

# 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

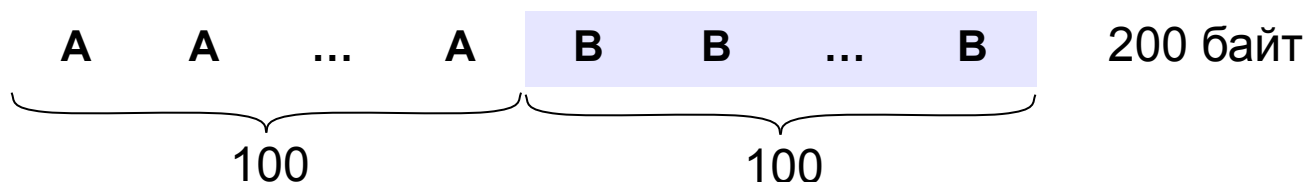
**Типы сжатия:**

- **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)

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)
- 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)

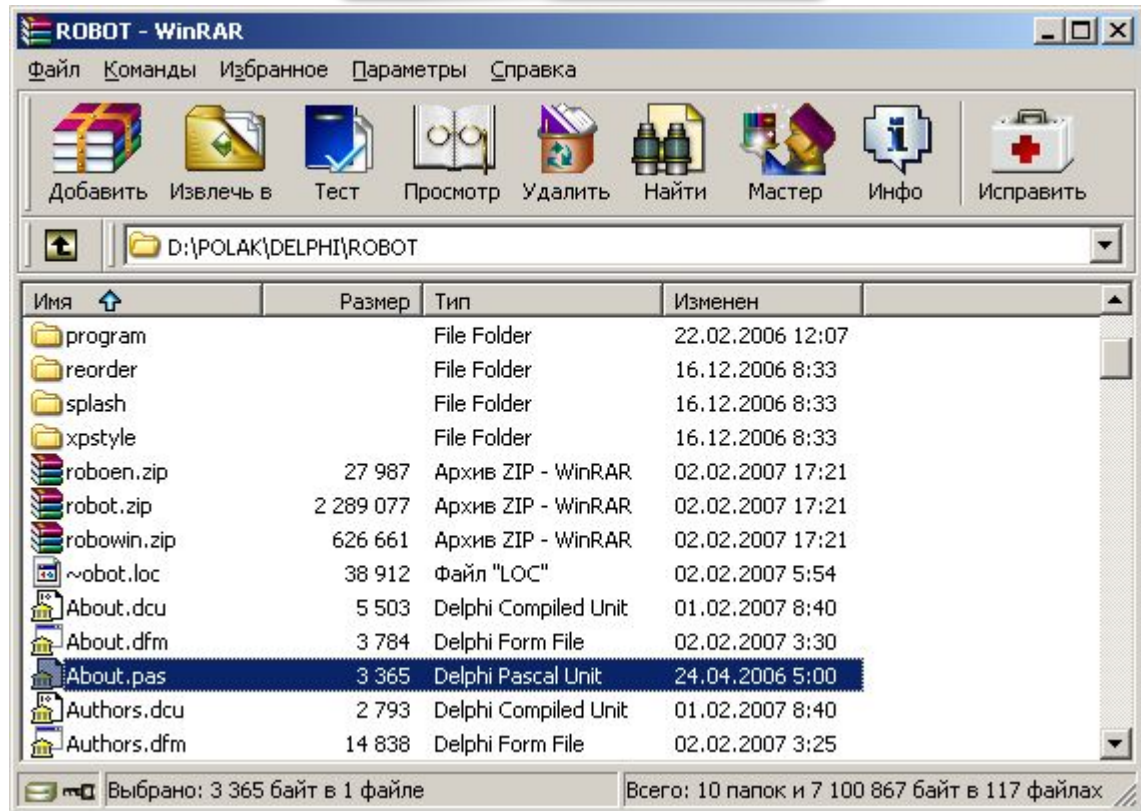
Запуск: Пуск – WinRAR

распаковать архив

сжать выделенные  
файлы

ВЫЙТИ ИЗ  
папки

двойной  
щелчок ЛКМ:  
войти в архив

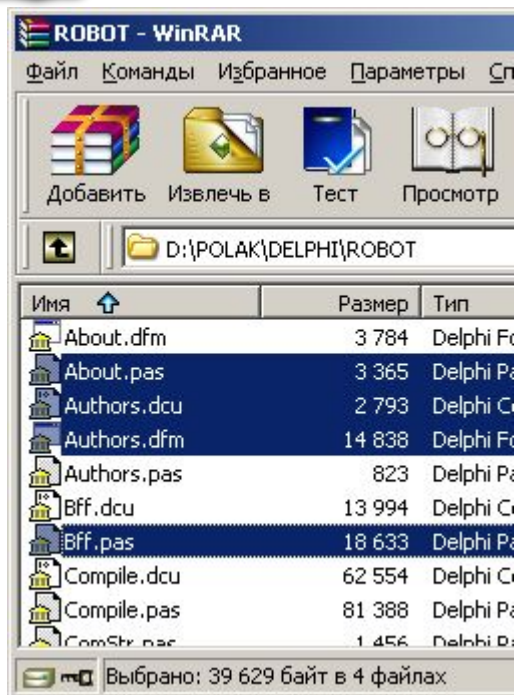


сменить диск

изменить пароль

