

Программное обеспечение

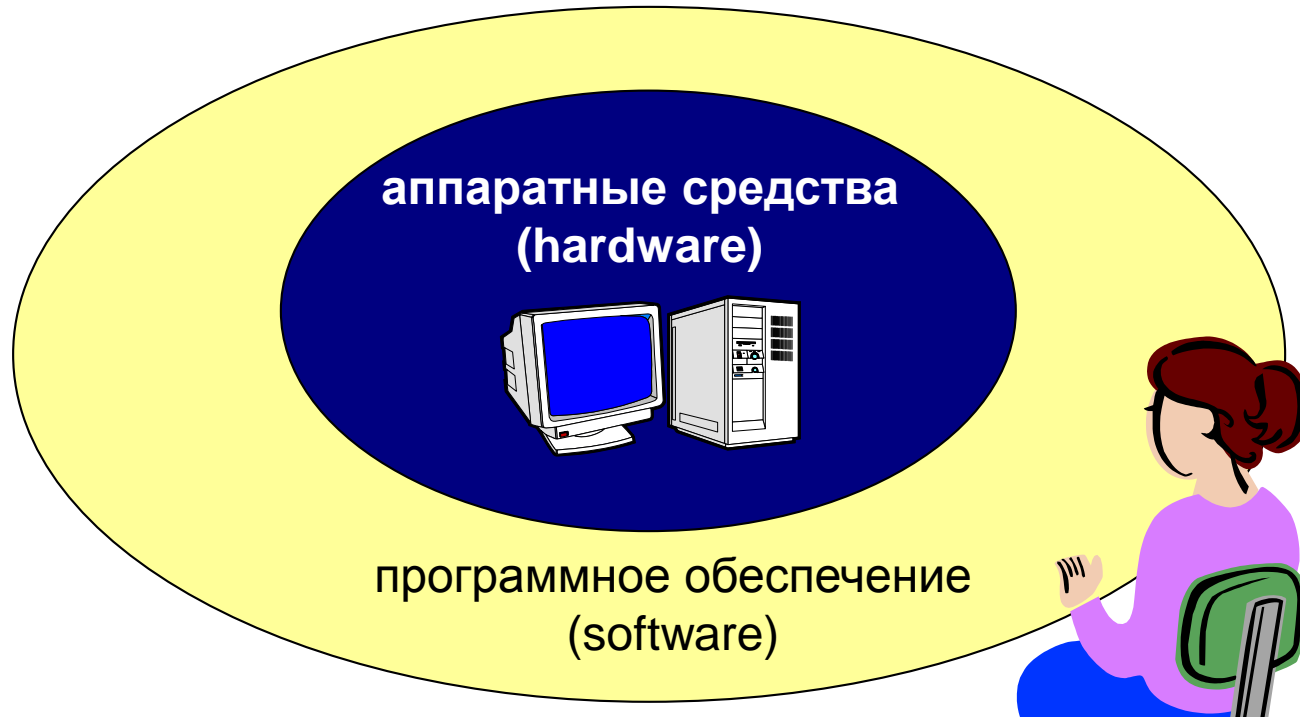
1. Введение
2. Прикладные программы
3. Системные программы
4. Системы программирования
5. Правовая охрана программ и данных
6. Сжатие файлов. Архиваторы
7. Компьютерные вирусы и антивирусы

Программное обеспечение

Тема 1. Введение

Программное обеспечение

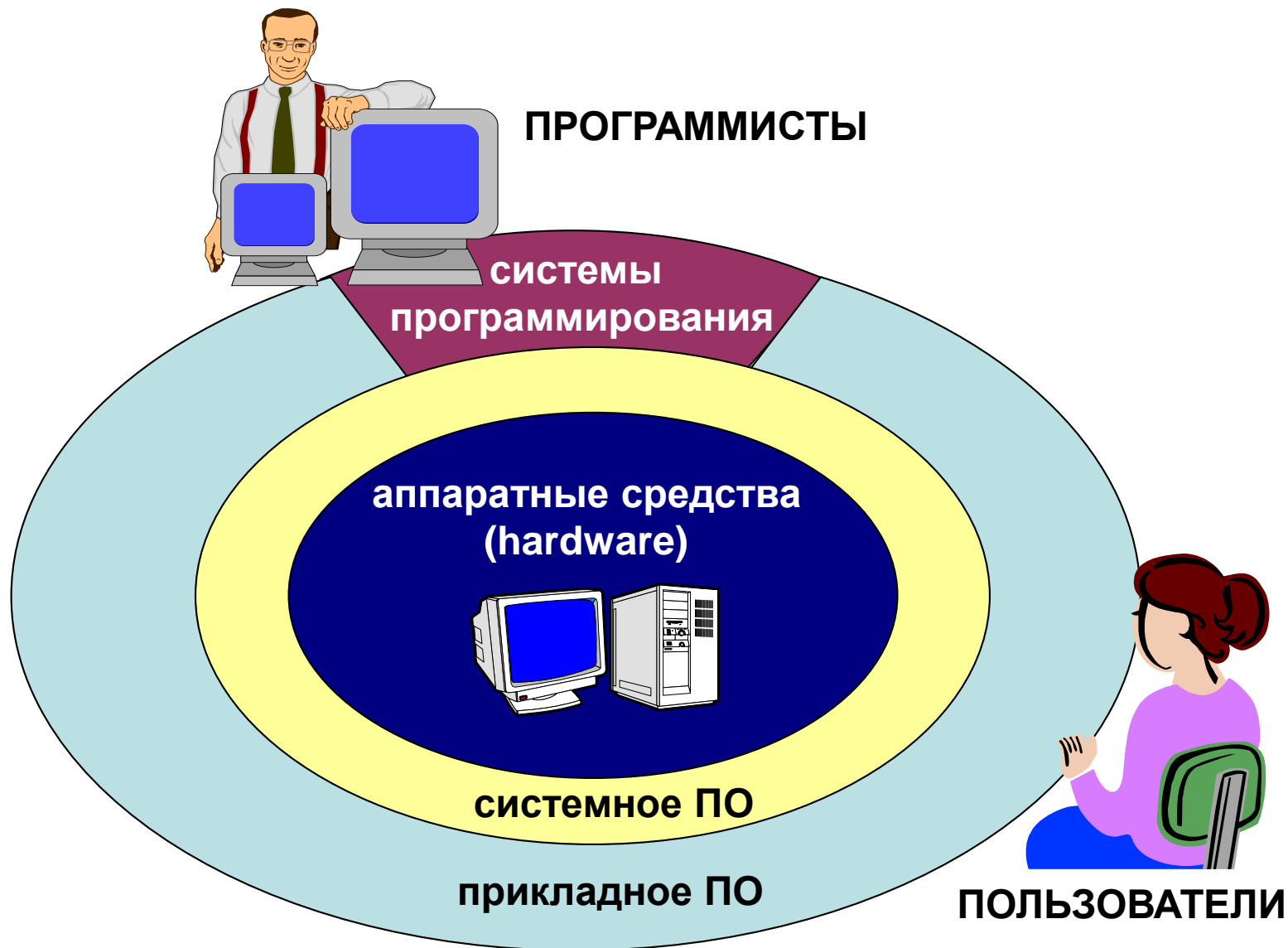
Взаимодействие человека с компьютером



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

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.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! 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

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
 - нет права доступа
- **NTFS** (Windows NT/2000/XP/Vista/7)
 - ⊕ ▪ право 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 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.

