ИНФОРМАТИКА

Курс лекций и практических занятий

Шеметова А.Д.

Доцент кафедры Прикладной математики

Лекция 7

Программное обеспечение ЭВМ. Архиваторы и антивирусы

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`

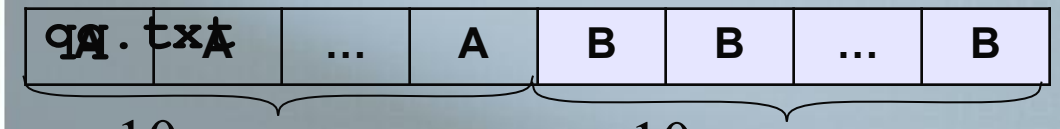
с потерями: при сжатии часть информации безвозвратно теряется

- 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



200 байт

Файл `qq.rle` (сжатый)

4

сжатие в 50 раз!

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

Влга впдт в Кспске мре.

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`)

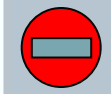
плохо

- 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*)

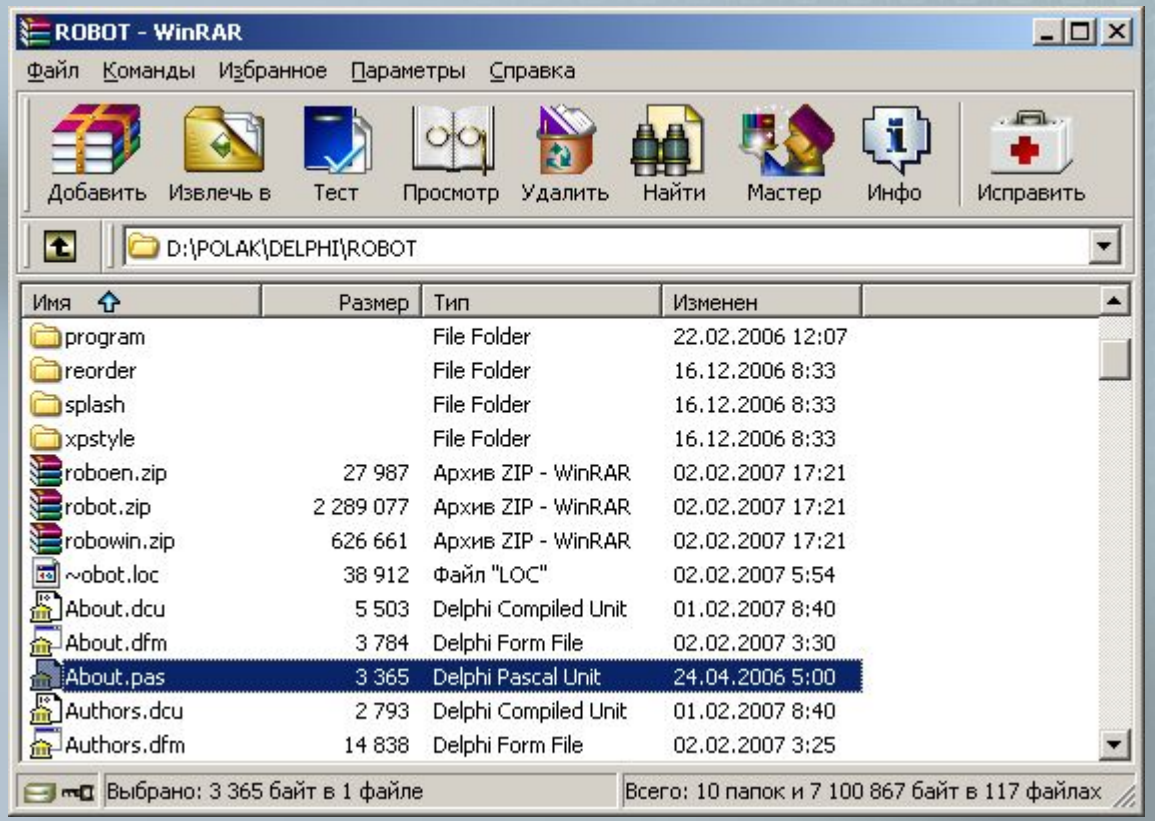
Запуск: *Пуск – WinRAR*

распаковать архив

сжать выделенные файлы

выйти из папки

двойной щелчок ЛКМ: войти в архив



сменить диск

изменить пароль

Архиватор WinRAR: упаковка

ЛКМ