# Архиватор WinRAR: упаковка

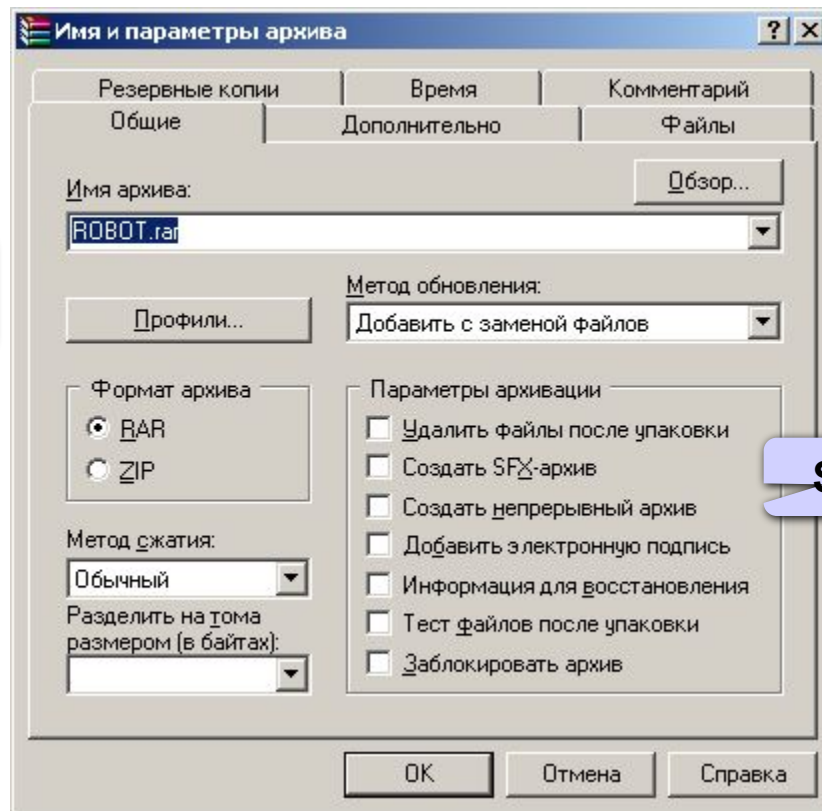
ЛКМ



ИМЯ  
архива

пароль

ТИП  
архива

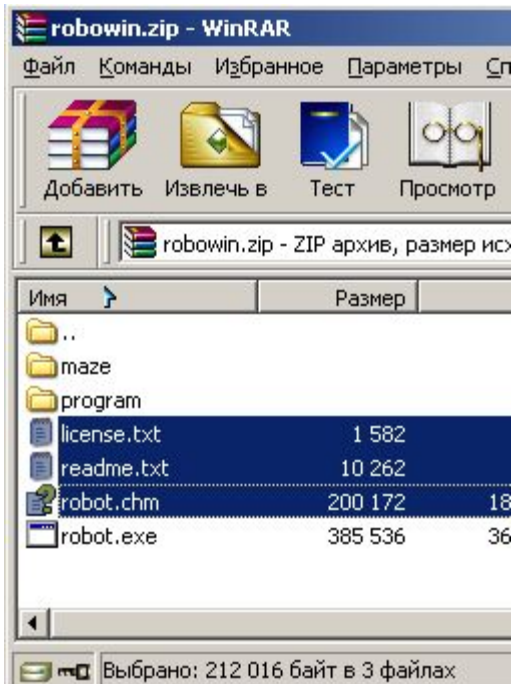


МНОГОТОМНЫЕ  
архивы

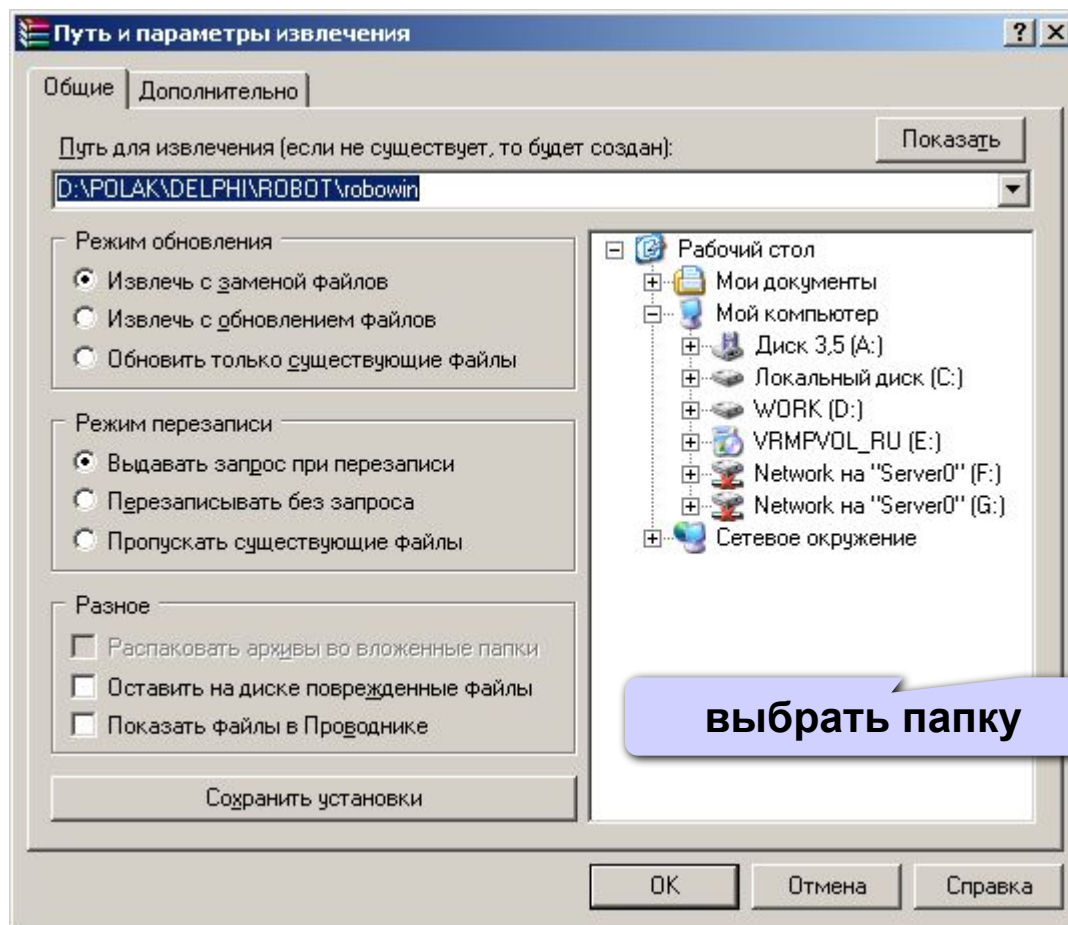
SFX

# Архиватор WinRAR: распаковка

ЛКМ



куда распаковать?



