

# Программное обеспечение

1. [Введение](#)
2. [Прикладные программы](#)
3. [Системные программы](#)
4. [Системы программирования](#)
5. [Правовая охрана программ и данных](#)
6. [Сжатие файлов. Архиваторы](#)
7. [Компьютерные вирусы и антивирусы](#)

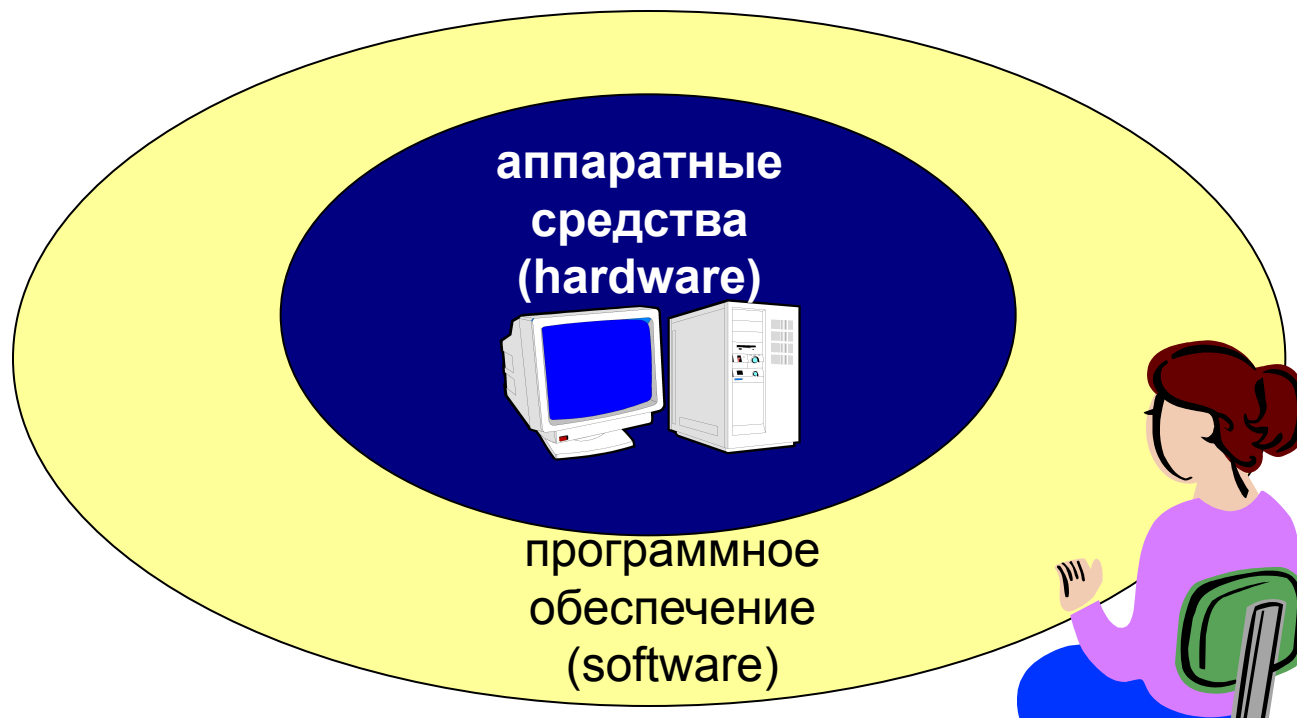
# Программное обеспечение

## Тема 1. Введение

# Программное обеспечение

---

## Взаимодействие человека с компьютером



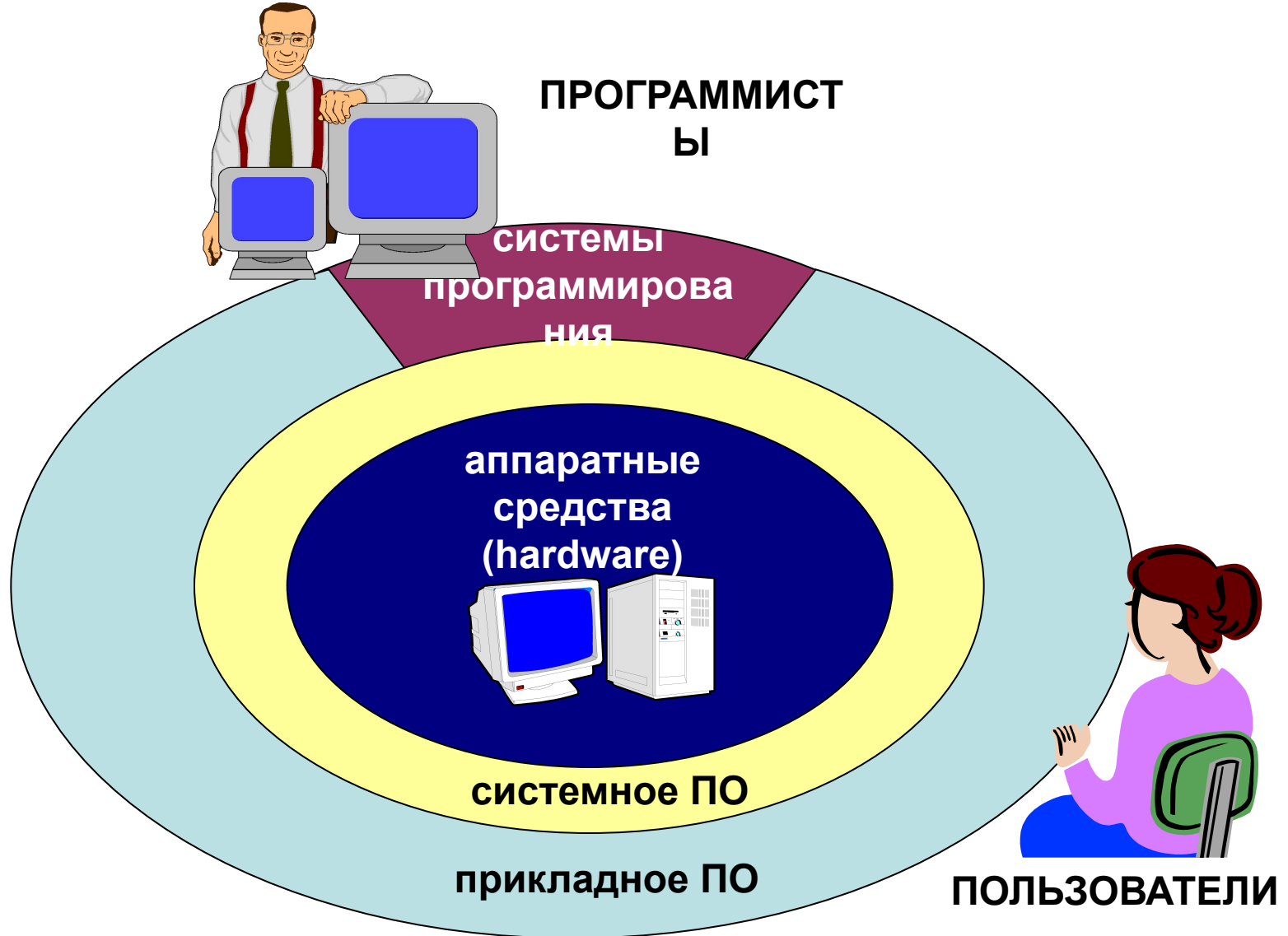
# Программное обеспечение

---

- **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

---



# Программное обеспечение

## Тема 2. Прикладные программы

# 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](http://openoffice.org)

# ПО для обработки изображений

---

## ■ Графические редакторы

*Растровые рисунки:*



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



**Adobe Photoshop** – файлы \*.psd [www.adobe.com](http://www.adobe.com)



**Gimp** – **бесплатно** [www.gimp.org](http://www.gimp.org)



**Paint.NET** – **бесплатно** [www.getpaint.net](http://www.getpaint.net)

*Векторные рисунки:*



**CorelDraw** – файлы \*.cdr [www.corel.com](http://www.corel.com)



**Adobe Illustrator** – файлы \*.ai [www.adobe.com](http://www.adobe.com)



**Inkscape** – **бесплатно** [www.inkscape.org](http://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](http://www.pinnaclesys.ru)



