

Вирусы и антивирусные программы

*Виды компьютерных вирусов.
Антивирусные программы.*





Что такое вирус???

- **Вирус** – это программа, которая может «размножаться» и скрытно внедрять свои копии в файлы, загрузочные секторы дисков и документы.
- Активизация компьютерного вируса может вызвать уничтожение программ и данных, и даже уничтожение составляющих компьютера (системного блока).

200 - 5000 байт

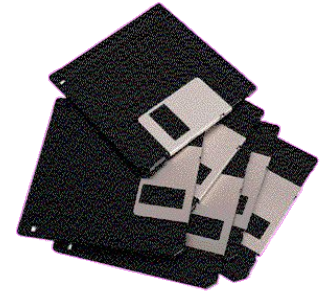
более 50 тыс. вирусов

Признаки появления вирусов:

- ▣ Неправильная работа нормально работающих программ**
- ▣ Частые зависания и сбои в работе ПК**
- ▣ Медленная работа ПК**
- ▣ Изменение размеров файлов**
- ▣ Исчезновение файлов и каталогов**
- ▣ Неожиданное увеличение количество файлов на диске**
- ▣ Уменьшение размеров свободной оперативной памяти**
- ▣ Вывод на экран неожиданных сообщений и изображений**
- ▣ Подача непредусмотренных звуковых сигналов**
- ▣ Невозможность загрузки операционной системы**


Классификация вирусов

- ▣ Загрузочные вирусы*
- ▣ Файловые вирусы*
- ▣ Макро-вирусы*
- ▣ Сетевые вирусы*



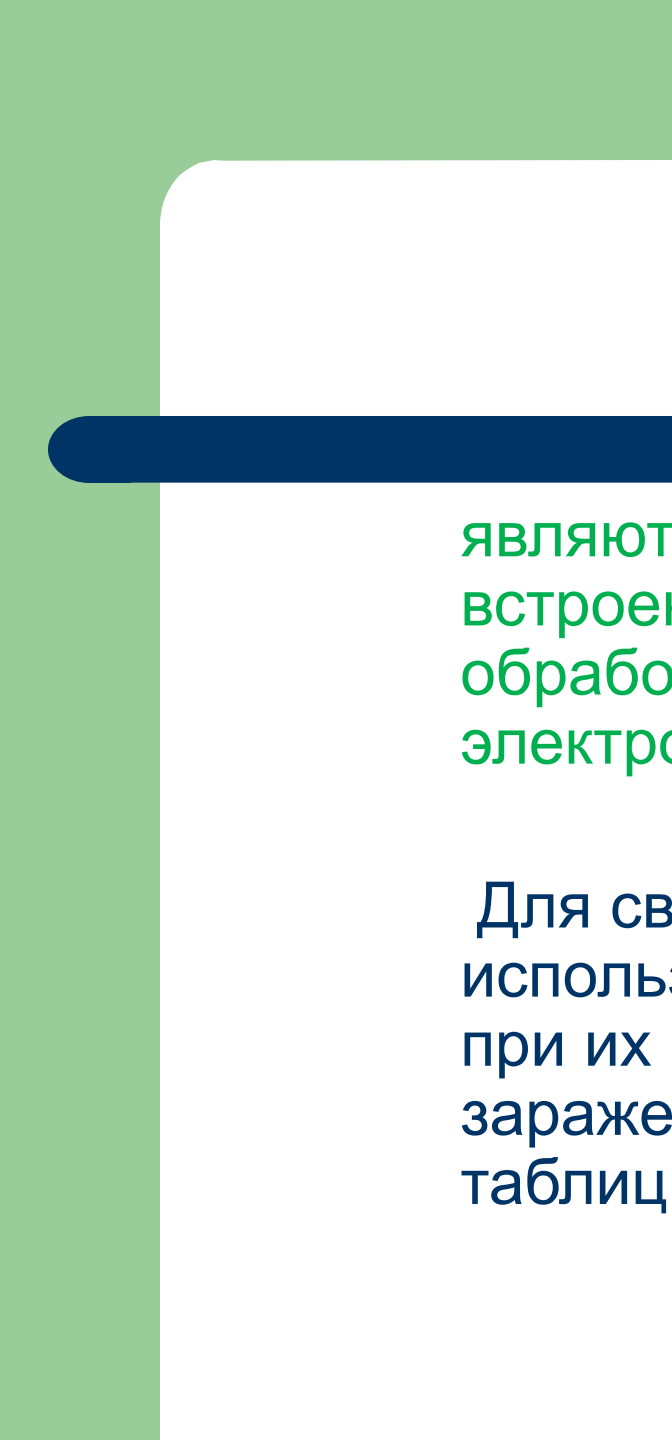
заражают загрузочный сектор гибкого диска или винчестера.