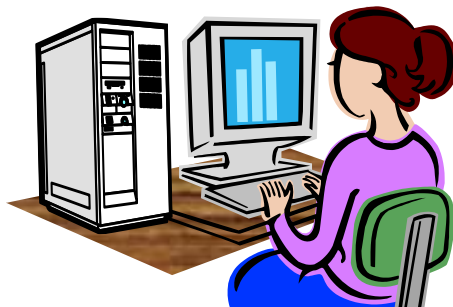
Примеры: *MS DOS, FreeDOS, DR DOS, PC DOS*

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

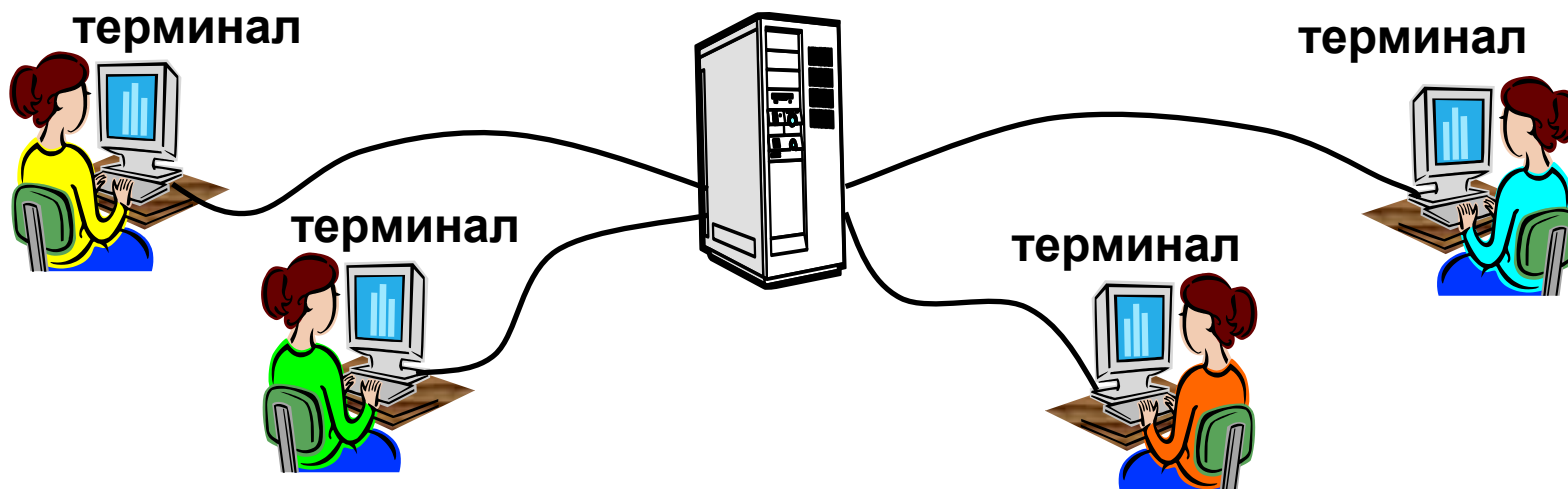
Типы ОС

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



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

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:

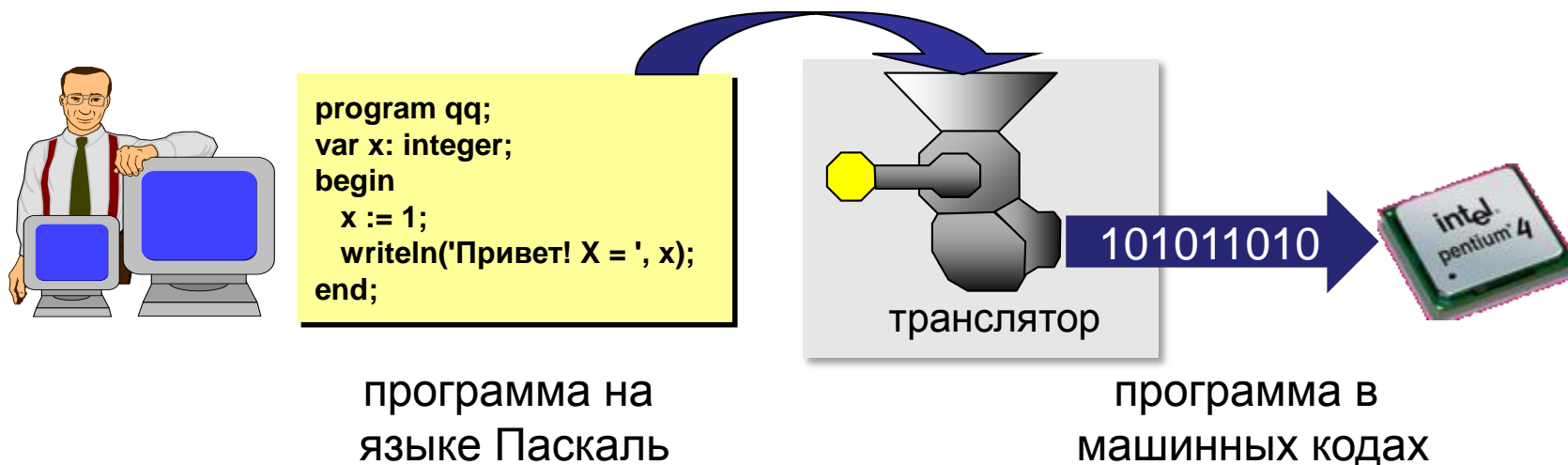
- **машинные коды:** 09 FE AC 3F
- **ассемблеры:** символическая запись машинных команд:
mov AX, BX
- **макросассемблеры:** одна команда языка заменяет несколько машинных команд

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.



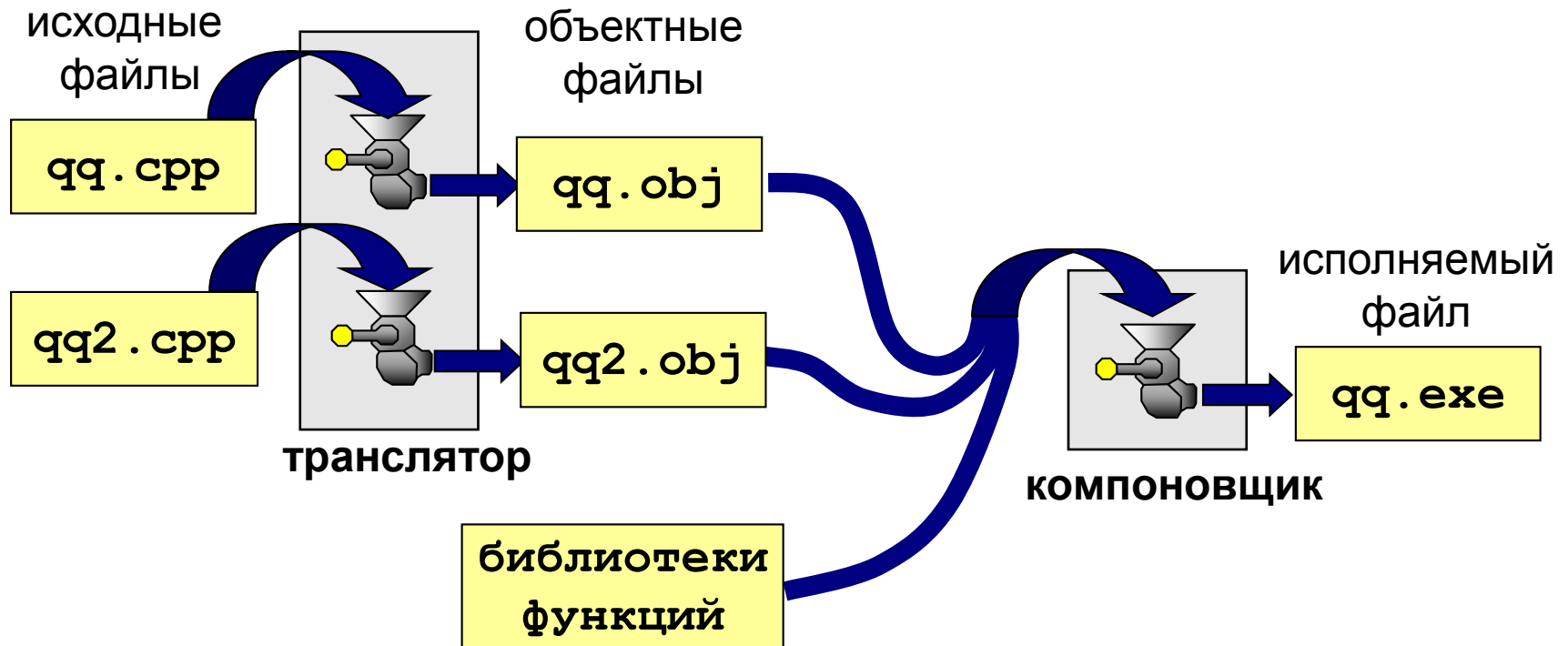
Могут ли быть ошибки в трансляторах?

