

Тема 3.3.

Антивирусные средства защиты информации

1. Характеристика компьютерных вирусов
2. Программы обнаружения и защиты от вирусов

Что такое вирус?

Компьютерный вирус – это программа, которая при запуске способна распространяться без участия человека.

Вредные действия:

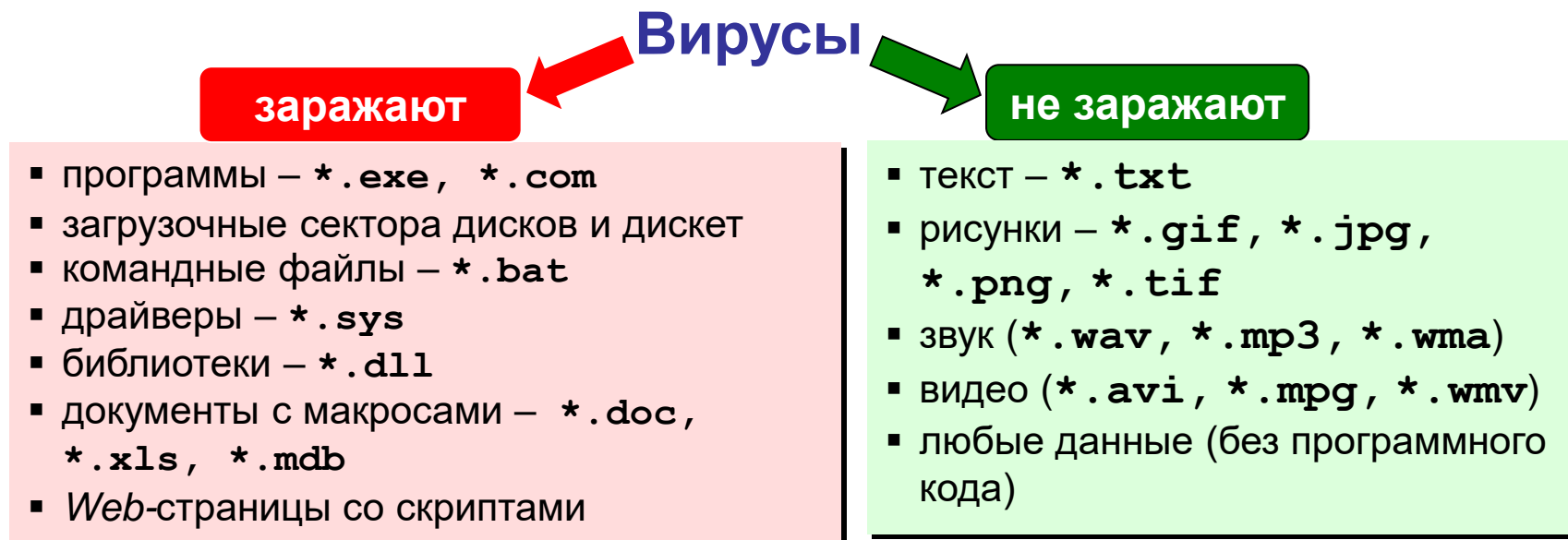
- ☐ звуковые и зрительные эффекты
- ☐ имитация сбоев ОС и аппаратуры
- ☐ перезагрузка компьютера
- ☐ разрушение файловой системы
- ☐ уничтожение информации
- ☐ передача секретных данных через Интернет
- ☐ массовые атаки на сайты Интернет

Признаки:

- ☐ замедление работы компьютера
- ☐ перезагрузка или зависание компьютера
- ☐ неправильная работа ОС или прикладных программ
- ☐ изменение длины файлов
- ☐ появление новых файлов
- ☐ уменьшение объема оперативной памяти

Что заражают вирусы?

Для того, чтобы вирус смог выполнить какие-то действия, он должен оказаться в памяти в виде **программного кода** и получить управление.



