, в декабре 2009 года, Toshiba заявила, что 64 Гб NAND память уже поставляется заказчикам, а массовый выпуск начнётся в первом квартале 2010 года.

Для увеличения объёма в устройствах часто применяется массив из нескольких чипов. К 2007 году USB устройства и карты памяти имели объём от 512 Мб до 64 Гб. Самый большой объём USB-устройств составлял 4 терабайта.

Файловые системы

Основное слабое место флеш-памяти — количество циклов перезаписи. Ситуация ухудшается также в связи с тем, что операционные системы часто записывают данные в одно и то же место. Часто обновляется таблица файловой системы, так что первые сектора памяти израсходуют свой запас значительно раньше. Распределение нагрузки позволяет существенно продлить срок работы памяти.

Для решения этой проблемы были созданы специальные файловые системы: JFFS2 и YAFFS[для GNU/Linux и exFAT для Microsoft Windows.

USB флеш-носители и карты памяти, такие, как Secure Digital и CompactFlash, имеют встроенный контроллер, который производит обнаружение и исправление ошибок и старается равномерно использовать ресурс перезаписи флеш-памяти. На таких устройствах не имеет смысла использовать специальную файловую систему и для лучшей совместимости применяется обычная FAT.

Применение

Флеш-память наиболее известна применением в USB флеш-накопителях (англ. USB flash drive). В основном применяется NAND-тип памяти, которая подключается через USB по интерфейсу USB mass storage device (USB MSC). Данный интерфейс поддерживается всеми современными операционными системами.

Благодаря большой скорости, объёму и компактным размерам USB флеш-накопители полностью вытеснили с рынка дискеты. Например, компания Dell с 2003 года перестала выпускать компьютеры с дисководом гибких дисков.

В данный момент выпускается широкий ассортимент USB флеш-накопителей, разных форм и цветов. На рынке присутствуют флешки с автоматическим шифрованием записываемых на них данных. Японская компания Solid Alliance даже выпускает флешки в виде еды.

Есть специальные дистрибутивы GNU/Linux и версии программ, которые могут работать прямо с USB носителей, например, чтобы пользоваться своими приложениями в интернет-кафе.

Технология ReadyBoost в Windows Vista способна использовать USB флеш-накопитель или специальную флеш-память, встроенную в компьютер, для увеличения быстродействия.

На флеш-памяти также основываются карты памяти, такие как Secure Digital (SD) и Memory Stick, которые активно применяются в портативной технике (фотоаппараты, мобильные телефоны). Флеш-память занимает большую часть рынка переносных носителей данных.

NOR-тип памяти чаще применяется в BIOS и ROM-памяти устройств, таких, как DSL-модемы, маршрутизаторы и т. д. Флеш-память позволяет легко обновлять прошивку устройств, при этом скорость записи и объём для таких устройств не так важны.

Сейчас активно рассматривается возможность замены жёстких дисков на флеш-память. В результате увеличится скорость включения компьютера, а отсутствие движущихся деталей увеличит срок службы. Например, в XO-1, «ноутбуке за 100 $», который активно разрабатывается для стран третьего мира, вместо жёсткого диска будет использоваться флеш-память объёмом 1 Гб. Распространение ограничивает высокая цена и меньший срок службы, чем у жёстких дисков, из-за ограниченного количества циклов перезаписи.

Типы карт памяти

Существуют несколько типов карт памяти, используемых в портативных устройствах:

CF (Compact Flash): карты памяти CF являются старейшим стандартом карт флеш-памяти. Первая CF карта была произведена корпорацией SanDisk в 1994 году. Этот формат

памяти очень распространен. Чаще всего в наши дни он применяется в профессиональном фото и видео оборудовании, так как ввиду своих размеров (43×36×3,3 мм) слот расширения для Compact Flash-карт физически проблематично разместить в мобильных телефонах или MP3-плеерах. Зато ни одна карта не может похвастаться такими скоростями, объемами и надежностью, как CF.

MMC (Multimedia Card): карта в формате MMC имеет небольшой размер — 24×32×1,4 мм. Разработана совместно компаниями SanDisk и Siemens. MMC содержит контроллер памяти и обладает высокой совместимостью с устройствами самого различного типа. В большинстве случаев карты MMC поддерживаются устройствами со слотом SD.

RS-MMC (Reduced Size Multimedia Card): карта памяти, которая вдвое короче стандартной карты MMC. Её размеры составляют 24×18×1,4 мм, а вес — около 6 г, все остальные характеристики не отличаются от MMC. Для обеспечения совместимости со стандартом MMC при использовании карт RS-MMC нужен адаптер.

DV-RS-MMC (Dual Voltage Reduced Size Multimedia Card): карты памяти DV-RS-MMC с двойным питанием (1,8 и 3,3 В) отличаются пониженным энергопотреблением, что позволит работать мобильному телефону немного дольше. Размеры карты совпадают с размерами RS-MMC, 24×18×1,4 мм.

MMCmicro: миниатюрная карта памяти для мобильных устройств с размерами 14×12×1,1 мм. Для обеспечения совместимости со стандартным слотом MMC необходимо использовать переходник.

SD Card (Secure Digital Card): поддерживается фирмами SanDisk, Panasonic и Toshiba. Стандарт SD является дальнейшим развитием стандарта MMC. По размерам и характеристикам карты SD очень похожи на MMC, только чуть толще (32×24×2,1 мм). Основное отличие от MMC — технология защиты авторских прав: карта имеет криптозащиту от несанкционированного копирования, повышенную защиту информации от случайного стирания или разрушения и механический переключатель защиты от записи. Несмотря на родство стандартов, карты SD нельзя использовать в устройствах со слотом MMC.

SDHC (SD High Capacity, SD высокой ёмкости): Старые карты SD (SD 1.0, SD 1.1) и новые SDHC (SD 2.0) и устройства их чтения различаются ограничением на максимальную ёмкость носителя, 4 Гб для SD и 32 Гб для SDHC. Устройства чтения SDHC обратно совместимы с SD, то есть SD-карта будет без проблем прочитана в устройстве чтения SDHC, но в устройстве SD карта SDHC не будет читаться вовсе. Оба варианта могут быть представлены в любом из трёх форматов физических размеров (стандартный, mini и micro).

miniSD (Mini Secure Digital Card): От стандартных карт Secure Digital отличаются меньшими размерами 21,5×20×1,4 мм. Для обеспечения работы карты в устройствах, оснащённых обычным SD-слотом, используется адаптер.

microSD (Micro Secure Digital Card): являются на настоящий момент (2008) самыми компактными съёмными устройствами флеш-памяти (11×15×1 мм). Используются, в первую очередь, в мобильных телефонах, коммуникаторах, и т. п., так как, благодаря своей компактности, позволяют существенно расширить память устройства, не увеличивая при этом его размеры. Переключатель защиты от записи вынесен на адаптер microSD-SD.

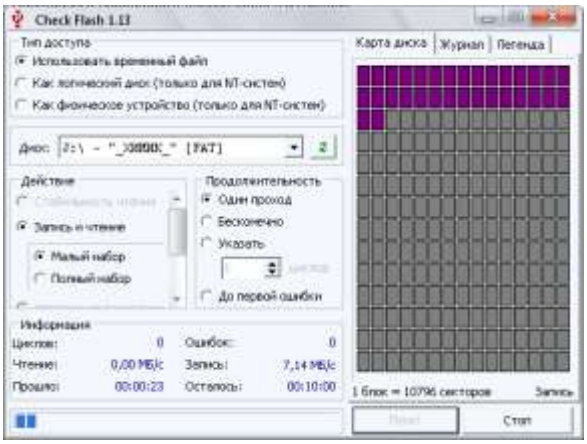
Memory Stick Duo: данный стандарт памяти разрабатывался и поддерживается компанией Sony. Корпус достаточно прочный. На данный момент — это самая дорогая память из всех представленных. Memory Stick Duo был разработан на базе широко распространённого стандарта Memory Stick от той же Sony, отличается малыми размерами (20×31×1,6 мм).

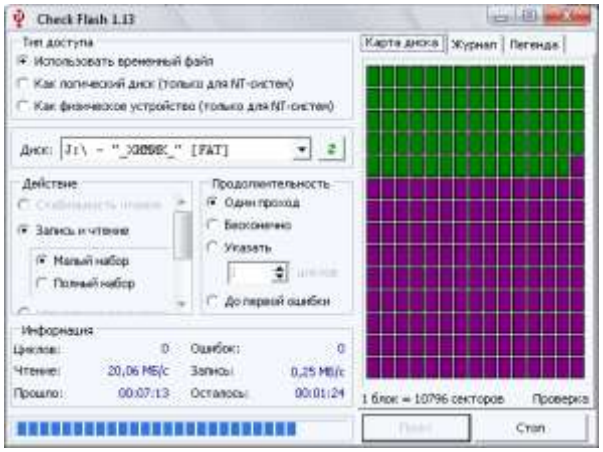
Memory Stick Micro (M2): Данный формат является конкурентом формата microSD (по аналогичному размеру), сохраняя преимущества карт памяти Sony.

xD-Picture Card: используются в цифровых фотоаппаратах фирм Olympus, Fujifilm и некоторых других.

Скорости и время записи/чтения файлов.

Тестировании скорости чтения/записи с помощью специальных утилит показал что скорость записи существенно меньше скорости чтения.





Порядок выполнения работы

1. Скачать любую программу и протестировать HDD?
2. Записать технические характеристики

3. Используя сеть интернет найти программы для тестирования приводов, установить и результат тестирования записать?

4. Проведем вручную тест скорости записи/чтения флеш диска. Для этого будем копировать/считывать информацию размером 920 мб, одним файлом и несколькими с разным размером. При этом определим примерное время чтения/записи и вычислим скорость передачи данных.

	Чтение		Запись	
920 Мб	1 файл	318 файлов	1 файл	318 файлов
	55 с	62 с	152 С	175 с
	16,73 Мб/с	14,84 Мб/с	6,05 Мб/с	5,26 Мб/с

Проведенный тест опять же показал что скорость записи существенно меньше скорости чтения. Еще можно заметить что скорость чтения/записи одного файла выше чем скорость чтения/записи нескольких файлов сумма размеров, которых такая же как и у одного файла.

5. Сделать выводы.

Содержание отчета.

Отчет должен содержать:

- цель работы;
- индивидуальное задание;
- описание выполнения индивидуального задания;
- ответы на контрольные вопросы;
- выводы.

Контрольные вопросы

1. Указать основные возможности программ тестирования жестких дисков.
2. Записать известные фирмы производителей жестких дисков?
3. Какие жесткие диски называются твердотельные или SSD, сравнить принцип работы с HDD – классический?
4. Какие типы памяти применяются в цифровых устройствах?
5. Какой объем памяти поддерживают современные телефоны?
6. Какой принцип работы у современных флэш-накопителей?
7. Какая файловая система используется в флэш-накопителях?

Практическая работа №7 Защита от вторжений. Брандмауэры. Отключение ненужных служб.

Цель работы

1. Ознакомление с методами защиты от вторжений.
2. Овладение навыками настройки брандмауэров.
3. Знакомство со средствами защиты от спама.
4. Знакомство со средствами защиты от вредоносных программ и вирусов.
5. Освоение элементарных приемов защиты конфиденциальной.

Краткие теоретические сведения

1. *Защита от вторжений. Брандмауэры*.

Учитывая все возрастающее количество программ, разрабатываемых для атак на операционные системы, важнейшей проблемой стало обеспечение безопасности компьютера. Поскольку взаимодействие компьютера с внешним миром осуществляется через порты, а их достаточно много (65536 в IBM-совместимом компьютере), то целесообразна идея закрытия большинства из них, кроме немногих (одного-двух), абсолютно необходимых. Определить, насколько компьютер открыт для внешнего мира, можно с помощью специальных тестов, позволяющих оценить уровень уязвимости компьютера. Следующие сайты могут помочь в решении этой задачи:

- Symantec Security Check (http://security.symantec.com);
- Sygate Online Services (http://scan.sygate.com);
- Gipson Research Shields Up (www.grc.com);
- DSL Reports (www.dslreports.com/scan).

Для проверки компьютера нужно зайти на один из этих сайтов и выполнить представленные там инструкции.

Идеальных операционных систем не существует, в их числе и Windows. Поэтому Microsoft выпускает ежемесячные обновления безопасности, а также срочные внеплановые обновления. Веб-сайт Windows Update позволяет познакомиться со всеми критически важными обновлениями (critical update) и обновлениями механизмов операционной системы (features updates). Критически важные обновления призваны решать проблемы, связанные с безопасностью, например проблему защиты от широко распространенного эксплойта для Windows, известного под именем червя W32. Blaster.Worm. Этот червь распространялся через уязвимость в системе RPC (вызов удаленных процедур).

В Windows имеется полезная служба автоматического обновления: установив расписание для ежедневной автоматической проверки и установки новых обновлений, можно отказаться от интерактивных посещений веб-сайта Windows Update. Для настройки параметров автоматического обновления нужно щелкнуть правой кнопкой мыши по значку *Мой компьютер* и выбрать в контекстном меню строку *Свойства*, а затем перейти на вкладку *Автоматическое обновление*.

Установив открытые порты компьютера, как это рассмотрено выше, можно их заблокировать, оставив минимальное количество открытых, с помощью специальной программы - *брандмауэра*. Когда удаленный компьютер попытается через заблокированный порт получить доступ к компьютеру, на котором установлен брандмауэр, он не сможет этого сделать, потому что посылаемые удаленным компьютером данные будут игнорироваться.

При попадании данных в заблокированный порт в зависимости от настройки брандмауэр отвечает, что порт закрыт, или вообще ничего не отвечает, делая компьютер невидимым извне. Компьютер, на котором установлен брандмауэр, работающий в режиме невидимости, для любого удаленного компьютера, пытающегося к нему подключиться, будет выглядеть как выключенный, т.к. никакого ответа удаленный компьютер не получит.

В Windows XP имеется встроенный брандмауэр Internet Connection Firewall (ICF). Новая версия брандмауэра, являющаяся частью пакета обновлений Service Pack 2, имеет ряд новых возможностей, упрощающих работу с брандмауэром и обеспечивающих высокий уровень безопасности. Брандмауэр по умолчанию отключен. Для его использования нужно выполнить следующие действия.

1. В главном меню выбрать команду *Выполнить*, затем в поле ввода открывшегося окна набрать строку firewall.cpl и щелкнуть по кнопке *ОК*.

2. После открытия диалогового окна установить переключатель *Включить* и щелкнуть по кнопке *ОК*.

По умолчанию брандмауэр блокирует все подключения, поэтому его нужно настроить, чтобы трафик определенных приложений мог проходить через брандмауэр, Настройка заключается в указании программ, трафик которых не должен блокироваться брандмауэром. Для открытия брандмауэра для определенного приложения нужно выполнить следующие шаги.

1. Перейти на вкладку *Исключения*.
2. Просмотреть список всех разрешенных программ (слева от названий таких программ установлен флажок). Целесообразно сбросить флажки для всех программ, которые не предполагается использовать.
3. Если нужно добавить в список исключений новое приложение, которое должно обрабатывать подключения и данные из внешнего мира, следует щелкнуть по кнопке *Добавить программу*.
4. Из предложенного списка программ выделить название программы, щелкнуть по кнопке *ОК*, после чего название программы появится в списке.
5. Установить флажок возле имени добавленного приложения и щелкнуть *ОК* для активизации новых параметров брандмауэра.

Брандмауэр Windows позволяет задать режим ответа компьютера в случае посылки ему некоторых стандартных управляющих интернет-сообщений. Например, можно разрешить или запретить команду ping, которая используется для оценки интервала времени между посылкой данных какому-либо компьютеру и получением от него ответа. Для изменения соответствующего параметра нужно перейти на вкладку *Дополнительно* и щелкнуть по кнопке *Параметры* в разделе *Протокол* ICMP. Откроется диалоговое окно *Параметры* ICMP. Если требуется, чтобы компьютер был невидим в Интернете, нужно сбросить все флажки в данном окне.

Брандмауэр Windows относится к брандмауэрам одностороннего типа, т.е. может блокировать только входящий трафик. Компания Zone Labs разработала двухсторонний брандмауэр ZoneAlarm, который поставляется в двух вариантах: профессиональная версия и бесплатная версия (базовый вариант двухстороннего брандмауэра), которую можно загрузить с сайта (www.zonealarm.com). Двухсторонний брандмауэр может блокировать не только входящий, но и исходящий трафик, который пытаются отослать приложения с компьютера пользователя.

Блокировать исходящий трафик может понадобиться по следующим причинам. Пользователь заботится о своей конфиденциальности и не желает, чтобы приложения, установленные на компьютере, связывались с веб-сайтом разработчика для пересылки туда данных, проверки обновлений или лицензий. Пользователю необходим контроль за тем, какие приложения получают доступ к Интернету. Пользователю необходима защита от программ подобных троянским коням. Двухсторонние брандмауэры типа ZoneAlarm делают подобные приложения бесполезными, т.к. подобные вредоносные программы оказываются изолированными и не могут связаться с Интернетом.

Для установки, настройки и запуска ZoneAlarm нужно выполнить следующие действия.

1. Загрузить копию программы с сайта www.zonealarm.com.
2. Выполнить инструкции мастера Configuration Wizard для настройки политики компьютера и запустить программу.
3. Установить режим работы брандмауэра. Такой режим устанавливается:

- для зоны Интернета (защита от незнакомых компьютеров). Для временной работы в зоне Интернета рекомендуется средний уровень защиты, при котором другие компьютеры могут видеть защищаемый компьютер, но не могут использовать его ресурсы.
- для зоны надежных узлов Интернета (зона доверия), в которой предполагается совместная работа с компьютерами. Рекомендуется средний уровень защиты, при

котором другие компьютеры могут видеть защищаемый компьютер и могут использовать его ресурсы;

- для зоны блокированных узлов, через которые соединения запрещены. В эту зону включаются компьютеры, к которым нет доверительного отношения.

4. Если требуется настроить параметры блокировки приложений, нужно щелкнуть по ссылке *Program Control*, а затем на вкладке *Main* задать желаемый уровень контроля. Более детальный уровень контроля по каждому приложению можно задать на вкладке *Programs*. По умолчанию некоторые программы (например, Internet Explorer) всегда имеют доступ в Интернет. Однако при первом запуске программы, которой требуется выход в Интернет (например, Windows Messenger), ZoneAlarm спросит (Ask), действительно ли нужно пропустить трафик этого приложения. Нажав кнопку *Option*, можно получить сведения о выбранной программе.