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).

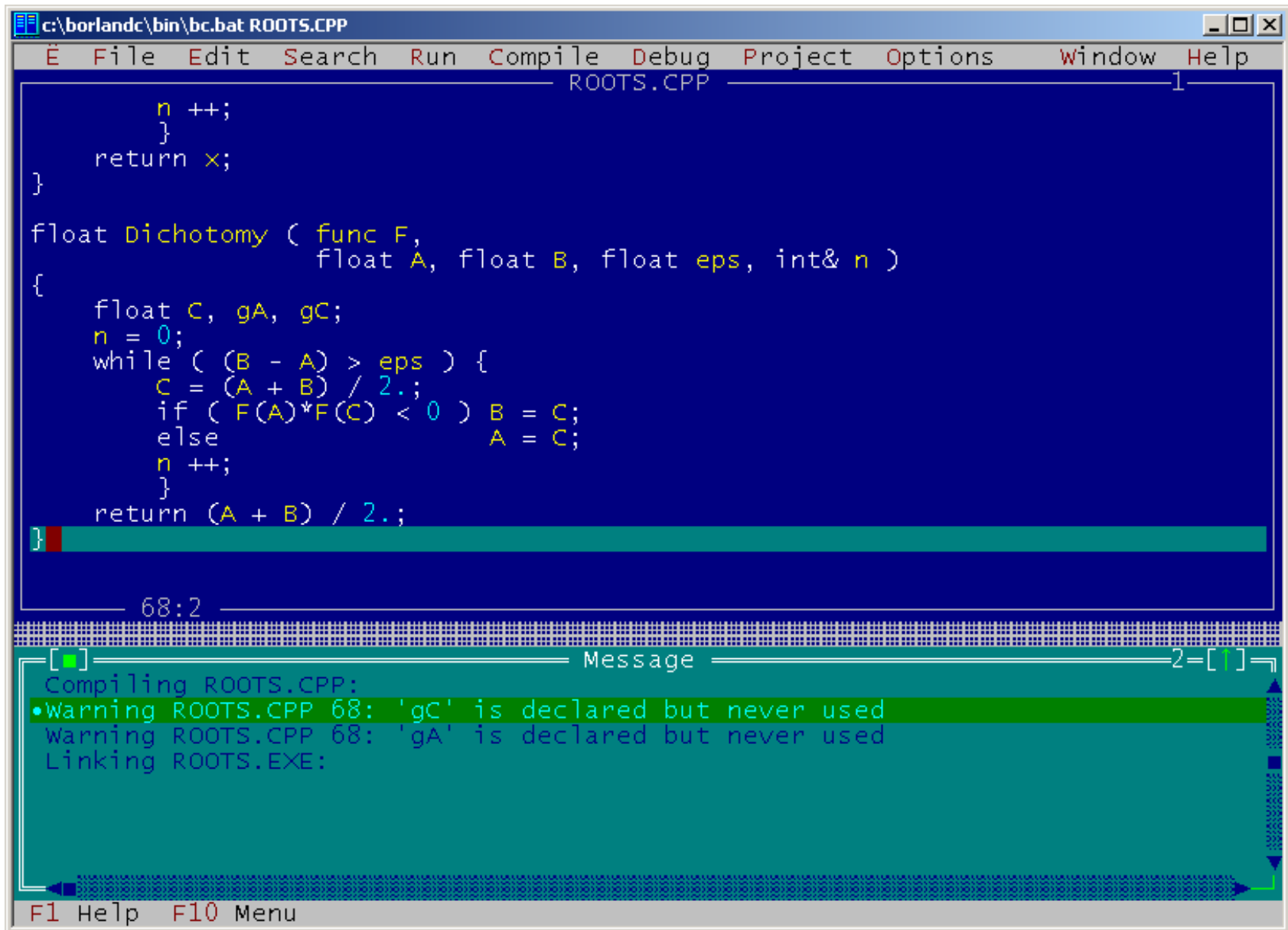
Возможности:

- 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 screenshot shows a Borland C++ IDE window titled "c:\borlandc\bin\bc.bat ROOTS.CPP". The menu bar includes File, Edit, Search, Run, Compile, Debug, Project, Options, Window, and Help. The main editor displays the following C++ code:

```
    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 shows "68:2". Below the editor is a "Message" window with the following output:

```
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:
```

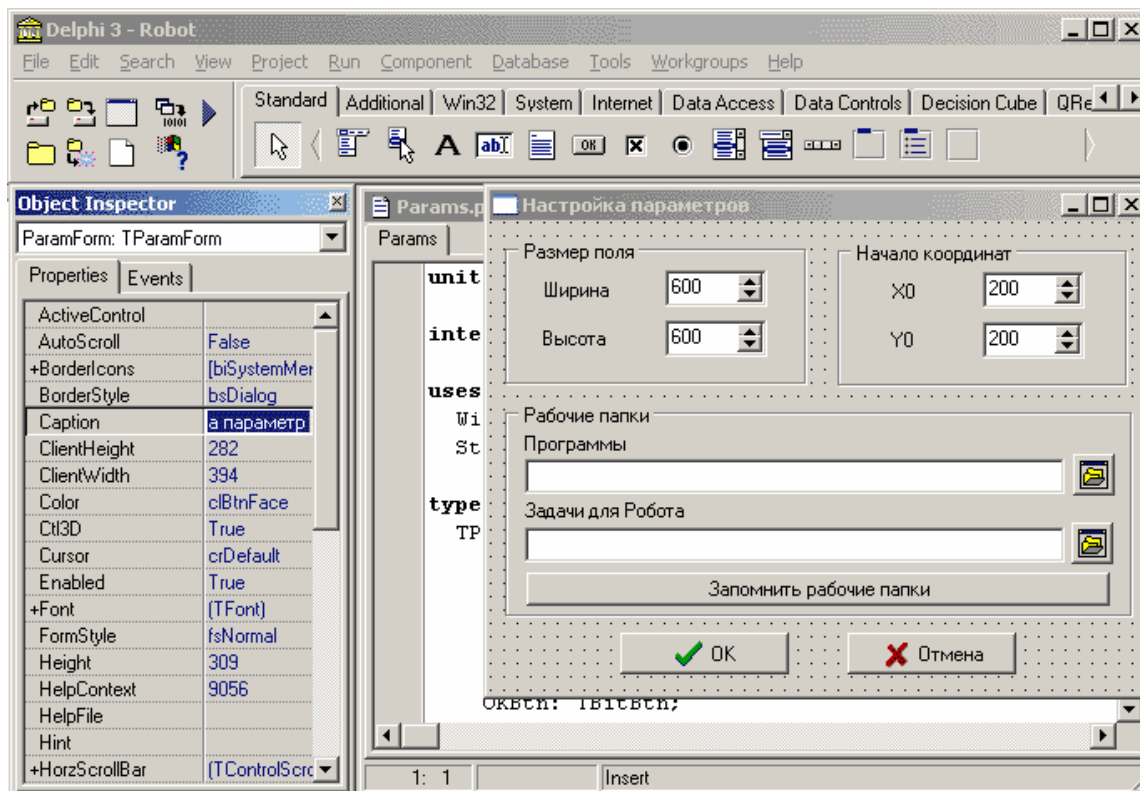
The status bar at the bottom of the IDE shows "F1 Help F10 Menu".

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

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)

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
- 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)



Nero Burning Rom



TheBat

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:

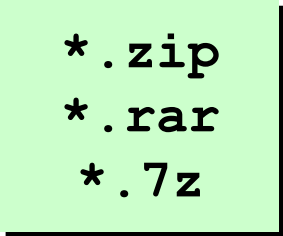
- сохранить данные на случай сбоя на диске
- объединить группу файлов в один архив
- зашифровать данные с паролем

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)

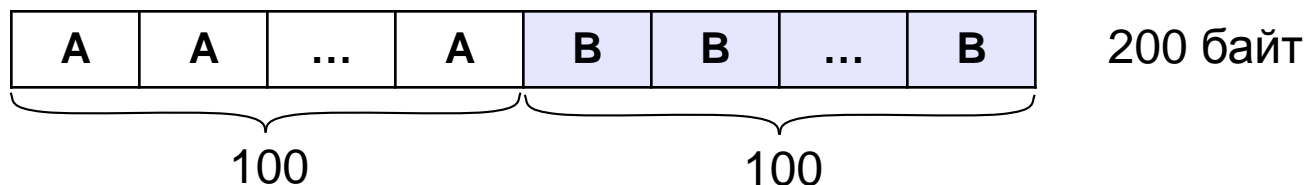


