Термин «компьютерный вирус» был введен сравнительно недавно – в середине 80-х годов. Считается, что его впервые употребил сотрудник Лехайского университета (США) Ф.Коэн в 1984 г. на 7-й конференции по безопасности информации, проходившей в США. Малые размеры, способность быстро распространяться, размножаясь и внедряясь в объекты (заражая их), негативное воздействие на систему – все эти признаки биологических вирусов присущи и вредительским программам, получившим по этой причине название «компьютерные вирусы».

Вместе с термином «вирус» при работе с компьютерными вирусами используются и другие медицинские термины: «заражение», «среда обитания», «профилактика», «вакцинация» и др.

«Компьютерные вирусы» – это небольшие исполняемые или интерпретируемые программы, обладающие свойством распространения и самовоспроизведения (репликации) в КС. Они, как правило, распространяются скрытно и оказывают негативное воздействие на ресурсы КС. В процессе распространения вирусы могут себя модифицировать.

Не смотря на огромное количество и разнообразие компьютерных вирусов, их можно распределить по классам в соответствии с выбранными признаками. Классификация позволяет лучше понять механизмы работы таких программ. В качестве признаков классификации компьютерных вирусов могут использоваться:

- среда обитания;
- операционная система;
- фаза активности;
- алгоритм функционирования;
- степень опасности деструктивных (вредительских) воздействий.

По среде обитания компьютерные вирусы делятся на:

- файловые;
- загрузочные;
- комбинированные,
- сетевые.

Файловые вирусы размещаются в исполняемых файлах. К файловым относятся также вирусы, которые создают файлы-двойники (компаньон-вирусы), либо используют особенности организации файловой системы (link-вирусы).

Загрузочные вирусы находятся в загрузочных секторах (областях) внешних запоминающих устройств (boot-секторах). Иногда загрузочные вирусы называют бутовыми.

Комбинированные вирусы размещаются в нескольких средах обитания. Примером таких вирусов служат загрузочно-файловые вирусы. Эти вирусы могут размещаться как в загрузочных секторах накопителей на магнитных дисках, так и в теле загрузочных файлов.

Сетевые вирусы используют для своего распространения протоколы или команды компьютерных сетей и электронной почты.

Вирусы способны функционировать в одной или в нескольких операционных системах. Причем отдельные вирусы могут нормально функционировать в нескольких ОС, если эти системы совместимы. Это относится к ОС, разработанных фирмой Microsoft. Например, Windows 95, Windows 98 Windows 2000, Windows XP. Это объясняется тем,

что компьютерные вирусы используют особенности файловой структуры ОС, а также ориентированы на конкретные форматы расположения системных данных в загрузочных секторах дисков.

По фазе активности компьютерные вирусы делятся на:

• резидентные;

• нерезидентные.

Резидентные вирусы после их активизации полностью или частично перемещаются из среды обитания (сеть, загрузочный сектор, файл) в оперативную память ЭВМ. Эти вирусы, используя, как правило, привилегированные режимы работы, разрешенные только операционной системе, заражают среду обитания и при выполнении определенных условий реализуют деструктивную функцию. Резидентный вирус или его часть постоянно находится в оперативной памяти и сохраняет активность до перезагрузки или выключения питания ЭВМ. Вирус перехватывает управление (выполняется) при наступлении определенных событий в вычислительном процессе.

В отличие от резидентных нерезидентные вирусы попадают в оперативную память ЭВМ только на время их активности, в течение которого выполняют функцию заражения среды обитания и, если требуется, выполняют деструктивную функцию. Затем вирус полностью покидает оперативную память, оставаясь в среде обитания. Следующее выполнение вируса возможно лишь в случае выполнения зараженной программы, или загрузки ОС с зараженного диска, или при поступлении вируса из сети и его активизации.

По сложности, степени совершенства и особенностям маскировки алгоритмов функционирования вирусы, делятся на:

• студенческие;

• стелс-вирусы (вирусы-невидимки);

• полиморфные.

К студенческим относят вирусы, создатели которых имеют низкую квалификацию. Такие вирусы, как правило, являются нерезидентными, часто содержат ошибки, довольно просто обнаруживаются и удаляются.