Если ничего не известно о программе, запрашивающей доступ в Интернет, нужно поискать в Интернете информацию об этой программе. Возможно, что такой информации не будет найдено. В этом случае будет сделан вывод, что это - spyware-программа, которую нужно удалить.

5. В список программ, трафик которых пропускается через брандмауэр, можно добавить нужные элементы, щелкнув по кнопке Add.
6. После установки всех настроек щелкнуть по кнопке Finish.

2. *Отключение ненужных служб*.

С целью повышения защищенности компьютера некоторые службы можно отключить.

1. *Запрет на подключение удаленного рабочего стола*. Удаленный рабочий стол в Windows XP - это компонент операционной системы, позволяющий получить доступ к своему компьютеру в те моменты, когда пользователь находится вдали от своего офиса или дома. Если компьютер недостаточно хорошо защищен, удаленный рабочий стол может стать средством проникновения на компьютер. Вся защита удаленного рабочего стола основывается на пароле, который во многих случаях несложно подобрать. В связи с этим, если удаленный рабочий стол не используется, его лучше отключить. Для этого нужно сделать следующее:

- щелкнуть правой кнопкой мыши по значку *Мой компьютер* и выбрать в контекстном меню команду *Свойства*;
- в открывшемся окне перейти на вкладку *Удаленные сеансы*, позволяющую задать параметры удаленного доступа;
- сбросить флажки в разделах *Удаленный помощник* и *Дистанционное управление рабочим столом*. Щелкнуть по кнопке *ОК* для сохранения изменений.

2. *Отключение службы сообщений*. В последних версиях Windows имеется служба, позволяющая системному администратору посылать сообщения всем компьютерам в локальной сети. Это отличная служба, если ее использовать правильно. Некоторые пользователи, знающие про эту службу, могут злоупотреблять ею, рассылая сообщения и, хуже того, спам всем пользователям сети.

Служба сообщений, как и любая другая программа, имеющая доступ во внешнюю сеть, является потенциальной угрозой безопасности компьютера. Поэтому из соображений безопасности службу сообщений лучше отключить. Для этого выполнить команды: *Пуск - Программы - Администрирование - Службы*. В открывшемся окне *Службы* выбрать из списка служб строку *Служба сообщений*, щелкнуть по ней правой клавишей мыши и выбрать в контекстном меню команду *Свойства*. Далее в раскрывающемся списке *Тип запуска* выбрать пункт *Отключено* и щелкнуть по кнопке ОК для сохранения изменений.

3. *Отключение поддержки универсальной технологии Plug-and-Play*. Универсальная технология Universal Plug-and-Play (UPnP) представляет собой развитие технологии Plug-and-Play. Она позволяет быстро и просто добавлять и контролировать самые различные устройства. Учитывая низкую в настоящее время распространенность устройств UPnP и факт снижения уровня безопасности при использовании службы поддержки таких

устройств, ее лучше отключить. Для этого нужно поступить так же, как и при отключении службы сообщений, но выбрать в перечне служб *Узел универсальных PnP-устройств*.

4. *Отключение удаленного доступа к реестру*. В состав Windows Professional входит служба *Удаленный реестр*, позволяющая пользователям с правами администратора подключаться к реестру компьютера и редактировать его. Чтобы не дать кому-либо дополнительный шанс проникнуть в один из наиболее важных компонентов операционной системы, лучше отключить эту службу.
5. *Отключение поддержки DCOM*. Поддерживаемая Windows технология DCOM (Distributed Component Object Model - распределенная объектная модель программных компонентов) предоставляет удобный интерфейс программирования для разработчиков сетевых приложений. Эксплойты, построенные на базе уязвимости DCOM, позволили распространиться интернет-червю по сотням тысяч машин с операционной системой Windows. Большинству пользователей можно отключить эту службу (исключение составляют лишь те пользователи, которые пользуются приложениями, реально требующими поддержки DCOM).

Компания Gibson Research разработала утилиту DCOMbobulator, которая поможет отключить DCOM на компьютере. Утилиту можно загрузить с сайта www.grc.com/dcom/. После ее запуска открывается окно, в котором нужно перейти на вкладку DCOMbobulator Me! и щелкнуть по кнопке Disable DCOM, а затем по кнопке Exit.

3. *Защита от спама.*

Наиболее распространенной причиной получения спама являются сами пользователи. Они посылают электронные сообщения на веб-сайты или в компании, которые в ответ рассылают им свою рекламу или продают их адреса другим компаниям, Еще одна распространенная причина получения спама - невнимательная подписка на различные новости и информационные рассылки.

Так как программ для рассылки спама создано огромное количество, то не существует программы, которая фильтрует спам с гарантией 100%. Однако, если утилита будет отсекать около 90% нежелательной корреспонденции, это будет хорошим результатом. Одной из неплохих утилит является McAfee SpamKiller - программа для защиты от спама с ежедневным автообновлением базы по спамерам и легким созданием собственных фильтров.

Работает SpamKiller в фоновом режиме, проверяет практически неограниченное число почтовых ящиков, выявляет полученный спам и удаляет его прямо на почтовом сервере - автоматически или в ручном режиме. В случае обнаружения новой почты возможна разнообразная сигнализация об этом, а также автоматический запуск почтовой программы.

Условно-бесплатный вариант программы имеется на множестве сайтов Интернета, например на сайте dl.softportal.com/load/spamkiller2908.exe. После загрузки и запуска программы открывается окно для инсталляции утилиты. Установленная утилита после ее запуска предлагает купить лицензионную версию или продолжить работу с 30-дневной демо-версией.

Нажав кнопку *Continue*, пользователь перейдет к мастеру установки параметров программы. После завершения работы с мастером настройки программы и нажатия кнопки *Finish* открывается окно программы, в котором можно просмотреть и установить параметры утилиты для фильтрации сообщений, в том числе поступающих из разных стран.

Если почтовый клиент пользователя поддерживает графические сообщения в формате HTML, то при каждом получении почты имеется вероятность того, что отправитель узнает, прочитал ли получатель его письмо. Это делается при помощи скрытых ссылок на изображения, обращающиеся к веб-серверу, на котором запущена специальная программа, отслеживающая подобные обращения. Если задержать сигналы, отправляемые на серверы распространителей спама, то, возможно, что адрес получателя будет удален из баз данных серверов как неактивный.

Последние версии некоторых почтовых программ, например Outlook 2003 и Outlook Express (после установки Windows Service Pack 2), автоматически блокируют все внешние ссылки в HTML-сообщениях. Режим блокировки внешних ссылок в Outlook Express можно включить на вкладке *Безопасность* в окне *Параметры*, вызываемого из меню *Сервис*. В *Outlook* и *Outlook Express* также имеется список надежных отправителей, с помощью которого можно включать внешнее содержимое только для определенных отправителей. Чтобы разрешить использование рисунков и другого внешнего содержимого для определенного отправителя, нужно щелкнуть правой кнопкой мыши по сообщению от него и добавить отправителя в список надежных отправителей.

4. *Защита от вредоносных программ и вирусов*.

В последнее время **spyware**-программы превратились в наиболее опасную угрозу для компьютеров. Скрываясь в свободно распространяемых приложениях, эти программы шпионят за пользователями компьютеров и затем отправляют собранную информацию злоумышленникам. Шпионское ПО, не проявляя себя, отслеживает поведение пользователя за компьютером, чтобы создать его «маркетинговый профиль», который также молча передается сборщикам информации, продающим данные пользователя рекламным организациям.

Существует еще один вид вредоносных программ - adware-программы, тесно связанные со spyware-программами. Они также тайно устанавливаются на компьютеры пользователей и начинают наблюдать за ними. Обычно подобные ситуации связаны с установкой программ, загружаемых с веб-сайтов. Пользователи часто перед установкой бесплатных программ не читают соответствующие соглашения о предоставлении услуг и пропускают сообщения, что данные программы будут отображать рекламу.

Если в браузере появятся новые панели инструментов, которые явно не устанавливались, если браузер постоянно «падает» или стартовая страница неожиданно изменилась, то вполне вероятно, что в компьютере завелся «шпион». Но даже если нет ничего необычного, то «шпионы» все равно могут быть - чем дальше, тем больше появляется программное обеспечение такого рода.

В Интернете имеется множество свободно распространяемых утилит, помогающих проверить компьютер на наличие spyware и adware-программ. Наибольшей популярностью пользуются две такие программы. Первая программа Ad-ware разработана компанией Lavasoft, ее базовую версию можно загрузить бесплатно с сайта www.lavasoft.de. Вторая программа называется Spybot S&D и распространяется также бесплатно (www.spybot.info).

Для загрузки и запуска программы Ad-ware нужно выполнить следующее.

1. Загрузить копию базовой версии программы Ad-ware с сайта www.lavasoft.de и установить ее на компьютере.
2. Запустить программу – откроется окно.
3. Обновить файлы данных, щелкнув по кнопке *Web Update*, а затем *Update*. Если имеются актуальные обновления, будет выдано соответствующее сообщение. В этом случае щелкнуть по кнопке *Yes*, а затем *OK*, после чего обновления будут автоматически загружены и установлены.
4. Для начала проверки компьютера щелкнуть по кнопке *Scan*. Из показанных режимов сканирования *Scan Mode* выбрать необходимый (например, Smart Scan) и нажать кнопку *Scan*. Начнется процесс сканирования.
5. После завершения сканирования будут показаны его результаты с перечислением всех spyware- и adware-программ, обнаруженных на компьютере. Нужно сбросить флажки у тех объектов, которые решено не удалять (например, у объектов типа Tracking cookie). Для удаления объектов нажать кнопку Remove. Программа автоматически сохраняет резервные копии всех удаляемых объектов на случай возникновения проблем в операционной системе после удаления файлов и параметров реестра.
6. Для завершения работы с программой нажать кнопку *Finish*.

Еще одна популярная программа Spybot - Search & Destroy (спайбот - найти и уничтожить) может обнаруживать и удалять с компьютера различного рода шпионское программное обеспечение. Программу Spybot-S&D в русскоязычном варианте можно загрузить с сайта www.spybot.info.

После загрузки, инсталляции и запуска программы открывается ее окно с подменю Spybot-S&D. При первом запуске нужно прочитать несколько соглашений об ответственности за использование программы.

Далее для работы с программой нужно выполнить следующие действия.

1. Обновить файлы данных, для чего щелкнуть по кнопке *Поиск обновлений*. Просмотрев список доступных обновлений, для их загрузки щелкнуть по кнопке *Загрузить обновления*.
2. После загрузки и установки обновлений нужно закрыть и заново открыть программу. Для проверки компьютера нажать кнопку *Начать проверку*. Начнется процесс сканирования.
3. Результаты сканирования будут через некоторое время выведены в окне результатов.
4. Для устранения выявленных проблем нужно нажать клавишу *Устранить отмеченные проблемы*. Устранению подлежат только те файлы, которые помечены флажками. Программа автоматически сохраняет резервные копии всех удаляемых объектов на случай возникновения проблем в операционной системе после удаления файлов и параметров реестра.
5. Перед устранением выявленных проблем программа создает резервную копию реестра. Если возникнут какие-либо трудности с операционной системой, можно восстановить удаленные файлы и исходное состояние реестра. Для этого нужно щелкнуть по клавише *Восстановить*. Предварительно программа предложит создать резервную копию реестра.

С помощью утилиты Spybot-S&D можно выполнять вакцинацию, защищающую компьютер от некоторых наиболее распространенных типов вредоносных программ. Данная возможность значительно повышает защищенность компьютера в борьбе с spyware-программами. Для выполнения вакцинации нужно запустить утилиту и щелкнуть по кнопке *Иммунизация*.

После удаления с компьютера всех spyware- и adware-программ можно отключить некоторые режимы работы браузера Internet Explorer, снизив тем самым риск новой случайной установки spyware-программ.

Целесообразно изменить параметры установки элементов ActiveX, запретив возможность их установки. Для этого необходимо выполнить следующие действия.

1. Открыть новое окно Internet Explorer.
2. Выбрать команду *Свойства обозревателя* в меню *Сервис*.
3. Перейти на вкладку *Безопасность* и щелкнуть по кнопке *Другой*. Откроется окно *Параметры безопасности*.
4. Найти в списке группу переключателей *Загрузка подписанных элементов ActiveX* и установить переключатель в состояние *Отключить* (загрузка неподписанных элементов также должна быть отключена).
5. Щелкнуть по кнопке *ОК*, а затем - по кнопке *Да*.
6. Еще раз щелкнуть по кнопке *ОК* для закрытия окна *Свойства обозревателя*.

Выполненная процедура приведет к запрету установки элементов управления ActiveX с любых веб-сайтов (как хороших, так и плохих). Если при посещении какого-либо сайта возникнут проблемы с загрузкой его содержимого, то можно выполнить обратную процедуру, т.е. разрешить загрузку подписанных элементов ActiveX.

5. *Защита конфиденциальной информации*.

Современные операционные системы, в том числе Windows, собирают много информации о работе пользователя за компьютером. Сюда относятся адреса веб-сайтов, имена запускаемых приложений и открываемых файлов. Эта информация используется системой для обеспечения комфортной работы пользователя. Однако иногда это нежелательно, например, если необходимо соблюдать конфиденциальность своей работы. Это особенно актуально,

если компьютером пользуется несколько человек. Для соблюдения конфиденциальности своей работы информацию о действиях пользователя необходимо с компьютера удалить.

Очистка Internet Explorer. В целях конфиденциальности приходится очищать четыре части данных браузера: список вводившихся адресов, журнал с историей посещения веб-сайтов, список временных файлов Интернета и список cokie-файлов. Первый список формируется на основе истории ранее вводившихся адресов и позволяет быстро вводить адреса, выбирая их среди возможных вариантов. Отключить функцию автоматического завершения ввода довольно непросто. Файл, в котором хранится это список, является URL-кэшем и имеет имя index.dat. Решение можно получить с помощью утилиты Dr.Delete (www.docsdownloads.com/dr-delete-l.html), для этого нужно выполнить следующие шаги.

1. Запустить программу Dr. Delete и щелкнуть по кнопке *Browse*, чтобы выбрать удаляемый файл.
2. Открыть папку C:\documents and Settings.
3. Открыть папку, название которой совпадает с вашим именем пользователя.
4. Открыть папку Cookies, выделить файл index.dat и щелкнуть по кнопке *Open.*
5. После того как в поле ввода появится путь к файлу, щелкнуть по кнопке *Delete.*
6. Щелкнуть по кнопке *Yes* в диалоговом окне подтверждения. Появится сообщение о том, что данный файл будет удален при следующей перезагрузке компьютера.

По умолчанию Internet Explorer настроен на запись адресов веб-сайтов, которые посещались в течение 30 дней. Если важно сохранить конфиденциальность этих посещений, нужно периодически очищать журнал посещений. Для очистки журнала посещений нужно выполнить следующие действия.

1. Открыть окно браузера Internet Explorer и в меню *Сервис* выбрать команду *Свойства*. Откроется окно *Свойства*: *Интернет*.
2. На вкладке *Общие* щелкнуть по кнопке *Очистить*. Появится диалоговое окно *Свойства обозревателя*, в котором нажать кнопку *Да*.
3. Указать интервал времени, в течение которого должна храниться информация о посещении сайтов. Щелкнуть по кнопке *Применить* и *ОК*.

Каждый раз при посещении сайтов Интернета в компьютере в папку Temporary Internet Files записываются соответствующие файлы. Со временем папка вырастает в объеме и может содержать информацию, которую нежелательно показывать другим пользователям этого компьютера. Однако папка доступна для просмотра каждому пользователю. Если это нежелательно, папку Temporary Internet Files следует очистить.

Еще один вид файлов, которые создаются при посещении Интернета, - Cookie-файлы. С точки зрения конфиденциальности, единственный минус хранения этих файлов на компьютере связан с тем, что он доступен локальным пользователям этого компьютера. Следовательно, при желании они могут определить, какие сайты кто посещал. Для очистки папки Temporary Internet Files и удаления Cookie-файлов нужно выполнить следующие действия.

1. Открыть новое окно браузера Internet Explorer и в меню *Сервис* выбрать команду *Свойства обозревателя*.
2. Щелкнуть по кнопке *Удалить файлы* в разделе *Временные файлы Интернета*. Появится запрос, в котором нужно установить флажок и щелкнуть по кнопке *ОК*.
3. После возврата в окно *Свойства обозревателя* нужно щелкнуть по кнопке *Удалить* «Cookie».
4. Щелкнуть по кнопке *ОК* в диалоговом окне подтверждения и еще раз *ОК* для закрытия окна *Свойства обозревателя*.

В последней версии Internet Explorer появилось много новых функций, в том числе функция настройки вариантов создания cookie-файлов. Можно установить режим блокировки создания cookie-файлов. Следует различать два их типа: основные (firstparty) и сторонние (third-party). Основные cookie-файлы размещаются на компьютере тем сайтом, который

посетил пользователь. Сторонние cookie-файлы размещаются на компьютере удаленными сайтами (например, рекламными).

Если нежелательно получение и, следовательно, хранение сторонних cookie-файлов, нужно сделать следующее.

1. Открыть новое окно Internet Explorer, выбрать в меню *Сервис* команду *Свойства обозревателя* и перейти на вкладку *Конфиденциальность*.
2. Оставить ползунок уровня конфиденциальности в положении *Умеренно высокий* и щелкнуть по кнопке *Дополнительно*. Откроется окно *Дополнительные параметры конфиденциальности*.
3. Установить флажок *Перекрыть автоматическую обработку файлов* «cookie» и установить следующие параметры приема cookie-файлов: основные «cookie» - принимать, сторонние «cookie» – запрашивать, всегда разрешать сеансовые «cookie».
4. Два раза щелкнуть по кнопке *ОК* для возврата в окно *Свойства обозревателя*, а затем его закрытия.

При работе пользователя с безопасным веб-подключением, реализуемым с помощью протокола SSL (Security Sockets Layer - слой защищенных сокетов), например при работе со своей учетной записью в виртуальном магазине или банке, происходит шифрование данных, пересылаемых с веб-сервера на клиентскую машину. После получения данных браузер клиентской машины с помощью специального ключа дешифрует информацию и отображает ее на компьютере. Расшифрованный файл остается в каталоге Temporary Internet Files. Следовательно, он доступен всем, кто имеет возможность локально зарегистрироваться на компьютере.