```
*.zip  
*.rar  
*.7z
```

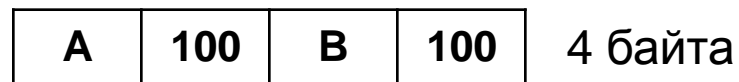
Почему файлы можно сжать?

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,`

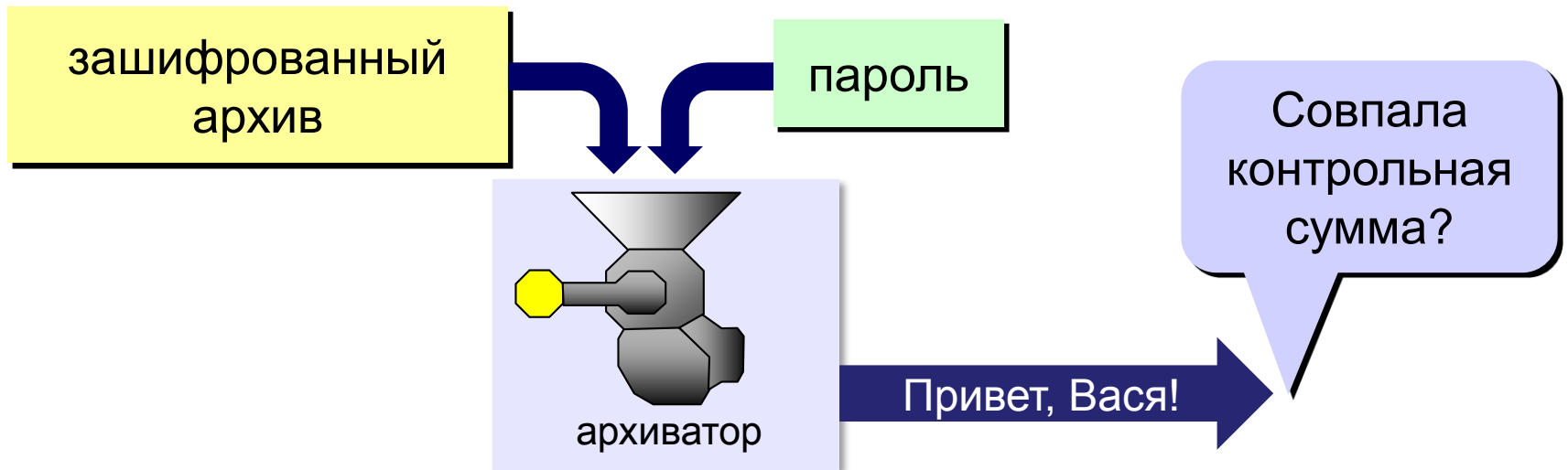
7Zip:

- `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
- ReI\$%_aS&

плохие

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

Архиватор WinRAR (Е. Рошал)

Запуск: Пуск – WinRAR

сжать выделенные файлы

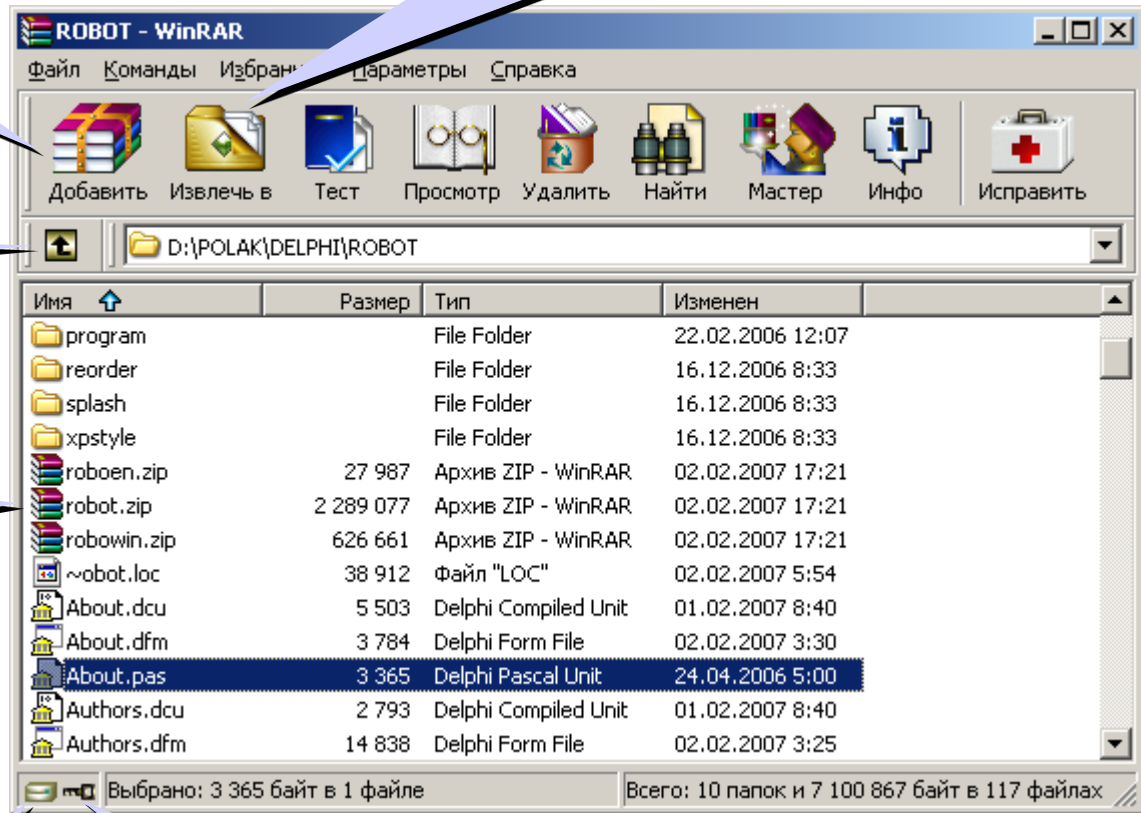
распаковать архив

ВЫЙТИ ИЗ папки

двойной щелчок ЛКМ: войти в архив

сменить диск

изменить пароль



Архиватор WinRAR: упаковка

The image shows the WinRAR interface with two windows. The left window, titled "ROBOT - WinRAR", displays a file list in a table. The right window, titled "Имя и параметры архива", shows the configuration for creating a new archive. Callouts in Russian identify various elements: "ЛКМ" (Left Mouse Button) points to the "Добавить" (Add) button; "ИМЯ архива" (Archive Name) points to the "Имя архива:" field containing "ROBOT.rar"; "пароль" (password) points to the "Дополнительно" (Advanced) tab; "тип архива" (Archive Type) points to the "RAR" radio button under "Формат архива"; "СFX" points to the "Создать SFX-архив" checkbox; and "МНОГОТОМНЫЕ архивы" (Multi-volume Archives) points to the "Разделить на тома размером" field.