**Adobe Premier**

[www.adobe.com](http://www.adobe.com)

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



**Microsoft Publisher**



**QuarkXPress** [www.quark.com](http://www.quark.com)



**Adobe InDesign** [www.adobe.com](http://www.adobe.com)



**Scribus** – **бесплатно** <http://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](http://www.mozilla.org)



**Opera** – **бесплатно** [www.opera.com](http://www.opera.com)



**Safari** – **бесплатно** [www.apple.com](http://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](http://www.rttlabs.com)



**Mozilla Thunderbird** – **бесплатно**

[www.mozilla-russia.org](http://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)



# Использование программ

---

## Основания:

- *договор* в письменной форме
- при массовом распространении – *лицензионное соглашение* на экземпляре

## Можно без разрешения автора:

- хранить в памяти *1 компьютера* (или по договору)
- вносить *изменения*, необходимые для работы на компьютере пользователя (но не распространять!)
- исправлять явные *ошибки*
- изготовить *копию* для архивных целей
- *перепродать* программу

# Программное обеспечение

## Тема 3. Системные программы

# 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* – бесплатная *UNIX*-подобная ОС
- *QNX* – ОС реального времени

# Типы ОС

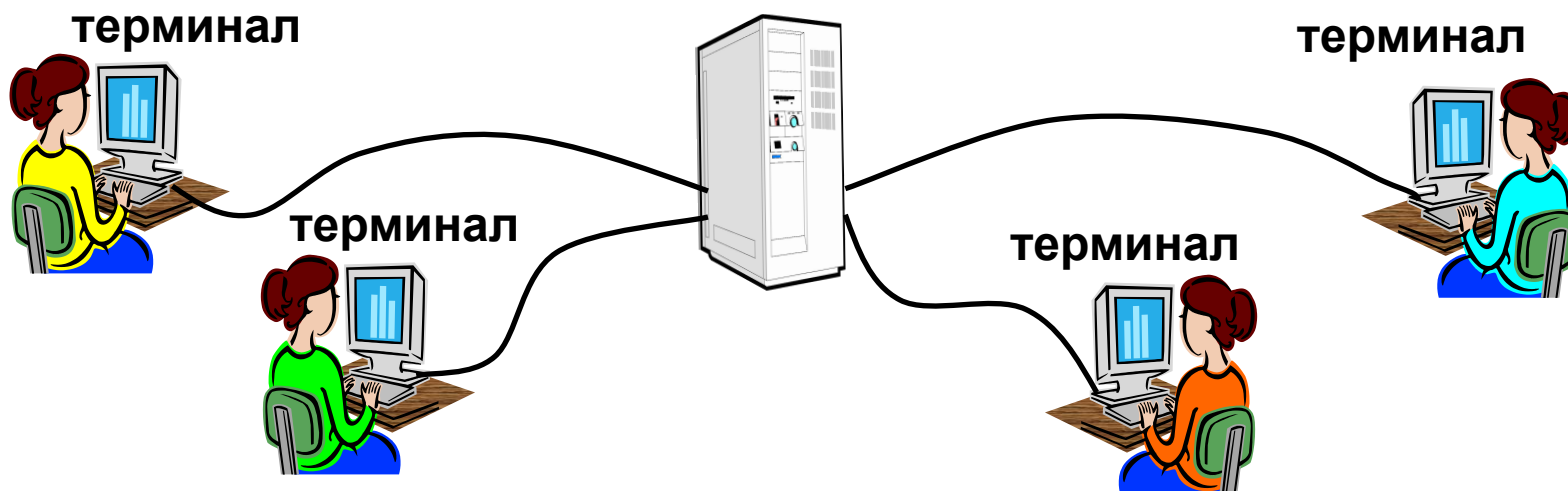
---

**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](http://www.avp.ru)



**DrWeb**, И. Данилов [www.drweb.com](http://www.drweb.com)

NORTON



**Norton Antivirus** [www.symantec.com](http://www.symantec.com)



**McAfee**

[www.mcafee.com](http://www.mcafee.com)



**NOD32** [www.eset.com](http://www.eset.com)

## ■ архиваторы – программы для упаковки файлов



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

[www.rarsoft.com](http://www.rarsoft.com)



**WinZIP** – архивы \*.zip – [www.winzip.com](http://www.winzip.com)

# Утилиты, не входящие в ОС

---

- информация о системе



**Everest** [www.lavalys.com](http://www.lavalys.com)



**SiSoft – бесплатно** [www.sisoftware.net](http://www.sisoftware.net)

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



**Nero Burning ROM** [www.nero.com](http://www.nero.com)



**DeepBurner Free – бесплатно**

[www.deepburner.com](http://www.deepburner.com)

# Программное обеспечение

## Тема 4. Системы программирования (инструментальные средства)



# Системы программирования

---

**Системы программирования (или инструментальные средства)** – это ПО, предназначенное для разработки и отладки новых программ.

## Проблема:

- компьютеры понимают только **язык кодов** (последовательность нулей и единиц)
- для человека удобнее давать задания на **естественном языке** (русском, английском)

## Компромисс:

программы составляются на **языках программирования** и затем переводятся в коды с помощью специальных программ

# Языки программирования

---

Всего более 600, широко используется примерно 20.

## Машинно-ориентированные языки:

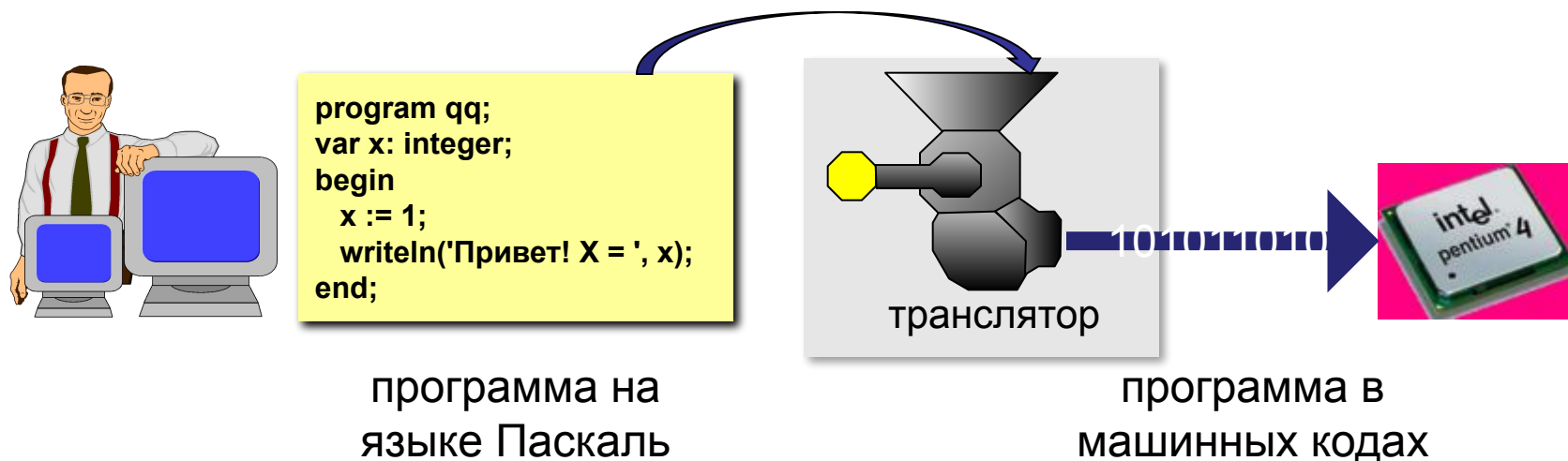
- **машинные коды:** 09 FE AC 3F
- **ассемблеры:** символическая запись машинных команд:  
mov AX, BX
- **макросассемблеры:** одна команда языка заменяет несколько машинных команд

## Языки высокого уровня (алгоритмические):

- **для обучения:** Бейсик (1965), Паскаль (1970), Лого, Рапира
- **профессиональные:** Си (1972), Паскаль (Delphi), Фортран (1957), Visual Basic
- **для задач искусственного интеллекта:** ЛИСП, Пролог
- **для параллельных вычислений:** Ада
- **для программирования в Интернете:** JavaScript, Java, PHP, Perl, ASP, ...

