

Программное обеспечение

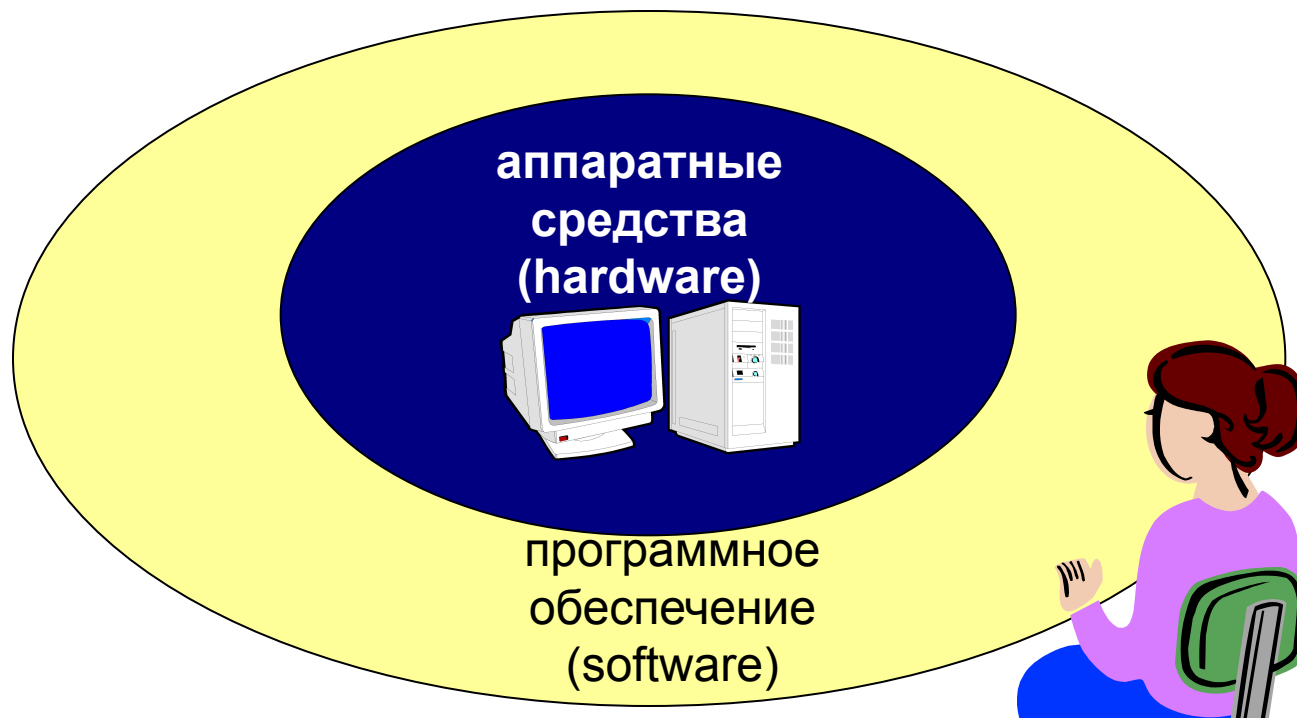
1. Введение
2. Прикладные программы
3. Системные программы
4. Сжатие файлов. Архиваторы
5. Компьютерные вирусы и антивирусы

Программное обеспечение

Тема 1. Введение

Программное обеспечение

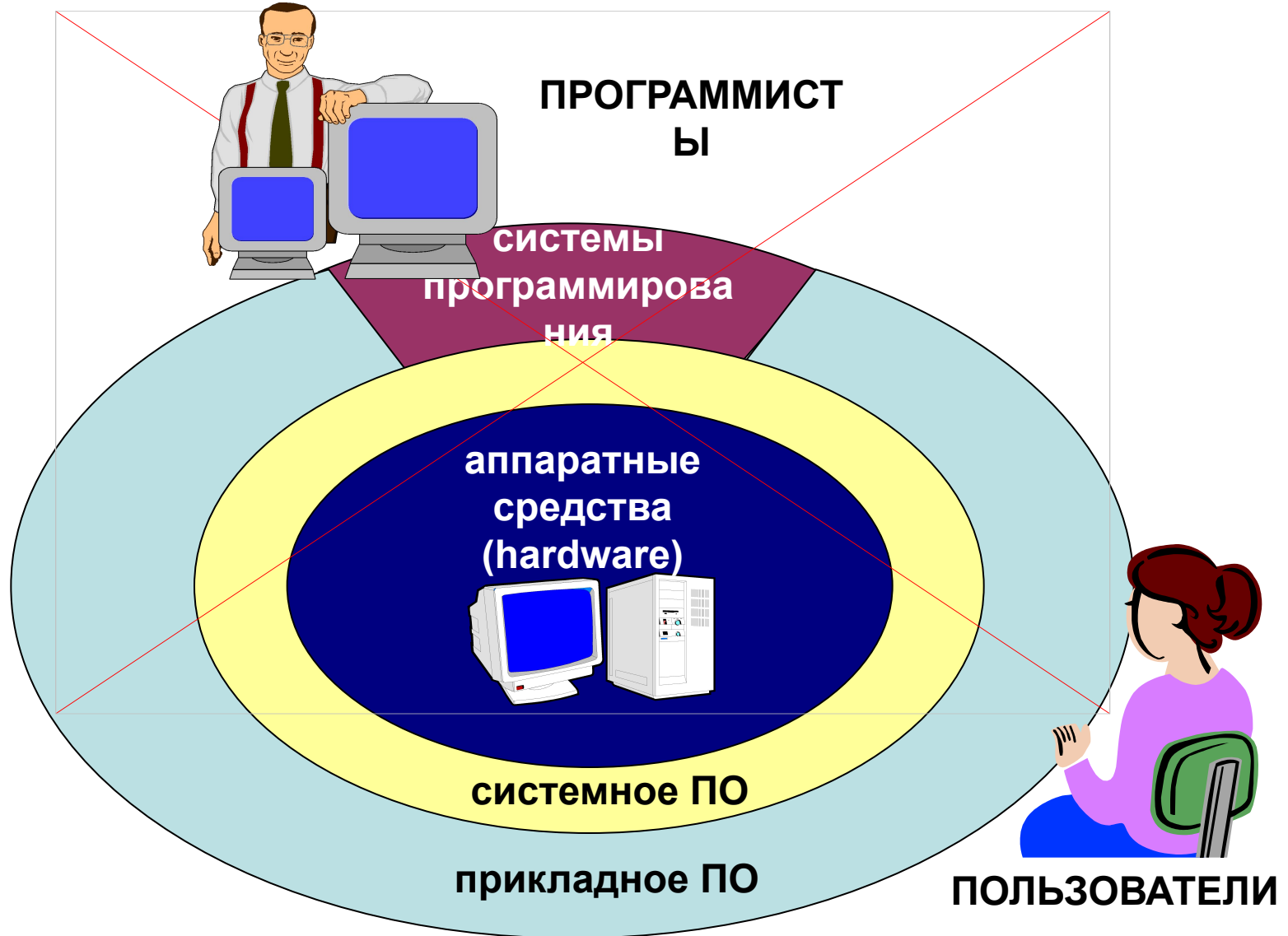
Взаимодействие человека с компьютером



Программное обеспечение

- **Прикладное ПО** – программы, которые пользователь использует для решения своих задач
 - текстовые редакторы
 - графические редакторы
 - базы данных ...
- **Системное ПО** – обеспечивает взаимодействие пользователя и прикладных программ с аппаратными средствами
 - операционные системы
 - драйверы
 - утилиты
- **Системы программирования** – средства создания новых программ.
- **Программы пользователей** – пользователи составляют их для своих собственных нужд.

Программное обеспечение



Вычислительная система (ВС)

Объект, способный осуществлять

- **хранение,**
- **обработку и**
- **передачу данных.**

В простейшем случае это компьютер. Структура ВС может быть проиллюстрирована следующим рисунком.

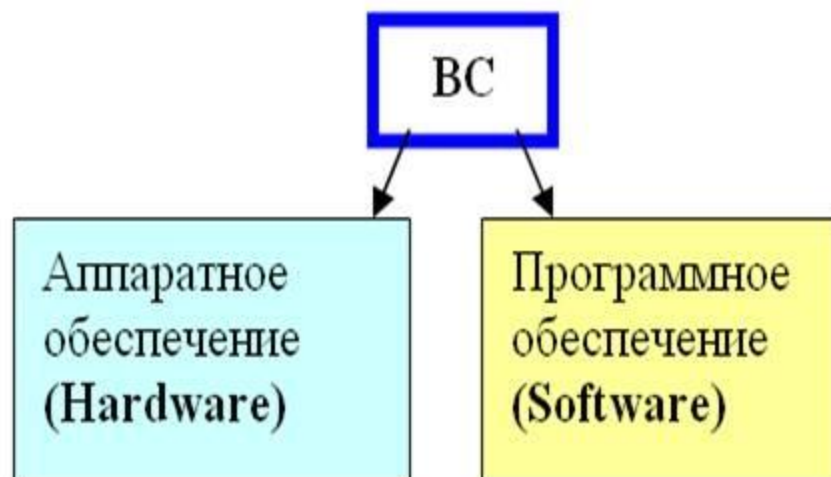


Рисунок 1 Вычислительная система - ВС

Программное обеспечение (ПО)

- **Структура ПО** может быть проиллюстрирована следующей схемой

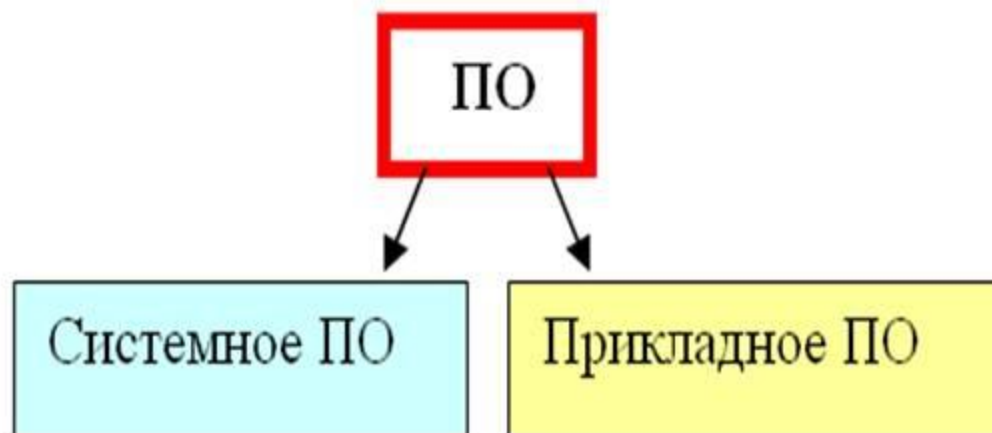


Рисунок 2 Структура ПО

Прикладное ПО взаимодействует с аппаратными компонентами ВС через системное ПО.

■ Системное ПО

обеспечивает и контролирует доступ к аппаратному обеспечению ВС

(например:
к персональному компьютеру

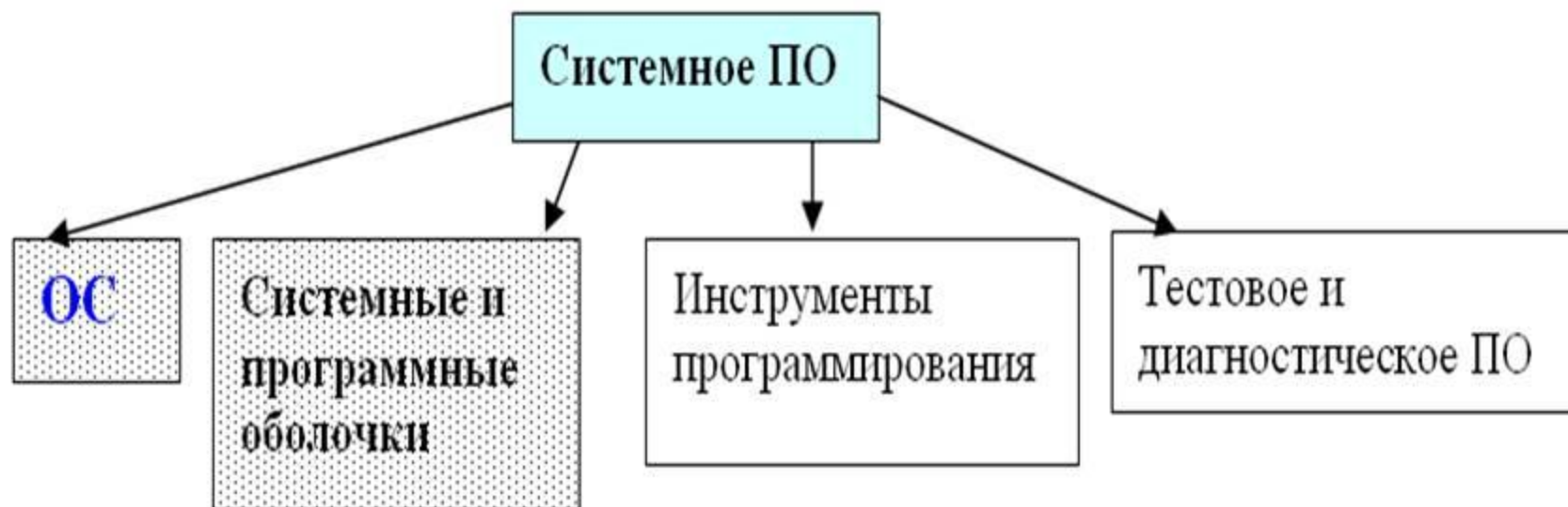
■ Прикладное ПО

призвано обеспечить решение конкретных прикладных задач.

- Компоненты прикладного ПО называются **приложениями.**



Структура системного ПО



Структура системного ПО представлена на этом рисунке

Операционные системы

Операционная система (ОС)

- определение

ОС – это организованная совокупность программ (систем), которая действует как интерфейс между аппаратурой ВС и «Пользователями».



ОС управляет распределением ресурсов ВС для обеспечения эффективной работы.

ОС обеспечивает «пользователей» набором базовых средств для облегчения проектирования, написания, отладки и сопровождения программ.