Стелс-вирусы и полиморфные вирусы создаются квалифицированными специалистами, хорошо знающими принцип работы аппаратных средств и операционной системы, а также владеющими навыками работы с машиноориентированными системами программирования.

Стелс-вирусы маскируют свое присутствие в среде обитания путем перехвата обращений операционной системы к пораженным файлам, секторам и переадресуют ОС к незараженным участкам информации. Вирус является резидентным, маскируется под программы ОС, может перемещаться в памяти. Такие вирусы активизируются при возникновении прерываний, выполняют определенные действия, в том числе и по маскировке, и только затем управление передается на программы ОС, обрабатывающие эти прерывания. Стелс-вирусы обладают способностью противодействовать резидентным антивирусным средствам.

Полиморфные вирусы не имеют постоянных опознавательных групп – «масок» («сигнатур»). Обычные вирусы для распознавания факта заражения среды обитания размещают в зараженном объекте специальную опознавательную двоичную последовательность или последовательность символов (маску), которая однозначно идентифицирует зараженность файла или сектора. Сигнатуры используются на этапе

распространения вирусов для того, чтобы избежать многократного заражения одних и тех же объектов, так как при многократном заражении объекта значительно возрастает вероятность обнаружения вируса. Для устранения демаскирующих признаков полиморфные вирусы используют шифрование тела вируса и модификацию программы шифрования. За счет такого преобразования полиморфные вирусы не имеют совпадений кодов.

Арсенал деструктивных или вредительских возможностей компьютерных вирусов весьма обширен. Деструктивные возможности вирусов зависят от целей и квалификации их создателя, а также от особенностей компьютерных систем.

По степени опасности для информационных ресурсов пользователя компьютерные вирусы можно разделить на:

- безвредные вирусы;
- опасные вирусы;
- очень опасные вирусы.

Безвредные компьютерные вирусы создаются авторами, которые не ставят себе цели нанести какой-либо ущерб ресурсам КС. Ими, как правило, движет желание показать свои возможности программиста. Другими словами, создание компьютерных вирусов для таких людей – своеобразная попытка самоутверждения. Деструктивное воздействие таких вирусов сводится к выводу на экран монитора невинных текстов и картинок, исполнению музыкальных фрагментов и т. п.

Однако при всей кажущейся безобидности таких вирусов они наносят определенный ущерб КС. Во-первых, такие вирусы расходуют ресурсы КС, в той или иной мере снижая ее эффективность функционирования. Во-вторых, компьютерные вирусы могут содержать ошибки, вызывающие опасные последствия для информационных ресурсов КС. Кроме того, при модернизации операционной системы или аппаратных средств КС вирусы, созданные ранее, могут приводить к нарушениям штатного алгоритма работы системы.

К опасным относятся вирусы, которые вызывают существенное снижение эффективности КС, но не приводящие к нарушению целостности и конфиденциальности информации, хранящейся в запоминающих устройствах. Последствия таких вирусов могут быть ликвидированы без особых затрат материальных и временных ресурсов. Примерами таких вирусов являются вирусы, занимающие память ЭВМ и каналы связи, но не блокирующие работу сети; вирусы, вызывающие необходимость повторного выполнения программ, перезагрузки операционной системы или повторной передачи данных по каналам связи и т. п.

Очень опасными следует считать вирусы, вызывающие нарушение конфиденциальности, уничтожение, необратимую модификацию (в том числе и шифрование) информации, а также вирусы, блокирующие доступ к информации, приводящие к отказу аппаратных средств и наносящие ущерб здоровью пользователям. Такие вирусы стирают отдельные файлы, системные области памяти, форматируют диски, получают несанкционированный доступ к информации, шифруют данные и т. п.

Использование в современных ПЭВМ постоянной памяти с возможностью перезаписи привело к появлению вирусов, изменяющих программы BIOS, что приводит к необходимости замены постоянных запоминающих устройств.

Известны публикации, в которых упоминаются вирусы, вызывающие неисправности аппаратных средств. Предполагается, что на резонансной частоте движущиеся части

электромеханических устройств, например, в системе позиционирования накопителя на магнитных дисках, могут быть разрушены. Именно такой режим и может быть создан с помощью программы-вируса. Другие авторы утверждают, что возможно задание режимов интенсивного использования отдельных электронных схем (например, больших интегральных схем), при которых наступает их перегрев и выход из строя. Реализация подобных возможностей вредительских программ на практике если и возможна, то связана с большими сложностями.