# Трансляторы

**Транслятор** – это программа, которая переводит текст других программ в машинные коды.



**Могут ли быть ошибки в трансляторах?**

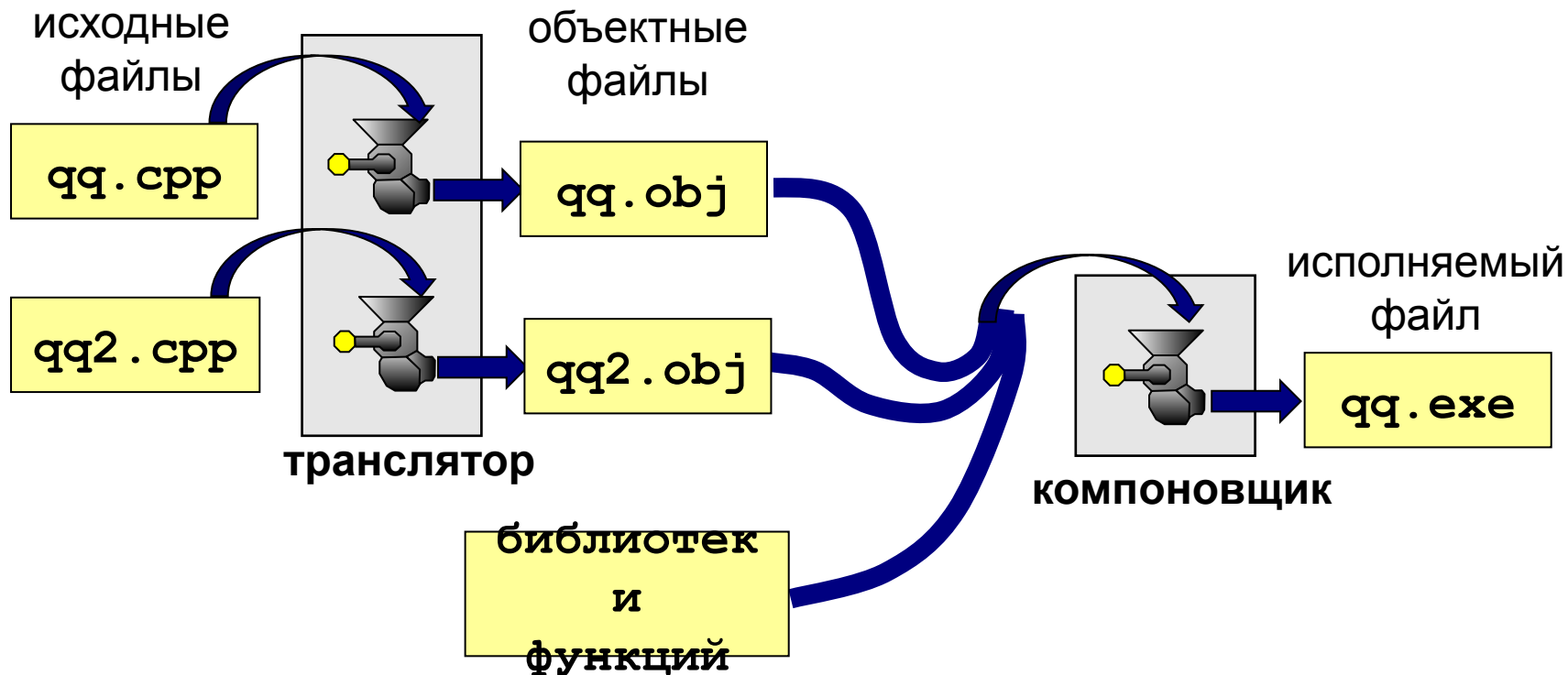
# Типы трансляторов

---

- **интерпретатор** – переводит в коды 1 строчку программы и сразу ее выполняет;
  - ⊕ ▪ удобнее отлаживать программу
  - ⊖ ▪ программы работают медленно (цикл из 400 шагов!)
    - для выполнения программы нужен транслятор
- **компилятор** – переводит в коды сразу всю программу и создает независимый исполняемый файл (\*.exe);
  - ⊖ ▪ сложнее отлаживать программу
  - ⊕ ▪ программы работают быстро
    - для выполнения программы не нужен транслятор

# Компоновщик

**Компоновщик (редактор связей, *Linker*)** – это программа, которая объединяет части одной программы и библиотечные функции в один исполняемый файл.