Следовательно:

Основными задачами для любой **ОС** являются:

- **Управление ресурсами** ВС (*т.е. повышение эффективности использования ВС путем рационального управления её ресурсами в соответствии с некоторыми критериями*).
- **Организация интерфейса** (*т. е. предоставление пользователю соответствующего набора услуг*).



Подсистема ОС – “Управление ресурсами.”

Основные функции:

- **Управление процессами (программами) .**
- **Управление памятью.**
- **Управление I/O (ввода - вывода) устройствами.**
- **Управление файлами (файловая система).**

- ✓ **Программы и данные** рассматриваются как **файлы.**
- ✓ **Ресурсы** распределяются между **процессами.**
- ✓ **Процесс (задача)** – представляет собой базовое понятие современных ОС и часто кратко определяется как - *программа в стадии выполнения*

Разрядность

- 16-разрядные (практически не используются)
- 32-разрядные (самые популярные)
- 64-разрядные (набирают популярность)
- 128-разрядные (в настоящее время реализуется микрокодом на 64-разрядной аппаратуре)

Поддержка многозадачности

- однозадачные
- многозадачные
- системы реального времени

Многопроцессорность

- однопроцессорные
- многопроцессорные

Предназначение

- Для настольных ПК
- Для серверов
- Для мобильных устройств
- Для промышленных устройств, банкоматов, ПЛК и т. д.

Семейство

- ◎ Семейство DOS
- ◎ Семейство Microsoft Windows
- ◎ UNIX-подобные (стандарт POSIX)
 - Семейство Apple OS X
 - Семейство GNU/Linux
 - Семейство Solaris
 - Семейство BSD
- ◎ Альтернативные

Microsoft DOS

```
IDE/ATAPI CD-ROM Device Driver  Version 2.14   10:48:22 02/17/98  
CD-ROM drive #0 found on 1F0h port slave device, v1.04
```

```
Killer v1.0 Copyright 1995 Vincent Penquerc'h. All Rights Reserved.  
Killer installed in memory.
```

```
DOSKEY installed.
```

```
DOSLFN 0.320: high loaded consuming 11840 bytes.
```

```
MSCDEX Version 2.25
```

```
Copyright (C) Microsoft Corp. 1986-1995. All rights reserved.
```

```
Drive D: = Driver IDE-CD unit 0
```

```
SHARE v7.10 (Revision 4.11.1492)
```

```
Copyright (c) 1989-2003 Datalight, Inc.
```

```
installed.
```

```
CuteMouse v1.9.1 [DOS]
```

```
Installed at PS/2 port
```

```
Locking volumes...
```

```
Now you are in MS-DOS 7.10 prompt. Type 'HELP' for help.
```

```
C:\>_
```

Файловые менеджеры: NC, VC и другие

The screenshot shows a multi-pane file manager window with the title bar "D:\PROGRA~1\VC\VC.COM". The window is divided into two main sections, each containing a list of files and folders.

Left Pane: C:\WINDOWS

Name	Name
..	INF
APPATCH	INSTAL~1
ASSEMBLY	L2SCHE~1
BOOT	LIVEKE~1
BRANDING	LOGS
CURSORS	MEDIA
DD1865~1	MICROS~1
DEBUG	MODEML~1
DIGITA~1	MSAGENT
DOWNLO~1	NAP
DOWNLO~2	NUTMPI~1
EN-US	OFFLIN~1
FONTS	PANTHER
FTPCACHE	PCHEALTH
GLOBAL~1	PIF
HELP	PLA
ICO	POLICY~1
IME	PREFETCH

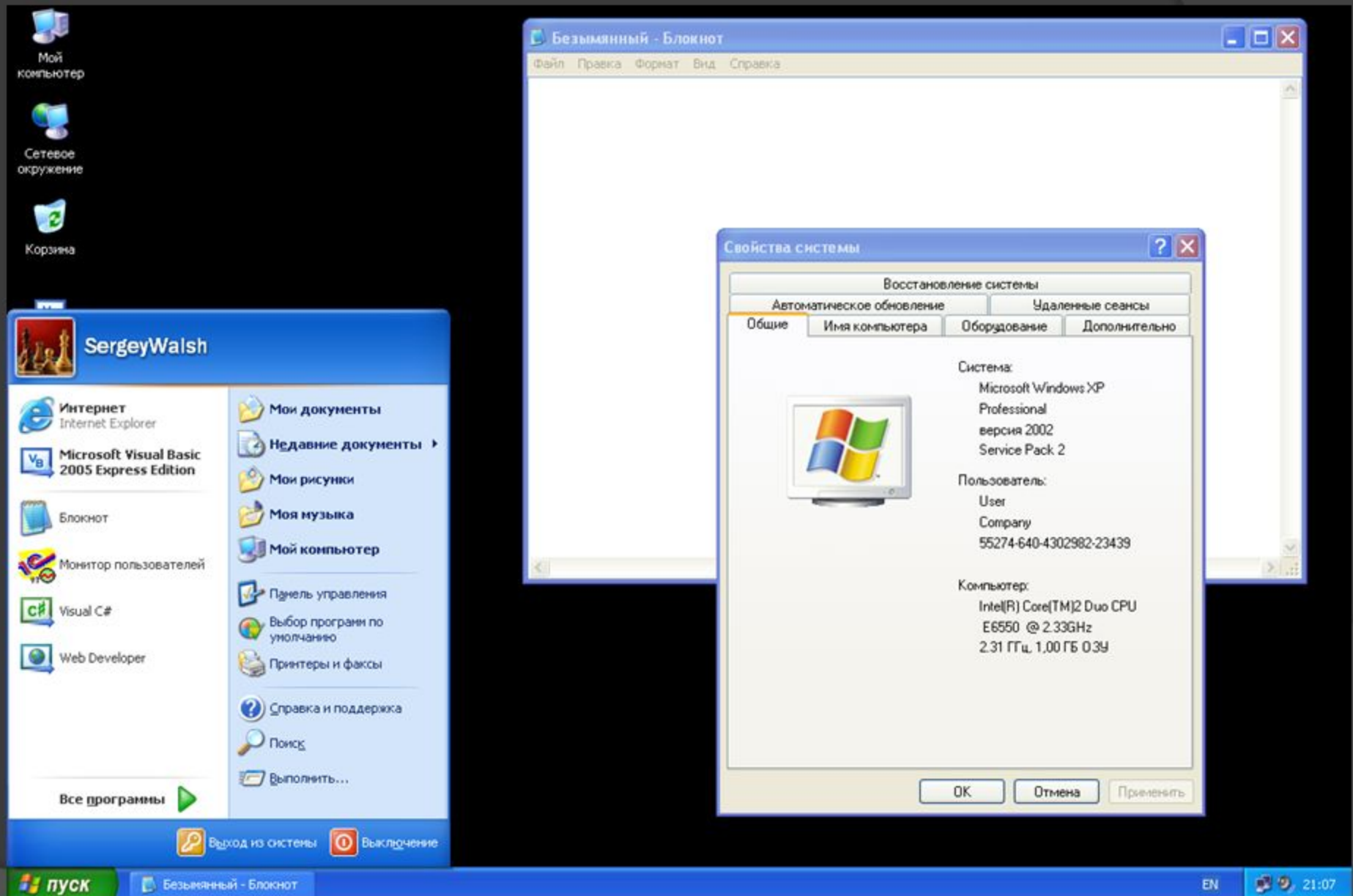
Right Pane: D:\PROGRAMS\FAR

Name	Name	Name
..	farrus	hlf
ADDONS	farrus	lng
DOCUME~1	file_id	diz
ENCYCL~1	restor~1	cmd
FEXCEPT	save~1	cmd
PLUGINS		
PLUGIN~1		
change~1		
clearp~1	cmd	
far	exe	
far	map	
farcze	lng	
fareng	hlf	
fareng	lng	
farger	lng	
farhun	hlf	
farhun	lng	
farpol	lng	

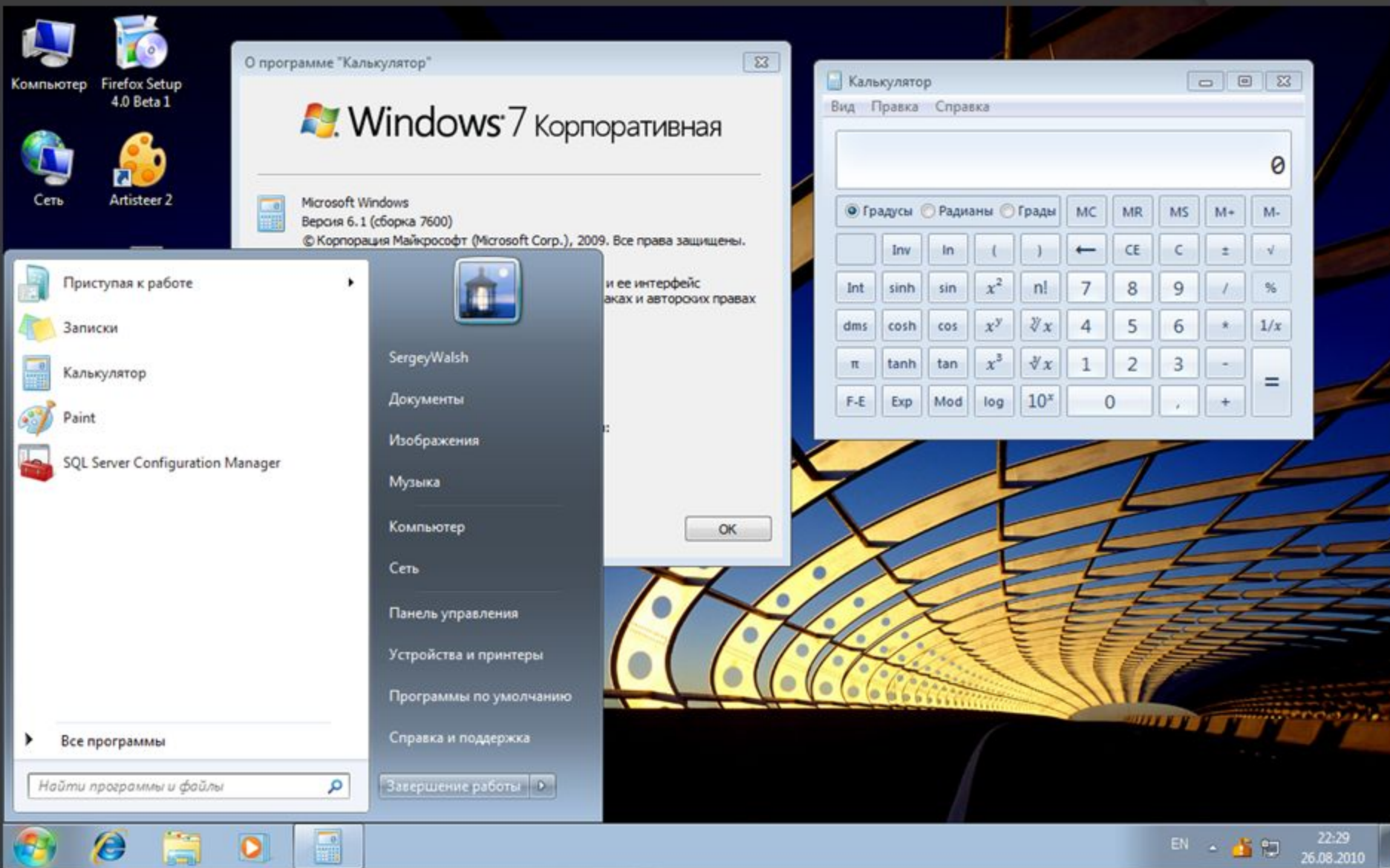
At the bottom of the window, there is a command line showing the current directory: "D:\Programms\far>". Below the command line is a menu bar with the following items: 1Left, 2Right, 3View.., 4Edit.., 5Memory, 6DirSiz, 7Find, 8History, 9EGA, Ln, 10Tree.

Microsoft[®]

Microsoft Windows XP Professional (x86)



Microsoft Windows 7 Enterprise (x86)



Microsoft Windows Server 2008 R2 DataCenter (x64)

Диспетчер сервера

Файл Действие Вид Справка

Диспетчер сервера (TFS2010)

- Роли
- Компоненты
- Диагностика
- Конфигурация
- Хранилище

Роли

Просмотр сведений о работоспособности ролей, установленных на сервере, добавление или удаление ролей и компонентов.

Сводка по ролям [Сводная справка по ролям](#)

Роли: 1 из 17 установлен

[Веб-сервер \(IIS\)](#)

[Добавить роли](#)

[Удалить роли](#)

Веб-сервер (IIS) [Справка Веб-сервер \(IIS\)](#)

Предоставляет надежную, управляемую и масштабируемую инфраструктуру для веб-приложений.

Состояние роли [Перейти к Веб-сервер \(IIS\)](#)

Сообщения: Нет
Системные службы: Выполняется 4, Остановлено 2
События: Нет за последние 24 час.
Анализатор соответствия рекомендациям: Чтобы выполнить сканирование при помощи анализатора соответствия рекомендациям, перейдите на вкладку анализатора на домашней странице этой роли и выберите "Проверить эту роль"

Службы ролей: Установлено 38 [Добавить службы ролей](#)
[Удалить службы ролей](#)

Служба ролей	Состояние
Веб-сервер	Установлено
Основные возможности HTTP	Установлено
Статическое содержимое	Установлено
Стандартный документ	Установлено
Обзор каталогов	Установлено
Ошибки HTTP	Установлено
Перенаправление HTTP	Установлено
Веб-публикация DAV	Не установлено
Разработка приложений	Установлено
ASP.NET	Установлено
Расширяемость .NET	Установлено

Последнее обновление: Сегодня в 22:43 [Настроить обновление](#)

Пуск

EN 22:46 26.08.2010



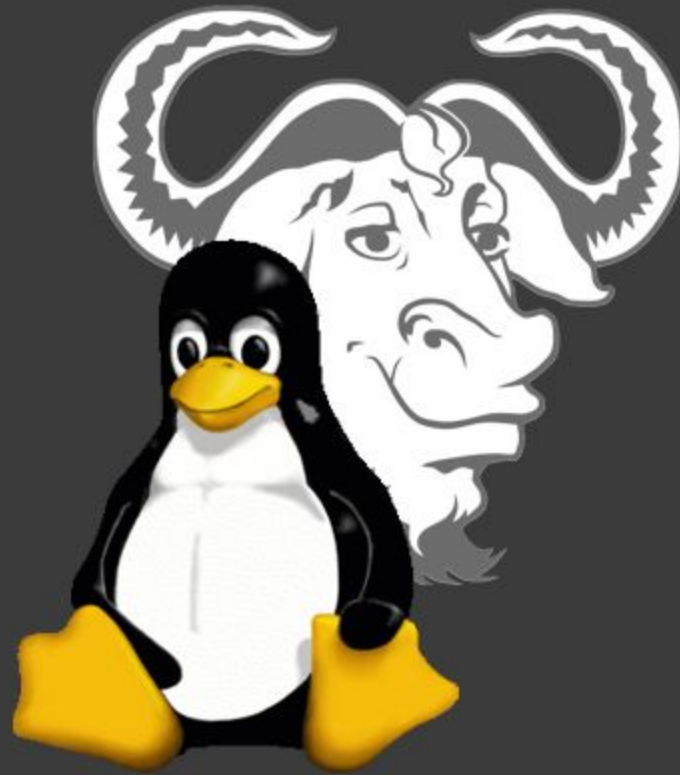
Apple Inc.

