

# **Компьютерные вирусы**



**АНТИВИРУСНЫЕ  
ПРОГРАММЫ**

# Что это такое – вирус?



- **Компьютерный вирус** – разновидность компьютерных программ, отличительной особенностью которых является **способность к размножению** (саморепликация).
- В дополнение к этому вирусы могут без ведома пользователя выполнять прочие произвольные действия, в том числе наносящие вред пользователю и/или компьютеру.
- По этой причине вирусы относят к вредоносным программам.

# Первый вирус



Компьютерные вирусы впервые появились в **1986 году**, хотя исторически возникновение вирусов тесно связано с идеей создания самовоспроизводящихся программ.

В начале эпохи компьютерных вирусов разработка вирусоподобных программ носила чисто исследовательский характер, постепенно превращаясь на откровенно вражеское отношение к пользователям безответственных, и даже криминальных "элементов".

# Первый вирус

Первая «эпидемия» компьютерного вируса произошла в 1986 году, когда вирус по имени Brain (англ. «мозг»), созданный пакистанским программистом по фамилии Алви, заразил дискеты персональных компьютеров. Только в США этот вирус поразил свыше 18 тыс. компьютеров.



# Сколько их?



В настоящее время известно более 50 тысяч вирусов, заражающих компьютеры и распространяющихся по компьютерным сетям.

# Основные признаки проявления вирусов



- 1) Существенное уменьшение размера свободной оперативной памяти
- 2) Неожиданное значительное увеличение количества файлов на диске
- 3) Вывод на экран непредусмотренных сообщений или изображений
- 4) Подача непредусмотренных звуковых сигналов
- 5) Частые зависания и сбои в работе компьютера
- 6) Прекращение работы или неправильная работа ранее успешно функционировавших программ
- 7) Медленная работа компьютера
- 8) Невозможность загрузки операционной системы
- 9) Исчезновение файлов и каталогов или искажение их содержимого
- 10) Изменение даты и времени модификации файлов

11) Изменение размеров файлов

# Классификация



## По способу заражения

### Резидентные

Такой вирус при инфицировании ПК оставляет в оперативной памяти свою резидентную часть, которая потом перехватывает обращение ОС к объектам заражения и поражает их. Резидентные вирусы живут до первой перезагрузки ПК.

### Нерезидентные

Не заражают оперативную память и могут быть активными ограниченное время.

# Классификация



## По среде обитания

Сетевые

Файловые

Загрузочные

Файлово-загрузочные

Используют для своего распространения протоколы или команды компьютерных сетей и электронной почты.

либо различными способами внедряются в выполняемые файлы (наиболее распространенный тип вирусов), либо создают файлы-двойники (компаньон-вирусы), либо используют особенности организации файловой системы (link-вирусы)

записывают себя либо в загрузочный сектор диска (boot-сектор), либо в сектор, содержащий системный загрузчик винчестера (Master Boot Record), либо меняют указатель на активный boot-сектор.



# Классификация



## По степени воздействия

### Неопасные

Эти вирусы забивают память компьютера путем своего размножения и могут организовывать мелкие пакости – проигрывать заложенную в них мелодию или показывать картинку.

### Опасные

Эти вирусы способны создать некоторые нарушения в функционировании ПК – сбои, перезагрузки, глюки, медленная работа компьютера и т.д.

### Очень опасные

Могут уничтожить программы, стереть важные данные, убить загрузочные и системные области жесткого диска.

# Классификация

## По особенностям алгоритмов

### Мутанты

Их очень тяжело обнаружить из-за применения в них алгоритмов шифрования. Каждая следующая копия размножающегося вируса не будет похожа на предыдущую.