Основные способы заражения

- ☐ Запустить зараженный файл.
- ☐ Загрузить компьютер с зараженной дискеты или диска.
- ☐ Открыть зараженный документ *Word* или *Excel*.
- ☐ Открыть сообщение e-mail с вирусом.
- ☐ Открыть Web-страницу с активным содержимым (ActiveX)

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)

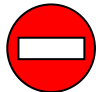
- ❑ **Backdoor** – программы удаленного администрирования
- ❑ **воровство паролей** (доступ в Интернет, к почтовым ящикам, к платежным системам)
- ❑ **шпионы** (введенный с клавиатуры текст, снимки экрана, список программ, характеристики компьютера, промышленный шпионаж)
- ❑ **DOS-атаки** (англ. *Denial 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



1) не могут предотвратить заражение

2) 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



- 1) непрерывное наблюдение
- 2) блокируют вирус в момент заражения
- 3) могут бороться с неизвестными вирусами



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

Антивирусные программы

Коммерческие

- ☐ Антивирус Касперского (www.kaspersky.ru)
- ☐ DrWeb (www.drweb.com)
- ☐ Norton Antivirus (www.symantec.com)
- ☐ McAfee (www.mcafee.ru)
- ☐ NOD32 (www.eset.com)



Есть бесплатные пробные версии!

Бесплатные

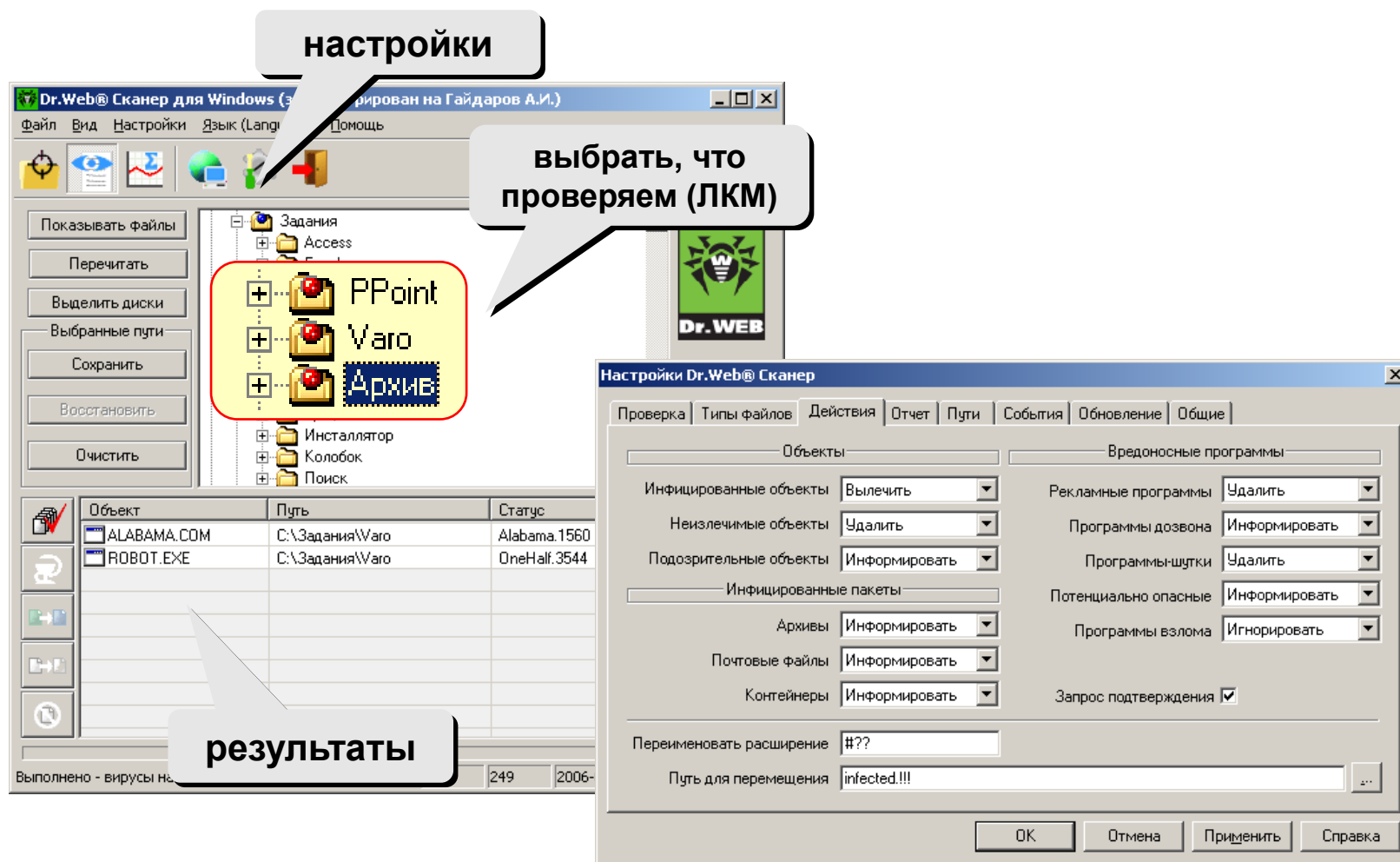
- ☐ Avast Home (www.avast.com)
- ☐ Antivir Personal (free-av.com)
- ☐ AVG Free (free.grisoft.com)



