

Программное обеспечение

Тема 7. Компьютерные вирусы и антивирусы

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.

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)

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)

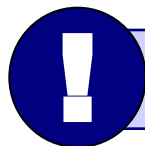
Классические вирусы

- ❑ **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)

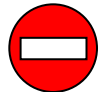
- ❑ **Backdoor** – программы удаленного администрирования
- ❑ **воровство паролей** (доступ в Интернет, к почтовым ящикам, к платежным системам)
- ❑ **шпионы** (введенный с клавиатуры текст, снимки экрана, список программ, характеристики компьютера, промышленный шпионаж)
- ❑ **DOS-атаки** (англ. *Denial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

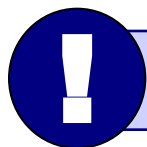


- 1) замедление работы компьютера
- 2) в случае ошибки ОС может выйти из строя

Антивирусные программы

Коммерческие

- ❑ 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

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



Возможности:

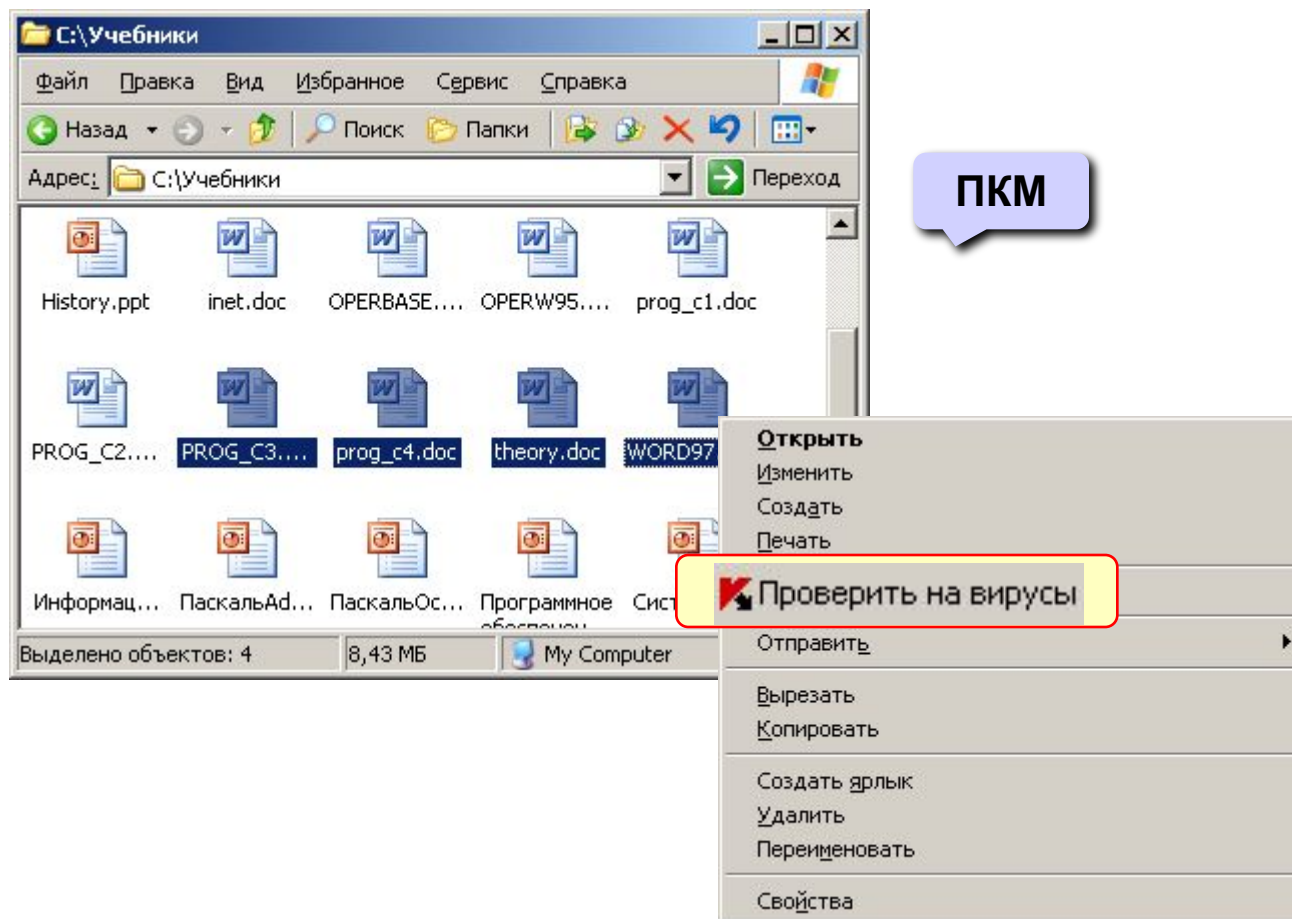
- ❑ **Файловый антивирус** (проверка файлов в момент обращения к ним)
- ❑ **Почтовый антивирус** (проверка входящих и исходящих сообщений)
- ❑ **Веб-антивирус** (Интернет, проверка *Web*-страниц)
- ❑ **Проактивная защита** (попытки обнаружить неизвестные вредоносные программы):
 - слежение за реестром
 - 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 vertical menu lists several options: "Проверка Моего Компьютера", "Поиск вирусов...", "Обновление", "Мониторинг сети", "Настройка...", "Антивирус Касперского", "Приостановка защиты...", and "Выход". Red arrows point from these menu items to the corresponding windows in the main interface. The main interface shows a taskbar with several windows: "1% - Проверка Моего Компьютера", "Антивирус Касперского 6.0 для Windows Workstations", "14% - Обновление", "Анти-Хакер: Мониторинг сети", "Настройка: Антивирус Касперского", and "Антивирус Касперского 6.0 для Windows Workstations". The "Настройка" window is active, showing the "Приостановка защиты" (Pause Protection) dialog box. The dialog box has a title bar "Приостановка защиты" and a close button. The main text reads "Защита будет автоматически включена:" followed by three radio button options: "Через 1 минуту" (selected), "После перезапуска приложения", and "Только по требованию пользователя". At the bottom of the dialog 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*

