Программное обеспечение

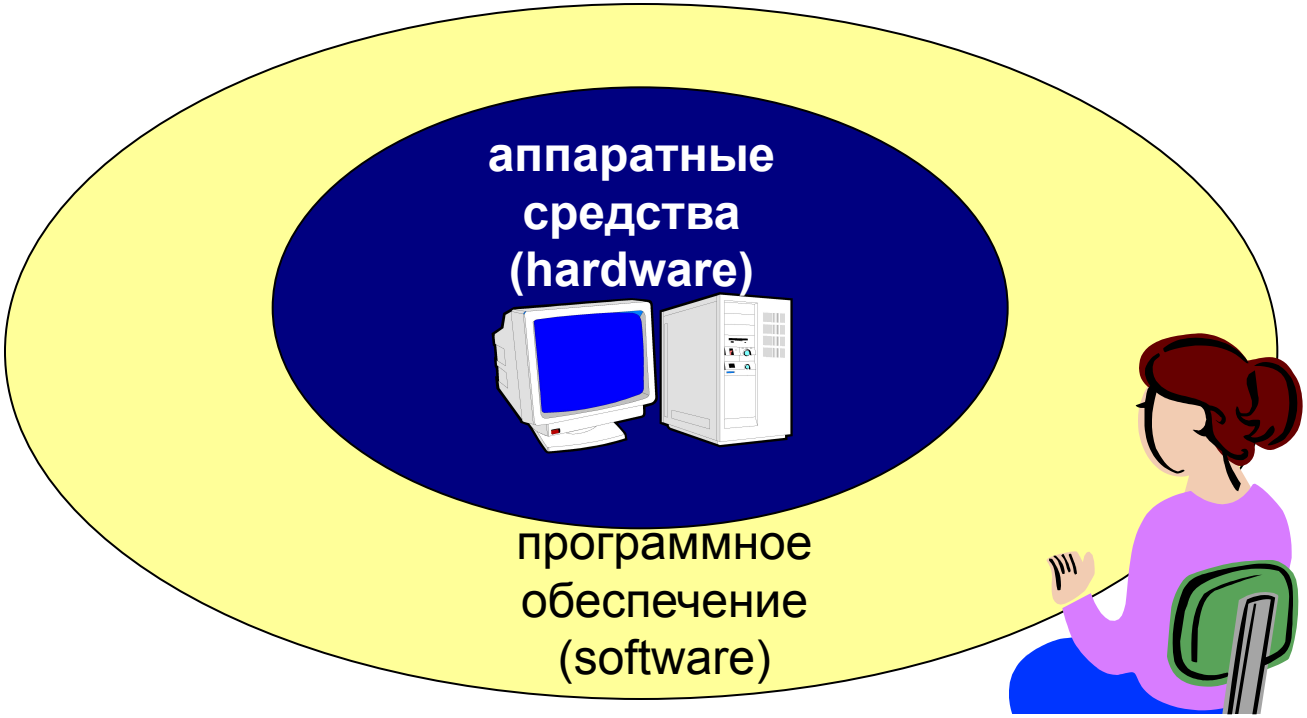
1. Введение
2. Прикладные программы
3. Системные программы
4. Сжатие файлов. Архиваторы
5. Компьютерные вирусы и антивирусы

Программное обеспечение

Тема 1. Введение

Программное обеспечение

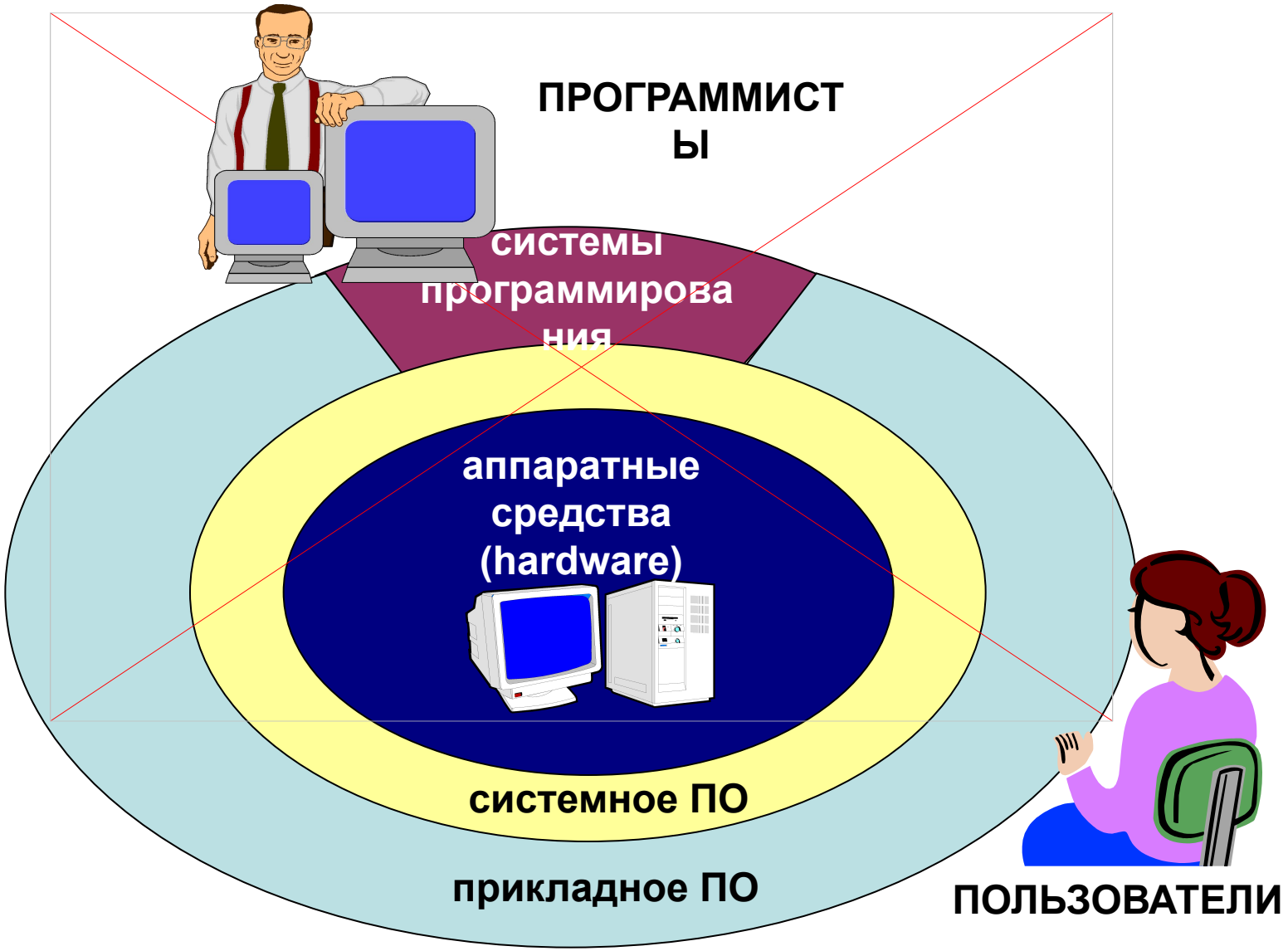
Взаимодействие человека с компьютером



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.

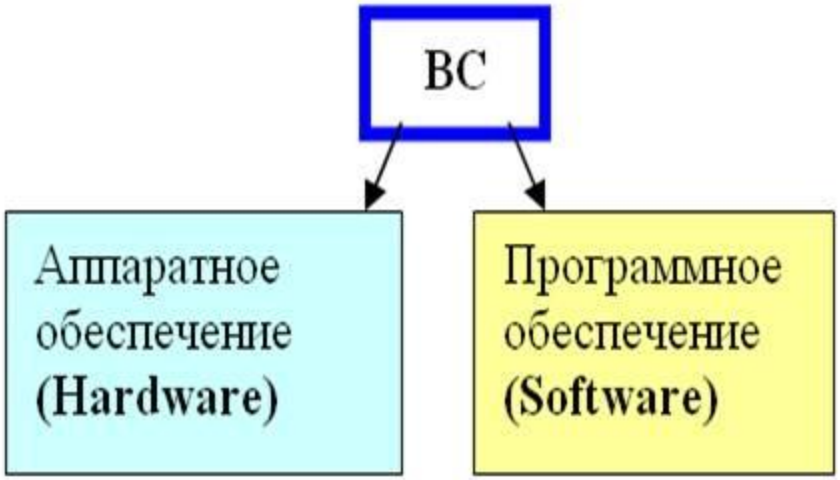


Рисунок 1 Вычислительная система - ВС

Программное обеспечение (ПО)

- **Структура ПО** может быть про-иллюстрирована следующей схемой

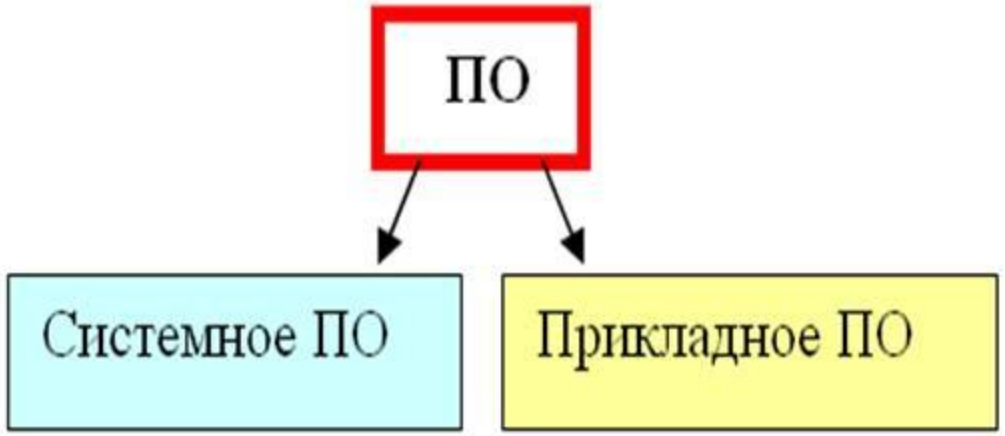
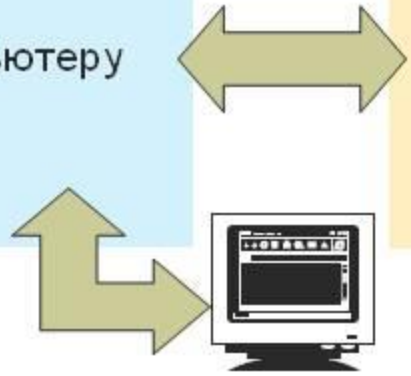


Рисунок 2 Структура ПО

Прикладное ПО взаимодействует с аппаратными компонентами ВС через системное ПО.

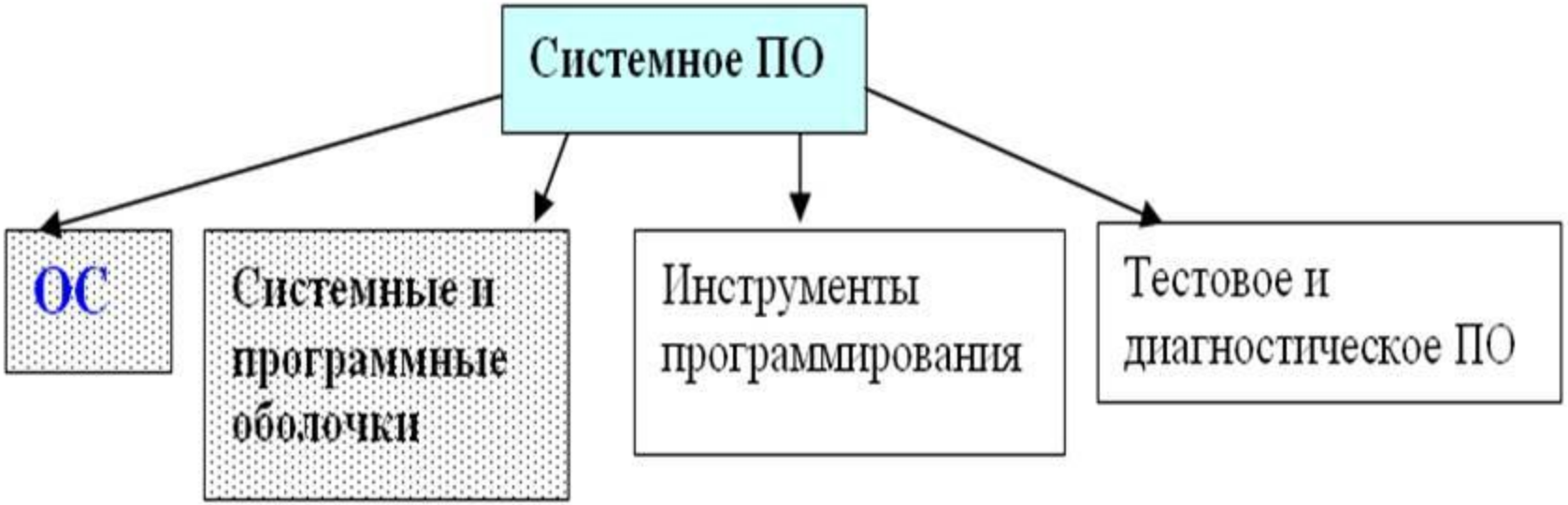
- **Системное ПО** обеспечивает и контролирует доступ к аппаратному обеспечению ВС