Проблема решается средствами Internet Explorer следующим образом.

1. Открыть новое окно Internet Explorer, выбрать в меню *Сервис* команду *Свойства обозревателя* и перейти на вкладку *Дополнительно*.
2. Найти в списке группу флажков *Безопасность*. Установить флажок *Не сохранять зашифрованные страницы на диске*.
3. Щелкнуть по кнопке *ОК* для сохранения и активизации сделанных изменений.

Функция автоматического заполнения URL-адресов, вводимых в адресной строке браузера, снижает уровень конфиденциальности, поэтому целесообразно очистить файл с историей вводившихся ранее адресов. Однако это не единственная ситуация, в которой срабатывает функция автоматического заполнения.

Система выдает список возможных вариантов и в том случае, когда заполняются поля ввода на веб-страницах. Эта особенность позволяет любому пользователю компьютера видеть, что искали другие пользователи на данном сайте, даже если журнал посещений сайтов в браузере был очищен. Следовательно, функция автоматического заполнения представляет угрозу конфиденциальности информации. Эту проблему можно решить следующим образом.

1. Открыть новое окно Internet Explorer, выбрать в меню *Сервис* команду *Свойства обозревателя* и перейти на вкладку *Содержание*.
2. Щелкнуть по кнопке *Автозаполнение*.
3. После открытия окна *Настройки автозаполнения* сбросить все флажки в группе *Использовать автозаполнение для*. Это позволит решить проблему, связанную с функцией автоматического заполнения,
4. В окне *Настройка автозаполнения* можно щелкнуть по двум кнопкам для удаления всех данных, хранящихся в журналах автоматического заполнения.
5. Щелкнуть по кнопке *ОК* для сохранения и активизации сделанных изменений.

Выше говорилось об удалении временных файлов Интернета. Удобно, если это делается автоматически при закрытии обозревателя. Для этого на вкладке *Дополнительно* окна *Свойства обозревателя* нужно установить флажок *Удалять все файлы из папки временных файлов Интернета* при закрытии обозревателя.

Интерфейс Windows. Проводник Windows сохраняет информацию о запускаемых пользователем приложениях и открываемых файлах. Это делается для удобства работы

пользователя, т.к.ускоряет его работу, однако отрицательно сказывается на уровне конфиденциальности, поскольку любой пользователь компьютера может увидеть, с какими программами чаще работает другой пользователь.

Если в целях сохранения конфиденциальности нужно очистить список часто запускаемых приложений, следует выполнить следующие шаги.

1. Щелкнуть правой кнопкой мыши по кнопке *Пуск* и выбрать в контекстном меню команду *Свойства*.
2. На вкладке *Меню* «*Пуск*» открывающегося окна щелкнуть по кнопке *Настроить*.
3. Щелкнуть по кнопке *Очистить список*.
4. Щелкнуть по кнопке *ОК* для закрытия окна *Настройка меню* «*Пуск*».
5. Еще раз щелкнуть по кнопке *ОК* для закрытия окна *Свойства панели задач* и меню «*Пуск*».

Система сохраняет информацию обо всех файлах, которые открывает пользователь. Это позволяет поддерживать список нескольких последних открывающихся файлов любого типа. Для сохранения в секрете перечня документов, с которыми работает пользователь, целесообразно периодически очищать список последних открывавшихся файлов. Сделать это можно следующим образом.

1. Щелкнуть правой кнопкой мыши по кнопке *Пуск* и выбрать в контекстном меню команду *Свойства*.
2. На вкладке *Меню* «*Пуск*» открывающегося окна щелкнуть по кнопке *Настроить*.
3. После открытия окна *Настройка меню* «*Пуск*» перейти на вкладку *Дополнительно*.
4. Щелкнуть по кнопке *Очистка списка.*
5. Щелкнуть по кнопке *ОК* для закрытия окна *Настройка меню* «*Пуск*».
6. Еще раз щелкнуть по кнопке *ОК* для закрытия окна *Свойства панели задач* и меню «*Пуск*».

Со временем жесткий диск может заполниться временными файлами, которые создают операционная система и некоторые приложения. Эти файлы могут быть использованы для анализа действий пользователя и, кроме того, занимают дисковую память. Поэтому следует периодически очищать диск от таких файлов. В системе имеется служебная программа *Очистка диска*. Для ее запуска следует выполнить команды *Пуск* → *Программы* → *Стандартные* → *Служебные* → *Очистка диска*. После запуска программы откроется окно: надо выбрать имя диска, на котором требуется удалить временные файлы, после чего нажать кнопку *ОК*. Через некоторое время открывается окно с перечнем файлов, которые можно удалить.

Существуют программы сторонних производителей, которые автоматически находят каталоги с временными файлами и очищают их. Популярна утилита TempCleaner, которую можно загрузить со многих веб-сайтов.

При посещении веб-сайтов, требующих аутентификации, или подключении к удаленным компьютерам пользователю часто предлагается сохранить пароль, чтобы при следующем доступе к сайту не приходилось вводить пароль заново. Данный режим удобен для пользователя, но создает дополнительную уязвимость в системе безопасности, поскольку любой другой пользователь, имеющий доступ к этому же компьютеру, сможет воспользоваться чужим именем и паролем, даже если он их не знает.

Удаление сохраненных паролей с компьютера позволит защитить свои учетные записи и повысить уровень их конфиденциальности. Предлагается следующий способ доступа к списку паролей.

1. В главном меню выбрать команду *Выполнить*.

2. В поле ввода открывшегося окна набрать строку rundll32.exe keymgr.dll.KRShowKeyMgr и щелкнуть по кнопке *ОК*.

3. Откроется окно *Сохранение имен пользователей и паролей* со списком всех учетных записей, сохраненных на компьютере.

4. Для удаления сохраненного пароля выбрать в списке нужную учетную запись и щелкнуть по кнопке *Удалить*.
5. Щелкнуть по кнопке *ОК* в диалоговом окне подтверждения, и учетная запись будет удалена из списка.
6. Повторить предыдущие шаги для всех учетных записей, которые нужно удалить.
7. Закончив удаление, щелкнуть по кнопке *Закрыть*.

На компьютерах с операционной системой Windows/2000/2003, использующих файловую систему NTFS, можно устанавливать разрешения на доступ к файлам и папкам. Это может быть очень мощным инструментом в обеспечении конфиденциальности информации.

Чтобы установить полный контроль над разрешениями на доступ, нужно сначала отключить режим общего доступа к файлам. Для этого следует открыть любую папку, в меню *Сервис* выбрать команду *Свойства папки*, перейти на вкладку *Вид* и сбросить флажок *Использовать простой общий доступ к файлам*. Далее можно перейти к настройке разрешений на доступ к требуемым папкам и файлам. Кроме того, для защиты данных в файловой системе NTFS можно их зашифровывать.

ЗАДАНИЯ ДЛЯ САМОСТОЯТЕЛЬНОГО ВЫПОЛНЕНИЯ

Задание 1.

1. Настройте брандмауэр Windows. Определите список программ, которым разрешено обрабатывать данные, поступающие в компьютер из внешнего окружения. Не нужно ли сократить этот список?
2. Установите брандмауэр ZoneAlarm (предварительно отключив брандмауэр Windows XP, чтобы не допустить конфликтов). Определите, какие ваши приложения пытаются посылать данные в Интернет.

Задание 2.

1. Запустите оснастку *Службы*. Просмотрите список установленных и работающих служб. Все ли они необходимы для вашей повседневной работы. Удалите ненужные службы.
2. Загрузите с веб-сайта программу SpamKiller. Настройте программу (установите параметры фильтрации сообщений). Проверьте, установлен ли режим блокировки внешних ссылок в почтовой программе.

Задание 3.

1. Установите и обновите утилиты Ad-ware и Spybot S&D. Проверьте компьютер с помощью этих программ. Удалите обнаруженные spyware- и adware-программы. Проведите вакцинацию компьютера.
2. Проверьте параметры настройки браузера. Запретите загрузку элементов ActiveX.

Задание 4.

1. В целях конфиденциальности вашей информации проведите очистку четырех частей данных браузера: списка вводившихся адресов, журнала с историей посещения веб-сайтов, списка временных файлов Интернета и списка cokie-файлов.
2. Измените интерфейс Windows компьютера в целях повышения конфиденциальности вашей работы на компьютере:

- очистите список часто запускавшихся приложений;
- очистите список последних открывавшихся документов;
- удалите временные файлы с жесткого диска;
- удалите сохраненные пароли;
- назначьте необходимые разрешения к файлам и папкам;
- зашифруйте важную для вас информацию.

Контрольные вопросы

1) Какие разновидности атак Вы знаете?
2) Какие функции по защите компьютера выполняет брандмауэр?
3) В чем заключается основное функциональное различие между брандмауэром Windows и брандмауэром различие между ZoneAlarm?
4) Как сделать компьютер невидимым в сети для других компьютеров?

5) Какие службы можно отключить с целью обеспечения безопасности компьютера? Как это сделать?
6) Что такое спам? Какие методы его распространения Вы знаете?
7) Какие способы борьбы со спамом Вы знаете?
8) Какие типы вредоносного программного обеспечения Вы знаете?
9) Какие применяются способы обнаружения и борьбы с вредоносным программным обеспечением?
10) Какая информация о действиях пользователя сохраняется в целях обеспечения комфортности его работы?
11) Какие действия следует предпринять, чтобы в целях конфиденциальности удалить с компьютера информацию о действиях пользователя?

Практическая работа №8 Защита от спама. Защита от вредоносных программ и вирусов. Защита конфиденциальной информации.

Теоретическая часть.

Компьютерный вирус – *это специально написанная, небольшая по размерам программа (т.е. некоторая совокупность выполняемого кода), которая может " приписывать" себя к другим программам ("заражать" их), создавать свои копии и внедрять их в файлы, системные области компьютера и т.д., а также выполнять различные нежелательные действия на компьютере.*

Программа, внутри которой находится вирус, называется "зараженной" Когда такая программа начинает работу, то сначала управление получает вирус. Вирус находит и заражает другие программы, а также выполняет какие-нибудь вредные действия (портит файлы или таблицу размещения файлов на диске, "засоряет" оперативную память и т.д.).

Классификация вирусов.

По среде обитания	*сетевые*	распространяются по компьютерной сети
	файловые	внедряются в выполняемые файлы
	загрузочные	внедряются в загрузочный сектор диска (Boot-сектор)
	файлово-загрузочые	внедряются в выполняемые файлы и в загрузочный сектор диска
	системные	проникают в системные модули и драйверы периферийных устройств, поражают программы-интерпретаторы
По способу заражения	*резидентные*	находятся в памяти, активны до выключения компьютера
	нерезидентные	не заражают память, являются активными ограниченное время
По деструктивным возможностям (по способам воздействия)	*безвредные*	практически не влияют на работу; уменьшают свободную память на диске в результате своего распространения
	неопасные	уменьшают свободную память; создают звуковые, графические и прочие эффекты

	опасные	могут привести к серьёзным сбоям в работе
	очень опасные	могут привести к потере программ или системных данных
По особенностям алгоритма вируса	*вирусы-«спутники»*	вирусы, не изменяющие файлы, создают для EXE-файлов файлы-спутники с расширением COM
	простейшие вирусы	паразитические программы, которые изменяют содержимое файлов и секторов диска и могут быть легко обнаружены
	Ретро-вирусы	обычные файловые вирусы, которые пытаются заразить антивирусные программы, уничтожая их, или делая неработоспособными
	репликаторные, вирусы-«черви»	распространяются по сети, рассылают свои копии, вычисляя сетевые адреса. Это самые распространенные в виртуальной сети вирусы. Они очень быстро «размножаются». Иногда дают своим копиям отдельные имена. Например, «install.exe».
	«паразитические»	изменяют содержимое дисковых секторов или файлов
	«студенческие»	примитив, содержат большое количество ошибок
	«стелс»-вирусы (невидимки)	это файловые вирусы, которых антивирусные программы не находят, потому что во время проверки они фальсифицируют ответ. Они перехватывают обращения DOS к пораженным файлам или секторам и подставляют вместо себя незараженные участки
	вирусы-призраки	не имеют ни одного постоянного участка кода, труднообнаруживаемы, основное тело вируса зашифровано
	макровирусы	пишутся не в машинных кодах, а на WordBasic, живут в документах Word, переписывают себя в шаблон Normal.dot
	квазивирусные, или «троянские»	это вирусы, не способные к «размножению». Троянская программа маскируется под полезную или интересную программу, выполняя во время своего функционирования ещё и разрушительную работу (например, стирает FAT-таблицу) или собирает на компьютере не подлежащую разглашению информацию. В

		отличие от вирусов, троянские программы не обладают свойством самовоспроизводства. Троянская программа маскируется, как правило, под коммерческий продукт. Её другое название «троянский конь».
	логические бомбы	программы, которые запускаются при определённых временных или информационных условиях для осуществления вредоносных действий (как правило, несанкционированного доступа к информации, искажения или уничтожения данных)
	мутанты	это один из видов вирусов, способных к самовоспроизведению. Однако их копия явно отличается от оригинала.

Основными путями проникновения вирусов в компьютер являются **съёмные диски** (гибкие и лазерные), а также **компьютерные сети**. Заражение жесткого диска вирусами может произойти при загрузке программы с дискеты, содержащей вирус. Такое заражение может быть и случайным, например, если дискету не вынули из дисковода A: и перезагрузили компьютер, при этом дискета может быть и не системной. Заражение дискеты происходит, даже если её просто вставили в дисковод зараженного компьютера или, например, прочитали её оглавление.

Признаки заражения

- вывод на экран непредусмотренных сообщений или изображений;
- подача непредусмотренных звуковых сигналов;
- неожиданное открытие и закрытие лотка CD-ROM-устройства;
- произвольный, без вашего участия, запуск на компьютере каких-либо программ;

Есть также **косвенные признаки заражения** вашего **компьютера**:

- частые зависания и сбои в работе компьютера;
- прекращение работы или неправильная работа ранее успешно работавших программ;
- медленная работа компьютера при запуске программ;
- невозможность загрузки операционной системы;
- исчезновение файлов и каталогов или искажение их содержимого;
- изменение размеров файлов;
- неожиданное значительное увеличение количества файлов на диске;
- существенное уменьшение размеров свободной оперативной памяти;
- частое обращение к жесткому диску (часто мигает лампочка на системном блоке);
- Microsoft Internet Explorer "зависает" или ведет себя неожиданным образом.

В 90% случаев наличие косвенных симптомов вызвано сбоем в аппаратном или программном обеспечении. Несмотря на то, что подобные симптомы с малой вероятностью свидетельствуют о заражении, при их появлении рекомендуем вам провести **полную проверку вашего компьютера**.

Антивирусные программы.

Для обнаружения, удаления и защиты от компьютерных вирусов разработаны специальные антивирусные программы. Различают следующие **виды антивирусных программ**:

- **Программы-детекторы** осуществляют поиск характерной для конкретного вируса сигнатуры в оперативной памяти и в файлах и при обнаружении выдают соответствующее сообщение. Недостатки: могут находить только те вирусы, которые известны разработчикам этой программы, поэтому быстро устаревают и требуют регулярного обновления.
- **Программы-доктора** или **фаги** не только находят зараженные вирусами файлы, но и «лечат» их, т.е. удаляют из файла тело программы-вируса, возвращая файл в исходное состояние. **Полифаги** – программы-доктора, предназначенные для поиска и уничтожения большого количества вирусов. Недостатки те же, что и у программ-детекторов.
- **Программы-ревизоры** относятся к самым надежным средствам защиты. Ревизоры запоминают исходное состояние программ, каталогов и системных областей диска тогда, когда компьютер не заражен вирусом, а затем периодически или по желанию пользователя сравнивают текущее состояние с исходным. Обнаруженные изменения выводятся на экран монитора.
- **Программы-фильтры** или **«сторожа»** представляют собой небольшие резидентные программы, предназначенные для обнаружения подозрительных действий при работе компьютера, характерных для вирусов (попытки коррекции файлов с расширением EXE или COM, изменение атрибутов файла, запись в загрузочные сектора и т.п.). При попытке какой-либо программы произвести указанные действия «сторож» посылает пользователю сообщение и предлагает запретить или разрешить соответствующее действие. Эти программы способны обнаружить вирус на самой ранней стадии его существования до размножения. Однако они не лечат файла и диски. Для уничтожения вируса требуется применить другие программы.
- **Вакцины** или **иммунизаторы** это резидентные программы, предотвращающие заражение файлов. Вакцины применяют, если отсутствуют программы-доктора, лечащие этот вирус. Вакцинация возможна только от известных вирусов. Вакцина модифицирует программу или диск таким образом, чтобы это не отражалось на их работе, а вирус будет воспринимать их зараженными и поэтому не внедрится. Имеют ограниченное применение.

Назначение и основные функции Антивируса Касперского Personal

Антивирус Касперского Personal предназначен для антивирусной защиты персональных компьютеров, работающих под управлением операционной системы Windows.

Антивирус Касперского Personal выполняет следующие **функции**:

- **Защита от вирусов и вредоносных программ** - обнаружение и уничтожение вредоносных программ, проникающих через съемные и постоянные файловые носители, электронную почту и протоколы интернета. Можно выделить следующие варианты работы программы (они могут использоваться как отдельно, так и в совокупности):
  - **Постоянная защита компьютера** - проверка всех запускаемых, открываемых и сохраняемых на компьютере объектов на присутствие вирусов.
  - **Проверка компьютера по требованию** - проверка и лечение как всего компьютера в целом, так и отдельных дисков, файлов или каталогов. Такую проверку вы можете запускать самостоятельно или настроить ее регулярный автоматический запуск.
- **Восстановление работоспособности после вирусной атаки**. Полная проверка и лечение позволяет вам удалить все вирусы, поразившие ваши данные при вирусной атаке.
- **Проверка и лечение входящей/исходящей почты** - анализ на присутствие вирусов и лечение входящей почты до ее поступления в почтовый ящик и исходящей почты в

режиме реального времени. Кроме того, программа позволяет проверять и лечить почтовые базы различных почтовых клиентов по требованию.