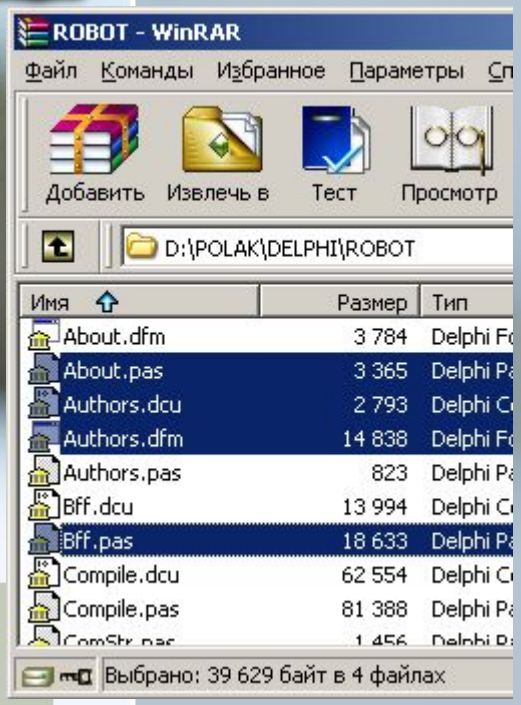
имя архива

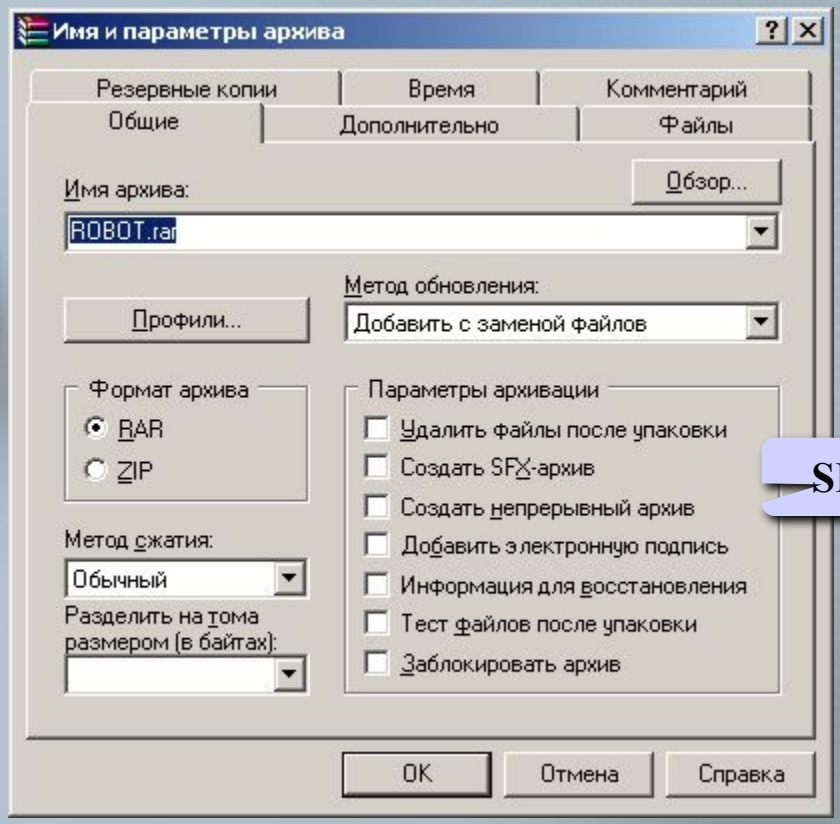
пароль

тип архива

SFX

многотомные архивы

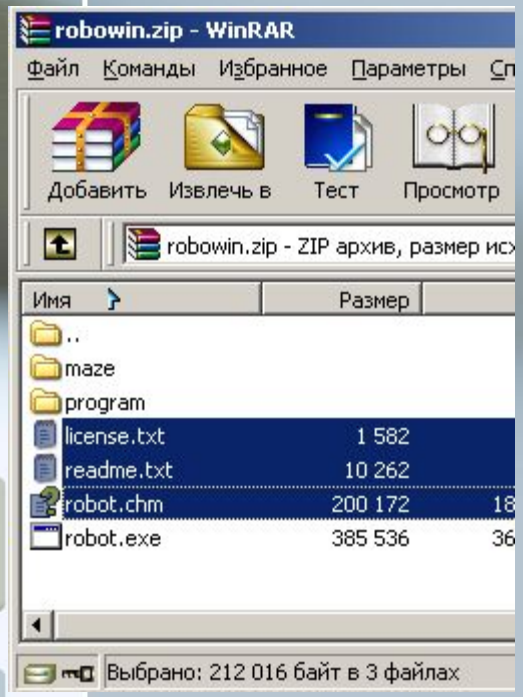


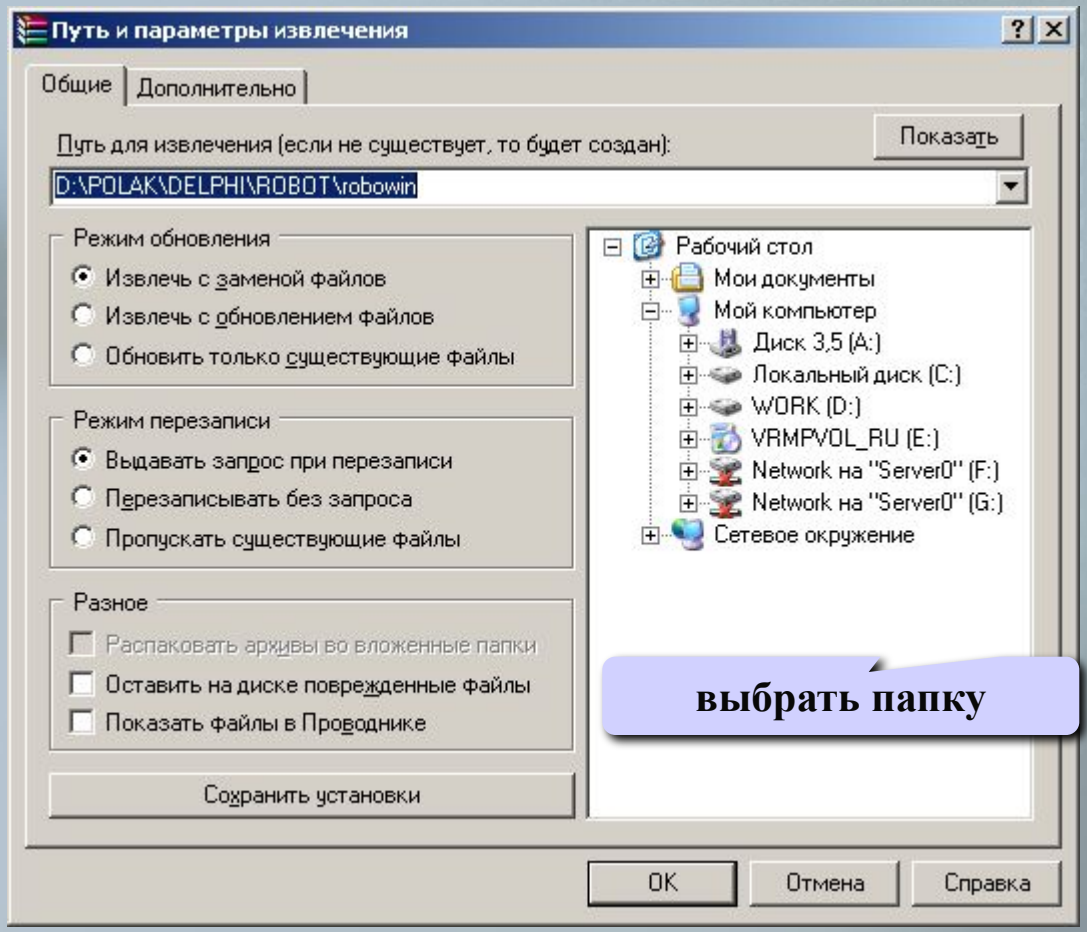


Архиватор WinRAR: распаковка

ЛКМ

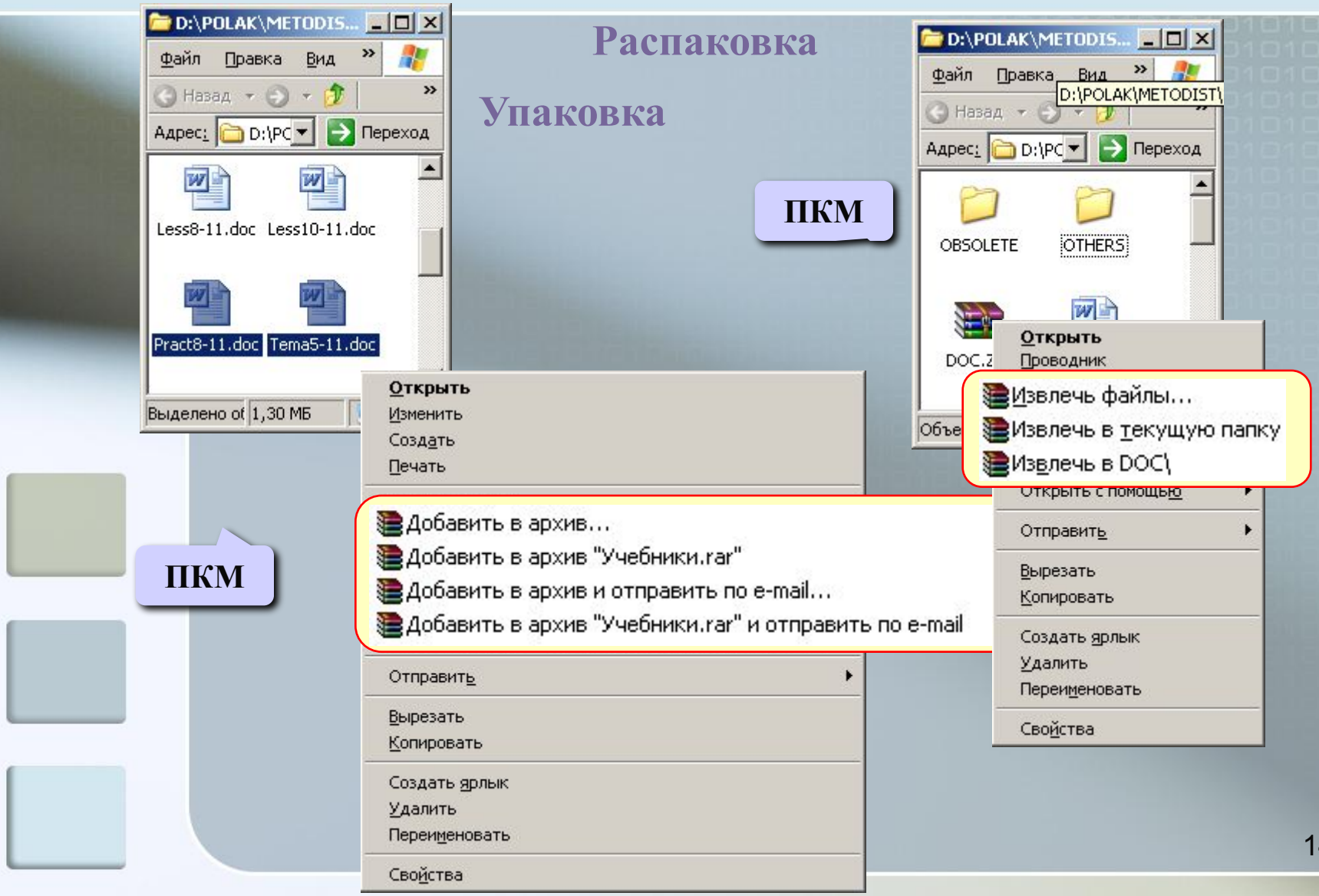
куда распаковать?