При заражении дисков загрузочный вирус «заставляет» систему при ее перезапуске считать в память и отдать управление не программному коду загрузчика операционной системы, а коду вируса.



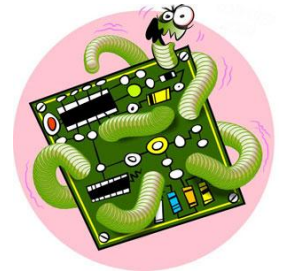
при своем размножении тем или иным способом используют файловую систему операционной системы.

Файловые вирусы могут поражать исполняемые файлы различных типов (EXE, COM, BAT, SYS и др.).



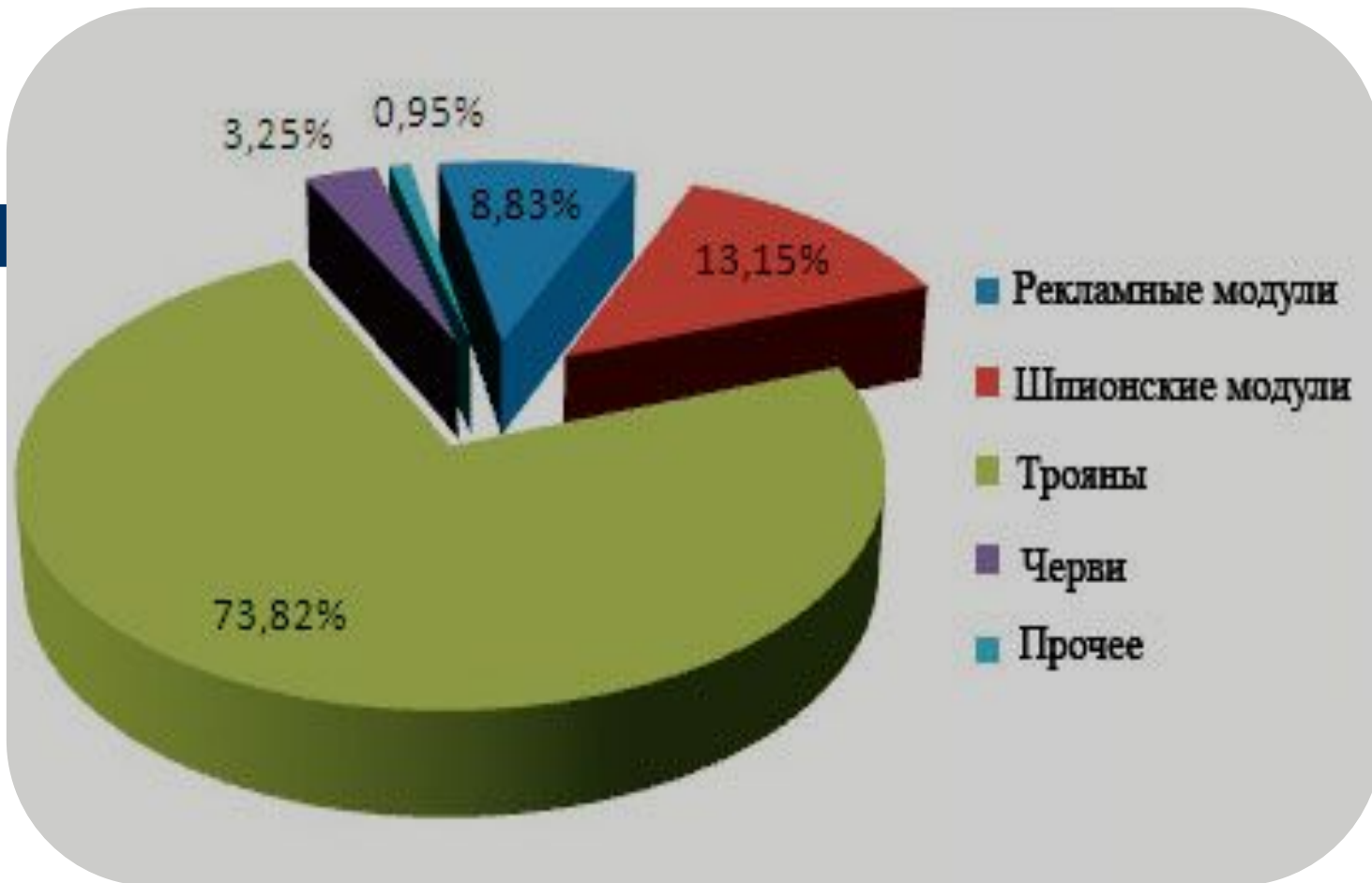
являются программами на языках, встроенных в некоторые системы обработки данных (текстовые редакторы, электронные таблицы и т.д.).