### Репликаторы

Они же сетевые черви, проникают через компьютерные сети, они находят адреса компьютеров в сети и заражают их

### Троянские

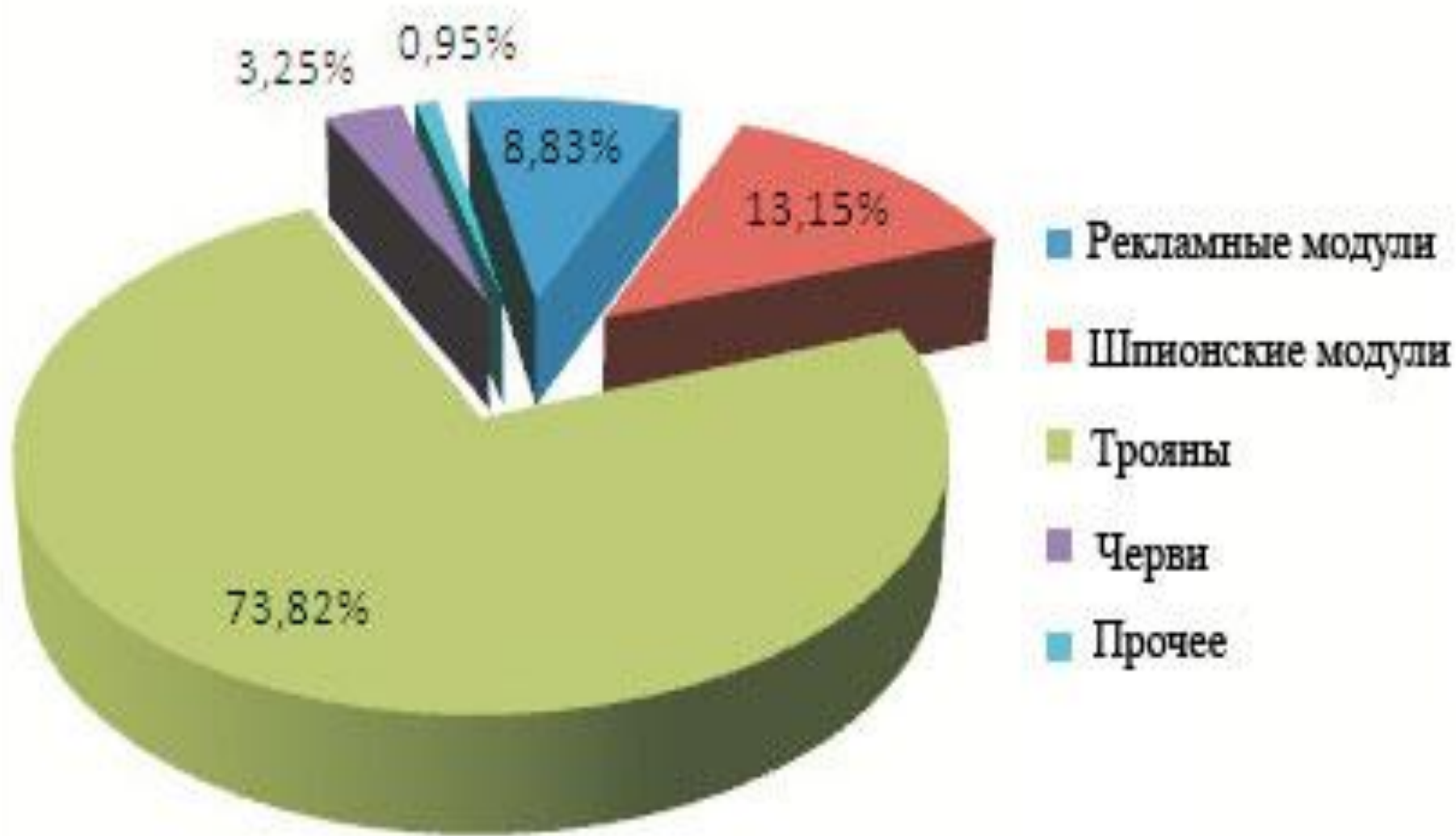
Один из самых опасных вирусов, так как трояны не размножаются, а воруют ценную информацию – пароли, банковские счета, электронные деньги и т.д.