Имя	Размер	Тип
About.dfm	3 784	Delphi F
About.pas	3 365	Delphi P
Authors.dcu	2 793	Delphi C
Authors.dfm	14 838	Delphi F
Authors.pas	823	Delphi P
Bff.dcu	13 994	Delphi C
Bff.pas	18 633	Delphi P
Compile.dcu	62 554	Delphi C
Compile.pas	81 388	Delphi P
ComStr.pas	1 456	Delphi P

Имя архива: ROBOT.rar

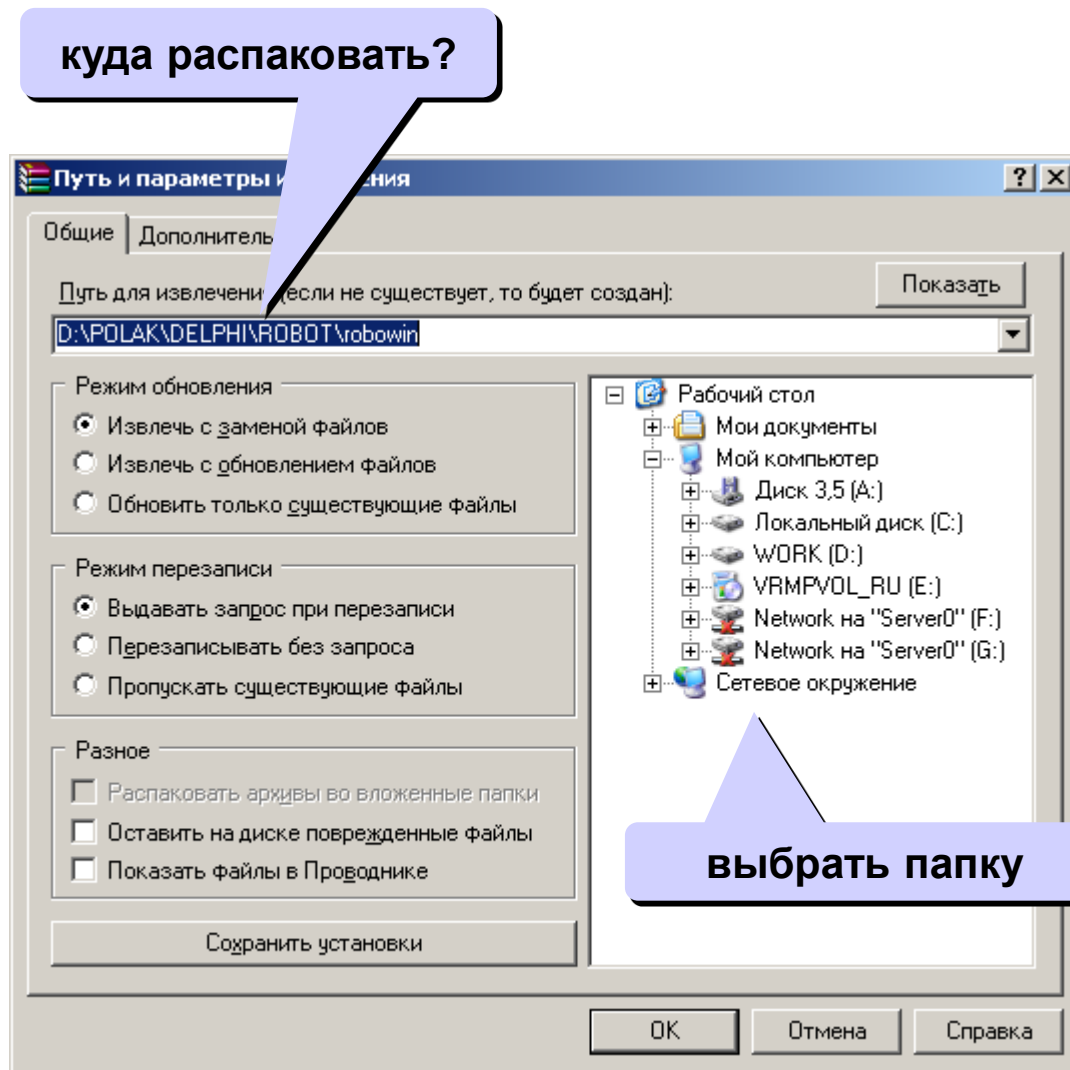
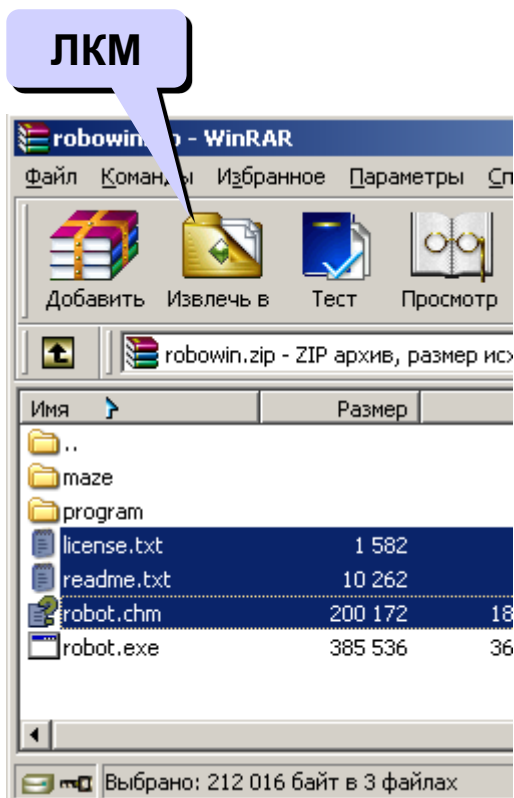
Формат архива: RAR ZIP

Метод сжатия: Обычный

Разделить на тома размером (в байтах):

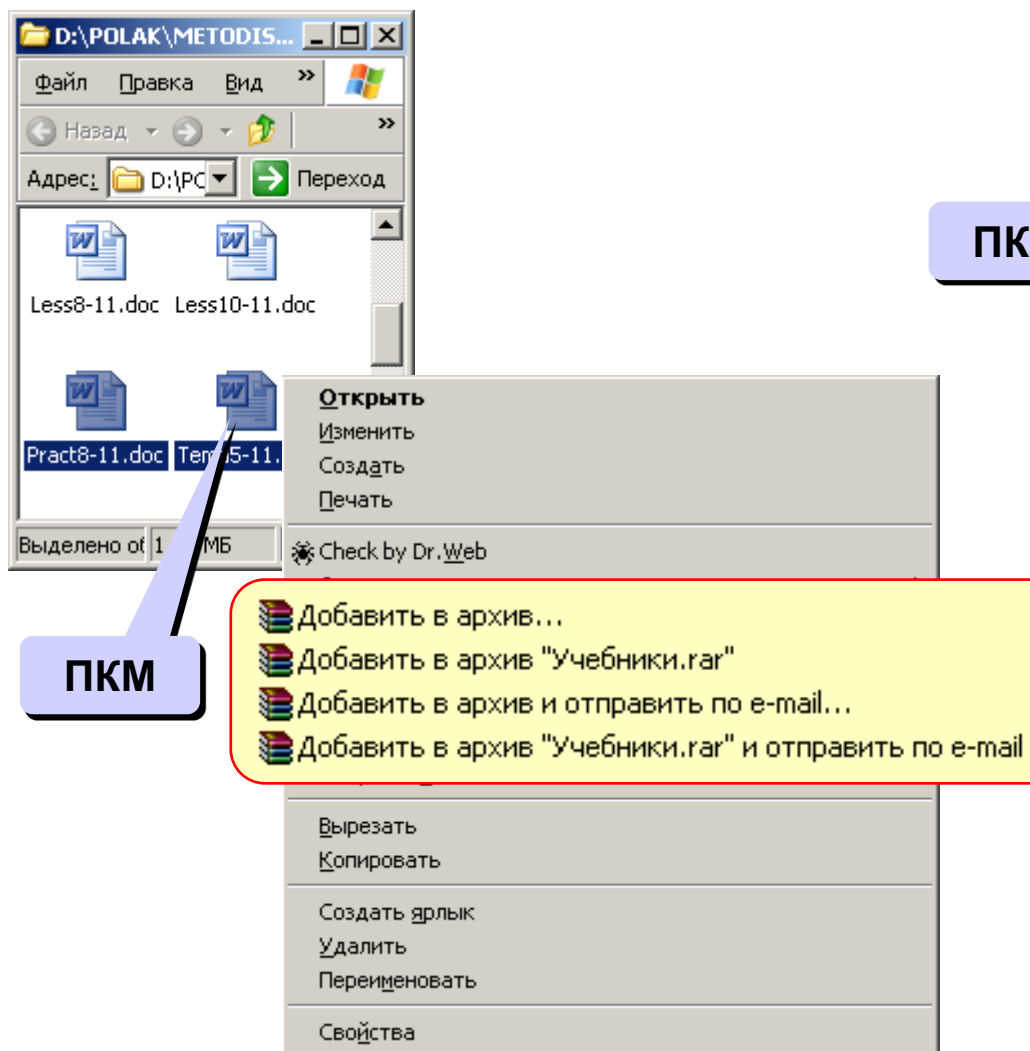
Параметры архивации: Удалить файлы после упаковки Создать SFX-архив Создать непрерывный архив Добавить электронную подпись Информация для восстановления Тест файлов после упаковки Заблокировать архив

Архиватор WinRAR: распаковка

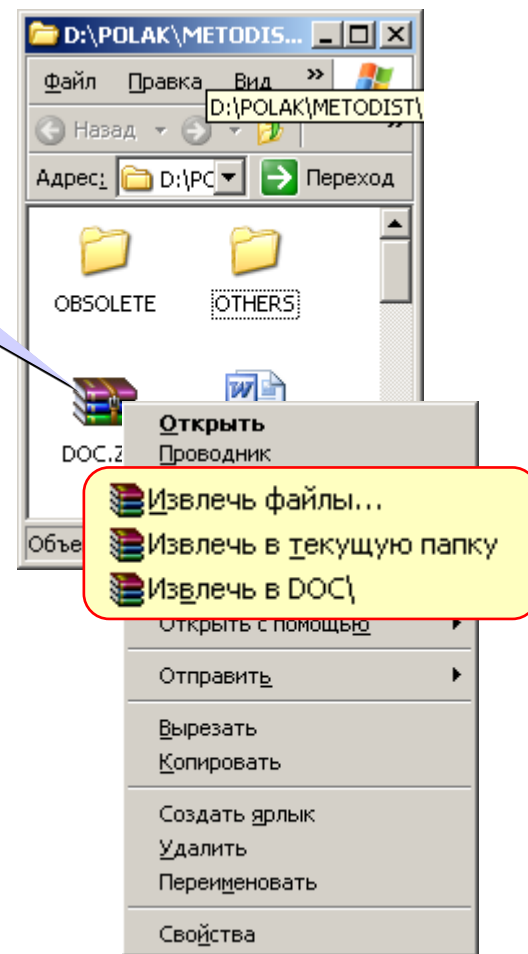


Архиватор WinRAR в Проводнике

Упаковка



Распаковка



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 a directory with several files. The dialog has several sections and options:

- Имя архива:** The archive name is set to 'ROBOT.7z'.
- Тип архива:** The format is set to '7z'.
- Режим изменения:** The mode is set to 'Добавить и заменить'.