Высказываются также предположения о возможности воздействия на психику человека–оператора ЭВМ с помощью подбора видеоизображения, выдаваемого на экран монитора с определенной частотой (каждый двадцать пятый кадр). Встроенные кадры этой видеоинформации воспринимаются человеком на подсознательном уровне. В результате такого воздействия возможно нанесение серьезного ущерба психике человека. В 1997 году 700 японцев попали в больницу с признаками эпилепсии после просмотра компьютерного мультфильма по телевидению. Предполагают, что именно таким образом была опробована возможность воздействия на человека с помощью встраивания 25-го кадра.

Любой вирус, независимо от принадлежности к определенным классам, должен иметь три функциональных блока: блок заражения (распространения), блок маскирования и блок выполнения деструктивных действий (если они предусмотрены). Разделение на функциональные блоки означает, что к определенному блоку относятся команды программы вируса, выполняющие одну из трех функций, независимо от места нахождения команд в теле вируса.

После передачи управления вирусу, как правило, выполняются определенные функции блока маскировки. Например, осуществляется расшифрование тела вируса. Затем вирус осуществляет функцию внедрения в незараженную среду обитания. Если вирусом должны выполняться деструктивные воздействия, то они выполняются либо безусловно, либо при выполнении определенных условий.

Завершает работу вируса всегда блок маскирования. При этом выполняются, например, следующие действия: шифрование вируса (если функция шифрования реализована), восстановление старой даты изменения файла, восстановление атрибутов файла, корректировка таблиц ОС и др.

Последней командой вируса выполняется команда перехода на выполнение зараженных файлов или на выполнение программ ОС.

Для удобства работы с известными вирусами используются каталоги вирусов. В каталог помещаются следующие сведения о стандартных свойствах вируса: имя, длина, заражаемые файлы, место внедрения в файл, метод заражения, способ внедрения в оперативную память для резидентных вирусов, вызываемые эффекты, наличие (отсутствие) деструктивной функции и ошибки. Наличие каталогов позволяет при описании вирусов указывать только особые свойства, опуская стандартные свойства и действия.

По статистике последних лет 97% всех заражений компьютерными вирусами происходит при работе с Internet. Практически не встречаются случаи попадания вредительских программ в компьютеры пользователей на дискетах и с дистрибутивными дисками, предназначенными для установки программного обеспечения. Вредительские программы могут попасть в компьютер из сети Internet следующими путями: при запуске файла-приложения почтового сообщения, при использовании файлов-программ,

полученных из сети, например, по протоколу FTP, при получении документов, зараженных макровирусами, а также при использовании средств автоматизации обмена информацией и «оживления» WEB-страниц с помощью Java-аплетов, Java-скриптов. технологии ActiveX. Особое распространение получили сетевые черви, которые распространяются с использованием почтового протокола (около 98% всех заражений при работе с Internet).

На втором месте находятся вирусы, распространяемые с использованием протокола IRC (протокол общения абонентов путем посылки сообщений). Протокол допускает использование сценариев (Java-скриптов). Программы сценариев пишутся на особом языке программирования и не могут нанести серьезный ущерб пользовательской системе, так как они лишены возможности доступа к файловой системе пользователя. Но именно в протоколе IRC имеется возможность пересылки файлов. Этой лазейкой и пользуются злоумышленники.

Выполнение Java-аплетов, Java-скриптов и использование технологии ActiveX может ограничиваться или полностью запрещаться настройками браузеров пользователей. В остальных случаях вирусы могут быть обнаружены только антивирусными средствами.

Для предотвращения заражения КС вирусами необходимо регулярно применять антивирусные средства и выполнять ряд организационных мер. Антивирусные средства применяются для решения следующих задач: обнаружение вирусов в КС, блокирование работы программ-вирусов, устранение последствий воздействия вирусов. Особое внимание должно быть направлено на проверку программ, получаемых из открытых сетей. Известны следующие методы обнаружения вирусов:

1) сканирование;
2) обнаружение изменений;
3) использование резидентных сторожей;
4) вакцинирование (иммунизация) программ;
5) аппаратно-программная защита от вирусов.

