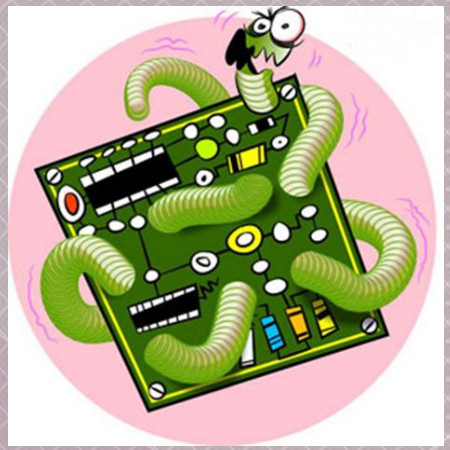
Компьютерные вирусы, их классификация и средства борьбы с ними

Содержание



ЧТО ТАКОЕ КОМПЬЮТЕРНЫЙ ВИРУС?

- **Компьютерный вирус** – специально созданная небольшая программа, способная к саморазмножению, засорению компьютера и выполнению других нежелательных действий.
- Название «вирус» пришло из биологии именно по признаку способности к размножению. Программа, внутри которой находится вирус, называется зараженной программой

Первые вирусы появились давно и не всегда были вредоносными. Например, в конце 60-х в лаборатории Xerox была создана специальная программа, являющаяся прообразом современных вирусов, которая самостоятельно путешествовала по локальной вычислительной сети и проверяла работоспособность включенных в нее устройств.

Однако позднее программы-вирусы стали разрабатываться со злым умыслом. Есть сведения, что некоторые компании специально инфицировали компьютеры конкурентов, чтобы таким образом шпионить за ними или вывести из строя их информационные системы.

В наши дни созданием вирусов обычно занимаются энтузиасты – одиночки. Ими могут быть и профессиональные программисты, и исследователи и обычные студенты, начинающие изучать программирование.

Что является стимулом для такой деятельности – сказать сложно. Это может быть как чувство мести, так и желание самоутвердиться.

Признаки заражения компьютера:

1. некоторые файлы оказываются испорченными и т.д.
2. неправильная работа нормально работавших программ;
3. медленная работа компьютера;
4. невозможность загрузки ОС;
5. исчезновение файлов и каталогов;
6. изменение размеров файлов;
7. неожиданное увеличение количества файлов на диске;
8. уменьшение размеров свободной оперативной памяти;
9. вывод на экран неожиданных сообщений и изображений;
10. подача непредусмотренных звуковых сигналов;
11. частые зависания и сбои в работе компьютера

АКТИВИЗАЦИЯ ВИРУСА МОЖЕТ БЫТЬ СВЯЗАНА С РАЗЛИЧНЫМИ СОБЫТИЯМИ:

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

КЛАССИФИКАЦИЯ ВИРУСОВ

ПРИЗНАКИ КЛАССИФИКАЦИИ

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

КЛАССИФИКАЦИЯ ВИРУСОВ

По среде обитания

- файловые вирусы
- загрузочные вирусы
- макро-вирусы

Файловые вирусы, которые внедряются в выполняемые файлы (*.COM, *.EXE, *.SYS, *.BAT, *.DLL).

Загрузочные вирусы, которые внедряются в загрузочный сектор диска (Boot-сектор) или в сектор, содержащий системный загрузчик винчестера (Master Boot Record).

Макро-вирусы, которые внедряются в системы, использующие при работе так называемые макросы (например, Word,

Существуют и сочетания - например, файлово-загрузочные вирусы, заражающие как файлы, так и загрузочные сектора.