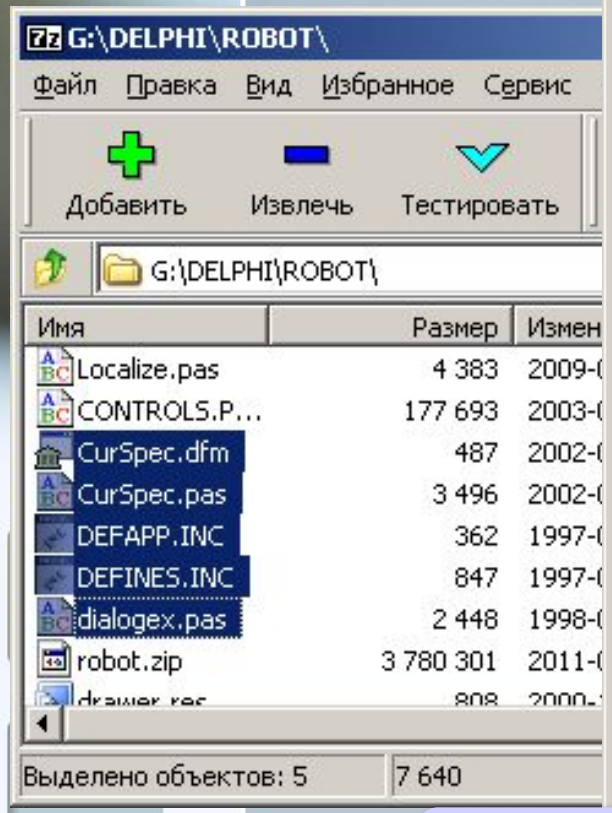
выбрать папку

Архиватор WinRAR в Проводнике



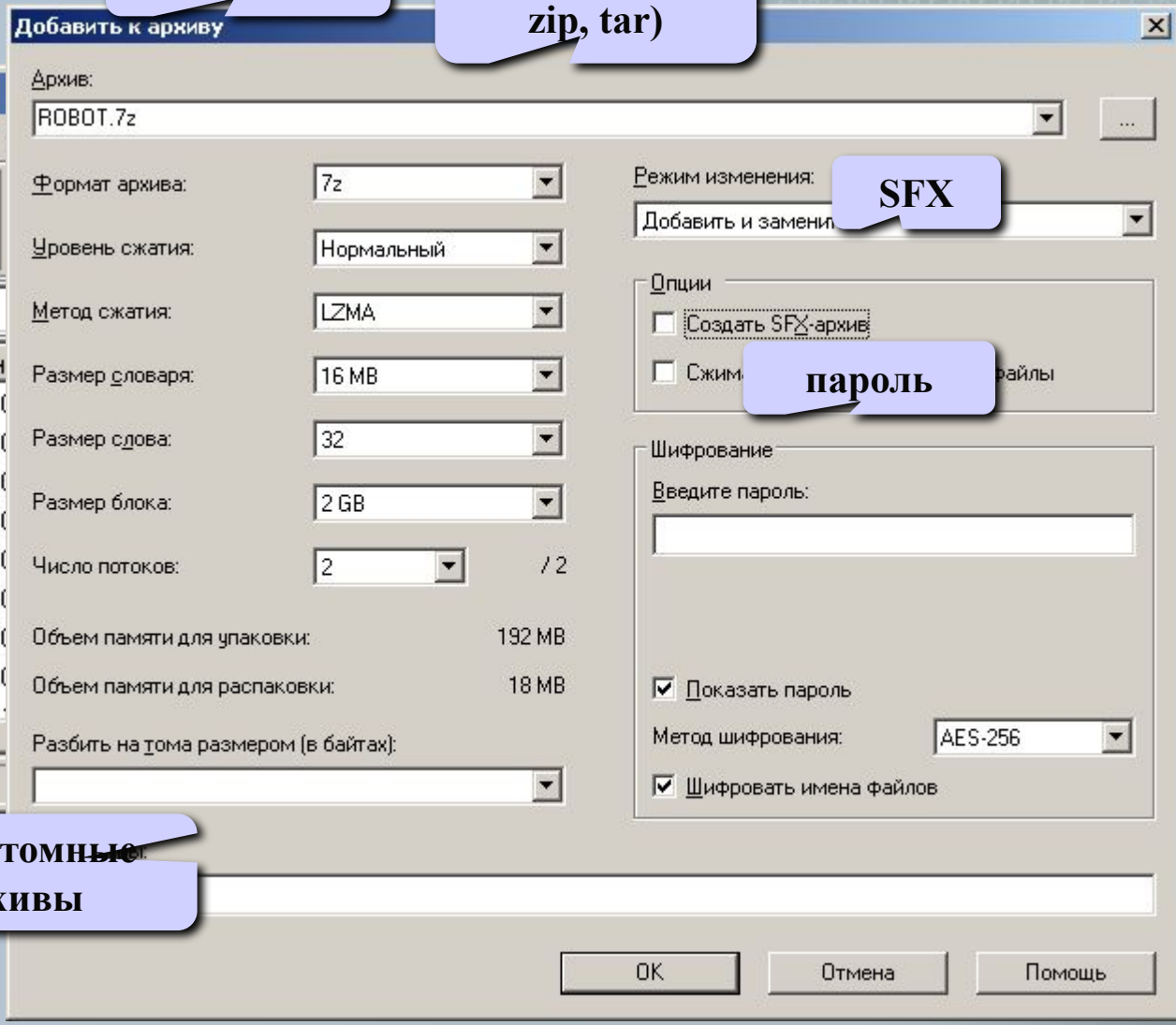
Архиватор 7Zip: упаковка

ЛКМ



имя архива

тип архива (7z, zip, tar)