# Другие программы

---

**Отладчик** (англ. *debugger*) – это программа, которая облегчает поиск ошибок в других программах (их отладку).

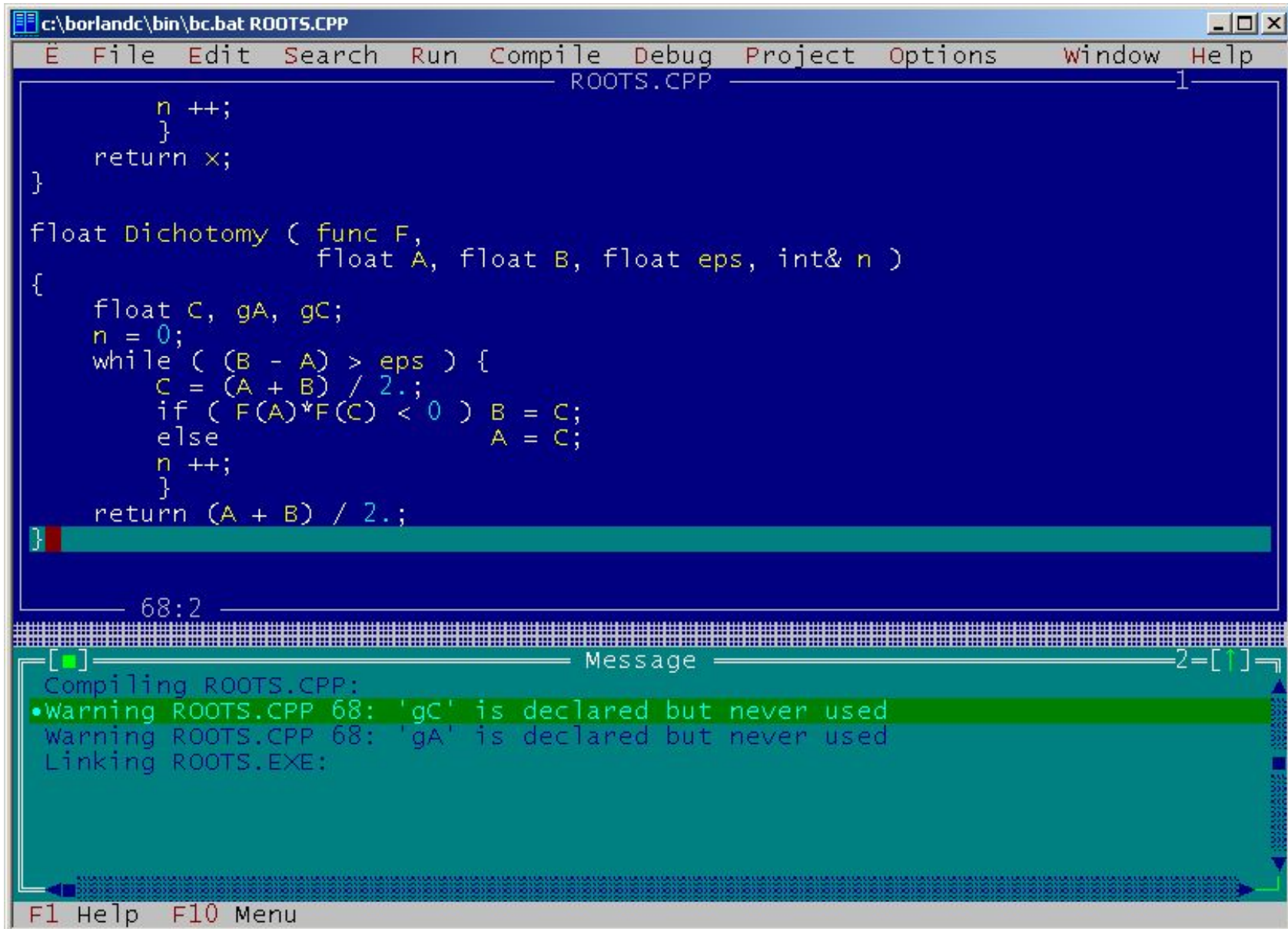
## **Возможности:**

- пошаговое выполнение
- «выполнить до курсора»
- просмотр и изменение значений переменных
- точки останова (англ. *breakpoints*)

**Профайлер** (англ. *profiler*) – это программа, которая определяет, сколько времени занимает выполнение каждой процедуры (и каждой команды) в программе в процентах от общего времени работы.

**Цель:** определить, какие части программы «тормозят» ее (англ. *bottleneck* – бутылочное горлышко), именно их и надо оптимизировать.

# Интегрированная среда разработки



The image shows a screenshot of the Borland C++ IDE. The main window displays the source code for a C++ program named ROOTS.CPP. The code implements a function called Dichotomy, which uses a binary search algorithm to find the root of a function F. The code is as follows:

```
    n ++;
  }
  return x;
}

float Dichotomy ( func F,
                 float A, float B, float eps, int& n )
{
  float C, gA, gC;
  n = 0;
  while ( (B - A) > eps ) {
    C = (A + B) / 2.;
    if ( F(A)*F(C) < 0 ) B = C;
    else A = C;
    n ++;
  }
  return (A + B) / 2.;
}
```

The status bar at the bottom of the editor window shows the current cursor position as 68:2.

Below the editor window is a Message window. It displays the output of the compilation process:

```
Compiling ROOTS.CPP:
•Warning ROOTS.CPP 68: 'gC' is declared but never used
Warning ROOTS.CPP 68: 'gA' is declared but never used
Linking ROOTS.EXE:
```

The Message window also shows the status bar with the text "2-[↑]".

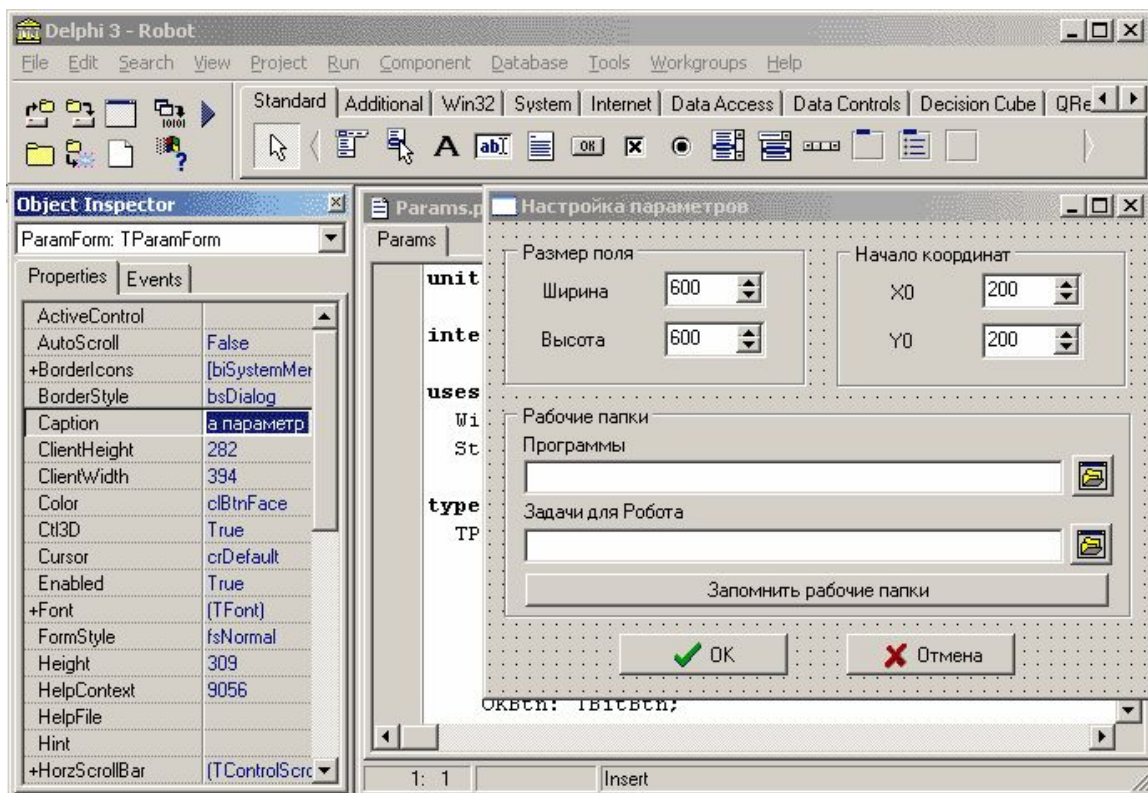
At the bottom of the IDE, the status bar displays "F1 Help" and "F10 Menu".

# Среда быстрой разработки

## Среда быстрой разработки программ (англ. *RAD = Rapid Application Development*)

- интерфейс строится с помощью мыши
- часть кода создается автоматически

**Примеры:** *Delphi, Borland C++ Builder, Visual Studio...*





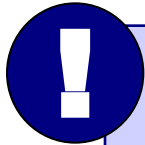
# Программное обеспечение

## Тема 5. Правовая охрана программ и данных

# Законодательство

---

- **Конституция РФ** ст. 44 ч. 1: «Интеллектуальная собственность охраняется законом»



**Интеллектуальная собственность – права на результаты творческой деятельности!**

- Гражданский кодекс РФ, часть IV «Права на результаты интеллектуальной деятельности и средства индивидуализации» (2006)  
<http://www.internet-law.ru/law/kodeks/gk4.htm>
- «Правила составления, подачи и рассмотрения заявок на официальную регистрацию программ для ЭВМ и баз данных» (1993)  
<http://www.morepc.ru/informatisation/osplaw0003.html>
- **Уголовный кодекс РФ**  
<http://www.interlaw.ru/law/docs/10008000/>