По особенностям алгоритма

компаньон-вирусы

вирусы-«черви»

сетевые черви

«паразитические»

«студенческие»

«полиморфик»-вирусы

«стелс»-вирусы

сетевые вирусы

макро-вирусы

компаньон-вирусы (companion) - Алгоритм работы этих вирусов состоит в том, что они создают для EXE-файлов файлы-спутники, имеющие то же самое имя, но с расширением COM. При запуске такого файла DOS первым обнаружит и выполнит COM-файл, т.е. вирус, который затем запустит и EXE-файл;

вирусы-«черви» (worm) - вариант компаньон-вирусов. «Черви» не связывают свои копии с какими-то файлами. Они создают свои копии на дисках и в подкаталогах дисков, никаким образом не изменяя других файлов и не используя COM-EXE прием, описанный выше;

«паразитические» - все вирусы, которые при распространении своих копий обязательно изменяют содержимое дисковых секторов или файлов. «студенческие» - крайне примитивные вирусы, часто нерезидентные и содержащие большое число ошибок;

«стелс»-вирусы (вирусы-невидимки, stealth), представляют собой весьма совершенные программы, которые «подставляют» вместо себя незараженные участки информации.
«полиморфик»-вирусы - достаточно труднообнаруживаемые вирусы, не содержащие ни одного постоянного участка кода.
макро-вирусы - вирусы этого семейства используют возможности макроязыков, встроенных в системы обработки данных
сетевые вирусы (сетевые черви) - вирусы, которые распространяются в компьютерной сети и, так же, как и компаньон-вирусы, не изменяют файлы или сектора на дисках.
На сегодняшний день сетевые вирусы не представляют никакой опасности, так как они нежизнеспособны в современных сетях, как глобальных (Internet), так и локальных (NetWare, NT). Однако это не мешает обычным DOS-вирусам и макро-вирусам поражать компьютерные сети (локальные и глобальные). Делают они это, в отличие от сетевых вирусов, не используя сетевые протоколы и «дыры» в программном обеспечении. Заражению подвергаются файлы на «общих» дисках на серверах и рабочих местах, через которые эти вирусы перебираются и на другие рабочие места, а часто и передаются в Internet.

По деструктивным возможностям

Безвредные, т.е. никак не влияющие на работу компьютера (кроме уменьшения свободной памяти на диске в результате своего распространения);

Неопасные, влияние которых ограничивается уменьшением свободной памяти на диске и графическими, звуковыми и пр. эффектами;

Опасные - вирусы, которые могут привести к серьезным сбоям в работе;

Очень опасные, могущие привести к потере программ, уничтожить данные, стереть необходимую для работы компьютера информацию, записанную в системных областях памяти и т.д.