Для своего размножения такие вирусы используют возможности макро-языков и при их помощи переносят себя из одного зараженного файла (документа или таблицы) в другие.



для своего распространения используют протоколы и возможности локальных и глобальных компьютерных сетей.

Основным принципом работы сетевых вирусов является возможность передать и запустить свой код на удаленном компьютере.



Распространенные виды вирусов

Вирусы делятся на резидентные и нерезидентные

Первые, в отличие от нерезидентных, при получении управления загружаются в память и могут действовать не только во время работы зараженного файла.

Хакерские утилиты и прочие вредоносные программы

К данной категории относятся:

- утилиты автоматизации создания вирусов, червей и троянских программ (конструкторы);
- программные библиотеки, разработанные для создания вредоносного ПО;
- хакерские утилиты скрытия кода зараженных файлов от антивирусной проверки (шифровальщики файлов);
- «злые шутки», затрудняющие работу с компьютером;
- программы, сообщающие пользователю заведомо ложную информацию о своих действиях в системе;
- прочие программы, тем или иным способом намеренно наносящие прямой или косвенный ущерб данному или удалённым компьютерам.



Каналы распространения

- **Флеш-накопители**

В настоящее время USB-флешки заменяют дискеты и повторяют их судьбу — большое количество вирусов распространяется через съёмные накопители, включая цифровые фотоаппараты, цифровые видеокамеры, цифровые плееры (MP3-плееры), сотовые телефоны. Использование этого канала преимущественно обусловлено возможностью создания на накопителе специального файла **autorun.inf**, в котором можно указать программу, запускаемую Проводником Windows при открытии такого накопителя. Флешки — основной источник заражения для компьютеров.



- **Электронная почта**

Сейчас один из основных каналов распространения вирусов. Обычно вирусы в письмах электронной почты маскируются под безобидные вложения: картинки, документы, музыку, ссылки на сайты.



- **Системы обмена мгновенными сообщениями**

Так же распространена рассылка ссылок на якобы фото, музыку либо программы, в действительности являющиеся вирусами, по ICQ и через другие программы мгновенного обмена сообщениями.



- **Веб-страницы**

Возможно также заражение через страницы Интернет ввиду наличия на страницах всемирной паутины различного «активного» содержимого: скриптов, ActiveX-компоненты, Java-апплетов



Антивирусные программы



*Для обнаружения, удаления и защиты от компьютерных вирусов разработаны специальные программы, которые позволяют обнаруживать и уничтожать вирусы. Такие программы называются **антивирусными**.*

avast!
Professional

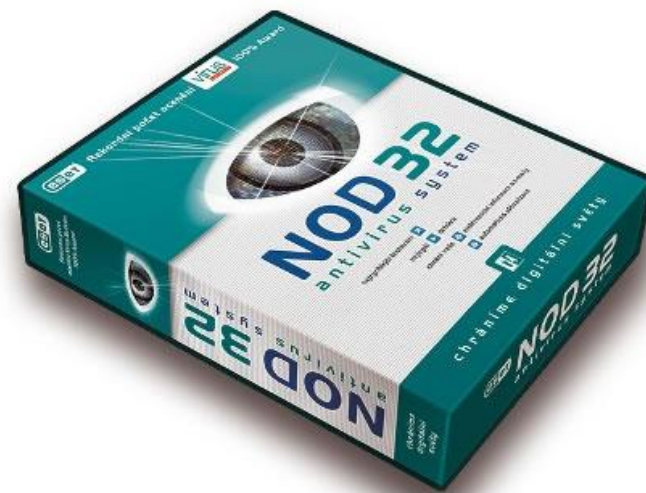


Их параметры...

Для быстрой и эффективной работы антивирусная программа должна отвечать некоторым параметрам:

- ✓ *стабильностью и надежностью*
- ✓ *размером вирусной базы программы*
- ✓ *многоплатформенностью*

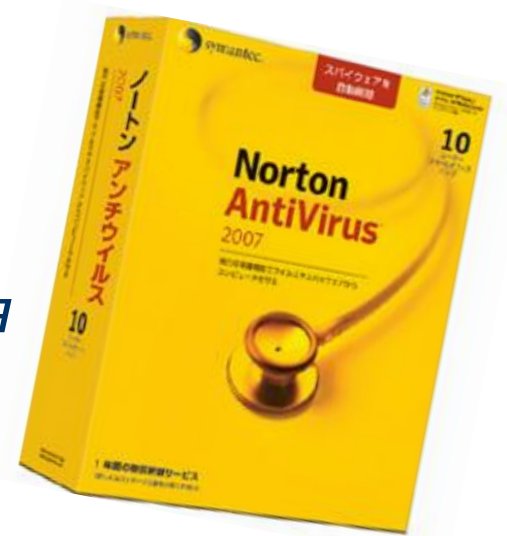
- ✓ *Антивирусные блокировщики*
- ✓ *Ревизоры*
- ✓ *Полифаги*
- ✓ *Полифаги-мониторы*



Антивирусные блокировщики

резидентные программы, которые перехватывают «вирусоопасные» ситуации и сообщают об этом пользователю.