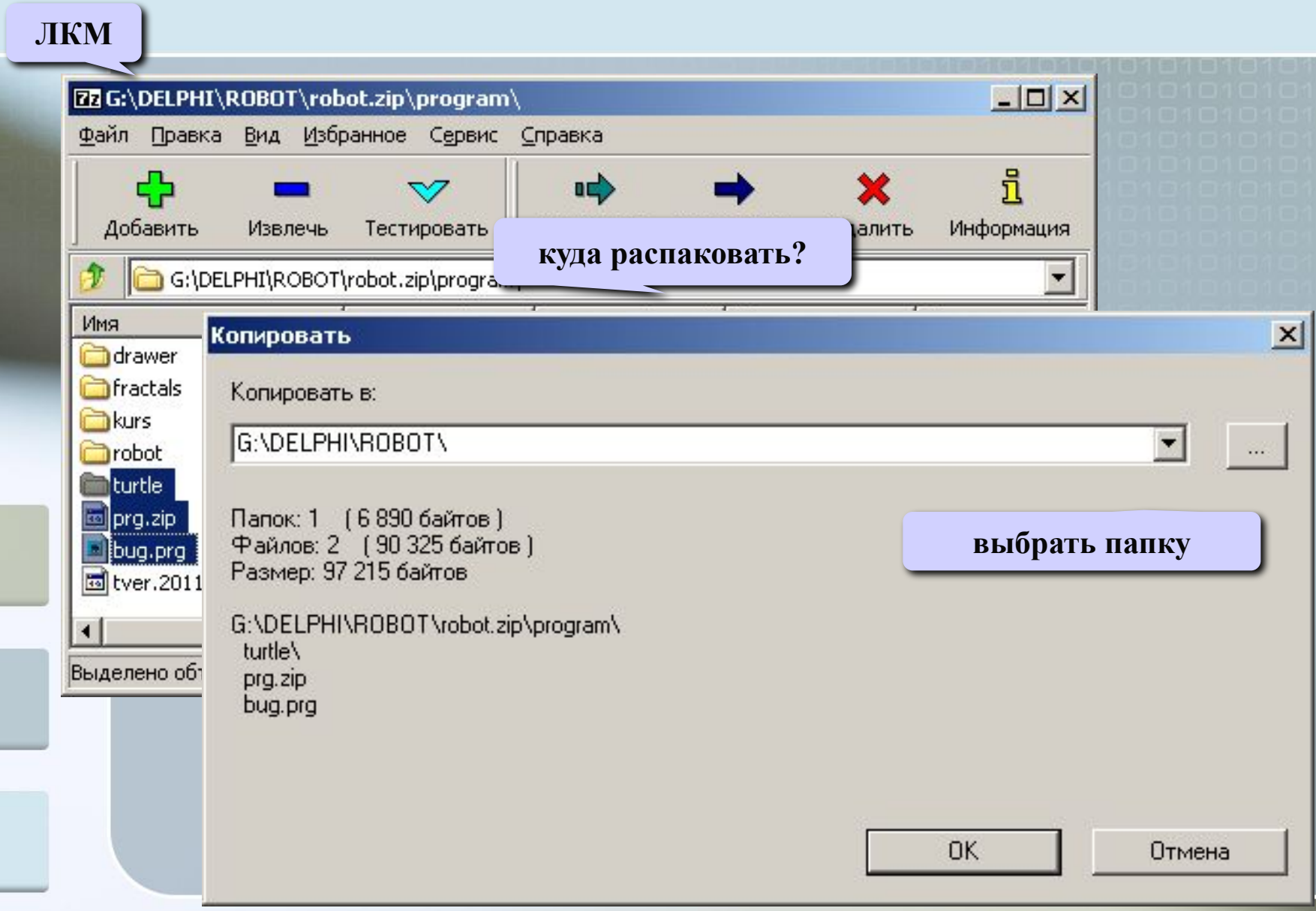


SFX

пароль

многотомные архивы

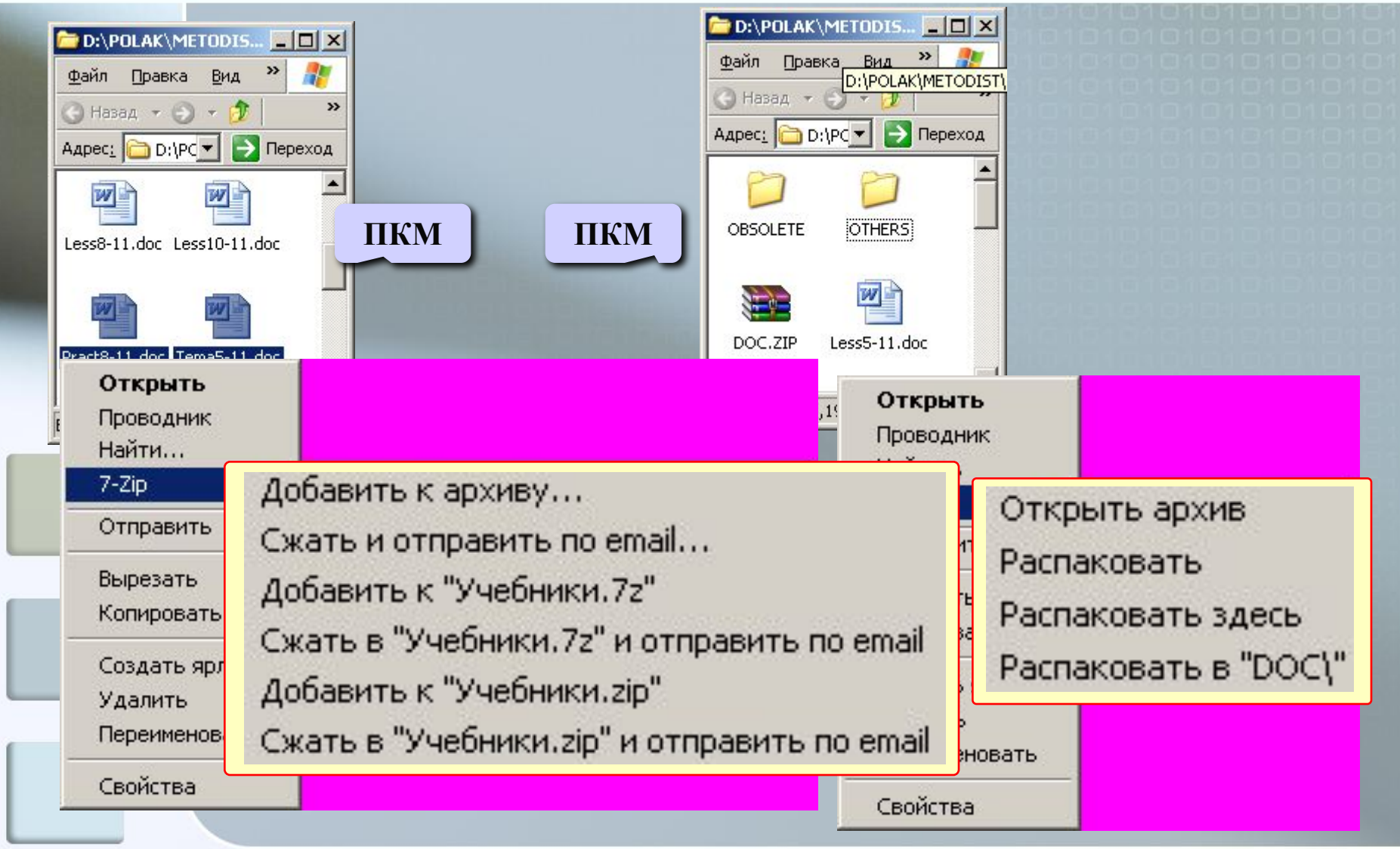
Архиватор 7Zip: распаковка



Архиватор 7Zip в Проводнике

Упаковка

Распаковка



Что такое вирус?

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

Вирусы действуют только программным путем. Они, как правило, присоединяются к файлу или проникают в тело файла. В этом случае говорят, что файл заражен вирусом. Вирус попадает в компьютер только вместе с зараженным файлом. Для активизации вируса нужно загрузить зараженный файл, и только после этого, вирус начинает действовать самостоятельно.

Действие вирусов может проявляться по разному: от разных визуальных эффектов, мешающих работать, до полной потери информации. Большинство вирусов заражают исполнительные программы, то есть файлы с расширением .EXE и .COM, хотя в последнее время большую популярность приобретают вирусы, распространяемые через систему электронной почты.

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`

не заражают

- текст – `*.txt`
- рисунки – `*.gif, *.jpg, *.png, *.tif`
