Компьютерные вирусы и антивирусные программы

Компьютерный вирус – это программа, способная создавать свои копии, внедрять их в различные объекты или ресурсы компьютерных систем, сетей и производить определенные действия без ведома пользователя.

Свое название компьютерный вирус 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 программой.

Когда инфицированная программа начинает работу, то сначала управление получает вирус. Вирус 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, наступления 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 обычна программа. Подобно настоящим вирусам компьютерные вирусы прячутся, размножаются и ищут возможность перейти на другие ЭВМ.

Таким образом, вирусы должны инфицировать ЭВМ достаточно незаметно, а активизироваться лишь через определенное время (время инкубации). Это необходимо для того, чтобы скрыть источник заражения.

Вирус не может распространяться в полной изоляции от других программ. Очевидно, что пользователь не будет специально запускать одинокую программу-вирус. Поэтому вирусы прикрепляются к телу других полезных программ.

Несмотря на широкую распространенность антивирусных программ, предназначенных для борьбы с вирусами, вирусы продолжают плодиться. В среднем в месяц появляется около 300 новых разновидностей. Различные вирусы выполняют различные действия:

- Выводят на экран мешающие текстовые сообщения (поздравления, политические лозунги, фразы с претензией на юмор, высказывания обиды от неразделенной любви, нецензурные выражения, рекламу, прославление любимых певцов, названия городов);
- Создают звуковые эффекты (проигрываю гимн, гамму или популярную мелодию);
- Создают видеоэффекты (переворачивают или сдвигают экран, имитируют землетрясение, вызывают падение букв в тексте или симулируют снегопад, имитируют скачущий шарик, прыгающую точку, выводят на экран рисунки и картинки);

- Замедляют работу ЭВМ, постепенно уменьшают объем свободной оперативной памяти;
- Увеличивает износ оборудования (например, головок дисководов);
- Вызывают отказ отдельных устройств, зависание или перезагрузку компьютера и крах работы всей ЭВМ;
- Имитируют повторяющиеся ошибки работы операционной системы (например, с целью заключения договора на гарантированное обслуживание ЭВМ);

- Уничтожают FAT – таблицу, форматируют жесткий диск, стирают BIOS, стирают или изменяют установки CMOS, стирают секторы на диске, уничтожают или искажают данные, стирают антивирусные программы;
- Осуществляют научный, технический, промышленный и финансовый шпионаж;
- Выводят из строя системы защиты информации, дают злоумышленникам тайный доступ к вычислительной машине;
- Делают незаконные отчисления с каждой финансовой операции 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.

Основные симптомы вирусного заражения ЭВМ следующие.

- 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 операционной системы (в том числе зависание).
- Запись информации на диски в моменты времени, когда этого не должно происходить.
- Прекращение работы или неправильная работа ранее нормально функционирующих программ.

Существует большое число различных классификаций вирусов.

- По **среде обитания** они делятся на сетевые, файловые, загрузочные и файлово –загрузочные вирусы.
- По **способу заражения** – на резидентные и нерезидентные вирусы.
- По **степени опасности** – на неопасные, опасные и очень опасные вирусы.
- По **особенностям алгоритма** – на вирусы-компаньоны, паразитические вирусы, репликаторы (черви), невидимки (стелс), мутанты (призраки, полиморфные вирусы, полиморфики), макро-вирусы, троянские программы.
- По **целостности** – на монолитные и распределенные вирусы.

- **Сетевые вирусы** распространяются по различным компьютерным сетям.
- **Загрузочные вирусы** 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 – таблице как “плохие” (Bad cluster).
- **Файловые вирусы** инфицируют исполняемые файла компьютера, имеющие расширения com и exe. К этому же классу относятся и макровирусы, написанные помощью макрокоманд. Они заражают неисполняемые файлы (например, в текстовом редакторе MS Word или в электронных таблицах MS Excel).

- **Загрузочно – файловые** вирусы способны заражать и загрузочные секторы и файлы.
- **Резидентные** вирусы оставляют в оперативной памяти компьютера свою резидентную часть, которая затем перехватывает обращения неинфицированных программ к операционной системе, и внедряются в них. Свои деструктивные действия и заражение других файлов, резидентные вирусы могут выполнять многократно.
- **Нерезидентные** вирусы не заражают оперативную память компьютера и проявляют свою активность лишь однократно при запуске инфицированной программы.