Mac OS X Leopard 10.5.3



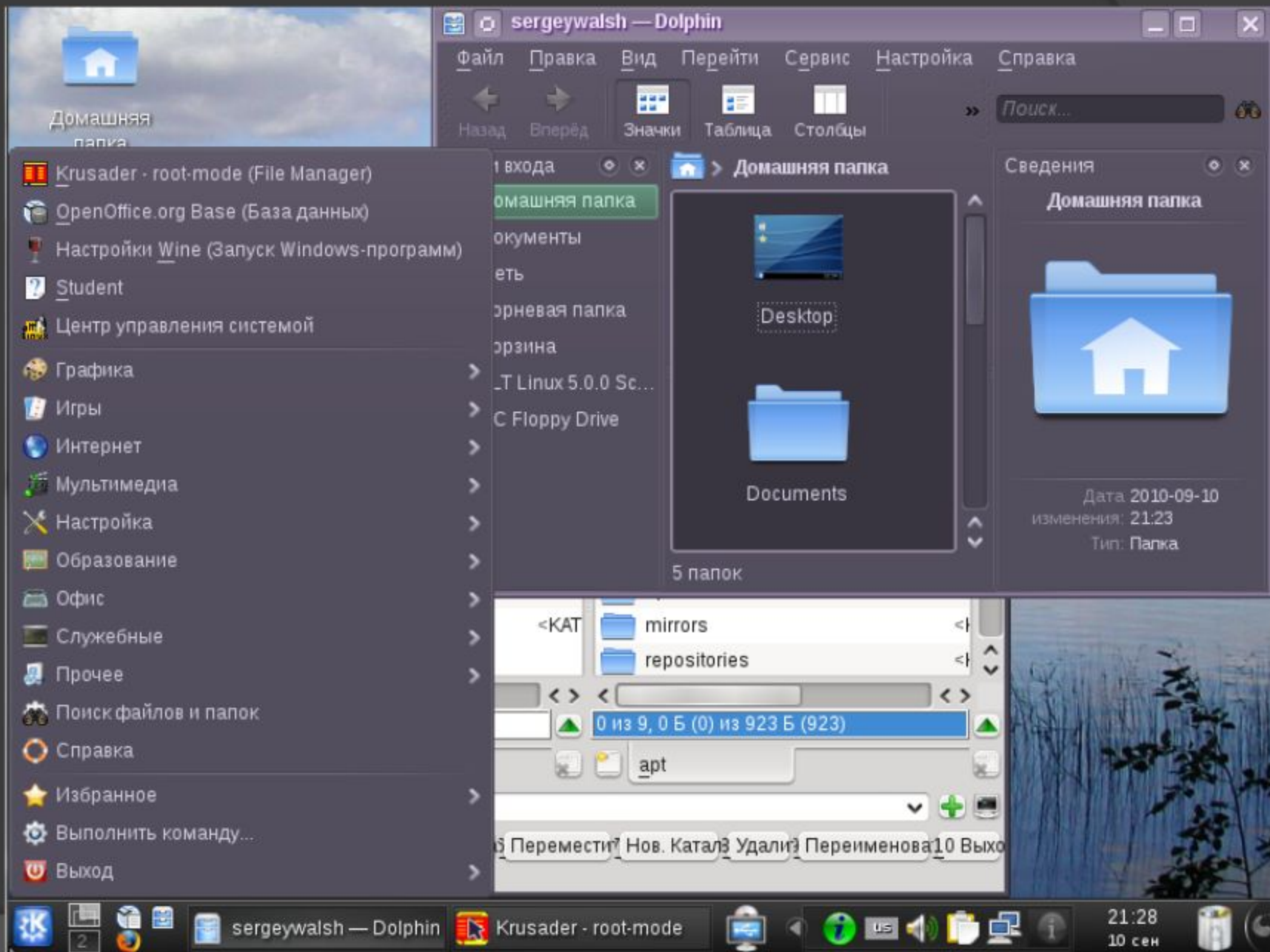
Mac OS X Leopard — Док с отражением



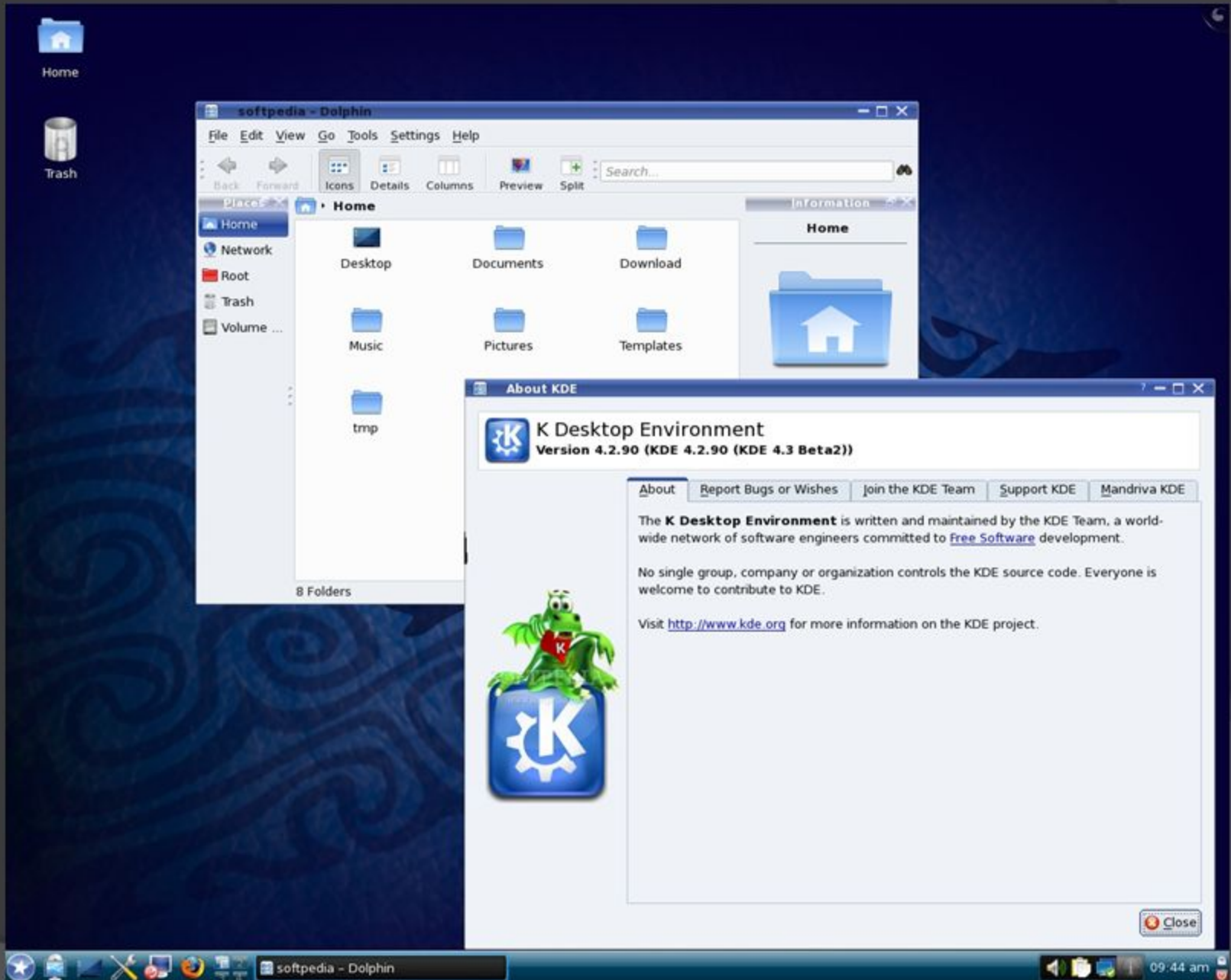


GNU / Linux

Linux [ALT Linux Master 5.0 (KDE, т.н. Школьный Линукс)]



Linux [Mandriva 2010]



Linux [Open SUSE 11.2 (KDE)]

Рабочий стол

Firefox openSUSE Мой компьютер Онлайн-помощь Офис

Сеть

eth0

24 KiB/s
18 KiB/s
12 KiB/s
6 KiB/s
0 KiB/s

SergeyWalsh (sergeywalsh) на linux-gdn openSUSE

Искать:

- Веб-браузер
- Электронный секретарь
- Текстовый процессор
- Аудио проигрыватель
- Программа управления фотографиями
- Диспетчер файлов
- Параметры системы
- Справка
- Терминал

Избранное Приложения Компьютер Последние Выход

Документы — Konqueror

Файл Правка Вид Переход Закладки Сервис Настройка Окно

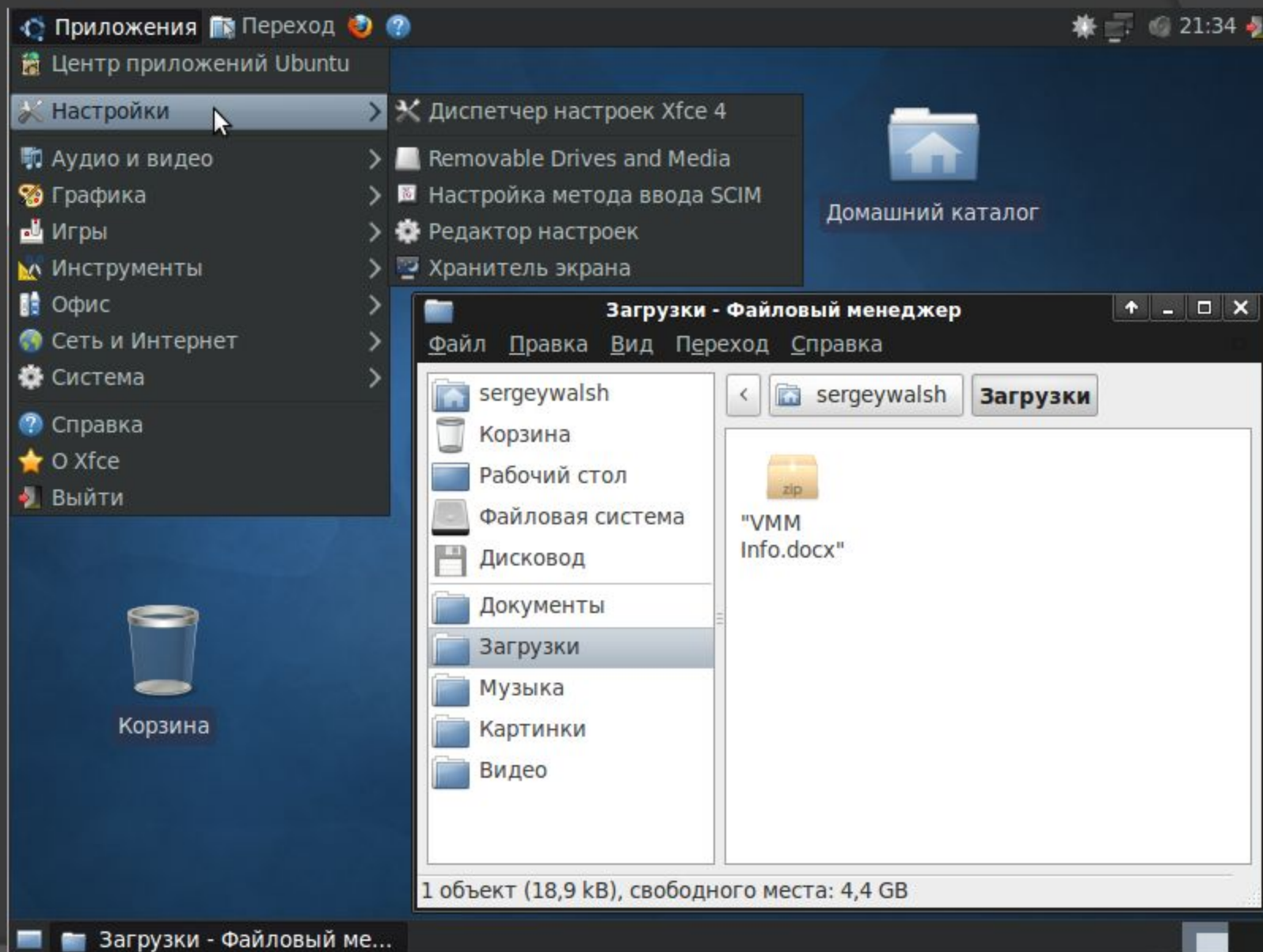
/home/sergey

openSuse.png

1 файл (379,1 киБ)

21:22

Linux [Xubuntu 9.10 (Xfce 4)]



Поддержка широкого спектра драйверов с возможностью простого включения в систему нового драйвера

- Достоинством подсистемы ввода-вывода операционной системы является разнообразие устройств, поддерживаемых данной ОС.
- Для создания драйверов необходимо наличие удобного и открытого интерфейса между драйверами и другими компонентами ОС.
- Драйвер взаимодействует, с одной стороны, с модулями ядра ОС, а с другой стороны – с контроллерами внешних устройств. Драйвер имеет два интерфейса DKI (driver kernel interface) и DDI (driver device interface).