выбрать папку



# Архиватор WinRAR в Проводнике

## Упаковка

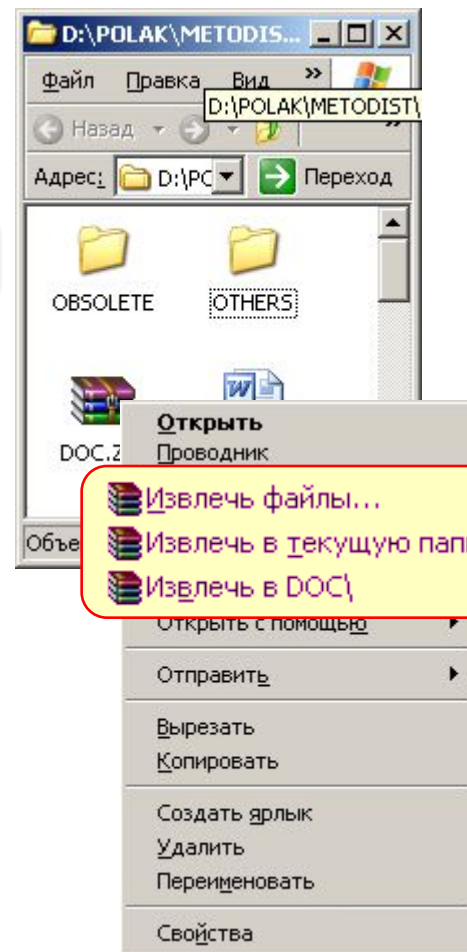


- Добавить в архив...
- Добавить в архив "Учебники.rar"
- Добавить в архив и отправить по e-mail...
- Добавить в архив "Учебники.rar" и отправить по e-mail

ПКМ

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

## Распаковка



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

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

# 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

---

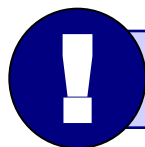
- **Файловые** – заражают файлы `*.exe`, `*.sys`, `*.dll` (редко – внедряются в тексты программ).
- **Загрузочные (бутовые, от англ. *boot* – загрузка)** – заражают загрузочные сектора дисков и дискет, при загрузке сразу оказываются в памяти и получают управление.
- **Полиморфные** – при каждом новом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

