

# **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](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

-  Security Essential  
([http://www.microsoft.com/security\\_essentials/](http://www.microsoft.com/security_essentials/))
-  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))

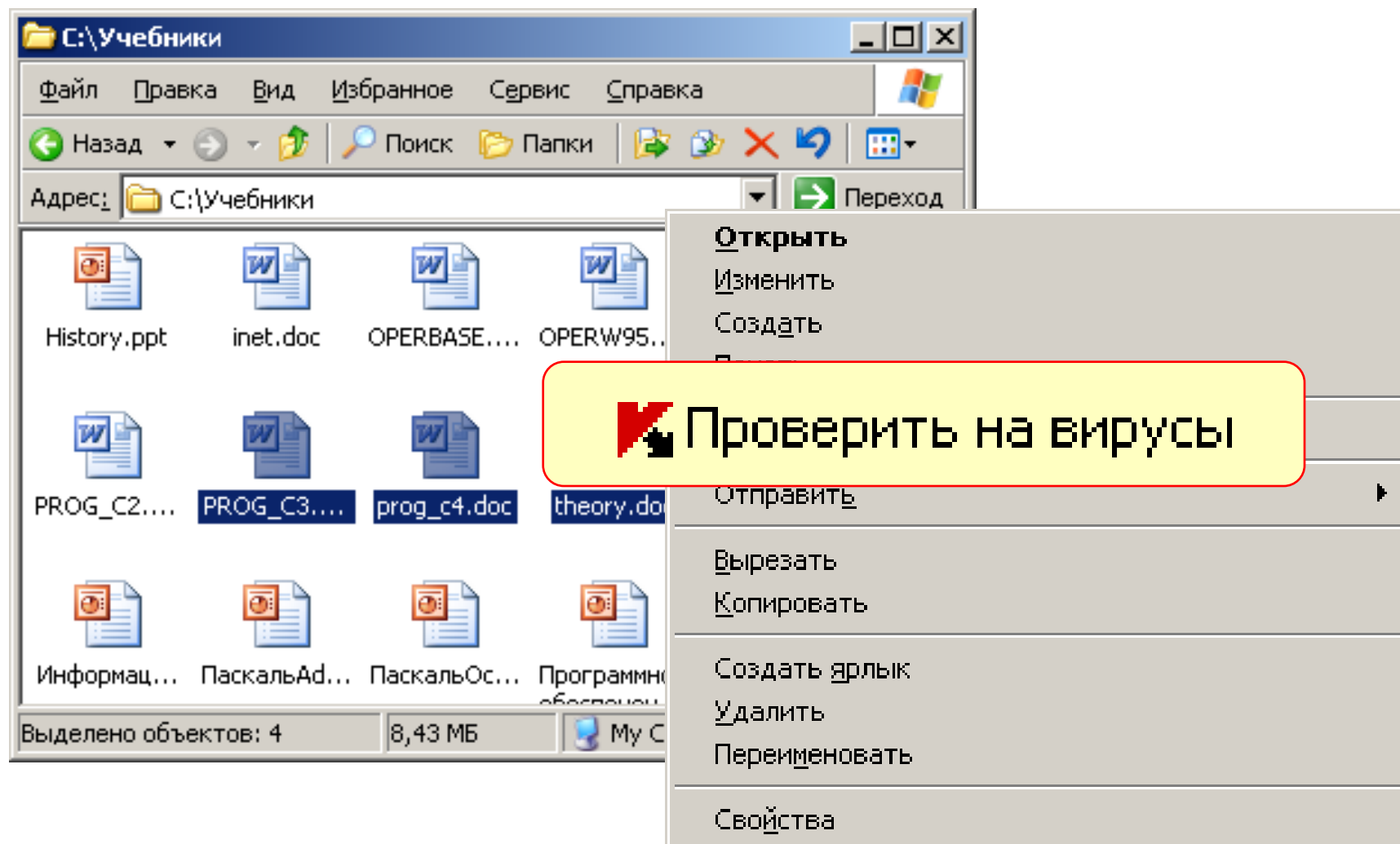
- **Файловый антивирус** (проверка файлов в момент обращения к ним)
- **Почтовый антивирус** (проверка входящих и исходящих сообщений)
- **Веб-антивирус** (Интернет, проверка *Web*-страниц)
- **Проактивная защита** (попытки обнаружить неизвестные вредоносные программы):
  - слежение за реестром
  - проверка 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 the 'Приостановка защиты' dialog box. The dialog box has the title 'Приостановка защиты' and contains the text: 'Защита будет автоматически включена:'. There are three radio button options: 'Через 1 минуту' (selected), 'После перезапуска приложения', and 'Только по требованию пользователя'. At the bottom of the dialog box are buttons for 'Справка', 'OK', and 'Отмена'. The background 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 scanning, and a file explorer on the left. The file explorer shows a folder structure with "Задания" expanded, containing "Access", "Excel", "PPoint", "Varo", and "Архив". The "Архив" folder is highlighted with a red box and a yellow callout bubble. The main scanning area is titled "Свойства сканируемых объектов" and contains two columns of settings: "Объекты" and "Вредоносные программы". The "Объекты" column includes settings for "Инфицированные объекты" (Вылечить), "Неизлечимые объекты" (Удалить), "Подозрительные объекты" (Информировать), "Инфицированные пакеты", "Архивы" (Информировать), "Почтовые файлы" (Информировать), and "Контейнеры" (Информировать). The "Вредоносные программы" column includes settings for "Рекламные программы" (Удалить), "Программы дозвона" (Информировать), "Программы-шутки" (Удалить), "Потенциально опасные" (Информировать), "Программы взлома" (Игнорировать), and "Запрос подтверждения" (checked). At the bottom, there are fields for "Переименовать расширение" (set to "##?") and "Путь для перемещения" (set to "infected!!!"). The status bar at the bottom left indicates "Выполнено - вирусы найдены".