Логическая организация файловой системы

- Одной из основных задач ОС – предоставление удобного пользовательского интерфейса при работе с данными, хранящимися на носителях. Логическая модель в рамках ОС подменяет физическую модель размещения данных на носителях.
- **Файл** – именованная область внешней памяти, в которую могут записываться и откуда могут считываться данные. Применение файлов позволяет решить следующие задачи:
 - Долговременное хранение информации;
 - Совместное использование информации.



Файловая система

- **Файловая система** – часть ОС, включающая:
 - Совокупность всех файлов на дисках;
 - Наборы структур данных, используемых для управления (каталоги, дескрипторы файлов, таблицы распределения свободного и занятого пространства);
 - Комплекс системных программных средств, реализующих операции над файлами (создание, удаление, чтение, запись, именование и поиск файлов).
 - В многопользовательских системах добавляются функции по обеспечению защиты данных от несанкционированного доступа.
- Файловые системы поддерживают несколько функционально различных типов файлов:
 - Обычные файлы;
 - Каталоги;
 - Ссылки;
 - Именованные каналы;
 - Конвейеры и т.д.

Состав компонентов и функции операционной системы:

1. Управление процессами
2. Управление памятью
3. Управление файлами
4. Управление внешними устройствами
5. Защита данных
6. Администрирование
7. Интерфейс прикладного программирования
8. Пользовательский интерфейс





Программное обеспечение компьютера

Операционная система – обеспечивает совместное функционирование всех устройств компьютера и предоставляет пользователю доступ к его ресурсам с использованием графического интерфейса ОС.

Драйверы устройств – специальные программы, обеспечивающие управление работой устройств компьютера и согласование информационного обмена с другими устройствами (каждому устройству соответствует свой драйвер).

Программное обеспечение

Тема 2. Прикладные программы



Стандартные программы ОС Windows

- **Paint** – графический редактор, позволяет создавать, просматривать и редактировать рисунки или отсканированные фотографии
- **Imaging** – используется для просмотра и редактирования графических файлов, например, цифровых рисунков или отсканированных фотографий
- **Калькулятор** – электронный калькулятор является аналогом обычного ручного калькулятора
- **Блокнот** – текстовый редактор, используется для создания и редактирования текстовых файлов простого формата
- **WordPad** – текстовый редактор, используется для создания и форматирования текстовых файлов со сложным форматированием



Прикладное программное обеспечение

Приложение – это программа, дающая возможность обрабатывать текстовую, графическую, числовую, аудио- и видеоинформацию, работать в компьютерных сетях, не владея программированием.









Приложение функционирует под управлением определенной операционной системы.

Типы приложений:

1. **Приложения общего назначения** (калькуляторы, электронные таблицы, текстовые, звуковые и графические редакторы, мультимедиапроигрыватели, базы данных, программы разработки презентаций, коммуникационные программы и т.д.).

2. **Приложения специального назначения** (бухгалтерские программы, энциклопедии, обучающие программы, системы автоматического перевода, системы программирования, компьютерные игры и т.д.)

Интегрированные офисные приложения Microsoft Office

	Microsoft Office Access	←	Создание баз данных
	Microsoft Office InfoPath	←	Создание динамических форм для сбора сведений
	Microsoft Office Outlook	←	Получение и отправка почтовых сообщений
	Microsoft Office PowerPoint	←	Создание презентаций и Веб-страниц
	Microsoft Office Word	←	Создание писем, докладов, рефератов и т.д. с графическим оформлением
	Microsoft Office Excel	←	Выполнение вычислений, построение диаграмм
	Microsoft Office Publisher	←	Создание публикаций, буклетов, Веб-узлов
	Microsoft Office FrontPage	←	Создание и управление Веб-узлами

ПО для работы с текстом

- **Текстовые редакторы** – для редактирования текстовых документов без оформления



Блокнот – файлы *.txt

- **Текстовые процессоры** – для редактирования текстовых документов



WordPad – файлы *.doc (текст + рисунки)



Word – файлы *.doc, *.docx (текст + рисунки + таблицы + автофигуры + диаграммы ...)



OpenOffice Writer – файлы *.odt – **бесплатно**
openoffice.org

ПО для обработки изображений

■ Графические редакторы

Растровые рисунки:



Paint – файлы *.bmp (также *.gif, *.jpg)



Adobe Photoshop – файлы *.psd www.adobe.com



Gimp – **бесплатно** www.gimp.org



Paint.NET – **бесплатно** www.getpaint.net

Векторные рисунки:



CorelDraw – файлы *.cdr www.corel.com



Adobe Illustrator – файлы *.ai www.adobe.com



Inkscape – **бесплатно** www.inkscape.org



OpenOffice Draw – файлы *.odg – **бесплатно**

Прикладное ПО

- **Редакторы видео** (файлы *.avi, *.mpg, *.wmv)



Movie Maker (в составе *Windows*)



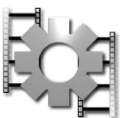
Pinnacle Studio

www.pinnaclesys.ru



Adobe Premier

www.adobe.com



VirtualDub – **бесплатно** www.virtualdub.org

- **Издательские системы** – для подготовки печатных материалов (газет, книг, буклетов)



Microsoft Publisher



QuarkXPress www.quark.com



Adobe InDesign www.adobe.com



Scribus – **бесплатно** www.scribus.net

Офисное ПО

- **Электронные таблицы** – для выполнения расчетов с табличными данными



Microsoft Excel – файлы *.xls, *.xlsx



OpenOffice Calc – файлы *.ods – **бесплатно**

- **Системы управления базами данных**



Microsoft Access – файлы *.mdb, *.accdb



OpenOffice Base – файлы *.odb – **бесплатно**

- **Создание презентаций**



Microsoft PowerPoint – файлы *.ppt, *.pptx



OpenOffice Impress – файлы *.odp – **бесплатно**

ПО для работы в Интернете

- **Браузеры** – для просмотра Web-страниц на экране



Internet Explorer – бесплатно



Mozilla Firefox – бесплатно www.mozilla.org



Opera – бесплатно www.opera.com



Safari – бесплатно www.apple.com



Chrome – бесплатно <http://www.google.com/chrome/>

- **Почтовые программы** – прием и отправка e-mail



Microsoft Outlook Express (в составе Windows)



Microsoft Outlook



TheBat www.rttlabs.com



Mozilla Thunderbird – бесплатно

www.mozilla-russia.org

Какие бывают программы?

- **Свободное ПО** с открытым исходным кодом (*Open Source*): можно бесплатно
 - запускать и использовать в любых целях
 - изучать текст программы
 - распространять (бесплатно или **за плату**)
 - изменять код (развитие и усовершенствование)



Linux



Firefox



Gimp



- **Бесплатное ПО** (*Freeware*): можно бесплатно использовать; исходного кода нет; есть ограничения на:

- коммерческое использование
- изменение кода
- извлечение данных



Opera



avast! antivirus
Avast

Какие бывают программы?

- **Условно-бесплатное ПО (*Shareware*):**

бесплатное ПО с ограничениями:

- отключены некоторые функции
- ограничен срок действия (30 дней)
- ограничено количество запусков
- раздражающие сообщения
- принудительная реклама

Платная регистрация снимает ограничения.

- **Коммерческое ПО:**

- плата за каждую копию
- *бесплатная техническая поддержка (!)*
- запрет на изменение кода и извлечение данных
- быстрое внесение изменений (сервис-паки, новые версии)



Nero Burning
Rom



TheBat

Программное обеспечение

Тема 3. Системные программы


```
Phoenix - AwardBIOS v6.00PG
Copyright (C) 1984-2003, Phoenix Technologies, LTD

(6A611T3) Release number 691N1P19
NVIDIA BIOS Version: 2.853.57
Main Processor : Intel(R) Core(TM)2 CPU 2.66GHz(266x10.8)

Press DEL to enter SETUP, ESC to Enter Boot Menu
10/31/2006-C55MCP55-6A611T3C-00
```

Начальная загрузка ПК

Работает микропрограмма, «зашитая» в чип BIOS

```
ward Workstation BIOS v6.00PC, An Energy Star Ally  
C) 1984-2003, Phoenix Technologies, LTD
```

```
1.1K 08/08/2006
```

```
: AMD Sempron(tm) Processor 3200+
```

```
: 1048576K
```

```
formation: Single Channel, 64-bit
```

```
906/19/06
```

```
Master : None
```

```
Slave : None
```

```
Master : SONY DVD RW DW-U10A 1.1d
```

```
Slave : None
```

```
Master : WDC WD2500JD-22HBB0 06.02D08
```

```
Master : None
```

```
Master : None
```

```
Master : None
```