- звук (`*.wav, *.mp3, *.wma`)
- видео (`*.avi, *.mpg, *.wmv`)

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.

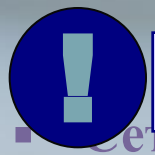
Макровирусы – заражают документы с макросами (**`*.doc, *.xls, *.mdb`**).

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

СТРУКТУРА КОМПЬЮТЕРНОГО ВИОРУСА

Условно выделяют две части вируса – голову и хвост.

Голова (загрузчик) – часть вируса, первой получающая управление.

Хвост (исполняемая часть) – это части вируса, расположенные отдельно от головы. Вирус без хвоста называют несегментированным.

Файловый нерезидентный вирус при запуске зараженной программы выполняет следующие действия:

- восстанавливает начало программы в оперативной памяти;
- находит очередную жертву;
- проверяет зараженность жертвы;
- внедряет тело вируса в программу- жертву;
- передает управление программе-вирусоносителю.

Жизненный цикл вируса

Различают два основных действия (фазы), выполняемых компьютерным вирусом: размножение и проявление. **Размножение** обычно является первым и обязательным действием вируса при получении им управления.

Фаза проявления, на которой выполняются несанкционированные действия, может чередоваться с размножением, начинаться через определенный период или при сочетании некоторых условий. Она может заключаться в изощренных визуальных или звуковых эффектах. Вирусы-вандалы на фазе проявления наносят повреждения файловой системе, вносят ошибки в данные или нарушают работу ПК.

Кроме того, возможна **латентная фаза**, когда нет размножения и проявления. Это может быть обусловлено:

системным временем (пятница, 13-е);

конфигурацией (должен быть винчестер);

аппаратными особенностями (только на клонах IBM PC).

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)

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)

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

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 удается, то могла быть испорчена таблица разделов диска. Тогда …
- создать заново таблицу разделов (**fdisk.exe**). Если не удается (винчестер не обнаружен), то…
- можно нести компьютер в ремонт.

Спасибо за внимание