- **Обновление антивирусных баз и программных модулей** - пополнение антивирусных баз информацией о новых вирусах и способах лечения зараженных ими объектов, а также обновление собственных модулей программы. Обновление выполняется с серверов обновлений Лаборатории Касперского или из локального каталога.
- **Рекомендации по настройке программы и работе с ней** - советы от экспертов Лаборатории Касперского, сопровождающие вас в процессе работы с Антивирусом Касперского Personal, и рекомендуемые настройки, соответствующие оптимальной антивирусной защите.

- **Карантин** - помещение объектов, возможно зараженных вирусами или их модификациями, в специальное безопасное хранилище, где вы можете их лечить, удалять, восстанавливать в исходный каталог, а также отправлять экспертам Лаборатории Касперского на исследование. Файлы на карантине хранятся в специальном формате и не представляют опасности.
- **Формирование отчета** - фиксирование всех результатов работы Антивируса Касперского Personal в отчете. Подробный отчет о результатах проверки включает общую статистику по проверенным объектам, хранит настройки, с которыми была выполнена та или иная задача, а также последовательность проверки и обработки каждого объекта в отдельности.

Как проверить CD-диск или дискету.

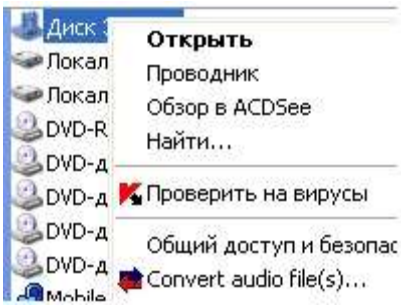
Через дискеты, CD и другие съемные диски легко заразить компьютер вирусом. Если дискета (или загрузочный CD-диск) заражена загрузочным вирусом, и вы оставили ее в дисководе и перезагрузились, результаты могут быть самые печальные.

Рекомендуем вам проверять все съемные диски перед их использованием.

Вы можете запустить проверку сменных дисков из главного окна Антивируса Касперского Personal, а также из контекстного меню Windows.

Для проверки сменных дисков из контекстного меню Windows

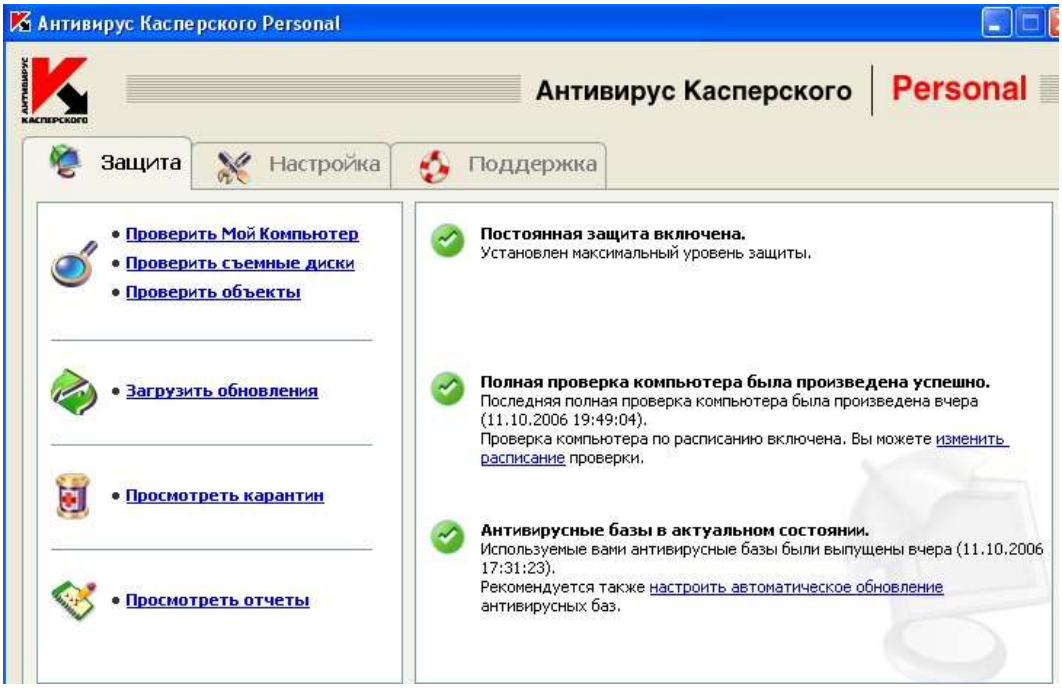
1. Выберите диски (вы можете выбрать сразу и CD-диск и дискету).
2. Установите курсор мыши на имени выбранного объекта.
3. Щелчком по правой кнопке мыши откройте контекстное меню Windows и выберите пункт **Проверить на вирусы**.



Чтобы проверить **CD-диск или дискету на присутствие вирусов из главного окна Антивируса Касперского Personal**

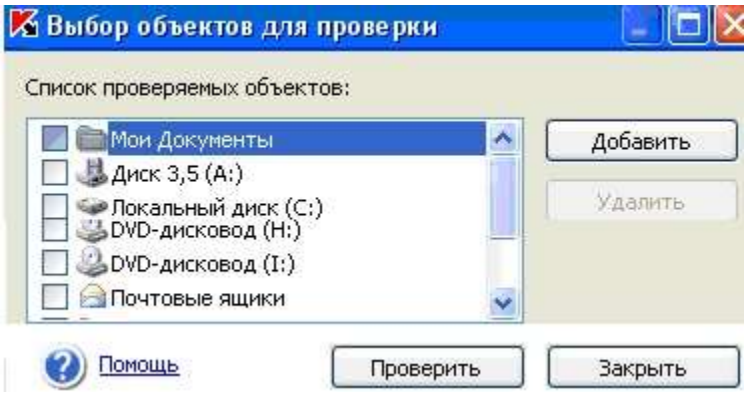
1. Вставьте CD-диск в CD-ROM-устройство или дискету в дисковод. Обратите внимание, программа сможет проверить и CD-диск и дискету за один прием.

2. Воспользуйтесь гиперссылкой Проверить съемные диски, расположенной в левой части закладки **Защита**.

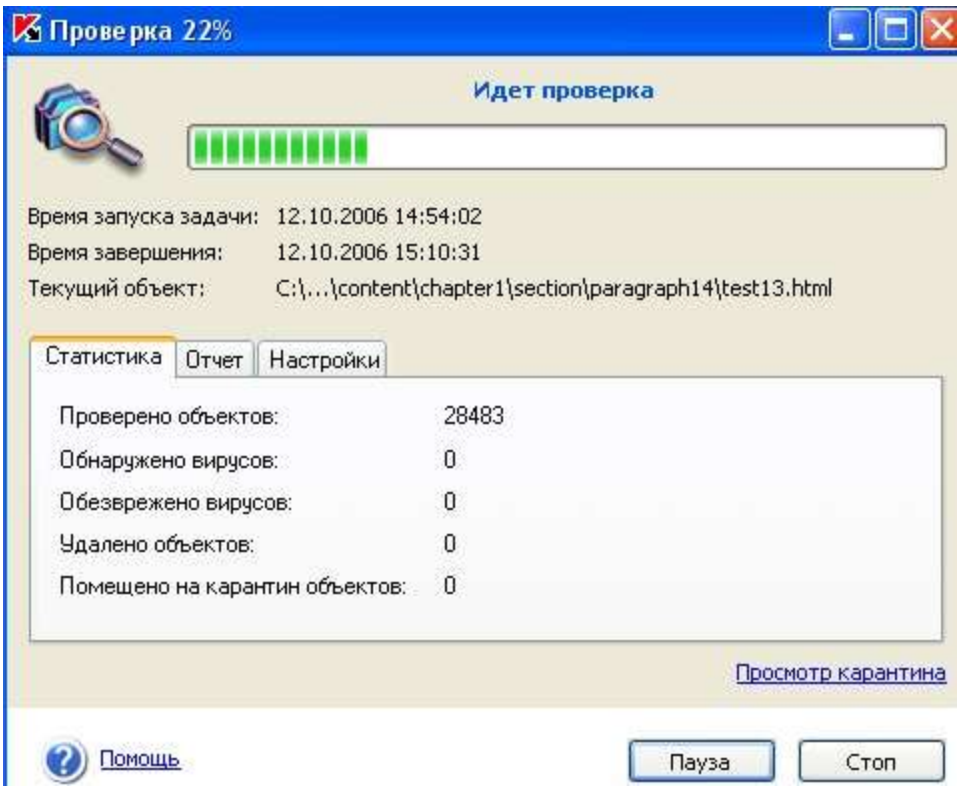


или

По гиперссылке Проверить объекты перейдите в окно **Выбор объектов для проверки**, выберите съемные диски и нажмите на кнопку **Проверить**.



Сразу после запуска проверки на экране откроется окно **Проверка**, где будет отображаться процесс выполнения действия над выбранными объектами списка.



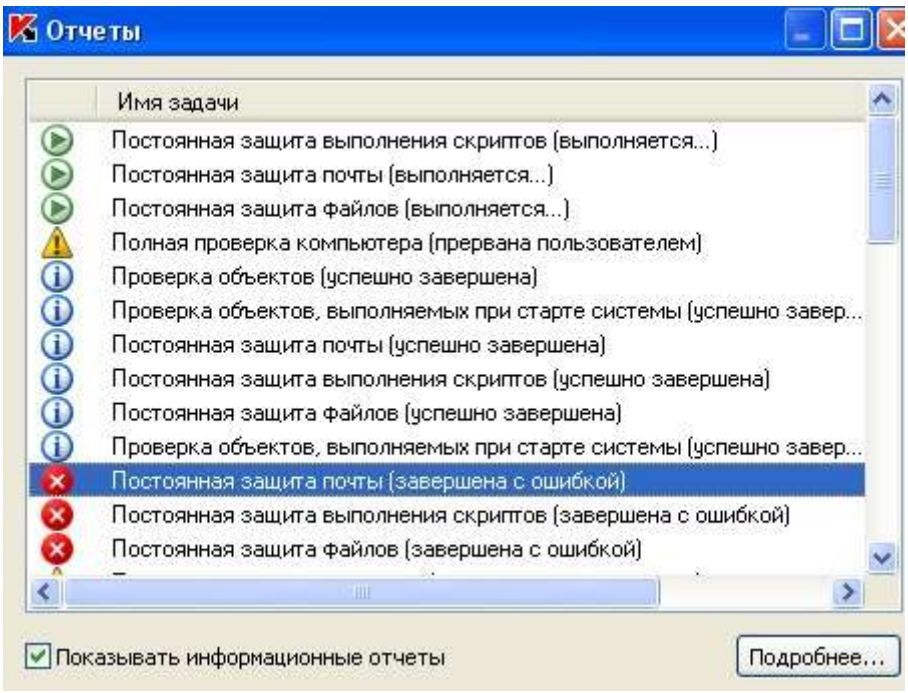
Если для проверки вы выбрали только один съемный диск (устройство), по окончании проверки Антивирус Касперского Personal предложит вставить следующий диск (устройство).

Обратите внимание на некоторые особенности работы программы:

- Если вы забыли вставить диск или дискету перед запуском проверки, либо съемный накопитель, дисковод или CD-ROM, отключен, проверка проводиться не будет, и программа не выдаст никакого дополнительного сообщения по этому поводу.
- Если вы вставили дискету в дисковод уже после запуска проверки, она не будет проверена. То же относится к CD-диску и другим съемным дискам.
- Если вы вынули дискету из дисковода или отключили съемный диск во время его проверки, программа занесет в отчет сообщение об ошибке, но не выдаст на экран никакого дополнительного сообщения. Программа перейдет к проверке следующего съемного диска, если таковой есть.

В момент монтирования съемного диска в систему (когда диск определяется операционной системой как новое устройство) Антивирус выполнит проверку такого диска и на присутствие **boot-вируса.**

Во время выполнения проверки компьютера, выбранных объектов, обновления антивирусных баз, а также постоянной защиты формируется отчет о проверенных объектах и результатах их обработки, а также общая статистика. Полный список всех выполняемых задач ведется Антивирусом Касперского в окне **Отчеты**, открыть который можно по гиперссылке Просмотреть отчеты в левой части закладки **Защита**. Здесь фиксируется статус каждой задачи, а также дата и время ее окончания.



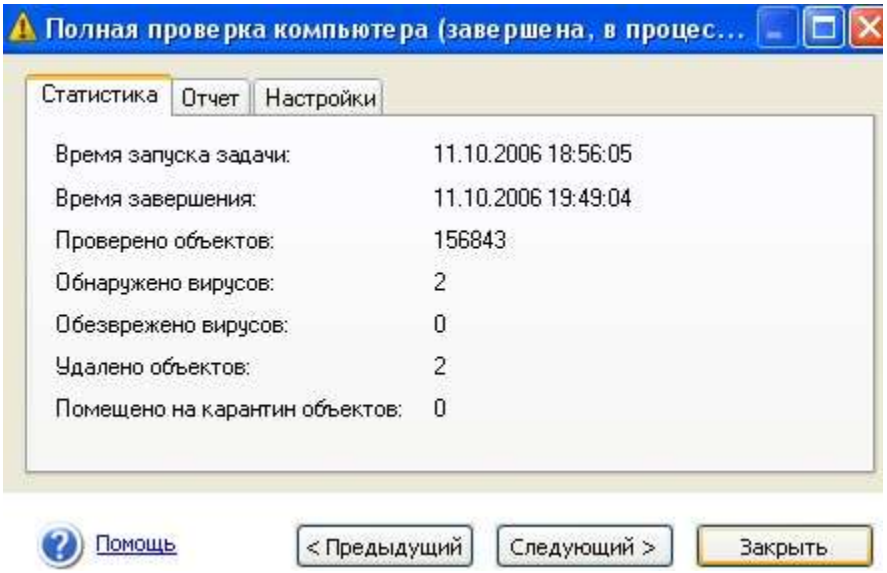
Информация по обработке объекта может быть следующих видов:

или *Информационное сообщение* (например: задача запущена, задача завершена, задача выполняется, задача приостановлена).

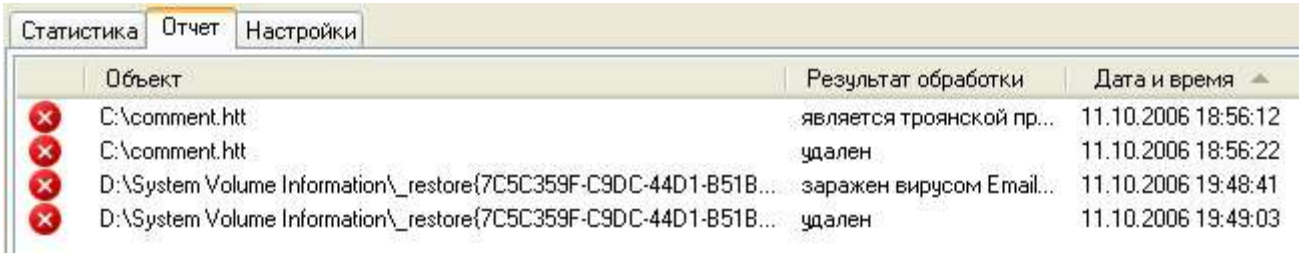
Внимание (например: Внимание! Остались необработанные объекты).

Примечание (например: задача прервана).

Выделив любой отчет и нажав на кнопку *Подробнее* можно просмотреть информацию о ходе проверки:



а на вкладке *Отчет* информацию о зараженных и вылеченных объектах:



Профилактика заражения компьютера вирусами.

Никакие самые надежные и разумные меры не смогут обеспечить стопроцентную защиту от компьютерных вирусов и троянских программ, но, выработав для себя ряд правил, вы существенно снизите вероятность вирусной атаки и степень возможного ущерба.

Одним из основных методов борьбы с вирусами является, как и в медицине, своевременная *профилактика*. Компьютерная профилактика состоит из небольшого количества правил, соблюдение которых значительно снижает вероятность заражения вирусом и потери каких-либо данных.

Ниже перечислены основные правила безопасности, выполнение которых позволит вам избегать вирусных атак.

Правило № 1: *защитите ваш компьютер с помощью антивирусных программ и программ безопасной работы в интернете*. Для этого:

- Безотлагательно установите антивирусную программу.
- Ежедневно обновляйте антивирусные базы. Обновление можно проводить несколько раз в день при возникновениях вирусных эпидемий
- Задайте рекомендуемые настройки для постоянной защиты. Постоянная защита вступает в силу сразу после включения компьютера и затрудняет вирусам проникновение на компьютер.
- Задайте рекомендуемые настройки для полной проверки компьютера и запланируйте ее выполнение не реже одного раза в неделю.

Правило № 2: *будьте осторожны при записи новых данных на компьютер*:

- Проверяйте на присутствие вирусов все съемные диски (дискеты, CD-диски, флэш-карты и пр.) перед их использованием.
- Осторожно обращайтесь с почтовыми сообщениями. Не запускайте никаких файлов, пришедших по почте, если вы не уверены, что они действительно должны были прийти к вам, даже если они отправлены вашими знакомыми. В особенности не доверяйте письмам якобы от антивирусных производителей.
- Внимательно относитесь к информации, получаемой из интернета. Если с какого-либо веб-сайта вам предлагается установить новую программу, обратите внимание на наличие у нее сертификата безопасности.
- Если вы копируете из интернета или локальной сети исполняемый файл, обязательно проверьте его антивирусной программой.
- Внимательно относитесь к выбору посещаемых вами интернет-сайтов. Некоторые из сайтов заражены опасными скрипт-вирусами или интернет-червями.

Правило № 3: *внимательно относитесь к информации об эпидемиях компьютерных вирусов.*.

В большинстве случаев о начале новой эпидемии сообщается задолго до того, как она достигнет своего пика. Вероятность заражения в этом случае еще невелика, и, скачав

обновленные антивирусные базы, вы сможете защитить себя от нового вируса заблаговременно.

Правило № 4: *с недоверием относитесь к вирусным мистификациям* - "страшилкам", письмам об угрозах заражения.

Правило № 5: *пользуйтесь сервисом Windows Update и регулярно устанавливайте обновления операционной системы Windows*.

Правило №6: *покупайте дистрибутивные копии программного обеспечения у официальных продавцов*.

Правило № 7: *ограничьте круг людей, допущенных к работе на вашем компьютере*.