(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

Лекция 2

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

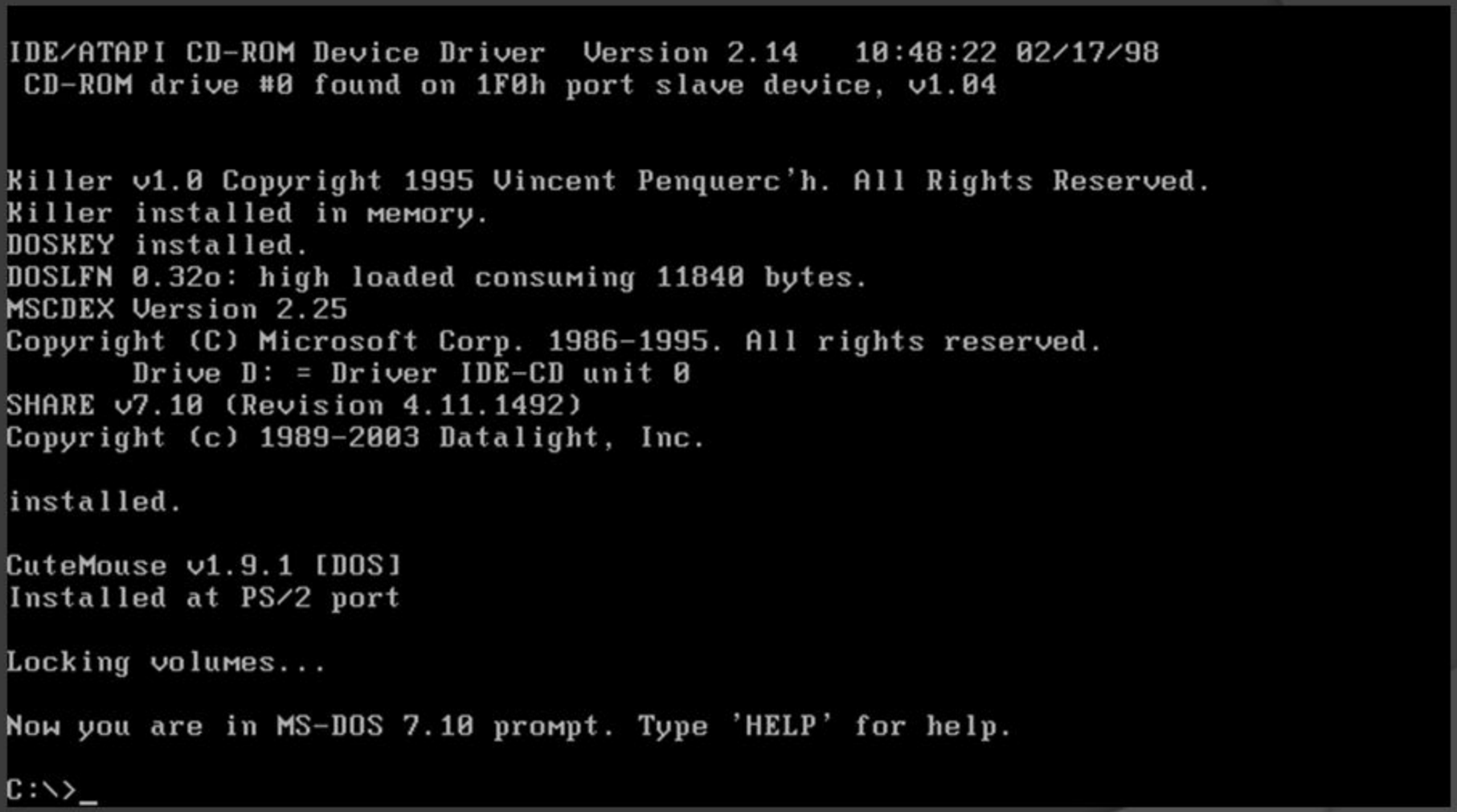
Предназначение

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

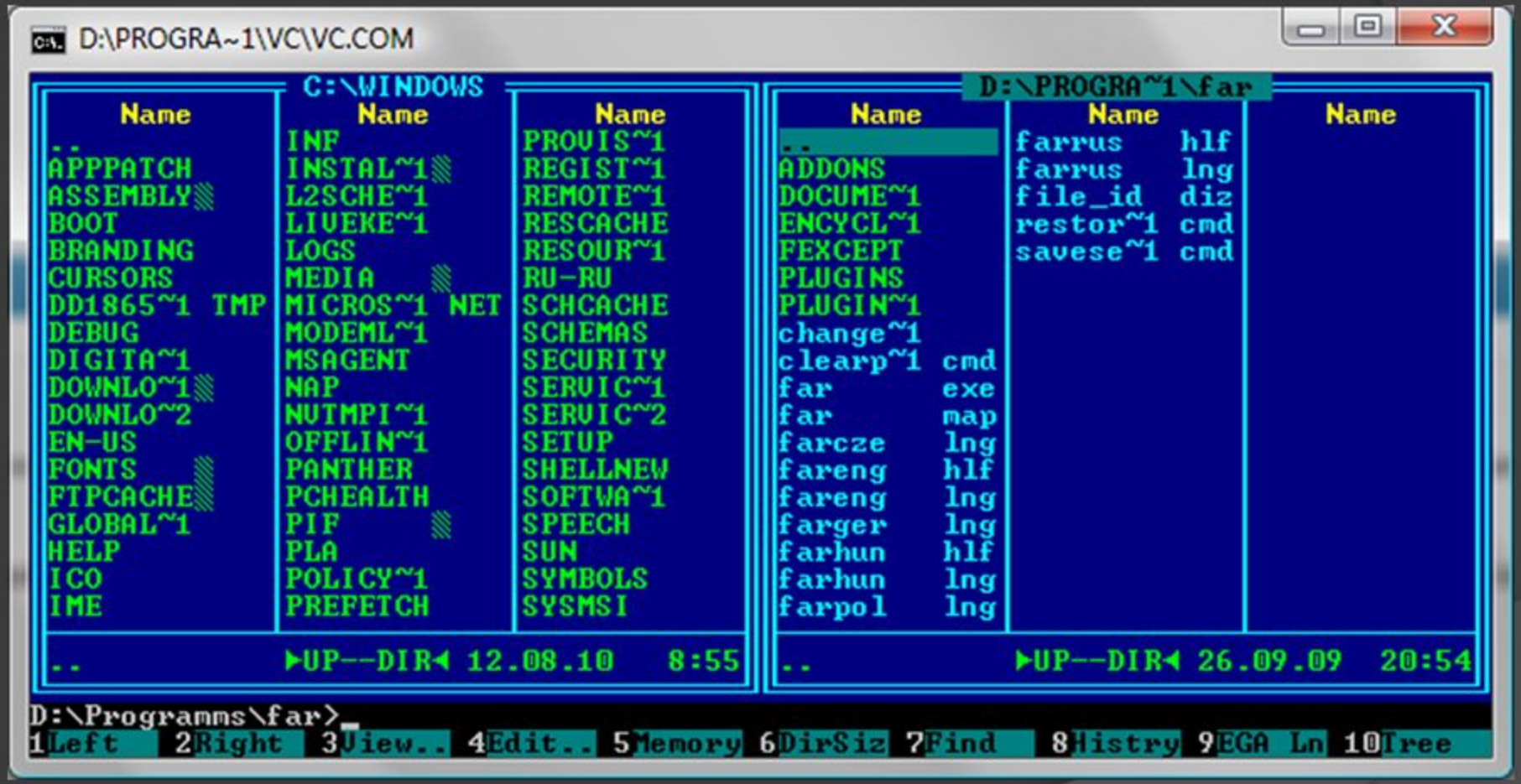
Семейство

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

Microsoft DOS