Действия вирусов могут быть не опасными, например, на экране появляется сообщение: “Хочу пироженку”. Если с клавиатуры набрать слово “пироженка”, то вирус временно “успокаивается”.

Значительно опаснее последствия действия вируса, который уничтожает часть файлов на диске.

- **Очень опасные** вирусы самостоятельно форматируют жесткий диск и этим уничтожают всю имеющуюся информацию. Примером очень опасного вируса может служить вирус CIN (Чернобыль), активизирующийся 26 числа каждого месяца и способный уничтожать данные на жестком диске и в BIOS.

- **Компаньон-вирусы** (companion) – это вирусы, не изменяющие файлы. Алгоритм работы этих вирусов состоит в том, что они создают для EXE – файлов новые файлы-спутники (дубликаты), имеющие то же самое имя, но с расширением COM, например, для файла XCOPY.EXE создается файл XCOPY.COM. Вирус записывается в COM – файл и никак не изменяет одноименный EXE – файл. При запуске такого файла DOS первым обнаружит и выполнит COM – файл, т.е. вирус, который затем запустит и EXE – файл.
- **Паразитические** вирусы при распространении своих копий обязательно изменяют содержимое дисковых секторов или файлов. В эту группу относятся все вирусы, которые не являются “червями” или “компаньонами”.
- Вирусы – **черви** (worm) – распространяются в компьютерной сети и, так же как и компаньон – вирусы, не изменяют файлы или секторы на дисках. Они проникают в память компьютера из компьютерной сети, вычисляют сетевые адреса других компьютеров и рассылают по этим адресам свои копии. Черви уменьшают пропускную способность сети, замедляют работу серверов.

- Репликаторы могут размножаться без внедрения в другие программы и иметь “начинку” из компьютерных вирусов.
- Вирусы – невидимки (стелс – Stealth) используют некоторый набор средств для маскировки своего присутствия в ЭВМ. Название вируса аналогично названию американского самолета – невидимки.
- Стелс – вирусы трудно обнаружить, так как они перехватывают обращения операционной системы к пораженным файлам или секторам дисков и “подставляют” незараженные участки файлов.

- Вирусы, которые шифруют собственное тело различными способами, называются полиморфными. Полиморфные вирусы (или вирусы – призраки, вирусы – мутанты, полиморфики) достаточно трудно обнаружить, так как 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.
- Макро – вирусы используют возможности макроязыков, встроенных в системы обработки данных (текстовые редакторы и электронные таблицы). В настоящее время широко распространяются макро – вирусы, заражающие документ Word и Excel.

- Троянская программа маскируется под полезную или интересную программу, выполняя во время своего функционирования еще и разрушительную работу (например, стирает FAT-таблицу) или собирает на компьютере информацию, не подлежащую разглашению. В отличии от вирусов троянские программы не обладают свойством самовоспроизводства.
- Троянская программа маскируется, как правило, под коммерческий продукт. Ее другое название “троянский конь”.

- Программа монолитного вируса представляет собой единый блок, который можно обнаружить после инфицирования.
- Программа распределенного вируса разделена на части. Эти части содержат инструкции, которые указывают компьютеру, как собрать их воедино, чтобы воссоздать вирус. Таким образом, вирус почти все время находится в распределенном состоянии, и лишь на короткое время собирается в единое целое.

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

Различают следующие виды антивирусных программ:

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

Программы – детекторы рассчитаны на обнаружение конкретных вирусов и основаны на сравнении характерной (спецификой) последовательности байтов (сигнатур или масок вирусов), содержащихся в теле вируса, с байтами проверяемых программ. Программы – детекторы нужно регулярно обновлять, так как они быстро устаревают и не могут выявлять новые виды вирусов.

Следует подчеркнуть, что программы – детекторы могут обнаружить только те вирусы, которые ей “известны”, то есть, есть сигнатуры этих вирусов заранее помещены в библиотеку антивирусных программ.

Таким образом, если проверяемая программа не опознается детектором как зараженная, то еще не следует считать, что она “здорова”. Она может быть инфицирована новым вирусом, который не занесен в базу данных детектора.

