Компьютерные вирусы, их классификация и средства борьбы с ними

LOGO

Современное общество все больше вовлекается в виртуальный мир Интернета. Но с активным развитием глобальных сетей актуальным становится вопрос информационной безопасности, так как проникающие в их сети вирусы могут нарушить целостность и сохранность вашей информации

Защита компьютера от вирусов – это та задача, решать которую приходится всем пользователям, и особенно тем, кто активно пользуется Интернетом или работает в локальной сети

- **Компьютерные вирусы**
  - ✔ **Что такое компьютерный вирус?**
  - ✔ **Испорченные и зараженные файлы**
  - ✔ **Классификация вирусов**
  - ✔ **Пути проникновения вирусов**
- **Профилактика и борьба с компьютерными вирусами**
  - ✔ **Методы защиты от компьютерных вирусов**
  - ✔ **Действия при заражении вирусом**
- **Литература и интернет-ресурсы**

ЧТО ТАКОЕ КОМПЬЮТЕРНЫЙ ВИРУС?

Компьютерный вирус – специально созданная небольшая программа, способная к саморазмножению, засорению компьютера и выполнению других нежелательных действий

Энциклопедия вирусов
«Лаборатории Касперского
http://www.viruslist.com/ru/viruses/encyclopedia

ЧТО ТАКОЕ КОМПЬЮТЕРНЫЙ ВИРУС?

Признаки заражения компьютера:

- некоторые программы перестают работать или начинают работать неправильно
- на экран выводятся посторонние сообщения, символы…
- работа на компьютере существенно замедляется
- некоторые файлы оказываются испорченными и т.д.

Активизация вируса может быть связана с различными событиями:

- наступлением определённой даты или дня недели
- запуском программы
- открытием документа…

ИСПОРЧЕННЫЕ И ЗАРАЖЕННЫЕ ФАЙЛЫ

Компьютерный вирус может испортить файл или «заразить».

Обычным вирусом могут быть заражены следующие виды файлов:

Тип вируса	Вид заражаемого файла
Файловый	Исполнимые файлы
Загрузочный или BOOT-вирус	Загрузчик операционной системы
Вирус драйвера устройства	Драйвер устройства

КЛАССИФИКАЦИЯ ВИРУСОВ

ПРИЗНАКИ КЛАССИФИКАЦИИ

- По среде обитания
- По поражаемым операционным системам
- По особенностям алгоритма
- По языку, на котором написан вирус
- По деструктивным возможностям

Классификация по среде обитания

- Файловые вирусы
- Загрузочные вирусы
- Макро-вирусы
- Сетевые черви
- Скриптовые вирусы

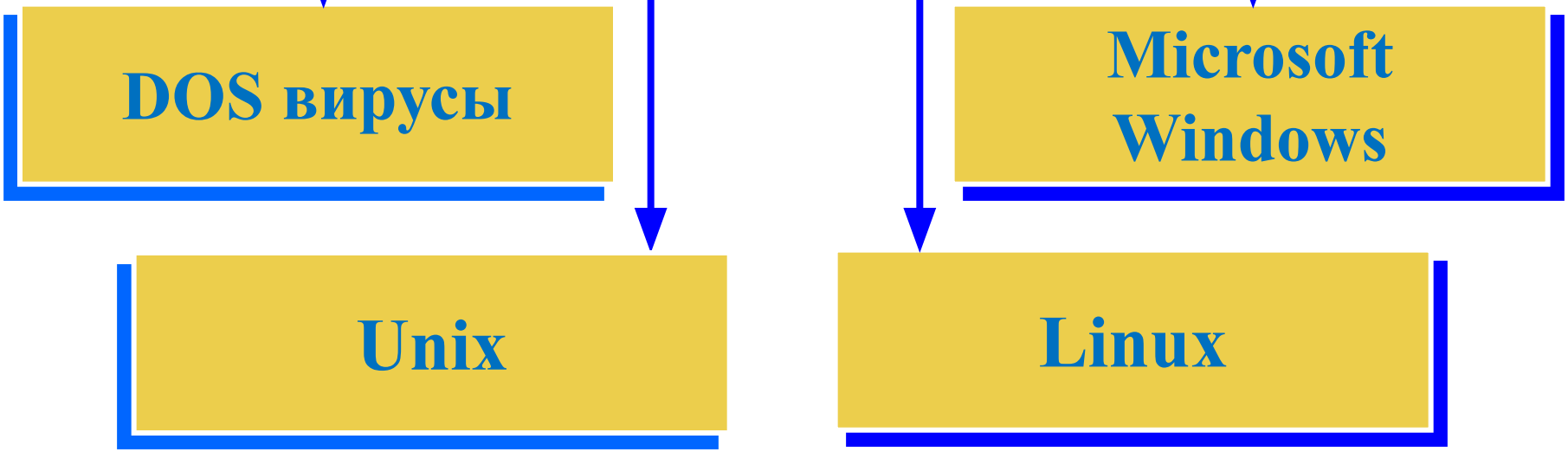
По особенностям алгоритма

- макровирусы
- файловые «черви»
- паразитические
- компаньоны
- «стелс»-вирусы
- «полиморфик»-вирусы
- сетевые