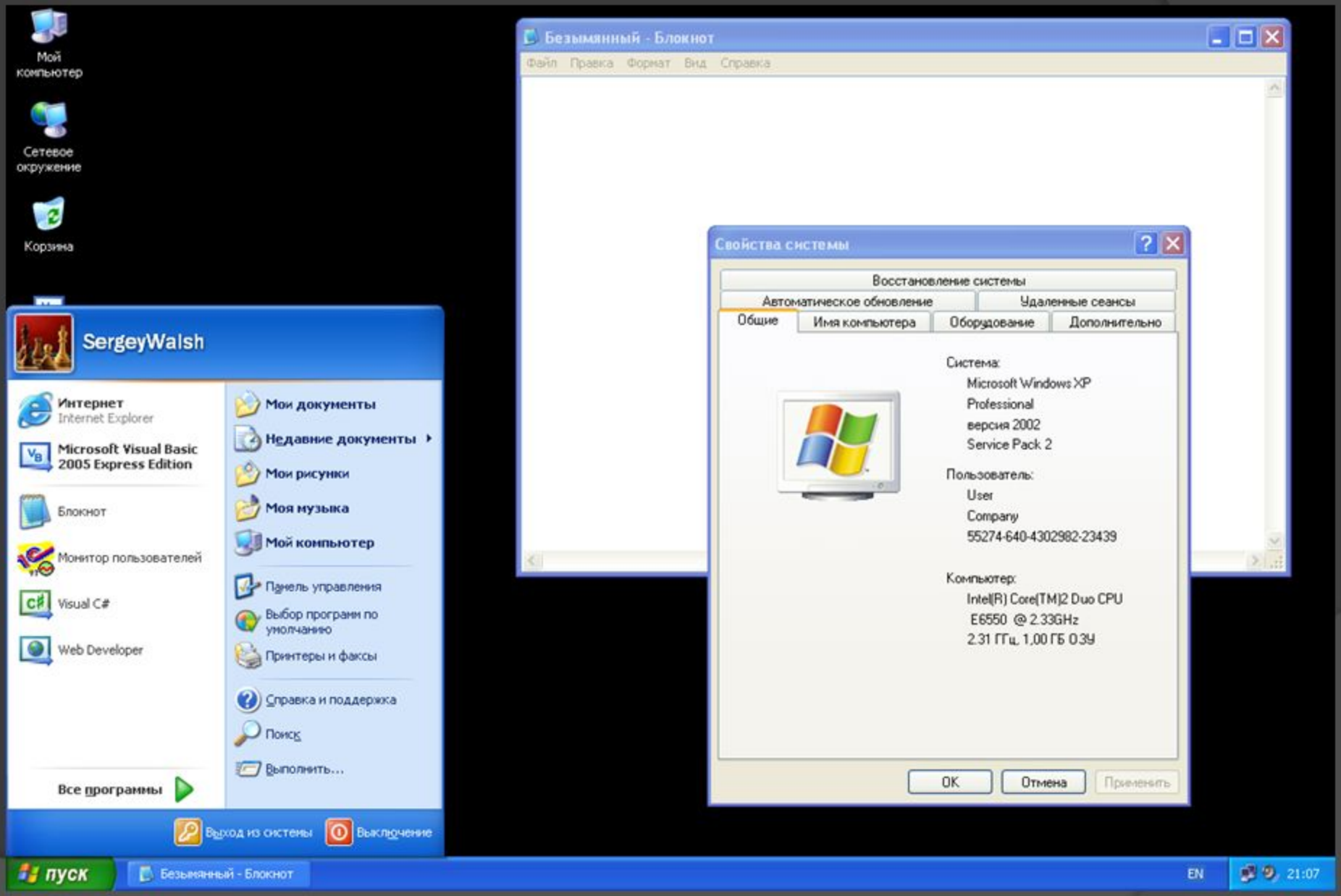


Файловые менеджеры: NC, VC и другие

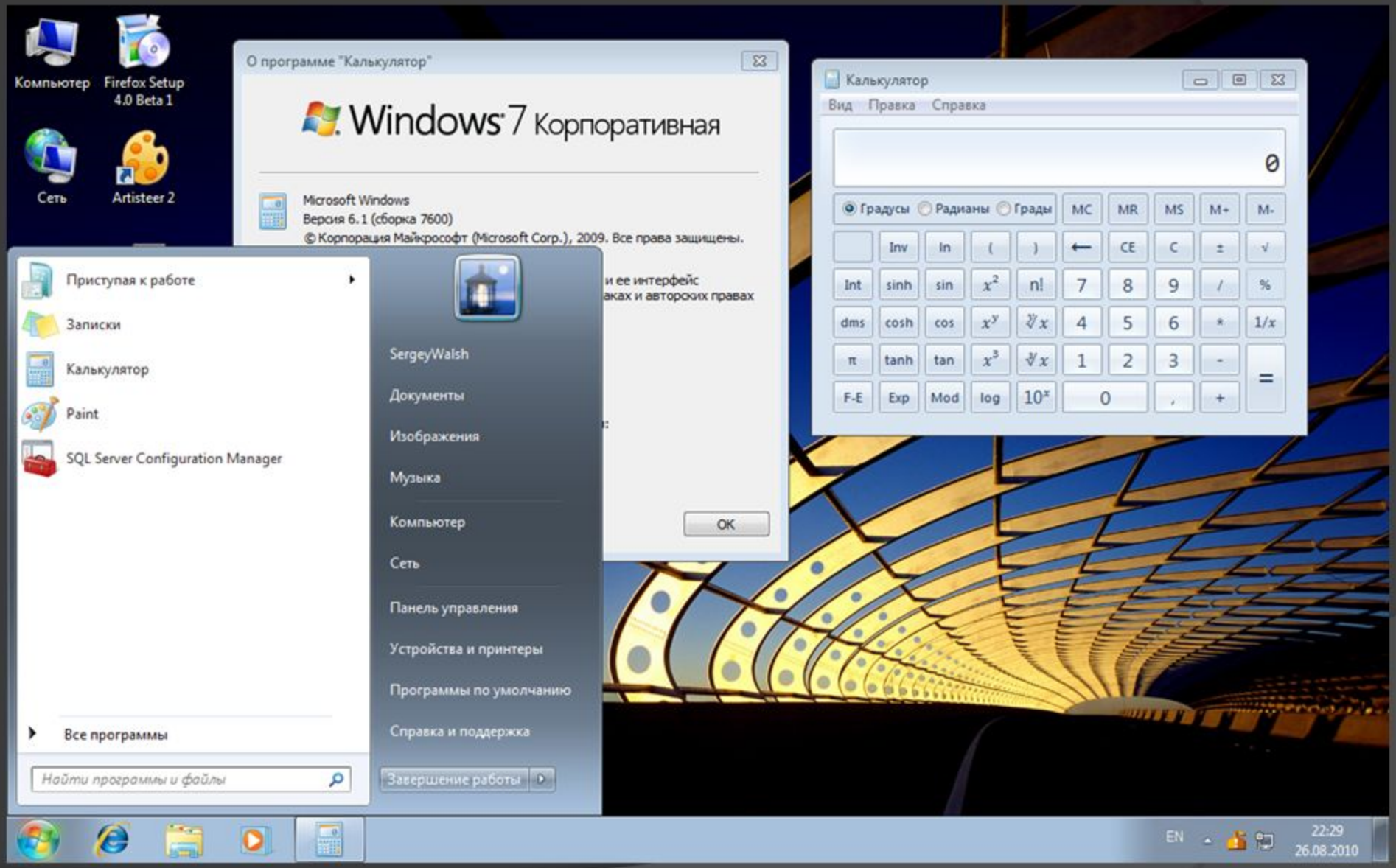


Microsoft®

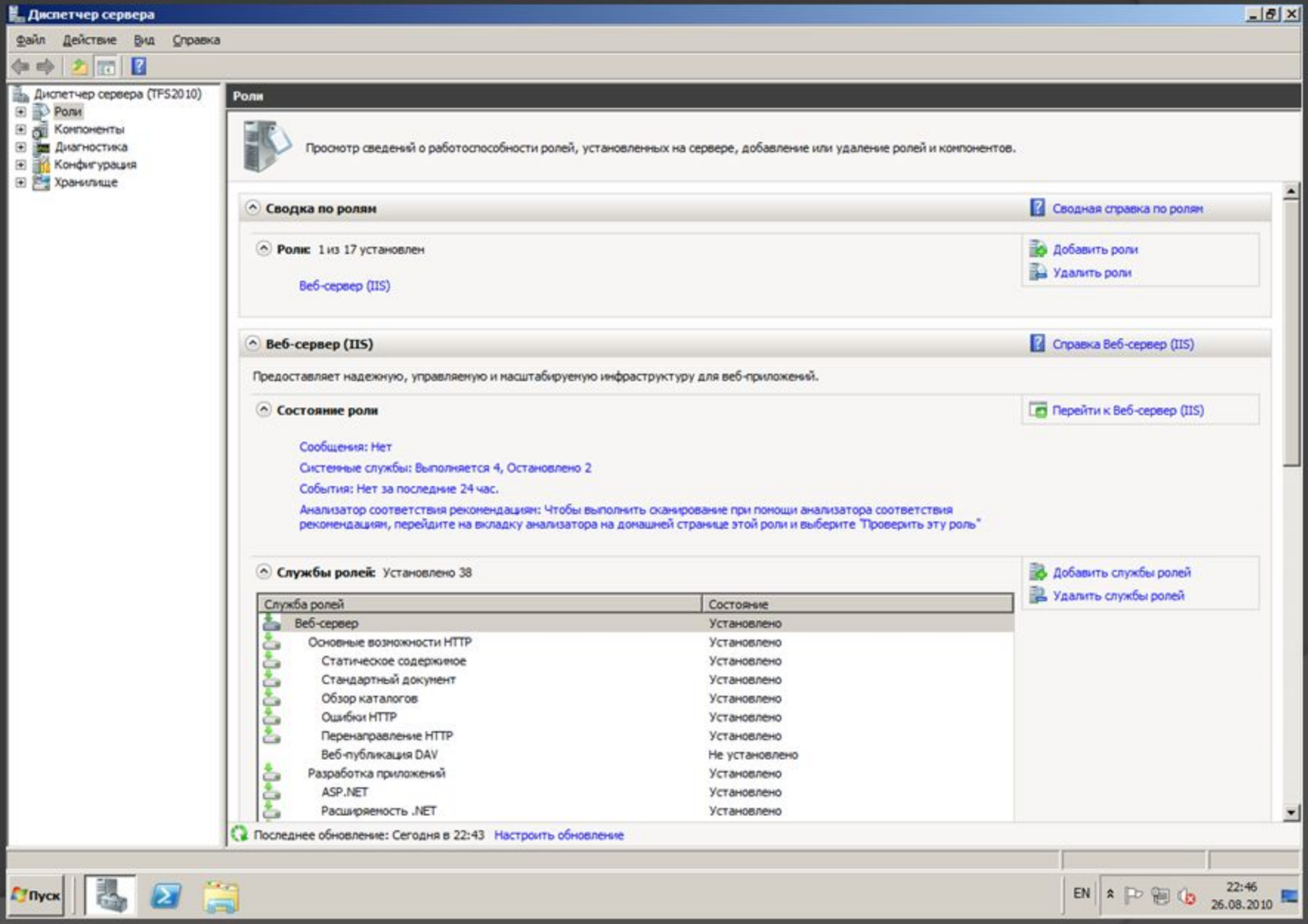
Microsoft Windows XP Professional (x86)



Microsoft Windows 7 Enterprise (x86)



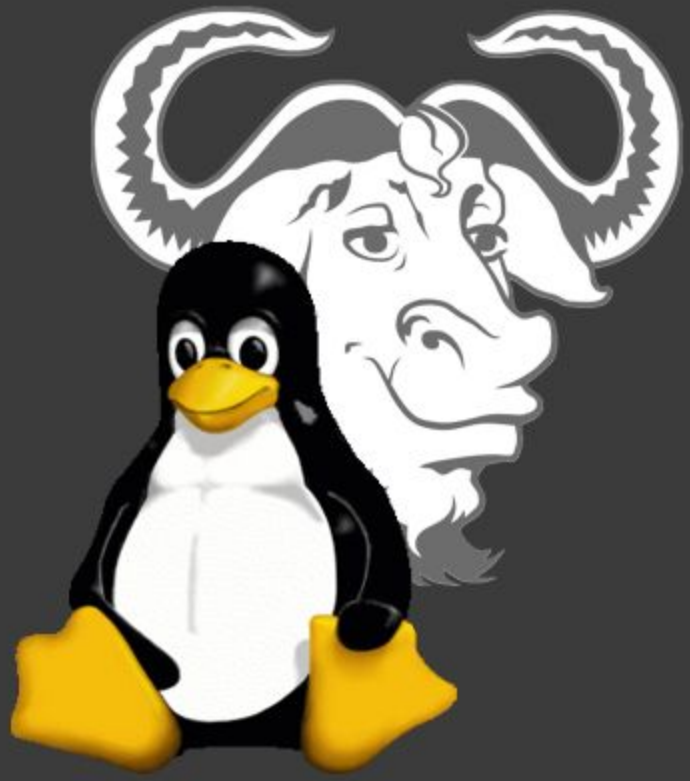
Microsoft Windows Server 2008 R2 DataCenter (x64)



Apple Inc.