**настройки**

**выбрать, что проверяем (ЛКМ)**

**результ**

Выполнено - вирусы найдены

| Объекты                | Вредоносные программы                                    |
|------------------------|--|
| Инфицированные объекты | Рекламные программы                                      |
| Неизлечимые объекты    | Программы дозвона  |
| Подозрительные объекты | Программы-шутки  |
| Инфицированные пакеты  | Потенциально опасные                                     |
| Архивы                 | Программы взлома   |
| Почтовые файлы         | Запрос подтверждения <input checked="" type="checkbox"/> |
| Контейнеры             |  |

Переименовать расширение: ##?

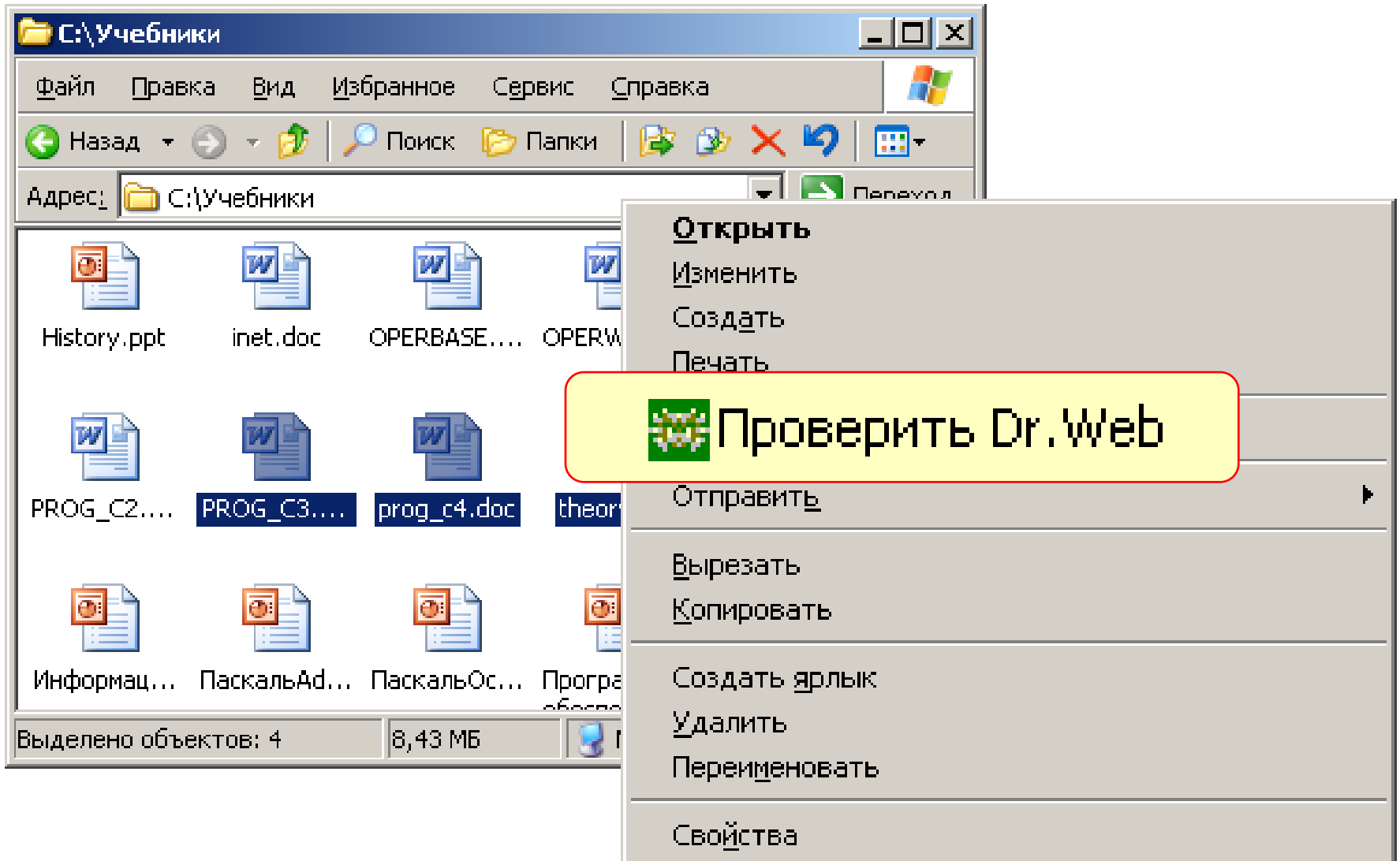
Путь для перемещения: infected!!!

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.

# Конец фильма

---