настройки

The screenshot shows the Dr.Web Scanner application window. A callout box labeled "настройки" points to the "Настройки" menu item in the top menu bar. Another callout box labeled "выбрать, что проверяем (ЛКМ)" points to the "Задания" (Tasks) folder in the left sidebar, which is expanded to show sub-items: "Access", "PPoint", "Varo", and "Архив". A red box highlights these sub-items. A third callout box labeled "результаты" points to the main results table at the bottom of the window.

Объект	Путь	Статус
ALABAMA.COM	C:\Задания\Varo	Alabama.1560
ROBOT.EXE	C:\Задания\Varo	OneHalf.3544

выбрать, что проверяем (ЛКМ)

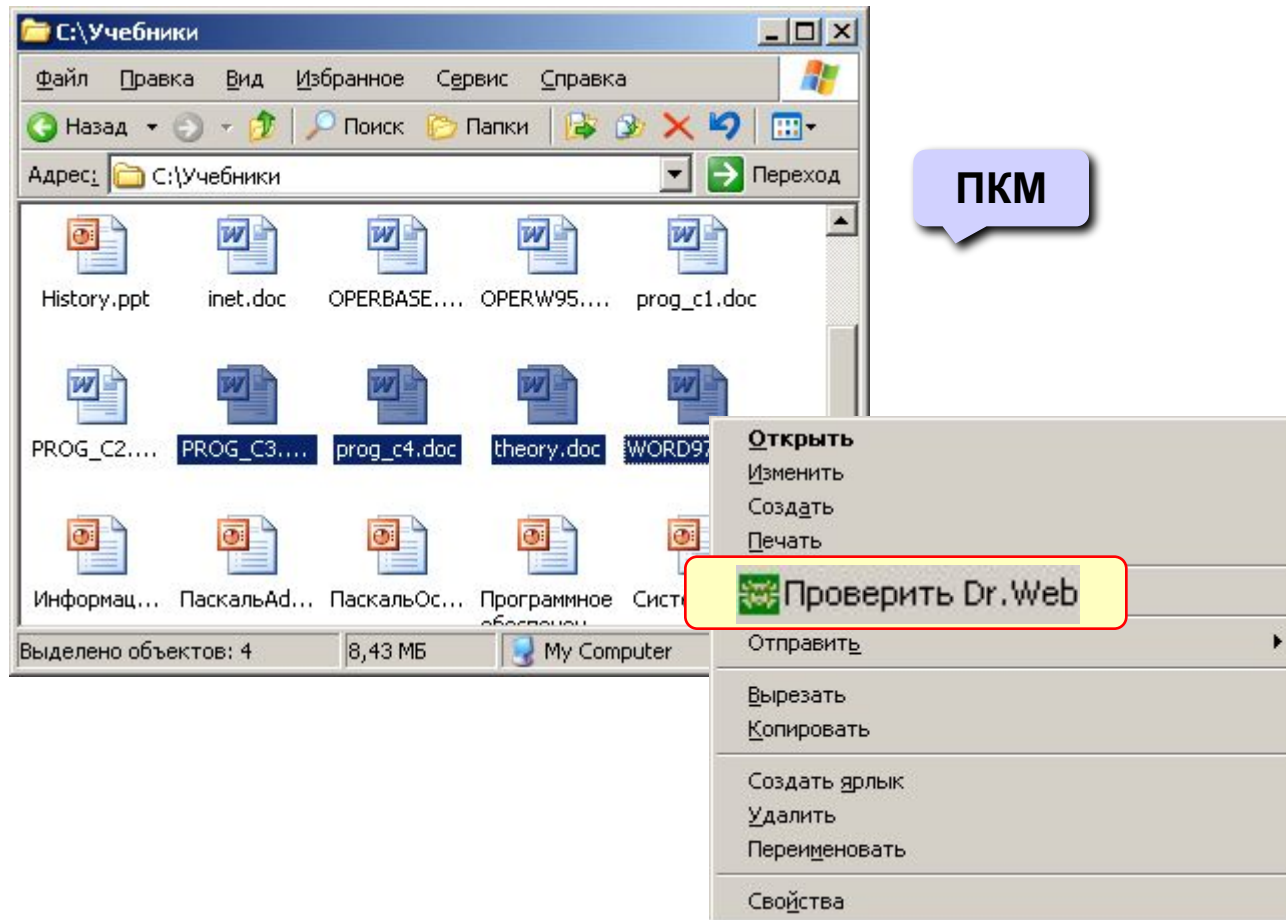
The screenshot shows the "Настройки Dr.Web@ Сканер" (Dr.Web Scanner Settings) dialog box. It has several tabs: "Проверка", "Типы файлов", "Действия", "Отчет", "Пути", "События", "Обновление", and "Общие". The "Действия" (Actions) tab is active. It contains two main sections: "Объекты" (Objects) and "Вредоносные программы" (Malicious programs). The "Объекты" section has dropdown menus for "Инфицированные объекты" (Infected objects), "Неизличимые объекты" (Unidentifiable objects), "Подозрительные объекты" (Suspicious objects), "Архивы" (Archives), "Почтовые файлы" (Mail files), and "Контейнеры" (Containers). The "Вредоносные программы" section has dropdown menus for "Рекламные программы" (Adware), "Программы дозвона" (Dialers), "Программы-шутки" (Jokes), "Потенциально опасные" (Potentially dangerous), and "Программы взлома" (Crackers). There is also a checked checkbox for "Запрос подтверждения" (Request confirmation). At the bottom, there are fields for "Переименовать расширение" (Rename extension) and "Путь для перемещения" (Move path). Buttons for "OK", "Отмена" (Cancel), "Применить" (Apply), and "Справка" (Help) are at the bottom.

результаты



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
