КОМПЬЮТЕРНЫЕ ВИРУСЫ И АНТИВИРУСНЫЕ ПРОГРАММЫ

Компьютерный вирус *(КВ)* – это программа, способная создавать свои копии (не обязательно полностью совпадающие с оригиналом), внедрять их в различные объекты или ресурсы компьютерных систем, сетей и производить определенные действия без ведома пользователя.

Свое название ***КВ*** получил за некоторое сходство с биологическим вирусом. Например, в зараженной программе самовоспроизводится другая программа-вирус, а инфицированная программа может длительное время работать без ошибок, как в стадии инкубации.

Программа, внутри которой находится вирус, называется *зараженной (инфицированной)* программой.

Когда инфицированная программа начинает работу, то сначала управление получает вирус. Он заражает другие программы, а также выполняет запланированные деструктивные действия. Для маскировки своих действий вирус активизируется не всегда, а лишь при выполнении определенных условий (истечение некоторого времени, выполнение определенного числа операций, наступление некоторой даты или дня недели и т.д.). После того, как вирус выполнит нужные ему действия, он передает управление той программе, в которой он находится. Внешне зараженная программа может работать так же, как и обычная программа. Подобно настоящим вирусам КВ прячутся, размножаются и ищут возможности перейти на другие ЭВМ.

Несмотря на широкую распространенность антивирусных программ, вирусы продолжают плодиться. В среднем в день появляется около 300 новых разновидностей.

Различные вирусы выполняют различные ***действия:***

- Выводят на экран мешающие **текстовые сообщения** (поздравления, политические лозунги, фразы с претензией на юмор и т.д.);
- Создают **звуковые эффекты** (гимн, гамма, популярная мелодия);
- Создают **видео эффекты** (переворачивают или сдвигают экран, имитируют землетрясение, вызывают опадание букв в тексте, выводят картинки и т.д.);
- **Замедляют** работу ЭВМ, постепенно уменьшают объем свободной оперативной памяти;
- Увеличивают **износ** оборудования (например, головок дисководов);
- Вызывают **отказ** отдельных устройств, зависание или перезагрузку компьютера и крах работы всей ЭВМ;

- **Уничтожают** FAT, форматируют жесткий диск, стирают BIOS, уничтожают или изменяют данные, стирают антивирусные программы;
- Осуществляют научный, технический, промышленный и финансовый **шпионаж**;
- Выводят из строя системы **защиты** информации и т.д.

Главная опасность самовоспроизводящихся кодов заключается в том, что программы-вирусы начинают жить собственной жизнью, практически не зависящей от разработчика программы. Так же, как в цепной реакции в ядерном реакторе, запущенный процесс трудно остановить.

Симптомы вирусного заражения ЭВМ:

- Замедление работы некоторых программ
- Увеличение размеров файлов (особенно выполняемых)
- Появление не существовавших ранее «странных» файлов
- Уменьшение объема доступной оперативной памяти (по сравнению с обычным режимом работы)
- Внезапно возникающие разнообразные видео и звуковые эффекты
- Появление сбоев в работе ОС (в т.ч. зависание)
- Запись информации на диски в моменты времени, когда этого не должно происходить
- Прекращение работы или неправильная работа ранее нормально функционировавших программ.

Существует большое число различных ***классификаций*** вирусов:

1. **По среде обитания:**
   - *Сетевые* – распространяются по сетям (Melissa).
   - *Файловые* – инфицируют исполняемые файлы с расширениями .exe, .com. Также к этому классу относятся макровирусы, которые заражают неисполняемые файлы (например, в MS WORD или в MS EXCEL).
   - *Загрузочные* – внедряются в загрузочный сектор диска (Boot-сектор) или в сектор, содержащий программу загрузки системного диска (Master Boot Record - MBR). Некоторые вирусы записывают свое тело в свободные сектора диска, помечая их в FAT как «плохие».
   - *Файлово-загрузочные* – способны заражать и загрузочные секторы и файлы.

2. По способу заражения:

- *Резидентные* – оставляют в оперативной памяти свою резидентную часть, которая затем перехватывает обращения программ к ОС и внедряется в них. Свои деструктивные действия вирус может повторять многократно.
- *Нерезидентные* – не заражают оперативную память и проявляют свою активность лишь однократно при запуске зараженной программы.

3. По степени опасности:

- *Неопасные* – например, на экране появляется сообщение: «Хочу чучу». Если набрать на клавиатуре слово «чуча», то вирус временно «успокаивается».
- *Опасные* – уничтожают часть файлов на диске.
- *Очень опасные* – самостоятельно форматируют жесткий диск. (CIH – активизируется 26 числа каждого месяца и способен уничтожать данные на жестком диске и в BIOS).