Сканирование – один из самых эффективных и распространенных методов обнаружения вирусов. Сканирование осуществляется программой-сканером, которая просматривает файлы в поисках опознавательной части вируса – маски. Маска представляет собой уникальный код и записывается некоторыми вирусами в тело зараженной программы (участка памяти). Маска используется вирусами на стадии размножения копий программы-вируса с целью предотвращения многократного заражения одного и того же объекта. Программа-сканер фиксирует наличие уже известных вирусов, за исключением полиморфных вирусов, которые применяют шифрование тела вируса, изменяя при этом каждый раз и маску. Программы-сканеры часто могут удалять обнаруженные вирусы. Такие программы называются полифагами.

Многие сканеры имеют в своем составе эвристические анализаторы, которые позволяют определять неизвестные вирусы. Сущность эвристического анализа заключается в проверке возможных сред обитания вирусов и выявление в них команд (групп команд), характерных для вирусов. Такими командами могут быть команды создания резидентных модулей в оперативной памяти, команды прямого обращения к дискам, минуя ОС и некоторые другие.

Эвристические анализаторы при обнаружении «подозрительных» команд в файлах или загрузочных секторах выдают сообщение о возможном заражении. После получения таких сообщений необходимо тщательно проверить предположительно зараженные

файлы и загрузочные сектора всеми имеющимися антивирусными средствами. Эвристический анализатор имеется, например, в антивирусной программе Doctor Web.

Сканеры можно разделить на две категории - "универсальные" и "специализированные". Универсальные сканеры рассчитаны на поиск и обезвреживание всех типов вирусов. Специализированные сканеры предназначены для обезвреживания ограниченного числа вирусов или только одного их класса, например макро-вирусов.

К достоинствам сканеров всех типов относится их универсальность, к недостаткам - размеры антивирусных баз и относительно небольшая скорость поиска вирусов. Для эффективного использования метода необходимо регулярное обновление базы данных о вирусах.

Метод обнаружения изменений базируется на использовании программ-ревизоров, которые называют также CRC-сканерами. Эти программы определяют и запоминают характеристики файлов и всех областей на дисках, в которых обычно размещаются вирусы. При периодическом выполнении программ-ревизоров сравниваются хранящиеся характеристики и характеристики, получаемые при контроле областей дисков. По результатам ревизии программа выдает сведения о предположительном наличии вирусов.

Обычно программы-ревизоры запоминают в своих базах данных образы главной загрузочной записи, загрузочных секторов логических дисков, каталогов и номера дефектных кластеров, а также характеристики всех контролируемых файлов (контрольные суммы, длины файлов, даты их последней модификации и т.п.). Могут контролироваться также объем установленной оперативной памяти, количество подключенных к компьютеру дисков и их параметры.

Главным достоинством метода является возможность обнаружения вирусов всех типов, а также новых неизвестных вирусов. Совершенные программы-ревизоры обнаруживают даже стелс-вирусы. Например, программа-ревизор Adinf работала с диском непосредственно по секторам через BIOS. Это не позволяло стелс-вирусам перехватывать прерывания и «подставлять» для контроля нужную вирусу область памяти. В настоящее время используется новая версия программы – Adinf32.

Имеются у этого метода и недостатки. С помощью программ-ревизоров невозможно определить вирус в файлах, которые поступают в систему уже зараженными. Вирусы будут обнаружены только после размножения в системе.

Метод использования резидентных сторожей (антивирусных блокираторов) основан на применении программ, которые постоянно находятся в оперативной памяти ЭВМ и отслеживают все действия остальных программ.

В случае выполнения какой-либо программой подозрительных действий (обращение для записи в загрузочные сектора, помещение в оперативную память резидентных модулей, попытки перехвата прерываний и т. п.) резидентный сторож блокирует выполнение «подозрительной программы» и выдает сообщение пользователю. Программа-сторож может загружать на выполнение другие антивирусные программы для проверки «подозрительных» программ, а также для контроля всех поступающих извне файлов (со сменных дисков, по сети).

Существенным недостатком данного метода является значительный процент ложных тревог, что мешает работе пользователя, вызывает раздражение и желание отказаться от использования резидентных сторожей. По этой причине такие программы не нашли

широкого применения.

