

ВИРУСЫ И АНТИВИРУСНЫЕ ПРОГРАММЫ

*Виды компьютерных
вирусов.*

*Антивирусные
программы.*

Оглавление:

- ❖ Вирус
 - ❖ Что такое вирус?
 - ❖ Классификация вирусов
- ❖ Антивирусные программы
 - ❖ Что такое антивирусная программа?
 - ❖ Некоторые её параметры
 - ❖ Виды антивирусных программ
- ❖ Вопросы по изученному материалу
 - ❖ Блок контроля
 - ❖ Блок самоконтроля



Вообще, что такое вирус???

- *Прежде всего, 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

Назад

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

Назад

Загрузочные 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.



Назад

Файловые вирусы

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.).

Макро-вирусы

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

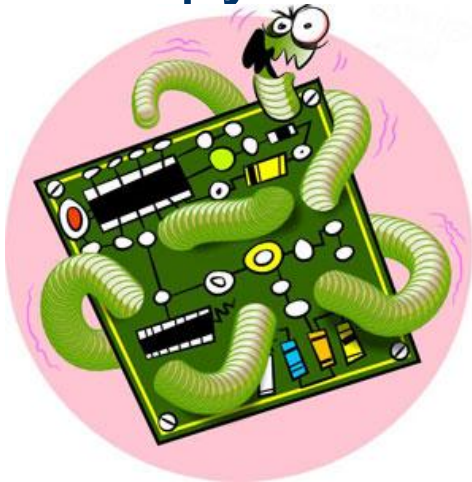
Для своего размножения такие вирусы используют возможности макро-языков и при их помощи переносят себя из одного зараженного файла (документа или таблицы) в другие.