По способам заражения

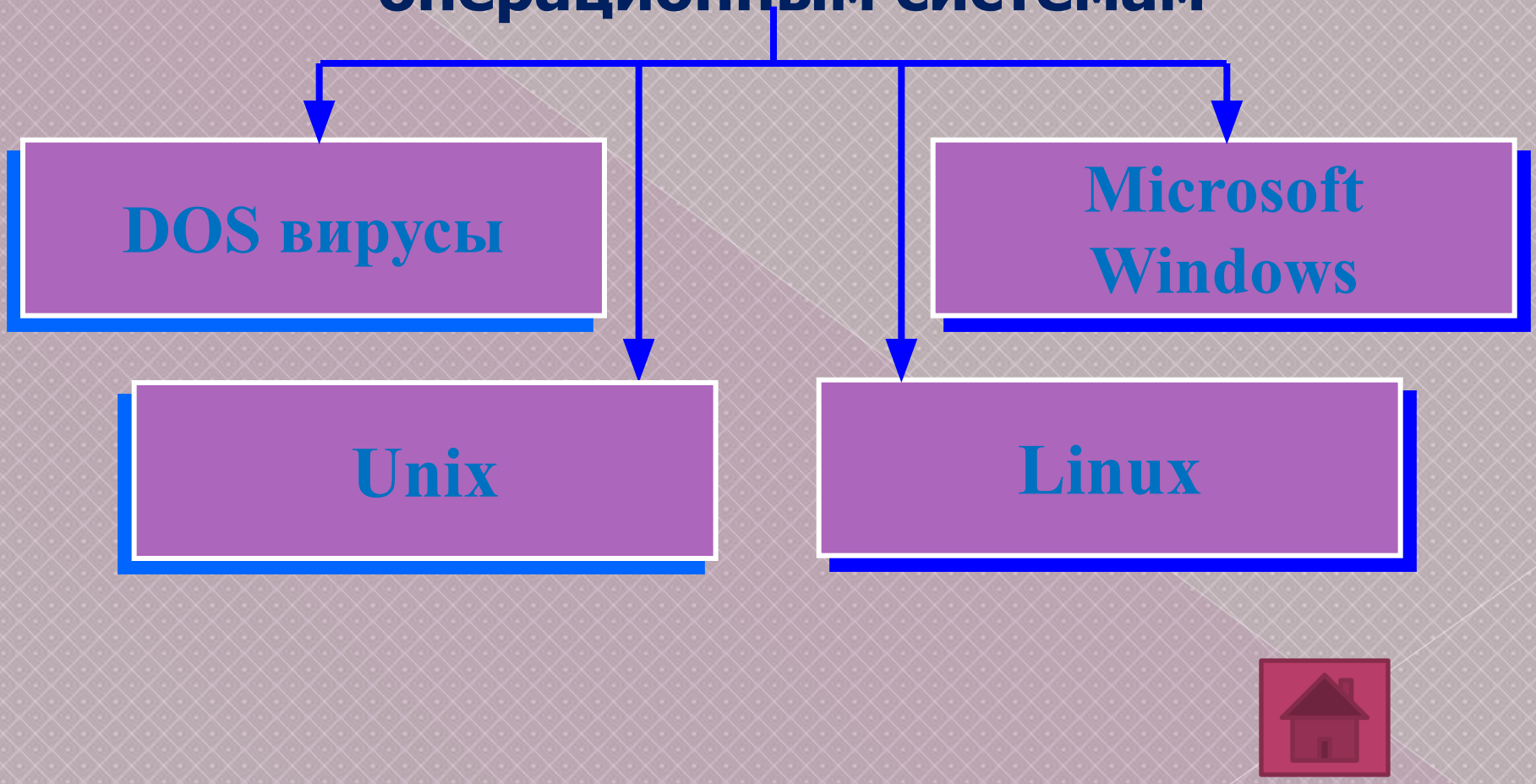
Резидентный вирус при инфицировании компьютера оставляет в оперативной памяти свою резидентную часть, которая затем перехватывает обращение операционной системы к объектам заражения и внедряется в них. Резидентные вирусы находятся в памяти и являются активными вплоть до выключения или перезагрузки компьютера.

Нерезидентные вирусы не заражают память компьютера и являются активными лишь ограниченное время.

Классификация по языку, на котором написан вирус

- Ассемблер
- Высокоуровневый язык
- Скриптовый

Классификация по поражаемым операционным системам



ПУТИ ПРОНИКНОВЕНИЯ ВИРУСОВ

- Гл

Антивирусная программа (антивирус) - программа, позволяющая выявлять вирусы, лечить зараженные файлы и диски, обнаруживать и предотвращать подозрительные действия.

Типы антивирусных программ

- Программы – детекторы (сканеры);
- Программы – доктора (или фаги, дезинфекторы);
- Программы – ревизоры;
- Программы – фильтры (сторожа, мониторы);
- Программы – иммунизаторы.

Ни один тип антивирусных программ по отдельности не дает полной защиты от вирусов. Поэтому в современные антивирусные комплекты программ обычно входят компоненты, реализующие все эти функции.

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

Примеры антивирусных программ

- Eset Nod32
- Kaspersky Anti-Virus,
- Dr.WEB,
- Adinf,
- Avast
- Norton AntiVirus и др

СПАСИБО ЗА ВНИМАНИЕ!