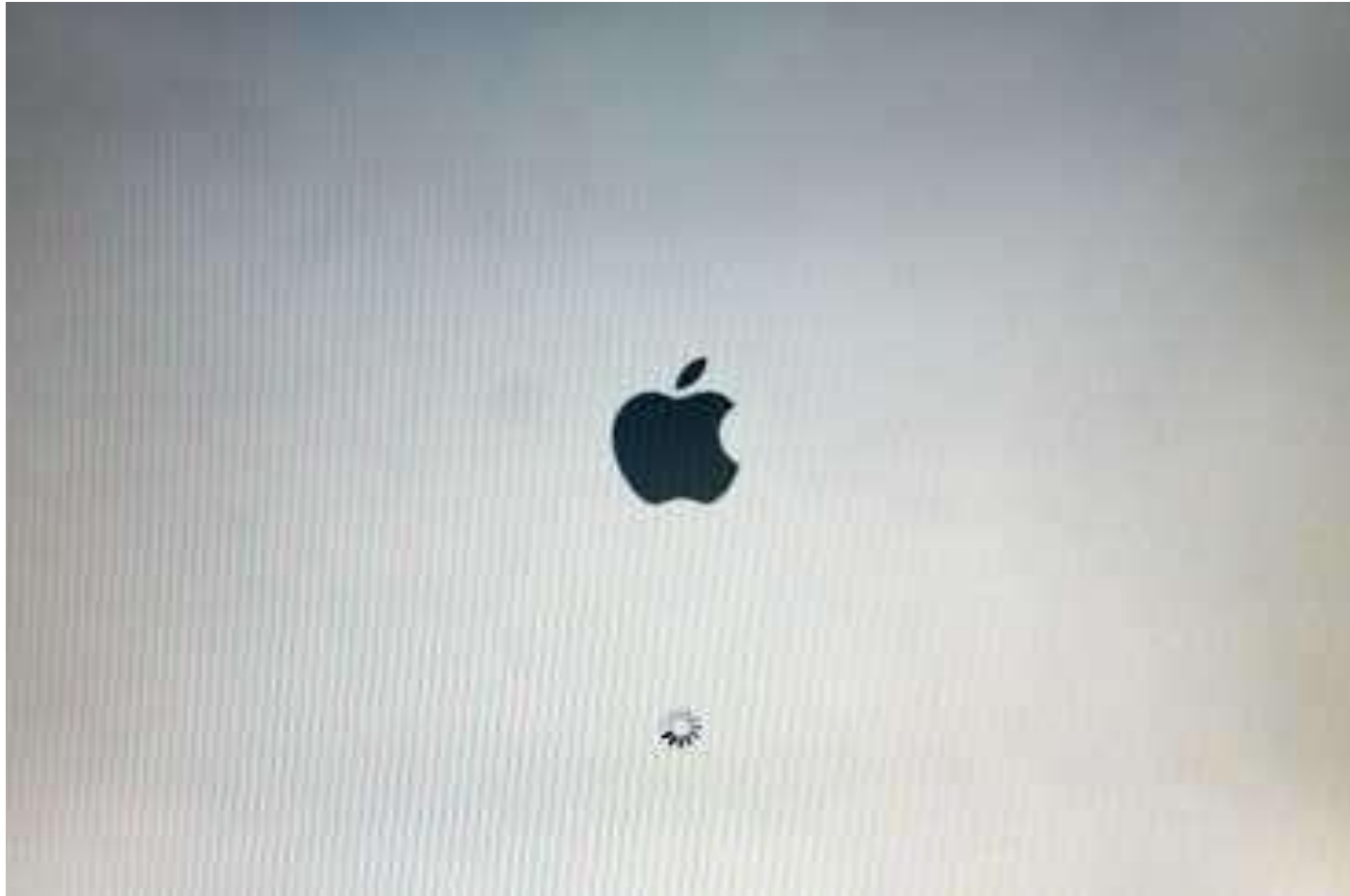
Начальная загрузка ПК

Работает микропрограмма, «зашитая» в чип BIOS – еще один вариант



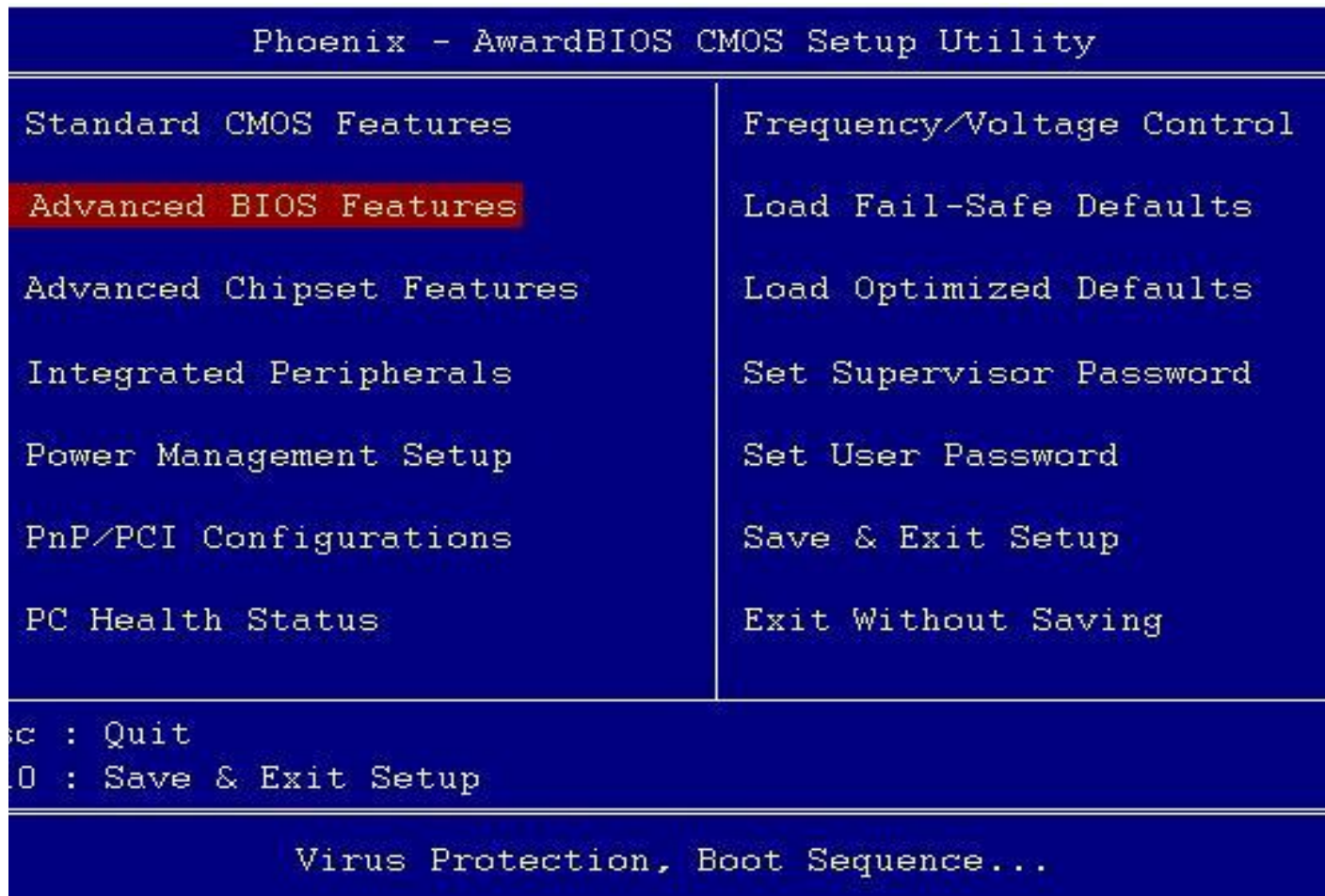
Начальная загрузка MacOS

Как мы видим, никакой дополнительной информации нет на экране



Начальная загрузка MacOS

Еще один вариант



Меню микропрограммы BIOS

Здесь можно получить информацию о системе («железе») и сделать нужные настройки, если есть необходимость

Операционные системы

Операционная система (ОС) – это комплекс программ, обеспечивающих пользователю и прикладным программам удобный **интерфейс** (способ обмена информацией) с аппаратными средствами компьютера.

Функции ОС (что она обеспечивает):

- обмен данными с **внешними устройствами**
- работу **файловой системы** (файлы, папки)
- **запуск и выполнение** остальных программ
- **тестирование** компьютера, обработка ошибок
- **распределение ресурсов** (процессор, память, внешние устройства)

Файловые системы

Windows:

- **FAT32** (Windows 95/98/2000/XP/Vista/7)
 - ⊖ ▪ медленно работает с большими дисками
 - не поставить права доступа
- **NTFS** (Windows NT/2000/XP/Vista/7)
 - ⊕ ▪ права на доступ
 - квоты для пользователей
 - сжатие дисков «на лету»
 - журналирование
 - ⊖ ▪ сложность

Linux:

- **ext3, ext4**

планируемые изменения
на диске записываются в
журнал (для
восстановления при сбое)

Состав операционной системы

- **загрузчик ОС** – это небольшая программа, которая находится в секторе 1 загрузочного диска, ее задача – загрузить в память основную часть (ядро) ОС
- **система распределения памяти**
- **система ввода и вывода** (*BIOS = Basic Input and Output System*), в микросхеме флэш-памяти на материнской плате
 - тестирование при запуске
 - чтение и запись на диски
 - обмен данными с клавиатурой, монитором, принтером
 - календарь и часы
 - настройки данного компьютера
- **командный процессор** (`command.com`, `cmd.exe`)
 - выполняет команды, введенные с клавиатуры
 - обеспечивает загрузку и выполнение других программ



Состав операционной системы (II)

- **утилита** (лат. *utilitas* – польза) – это служебные программы для проверки и настройки компьютера:
 - разбивка диска на разделы (**fdisk.exe**)
 - форматирование диска (**format.com**)
 - тестирование диска (**chkdsk.exe**)
 - редактирование реестра (**regedit.exe**)
 - проверка соединения (**ping.exe**)
- **драйвер** (англ. *driver* – водитель) – это программа, которая постоянно находится в памяти и обеспечивает обмен данными с внешним устройством (файлы ***.sys** в *Windows*)
 - драйвер видеокарты, звуковой карты, сетевой карты, принтера, сканера, ...

Типы ОС

Однозадачные – в каждый момент выполняется только одна задача (программа), она получает все ресурсы компьютера.

Примеры: *MS DOS, FreeDOS, DR DOS, PC DOS*

Многозадачные – может одновременно выполняться несколько задач; ОС распределяет *кванты* времени процессора между задачами.

- *Windows 95/98/Me*
- *Windows NT/2000/XP/2003/Vista/7*
- *UNIX* – надежная сетевая ОС (Интернет)
- *Linux* – *UNIX*-подобная ОС
- *QNX* – ОС реального времени

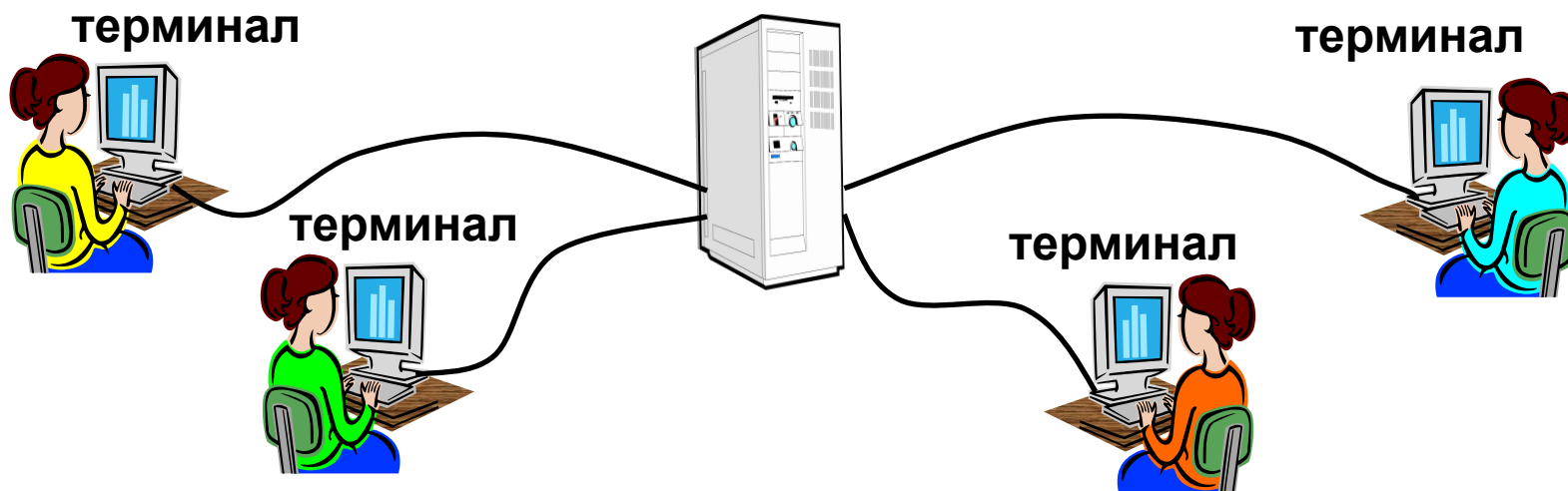
Типы ОС

Однопользовательские – в каждый момент с компьютером работает один пользователь, он получает все ресурсы компьютера.



Многопользовательские – с мощным компьютером одновременно работают несколько пользователей.

терминал = монитор + клавиатура



Утилиты, не входящие в ОС

- **антивирусные программы**



AVP, Е. Касперский, www.avp.ru



DrWeb, И. Данилов www.drweb.com

NORTON



Norton Antivirus www.symantec.com



McAfee

www.mcafee.com



NOD32 www.eset.com

- **архиваторы** – программы для упаковки файлов



WinRAR (Е. Рошал) – архивы *.rar, *.zip –

www.rarsoft.com



7zip – архивы *.7z, *.zip – www.7zip.org

Утилиты, не входящие в ОС

- информация о системе



Everest www.lavalys.com



SiSoft – бесплатно www.sisoftware.net

- сканирование (*MiraScan*, *EpsonScan*, со сканером)
- программы для записи CD и DVD



Nero Burning ROM www.nero.com



DeepBurner Free – бесплатно

www.deepburner.com

Лицензия GNU GPL

GNU General Public Licence:

- программное обеспечение поставляется с исходным кодом
- авторские права принадлежат разработчикам
- можно свободно и без оплаты
 - *запускать программы*
 - *изучать и изменять код*
 - *распространять бесплатно или за плату*
 - *улучшать и распространять улучшения*
- можно использовать код в своих разработках, но они могут распространяться только по лицензии GPL
- программы распространяются без гарантий
- за настройку и сопровождение можно брать плату

Программное обеспечение

Тема 4. Сжатие файлов. Архиваторы

Архивация и сжатие файлов

Архивация – создание резервных копий (на CD, DVD). Цели:

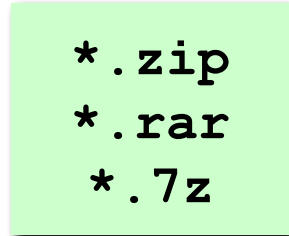
- сохранить данные на случай сбоя на диске
- объединить группу файлов в один архив
- зашифровать данные с паролем

Сжатие файлов – это уменьшение их размера. Цели:

- уменьшить место, которое занимают файлы на диске
- уменьшить объем данных для передачи через Интернет

Типы сжатия:

- **без потерь:** сжатый файл можно восстановить в исходном виде, зная алгоритм сжатия
 - тексты
 - программы
 - данные
- **с потерями:** при сжатии часть информации безвозвратно теряется
 - фотографии (* .jpg)
 - звук (* .mp3)
 - видео (* .mpg)

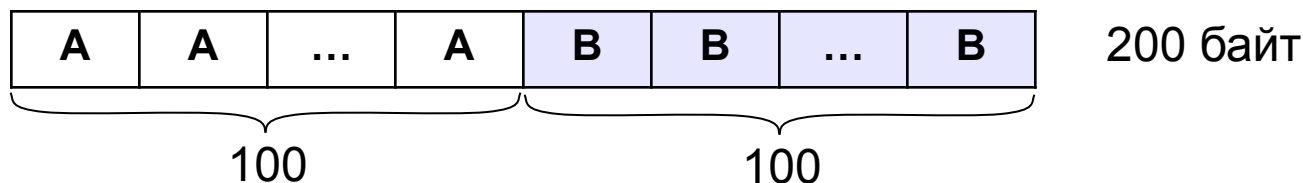


```
*.zip  
*.rar  
*.7z
```

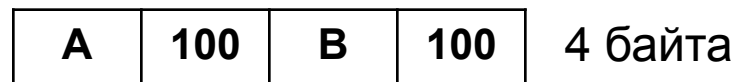

Почему файлы можно сжать?

Алгоритм RLE (англ. *Run Length Encoding*, кодирование цепочек одинаковых символов, используется для рисунков *.bmp)

Файл qq.txt



Файл qq.rle (сжатый)



сжатие в 50 раз!



Сжатие с потерями или без?

Сжатие возможно, если в данных есть повторяющиеся символы или цепочки символов, сжатие «устраняет» эту **избыточность**.

Почему файлы можно сжать?

Общий подход:

- найти в данных повторяющиеся цепочки символов
- обозначить их короткими кодами (битовыми, разной длины)
- в начало сжатого файла записать словарь

Эффективные алгоритмы:

- алгоритм Хаффмана
- алгоритм LZW (Лемпела-Зива-Велча)
- алгоритм PPM (WinRAR)

Сжимаются

хорошо

- тексты (*.txt)
- документы (*.doc, *.xls)
- несжатые рисунки (*.bmp)
- несжатый звук (*.wav)
- несжатое видео (*.avi)

плохо

- случайные данные
- программы (*.exe)
- архивы (*.zip, *.rar, *.7z)
- сжатые рисунки (*.gif, *.jpg, *.png, *.tif, ...)
- сжатый звук (*.mp3, *.wma)
- сжатое видео (*.mpg, *.wmv)

Самораспаковывающиеся архивы

SFX-архив (англ. *Self eXtracting* – самораспаковывающийся) – это файл с расширением ***.exe**, который содержит сжатые данные и программу распаковки (около 15 Кб).