Например, «вирусоопасной» является запись в загрузочные сектора дисков, которую можно запретить с помощью программы BIOS Setup



Ревизоры



Принцип работы основан на подсчете контрольных сумм для хранящихся на диске файлов. Эти суммы, а также некоторая другая информация (длины файлов, даты их последней модификации и др.) сохраняются в базе данных антивируса.

При последующем запуске ревизоры сверяют данные, содержащиеся в базе данных, с реально подсчитанными значениями. Если информация о файле, записанная в базе данных, не совпадает с реальными значениями, то ревизоры сигнализируют о том, что файл был изменен или заражен вирусом.

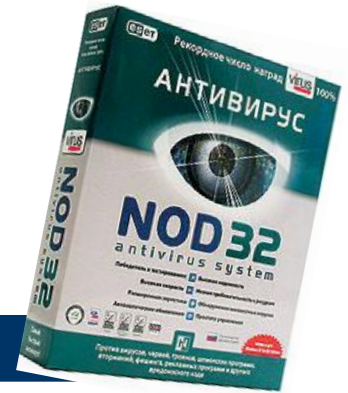
Полифаги



Принцип работы полифагов основан на проверке файлов, секторов и системной памяти и поиске в них известных и новых (неизвестных полифагу) вирусов.

Для поиска известных вирусов используются маски вирусов (некоторая постоянная последовательность программного кода, специфичная для каждого конкретного вируса).

Полифаги-мониторы



постоянно находятся в оперативной памяти компьютера и проверяют все файлы в реальном режиме времени.

Полифаги-сканеры производят проверку системы по команде пользователя.



Краткий обзор антивирусных программ

При выборе антивирусной программы необходимо учитывать не только процент обнаружения вирусов, но и способность обнаруживать новые вирусы, количество вирусов в антивирусной базе, частоту ее обновления, наличие дополнительных функций.



Наиболее известные из антивирусных программ

В настоящее время серьезный антивирус должен уметь распознавать не менее 25000 вирусов. Однако только 200-300 вирусов из них можно встретить, а опасность представляют лишь несколько десятков из них.

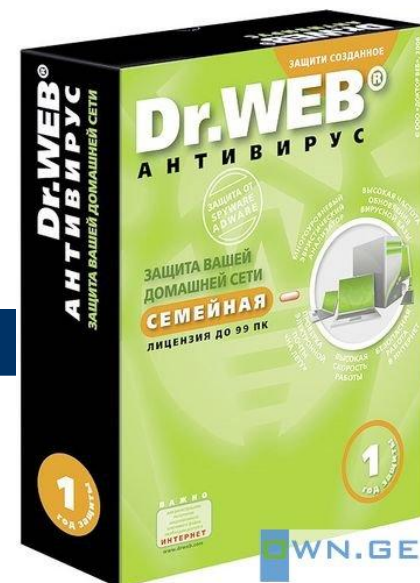


Norton AntiVirus

Один из известных и популярных антивирусов. Процент распознавания вирусов очень высокий (близок к 100%). В программе используется механизм, который позволяет распознавать новые неизвестные вирусы.

В интерфейсе программы Norton AntiVirus имеется функция LiveUpdate, позволяющая щелчком на одной-единственной кнопке обновлять через Web как программу, так и набор сигнатур вирусов.

DrWeb



*Популярный отечественный антивирус.
Хорошо распознает вирусы, но в его базе их
меньше чем у других антивирусных программ*

Достоинства антивируса Dr.Web

Нетребователен к ресурсам, работает, не перегружая систему, что позволяет ему уверенно защищать даже самые маломощные компьютеры прежних поколений.

Компактность и удобство

- ✓ процесс обновления происходит незаметно для пользователя – при каждом подключении к сети Интернет, по запросу или по расписанию.
- ✓ загрузка осуществляется быстро (даже на медленных модемных соединениях).
- ✓ всегда имеются доступные сервера обновлений.
- ✓ по завершении обновления не требуется перезагружать компьютер: Dr.Web сразу готов к работе с использованием самых свежих вирусных баз.