### Невидимки

Это трудно обнаружимые вирусы, которые перехватывают обращения ОС к зараженным файлам и секторам дисков и подставляют вместо своего незараженные участки.

### Паразитические

Меняют содержимое файлов и секторов диска. Такие вирусы легко вычисляются и удаляются.



*Распространенные виды вирусов*

# Пути проникновения вирусов



- Глобальная сеть Internet
- Электронная почта
- Локальная сеть
- Компьютеры «Общего назначения»
- Пиратское программное обеспечение
- Ремонтные службы
- Съемные накопители

# Пути проникновения вирусов

## Глобальная сеть Интернет

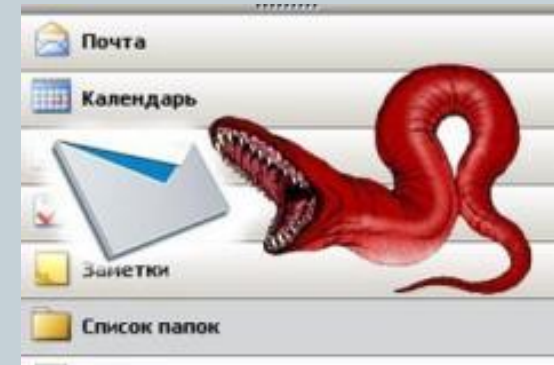
Основным источником вирусов на сегодняшний день является глобальная сеть Internet. Возможно заражение через страницы Интернет ввиду наличия на страницах всемирной паутины различного «активного» содержимого: скриптов, ActiveX-компоненты, Java-апплетов.



# Пути проникновения вирусов

## 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. В некоторых письмах могут содержаться действительно только ссылки, то есть в самих письмах может и не быть вредоносного кода, но если открыть такую ссылку, то можно попасть на специально созданный веб-сайт, содержащий вирусный код. Многие почтовые вирусы, попав на компьютер пользователя, затем используют адресную книгу из установленных почтовых клиентов типа Outlook для рассылки самого себя дальше.



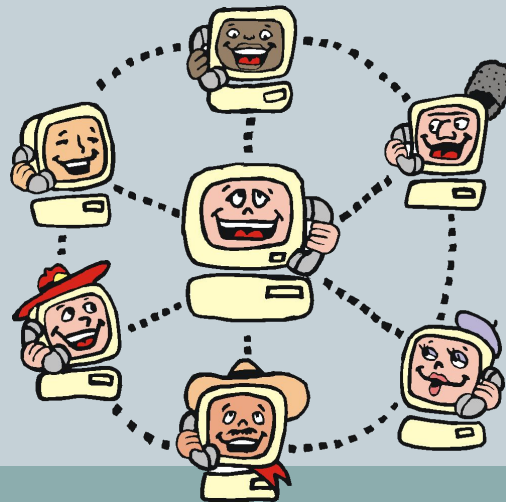
# Пути проникновения вирусов



## Локальные сети

Третий путь «быстрого заражения» — локальные сети. Если не принимать необходимых мер защиты, то зараженная рабочая станция при входе в сеть заражает один или несколько служебных файлов на сервере.

На следующий день пользователи при входе в сеть запускают зараженные файлы с сервера, и вирус, таким образом, получает доступ на компьютеры пользователей.



# Пути проникновения вирусов



## **Персональные компьютеры «общего пользования»**

Опасность представляют также компьютеры, установленные в учебных заведениях.

То же относится и к домашним компьютерам, если на них работает более одного человека.

## **Пиратское программное обеспечение**

Нелегальные копии программного обеспечения, как это было всегда, являются одной из основных «зон риска». Часто пиратские копии на дисках содержат файлы, зараженные самыми разнообразными типами вирусов.





# Пути проникновения вирусов



## **Ремонтные службы**

Достаточно редко, но до сих пор вполне реально заражение компьютера вирусом при его ремонте или профилактическом осмотре. Ремонтники — тоже люди, и некоторым из них свойственно наплевательское отношение к элементарным правилам компьютерной безопасности.