# Объектами авторского права...

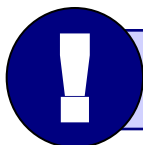
---

## ... являются

- **программы** для компьютеров (включая подготовительные материалы, а также звук, графику и видео, которые получаются с помощью программы)
- **базы данных** (данные, специально организованные для поиска и обработки с помощью компьютеров)

## ... не являются

- **алгоритмы и языки программирования**
- **идеи и принципы**, лежащие в основе программ, баз данных, интерфейса;
- **официальные документы**



**Охраняется форма, а не содержание!**

# Авторское право

---

- автор – физическое лицо (не организация)
- возникает «в силу создания» продукта, не требует формальной регистрации
- обозначение: © **Иванов, 2008** (год первого выпуска)
- действует в течение жизни и 70 лет после смерти автора
- передается по наследству

# Права автора

---

## Личные:

- *право авторства* (право считаться автором)
- *право на имя* (свое имя, псевдоним, анонимно)
- *право на неприкосновенность* (защита программы и ее названия от искажений)

## Имущественные: осуществлять или разрешать

- выпуск программы в свет
- копирование в любой форме
- распространение
- изменение (в т.ч. перевод на другой язык)

# Использование программ и БД

---

## Основания:

- *договор* в письменной форме
- при массовом распространении – *лицензионное соглашение* на экземпляре

## Можно без разрешения автора:

- хранить в памяти *1 компьютера* (или по договору)
- вносить *изменения*, необходимые для работы на компьютере пользователя (но не распространять!)
- исправлять явные *ошибки*
- изготовить *копию* для архивных целей
- *перепродать* программу

# Защита от копирования

---

- **инсталляция программ** (нельзя просто скопировать)
- **регистрационный код** (привязка к оборудованию, серийным номерам)
- **защита CD, DVD** (теряется при копировании)
- **не работает без диска**
- **аппаратный ключ**



для параллельного  
порта



для порта USB

- **сканирование сети** (обнаружение копий)
- **сервер в Интернете** проверяет серийные номера
- **техподдержка** – косвенная защита (!)

# Компьютерные преступления

---

## **Экономические**

- обогащение путем взлома информационных систем
- компьютерный шпионаж
- кража программ («пиратство»)

## **Против личных прав**

- ложная информация
- незаконный сбор информации
- разглашение банковской и врачебной тайны

## **Против общественных и государственных интересов**

- разглашение государственной тайны
- утечка информации
- искажение информации (подсчет голосов)
- вывод из строя информационных систем (диверсии)



# Уголовный кодекс РФ

---

## Статья 146. Нарушение авторских и смежных прав.

- только при крупном ущербе (50000 р.)
- *присвоение авторства* (плагиат) – до 6 месяцев лишения свободы
- *незаконное использование*, а также приобретение, хранение, перевозка в целях сбыта – до 2 лет
- *группой лиц*, в особо крупном размере (250000 р.) или с использованием служебного положения – до 5 лет

# Уголовный кодекс РФ

---

## **Признаки преступления:**

- уничтожение, блокирование, модификация или копирование информации
- нарушение работы компьютера или сети

## **Статья 272. Неправомерный доступ к компьютерной информации.**

- до 2 лет лишения свободы
- группой лиц – до 5 лет

## **Статья 273. Создание, использование и распространение вредоносных программ.**

- до 3 лет лишения свободы
- с тяжкими последствиями – до 7 лет

## **Статья 274. Нарушение правил эксплуатации компьютеров и сети.**

- до 2 лет лишения свободы
- с тяжкими последствиями – до 4 лет

# Авторские права в Интернете

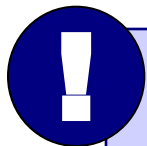
---

## При нелегальном использовании:

- всегда есть косвенная выгода (достижение своих целей);
- ущерб авторам, снижение дохода;
- снижение посещаемости и цитируемости сайтов ⇒ снижение дохода.

## Правила:

- при использовании материалов в учебных работах ссылаться на источник;
- для публикации в Интернете текста или фотографии получить разрешение автора или издателя.



**Официальные документы – не объекты авторского права!**

# Что можно без спроса...

---

- скопировать себе картинку (текст)
- послать картинку (текст) другу
- отсканировать книгу

## Разместить на сайте

- картинку с другого сайта
- Указ Президента РФ
- цитату из статьи с указанием автора
- статью с другого сайта (или из книги) с указанием автора
- описание алгоритма
- отсканированную книгу
- повесть А.С. Пушкина

# Какие бывают программы?

---

- **Свободное ПО** с открытым исходным кодом (*Open Source*): можно бесплатно
  - запускать и использовать в любых целях
  - изучать и адаптировать
  - 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*):**

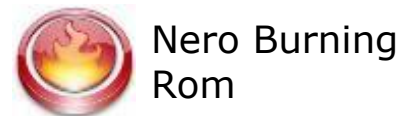
бесплатное ПО с ограничениями:

- 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)



# 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 6. 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

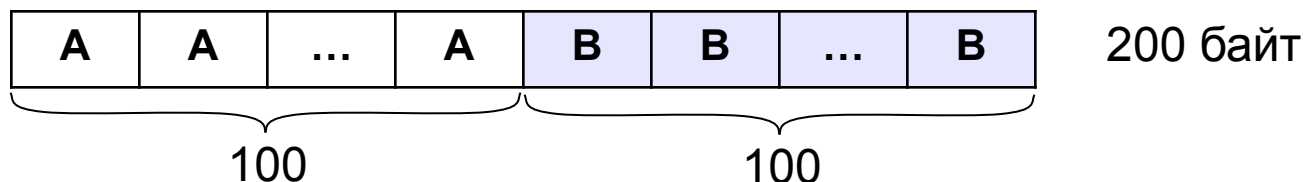
**Типы сжатия:**

- **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)

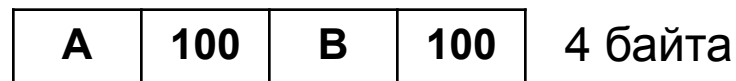
# Почему файлы можно сжать?

**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)
- сжатые рисунки (\*.gif, \*.jpg, \*.png, \*.tif, ...)
- сжатый звук (\*.mp3, \*.wma)
- сжатое видео (\*.mpg, \*.wmv)