- для распаковки не нужен архиватор
- может распаковать неквалифицированный пользователь



- увеличение размера файла
- опасность заражения вирусами

Многотомные архивы

Многотомный архив – это архив, разбитый на несколько частей. **Цели:**

- перенос через дискеты
- удобство скачивания через Интернет

WinRAR:

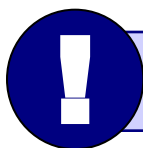
- `abc.part1.rar`, `abc.part2.rar`,
- многотомный SFX-архив: `abc.part1.exe`,
`abc.part2.rar`,

7Zip:

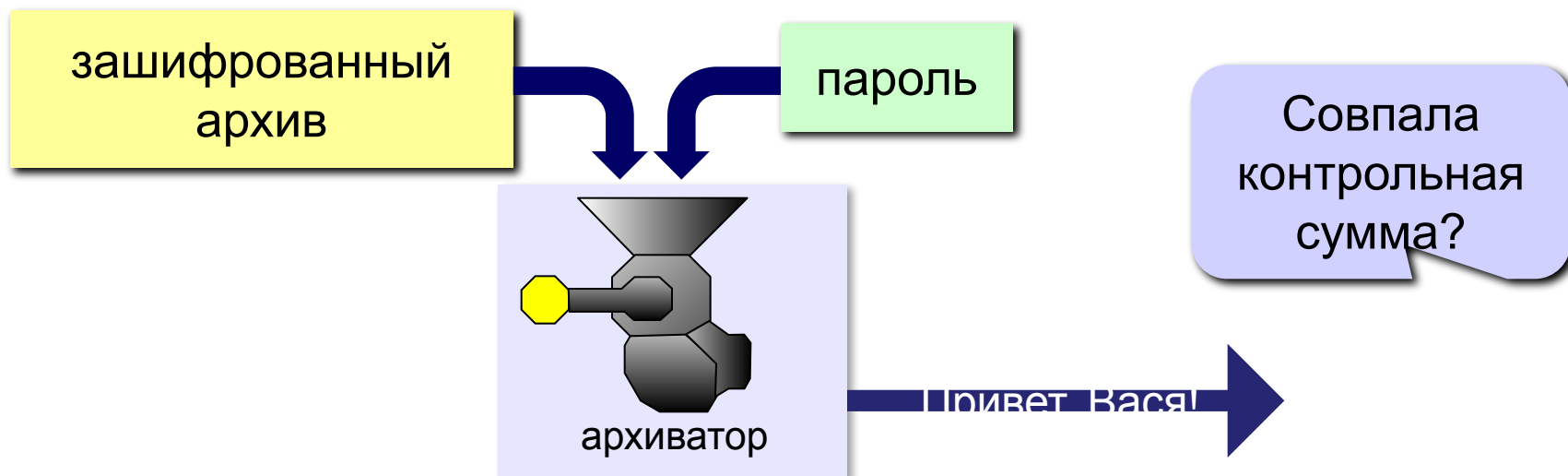
- `abc.zip.001`, `abc.zip.002`,
- `abc.7z.001`, `abc.7z.002`,

Архивы с паролем

Пароль – это секретный набор символов, предназначенный для подтверждения личности.



Пароль в архиве не хранится!



Как составить пароль?

Методы взлома:

- 1) догадаться (зная автора)
- 2) перебор по словарю
- 3) полный перебор вариантов
- 4) ...

Пароли

хорошие

- 6-15 символов
- заглавные и строчные буквы + цифры + знаки
- не слово из словаря
- Re!\$%_aS&

плохие

- 1-5 символов
- дата рождения
- телефон
- только цифры (12345)
- qwerty (йцукен)
- слово (только строчные буквы)

Архиватор WinRAR (Е. Рошал)

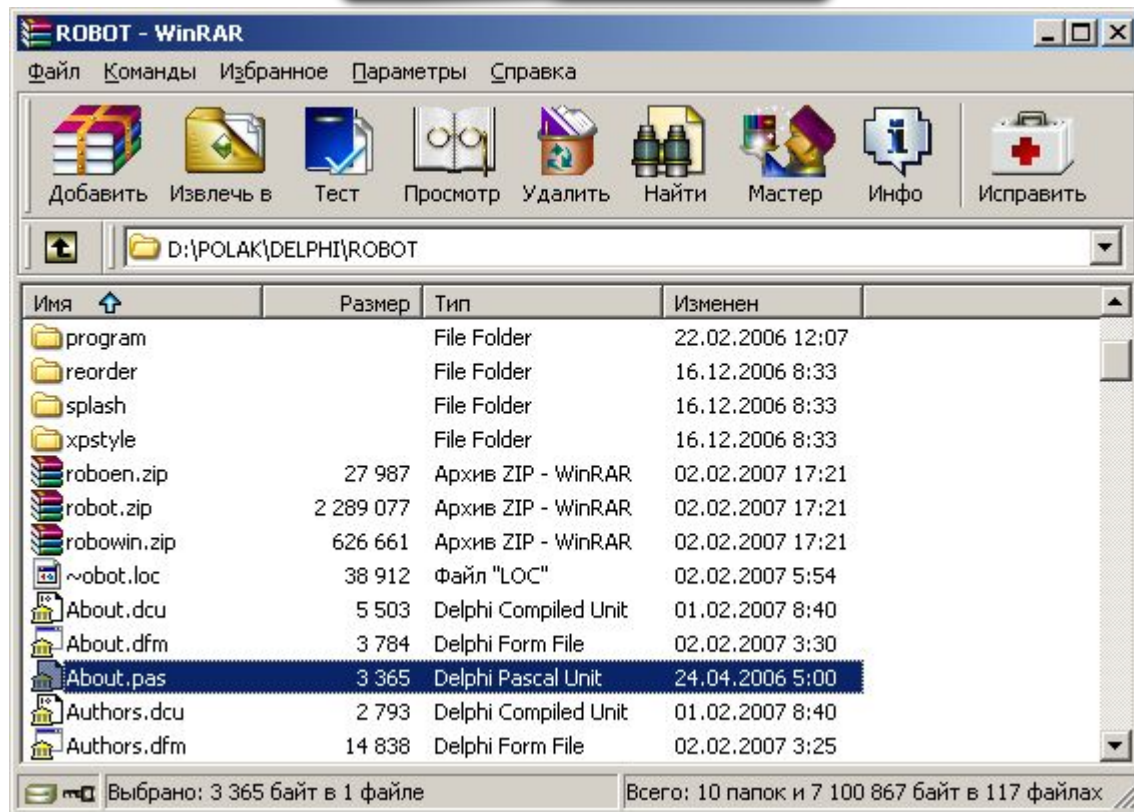
Запуск: Пуск – WinRAR

распаковать архив

сжать выделенные файлы

Выйти из папки

двойной щелчок ЛКМ: войти в архив

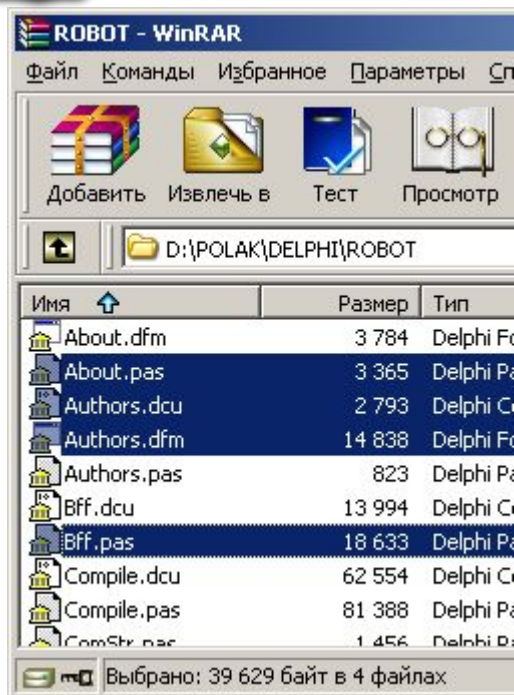


сменить диск

изменить пароль

Архиватор WinRAR: упаковка

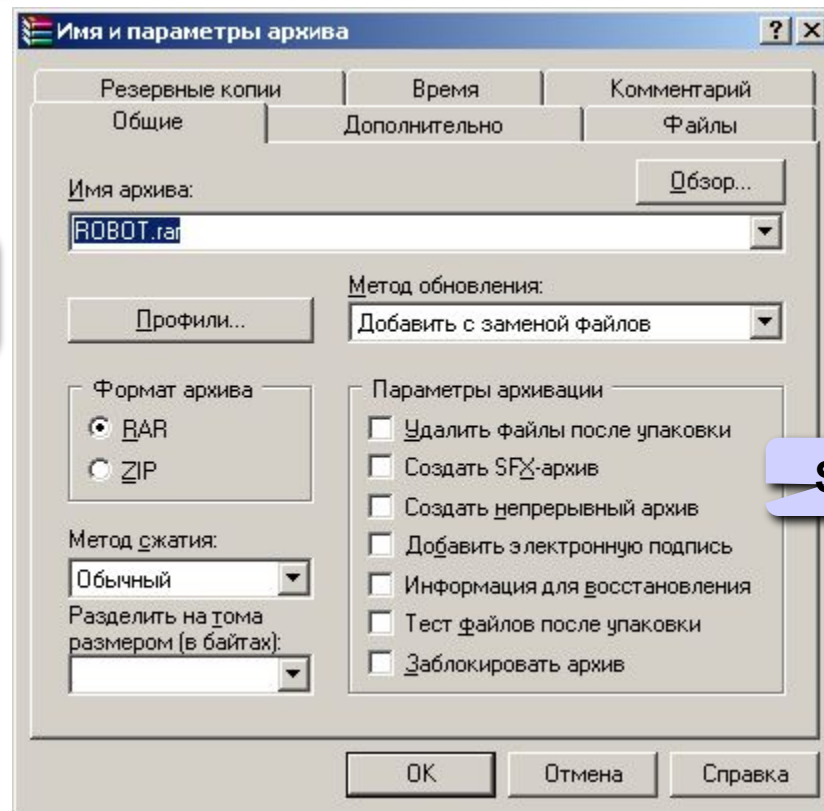
ЛКМ



ИМЯ
архива

пароль

ТИП
архива

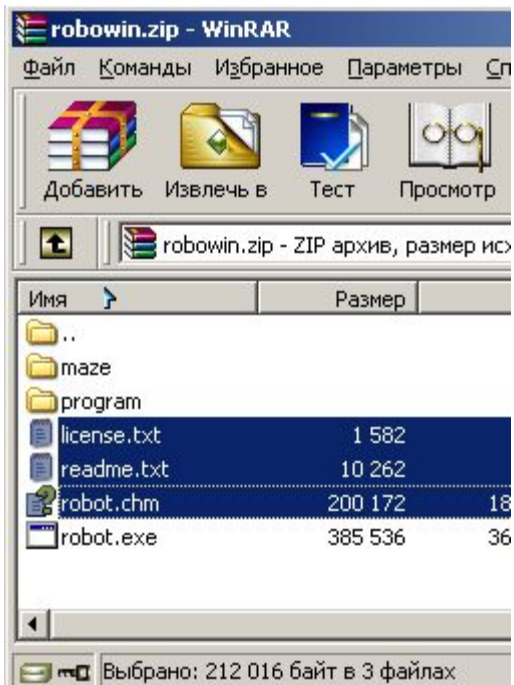


SFX

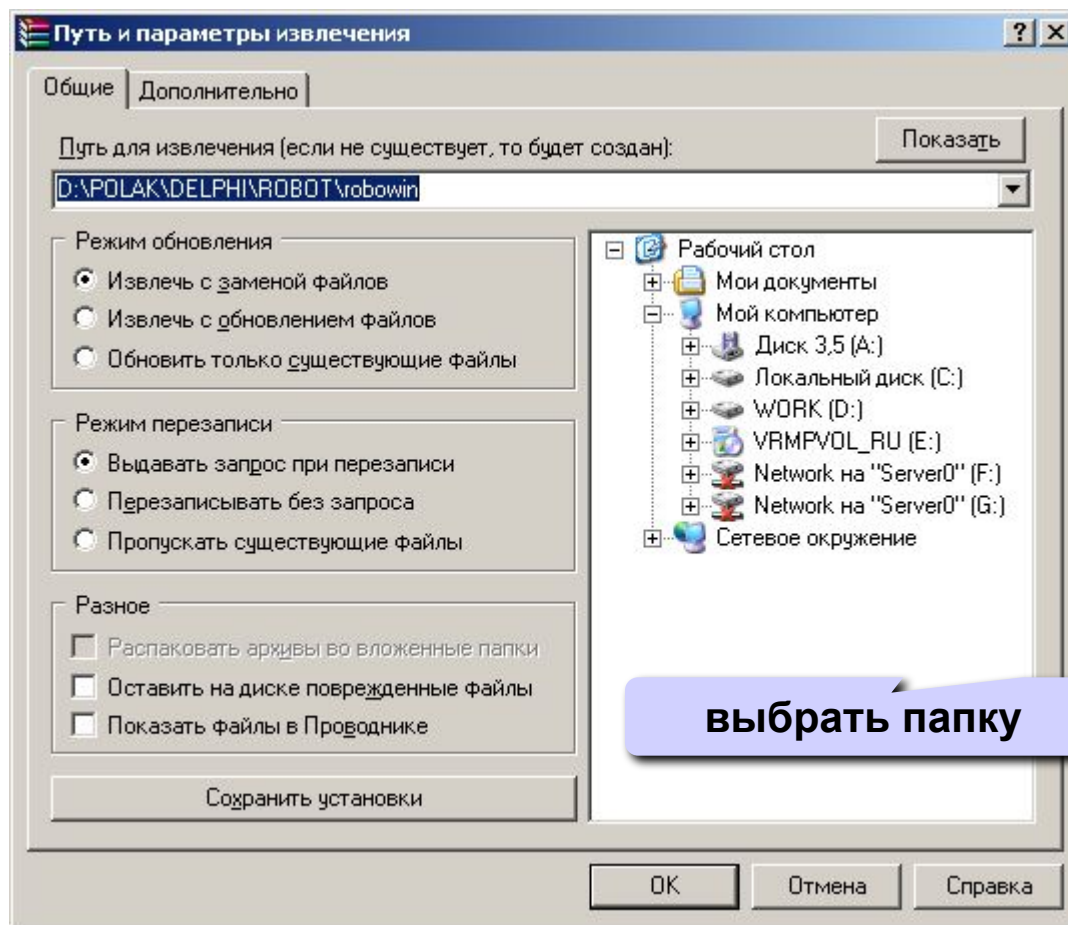
МНОГОТОМНЫЕ
архивы

Архиватор WinRAR: распаковка

ЛКМ



куда распаковать?