Правило № 8: *уменьшите риск неприятных последствий возможного заражения*:

- Своевременно делайте резервное копирование данных. В случае потери данных система достаточно быстро может быть восстановлена при наличии резервных копий. Дистрибутивные диски, дискеты, флэш-карты и другие носители с программным обеспечением и ценной информацией должны храниться в надежном месте.
- Обязательно создайте системную аварийную дискету, с которой при необходимости можно будет загрузиться, используя "чистую" операционную систему.

Задание 1. Тестирование дискеты на наличие компьютерного вируса.

1. Вставьте дискету в дисковод A:.
2. Запустите имеющуюся у вас антивирусную программу, например AVP Касперского.
3. Задайте область проверки —, режим проверки — лечение зараженных файлов и нажмите кнопку *Проверить*.
4. Обратите внимание на индикатор процесса сканирования. Если антивирусная программа обнаружила вирусы и произвела лечение файлов (что видно в отчете о сканировании), запустите процесс сканирования дискеты еще раз и убедитесь, что все вирусы удалены.
5. Составьте отчет о проделанной работе, описав каждый пункт выполнения задания.
6. Выполните дополнительные задания.
7. Запишите ответы на контрольные вопросы в тетрадь для лабораторных работ.

Дополнительные задания

Задание 2. Антивирусная проверка информации на жестком диске.

Запустите имеющуюся у вас антивирусную программу и проверьте наличие вирусов на локальном диске C:.

Задание 3. Проверка дискеты с записанным файлом на наличие вируса.

Найдите на диске C: файлы с любым расширением, начинающиеся на букву w (маска для поиска — w*). Скопируйте самый маленький по размеру из найденных файлов на дискету (проведите сортировку по размеру). Проверьте дискету с записанным файлом на наличие вирусов.

Контрольные вопросы:

1. Что такое компьютерный вирус?
2. На какие типы разделяют компьютерные вирусы в различных видах классификации?
3. Чем отличаются макровирусы от обычных загрузочных вирусов?
4. Каковы основные пути проникновения вирусов в компьютер?
5. По каким признакам можно судить о поражении компьютера вирусом?

6. Какие типы антивирусных программ вам известны?
7. Каковы назначение и основные функции Антивируса Касперского Personal?
8. Как проверить CD-диск или дискету на наличие вируса с помощью программы Антивирус Касперского?
9. В каком файле содержится информация о зараженных и вылеченных объектах?
10. Перечислите профилактические меры для борьбы с заражением вирусами.

Практическая работа № 9 Цифровая подпись драйверов. Откат драйверов.

Теоретические сведения.

Дра́йвер — компьютерное программное обеспечение, с помощью которого другое программное обеспечение (операционная система) получает доступ к аппаратному обеспечению некоторого устройства. Обычно с операционными системами поставляются драйверы для ключевых компонентов аппаратного обеспечения, без которых система не сможет работать. Однако для некоторых устройств (таких, как видеокарта или принтер) могут потребоваться специальные драйверы, обычно предоставляемые производителем устройства.

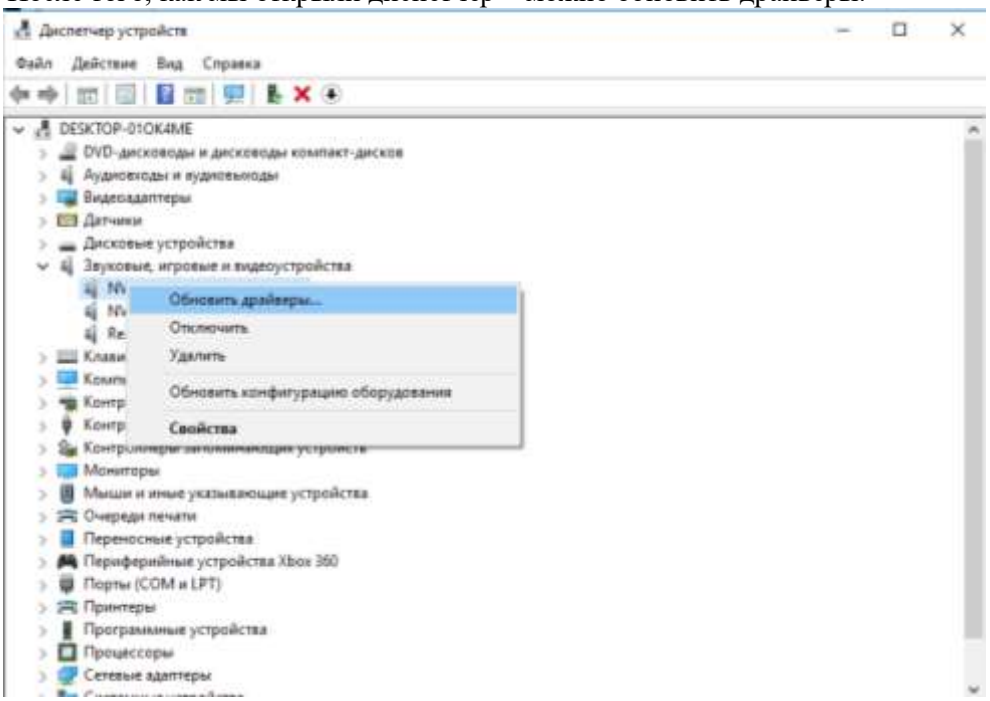
Обновление с помощью стандартных средств Windows.

Часто бывают ситуации, когда необходимо обновить драйвер. Обычно это происходит автоматически, при подключении в сети интернет. Но это происходит не всегда. Так что же делать, если вам необходимо обновить драйверы некоторых устройств, но вы не знаете их название и модель. В этом случае, как правило, пользователь обычно и не догадывается, есть ли у него тот или иной драйвер, пока не столкнется с определенной проблемой: нет звука например, или при запуске игры - выскакивает шибка о необходимости установки видео драйверов и пр.

При таком положении дел, в первую очередь, рекомендую зайти в диспетчер устройств и посмотреть, все ли драйвера установлены и нет ли конфликтов.

(Для входа в диспетчер устройств в Windows 7, 8, 10 - зайдите в панель управлении и введите в поисковую строку "диспетчер". Далее в найденных результатах выберите нужную вкладку, либо зайдите в панель управления, далее диспетчер устройств).

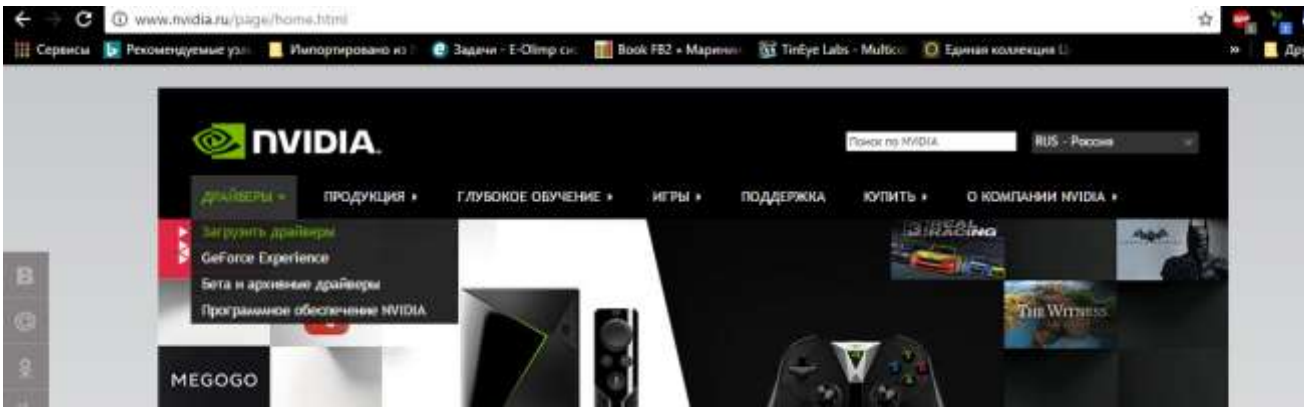
После того, как мы открыли диспетчер – можно обновить драйверы.



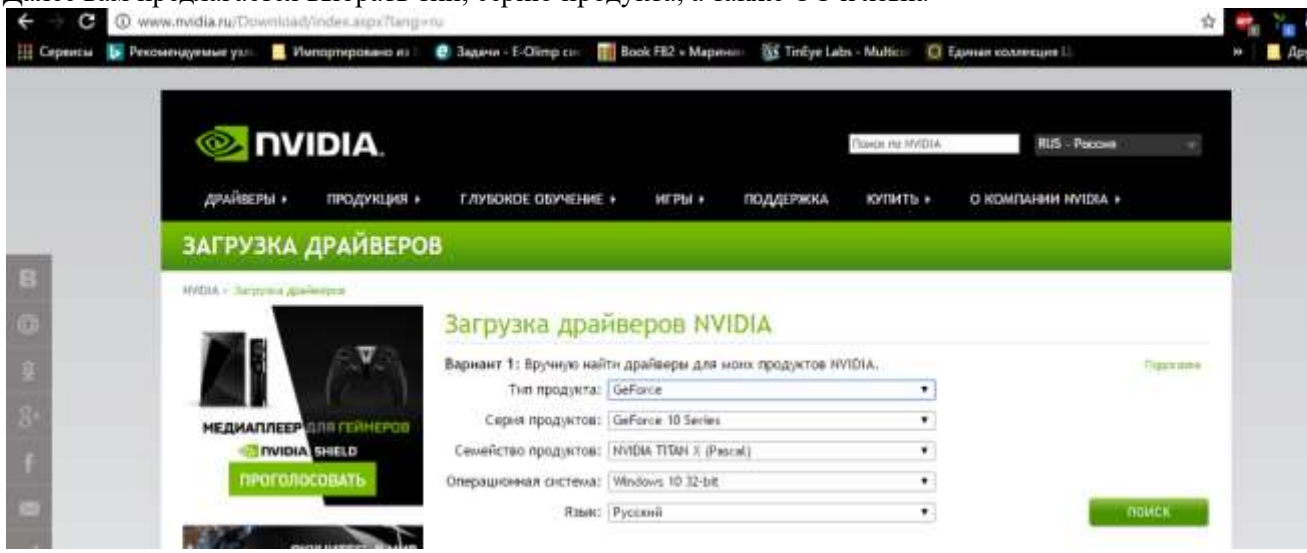
Обновление с помощью сайта производителя.

Если известна марка и модель устройства, можно зайти на официальный сайт и уже там найти необходимые драйвера. Например, вам необходимо обновить драйвер на видеокарту GeForce.

Для этого заходите на официальный сайт nvidia.ru и переходите в раздел Драйверы -> Загрузить драйверы.



Далее вам предлагается выбрать тип, серию продукта, а также ОС и язык.



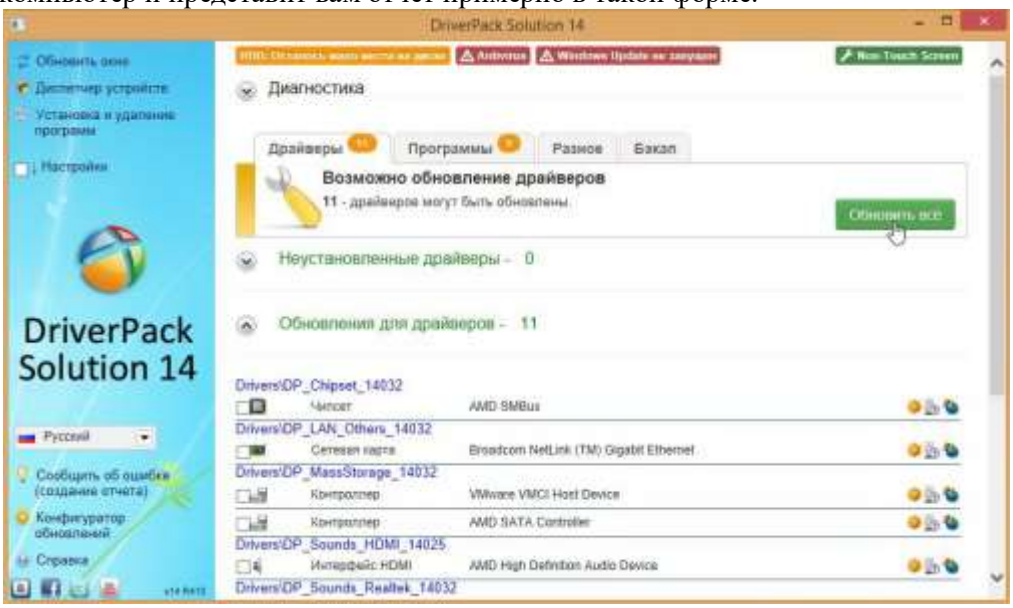
Обновление драйверов с помощью ПО.

Кроме этого существует еще множество программных продуктов, с помощью которых можно осуществить поиск и обновление драйверов. Давайте рассмотрим несколько из них.

DriverPack Solution (*http://drp.su/ru/download.htm)*

Одна из лучших программ для поиска и обновления драйверов - это пакет Driver Pack Solution. Представляет собой образ ISO.

После того, как скачанный образ будет открыт, программа автоматически просканирует ваш компьютер и представит вам отчет примерно в такой форме.

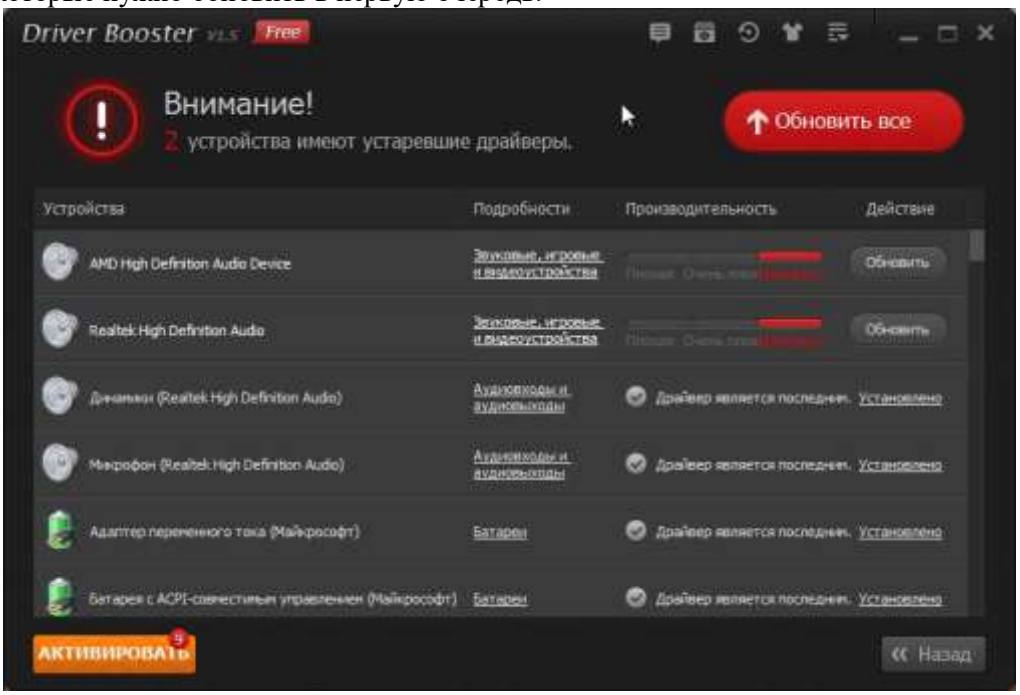


Для пользователя остается лишь поставить галочки напротив тех драйверов, которые нужно установить и нажать кнопку начала операции. Кстати, я например, почти всегда нажимаю "обновить

все" - и через 10-15 мин. на компьютере или ноутбуке есть все драйвера необходимые для работы (хотя, иногда, бывает нужно "руками" устанавливать некоторые редкие драйвера, которых в базе программы нет).

Driver Booster (*http://ru.iobit.com/driver-booster)*

Driver Booster - весьма неплохая программа (кстати русская + есть бесплатная версия), которая быстро может просканировать компьютер на наличие старых драйверов. К тому же, программа не просто покажет какие драйвера нужно обновить, но и укажет критичность обновления, т.е. те драйвера, которые нужно обновить в первую очередь.



Окно программы Driver Booster после выполнения сканирования системы. Как видно на скриншоте, нужно обновить звуковые драйвера.

Что радует в программе, драйвера можно обновлять в фоновом режиме, т.е. нажав всего одну кнопку. Программа автоматически создает контрольную точку, чтобы в случае чего - можно был откатить систему в рабочее состояние.

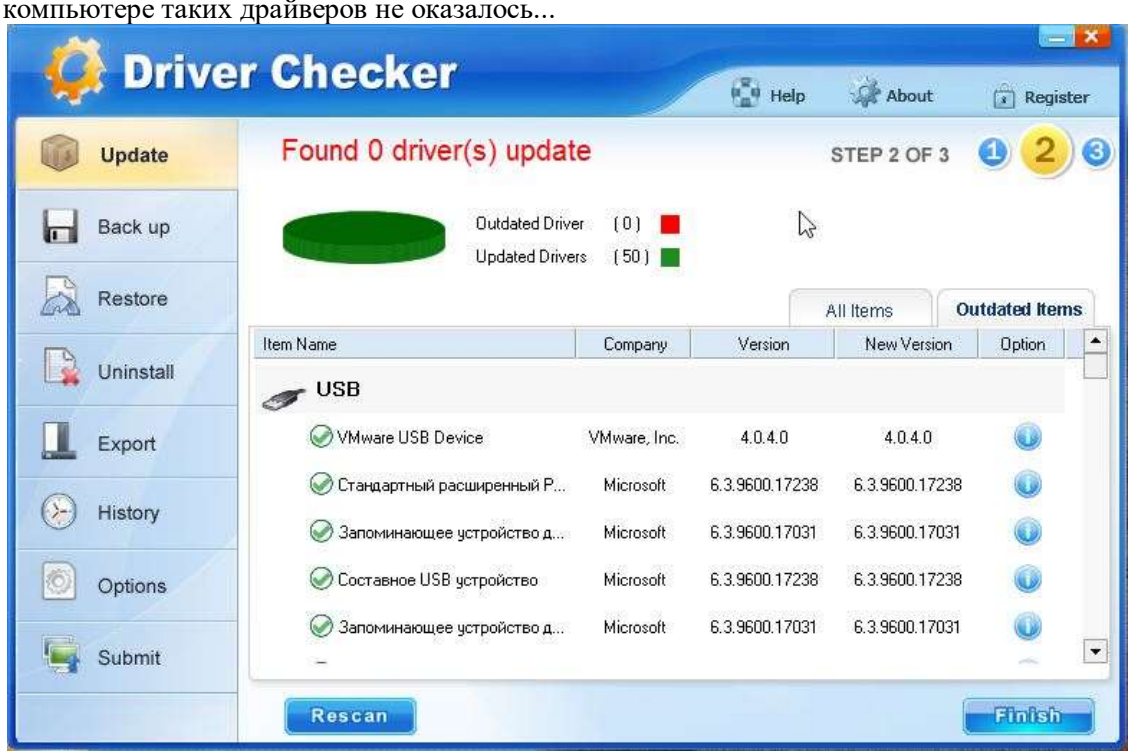
Driver Checker (*http://www.driverchecker.com/download.php*)

Об этой утилите нельзя не сказать. И вот почему...