- Опции:** There are two checkboxes: 'Создать SFX-архив' (checked) and 'Сжимать открытые для записи файлы' (unchecked).
- Шифрование:** There is a password field, a 'Показать пароль' checkbox (checked), a 'Метод шифрования' dropdown set to 'AES-256', and a 'Шифровать имена файлов' checkbox (checked).
- Параметры:** A section for multi-volume archives.

Callouts point to the following elements:

- ЛКМ:** Points to the 'Добавить' (Add) button in the file explorer.
- имя архива:** Points to the 'Архив:' field.
- тип архива (7z, zip, tar):** Points to the format dropdown.
- SFX:** Points to the 'Создать SFX-архив' checkbox.
- пароль:** Points to the password input field.
- МНОГОТОМНЫЕ архивы:** Points to the 'Параметры:' section.

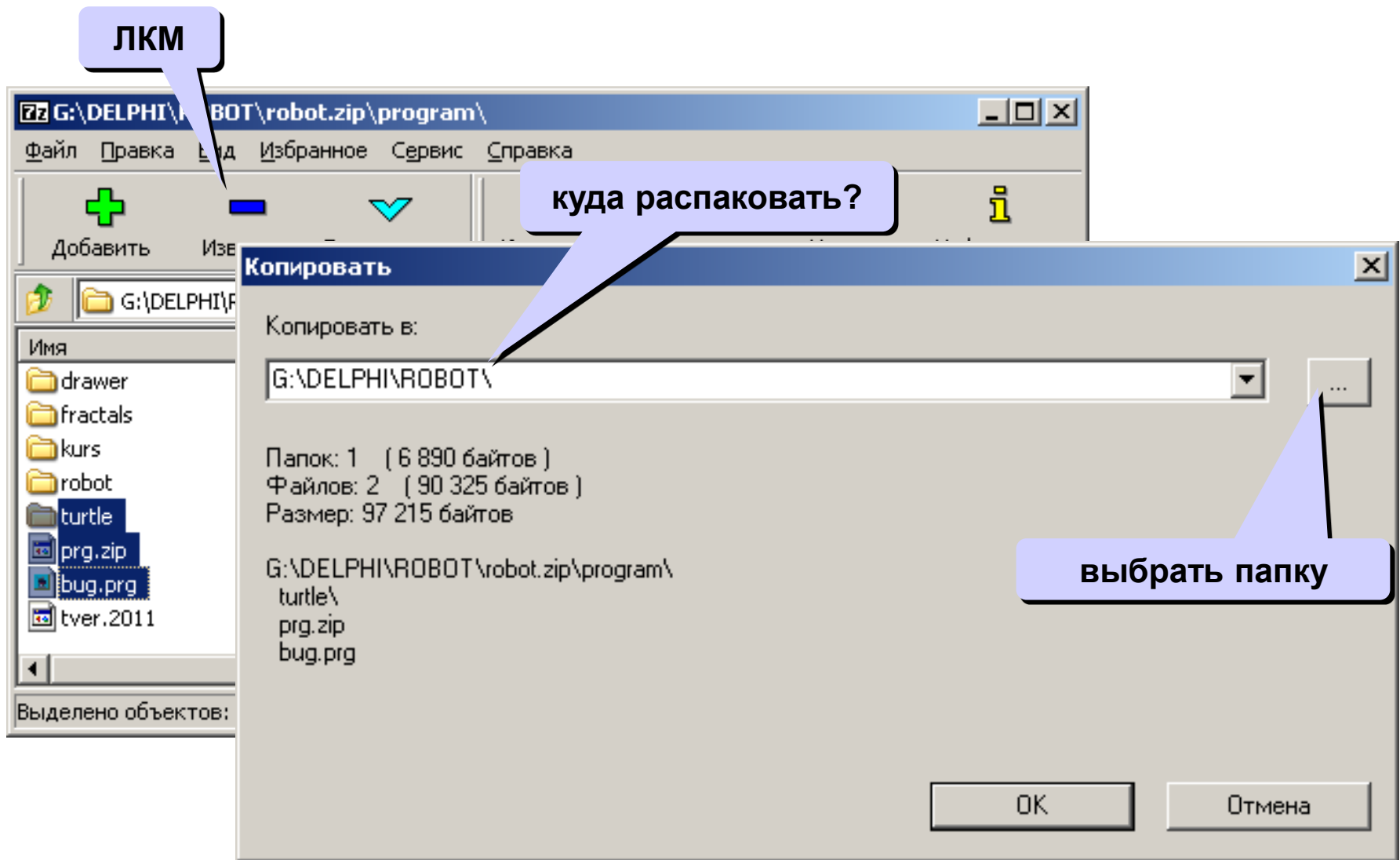
Имя	Размер
Localize.pas	4 38
CONTROLS.P...	177 69
CurSpec.dfm	48
CurSpec.pas	3 49
DEFAPP.INC	36
DEFINES.INC	84
dialogex.pas	2 44
robot.zip	3 780 30
drawex.res	80

Выделено объектов: 5 7 640

Параметры:

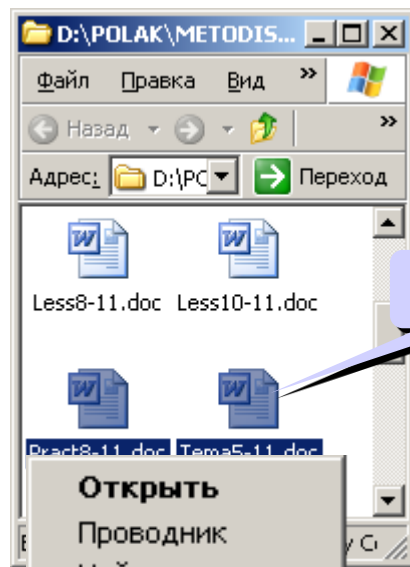
OK Отмена Помощь

Архиватор 7Zip: распаковка



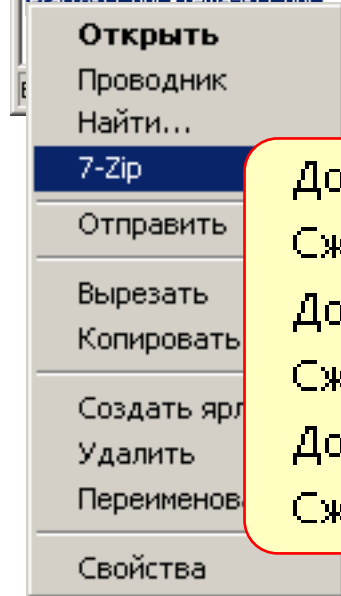
Архиватор 7Zip в Проводнике

Упаковка



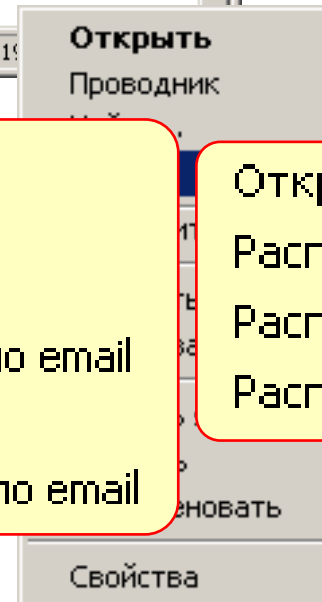
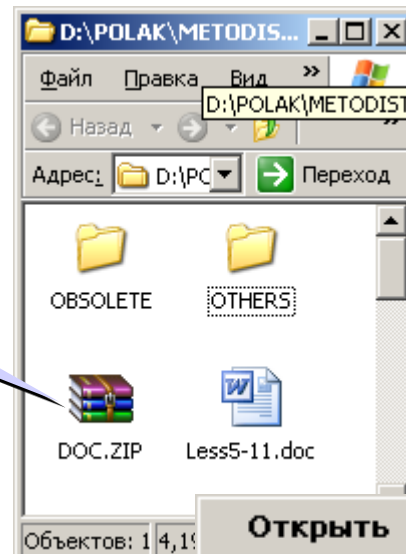