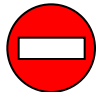
# Антивирусы-сканеры

---

- 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

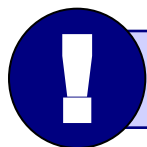


- замедление работы компьютера
- в случае ошибки ОС может выйти из строя

# 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))



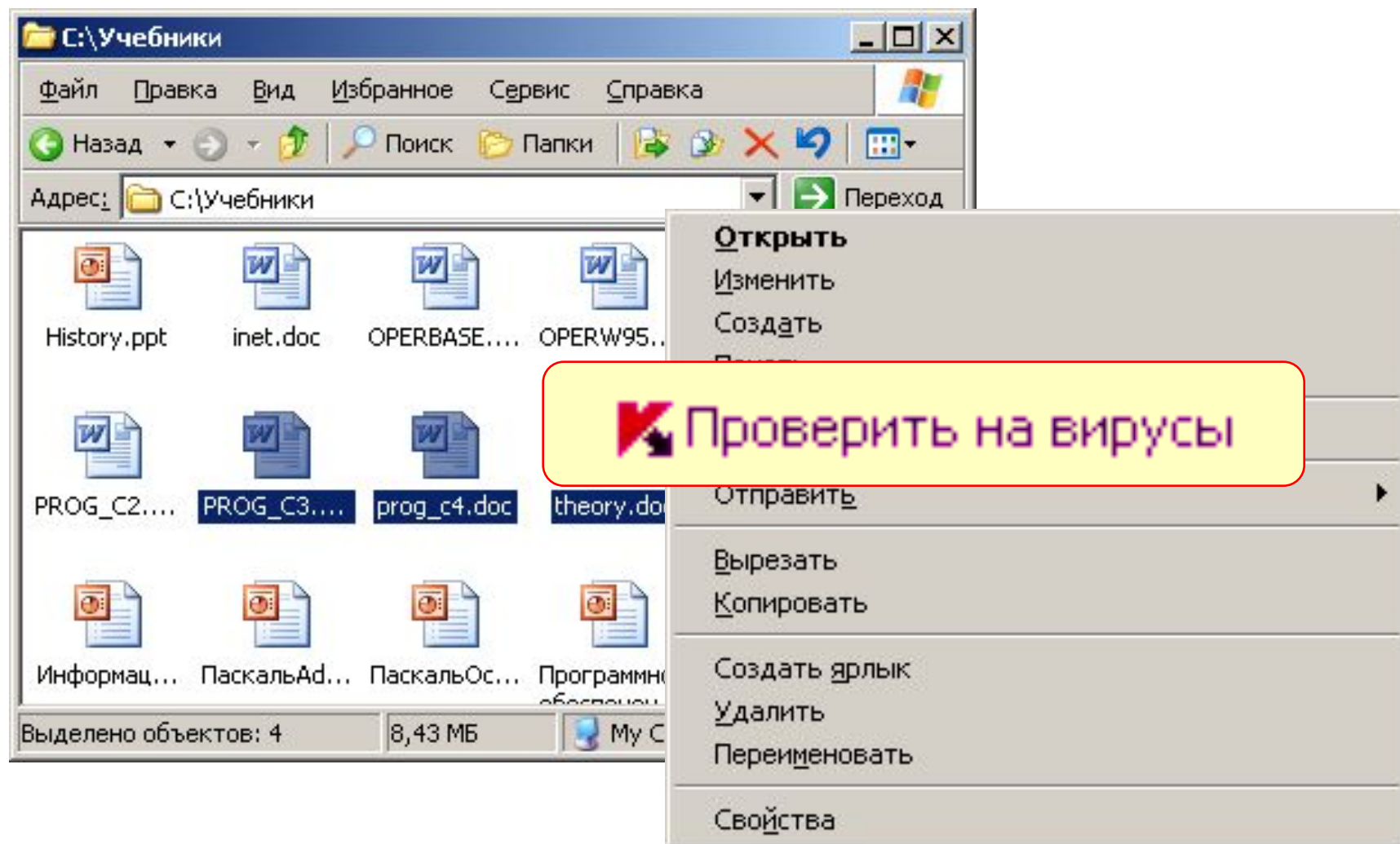
- **Файловый антивирус** (проверка файлов в момент обращения к ним)
- **Почтовый антивирус** (проверка входящих и исходящих сообщений)
- **Веб-антивирус** (Интернет, проверка *Web*-страниц)
- **Проактивная защита** (попытки обнаружить неизвестные вредоносные программы):
  - слежение за реестром
  - проверка 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 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. Below the options are buttons for 'Справка', 'OK', and 'Отмена'. At the bottom right of the main interface, a statistics table is visible:

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

Additional text in the interface includes 'Все вредоносные объекты обезврежены.', 'Просмотр статистики работы', and the website addresses 'kaspersky.ru' and 'viruslist.ru'.

**Проводник:** запуск через контекстное меню





# Антивирус *DrWeb* (сканер)

Запуск: Пуск – Сканер *DrWeb*

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

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

The scanner window displays the following settings:

Объекты	Вредоносные программы		
Инфицированные объекты	Вылечить	Рекламные программы	Удалить
Неизлечимые объекты	Удалить	Программы 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.!!!