Назад

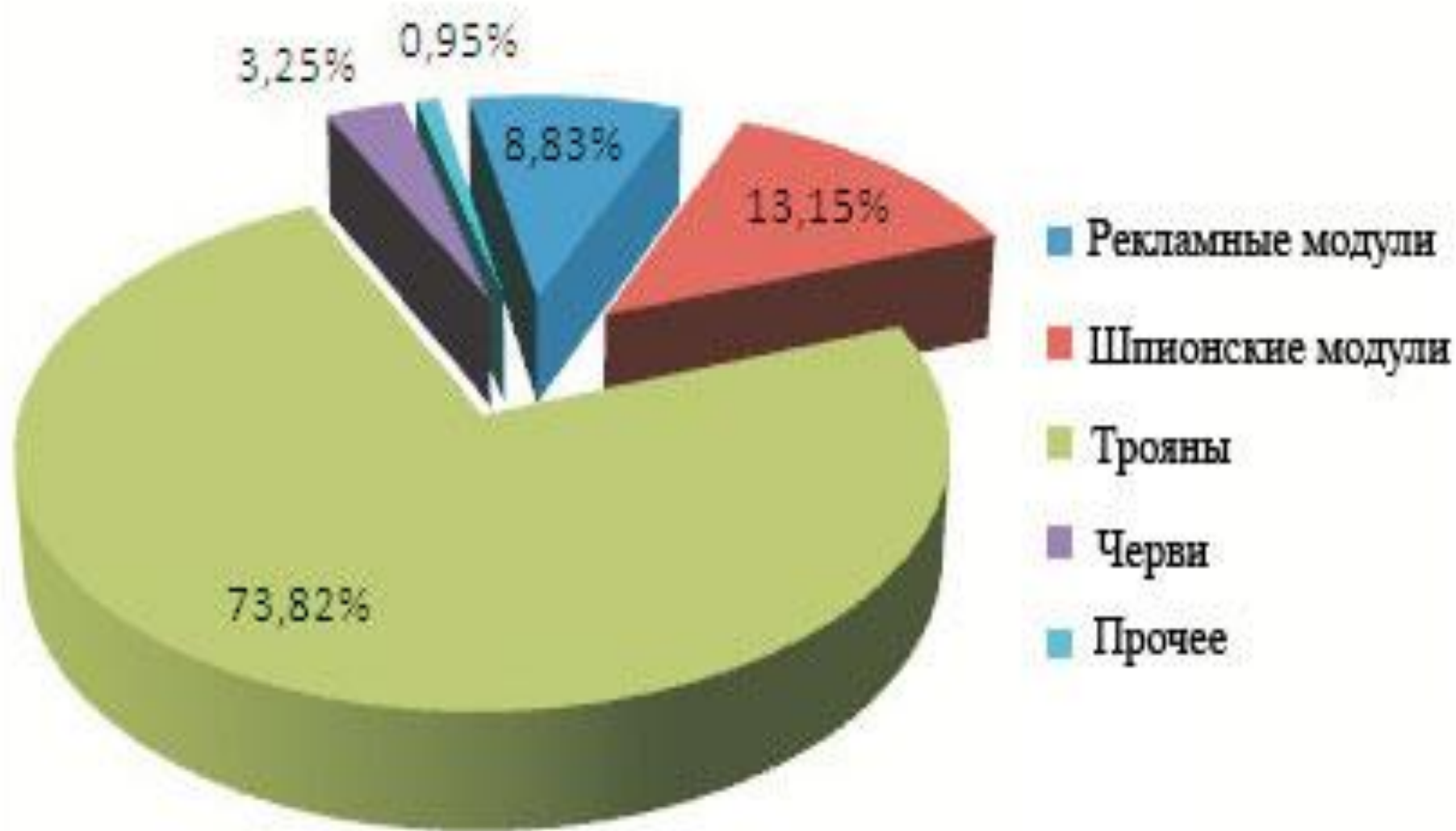
Сетевые вирусы

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

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



Назад



Распространенные виды вирусов

Вирусы делятся также 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.

Дополнительные типы вирусов

Зомби (Zombie) - это программа-вирус, которая после проникновения в компьютер, подключенный к сети Интернет управляется извне и используется злоумышленниками для организации атак на другие компьютеры. Зараженные таким образом компьютеры-зомби могут объединяться в сети, через которые распространяются вирусы и другие вредоносные программы.

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 (флешки)**
- 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
и
ты от компьютерных
ов разработаны
альные программы, которые
позволяют обнаруживать и уничтожать
вирусы. Такие программы называются
антивирусными.



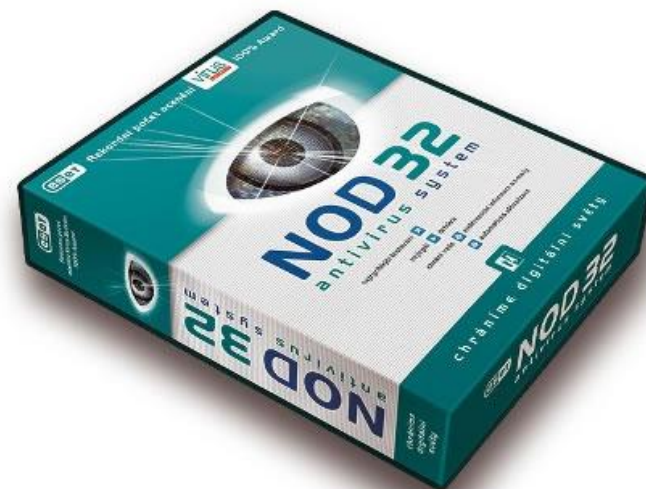
Их параметры...

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

- ✓ *Стабильность и надежность работы*
- ✓ *Размеры вирусной базы программы*
- ✓ *Многоплатформенность*

АНТИВИРУСНЫЕ ПРОГРАММЫ

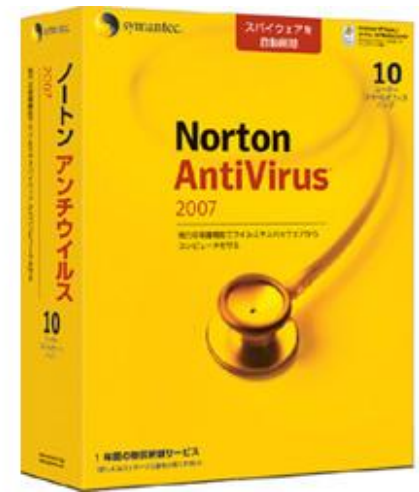
- Антивирусные блокировщики
- Ревизоры
- Полифаги
- Полифаги-мониторы



Назад

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



Назад



Ревизоры

Принцип работы ревизоров 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).