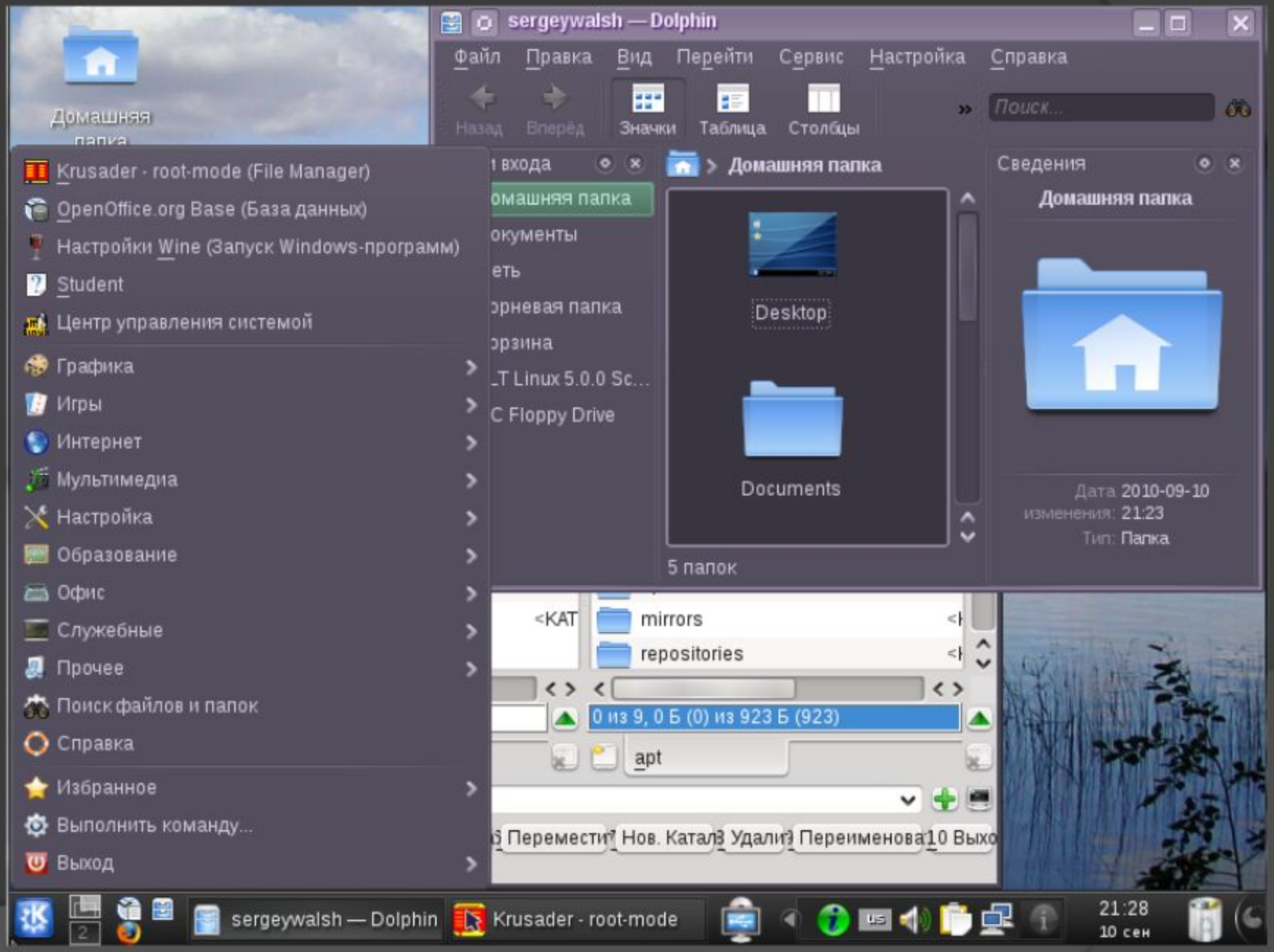
Mac OS X Leopard 10.5.3

Mac OS X Leopard — Док с отражением

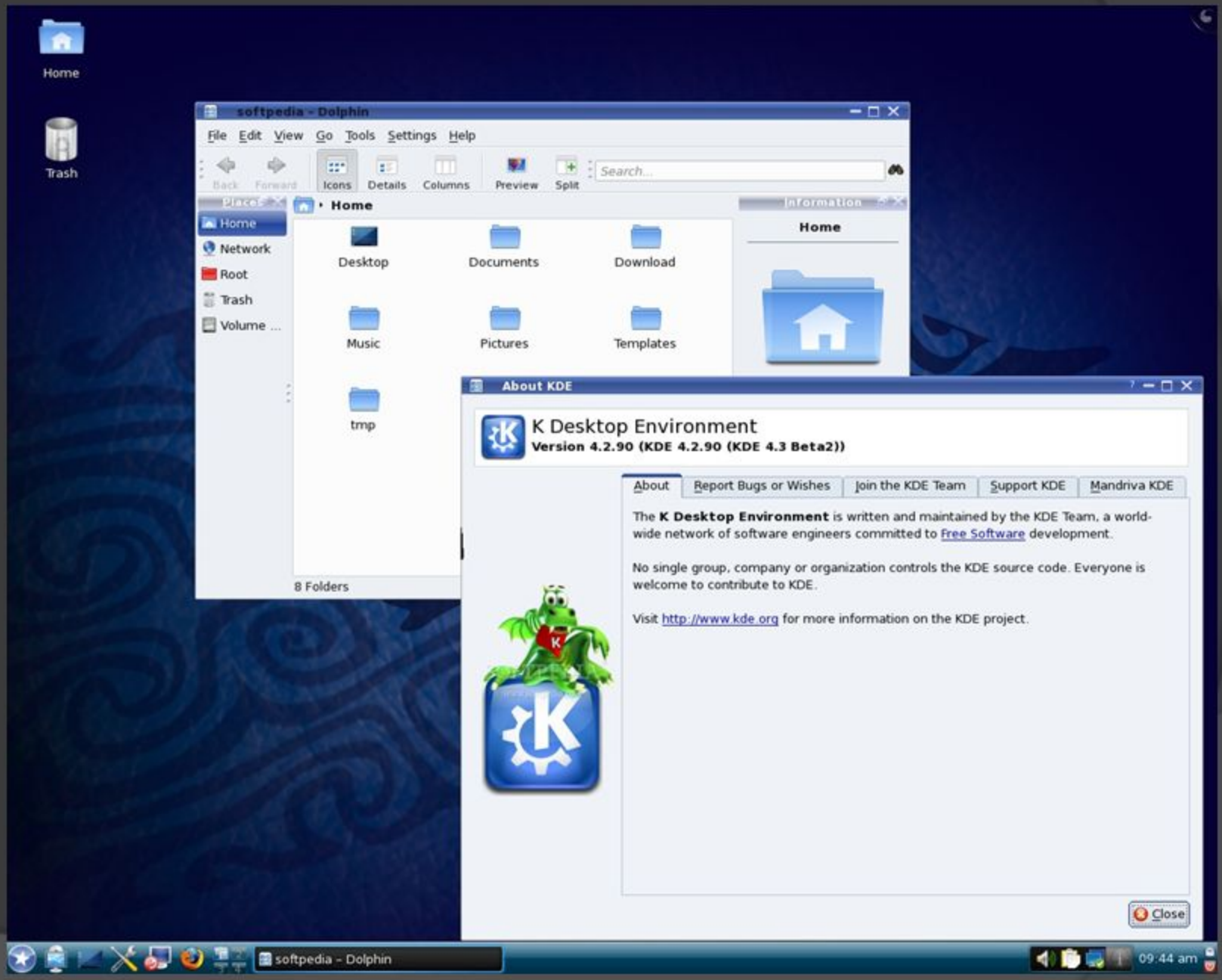


GNU / Linux

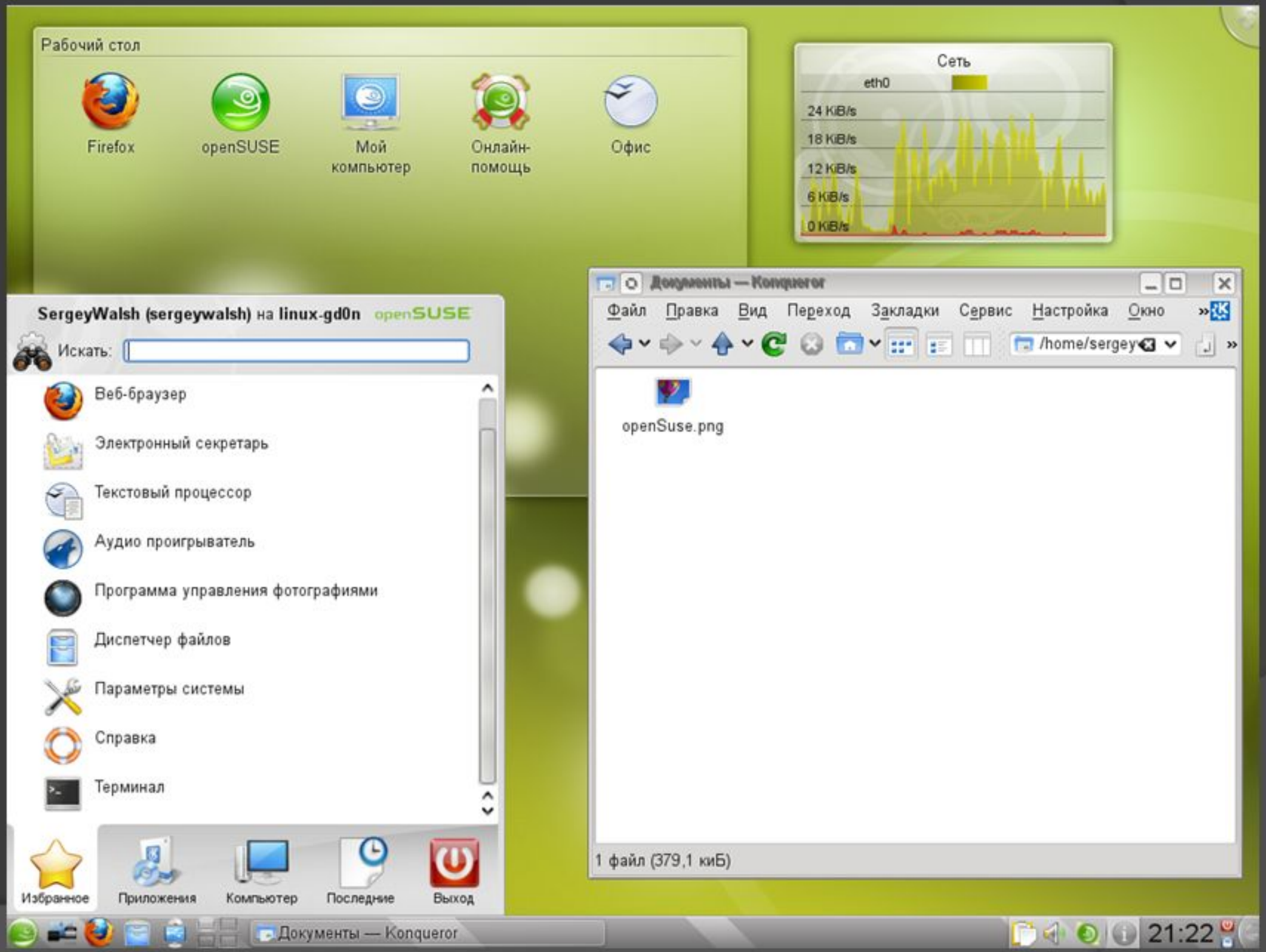
Linux [ALT Linux Master 5.0 (KDE, т.н. Школьный Линукс)]



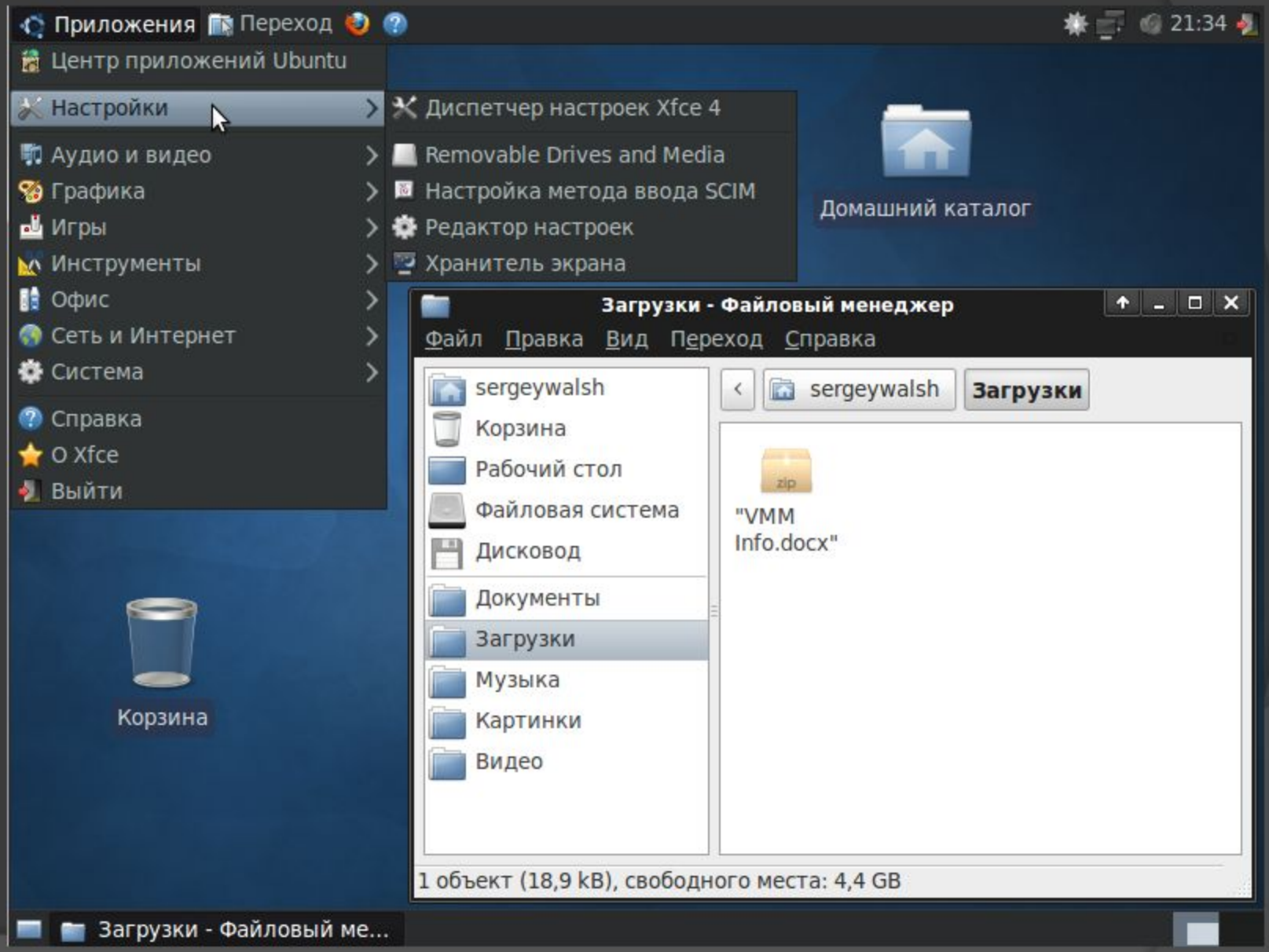
Linux [Mandriva 2010]



Linux [Open SUSE 11.2 (KDE)]



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

- **Создание баз данных**
- **Создание динамических форм для сбора сведений**
- **Получение и отправка почтовых сообщений**
- **Создание презентаций и Веб-страниц**
- **Создание писем, докладов, рефератов и т.д. с графическим оформлением**
- **Выполнение вычислений, построение диаграмм**
- **Создание публикаций, буклетов, Веб-узлов**
- **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*](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 пеатных 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.ritlabs.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

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.

Nero Burning Rom

TheBat

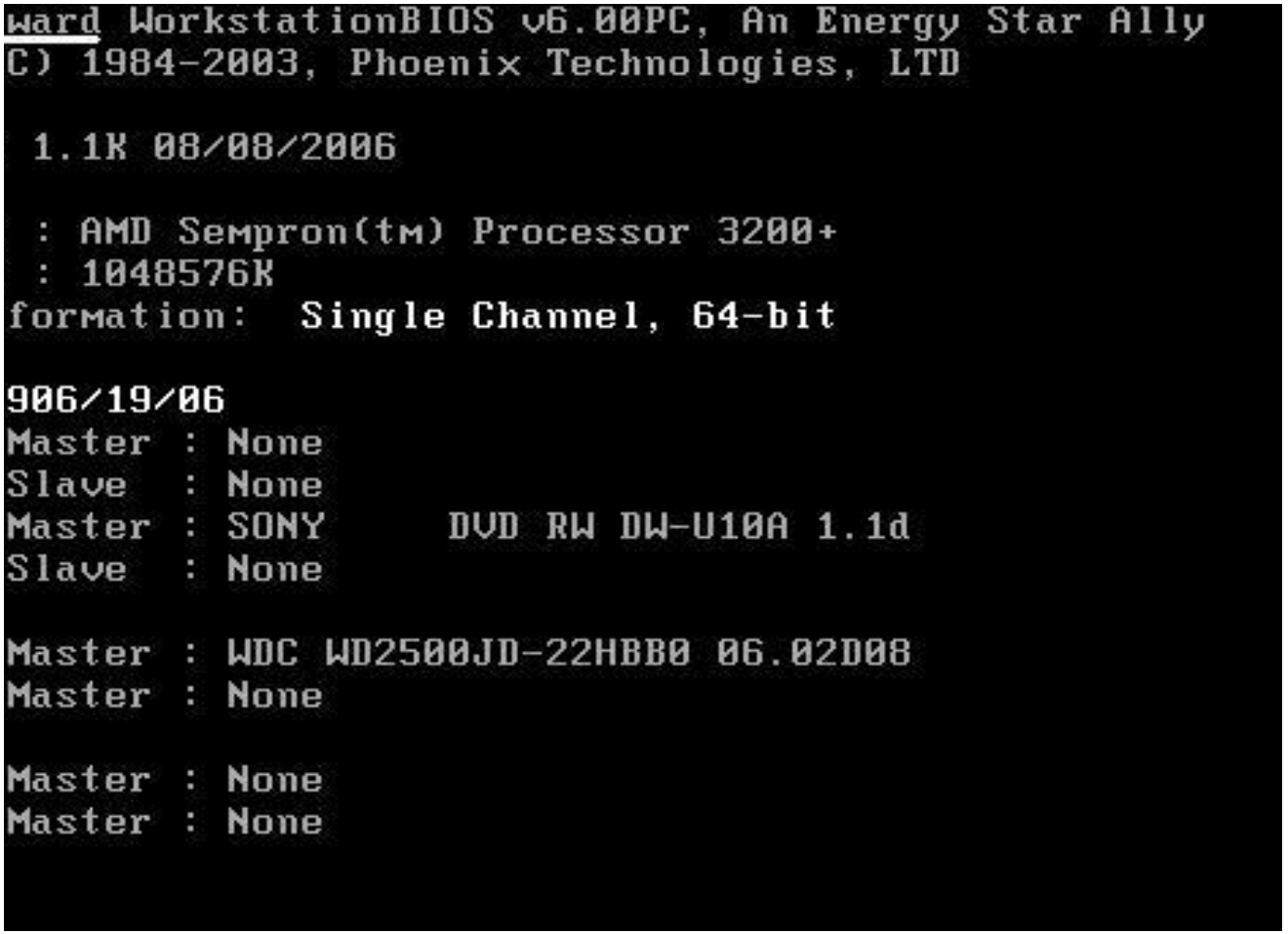
- **Коммерческое ПО**:
  - плата за каждую копию
  - *бесплатная техническая поддержка* (!)
  - запрет на изменение кода и извлечение данных
  - быстрое внесение изменений (сервис-паки, новые версии)