Представьте, вам предстоит переустановить ОС Windows, а у вас нет ни одного установочного пакета драйверов. Эта программа позволяет сохранить все установленные драйвера из системы (сделать бэкап), а затем, в любое время восстановить их из бэкапа. Очень удобно!

Пользоваться программой очень легко, после запуска она сама предложит просканировать систему.

После сканирование предоставит отчет, какие драйвера следовало бы обновить. Например, на моем компьютере таких драйверов не оказалось...



Задание:

1. Просмотреть в диспетчере устройств, какие устройства нуждаются в установке драйвера.
2. Если таковые имеются, то необходимо обновить его автоматически, либо на сайте производителя найти необходимый драйвер.
3. **Запустить программу Driver Booster.**
4. **Просканировать ПК.**
5. Определить, какие устройства нуждаются в обновлении драйверов.
6. Обновить драйверы.

Отчёт должен быть оформлен в программе MS Word и содержать следующие пункты:

1. Название работы.
2. Цель работы.
3. Оборудование.
4. Задание.
5. Скриншоты выполнения задания.

Практическая работа № 10 Безопасный режим загрузки. Точки восстановления системы. Резервное копирование и восстановление. Аварийное восстановление

Задание. Проверить работу средства **Восстановление системы** путем запуска восстановления через командную строку и создания контрольной точки и выполнения восстановления системы до более раннего состояния.

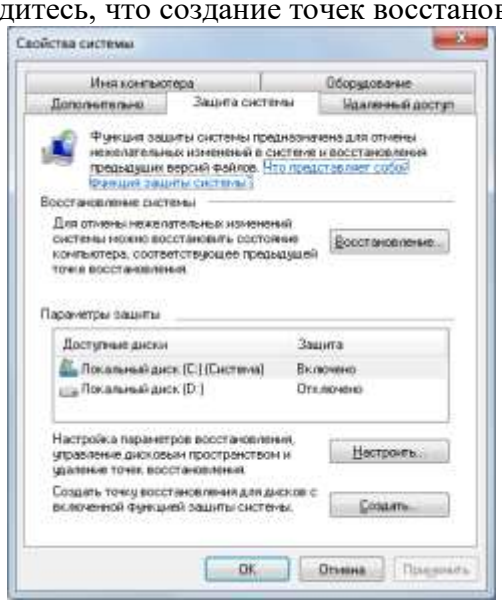
Последовательность выполнения

1. Убедитесь, что средство **Восстановление системы** включено. Для этого:

1) щелкните правой кнопкой мыши на значке **Компьютер** и выберите пункт Свойства**;**

2) перейдите по ссылке **Защита системы** и подтвердите действия в окне ;

3) убедитесь, что создание точек восстановления включено по крайней мере для системного



диска

2. Создайте новую точку восстановления следующим способом:

1) запустите программу **Восстановление системы,** выполнив ее поиск в меню **Пуск и** подтвердив действия в окне;

2) в появившемся окне перейдите по ссылке **Защита системы;**

3) в следующем окне нажмите кнопку **Создать,** введите любое описание создаваемой точки, еще раз щелкните на кнопке **Создать** и дождитесь завершения операции.

3. Выполните какие-либо действия на компьютере, например:

1) измените настройки **Рабочего стола** и **Панели задач** ;

2) создайте несколько рисунков или текстовых документов и сохраните их в папку **Документы;**

3) установите любую небольшую программу и проверьте ее работу.

4. Используя любой метод запуска командной строки и команду **rstrui.exe** Выполните восстановление системы до ранее созданной контрольной точки:

1) запустите программу **Восстановление системы** с помощью поиска в меню **Пуск и** подтвердите запуск программы в окне;

2) в окне **Восстановление системы** установите переключатель в положение **Выбрать другую точку восстановления** и нажмите кнопку **Далее;**
3) в следующем окне выберите созданную точку и щелкните на кнопке **Далее;**
4) для начала восстановления еще раз нажмите кнопку **Далее** и затем **Готово;** подтвердите действия в появившемся диалоговом окне и дождитесь завершения всех операций, а также автоматической перезагрузки компьютера.
5. Проверьте, сохранились ли изменения, внесенные после создания контрольной точки:
• для всех системных настроек должны установиться прежние значения;
• восстановление системы не должно затронуть документы любых типов;
• программа, установленная позже контрольной точки, должна быть удалена.
Ответьте на вопросы:
1. Перечислите способы запуска **Восстановления системы**
2. Перечислите способы запуска **Командной строки**
3. Дайте понятие Утилит
4. Какие служебные программы вы знаете
5. Каково назначение Архиваторов?

Практическая работа № №11 Установка и настройка системы. Установка параметров автоматического обновления системы. Устранение проблем, возникающих во время установки. Диагностика и мониторинг устройств компьютера. Установка нового устройства. Поддержка аппаратных средств.

Краткие теоретические сведения.
Windows 7 – наиболее новая клиентская ОС фирмы Microsoft, выпущенная в октябре 2009 года. От предыдущих версий Windows она отличается значительно более удобным пользовательским интерфейсом, с которым Вы и познакомитпесь в данной работе, и более высоким быстродействием. Система все больше завоевывает популярность пользователей.
Запуск системы

- Включите компьютер с инсталлированной Windows 7.
- Менее чем через минуту система загружается и готова к работе.
- Выводится начальное меню с именами пользователей.

Вход в систему и аутентификация пользователя
Выберите Ваше имя пользователя и кликните мышкой по картинке рядом с именем. Как правило, в систему уже введено стандартное имя User. Если для пользователя установлен пароль, введите его.
После входа в систему на экране визуализируется рабочий стол.
Структура рабочего стола, мой компьютер, панель управления
Рабочий стол состоит из иконок приложений (например, Internet Explorer) и панели задач (taskbar) – обычно серого цвета, в нижней части. В левом нижнем углу расположена кнопка Start, при нажатии на которую пользователь может выбрать начальное действие – запуск какого-либо приложения, создание документа и др.
Вид и фон рабочего стола при разных настройках могут отличаться. Для изменения фона рабочего стола необходимо на фоновом рисунке нажать правую кнопку мыши и в контекстном меню выбрать Properties / Desktop, после чего выбрать нужный рисунок фона в выпадающем списке.
Основные пункты стартового меню, визуализируемого в результате нажатия кнопки Start:

- Computer – информация о компьютере, его ресурсах, устройствах, имени, установеленной на нем ОС
- Documents – стандартная папка для создаваемых документов (Вы можете помещать документы и в любую другую более удобную Вам папку)
- Control Panel – панель управления (рис. 36.3)

- Search programs and files – поиск и запуск программ и открытие файлов
- (в нижней части) Shut down – выход из Вашего пользовательского сеанса, выключение компьютера или перезапуск системы.

Рассмотрите более подробно панель управления. Она позволяет управлять ресурсами компьютера. Например, пункт Programs and Features позволяет инсталлировать новые программы, деинсталлировать или инсталлировать вновь ("ремонтировать") уже установленные.

Выберите в стартовом меню пункт Мой компьютер. При этом в специальном окне визуализируется информация о состоянии компьютера.

В окне Мой компьютер визуализируется информация о дисках и некоторых наиболее важных папках и предлагается набор возможных действий и набор других информационных узлов для перехода к ним (например, Network).

Для визуализации основных свойств компьютера (системной информации) выберите в стартовом меню: Мой компьютер / (Правая кнопка мыши) / Свойства. Возникает окно с системной информацией.

Вы видите информацию об ОС, объеме памяти, типе процессора и ряд ссылок, например, Device Manager, кликнув на которую, получите подробную информацию о составе оборудования компьютера и установленных драйверах. Интерфейс оформлен в виде веб-страницы.

Работа с файлами и папками

Работа с файлами и папками (folders) – хранилищами ссылок на файлы и другие папки – осуществляется с помощью программы Windows Explorer.

Выбор файла или папки в директории выполняется одним кликом мышки, вход в директорию или открытие файла – двойным кликом мышки на имени директории или файла. При этом для файла выполняется действие его открытия, зависящее от его типа, - для текстовых файлов – вызов соответствующего редактора (notepad, WordPad, MS Word и др.), для файлов .pdf – вызов Adobe Acrobat, для исполняемых кодов или командных файлов – запуск соответствующей программы или скрипта и т.д. Поэкспериментируйте на своем компьютере с навигацией по файлам и папкам и открытием файлов с документами.

Есть несколько способов запустить программу:

- из Windows Explorer – дважды кликнуть на имени ее файла;
- из меню Start – выбрать пункт Search programs and files. Это – одно из самых удобных нововведений в пользовательском интерфейсе системы Windows 7. При поиске, по мере набора имени программы, выводятся списки программ и файлов с таким именем (префиксом имени), что позволяет очень комфортно выбирать программу для запуска. Выбрав имя редактора notepad. получите окно для его запуска кликом мышки на имени программы.
- Запуск программы из командной строки (Command Prompt): выберите Start / Search Programs and Files / cmd. После запуска командного процессора визуализируется его окно. В окне командной строки наберите имя программы (например, notepad) и нажмите Enter.

Сетевые установки

Для подсоединения компьютера к локальной TCP/IP - сети необходимо выполнить для него сетевые установки – задать IP-адрес и сетевую маску.

Физическое подсоединение к сети сделайте (проверьте) путем подсоединения к сетевому разъему (RJ45) сетевого кабеля вида twisted pair (витая пара), который соединяет Ваш компьютер с сетевым концентратором (hub) или переключателем (switch). Наличие физического соединения индицируется зеленым световым индикатором (проверьте).

Для соединения в сеть служит сетевая карта (сетевой адаптер). Ваша задача – правильно задать IP-адрес компьютера.

Работа на удаленных компьютерах

При работе в локальной сети очень полезная возможность Windows 7 – удаленный вход на другой компьютер Вашей локальной сети. В Windows такая функция системы называется Remote Desktop Connection (удаленный рабочий стол). Для соединения Вы должны знать имя другого компьютера, например, aphrodite.

Настройка оборудования и звука в Windows 7

В этом меню в панели управления теперь собраны все настройки касающиеся внешнего оборудования Вашего компьютера.

1.Устройства и принтеры. Здесь собрано все оборудование, которое так или иначе можно отключать и подключать к компьютеру через порт или через сетевое соединение. Так же, здесь отображается сам компьютер.

1. Для каждого устройства доступны как общие настройки, такие как обновление драйвера или удаление его, так и индивидуальные. К примеру, если кликнуть правой кнопкой мыши по значку мыши мы увидим, что возможно прямо отсюда изменить параметры мыши и указателей.

2. Если устройство подключено к компьютеру, но не отображается в списке, то Вам следует воспользоваться мастером добавления устройства, благодаря которому новое устройство будет распознано и установлено. Для этого нажмите кнопку *"Добавление устройства"* в верхнем левом углу.

2. Автозапуск. Выбрав пункт автозапуск Вы сможете настроить автоматический запуск определенных типов устройств или носителей.

3. Звук. В настройках звука есть выбор устройства для воспроизведения и для записи по умолчанию. Здесь, как и в меню персонализации, вы можете настроить и выбрать звуковую схему оформления. Так же, здесь появилась функция, позволяющая автоматически понижать громкость всех системных звуков при поступлении звонка по Voip-каналу. Автоматически громкость может быть понижена на 80 или 50%, а так же Вы можете отключить все системные звуки при поступлении звонка или оставить их без изменения.

Выход из системы

Для выхода из Вашего сеанса пользователя выберите Start / Shut down.

4. Задания

Задание 1. Просмотрите предложенный видеоматериал. Установка и настройка операционной системы Windows 7.

Задание 2. Напишите понятия и классификацию:

- Операционная система (ОС)
- Операционная система как виртуальная машина
- Операционная система как менеджер ресурсов
- Операционная система как защитник пользователей и программ
- Операционная система как постоянно функционирующее ядро
- Классификация ОС

Задание 3. Опишите этапы подготовки к установке Windows 7

Задание 4. Заполните таблицу. Установка и настройка Windows 7

№	Задание	Этапы установки Windows 7. Опишите действия на каждом из этапов.					
	Установка Windows 7	Подготовка жесткого диска.	Загрузка с установочного диска.	Определение параметров установки.	Следование инструкциям мастера установки.	Установка драйверов.	Активация ОС

<table>
<tr><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td></tr>
<tr><td></td><td>Первичные настройки Windows 7</td><td colspan="6">Основные этапы настройки Windows 7. Опишите действия на каждом из этапов.<table><tr><td>Персонализация</td><td>Свойства компьютера</td><td>Учетные записи</td><td>Антивирусное ПО</td></tr><tr><td></td><td></td><td></td><td></td></tr></table></td></tr>
<tr><td></td><td>Контекстное меню Windows 7</td><td colspan="6">Опишите работу с контекстным меню Windows 7</td></tr>
<tr><td></td><td></td><td colspan="6"></td></tr>
<tr><td></td><td>Оборудование и звук Windows 7</td><td colspan="6">Этапы настройки оборудования и звука Windows 7. Опишите действия на каждом из этапов.<table><tr><td>Устройства и принтеры</td><td>Автозапуск</td><td>Звук</td></tr><tr><td></td><td></td><td></td></tr></table></td></tr>
<tr><td></td><td>Сетевые настройки Windows 7</td><td colspan="6">Этапы настройки домашней сети Windows 7. Опишите действия на каждом из этапов.
Настройка сетевого подключения Windows 7.
В ОС Windows 7 настройка сетевого подключения сводится к следующим этапам:
• Подсоедините компьютер к свитчу, роутеру или концентратору. Для этого подключите коннектор RJ-45 к порту Ethernet. Чтобы быть уверенным в успешном коннекте к сети, щелкните вкладку «Сеть». Откроется окно со значками, свидетельствующими о добавлении устройств в сеть.
• В Windows 7 настройки сетевого подключения в основном вращаются вокруг апплета «Сеть». Эта папка является удобным инструментом доступа к узлам сети. Итак, если не обнаруживается значок, то возможно было отключено обнаружение или общий доступ.<table><tr><td>1. Разработка схемы сети
• •</td><td>2. Выбор необходимого оборудования и поставщика услуг
•</td><td>3. Настройка маршрутизатора
• •</td><td>4. Подключение маршрутизатора к Интернету (дополнительно)
•</td><td>5. Подключение компьютеров и устройств к сети
• •</td><td>6. Создание домашней группы или включение общего доступа к файлам и принтерам
•</td></tr><tr><td></td><td></td><td></td><td></td><td></td><td></td></tr></table></td></tr>
</table>

5. Содержание отчета

Отчет должен содержать:

1. Название работы.
2. Цель работы.
3. Задание и его решение.
4. Вывод по работе.

6. Контрольные вопросы

1. Что такое операционная система?

2. Как сделать загрузочный диск (флэшнакопитель)?
3. Какие способы запуска программ в Windows 7 применяются?

Практическая работа №12 Работа с дисками и томами. Управление дисковыми ресурсами. Виртуализация. Множественные прикладные среды.

Задание

5. Запустить командную строку. Просмотреть версию операционной системы, текущую дату и время.
6. Создать на рабочем диске каталог.
7. Выполнить команды для работы с диском, каталогами и файлами.
8. Ответить на вопросы.

Ход выполнения работы

3. Запустить командную строку Пуск - Программы - Стандартные:

а) С помощью команды (например, D:) выполнить переход к диску пользователя.

б) С помощью команды ver через командную строку просмотреть версию операционной системы, текущую дату и время.

4. Создать на рабочем диске каталог с помощью команды md.

а) В каталоге с номером своей группы создать папку под своей фамилией (команда md). Перейти к своей папке.

б) В своей папке создать два каталога с именами Proba и Zadanie.

в) Просмотреть содержимое своей папки (команда dir).

г) В папке Proba создать 2 текстовых файла (команда copy con) с именами text1.txt, , записав в них следующую информацию: в файл text1.txt - ваши фамилия, имя, отчество, в файл text2.txt - сведения о вашей специальности.

д) Выполнить соединение информации двух текстовых файлов (copy text1.txt+text2.txt) в файл itog.txt в папку Zadanie.

е) Просмотреть содержимое папок Proba и Zadanie.

ж) Просмотреть содержимое файла itog.txt (команда type).

з) Скопировать файл itog.txt в папку Proba, задав ему новое имя new.txt.

и) В папку Zadanie скопировать 4 других файла разного типа, предварительно выполнив их поиск на компьютере. Просмотреть содержимое папки Zadanie.

к) Выполнить сортировку файлов в папке Zadanie по размеру, по дате, типу, имени.

л) Переименовать папку Proba в PRIMER (команда move).

м) Представить работу преподавателю.

н) После проверки удалить свою папку.

Вопросы для самопроверки

6. Каково назначение командной строки?
7. Как произвести запуск командной строки?
8. Назовите команды для работы с дисками (переход к другому диску).
9. Назовите команды для работы с каталогами (переход к каталогу, создание, копирование, переименование, просмотр, удаление).
10. Назовите команды для работы с файлами (создание, копирование, переименование, просмотр, удаление, сортировка).