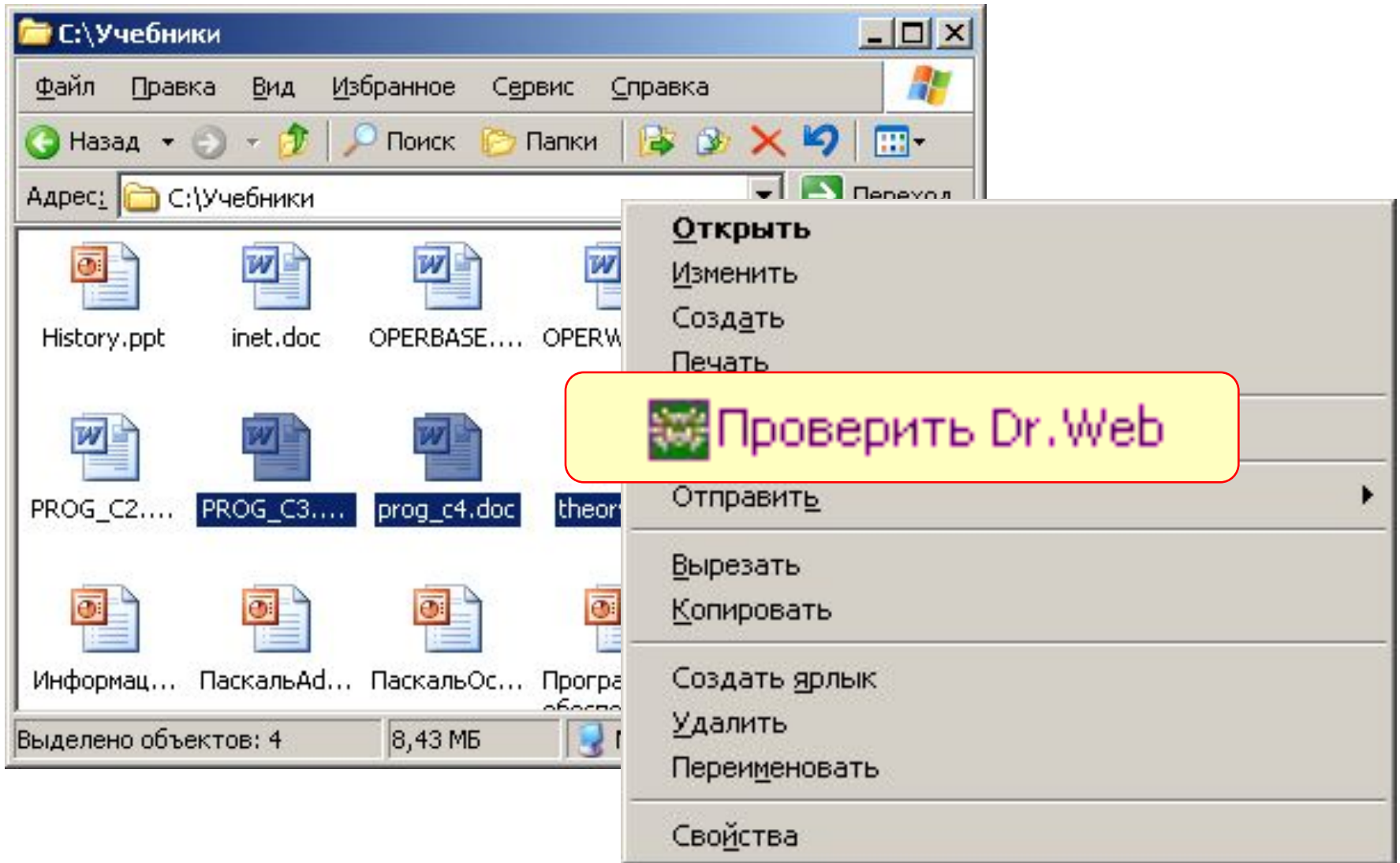
Buttons at the bottom: OK, Отмена, Применить, Справка





# 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

- устанавливаются 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

---