# Специальные типы архивов

---

**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

**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`, ....

# Архиватор WinRAR (Е. Рошал)

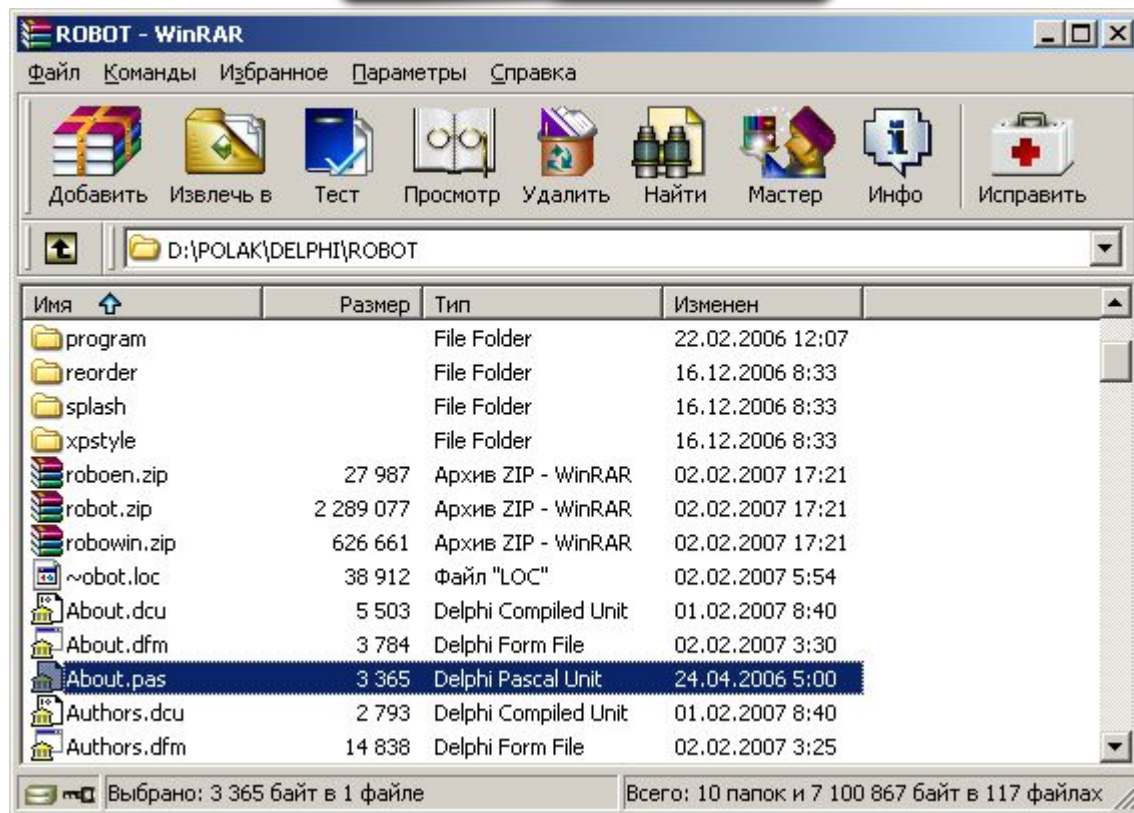
Запуск: Пуск – WinRAR

распаковать архив

сжать выделенные файлы

Выйти из папки

двойной щелчок ЛКМ: войти в архив

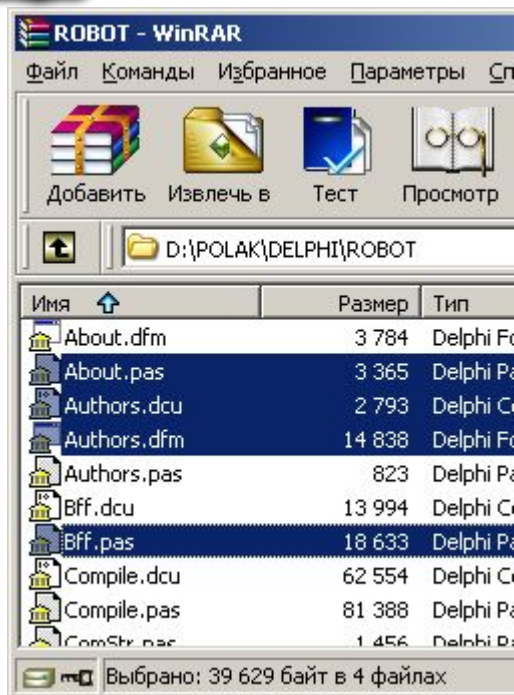


сменить диск

изменить пароль

# Архиватор WinRAR: упаковка

ЛКМ

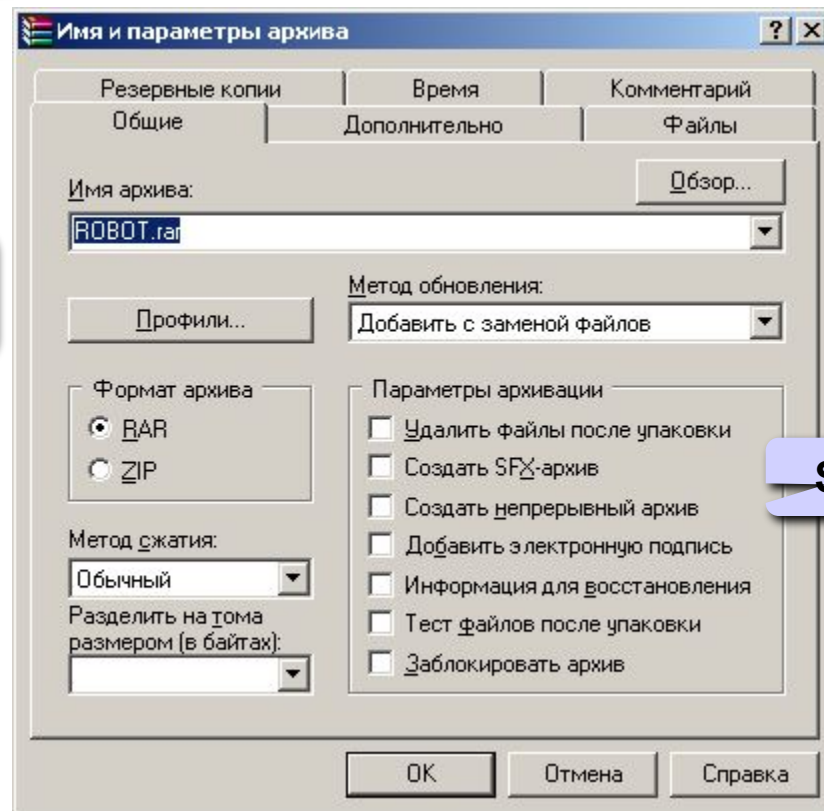


ИМЯ  
архива

пароль

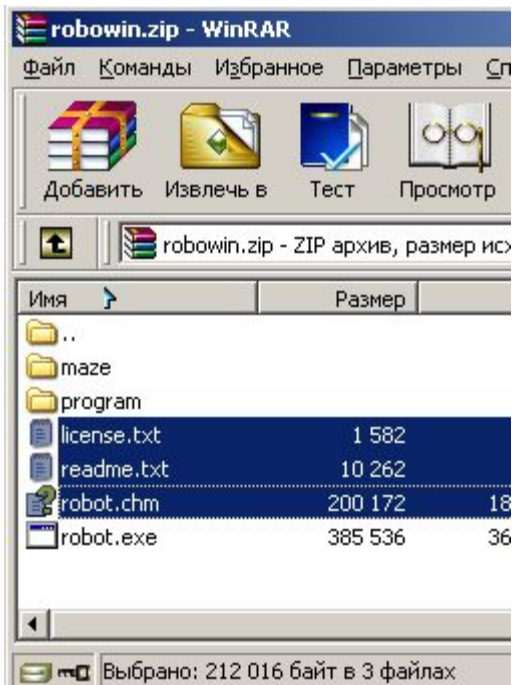
ТИП  
архива

МНОГОТОМНЫЕ  
архивы

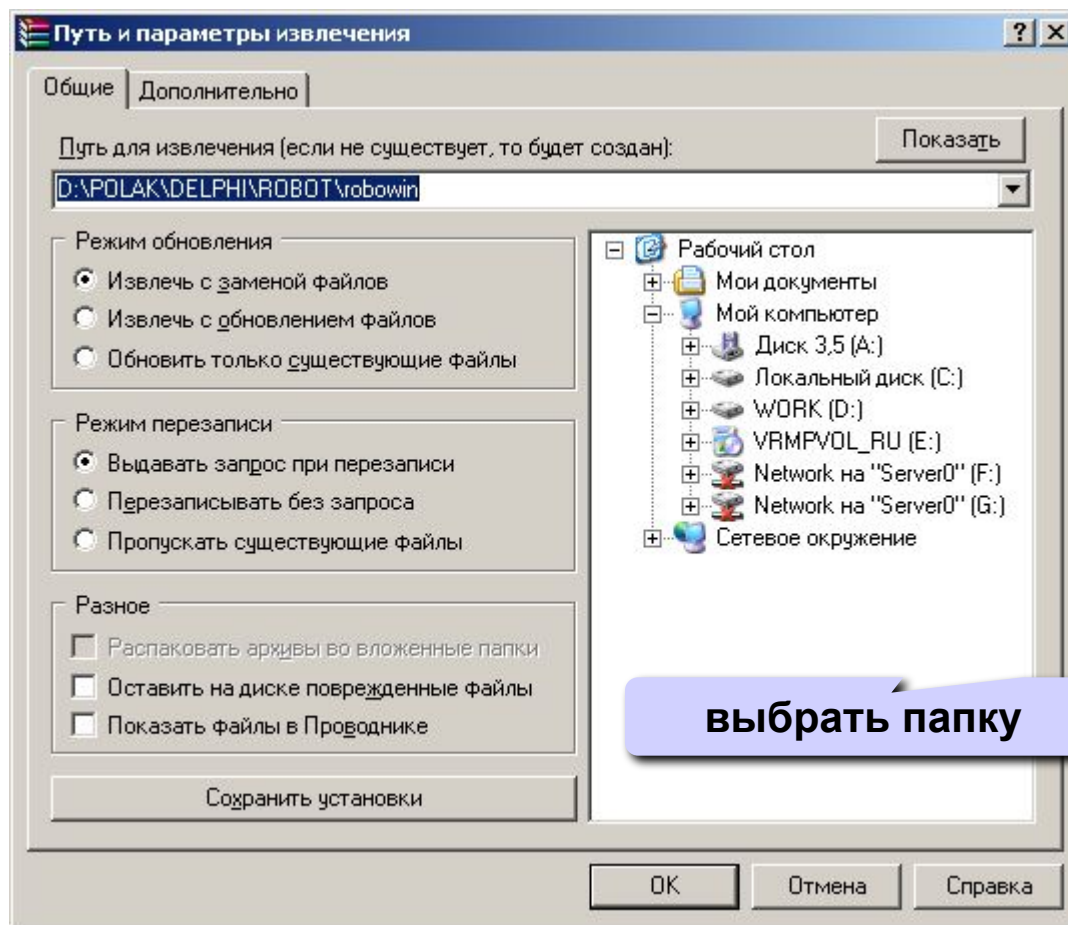


# Архиватор WinRAR: распаковка

ЛКМ



куда распаковать?



выбрать папку

# Архиватор WinRAR в Проводнике

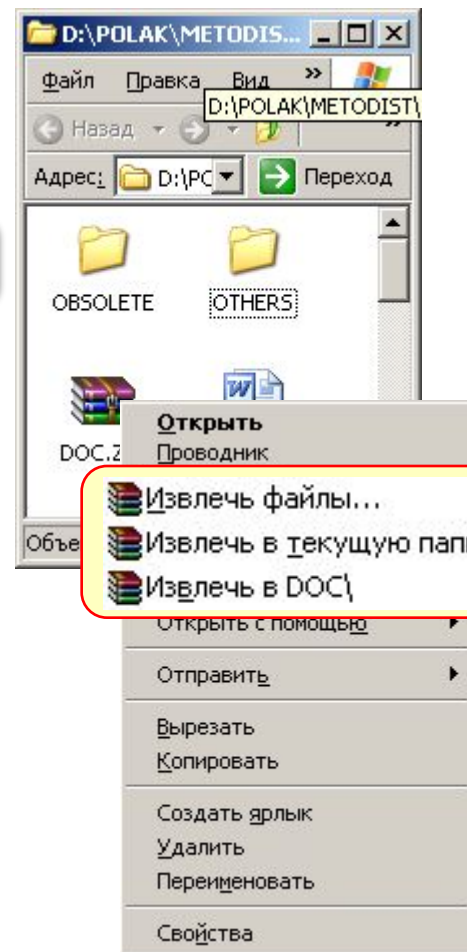
## Упаковка



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

## Распаковка



ПКМ

- Извлечь файлы...
- Извлечь в текущую папку
- Извлечь 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

---

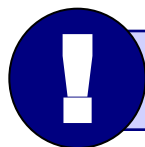
- **Файловые** – заражают файлы `*.exe`, `*.sys`, `*.dll` (редко – внедряются в тексты программ).
- **Загрузочные (бутовые, от англ. *boot* – загрузка)** – заражают загрузочные сектора дисков и дискет, при загрузке сразу оказываются в памяти и получают управление.
- **Полиморфные** – при каждом новом 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



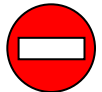
# Антивирусы-сканеры

---

- 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



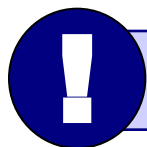
- замедление работы компьютера
- в случае ошибки ОС может выйти из строя

# Антивирусные программы

---

## Условно-бесплатные:

- AVP = Antiviral Toolkit Pro ([www.avp.ru](http://www.avp.ru)) – Е. Касперский
- DrWeb ([www.drweb.com](http://www.drweb.com)) – И. Данилов
- Norton Antivirus ([www.symantec.com](http://www.symantec.com))
- McAfee ([www.mcafee.ru](http://www.mcafee.ru))
- NOD32 ([www.eset.com](http://www.eset.com))



Есть бесплатные пробные версии!

## Бесплатные:

- Avast Home ([www.avast.com](http://www.avast.com))
- Antivir Personal ([free-av.com](http://free-av.com))
- AVG Free ([free.grisoft.com](http://free.grisoft.com))