Практическая работа №13 Решение типовых задач администрирования. Работа с консолью управления Microsoft(MMC). Средства управления реестром.
Краткие теоретические и учебно-методические материалы по теме практической работы:

Консоль управления Microsoft Management Console (MMC) *группирует средства администрирования, которые используются для администрирования сетей, компьютеров, служб и других системных компонентов.* Консоль MMC непосредственно не выполняет административные функции, однако предоставляет возможности интеграции в нее компонентов или системных приложений, выполняющие эти функции. Основной тип интегрируемых на консоль компонентов называется оснасткой, которые не могут выполняться отдельно без консоли. Среди других добавляемых элементов могут быть элементы управления ActiveX, ссылки на Web-страницы, папки, видов панели задач и собственно задачи для выполнения. Дополнительные теоретические сведения об оснастках и других используемых для интеграции на консоль элементах будут добавлены в дальнейшем, в соответствующих разделах настоящей практической работы. Базовое окно консоли MMC представляет собой графическую форму с контекстными меню, реализующие дружественный пользовательский интерфейс. Имеется панель инструментов с командами создания, открытия и сохранения консолей и, кроме того, область описания и строка состояния в нижней части окна. Чтобы увидеть базовое окно, а также непосредственно саму консоль MMC, необходимо выполнить следующие действия:

- нажмите Пуск | Выполнить,
- наберите в появившемся окне MMC.exe (или просто mmc),
- нажмите Enter для ввода.

Новая консоль MMC представляет собой отдельное окно, разделенное на две вертикальные области, в левой из которых отображается дерево консоли с его корнем. Дерево консоли показывает доступные элементы и компоненты консоли. Правая область является областью сведений, которая содержит описания элементов и выполняемых ими функций. Содержание области сведений соответствует выбранному элементу в дереве консоли и может включать Web-страницы, графики, диаграммы, таблицы и столбцы.
Создавая надежные средства управления компьютерами сети, можно собрать и настроить собственную консоль MMC, выполняющую заданные функции администрирования. После того как добавлены все необходимые элементы и компоненты консоли, панель главного меню, панель инструментов, а также область описания и строка состояния могут быть скрыты для предотвращения в дальнейшем нежелательных изменений. Созданные таким образом управляющие системы сохраняются в файлах с расширением .msc (Management Saved Console, сохраненная консоль управления) и могут быть, в частности, распространены в пределах всей системы посредством задания к ним доступа с помощью ярлыков или элементов меню Пуск. Чтобы увидеть консоль управления локальным компьютером в качестве примера готовой и отлаженной консоли MMC, необходимо выполнить:

- нажмите Пуск | Выполнить,
- наберите в появившемся окне compmgmt.msc (или compmgmt),
- нажмите Enter для ввода.

Существует два основных режима доступа консоли администрирования, задающиеся непосредственно при ее создании:

- пользовательский, в котором можно администрировать систему, работая с уже существующими консолями,
- авторский, в котором можно создавать новые консоли или изменять существующие.

В свою очередь, имеется три уровня режима пользователя, что обусловливает всего четыре варианта предустановленного режима доступа:
1. авторский режим;
2. режим пользователя — полный доступ;

3. режим пользователя — ограниченный доступ, многооконный;
4. режим пользователя — ограниченный доступ, однооконный.
Консоль ММС, инициализированная в авторском режиме, предоставляет полный доступ ко всем ее возможностям, включая добавление и удаление оснасток, создание новых окон и панелей задач, а также просмотр любых частей дерева консоли и другие. Однако при выборе одного из трех режимов пользователя авторские возможности исключаются. В частности, если для консоли установлен параметр «пользовательский режим — полный доступ», то предоставляются все команды управления окном консоли и полный доступ к ее дереву, но запрещается добавление, удаление оснасток и изменение свойств консоли администрирования. Изменения консоли ММС в авторском и пользовательском режимах сохраняются по-разному. При закрытии консоли в авторском режиме выводится диалоговое окно с предложением сохранить изменения. Однако в пользовательском режиме и снятом флажке «Не сохранять изменения для этой консоли» изменения будут сохранены автоматически при закрытии. Если консоль открыта при соблюдении одного из следующих условий:
- в базовом окне при загрузке,
- с помощью команды контекстного меню Автор,
- в командной строке с параметром /a,
то предустановленный режим игнорируется, а открытие консоли осуществляется в авторском режиме. Очевидно, что загрузка консоли ММС в авторском режиме не требуется рядовым пользователям. Системный администратор может настроить профили пользователей так, чтобы запретить им переход в авторский режим, как из командной строки, так и через контекстное меню. Кроме того, запрет перехода в авторский режим может быть организован при использовании возможностей групповой политики, при которой, в частности, осуществляется ограничение доступа к определенным оснасткам. Рассмотрению базовых возможностей оснастки групповой политики будет посвящена вторая часть настоящей практической работы. Прежде чем создавать новую консоль ММС, необходимо определить действия, для которых предназначена эта консоль, список администрируемых компонентов, оснасток и других элементов, которые потребуются для выполнения поставленных задач. Следует также рассмотреть необходимость создания видов панели задач. После принятия этих решений можно открыть новую консоль и начать добавлять элементы к дереву консоли. Полное руководство по созданию и настройке консолей ММС находится на Web-узле корпорации Майкрософт (http://www.microsoft.com). В практической работе предполагается ознакомление с основными принципами организации и построения консоли администрирования ММС, а также с базовыми возможностями основных инструментов системного администратора — оснасток «Локальные пользователи и группы» и «Редактор объекта групповой политики» («Групповая политика»). Перед началом выполнения заданий в среде ОС Windows необходимо выполнить следующее:
1. запустить виртуальную машину с ОС Windows и активировать справочное меню (Пуск | Справка и поддержка);
2. ознакомиться с описанием и возможностями запуска и применения консоли администрирования ММС;
3. ознакомиться возможностью получения сведений пункта 2 из альтернативного источника информации, доступного непосредственно в справке консоли администрирования ММС (Справка | Вызов справки);
4. ознакомиться с описанием и возможностями оснасток «Локальные пользователи и группы» и «Редактор объекта групповой политики» («Групповая политика»).

Задание для практической работы

Задание 1. Изменение параметров и способов настройки консоли администрирования ММС

Порядок выполнения:

I. Создание консоли администрирования MMC в авторском режиме требует выполнения следующих действий:

- нажмите Пуск | Выполнить,
- наберите в появившемся окне MMC.exe (или просто mmc),
- нажмите Enter для ввода.

Возможны следующие альтернативные варианты авторского запуска консоли администрирования:

1) запуск из командной строки, используя синтаксис:

Mmc *путь\имя_файла*.**msc /a**,

где параметр:

путь\имя_файла.**msc** — запускает консоль MMC с одновременным открытием файла сохраненной консоли с именем *имя_файла*.**msc** (Приложение 2). Если файл консоли не указан, будет открыта новая консоль MMC.

/a — открывает консоль MMC в авторском режиме.

Дополнительными параметрами команды могут быть:

/64 — открывает 64-разрядную версию консоли MMC (MMC64). Этот параметр используется
только при работе в ОС Windows 64-Bit Edition.

/32 — открывает 32-разрядную версию консоли MMC (MMC32). При работе в ОС Windows 64-Bit Edition в окне консоли MMC, запущенной с этим параметром, открываются 32-разрядные
оснастки.

2) запуск из файлового менеджера Проводник ОС Windows:

- наведите манипулятор мышь на файл с расширением .msc, находящийся в системной папке ОС (%systemroot%\system32\),
- кликните правой кнопкой мыши на файле и из контекстного меню выберите Автор.

II. Настройка параметров консоли администрирования MMC предназначена для ее конфигурирования с целью придания ей уникального вида.

Содержание задания

Для придания уникального вида сохраненной (новой) консоли администрирования MMC в авторском режиме выполните следующие действия:

1. В меню Консоль выберите команду Параметры.
2. На вкладке Консоль в поле названия введите новый заголовок.
3. На вкладке Консоль выполните следующие действия:
   - нажмите кнопку Сменить значок,
   - в поле Имя файла введите путь к файлу, содержащему значки (например, %systemroot%\system32\shell32.dll),
   - в поле Текущий значок выберите необходимый значок,
   - кликните ОК для ввода и Применить для подтверждения.
4. На вкладке Консоль из списка Режим консоли выберите пользовательский режим с полным доступом, в котором будет открываться консоль MMC при ее непосредственном запуске,
5. Для установленного в предыдущем пункте режима выполните указанные ниже действия:
   - запретите изменение консоли MMC при ее непосредственном запуске, установив флажок «Не сохранять изменения для этой консоли»,
   - сделайте активным диалоговое окно Вид | Настройка вида консоли MMC при запуске, установив флажок «Позволить пользователю настраивать вид консоли»,
6. Если необходимо удалить файлы, содержащие параметры отображения файлов консоли, на вкладке Очистка диска нажмите кнопку Удалить файлы.

7. Сохраните окончательно сконфигурированную консоль администрирования MMC, выбрав самостоятельно ее имя и путь к месту расположения в меню Консоль | Сохранить как... При сохранении обратите внимание на то, что файлы консоли по умолчанию размещаются в папке «Администрирование», имеющей полный путь %Pathname%\Главное меню\Программы\Admini-стрирование\.
8. Закройте сконфигурированную и сохраненную консоль администрирования MMC, выполнив соответствующие необходимые действия.

В файловом менеджере Проводник ОС Windows выполните следующие инструкции:

- наведите манипулятором мышь на сохраненный файл консоли администрирования MMC и, дважды кликнув на нем, запустите консоль,
- откройте диалоговое окно Вид | Настройка вида и, изменяя положение флажков, обратите внимание на получаемый результат,
- изменив вид консоли MMC приемлемым образом, кликните OK для подтверждения полученного результата,
- в контекстном меню Консоль кликните Выход,
- снова запустите консоль администрирования MMC, кликнув манипулятором мышь на сохраненном файле консоли,
- изучите полученный результат,
- сделайте вывод о проделанной работе и запишите его в отчет.

Задание 2. Добавление различных элементов и компонентов к дереву консоли администрирования MMC

Основным, интегрируемым на консоль компонентом является оснастка. Оснастки существуют двух видов:

- изолированные,
- расширения.

Изолированная оснастка (или просто оснастка) добавляется к дереву консоли MMC без предварительного добавления других элементов, то есть непосредственно в корень дерева консоли.

Оснастка расширения (или просто расширение) всегда добавляется к другой изолированной оснастке или расширению, которые уже имеются в дереве консоли MMC. Если для определенной оснастки разрешены расширения, то, как правило, они работают с объектами, управляемыми непосредственно этой оснасткой, например, с компьютером, принтером, модемом или другим внешним устройством.

В дереве консоли оснастки и расширения располагаются для удобства иерархически или по группам. При добавлении новой оснастки или расширения, они появляются в виде нового элемента в дереве консоли MMC или в виде нового пункта контекстного меню, дополнительной панели инструментов, страницы свойств, а также возможно мастера, организующего определенную последовательность действий, к уже установленной оснастке.

Другими элементами, по необходимости применимыми для интеграции на консоль администрирования MMC, являются виды панели задач и собственно задачи, которые могут включать в себя команды меню для элементов консоли и команды, запускаемые из командной строки. Кроме того, могут быть созданы команды, действующие как часть дерева консоли или открывающие другой компонент.

Прежде всего, перед добавлением указанных элементов к консоли MMC, необходимо определить их число. Если, в частности, требуется добавить несколько видов панели задач, то наряду с этим необходимо определить тип каждой панели (для отображения списка и задач или только задач), а также разделить задачи по интегрированным видам панели. Добавление видов панели задач и собственно задач осуществляется посредством работы мастера создания этих элементов. При этом важно помнить, что консоль MMC должна содержать, по крайней мере, одну оснастку, чтобы возможность интеграции появилась в принципе.

Отдельной возможностью, иногда необходимой при администрировании сетей, является

добавление элементов и компонентов дерева консоли администрирования MMC в виде списка ярлыков в меню «Избранное».

Дополнительные сведения о добавлении различных элементов в дерево консоли администрирования MMC можно получить, воспользовавшись справкой ОС Windows (Пуск | Справка и поддержка) в разделе Общее представление о MMC \ Консоль MMC в авторском режиме \ Оснастки \ Создание консолей.

Содержание задания

Первым необходимым компонентом, добавляемым к дереву консоли администрирования MMC при ее организации и построении, является оснастка. Для добавления оснастки в авторском режиме выполните следующие действия:

1. Создайте новую Консоль управления MMC одним их описанных в пункте I текущего учебного задания способов.
2. В меню Консоль выберите команду Добавить или удалить оснастку.
3. В диалоговом окне Добавить/удалить оснастку нажмите кнопку Добавить вкладки Изолированная оснастка. Список Оснастки в диалоговом окне Добавить/удалить оснастку определяет элемент дерева консоли, к которому выполняется добавление элементов. В этом списке можно найти любой элемент дерева консоли. Обратите внимание на то, что по умолчанию это Корень консоли.
4. В диалоговом окне Добавить изолированную оснастку, выберите оснастки Службы из списка доступных в системе, кликнув на ней манипулятором мышь и нажав кнопку Добавить. Для добавления другой оснастки из списка, повторите указанные действия настоящего пункта повторно.
5. Для некоторых оснасток в процессе их инсталляции выводится диалоговое окно Выбор целевого компьютера, определяющее чем, устанавливаемая оснастка, будет управлять в дальнейшем — локальным или сетевым компьютером. Выберите Локальный компьютер, установив переключатель в соответствующее положение.
6. Нажмите Готово, Закрыть и затем кликните OK для подтверждения ввода.
7. Скройте меню и панель инструментов оснастки Службы, выполнив действия указанные ниже:

- В меню Вид выберите команду Настроить,
- В группе Оснастка снимите флажок Меню,
- В группе Оснастка снимите флажок Панели инструментов.

При устанавливании или снятии флажков, соответствующие им меню и панели инструментов отображаются или скрываются, причем, для всех оснасток консоли, включая текущую. Если переключение флажков не приводит к изменению вида консоли, тогда текущая оснастка не имеет специальных меню или панелей инструментов.

8. Не закрывая консоль администрирования MMC, сохраните ее, выбрав команду Сохранить в меню Консоль.

Для добавления расширений к уже установленной в предыдущем задании оснастке Службы выполните следующее:

9. В меню Консоль выберите команду Добавить или удалить оснастку.
10. В диалоговом окне Добавить/удалить оснастку выберите вкладку Расширение. На этой вкладке можно выбрать любой элемент дерева консоли из списка Оснастки, которые могут быть расширены, и просмотреть Доступные расширения, которые могут быть включены или отключены. После подключения расширение автоматически размещается в дереве консоли под оснасткой, к которой оно относится. Если дерево консоли содержит больше одного экземпляра оснастки, к которой подключено расширение, все остальные экземпляры автоматически получают это расширение.
11. Среди Доступных расширений оснастки Службы удалите флажок с расширения Расширенный вид и отметьте к чему привело это действие. Повторите аналогичные действия с другими расширениями данной оснастки и изучите получаемый результат.

12. Не закрывая консоль администрирования MMC, сохраните ее. В окне консоли администрирования выполните следующие инструкции:

- последовательно перебирая доступные в системе оснастки, найдите те из них, которые обладают дополнительным меню, панелью инструментов или расширениями,
- изучите полученный результат и сделайте вывод о проделанной работе,
- запишите полученную информацию в отчет, заполнив табл. 13.

Таблица 1. Результат поиска оснастки

№ п.п.	**Оснастка**	**Результат поиска и вывод по способу применения дополнительных меню, панелей инструментов и/или расширений оснасток**
1		
n		

Задание 3. Создание нового вида панели задач консоли администрирования MMC

Содержание задания

Для добавления видов панелей задач и собственно задач в авторском режиме выполните следующее:

1. Создайте новую Консоль управления MMC одним их описанных в пункте I текущего учебного задания способов.
2. Добавьте оснастку Службы в корень консоли MMC.
3. В дереве консоли кликните манипулятором мышь на этой оснастке.
4. В меню Действие или кликнув правой кнопкой манипулятора на оснастке, выберите команду Новый вид панели задач.
5. Следуйте инструкциям «Мастера создания вида панели задач», чтобы добавить на консоль новую панель вида.
6. Если сразу после создания вида панели задач необходимо создать задачи, установите флажок «Запустить мастер создания новой задачи» на последнем экране «Мастера создания вида панели задач».
7. Следуйте инструкциям «Мастера создания новой задачи», чтобы добавить
8. на консоль новую задачу к существующей панели вида.
9. В дереве консоли кликните элемент или компонент (в нашем случае это оснастка), связанный с видом панели задач, затем в меню Действие выберите команду Правка вида панели задач.
10. На вкладке Задачи нажмите кнопку Создать.
11. Повторите инструкции пункта 7 настоящего задания.
12. Не закрывая консоль администрирования MMC, сохраните ее.

Измените вид панели задач сохраненной консоли администрирования MMC, выполнив следующие действия:

- введите новое имя,
- введите новое описание,
- установите переключатель Стиль для области сведений в положение, соответствующее новому формату списка,
- удалите соответствующий флажок, чтобы скрыть стандартную вкладку,
- установите переключатель Стиль для описания задачи в положение, соответствующее новому стилю задачи,
- выберите новое значение ширины для вертикального списка или высоты для горизонтального списка,
- нажмите кнопку Параметры и установите переключатель в одно из необходимых положений,

- нажмите OK для подтверждения ввода,
- изучите полученный результат,
- сделайте вывод о проделанной работе и запишите его в отчет.

Задание 4. Добавление элементов и компонентов дерева консоли в виде списка ярлыков в меню «Избранное»

Содержание задания

Для добавления элемента или компонента в авторском режиме выполните следующее:

1. Создайте новую Консоль управления MMC одним их описанных в пункте I текущего учебного задания способов.
2. В дереве консоли кликните элемент или компонент (в нашем случае это оснастка), который нужно добавить в список «Избранное».
3. В области сведений выберите вкладку вида панели задач, которую нужно добавить, в случае, если для элемента или компонента, указанного в дереве консоли, настроен вид панели задач. В противном случае в области сведений вкладки не видны.
4. Выберите в меню Избранное команду Добавить в избранное.
5. В поле Создать в диалогового окна Добавление в папку «Избранное» выполните указанные ниже действия:

- создайте новую папку с названием, выбранным самостоятельно, кликнув папку, которая будет выступать в качестве родительской для создаваемой папки и нажав кнопку Создать папку,
- нажмите кнопку OK для ввода,
- в поле Имя папки введите имя, под которым будет добавлен элемент,
- кликните OK для подтверждения ввода.

6. Не закрывая консоль администрирования MMC, сохраните ее. Упорядочите «Избранное» сохраненной консоли администрирования MMC, выполнив следующие действия:

- добавьте новую папку, введя ее имя в соответствующее поле и кликнув OK для подтверждения ввода,
- переместите элемент, созданный в пункте 5 настоящего задания, в новую, только что созданную, папку и кликните OK для ввода,
- переименуйте выбранный элемент и нажмите клавишу Enter для подтверждения ввода,
- удалите все элементы, расположенные ниже папки «Избранное»,
- нажмите Закрыть для завершения задания,
- изучите полученный результат,
- сделайте вывод о проделанной работе и запишите его в отчет.