Программное обеспечение

Тема 3. Системные программы

Начальная загрузка ПК

Работает микропрограмма, «зашитая» в чип BIOS



Начальная загрузка ПК

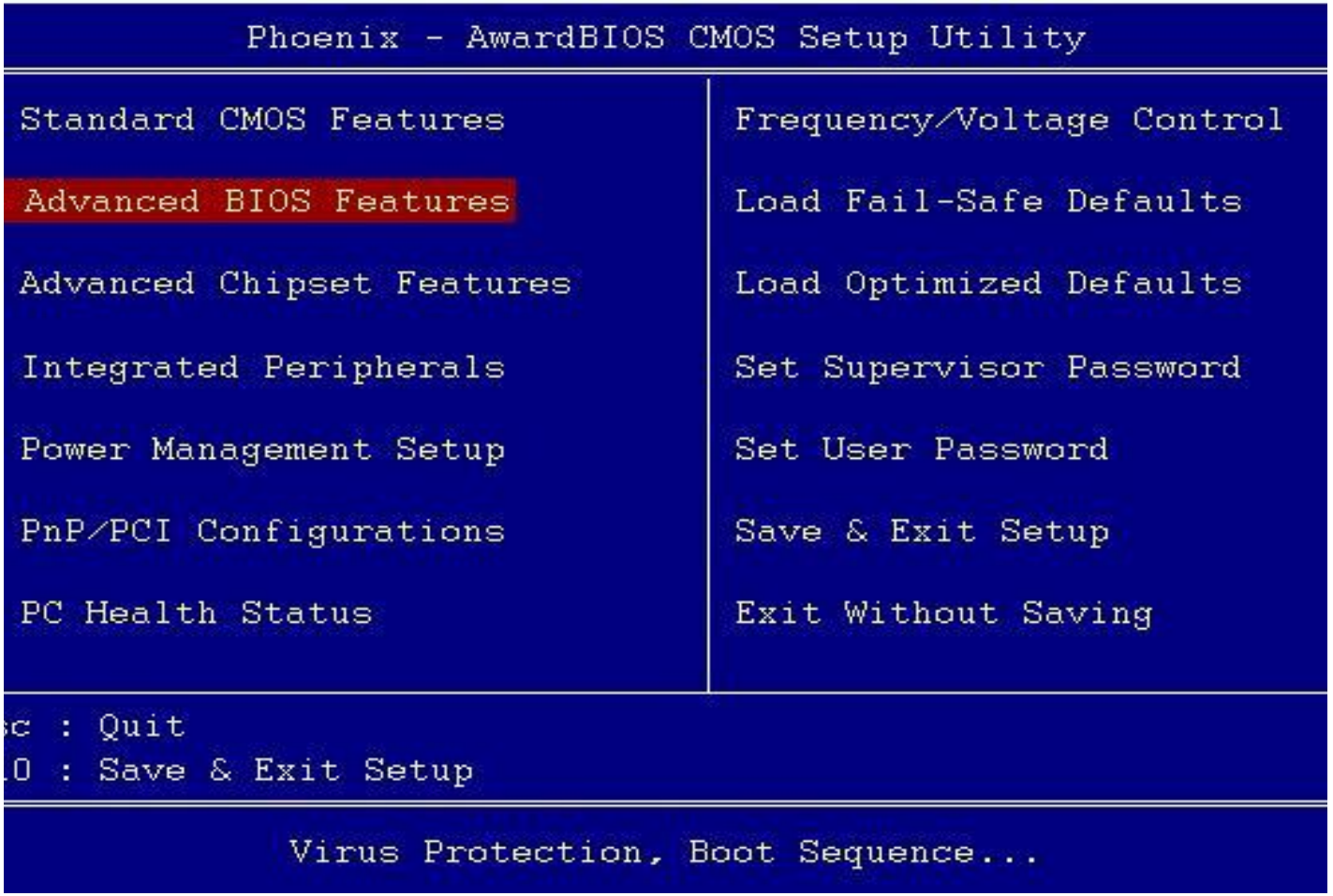
Работает микропрограмма, «зашитая» в чип BIOS – еще один вариант

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 изменениях 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.

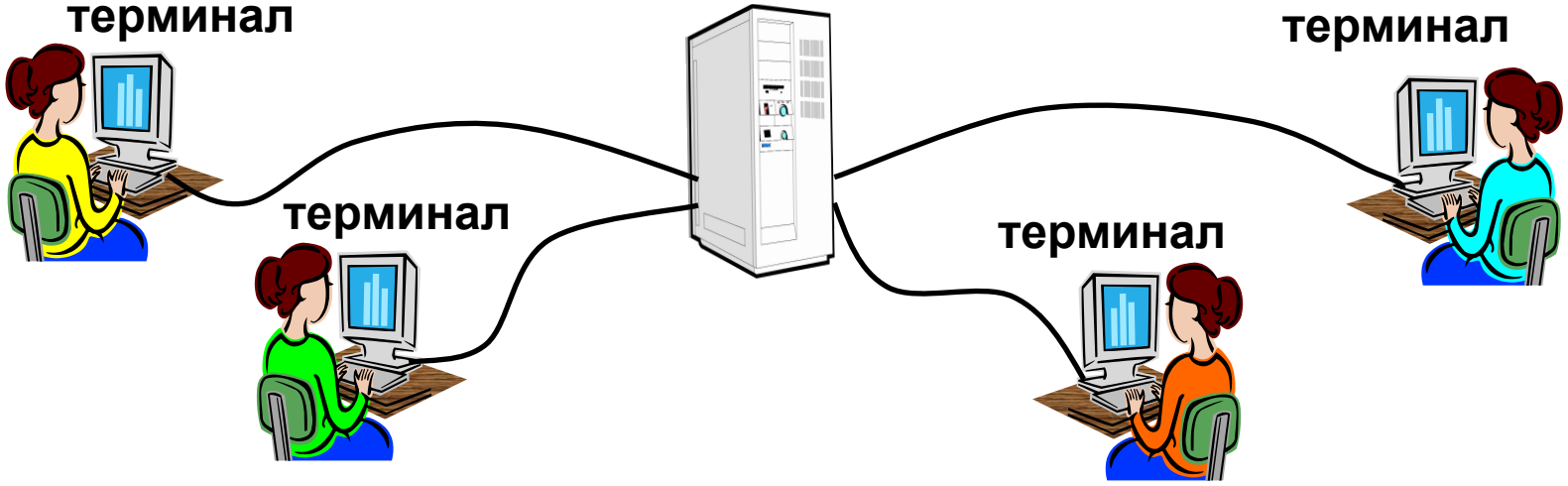
- ***Windows 95/98/Me***
- ***Windows NT/2000/XP/2003/Vista/7***
- ***UNIX*** – надежная сетевая ОС (Интернет)
- ***Linux*** – *UNIX*-подобная ОС
- **QNX** – ОС реального времени

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 Antivirus *www.symantec.com*

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

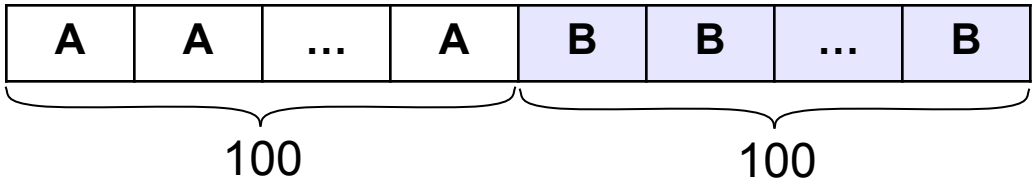
```
*.zip
*.rar
*.7z
```

- **с потерями**: при сжатии часть информации безвозвратно теряется
  - фотографии (`*.jpg`)
  - звук (`*.mp3`)
  - видео (`*.mpg`)

Почему файлы можно сжать?

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

Файл `qq.txt`



200 байт

Файл `qq.rle` (сжатый)

A	100	B	100

4 байта

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 – самораспако-вывающийся*) – 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, ….`**

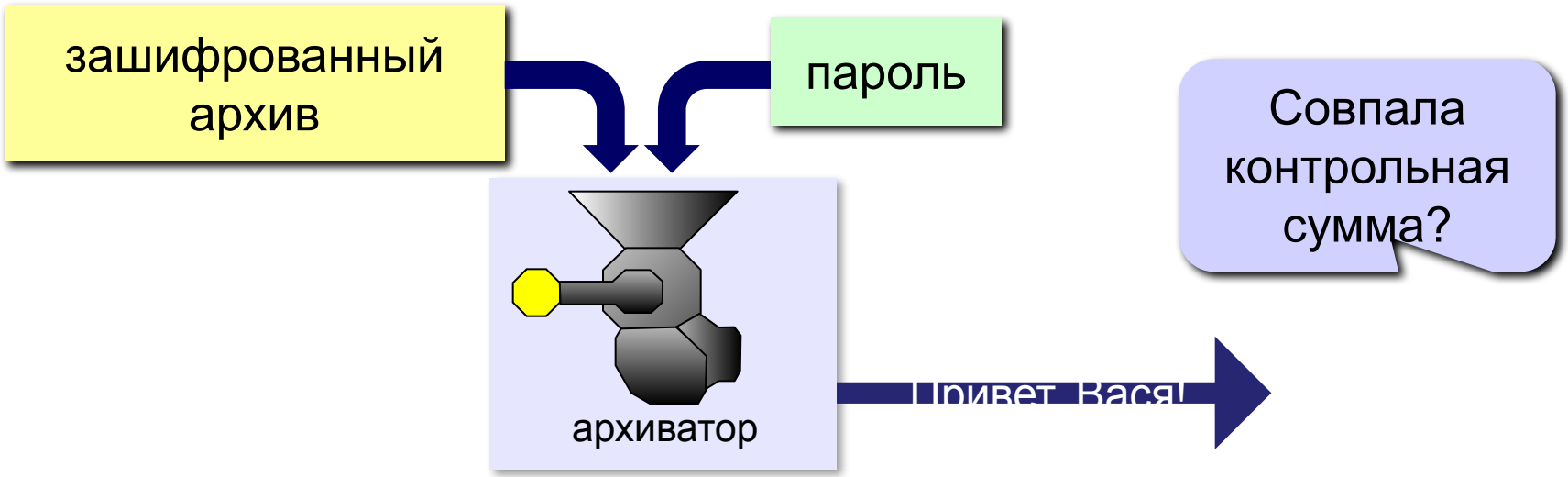
***7Zip*:**

- **`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!



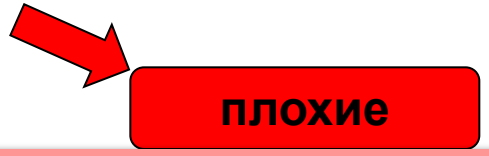
Как составить пароль?

Методы взлома:

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

Пароли

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



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

Архиватор WinRAR (*Е. Рошал*)