выбрать папку

Архиватор WinRAR в Проводнике

Упаковка

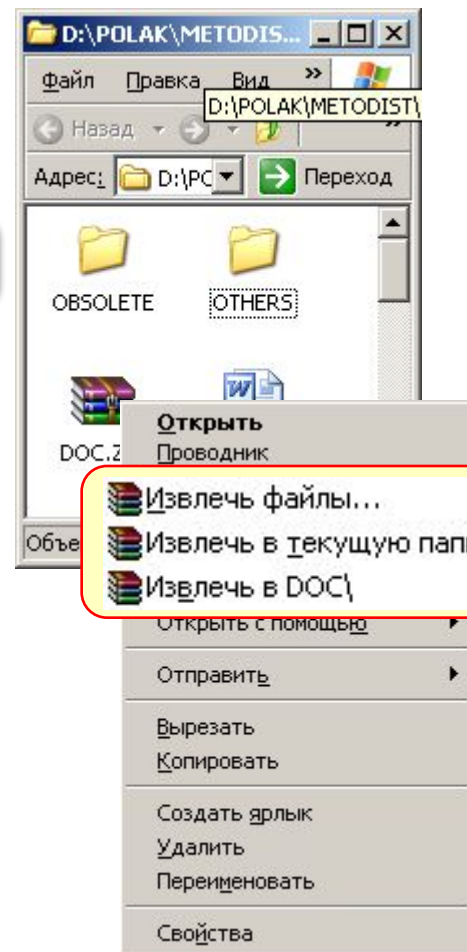


ПКМ

- Добавить в архив...
- Добавить в архив "Учебники.rar"
- Добавить в архив и отправить по e-mail...
- Добавить в архив "Учебники.rar" и отправить по e-mail

- Вырезать
- Копировать
- Создать ярлык
- Удалить
- Переименовать
- Свойства

Распаковка



ПКМ

- Извлечь файлы...
- Извлечь в текущую папку
- Извлечь в DOC\

- Открыть с помощью
- Отправить
- Вырезать
- Копировать
- Создать ярлык
- Удалить
- Переименовать
- Свойства

Архиватор 7Zip: упаковка

The image shows the 'Добавить к архиву' (Add to Archive) dialog box in 7-Zip. The dialog is overlaid on a file explorer window showing the directory G:\DELPHI\ROBOT\ with several files selected. The dialog box contains the following elements:

- ЛКМ** (Left Mouse Button): A callout pointing to the 'Добавить' (Add) button in the file explorer.
- имя архива** (Archive Name): A callout pointing to the 'Архив:' field, which contains 'ROBOT.7z'.
- тип архива (7z, zip, tar)** (Archive Type): A callout pointing to the 'Формат архива:' dropdown menu, which is set to '7z'.
- Режим изменения:** (Change Mode): A dropdown menu set to 'Добавить и заменить' (Add and replace).
- SFX**: A callout pointing to the 'Создать SFX-архив' (Create SFX archive) checkbox, which is currently unchecked.
- пароль** (Password): A callout pointing to the 'Введите пароль:' (Enter password) text box.
- МНОГОТОМНЫЕ архивы** (Multi-volume Archives): A callout pointing to the 'Разбить на тома размером (в байтах):' (Split to volumes of size (in bytes)) field.

The dialog box also includes a list of compression options:

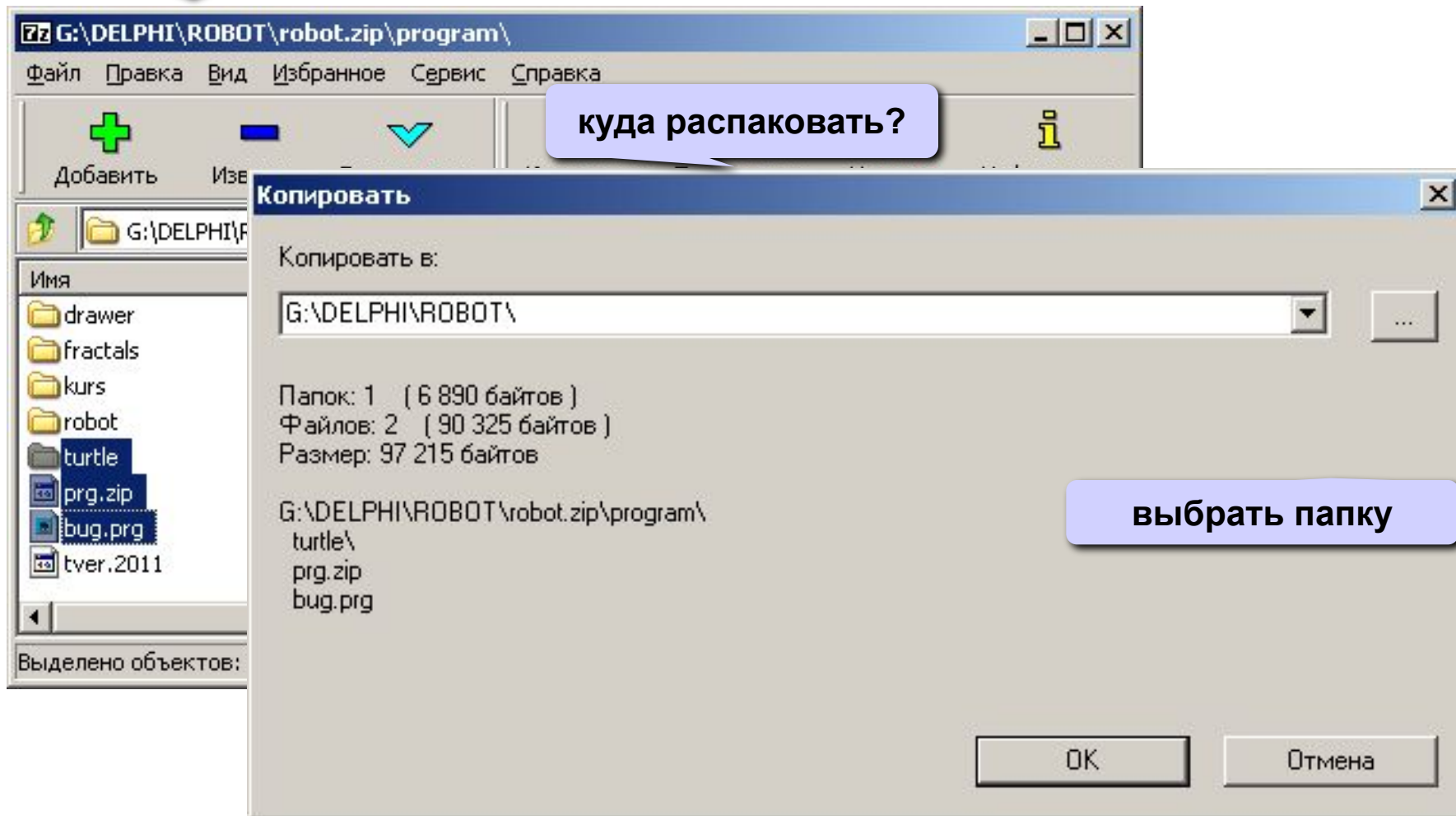
- Формат архива: 7z
- Режим изменения: Добавить и заменить
- Уровень сжатия: Нормальный
- Метод сжатия: LZMA
- Опции:
 - Создать SFX-архив
 - Сжимать открытые для записи файлы
- Размер словаря: 16 MB
- Размер слова: 32
- Размер блока: 2 GB
- Число потоков: 2 / 2
- Объем памяти для упаковки: 192 MB
- Объем памяти для распаковки: 18 MB
- Шифрование:
 - Введите пароль: [Empty text box]
 - Показать пароль
 - Метод шифрования: AES-256
 - Шифровать имена файлов
- Параметры: [Empty text box]

Buttons at the bottom: OK, Отмена (Cancel), and Помощь (Help).

Архиватор 7Zip: распаковка

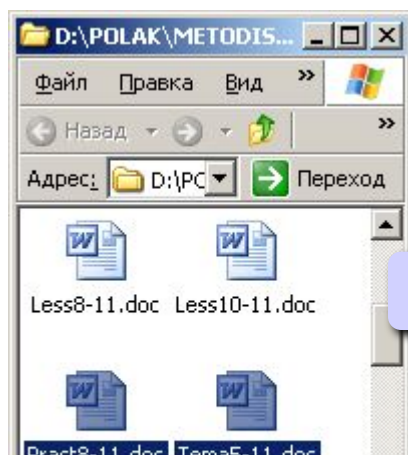
ЛКМ

куда распаковать?



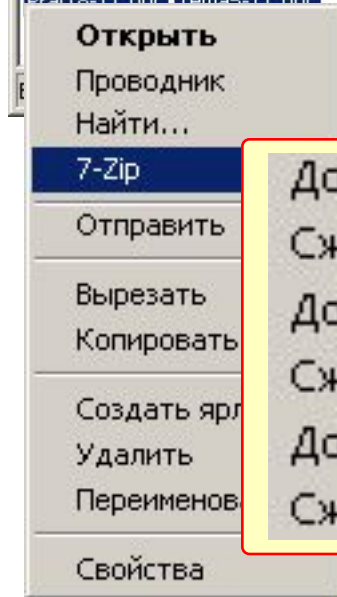
Архиватор 7Zip в Проводнике

Упаковка



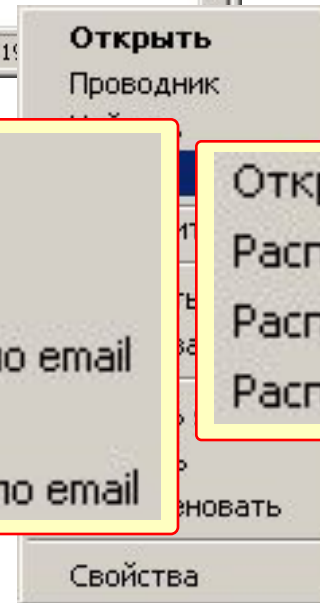
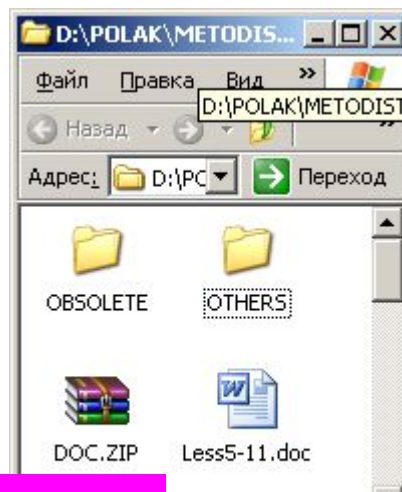
ПКМ

ПКМ



Добавить к архиву...
Сжать и отправить по email...
Добавить к "Учебники.7z"
Сжать в "Учебники.7z" и отправить по email
Добавить к "Учебники.zip"
Сжать в "Учебники.zip" и отправить по email

Распаковка



Открыть архив
Распаковать
Распаковать здесь
Распаковать в "DOC\"

Программное обеспечение

Тема 7. Компьютерные вирусы и антивирусы

Что такое вирус?

Компьютерный вирус – это программа, которая при запуске способна распространяться **без участия человека**.

Признаки заражения:

- замедление работы компьютера
- перезагрузка или зависание компьютера
- неправильная работа ОС или прикладных программ
- изменение длины файлов
- появление новых файлов
- уменьшение объема оперативной памяти
- рассылка сообщений *e-mail* без ведома автора

Вредные действия вирусов

- звуковые и зрительные эффекты
- имитация сбоев ОС и аппаратуры
- перезагрузка компьютера
- разрушение файловой системы
- уничтожение информации
- шпионаж – передача секретных данных
- массовые атаки на сайты Интернет

Что заражают вирусы?

Для того, чтобы вирус смог выполнить какие-то действия, он должен оказаться в памяти в виде **программного кода** и получить управление.

Вирусы

заражают

- программы – *.exe, *.com
- загрузочные сектора дисков и дискет
- командные файлы – *.bat
- драйверы – *.sys
- библиотеки – *.dll
- документы с макросами – *.doc, *.xls, *.mdb
- Web-страницы со скриптами

не заражают

- текст – *.txt
- рисунки – *.gif, *.jpg, *.png, *.tif
- звук (*.wav, *.mp3, *.wma)
- видео (*.avi, *.mpg, *.wmv)
- любые данные (без программного кода)

Способы заражения

- запустить зараженный файл;
- загрузить компьютер с зараженной дискеты или диска;
- при автозапуске CD(DVD)-диска или флэш-диска;
- открыть зараженный документ с макросами (*Word* или *Excel*);
- открыть сообщение e-mail с вирусом;
- открыть *Web*-страницу с вирусом;
- разрешить установить активное содержимое на *Web*-странице.

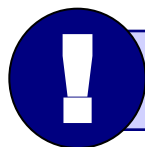
Классические вирусы

- **Файловые** – заражают файлы `*.exe`, `*.sys`, `*.dll` (редко – внедряются в тексты программ).
- **Загрузочные (бутовые, от англ. *boot* – загрузка)** – заражают загрузочные сектора дисков и дискет, при загрузке сразу оказываются в памяти и получают управление.
- **Полиморфные** – при каждом новом заражении немного меняют свой код.
- **Макровирусы** – заражают документы с макросами (`*.doc`, `*.xls`, `*.mdb`).
- **Скриптовые вирусы** – скрипт (программа на языке *Visual Basic Script*, *JavaScript*, *BAT*, *PHP*) заражает командные файлы (`*.bat`), другие скрипты и Web-страницы (`*.htm`, `*.html`).

Сетевые вирусы

распространяются через компьютерные сети, используют «дыры» – ошибки в защите *Windows, Internet Explorer, Outlook* и др.

- **Почтовые черви** – распространяются через электронную почту в виде приложения к письму или ссылки на вирус в Интернете; рассылают себя по всем обнаруженным адресам



Наиболее активны – более 90%!

- **Сетевые черви** – проникают на компьютер через «дыры» в системе, могут копировать себя в папки, открытые для записи (сканирование – поиск уязвимых компьютеров в сети)
- **IRC-черви, IM-черви** – распространяются через IRC-чаты и интернет-пейджеры (*ICQ, AOL, Windows Messenger, MSN Messenger*)
- **P2P-черви** – распространяются через файлообменные сети P2P (*peer-to-peer*)

Троянские программы

позволяют получать управление удаленным компьютером, распространяются через компьютерные сети, часто при установке других программ (зараженные инсталляторы)

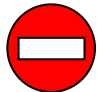
- **Backdoor** – программы удаленного администрирования
- **воровство паролей** (доступ в Интернет, к почтовым ящикам, к платежным системам)
- **шпионы** (введенный с клавиатуры текст, снимки экрана, список программ, характеристики компьютера, промышленный шпионаж)
- **DOS-атаки** (англ. *Denial Of Service* – отказ в обслуживании) – массовые атаки на сайты по команде, сервер не справляется с нагрузкой
- **прокси-сервера** – используются для массовой рассылки рекламы (спама)
- **загрузчики** (англ. *downloader*) – после заражения скачивают на компьютер другие вредоносные программы

Антивирусы-сканеры

- умеют находить и лечить **известные им** вирусы в памяти и на диске;
- используют базы данных вирусов;
- ежедневное обновление баз данных через Интернет.