# Антивирус Касперского

---

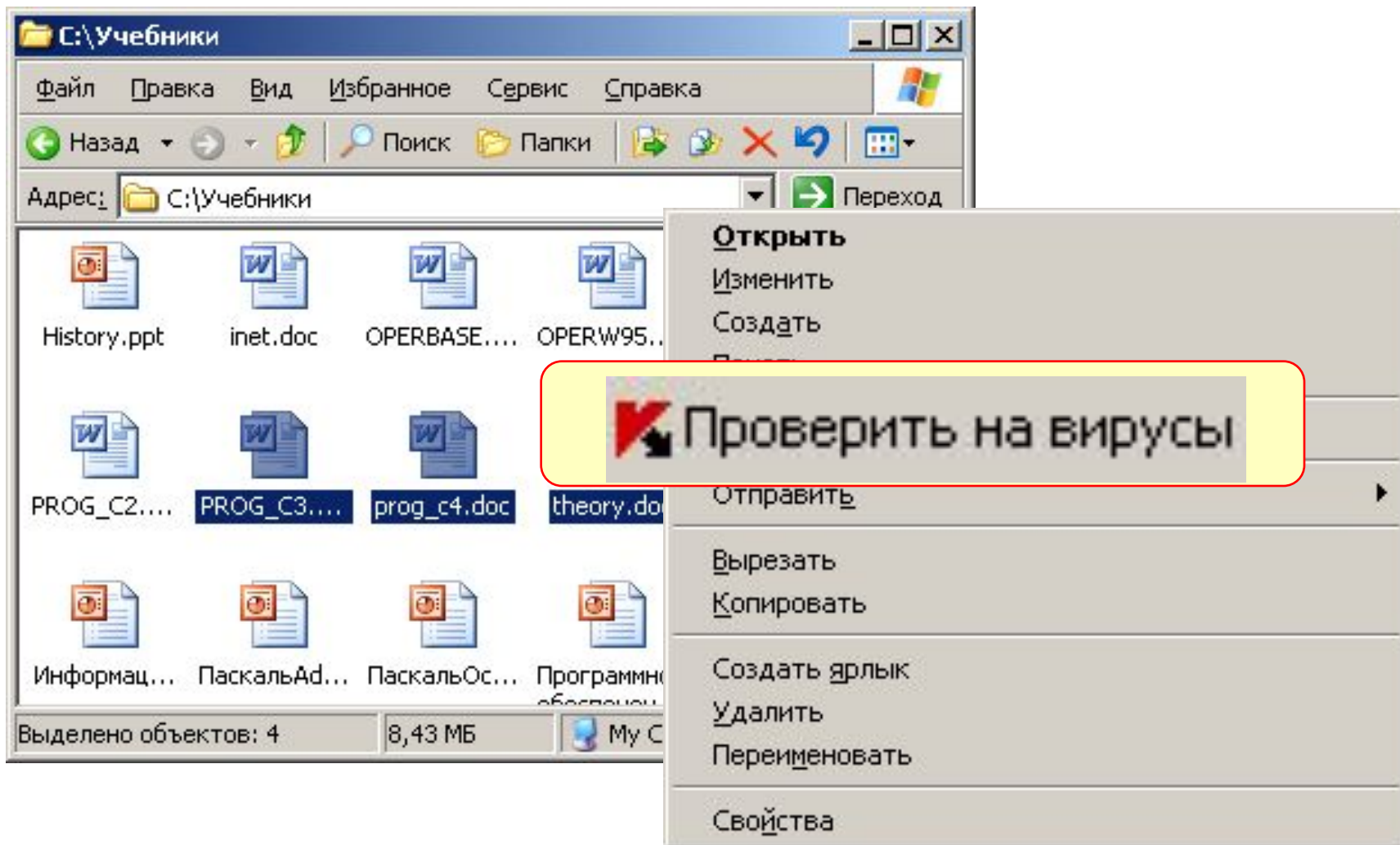
- **Файловый антивирус** (проверка файлов в момент обращения к ним)
- **Почтовый антивирус** (проверка входящих и исходящих сообщений)
- **Веб-антивирус** (Интернет, проверка *Web*-страниц)
- **Проактивная защита** (попытки обнаружить неизвестные вредоносные программы):
  - слежение за реестром
  - проверка 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 main interface. The main interface shows several windows: '1% - Проверка Моего Компьютера', 'Антивирус Касперского 6.0 для Windows Workstations', '14% - Обновление', 'Анти-Хакер: Мониторинг сети', and 'Настройка: Антивирус Касперского'. The 'Настройка' window is active, showing a green checkmark and the text 'Настройка' and 'Защита'. A dialog box titled 'Приостановка защиты' is open, displaying the following options for when protection will be automatically turned on: 'Через 1 минуту', 'После перезапуска приложения', and 'Только по требованию пользователя' (which is selected). The dialog box also includes a 'Справка' button and 'OK' and 'Отмена' buttons. At the bottom of the main interface, there is a status bar with the text 'Все вредоносные объекты обезврежены.' and a table of statistics:

Всего проверено:	3080
Обнаружено:	35
Не вылечено:	0
Заблокировано атак:	0

Additional text in the status bar includes 'Просмотр статистики работы', 'kaspersky.ru', and 'viruslist.ru'. The system clock shows 11:21.

## 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**: Points to the menu bar.
- выбрать, что проверяем (ЛКМ)**: Points to the file list in the left pane.
- результ**: Points to the status bar at the bottom left.

The main window displays the following settings:

Объекты	Вредоносные программы		
Инфицированные объекты	Вылечить	Рекламные программы	Удалить
Неизлечимые объекты	Удалить	Программы дозвона	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:

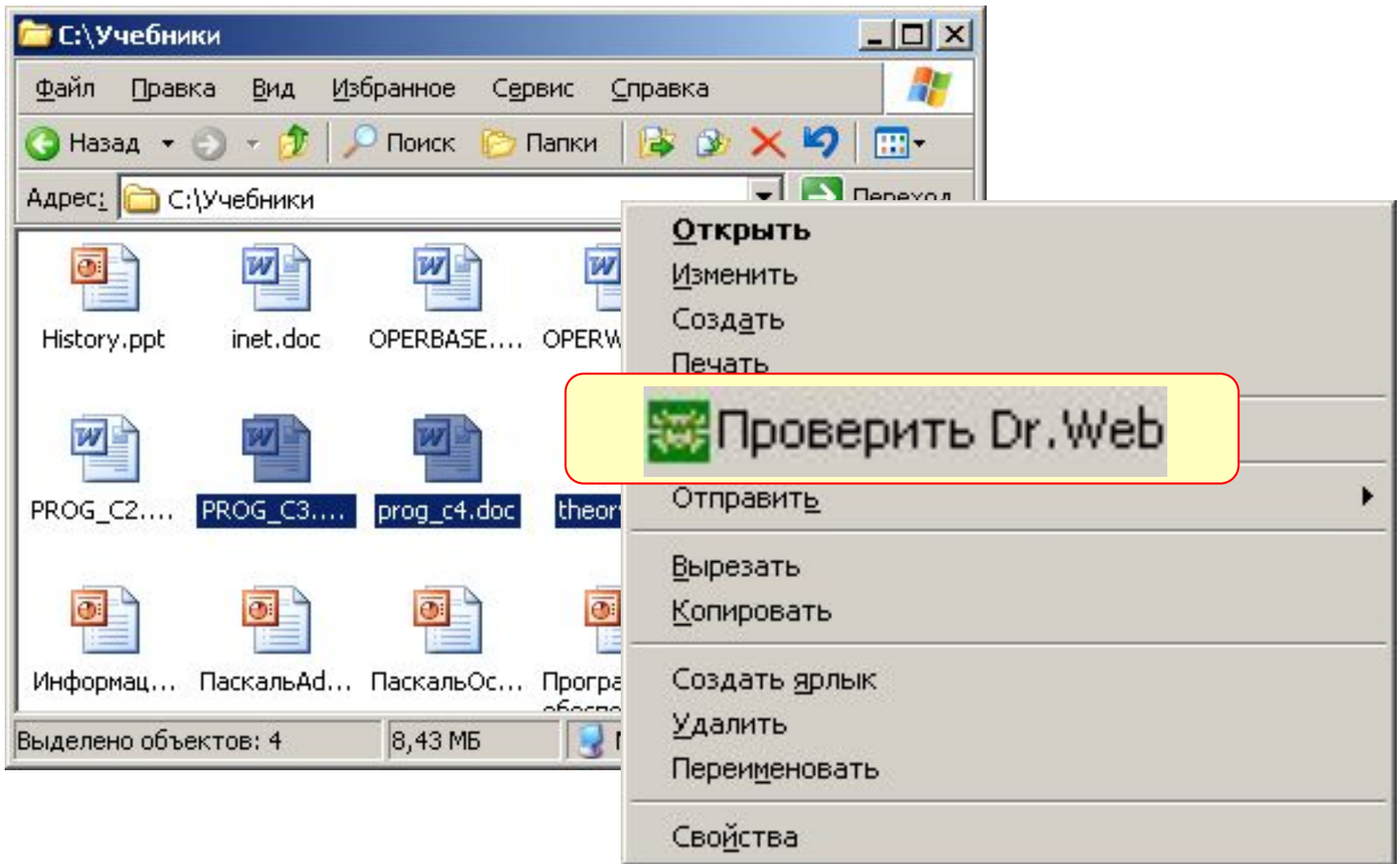
- Переименовать расширение: #??
- Путь для перемещения: infected.!!!

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...
- удалить *Windows* и установить ее заново. Если не помогает, то...
- отформатировать винчестер (**format.com**). Если сделать это не удастся, то могла быть испорчена таблица разделов диска. Тогда ...
- создать заново таблицу разделов (**fdisk.exe**). Если не удастся (винчестер не обнаружен), то...
- можно нести компьютер в ремонт.

# Конец фильма

---