## **Съемные накопители**

В настоящее время большое количество вирусов распространяется через съёмные накопители, включая цифровые фотоаппараты, цифровые видеокамеры, цифровые плееры (MP3-плееры), сотовые телефоны.



# Рынок антивирусных программ очень

нообразен



# Антивирусные программы



ДЛЯ ОБНАРУЖЕНИЯ, УДАЛЕНИЯ И ЗАЩИТЫ ОТ КОМПЬЮТЕРНЫХ ВИРУСОВ РАЗРАБОТАНЫ СПЕЦИАЛЬНЫЕ ПРОГРАММЫ, КОТОРЫЕ ПОЗВОЛЯЮТ ОБНАРУЖИВАТЬ И УНИЧТОЖАТЬ ВИРУСЫ. ТАКИЕ ПРОГРАММЫ НАЗЫВАЮТСЯ АНТИВИРУСНЫМИ.

## Их параметры...



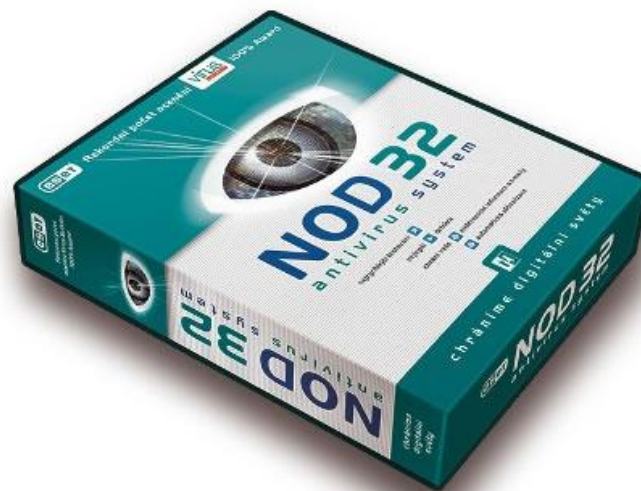
Для быстрой и эффективной работы антивирусная программа должна отвечать некоторым параметрам:

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

# АНТИВИРУСНЫЕ ПРОГРАММЫ



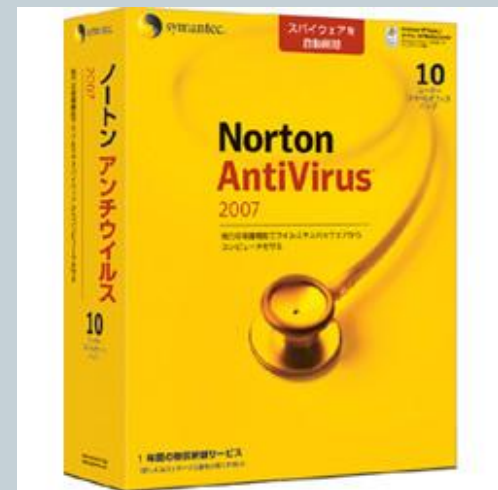
- *Антивирусные блокировщики*
- *Ревизоры*
- *Полифаги*
- *Полифаги-мониторы*



# 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 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).*



# 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.



# Как защититься от вирусов



1. установите на свой ПК современную антивирусную программу.
2. перед просмотром информации принесенной на флэш-карте (дискете) с другого компьютера проверьте носитель антивирусом;
3. после разархивирования архивных файлов сразу проверьте их на вирусы (не все антивирусные программы могут искать вредоносный код в архивах или могут делать это не корректно);
4. периодически проверяйте компьютер на вирусы (если активно пользуетесь Интернетом – запускайте раз в неделю, а то и чаще);
5. как можно чаще делайте резервные копии важной информации (backup);
6. используйте совместно с антивирусной программой файервол (firewall) если компьютер подключен к Интернет;
7. настройте браузер (программа просмотра Интернет страниц – IE, Opera и т.д.) для запрета запуска активного содержимого html-страниц.



**Спасибо за внимание!**