Назад

Полифаги-мониторы



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

Полифаги-сканеры производят проверку системы по команде пользователя.



Назад

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.



Created

Norton 2006 Four in One

by RaySmith



Norton Antivirus 2006



Norton Antivirus 2006 Serial



Norton Internet Security 2006



Norton Internet Security 2006 Serial



Activation Method for All



Norton SystemWorks Premium



Norton SystemWorks Premium Serial



Norton Personal Firewall

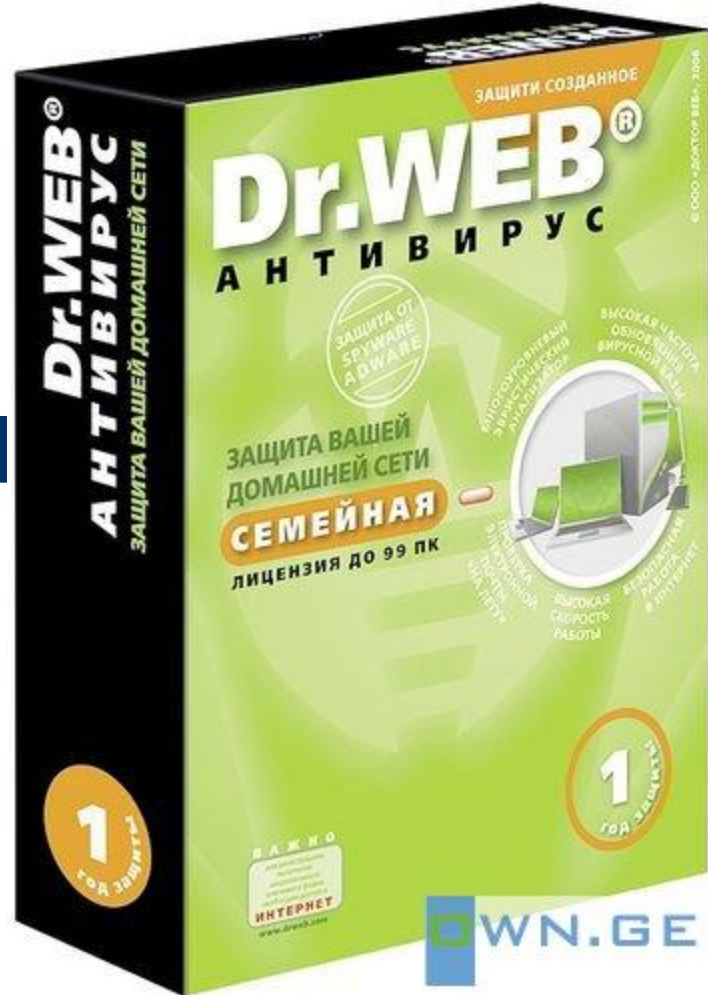


Norton Personal Firewall Serial

Exit

DrWeb

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



Нетребовательность к ресурсам

- *Антивирус 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.

Файл Настройки Помощь

Проверка

Статистика

☒ Быстрая проверка☐ Полная проверка☐ Выборочно

В этом режиме проверяются:

- * Оперативная память
- * Загрузочные секторы всех дисков
- * Объекты автозапуска
- * Корневой каталог загрузочного диска
- * Корневой каталог диска установки Windows
- * Системный каталог Windows
- * Папка Мои Документы
- * Временный каталог системы
- * Временный каталог пользователя



Объект

Путь

Статус

Действие

Выделить все

Вылечить

Переименовать

Переместить

Удалить

Подготовка сканирования

2008-11-17 (14:31)

421526

Блок контроля...

- Что такое вирус? И чем он опасен?
- Признаки появления вирусов.
- Какие вирусы бывают?
- Для чего нужна антивирусная программа?
- Её виды.
- Какое количество вирусов можно сейчас встретить?

Блок самоконтроля

*Тест по пройденному
материалу*

Репортаж о вирусах



[Видео в Интернете](#)