Вирусы и антивирусные программы

Компьютерный вирус— 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.

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 (нужных) программ.

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 (инфицированной)** программой.

Когда инфицированная программа начинает работу, то сначала управление получает вирус. Вирус заражает другие программы, а также выполняет запланированные 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 обычная программа. Подобно настоящим вирусам, компьютерные вирусы действуют незаметно, размножаются и ищут возможность перейти на другие ЭВМ.

Несмотря на широкую распространенность антивирусных программ, предназначенных для борьбы с вирусами, вирусы продолжают плодиться. В среднем в месяц появляется около 300 новых разновидностей. Естественно, что вирусы появляются не самостоятельно, а их создают кракеры — вандалы.

Действия выполняемые вирусами**:**

- 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 (проигрывают гимн, гамму или популярную мелодию);
- создают видеоэффекты (переворачивают или сдвигают экран, имитируют землетрясение, вызывают опадание букв в тексте или симулируют снегопад, имитируют скачущий шарик, прыгающую точку, выводят на экран рисунки или картинки);
- 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;
- 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 в CMOS, стирают секторы на диске, уничтожают или искажают данные, стирают антивирусные программы;
- осуществляют научный, технический, промышленный и финансовой **шпионаж;**
- выводят из строя системы защиты информации, дают злоумышленникам тайный доступ к вычислительной машине;
- делают незаконные отчисления с каждой финансовой операции;
- автоматически рассылают письма по адресам, указанным в адресной книге почтового клиента, и т. д.

Основные **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 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 функционировавших программ.
- Поступление электронного письма с исполняемым приложением от неизвестного корреспондента.

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, происходящей в ядерном реакторе, запущенный процесс трудно остановить.

Первые исследования саморазмножающихся искусственных конструкций проводились в середине XX столетия. В работах фон Неймана, Винера и других дано определение и проведен математический анализ конечных автоматов, в том числе и самовоспроизводящихся.

Впервые большое внимание к проблеме вирусов привлекла книга Фреда Коэна (F. Cohen) «Компьютерные вирусы, теория и эксперименты», вышедшая в свет в 1984 г.

Первый эксперимент по распространению вируса Ф. Коэн провел 10 сентября 1983 г. в Университете Южной Калифорнии в рамках семинара по безопасности.

Большой общественный резонанс вызвало первое неконтролируемое распространение вируса в сети. 2 ноября 1988 г. двадцатитрехлетний студент последнего курса Корнельского университета Роберт Таппан **Моррис** запустил в сеть свою программу, которая из-за ошибки начала бесконтрольное распространение и многократное инфицирование узлов сети. В результате было заражено около 6200 машин, что составило 7,3% общей численности машин в сети.

Виды 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 (стеле), мутанты (призраки, полиморфные вирусы, полиморфики), макровирусы, троянские программы.

По **целостности** — на монолитные и распределенные вирусы.

Загрузочные вирусы внедряются в загрузочный сектор диска (Boot-сектор) или в секторы, содержащий программу загрузки системного диска (Master Boot Record — MBR). Некоторые вирусы записывают свое тело в свободные секторы диска, помечая их в FAT-таблице как «плохие» (Bad uster).

Файловые вирусы инфицируют исполняемые файлы компьютера, имеющие расширения com и exe. К этому же классу относятся и макровирусы, написанные с 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 конструктивные 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 чучу». Если с клавиатуры набрать слово «чуча», 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 CIH «Чернобыль», активизирующийся 26-го 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-фаилов новые файлы-спутники (дубликаты), имеющие то же самое имя, но с расширением 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, находят 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.

В конце 80-х годов XX столетия сетевой вирус «Червь Морриса» парализовал несколько глобальных сетей в США.

Вирусы-невидимки (стеле — 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** (polymorphic). 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

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 отличие 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 программы. Говоря медицинским языком, эти программы могут выявлять (диагностировать), лечить (уничтожать) вирусы и делать прививку «здоровым» программам.

Виды антивирусных программ:

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

Программы-детекторы рассчитаны на обнаружение конкретных вирусов. Принцип их действия основан на сравнении характерной (специфической) последовательности байтов **(сигнатур,** портретов или масок вирусов), содержащихся в теле вируса, с текстом 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», т. е., если 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, называются полифагами.

В России получили широкое распространение программы-детекторы, одновременно выполняющие и функции программ-докторов. Наиболее известные представители этого класса — AVP (Antiviral Toolkit

Е. Касперский), Aidstest (автор — Д. Лозинский) и Doctor Web (авторы — И. Данилов, В. Лутовинов, 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-секторы, 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 два всех байтов файла. Практически всякое изменение кода программы приводит к изменению контрольной суммы файла.

Ревизоры сначала запоминают сведения о состоянии программ и системных областей дисков (загрузочного сектора и сектора с таблицей разбиения жесткого диска). Предполагается, что в этот

момент программы и системные области дисков не заражены. После этого с помощью ревизора можно в любой момент времени сравнить состояние программ и системных областей дисков с их исходными состояниями. О выявленных несоответствиях ревизор сообщает пользователю. Ревизоры контролируют файловую систему, отслеживая перемещение, переименование, создание и удаление файлов и папок. Доктора-ревизоры не только обнаруживают изменения в файлах и системных областях дисков, но и могут в случае обнаружения изменений вернуть их в исходное состояние.

Антивирусная программа ADinf (Advanced Diskinfoscope, автор — Д. Мостовой) относится к классу ревизоров. Антивирус имеет высокую скорость работы, способен с успехом противостоять вирусам, находящимся в памяти. Он позволяет контролировать диск, читая его по секторам через BIOS и не используя системные прерывания DOS, которые может перехватить вирус. В отличие от полифагов, ADinf не использует в своей работе «портреты» (сигнатуры) конкретных вирусов. Поэтому ADinf особенно эффективен при обнаружении новых вирусов, противоядие для которых еще не придумано. Ревизор ADinf может быть дополнен лечащим блоком ADinf Cure Module.

Среди зарубежных антивирусных программ чаще других упоминаются в печати программы Dr Solomon's Anti-Virus 7.0, McAfee VirusScan 3.0, Norton AntiVirus 4.0.

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.**
- 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 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, т. е. после ее загрузки с отдельной системной дискеты.
- Следует иметь ввиду, что невозможно заразиться вирусом, просто подключившись к Интернету. Чтобы вирус активизировался, программа, полученная с сервера из сети, должна быть на компьютере-клиенте запущена на выполнение.
- Получив электронное письмо, к которому приложен исполняемый файл, **не следует запускать этот файл без предварительной** проверки. По электронной почте часто распространяются троянские программы.
- 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, магнитную ленту для ввода программ и документов. Отключитесь от локальной и глобальной сетей. Не включайте питание, так как возможно, что вирус уже зашит в ПЗУ.

Как и всякие автоматические средства, антивирусные программы могут совершать ошибки первого и второго родов: пропускать имеющиеся вирусы и давать ложные сигналы даже при отсутствии вирусов.

В ряде программ используется так называемое эвристическое сканирование, основанное на вероятностном методе выявления вирусов. При эвристическом сканировании антивирусная программа отыскивает характерные для вирусов комбинации команд (перезапись, удаление и т. п.). Для таких программ не требуется обновления портретов вирусов (сигнатур), и они способны обнаружить новые разновидности вирусов.