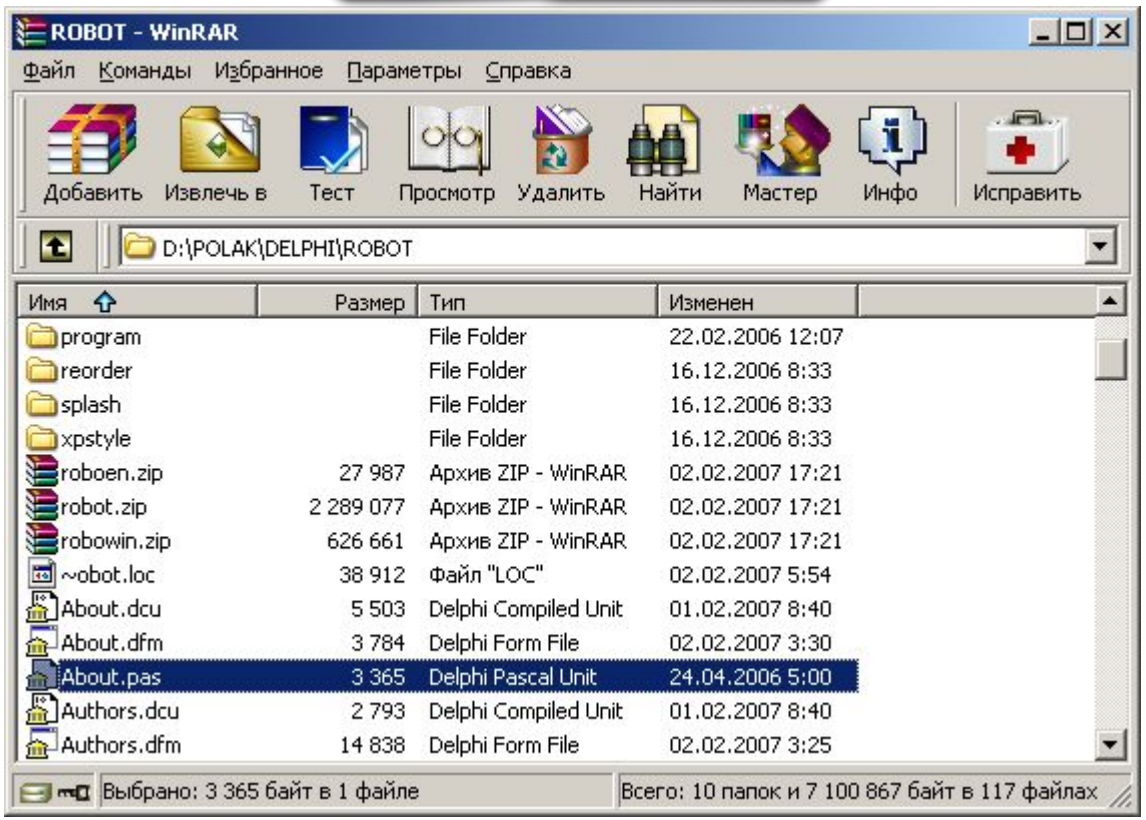
Запуск: *Пуск – WinRAR*

распаковать архив

сжать выделенные файлы

выйти из папки

двойной щелчок ЛКМ: войти в архив

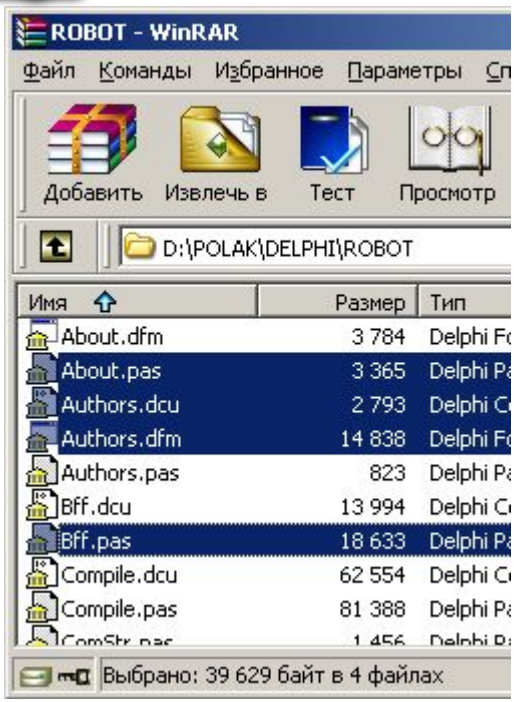


сменить диск

изменить пароль

Архиватор WinRAR: упаковка

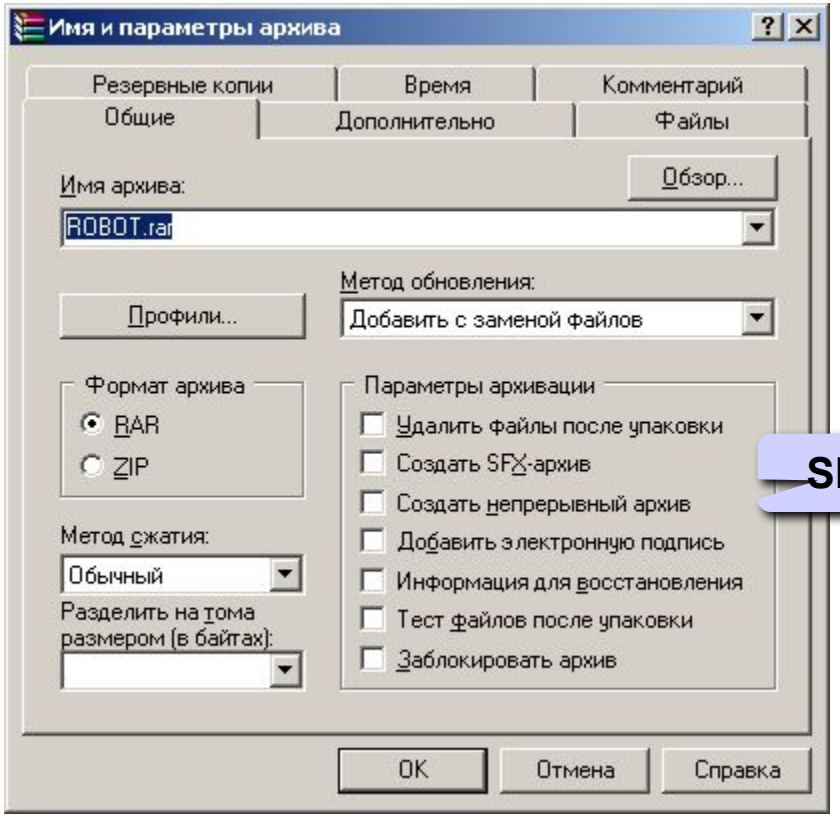
ЛКМ



имя архива

пароль

тип архива

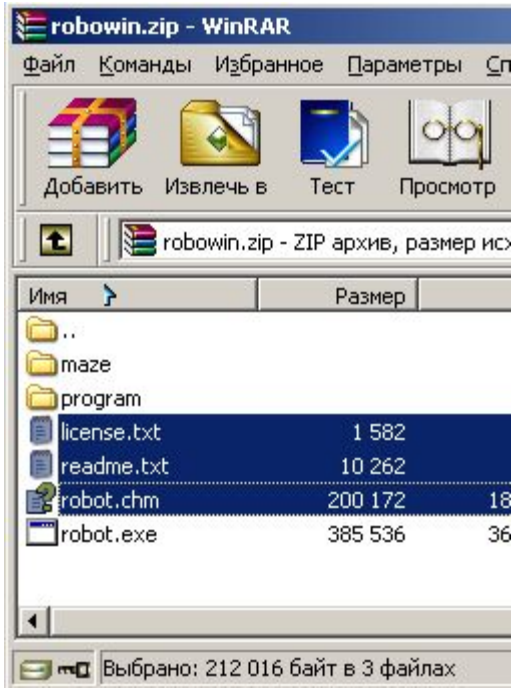


SFX

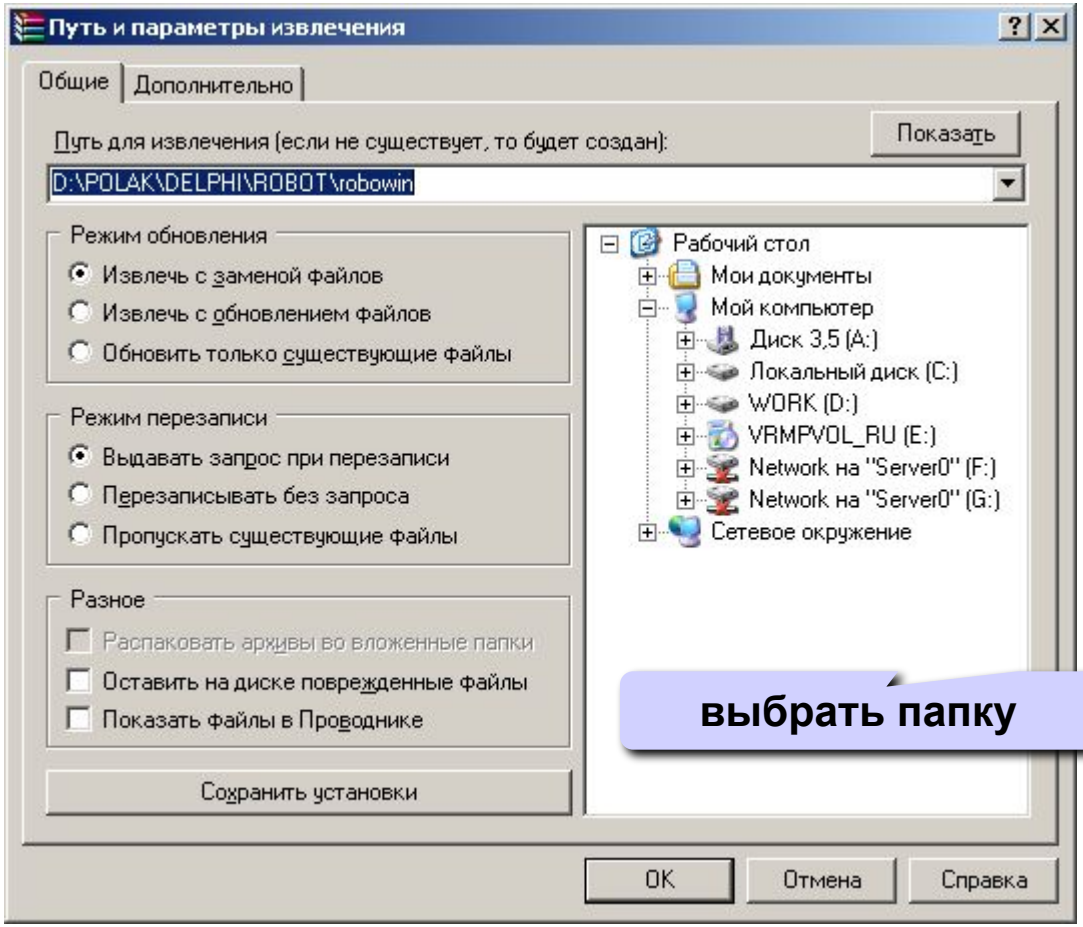
многотомные архивы

Архиватор WinRAR: распаковка

ЛКМ



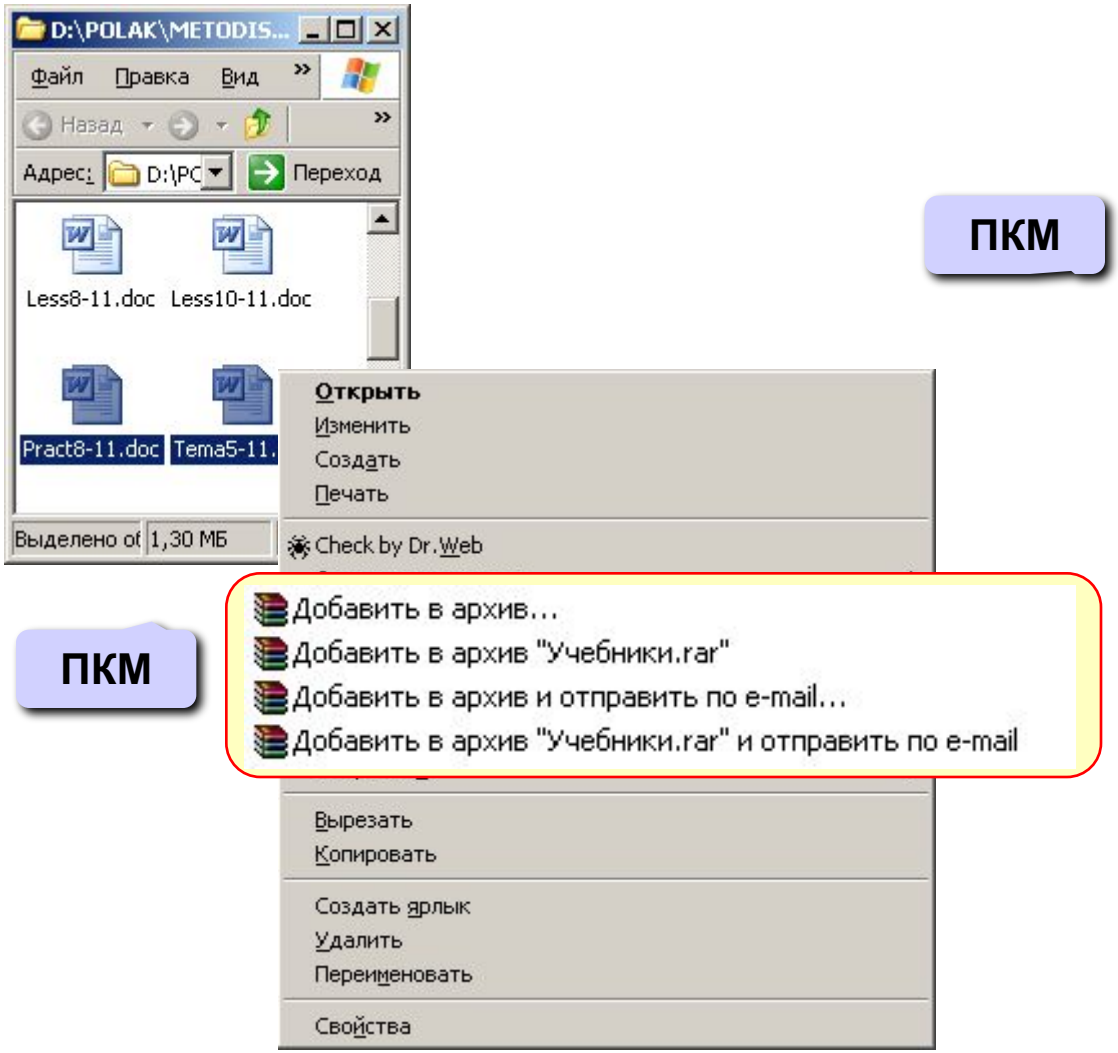
куда распаковать?