Специальные программные блоки, выполняющие вакцинацию или иммунизацию программ, называют иммунизаторами. Вакцинация осуществляется двумя способами. Первый способ заключается во внедрении в вакцинируемую программу блока, проверяющего целостность программы при ее запуске. Как правило, такой блок подсчитывает контрольную сумму программы и сравнивает ее с эталонной. При несовпадении контрольных сумм выдается соответствующее сообщение оператору.

Этот способ позволяет обнаруживать все вирусы, в том числе и незнакомые, за исключением стелс-вирусов, если вакцинация произведена до внедрения вируса в защищаемую программу. Неспособность таких иммунизаторов определять наличие стелс-вирусов привела к тому, что они, как и блокировщики, практически не используются в настоящее время.

Второй тип иммунизации защищает систему от поражения вирусом какого-то определенного вида. Файлы на дисках модифицируются таким образом, что вирус принимает их за уже зараженные. Для защиты от резидентного вируса в память компьютера заносится программа, имитирующая копию вируса. При запуске вирус натыкается на нее и считает, что система уже заражена.

Наибольшее распространение в нашей стране получили комплексы антивирусных средств AVP и Doctor Web. Семейства антивирусных программ разработаны для наиболее распространенных операционных системы и позволяют обнаруживать и удалять вирусы всех видов. Пакеты этих фирм стабильно признаются одними из лучших в мире среди антивирусных средств. Они включают в свой состав наборы антивирусных программ пользователей всех классов и применимы для защиты, как автономных ПЭВМ, так и сетевых компонент.

Для того, чтобы снизить вероятность попадания компьютерных вирусов в КС, необходимо выполнять следующие несложные правила: использовать программные средства, полученные официальным путем, регулярно применять антивирусные средства, особую осторожность проявлять при использовании новых файлов, полученных извне по каналам связи или на носителях. Для сохранения информации необходимо выполнять ее дублирование на съемные носители.

Даже при скрупулезном выполнении всех правил профилактики возможность заражения ЭВМ компьютерными вирусами полностью исключить нельзя. И если вирус все же попал в КС, то последствия его пребывания можно свести к минимуму, придерживаясь определенной последовательности действий.

О наличии вируса в КС пользователь может судить по следующим событиям:

• появление сообщений антивирусных средств о заражении или о предполагаемом заражении;

• явные проявления присутствия вируса, такие как сообщения, выдаваемые на монитор или принтер, звуковые эффекты, уничтожение файлов и другие аналогичные действия, однозначно указывающие на наличие вируса в КС;

• неявные проявления заражения, которые могут быть вызваны и другими причинами, например, сбоями или отказами аппаратных и программных средств КС.

К неявным проявлениям наличия вирусов в КС можно отнести «зависания» системы, замедление выполнения определенных действий, нарушение адресации, сбои устройств и тому подобное.

Получив информацию о предполагаемом заражении, пользователь должен убедиться в

этом. Решить такую задачу можно с помощью всего комплекса антивирусных средств. Убедившись в том, что заражение произошло, пользователю следует выполнить следующую последовательность шагов:

Шаг 1. Выключить ЭВМ для уничтожения резидентных вирусов.

Шаг 2. Осуществить загрузку эталонной операционной системы со сменного носителя информации, в которой отсутствуют вирусы.

Шаг 3. Сохранить на сменных носителях информации важные для вас файлы, которые не имеют резервных копий.

Шаг 4. Использовать антивирусные средства для удаления вирусов и восстановления файлов, областей памяти. Если работоспособность ЭВМ восстановлена, то осуществляется переход к шагу 8, иначе – к шагу 5.

Шаг 5. Осуществить полное стирание и разметку (форматирование) несъемных внешних запоминающих устройств.

Шаг 6. Восстановить ОС, другие программные системы и файлы с дистрибутивов и резервных копий, созданных до заражения.

Шаг 7. Тщательно проверить файлы, сохраненные после обнаружения заражения, и, при необходимости, удалить вирусы и восстановить файлы;

Шаг 8. Завершить восстановление информации всесторонней проверкой ЭВМ с помощью всех имеющихся в распоряжении пользователя антивирусных средств.

При выполнении рекомендаций по профилактике заражения компьютерными вирусами, а также при умелых и своевременных действиях в случае заражения вирусами, ущерб информационным ресурсам КС может быть сведен к минимуму.