Для устранения этого недостатка программы – детекторы стали снабжаться блоками эвристического анализа программ. В этом режиме делается попытка обнаружить новые или неизвестные вирусы по характерным для всех вирусов кодовым последовательностям. Наиболее развитые эвристические механизмы позволяют с вероятностью около 80% обнаружить новый вирус.

Программы – доктора не только находят файлы, зараженные вирусами, но и лечат их, удаляя из файла тело программы – вируса. Программы – доктора, которые позволяет лечить большое число вирусов, называют полифагами.

В России получили широкое распространение программы – детекторы, одновременно выполняющие и функции программ – докторов. Наиболее известные представители этого класса – AVP (Antiviral Toolkit Pro, автор – Е. Касперский), Aidstest (автор – Д. Лозинский) и Doctor Web (авторы – И. Данилов, В. Лутовин, Д. Белоусов).

Ревизоры – это программы, которые анализируют текущее состояние файлов и системных областей диска и сравнивают его с информацией, сохраненной ранее в одном из файлов ревизора. При этом проверяется состояние BOOT – сектора, FAT – таблицы, а также длина файлов, их время создания, атрибуты, контрольные суммы.

Контрольная сумма является интегральной оценкой всего файла (его слепком). Получается контрольная сумма путем суммирования по модулю для всех байтов файла. Практически всякое изменение кода программы приводит к изменению контрольной суммы файла.

- Антивирусы – фильтры – это резидентные программы (сторожа), которые оповещают пользователя обо всех попытках какой – либо программы выполнить подозрительные действия. Фильтры контролируют следующие операции:
- Обновление программных файлов и системной области диска;
- Форматирование диска;
- Резидентное размещение программ в ОЗУ.

- Обнаружив попытку выполнения таких действий, сторож (монитор) сообщает об этом пользователю, который окончательное решение по выполнению данной операции. Заметим, что она не способна обезвредить даже известные вирусы. Для “лечения” обнаруженных фильтром вирусов нужно использовать программы – доктора.
- К последней группе относятся наименее эффективные антивирусы – вакцинаторы (иммунизаторы). Они записывают в вакцинируемую программу признаки конкретного вируса так, что вирус считает ее уже зараженной, и поэтому не производит повторное инфицирование. Этот вид антивирусных программ морально устарел.

Рассмотрим основные меры по защите ЭВМ от заражения вирусами.

- Необходимо оснастить ЭВМ современными антивирусными программами и постоянно обновлять их версии.
- При работе в глобальной сети обязательно должна быть установлена программа – фильтр (сторож, монитор).
- Перед считыванием с дискет информации, записанной на других ЭВМ, следует всегда проверять эти дискеты на наличие вирусов.

- При переносе на свой компьютер файлов в архивированном виде необходимо их проверять сразу же после разархивации.
- При работе при работе на других компьютерах необходимо всегда защищать свои дискеты от записи.
- Целесообразно делать архивные копии ценной информации на других носителях информации.
- Не следует оставлять дискету в дисководе при включении или перезагрузке ЭВМ, так как это может привести к заражению загрузочными вирусами.

- Антивирусную проверку желательно проводить в “чистой” операционной системе, то есть после ее загрузки с отдельной системной дискеты.
- Следует иметь ввиду, что невозможно заразиться вирусом, просто подключившись к Internet. Чтобы вирус активизировался программа, полученная с сервера из сети, должна быть запущена на клиенте.
- Получив электронное письмо, к которому приложен исполняемый файл, не следует запускать этот файл без предварительной проверки. По электронной почте часто распространяются “троянские кони”.

- Целесообразно иметь под рукой аварийную загрузочную дискету, с которой можно будет загрузиться, если система откажется сделать это обычным образом.
- При установке большого программного продукта необходимо вначале проверить все дистрибутивные файлы, а после инсталляции продукта повторно произвести контроль наличия вирусов.
- Последняя – не совсем серьезная мера. Если Вы хотите полностью исключить вероятность попадания вирусов в Ваш компьютер, то не набирайте на клавиатуре непонятных для Вас программ, не используйте дискеты, лазерные диски для ввода программ и документов. Отключитесь от локальной и глобальной сетей. Не включайте питание, так как возможно, что вирус уже зашит в ПЗУ.