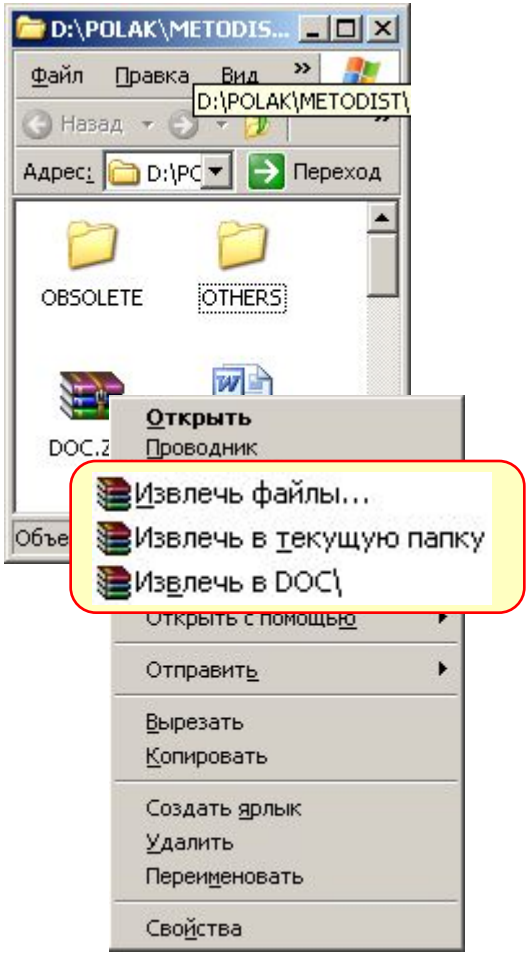
выбрать папку

Архиватор WinRAR в Проводнике

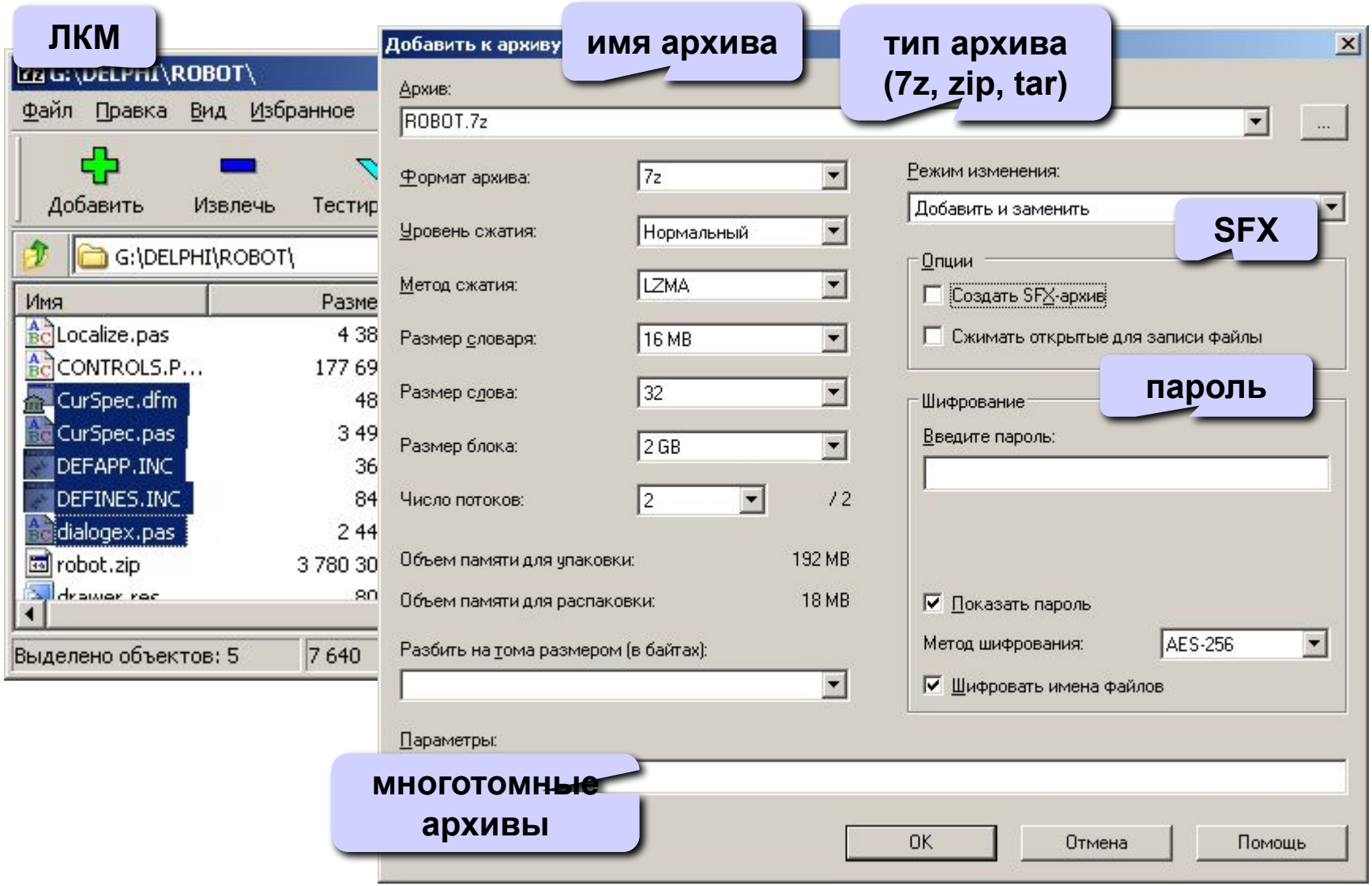
Упаковка



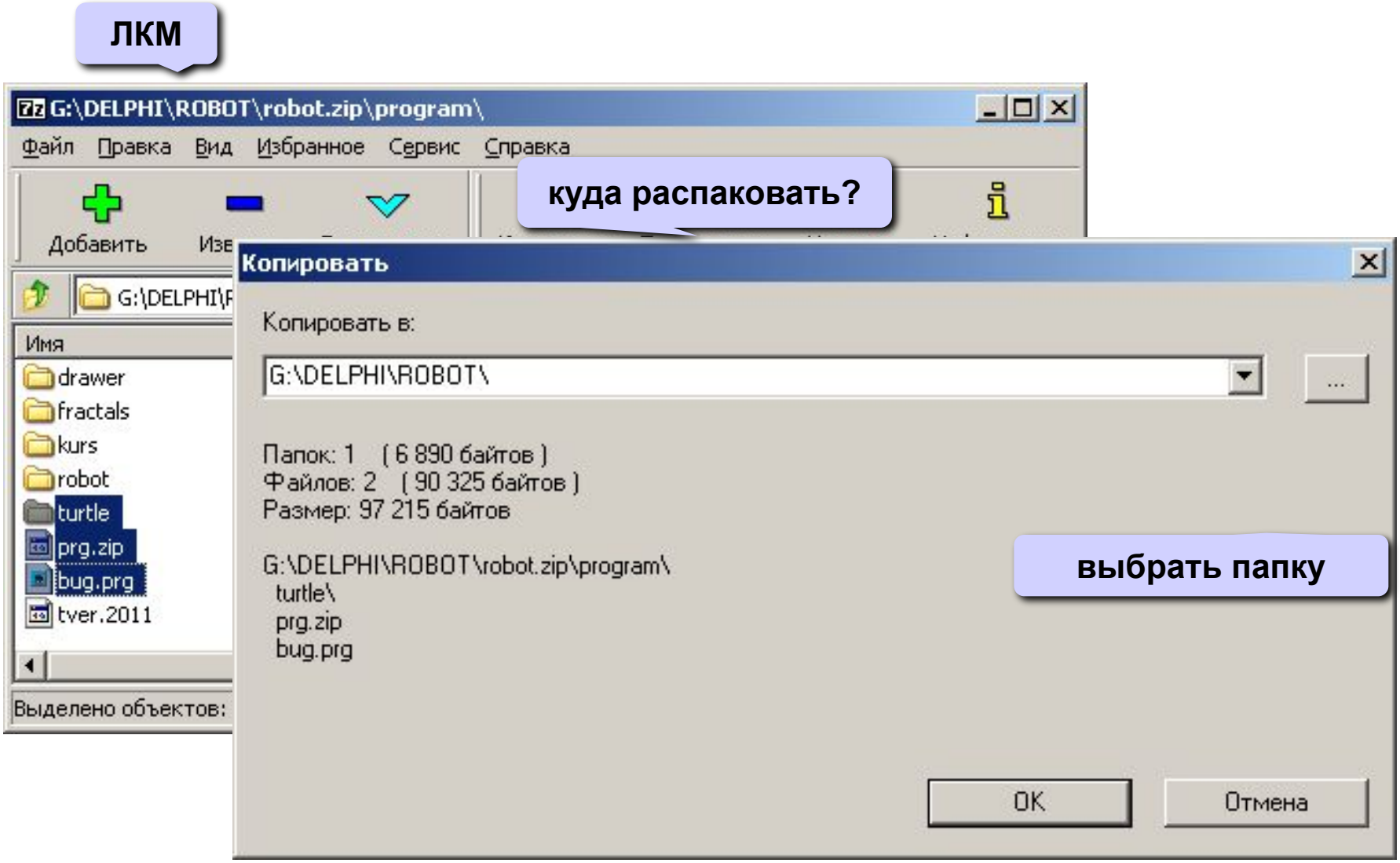
Распаковка



Архиватор 7Zip: упаковка



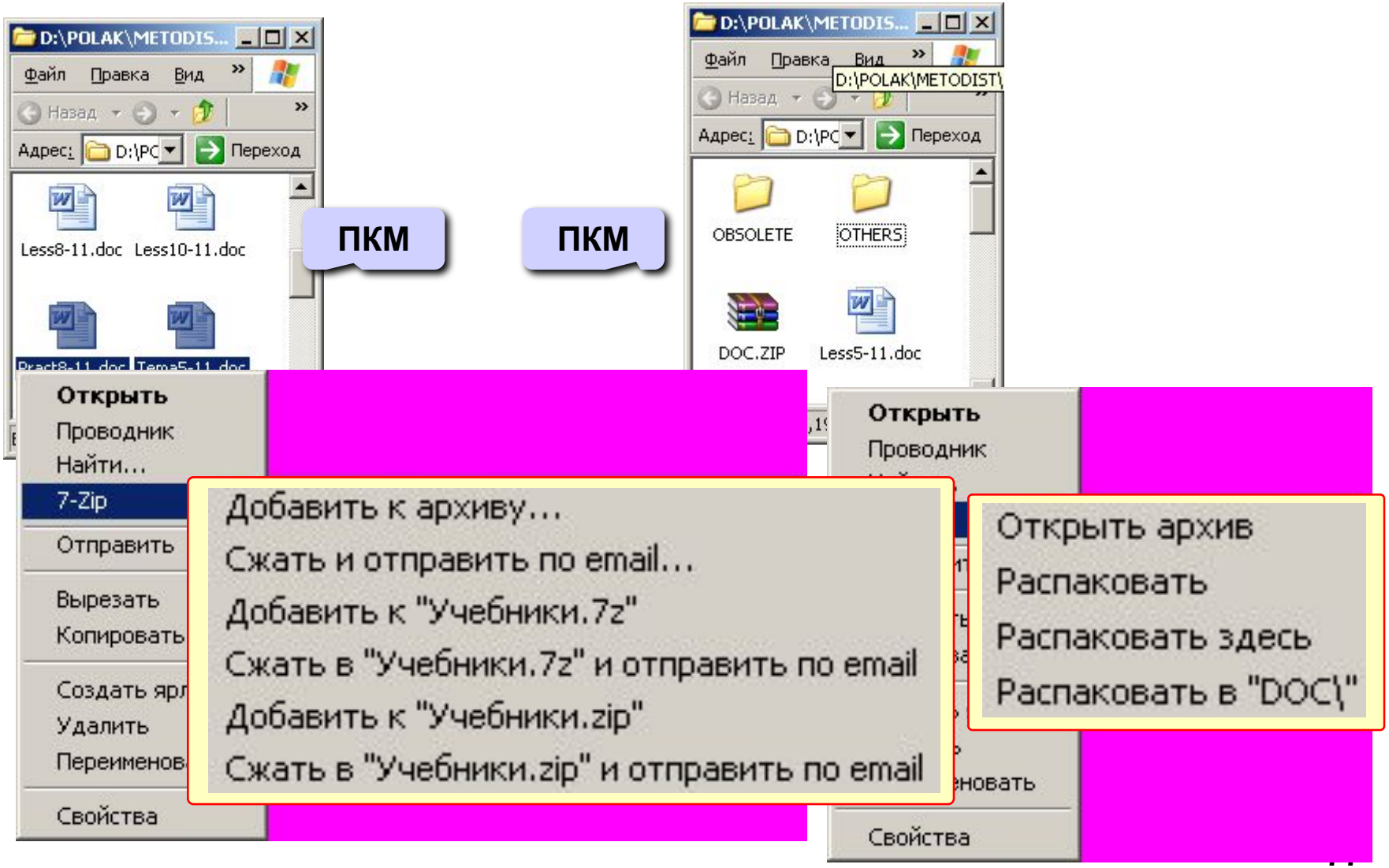
Архиватор 7Zip: распаковка



Архиватор 7Zip в Проводнике

Упаковка

Распаковка



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

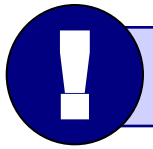
- AVP = Antiviral Toolkit Pro (www.avp.ru) – Е. Касперский

- 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)

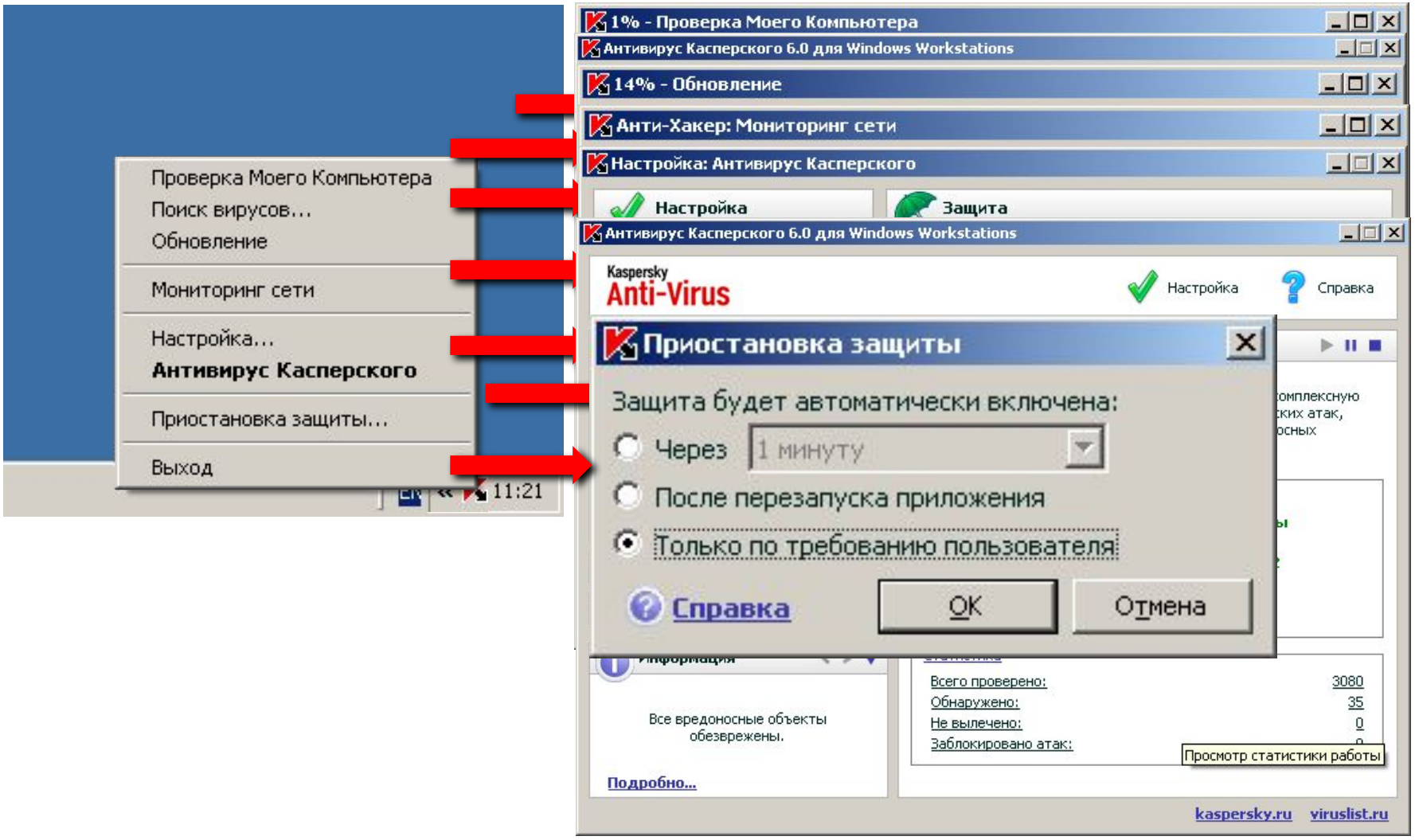
- Antivir Personal (free-av.com)