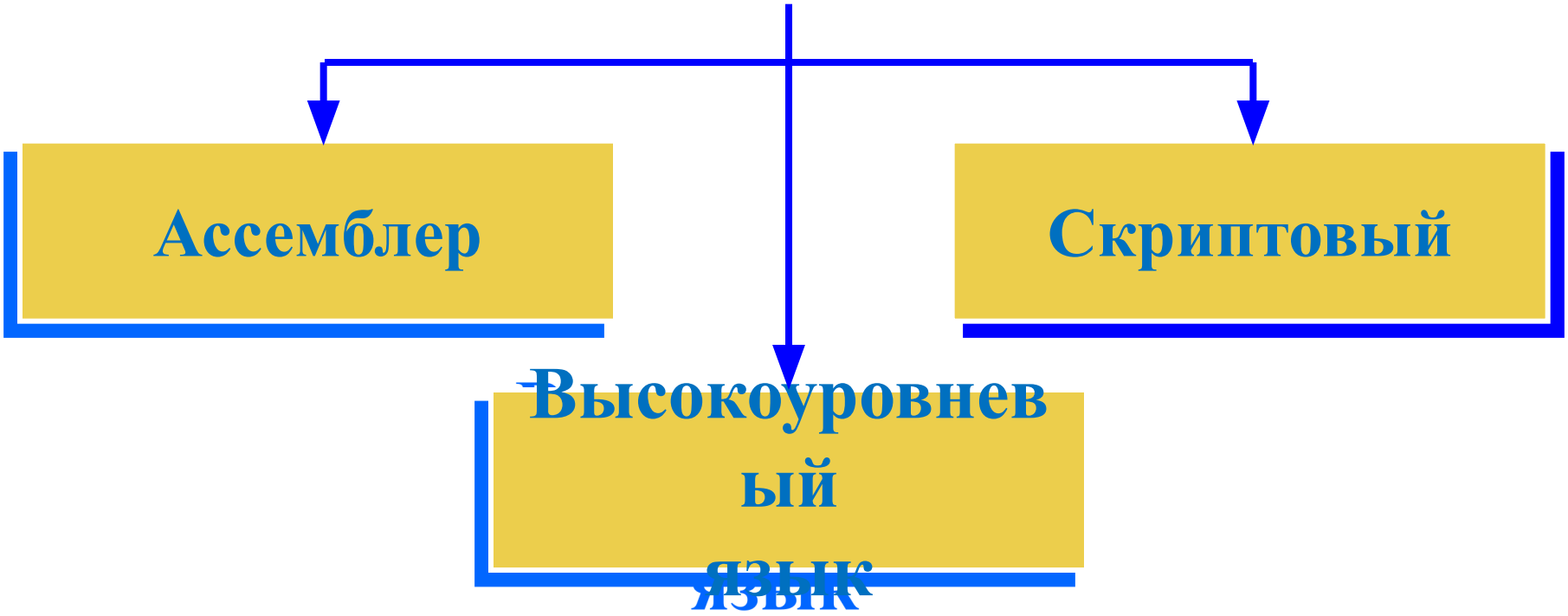
Классификация по деструктивным возможностям

- Безвредные
- Неопасные
- Опасные
- Очень опасные

Классификация по поражаемым операционным системам



Классификация по языку, на котором написан вирус



ПУТИ ПРОНИКНОВЕНИЯ ВИРУСОВ

- Гл

МЕТОДЫ ЗАЩИТЫ ОТ КОМПЬЮТЕРНЫХ ВИРУСОВ

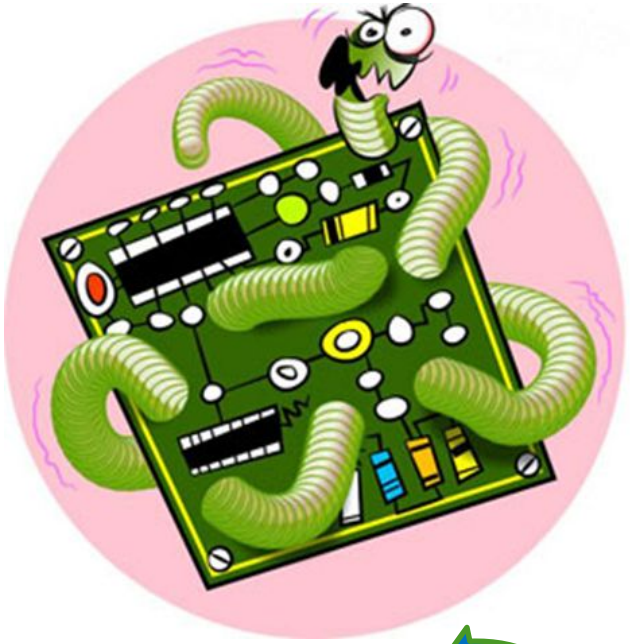
Для защиты от вирусов можно использовать:

- **общие средства защиты информации**
- **специализированные программы для защиты от вирусов**
- **профилактические меры, позволяющие уменьшить вероятность заражения вирусом**

ОБЩИЕ СРЕДСТВА ЗАЩИТЫ ИНФОРМАЦИИ

Общие средства защиты информации полезны не только для защиты от вирусов, но и как страховка от физической порчи дисков, неправильно работающих программ или ошибочных действий пользователей:

- ***копирование информации*** — создание копий файлов и системных областей дисков;
- ***разграничение доступа*** предотвращает несанкционированное использование информации



СПЕЦИАЛИЗИРОВАННЫЕ ПРОГРАММЫ ДЛЯ ЗАЩИТЫ ОТ ВИРУСОВ

- ***Программы – детекторы*** позволяют обнаруживать файлы, зараженные одним из нескольких известных вирусов
- ***Программы – доктора*** «лечат» зараженные программы или диски, удаляя из зараженных программ тело вируса
- ***Программы – ревизоры*** запоминают сведения о состоянии программ и системных областей дисков, сравнивают их состояние с исходным, при выявлении несоответствий об этом сообщается пользователю
- ***Доктора – ревизоры*** — это программы, которые не только обнаруживают изменения в файлах и системных областях дисков, но и могут автоматически вернуть их в исходное состояние
- ***Программы – фильтры*** располагаются резидентно в оперативной памяти компьютера и перехватывают те обращения к операционной системе, которые используются вирусами для размножения и нанесения вреда
- ***Программы – вакцины*** — модифицируют программы и диски таким образом, что это не отражается на работе программ, но вирус, от которого производится вакцинация, считает эти программы и диски уже зараженными

ПРОФИЛАКТИЧЕСКИЕ МЕРЫ, ПОЗВОЛЯЮЩИЕ УМЕНЬШИТЬ ВЕРОЯТНОСТЬ ЗАРАЖЕНИЯ ВИРУСОМ

Защитить компьютер от заражения вирусом помогут следующие профилактические меры:

- Необходимо обновлять архивные копии используемых пакетов программ и данных. Перед архивацией данных целесообразно проверить их на наличие вируса
- Следует устанавливать защиту от записи на архивных дисках
- Не следует заниматься нелицензионным и нелегальным копированием программного обеспечения с других компьютеров
- Все данные, поступающие извне, стоит проверять на вирусы
- Заблаговременно подготавливать восстанавливающие пакеты на дисках с защитой от записи
- Периодически проверять диск программами-детекторами
- Обновлять базу антивирусных программ.
- Не допускать к компьютеру сомнительных пользователей.

ДЕЙСТВИЯ ПРИ ЗАРАЖЕНИИ ВИРУСОМ

1. Отключить компьютер от интернета и от локальной сети
2. Если симптом заражения состоит в том, что вы не можете загрузиться с жесткого диска компьютера, попробуйте загрузиться в режиме защиты от сбоев или с диска аварийной загрузки операционной системы
3. Сохраните результаты вашей работы на внешний носитель
4. Скачайте и установите пробную или же купите полную версию антивируса, если на вашем компьютере не установлено антивирусное обеспечение
5. Получите последние обновления антивирусных баз. Если это возможно, для их получения выходите в интернет не со своего компьютера, а с незараженного
6. Запустите полную проверку компьютера
7. Если программа-детектор обнаружит файловый вирус, то:
   - если у вас установлена программа-ревизор с лечащим модулем, то восстановление файлов лучше делать с ее помощью
   - если такой программы нет, то необходимо воспользоваться для лечения одним из детекторов
8. Испорченные файлы необходимо удалить

ЛИТЕРАТУРА И ИНТЕРНЕТ-РЕСУРСЫ

Литература

- Анин Б. Защита компьютерной информации. – СПб. : БХВ – Санкт – Петербург, 2000. – 368 с.
- Караменс В.В., Григ Н.Р. Компьютер: прошлое, настоящее, будущее. М., 2001.
- Семененко В. А., Н. В. Федоров. Программно – аппаратная защита информации: учеб. пособие для студ. вузов. – М. : МГИУ, 2007. – 340 с.

Интернет-ресурсы

- Википедия. Свободная энциклопедия http://ru.wikipedia.org/wiki/%CA%EE%EC%EF%FC%FE%F2%E5%F0%ED%FB%E9_%E2%E8%F0%F3%F1
- Проект «Безопасный Интернет» http://brschool.okis.ru/file/brschool/proekty/KV.pdf
- Лаборатория Касперского. Об угрозах http://www.kaspersky.ru/internet-security-center

Спасибо за внимание!