AVG

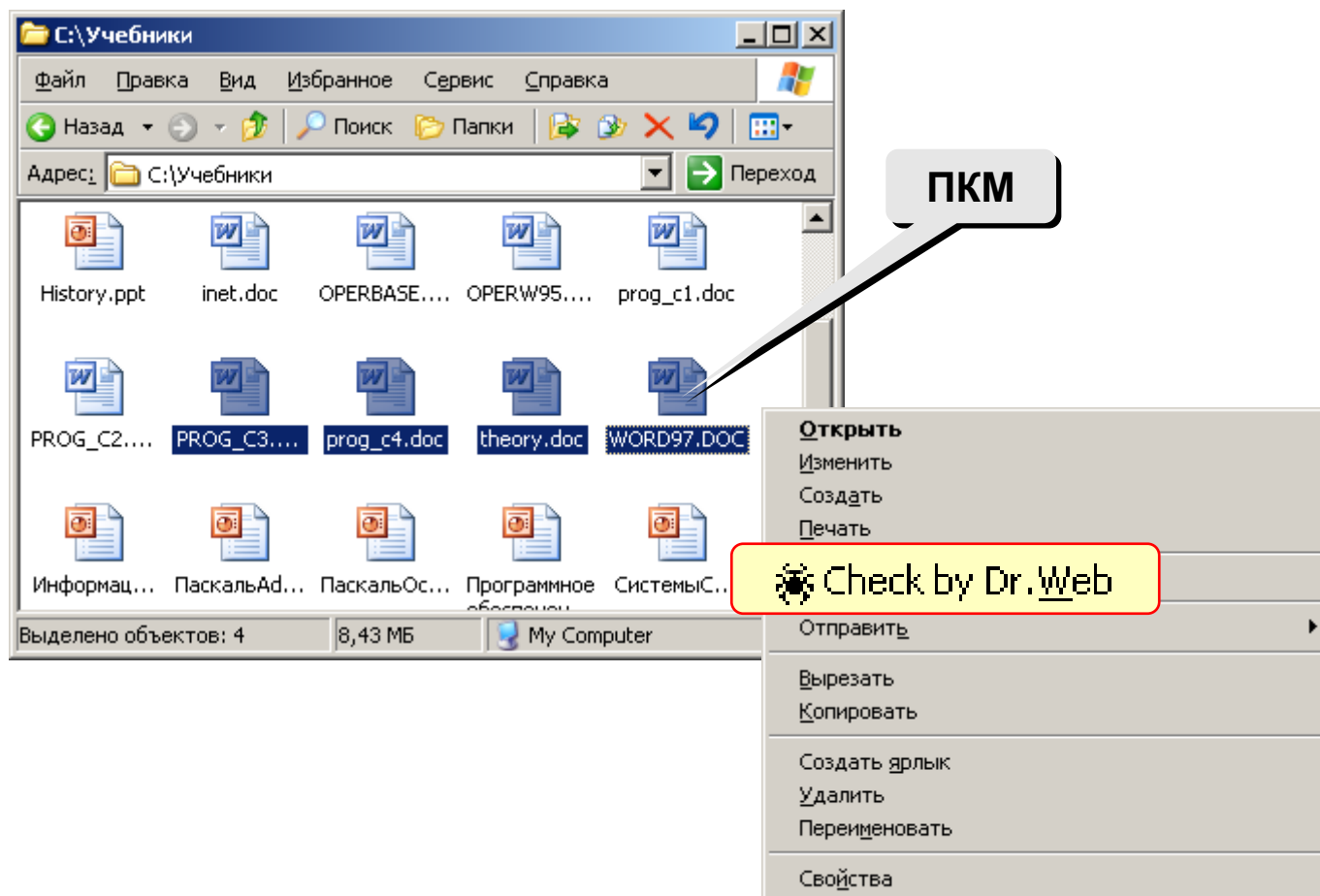
Антивирус *DrWeb* (сканер)

Запуск: Пуск – Сканер DrWeb



Антивирус *DrWeb*

Проводник: запуск *DrWeb* 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.