Задание 5. Основные возможности оснастки «Редактор объекта групповой политики»

Административное средство Active Directory предназначено для решения повседневных задач сетевого управления, в число которых входят: создание, удаление, изменение, перемещение и предоставление разрешений на объекты каталога. Объектами управления могут являться подразделения, пользователи, контакты, группы, компьютеры, принтеры, а также объекты общих файлов.

Active Directory обеспечивает системного администратора иерархическим представлением сети и едиными возможностями управления всеми сетевыми объектами ОС Windows 2000 Server, где она является основой групповой политики. Для реализации указанных возможностей в ОС Windows 2000 Server имеются три оснастки «Пользователи и компьютеры Active Directory», «Домены и доверие Active Directory» и «Сайты и службы Active Directory», первые две из которых предназначены для создания объектов групповой политики домена или подразделения, третья — соответственно, для создания объекта групповой политики сайта. Для запуска этих оснасток из ОС Windows необходимо осуществить подключение к удаленному столу сервера с установленными средствами

администрирования ОС Windows 2000 Server, поскольку служба каталогов Active Directory в ОС Windows является по умолчанию не доступной.

Понятие групповая политика в области администрирования применяется не только к пользователям и компьютерам, но и к серверам, контроллерам доменов и другим компьютерам под управлением ОС Windows. По умолчанию групповая политика применяется к домену и влияет на все его компьютеры и пользователи. Обеспечение групповой политики подразумевает конфигурирование системы и задания набора условий и параметров групповой политики, приводящих к определенным ограничениям или разрешениям в ОС.

Параметры групповой политики определяют различные компоненты конфигурации пользователя, в частности, окружения пользовательского рабочего стола (программы, доступные пользователям, программы, отображающиеся на рабочем столе, и параметры меню Пуск) и конфигурации компьютера, включая параметры, применяемые вне зависимости от того, кто работает на этих компьютерах. Чтобы создать частную конфигурацию компьютера для определенной группы пользователей используется оснастка «Редактор объекта групповой политики». Набор указанных параметров групповой политики содержится в объекте групповой политики, который, в свою очередь, связан с выбранными объектами Active Directory — сайтами, доменами или подразделениями. Объектами групповой политики являются документы, создаваемые оснасткой. Они хранятся на уровне домена и оказывают влияние на пользователей и компьютеры доменов и подразделений. Кроме того, каждый компьютер с ОС Windows имеет единственную, хранящуюся локально, группу параметров, которая называется локальным объектом групповой политики. Все многообразие параметров групповой политики содержится в соответствующих расширениях оснастки «Групповая политика», посредством которых системному администратору предоставляются широкие возможности по управлению процессами и ресурсами ОС Windows:

- на основе реестра, используя расширение Административные шаблоны (A). При этом создается файл, содержащий параметры реестра, записанные в область базы данных реестра пользователя, в разделе HKEY_CURRENT_USER и в разделе HKEY_LOCAL_MACHINE для локального компьютера.
- посредством расширения Назначение сценариев (B). Групповая политика указывает сценарии входа/выхода пользователей из системы и загрузки/завершения работы.
- используя Редактор перенаправления папок (C). Групповая политика имеет возможность перенаправить системные папки «Мои документы» и «Мои рисунки», из папки «Documents and Settings» локального компьютера в новое место расположения в сети.
- на основе расширения Установка программ (D), которое позволяет назначать, публиковать и восстанавливать приложения.
- посредством расширения Параметры безопасности (E), позволяющей устанавливать ограничения на использование программ, политику отрытого ключа, а также осуществлять управление политикой безопасности IP.

Административные шаблоны это текстовые файлы с расширением .adm, содержащие сведения о политике для элементов, расположенных в папке «Административные шаблоны» оснастки. В ОС Windows доступно четыре файла административных шаблонов, приведенных в табл. 14.

Файлы административные шаблонов состоят из иерархии категорий и подкатегорий, которые вместе определяют отображение параметров групповой политики. В них содержатся следующие сведения:

- размещение параметров реестра, соответствующих каждому параметру административного шаблона групповой политики,
- величина параметров или ограничений, связанных с каждым параметром административного шаблона,

- значение по умолчанию для большинства параметров,
- объяснение функции каждого параметра,
- версии ОС Windows, поддерживающие каждый параметр.

Таблица 2. Административные шаблоны ОС Windows

Шаблон (.adm)	**Справка по параметрам**	**Описание**
System	%systemroot%\help\system.chm	В групповой политике шаблон установлен по умолчанию для клиентов ОС Windows 2000 и XP
Inetres	%systemroot%\ help\inetres.chm	В групповой политике шаблон Internet Explorer установлен по умолчанию для клиентов ОС Windows 2000 и XP
Wmplayer	%systemroot%\help\wmplay.chm	Параметры WMP для клиентов ОС Windows 2000 и XP
Conf	%systemroot%\help\conf1.chm	Параметры программы NetMeeting для клиентов ОС Windows 2000 и XP

В среде ОС Windows имеется возможность использования сценариев посредством двух серверов Wscript.exe или Cscript.exe, поддерживающих как Visual Basic Scripting Edition (расширение .vbs), так и JScript (расширение .js) файлы. В частности, в средствах оснастки «Групповая политика» имеется два расширения, расположенные в узлах консоли «Конфигурация компьютера | Конфигурация Windows» или «Конфигурация пользователя | Конфигурация Windows», позволяющие развертывать сценарии с использованием указанных серверов ОС Windows. Эти расширения следующие:

- сценарии (запуск/завершение) — расширение, посредством которого можно указать локально выполняемый сценарий при запуске и завершении работы компьютера.
- сценарии (вход/выход из системы) — расширение, посредством которого можно указать выполняемый сценарий при входе и выходе пользователя из системы. Эти сценарии запускаются с правами пользователя, а не администратора.

Перенаправление папки используется для перемещения некоторых специальных папок, например «Мои документы» и «Мои рисунки», в заданное место в сети, для их последующего доступа с разных узлов. В ОС Windows возможны следующие специальные папки для перенаправления (табл. 15).

Таблица 3. Специальные папки ОС Windows

Специальная папка	**Примечания**
Application Data	Параметры групповой политики управляют поведением папки «Application Data» при включении кэширования на стороне клиента. Параметры расположены в дереве консоли «Групповая политика» в Административных шаблонах\Сеть\Автономные файлы.
Рабочий стол	Папка может быть перенаправлена независимо от всех остальных специальных папок.
Мои документы	Особенности и преимущества перенаправления этой папки описаны ниже.
Мои документы\ Мои рисунки	Эта папка может быть перенаправлена независимо от предыдущей папки «Мои документы» или совместно с ней, как это происходит по умолчанию. Именно эта комбинация является рекомендуемой.
Главное меню	При перенаправлении папки «Главное меню» ее подпапки всегда перенаправляются вместе с ней.

Некоторые из преимуществ, описанных ниже, относятся к перенаправлению любой специальной папки, однако перенаправление папки «Мои документы» может быть особенно удобным, поскольку со временем размер этой папки может увеличиваться.

- При использовании перемещаемого профиля пользователя его частью является только сетевой путь к папке «Мои документы», но не сама папка. Поэтому ее содержимое не нужно копировать и перемещать между клиентом и сервером каждый раз при входе пользователя в систему или его выходе, что делает процессы входа и выхода сравнительно быстрее.
- Даже если пользователь входит в сеть с различных компьютеров, все его документы всегда доступны.
- Технология автономных файлов обеспечивает пользователям доступ к папке «Мои документы» даже при отсутствии подключения к сети. Это особенно полезно для пользователей, использующих мобильные компьютеры.
- Имеется возможность архивировать данные, хранящиеся на сервере, при управлении перемещаемыми профилями. Это является более безопасным, поскольку не требуется вмешательство пользователя.
- Системный администратор может устанавливать дисковые квоты с помощью групповой политики, ограничивая дисковое пространство, выделенное пользователю для специальных папок.
- Данные пользователя могут быть перенаправлены на жесткий диск локального компьютера с другого жесткого диска, на котором хранятся системные файлы ОС. Это может обезопасить пользовательские файлы, если необходимо будет ее переустанавливать.

Кроме всего прочего, в ОС Windows имеется возможность предоставления исключительных прав на специальные папки. Если на вкладке Параметры диалогового окна свойств каждой папки установить флажок Предоставить права монопольного доступа к папке «Мои документы», пользователь и локальная система получают полный контроль над папкой, и никто другой, включая администратора, не будет иметь на нее никаких прав. В противном случае, если этот параметр отключен, то разрешения для папки не изменяются, а используются, применяемые по умолчанию разрешения. Еще одна возможность заключается в том, что на специальные папки могут быть расширены дополнительные разрешения, полный список которых доступен в справке ОС Windows.

Установка программного обеспечения является неотъемлемой процедурой при работе с любой ОС. Для этого используется одноименная оснастка «Установка программного обеспечения», которая помогает определить способ установки и сопровождения приложений. Также с ее помощью можно управлять приложением внутри объекта групповой политики посредством службы каталогов Active Directory.

Приложения управляются в одном из двух режимов: назначения или публикации. Приложение назначается, когда необходимо, чтобы оно было установлено на всех узлах сети. Например, требуется, чтобы на всех компьютерах аудитории было установлено одно и тоже приложение. Поскольку объект групповой политики управляет всеми пользователями аудитории, при назначении приложения в объекте групповой политики, оно одновременно объявляется на всех компьютерах, но при этом фактически не устанавливается. Устанавливаются лишь только необходимые данные для создания ярлыка этого приложения в меню Пуск, а в реестре осуществляется связывание расширения его документа с ним самим. При первом выборе приложения на загрузку, а также, если пользователь, не запускавший приложение ранее, выбирает его документ для работы, приложение устанавливается автоматически с одновременным открытием этого документа.

Назначенное в системе приложение можно удалить, но оно будет объявлено снова при следующем входе. Если выбрать его в меню Пуск, оно будет повторно автоматически установлено.

Приложение публикуется, если необходимо сделать его доступным для тех пользователей,

управляемых объектом групповой политики, кто хочет установить это приложение. При этом у пользователей имеется выбор самостоятельно решать, устанавливать приложение или нет. Например, если приложение публикуется для пользователей, желающих его установить, им следует для этого открыть компонент «Установка и удаление программ» на панели управления и произвести установку. В случае если пользователям не удалось установить приложение с помощью этого компонента, но файлы с соответствующим расширением связаны с приложением, оно будет установлено при первой попытке открыть файл с этим расширением.

Безопасность компьютера, уязвимость системы безопасности, а также различного вида угрозы заботят не только профессионалов в области информационных технологий, но и рядовых пользователей компьютеров. Многие организации и отдельные пользователи имеют постоянные подключения к Интернету, что подвергает их компьютеры рискам заражения вирусами, несанкционированного проникновения, атак на службы и другим угрозам.

Существуют некоторые правила, называемые политиками или параметрами безопасности, которые предназначены для обеспечения защиты ресурсов одного или нескольких компьютеров в сети. Параметры безопасности позволяют контролировать:

- проверку подлинности пользователей при входе в сеть или отдельный узел,
- ресурсы, которые пользователи могут использовать,
- включение и отключение записи действий пользователя или группы в журнале событий,
- принадлежность к группам.

Настраиваются параметры безопасности, используя средства диспетчера настройки безопасности. К этим средствам относятся:

- шаблоны безопасности,
- анализ и настройка безопасности,
- программа командной строки Secedit.exe,
- локальная политика безопасности,
- расширение «Параметры безопасности» для групповой политики.

Расширение «Параметры безопасности» позволяет пользователям изменять настройку безопасности в оснастке «Групповая политика», влияющей, в свою очередь, одновременно на все узлы сети посредством объекта групповой политики. Однако чтобы установить или изменить отдельные параметры безопасности на отдельных компьютерах, используется средство «Локальная политика безопасности», включающее политику аудита, назначение прав пользователя и локальные параметры безопасности.

Чтобы применить несколько параметров безопасности единовременно, имеется возможность определить их с помощью шаблонов безопасности и затем применить к системе с помощью средства «Анализ и настройка безопасности» или программы Secedit.exe (Пуск | Выполнить | Secedit.exe), а также импортировать готовый шаблон в соответствующую локальную или групповую политику.

В заключение следует отметить, что в пакете обновления SP2 для ОС Windows с целью повышения безопасности вводятся некоторые изменения параметров безопасности. Обобщая нововведения, параметры безопасности сгруппированы по соответствующим областям (табл. 16).

Таблица 4. Области безопасности ОС Windows

Область безопасности	**Описание**
Политики учетных записей	Политика паролей, политика блокировки учетной записи и политика Kerberos
Локальные политики	Политика аудита, назначение прав пользователя и параметры безопасности
Журнал событий	Параметры журналов событий приложений, системных событий и событий безопасности

Группы с ограниченным доступом	Состав групп с особыми требованиями к безопасности
Системные службы	Параметры запуска и разрешения для системных служб
Реестр	Разрешения для разделов реестра
Файловая система	Разрешения для файлов и папок

Содержание задания

Прежде чем непосредственно перейти к ознакомлению с возможностями изучаемой оснастки, следует обратить внимание на имеющиеся в системе способы ее открытия в изолированном виде. Имеется возможность открыть оснастку через меню Пуск | Выполнить. Для этого необходимо ввести gpedit.msc и нажать Enter для ввода. Кроме того, загрузка оснастки возможна в среде командной оболочки, различные варианты которой отображены ниже (табл. 17). Поэкспериментируйте с имеющимися возможностями загрузки изолированной оснастки «Групповая политика».

Таблица 5. Варианты загрузки групповой политики посредством командной оболочки

№ п.п.	**Пример команды**	**Описание**
1	gpedit.msc /gpcomputer:"Имя_компьютера"	редактирование групповой политики локального компьютера.
2	gpedit.msc /gpcomputer:"Имя_компьютера.WingTip Toys.com"	редактирование локального объекта групповой политики на локальном компьютере, имя которого задается в формате DNS.
3	gpedit.msc /gpobject:"LDAP://CN={31B2F340016D-11D2-945F00C04FB984F9},CN=Policies,CN=System,DC=WingTipToys,DC=com" в фигурных скобках {16-байтное число} — глобальный уникальный идентификатор GUID	редактирование объекта групповой политики с применением Active Directory.

1. Загрузите пользовательскую консоль администрирования, созданную в задании 39, с возможностью ее редактирования.
2. Добавьте оснастку «Редактор объекта групповой политики» в корень консоли администрирования, выбрав в поле Объекта групповой политики значение Локальный компьютер.
3. Откройте поочередно все ветви дерева консоли в узле Политика «Локальный компьютер» и изучите где и какие параметры групповой политики располагаются. Обратите внимание на то, что некоторые параметры находятся в состоянии Включено, другие, напротив — Отключено или Не определено (Не задано).
4. В левой части окна консоли выберите «Политика Локальный компьютер | Конфигурация компьютера | Конфигурация Windows | Параметры безопасности | Локальные политики | Назначение прав пользователей / Параметры безопасности».
5. Изучите локальные политики Назначение прав пользователя и Параметры безопасности.
6. Сохраните и закройте консоль администрирования MMC.

При выполнении пункта 6 используйте следующие инструкции:

- последовательно перебирая каждую из локальных политик, изучите ее содержимое, принадлежность к пользователю, а также состояние, в котором она находится,
- запишите полученную информацию в отчет, заполнив табл. 18.
- сделайте вывод о проделанной работе и запишите его в отчет.

Таблица 6. Локальная политика безопасности ОС Windows

№	Политика		Привилегией обладает	Состояние
п.п.	Название	описание		
1	**Изменение системного времени**	**Определяет, какие пользователи и группы могут изменять время и дату компьютера.**	**Администратор Опытный пользователь**	**Включено**
n				

Задание 6 . Возможности оснастки «Групповая политика» при настройке локального узла

Как утверждалось ранее, с помощью параметров узла Конфигурация компьютера устанавливаются политики, которые применяются к компьютеру независимо от того, кто его использует для входа в сеть, в то время как, с помощью параметра Конфигурация пользователя устанавливаются политики, которые применяются к каждому пользователю, работающему на компьютере.

Таким образом, существует ряд параметров групповой политики предназначенных исключительно для изменений, направленных на создание специальных настроек среды пользователя ОС Windows, в частности, для придания системе уникального вида. В качестве примера, с помощью групповой политики можно удалить значки с рабочего стола, изменить содержимое меню Пуск и упростить структуру панели управления.

Содержание задания

1. Загрузите пользовательскую консоль администрирования, созданную ранее, с возможностью ее редактирования.
2. В левой части окна консоли выберите «Политика Локальный компьютер | Конфигурация пользователя | Административные шаблоны | Панель задач и меню «Пуск» / Панель управления / Рабочий стол».
3. Изучите параметры политик | Административные шаблоны | Панель задач и меню «Пуск» / Панель управления / Рабочий стол.
4. Выберите любые пять параметров в каждой из политик Панель задач и меню «Пуск» / Панель управления / Рабочий стол. Измените выбранные параметры на противоположные, перезагрузите компьютер и отметьте полученные визуальные изменения графического интерфейса.
5. Сохраните и закройте консоль администрирования ММС.

При выполнении пункта 3 используйте следующие инструкции:

- самостоятельно последовательно выбирая политики указанных административных шаблонов, в общем количестве не менее десяти, измените их состояние, делая его активным,
- исследуйте влияние смены состояния на внешний вид соответствующего элемента графического интерфейса ОС Windows,
- запишите полученную информацию в отчет, заполнив табл. 19.
- сделайте вывод о проделанной работе и запишите его в отчет.
- продемонстрируйте преподавателю конечный результат изменения параметров административных шаблонов, применяемых для настройки уникального вида элементов графического интерфейса.

Таблица 7. Настройка некоторых административных шаблонов

№	Административный шаблон		Результат при активации политики
п.п.	Название шаблона	Описание политики	

1	Рабочий стол	Не показывать значок Internet Explorer (IE)	При изменении состояния политики в положение Включено значок IE убирается с рабочего стола и панели быстрого запуска
n			