- AVG Free (free.grisoft.com)

Антивирус *Касперского*

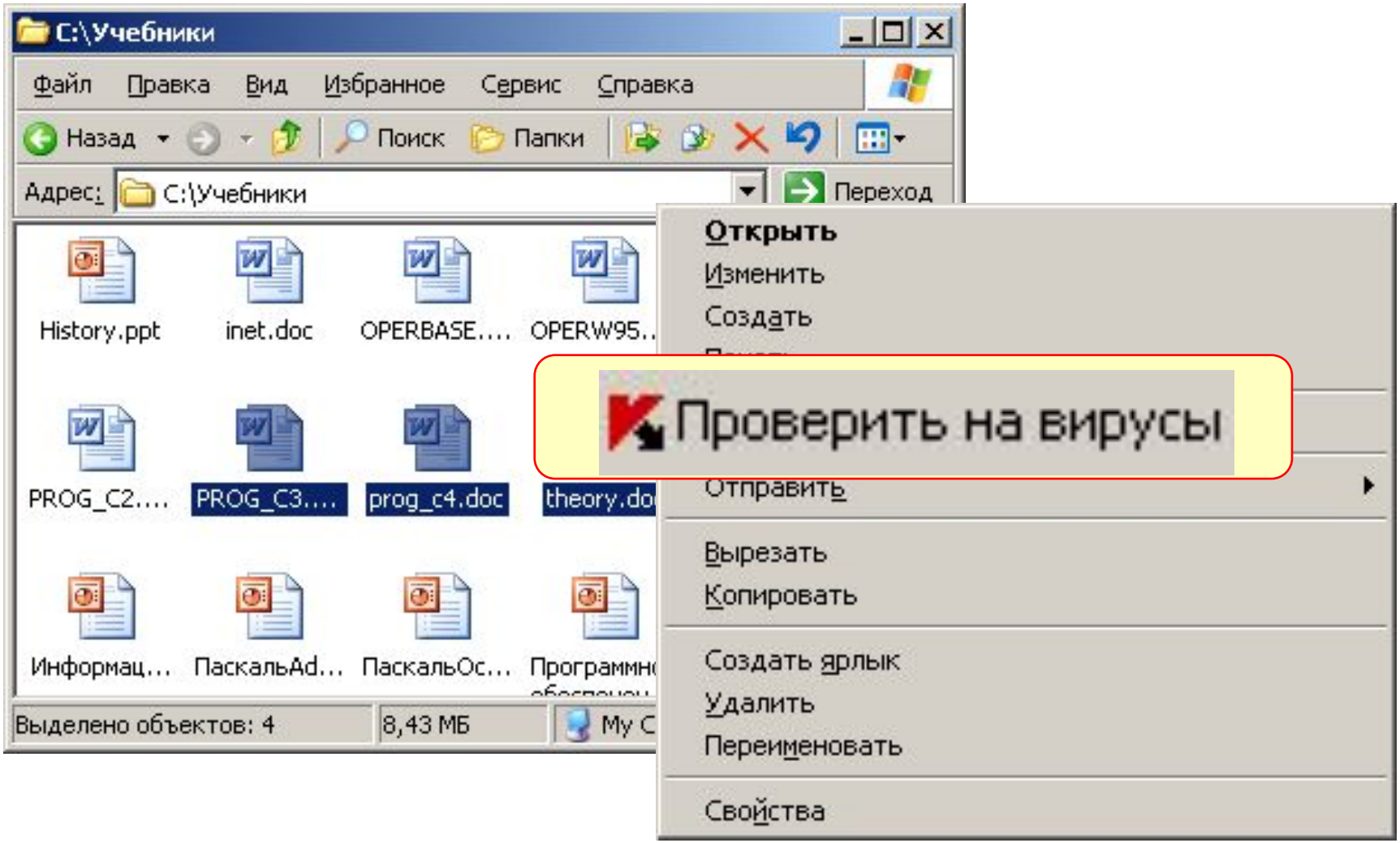
- **Файловый антивирус** (проверка файлов в момент обращения к ним)
- **Почтовый антивирус** (проверка входящих и выходящих сообщений)
- **Веб-антивирус** (Интернет, проверка *Web*-страниц)
- **Проактивная защита** (попытки обнаружить неизвестные вредоносные программы):
  - слежение за реестром
  - проверка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

Антивирус *Касперского*



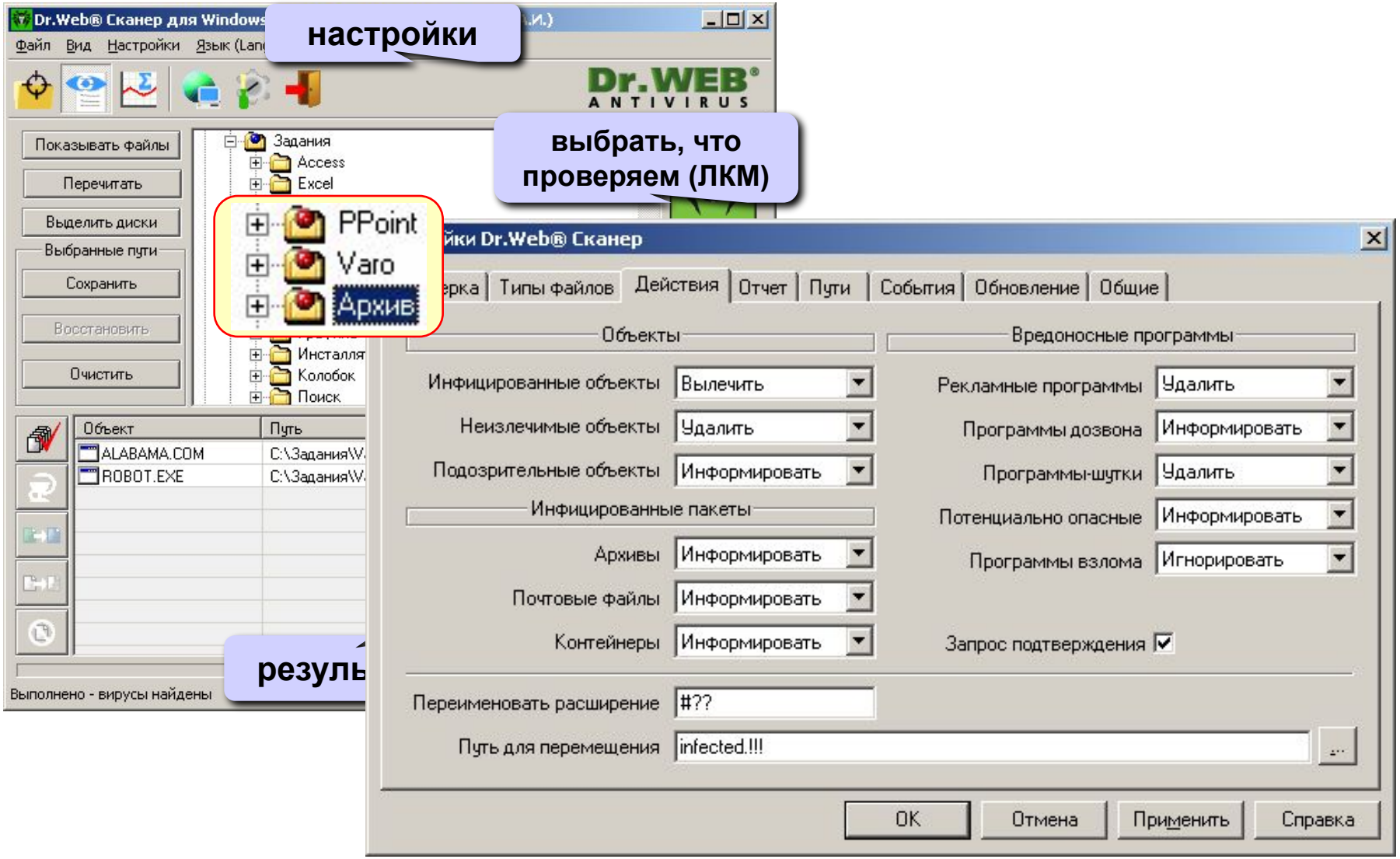
Антивирус *Касперского*

Проводник: запуск через контекстное меню



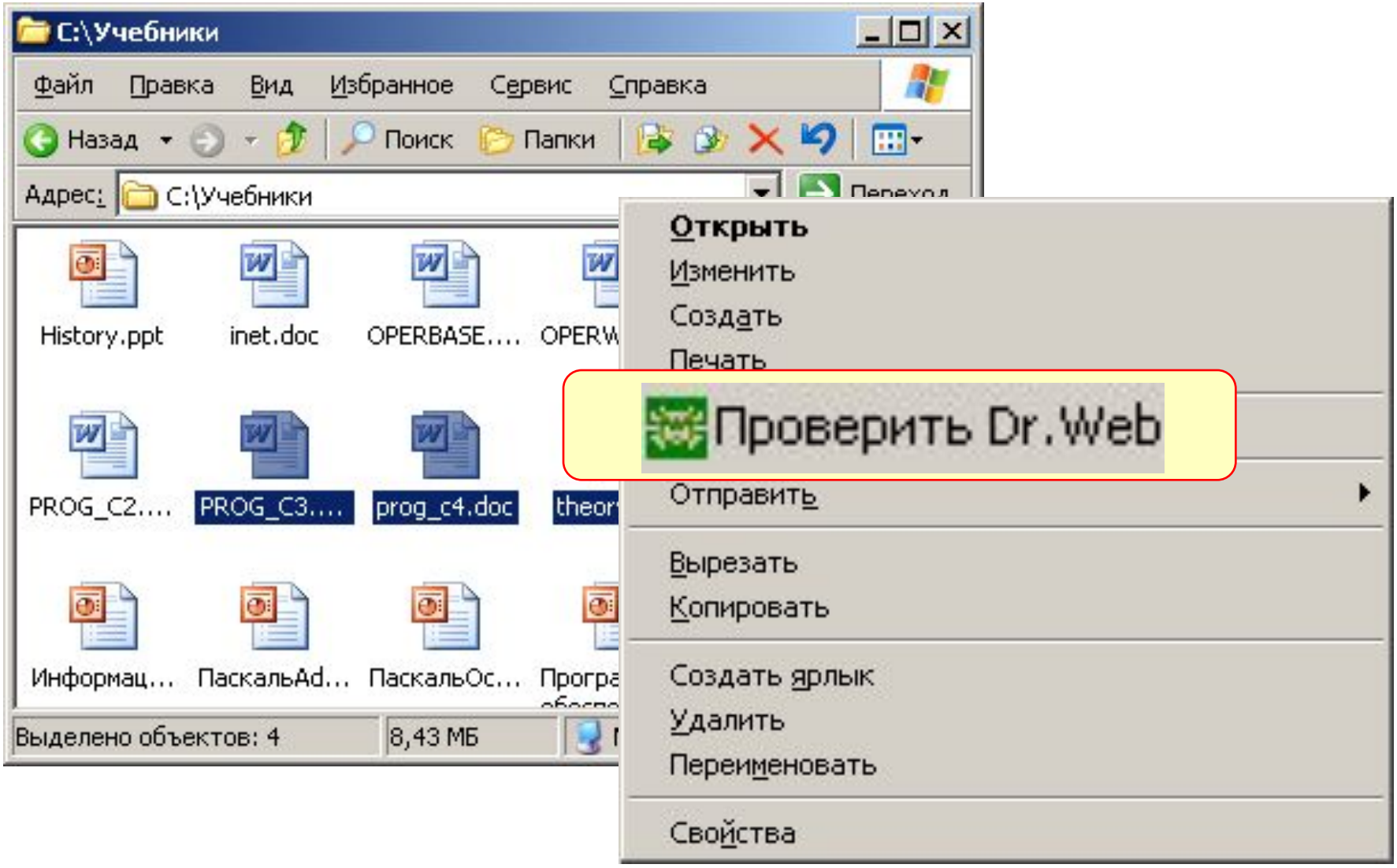
Антивирус *DrWeb* (сканер)

Запуск: *Пуск – Сканер DrWeb*



Антивирус *DrWeb*

Проводник: запуск через контекстное меню



Другие виды антивирусной защиты

брандмауэры (файрволы, сетевые экраны)

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

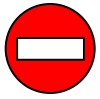
аппаратные антивирусы

- 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…