4. По особенностям алгоритма:

- *Вирусы-компаньоны* – создают для exe-файлов новые файлы-спутники, имеющие то же имя, но с расширением com. Вирус записывается в com-файл и никак не изменяет одноименный exe-файл. При запуске такого файла ОС первым обнаружит и выполнит com-файл, т.е. вирус, который затем запустит и exe-файл.
- *Паразитические* – изменяют содержимое дисковых секторов или файлов.
- *Репликаторы (черви)* – распространяются в сети. Они проникают в память компьютера из сети, вычисляют сетевые адреса других компьютеров и рассылают по этим адресам свои копии. Черви уменьшают пропускную способность сети, замедляют работу серверов. Могут размножаться без внедрения в другие программы и иметь «начинку» из компьютерных вирусов. («Червь Морриса» в конце 80-х парализовал несколько глобальных сетей в США).
- *Невидимки (стелс)* – маскируют свое присутствие в ЭВМ, их трудно обнаружить. Они перехватывают обращения ОС к пораженным файлам или секторам дисков и «подставляют» незараженные участки файлов.
- *Мутанты (призраки, полиморфные вирусы, полиморфики)* – их трудно обнаружить, т.к. их копии практически не содержат полностью совпадающих участков кода. Это достигается тем, что в программы вирусов добавляются пустые команды (мусор), которые не изменяют алгоритм работы вируса, но затрудняют их выявление. (OneHalf – локальные «эпидемии» его возникают регулярно).
- *Макро-вирусы* – используют возможности макроязыков, встроенных в системы обработки данных (Word, Excel).
- *«Троянские кони»* – маскируются под полезную или интересную программу, выполняя во время своего функционирования еще и разрушительную работу (например, стирает FAT) или собирает на компьютере информацию, не подлежащую разглашению. Не обладают свойством самовоспроизводства.

5. **По целостности:**

- Монолитные – программа вируса - единый блок, который можно обнаружить после инфицирования.
- *Распределенные* – программа разделена на части. Эти части содержат инструкции, которые указывают компьютеру, как собрать их воедино, чтобы воссоздать вирус.

Для борьбы с вирусами разрабатываются **антивирусные программы**. Говоря медицинским языком, эти программы могут выявлять (диагностировать), лечить (уничтожать) вирусы и делать прививку «здоровым» программам.

***Виды* антивирусных программ**:

- *Программы-детекторы (сканеры)* – рассчитаны на обнаружение конкретных вирусов. Основаны на сравнении характерной (специфической) последовательности байтов (*сигнатур* или масок вирусов), содержащихся в теле вируса, с байтами проверяемых программ. Эти программы нужно регулярно обновлять, т.к. они быстро устаревают и не могут выявлять новые виды вирусов. Если программа не опознается детектором как зараженная, это еще не значит, что она «здорова». В ней может быть вирус, который не занесен в базу данных детектора.
- *Программы-доктора (фаги, дезинфекторы)* –не только находят файлы, зараженные вирусом, но и лечат их, удаляя из файла тело программы-вируса. Полифаги – позволяют лечить большое число вирусов. Широко распространены программы-детекторы, одновременно выполняющие и функции программ-докторов. Примеры: **AVP** (автор Е. Касперский), **Aidstest** (Д. Лозинский), **Doctor Web** (И. Данилов).
- *Программы-ревизоры* – анализируют текущее состояние файлов и системных областей дисков и сравнивают его с информацией, сохраненной ранее в одном из файлов ревизора. При этом проверяется состояние Boot-сектора, FAT, а также длина файлов, их время создания, атрибуты, контрольные суммы (суммирование по модулю 2 всех байтов файла). Пример такой программы – **Adin f** (Д. Мостовой).
- *Программы-фильтры (сторожа, мониторы)* – резидентные программы, которые оповещают пользователя обо всех попытках какой-либо программы выполнить подозрительные действия, а пользователь принимает решение о разрешении или запрещении выполнения этих действий. Фильтры контролируют следующие операции: обновление программных файлов и системной области дисков; форматирование диска; резидентное размещение программ в ОЗУ. Примером служит программа **Vsafe**. Она не способна обезвредить вирус, для этого нужно использовать фаги.
- *Программы-иммунизаторы* – записывают в вакцинируемую программу признаки конкретного вируса так, что вирус считает ее уже зараженной, и поэтому

не производит повторное инфицирование. Эти программы наименее эффективны и морально устарели.

Меры **по защите ЭВМ от заражения вирусами:**

- Оснащение ЭВМ современными антивирусными программами и регулярное обновление их версий.
- Установка программы-фильтра при работе в глобальной сети.
- Проверка дискеты на наличие вирусов перед считыванием с дискет информации, записанной на других ЭВМ.
- При переносе на свой ПК файлов в архивированном виде проверка их сразу после разархивации.
- Защита своих дискет от записи при работе на других ПК.
- Создание архивных копий ценной информации на других носителях информации.
- Не оставлять дискету в дисководе при включении или перезагрузки ПК, т.к. возможно заражение загрузочными вирусами. Наличие аварийной загрузочной дискеты, с которой можно будет загрузиться, если система откажется сделать это обычным образом.
- При установке большого программного продукта вначале проверить все дистрибутивные файлы, а после инсталляции продукта повторно произвести контроль наличия вирусов.