ПКМ

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



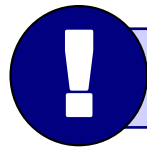
- Norton Antivirus (www.symantec.com)



- 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)

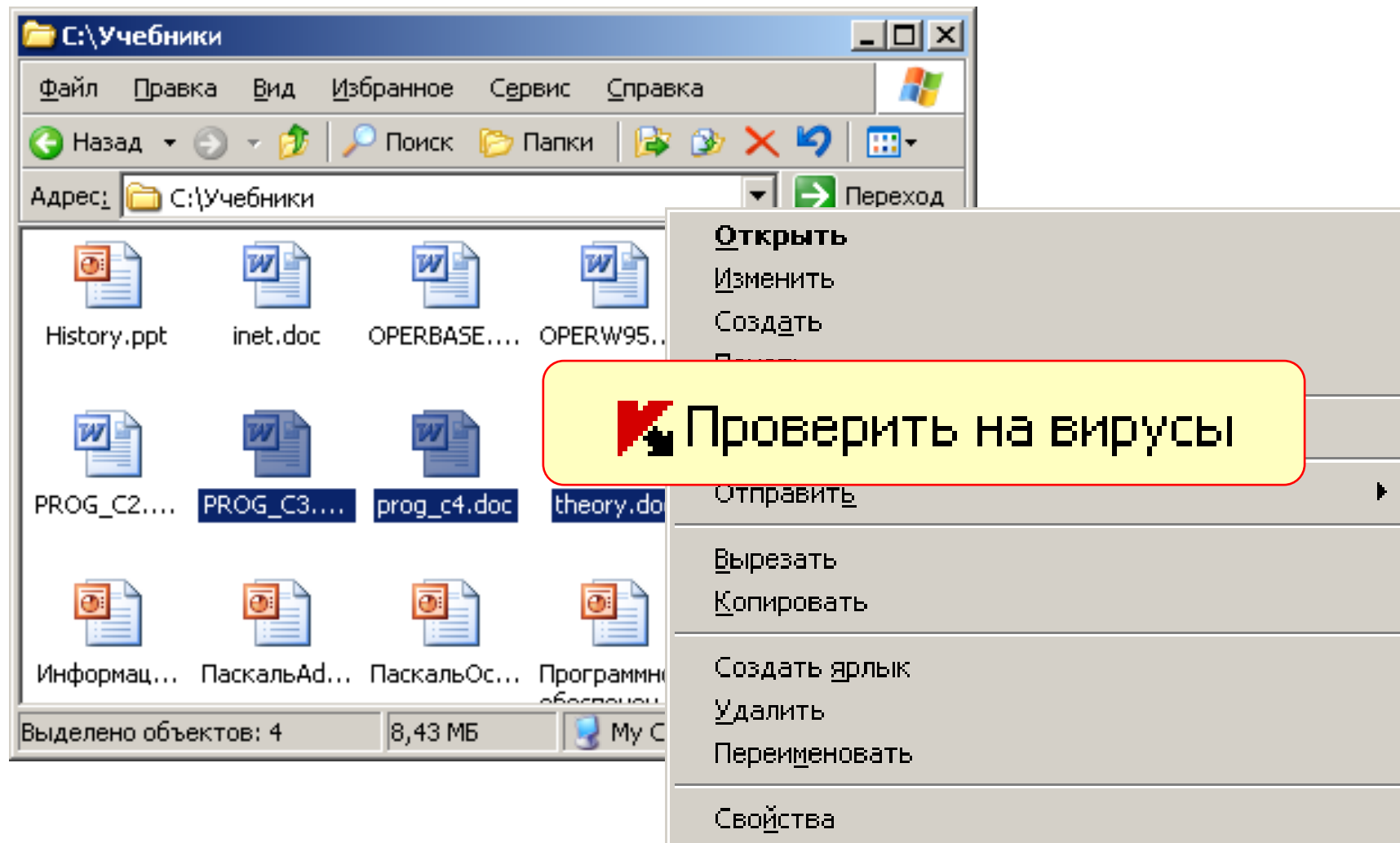
- **Файловый антивирус** (проверка файлов в момент обращения к ним)
- **Почтовый антивирус** (проверка входящих и исходящих сообщений)
- **Веб-антивирус** (Интернет, проверка *Web*-страниц)
- **Проактивная защита** (попытки обнаружить неизвестные вредоносные программы):
 - слежение за реестром
 - проверка 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 the 'Приостановка защиты' dialog box. The dialog box contains the following text: 'Защита будет автоматически включена:' followed by three radio button options: 'Через 1 минуту', 'После перезапуска приложения', and 'Только по требованию пользователя'. The 'Только по требованию пользователя' option is selected. At the bottom of the dialog box are buttons for 'Справка', 'OK', and 'Отмена'. In the background, the main interface shows a status bar with 'Все вредоносные объекты обезврежены.' and a statistics table:

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