- лечат известные им вирусы



- не могут предотвратить заражение
- чаще всего не могут обнаружить и вылечить неизвестный вирус

Антивирусы-мониторы

ПОСТОЯННО НАХОДЯТСЯ В ПАМЯТИ В АКТИВНОМ СОСТОЯНИИ

- перехватывают действия, характерные для вирусов и блокируют их (форматирование диска, замена системных файлов);
- блокируют атаки через Интернет;
- проверяют запускаемые и загружаемые в память файлы (например, документы *Word*);
- проверяют сообщения электронной почты;
- проверяют *Web*-страницы;
- проверяют сообщения ICQ



- непрерывное наблюдение
- блокируют вирус в момент заражения
- могут бороться с неизвестными вирусами



- замедление работы компьютера
- в случае ошибки ОС может выйти из строя

Антивирусные программы

Коммерческие



- AVP = Antiviral Toolkit Pro (www.avp.ru) – Е. Касперский



- DrWeb (www.drweb.com) – И. Данилов



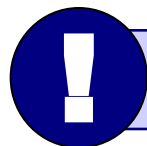
- Norton Antivirus (www.symantec.com)



- McAfee (www.mcafee.ru)



- NOD32 (www.eset.com)



Есть бесплатные пробные версии!

Бесплатные



- Security Essential
(http://www.microsoft.com/security_essentials/)



- Avast Home (www.avast.com)



- Antivir Personal (free-av.com)



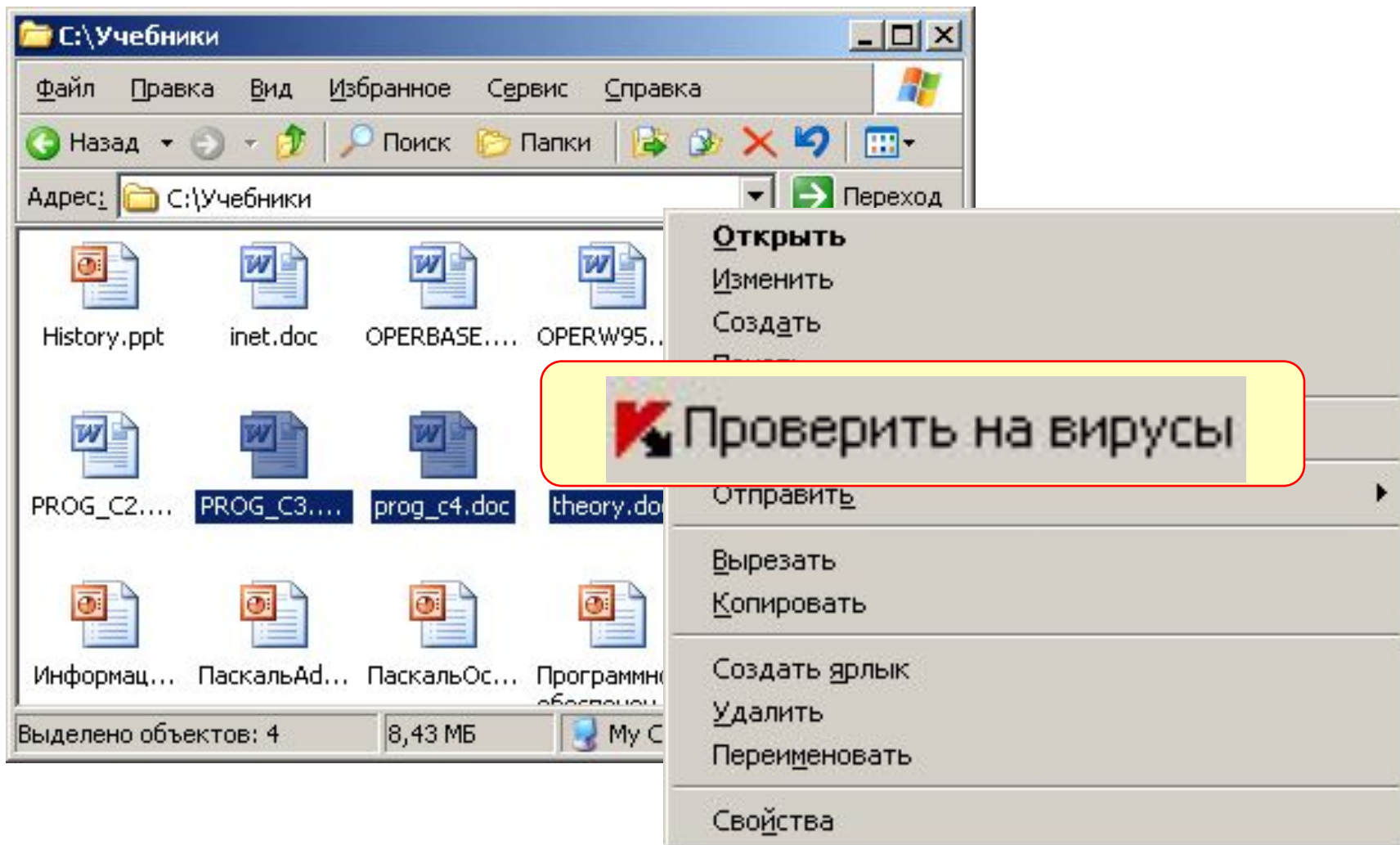
- AVG Free (free.grisoft.com)

Антивирус Касперского

- **Файловый антивирус** (проверка файлов в момент обращения к ним)
- **Почтовый антивирус** (проверка входящих и исходящих сообщений)
- **Веб-антивирус** (Интернет, проверка *Web*-страниц)
- **Проактивная защита** (попытки обнаружить неизвестные вредоносные программы):
 - слежение за реестром
 - проверка критических файлов
 - сигналы о «подозрительных» обращениях к памяти
- **Анти-шпион** (борьба с Интернет-мошенничеством)
- **Анти-хакер** (обнаружение сетевых атак)
- **Анти-спам** (фильтр входящей почты)

The screenshot displays the Kaspersky Anti-Virus interface. On the left, a menu is open with the following items: Проверка Моего Компьютера, Поиск вирусов..., Обновление, Мониторинг сети, Настройка..., **Антивирус Касперского**, Приостановка защиты..., and Выход. Red arrows point from the menu items to the corresponding windows in the background. The main window shows the 'Приостановка защиты' (Pause Protection) dialog box. The dialog box has a title bar with the Kaspersky logo and the text 'Приостановка защиты'. The main text reads: 'Защита будет автоматически включена:'. Below this, there are three radio button options: 'Через 1 минуту' (selected), 'После перезапуска приложения', and 'Только по требованию пользователя'. At the bottom of the dialog box, there are buttons for 'Справка', 'OK', and 'Отмена'. In the background, the main interface shows a status bar with a green checkmark and the text 'Настройка' and 'Защита'. A statistics window is visible in the bottom right corner, showing: 'Всего проверено: 3080', 'Обнаружено: 35', 'Не вылечено: 0', and 'Заблокировано атак: 0'. A button 'Просмотр статистики работы' is located below the statistics.

Проводник: запуск через контекстное меню





Антивирус *DrWeb* (сканер)

Запуск: Пуск – Сканер *DrWeb*

The image shows the Dr.Web Antivirus scanner interface with several annotations in blue callout boxes:

- настройки** (settings) points to the menu bar.
- выбрать, что проверяем (ЛКМ)** (select what to scan (LMB)) points to the file list.
- результ** (result) points to the status bar at the bottom left.

The scanner window displays the following settings:

Объекты	Вредоносные программы		
Инфицированные объекты	Вылечить	Рекламные программы	Удалить
Неизлечимые объекты	Удалить	Программы дозвола	Информировать
Подозрительные объекты	Информировать	Программы-шутки	Удалить
Инфицированные пакеты		Потенциально опасные	Информировать
Архивы	Информировать	Программы взлома	Игнорировать
Почтовые файлы	Информировать	Запрос подтверждения	<input checked="" type="checkbox"/>
Контейнеры	Информировать		

Additional settings at the bottom:

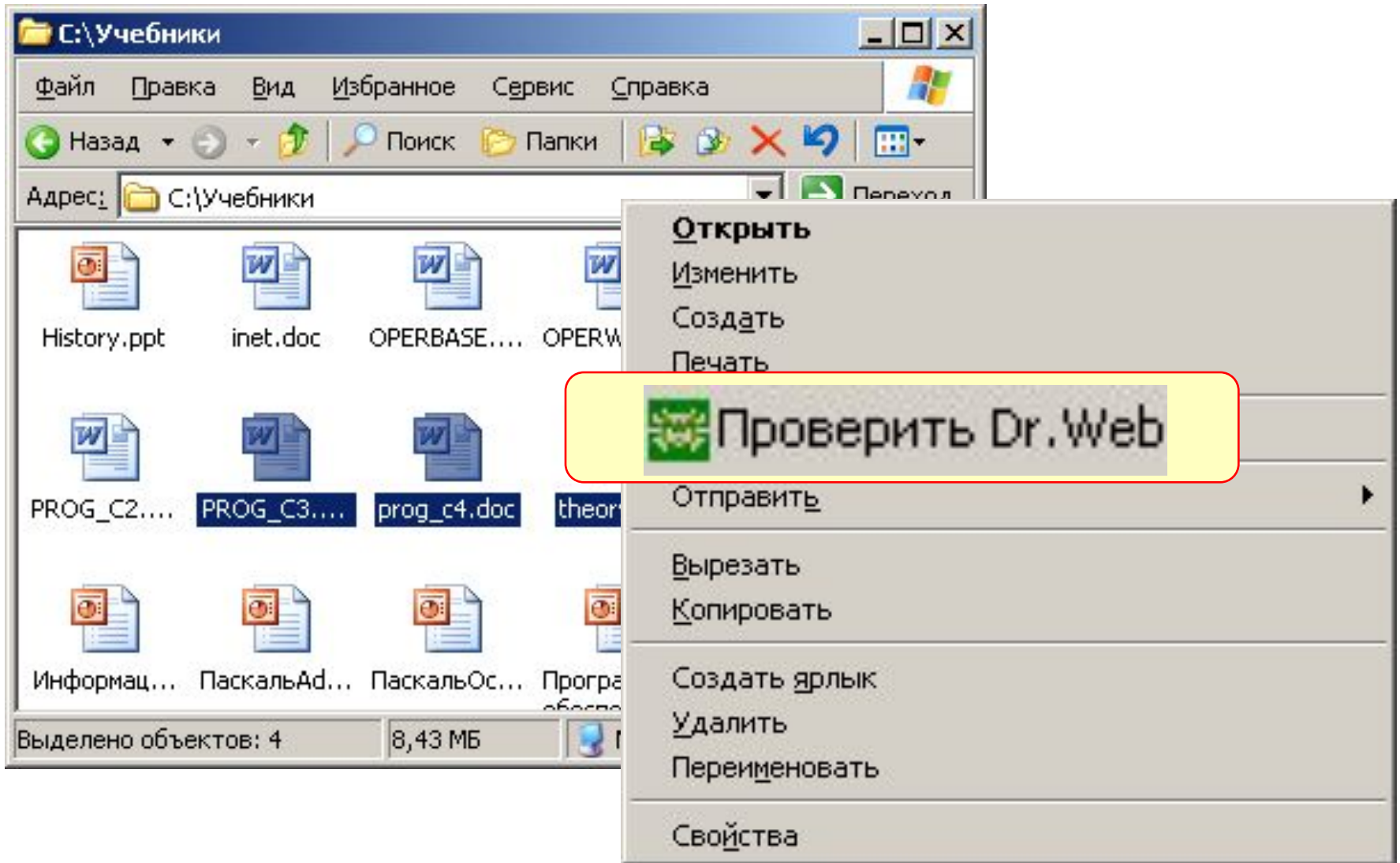
- Переименовать расширение: #??
- Путь для перемещения: infected.!!!

Buttons at the bottom: OK, Отмена, Применить, Справка



Антивирус *DrWeb*

Проводник: запуск через контекстное меню



Другие виды антивирусной защиты

брандмауэры (файрволы, сетевые экраны)

- блокируют «лишние» обращения в сеть и запросы из сети

аппаратные антивирусы

- защита от изменения загрузочного сектора
- запрет на выполнение кода из области данных
- аппаратный брандмауэр ZyWALL UTM (ZyXEL и Лаборатории Касперского)



онлайновые (on-line) антивирусы

- устанавливают на компьютер модуль *ActiveX*, который проверяет файлы...
- или файл пересылается на сайт разработчика антивирусов

<http://www.kaspersky.ru/virusscanner>

<http://www.bitdefender.com>

<http://security.symantec.com>

<http://us.mcafee.com/root/mfs/default.asp>



чаще всего не умеют лечить, предлагает купить антивирус-доктор

Профилактика

- ✓ делать **резервные копии** важных данных на CD и DVD (раз в месяц? в неделю?)
- ✓ использовать **антивирус-монитор**, особенно при работе в Интернете
- ✓ при работе в Интернете включать **брандмауэр** (англ. *firewall*) – эта программа запрещает обмен по некоторым каналам связи, которые используют вирусы
- ✓ **проверять** с помощью антивируса-доктора все новые программы и файлы, дискеты
- ✓ **не открывать** сообщения e-mail с неизвестных адресов, особенно файлы-приложения
- ✓ иметь **загрузочный диск** с антивирусом

Если компьютер заражен...

- Отключить компьютер от сети.
- Запустить антивирус. Если не помогает, то...
- выключить компьютер и загрузить его с загрузочного диска (дискеты, CD, DVD). Запустить антивирус. Если не помогает, то...
- попробовать восстановить одно из предыдущих состояний системы, если нет, то...
- удалить *Windows* и установить ее заново. Если не помогает, то...
- Обратиться за помощью...