At the bottom right of the interface, there are links for 'kaspersky.ru' and 'viruslist.ru'.

Проводник: запуск через контекстное меню





Антивирус *DrWeb* (сканер)

Запуск: Пуск – Сканер *DrWeb*

The screenshot shows the Dr.Web Antivirus scanner interface. The main window is titled "Dr.Web® Сканер для Windows". The interface includes a menu bar (Файл, Вид, Настройки, Язык), a toolbar with icons for navigation and settings, and a central pane for file selection. A yellow callout box labeled "настройки" points to the settings icon in the toolbar. A blue callout box labeled "выбрать, что проверяем (ЛКМ)" points to the file list. A red callout box labeled "результ" points to the results table. The results table shows two items: ALABAMA.COM and ROBOT.EXE, both located in C:\Задания\W. The interface also features a "Вредоносные программы" (Malicious Programs) section with various action options for different types of threats.

настройки

выбрать, что проверяем (ЛКМ)

результ

Объект	Путь
ALABAMA.COM	C:\Задания\W
ROBOT.EXE	C:\Задания\W

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		

Переименовать расширение: #??

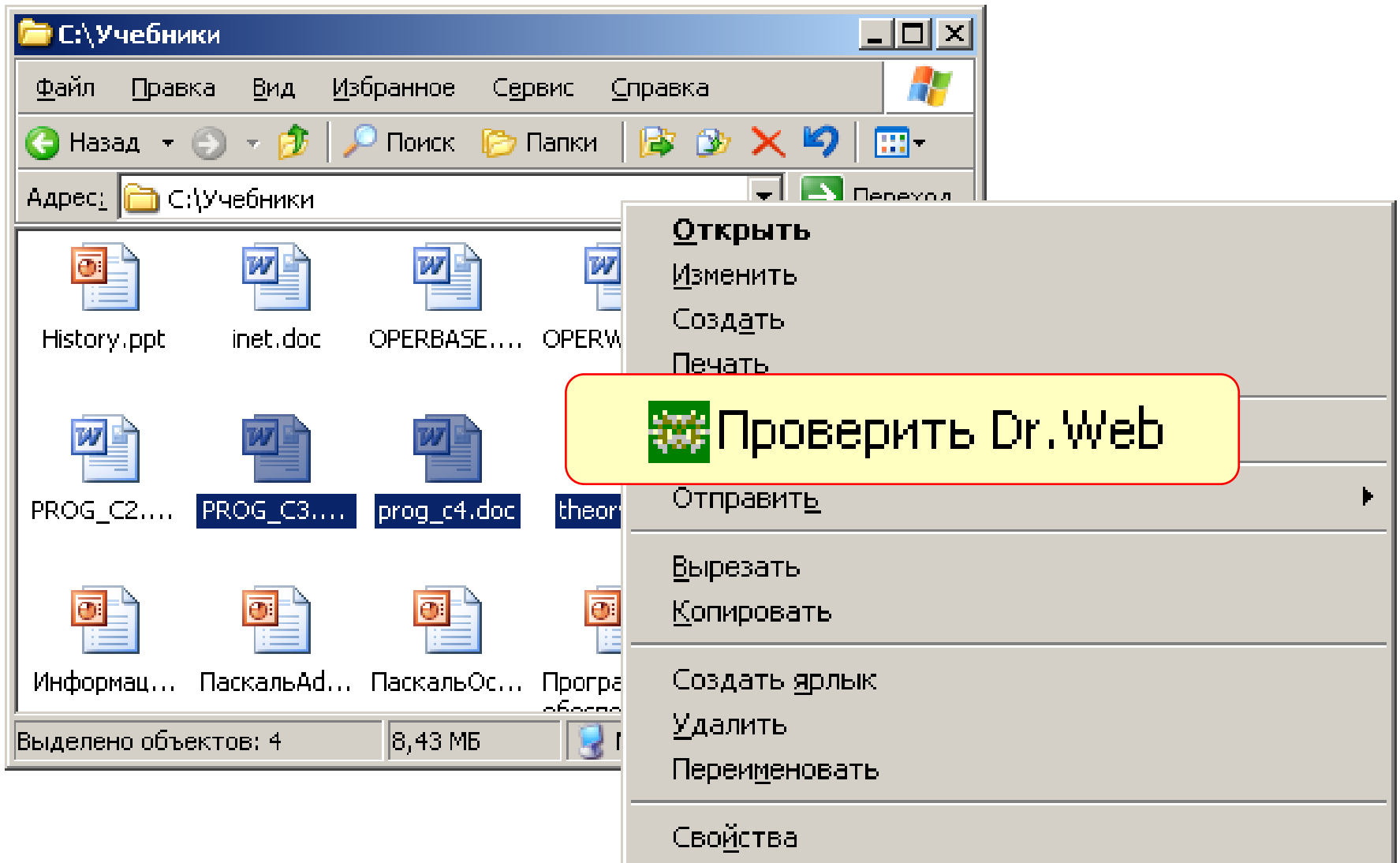
Путь для перемещения: infected.!!!

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.