**КОМПЬЮТЕРНЫЕ ВИРУСЫ, ИХ КЛАССИФИКАЦИЯ. АНТИВИРУСНЫЕ ПРОГРАММНЫЕ СРЕДСТВА**

***Компьютерный вирус*** — это специальная программа, Способная самопроизвольно присоединяться к другим программам и при запуске последних выполнять различные нежелательные действия: порчу файлов и каталогов; искажение результатов вычислений; засорение или стирание памяти; создание помех в работе компьютера. Наличие вирусов проявляется в разных ситуациях.

1. Некоторые программы перестают работать или начинают работать некорректно.
2. На экран выводятся посторонние сообщения, сигналы и другие эффекты.
3. Работа компьютера существенно замедляется.
4. Структура некоторых файлов оказывается испорченной.

**Имеются несколько признаков классификации существующих вирусов:**

* по среде обитания;
* по области поражения;
* по особенности алгоритма;
* по способу заражения;
* по деструктивным возможностям.

**По среде обитания** различают файловые, загрузочные, макро- и сетевые вирусы.

Файловые вирусы — наиболее распространенный тип вирусов. Эти вирусы внедряются в выполняемые файлы, создают файлы-спутники (companion-вирусы) или используют особенности организации файловой системы (link-вирусы).

Загрузочные вирусы записывают себя в загрузочный сектор диска или в сектор системного загрузчика жесткого диска. Начинают работу при загрузке компьютера и обычно становятся резидентными.

Макровирусы заражают файлы широко используемых пакетов обработки данных. Эти вирусы представляют собой программы, написанные на встроенных в эти пакеты языках программирования. Наибольшее распространение получили макровирусы для приложений Microsoft Office.

Сетевые вирусы используют для своего распространения протоколы или команды компьютерных сетей и электронной почты. Основным принципом работы сетевого вируса является возможность самостоятельно передать свой код на удаленный сервер или рабочую станцию. Полноценные компьютерные вирусы при этом обладают возможностью запустить на удаленном компьютере свой код на выполнение.

На практике существуют разнообразные сочетания вирусов — например, файлово-загрузочные вирусы, заражающие как файлы, так и загрузочные секторы дисков, или сетевые макровирусы, которые заражают редактируемые документы и рассылают свои копии по электронной почте.

Как правило, каждый вирус заражает файлы одной или нескольких ОС. Многие загрузочные вирусы также ориентированы на конкретные форматы расположения системных данных в загрузочных секторах дисков. По особенностям алгоритма выделяют резидентные ; вирусы, стелс-вирусы, полиморфные и др. Резидентные вирусы способны оставлять свои копии в ОП, перехватывать обработку событий (например, обращение к файлам или дискам) и вызывать при этом процедуры заражения объектов (файлов или секторов). Эти вирусы активны в памяти не только в момент работы зараженной программы, но и после. Резидентные копии таких вирусов жизнеспособны до перезагрузки ОС, даже если на диске уничтожены все зараженные файлы. Если резидентный вирус является также загрузочным и активизируется при загрузке ОС, то даже форматирование диска при наличии в памяти этого вируса его не удаляет.

К разновидности резидентных вирусов следует отнести также макровирусы, поскольку они постоянно присутствуют в памяти компьютера во время работы зараженного редактора.

Стелс-алгоритмы позволяют вирусам полностью или частично скрыть свое присутствие. Наиболее распространенным стелс-алгоритмом является перехват запросов ОС на чтение/запись зараженных объектов. Стелс-вирусы при этом либо временно лечат эти объекты, либо подставляют вместо себя незараженные участки информации. Частично к стелс-вирусам относят небольшую группу макровирусов, хранящих свой основной код не в макросах, а в других областях документа — в его переменных или в Auto-text.

Полиморфность (самошифрование) используется для усложнения процедуры обнаружения вируса. Полиморфные вирусы — это трудно выявляемые вирусы, не имеющие постоянного участка кода. В общем случае два образца одного и того же вируса не имеют совпадений. Это достигается шифрованием основного тела вируса и модификациями программы-расшифровщика.

При создании вирусов часто используются нестандартные приемы. Их применение должно максимально затруднить обнаружение и удаление вируса.

**По способу заражения различают** троянские программы, утилиты скрытого администрирования, Intended-вирусы и т. д.

Троянские программы получили свое название по аналогии с троянским конем. Назначение этих программ — имитация каких-либо полезных программ, новых версий популярных утилит или дополнений к ним. При их записи пользователем на свой компьютер троянские программы активизируются и выполняют нежелательные действия.

Разновидностью троянских программ являются утилиты скрытого администрирования. По своей функциональности и интерфейсу они во многом напоминают системы администрирования компьютеров в сети, разрабатываемые и распространяемые различными фирмами — производителями программных продуктов. При инсталляции эти утилиты самостоятельно устанавливают на компьютере систему скрытого удаленного управления. В результате возникает возможность скрытого управления этим компьютером. Реализуя заложенные алгоритмы, утилиты без ведома пользователя принимают, запускают или отсылают файлы, уничтожают информацию, Эрезагружают компьютер и т. д. Возможно использование этих утилит для обнаружения и передачи паролей и ной конфиденциальной информации, запуска вирусов, ничтожения данных.

К Intended-вирусам относятся программы, которые не способны размножаться из-за существующих в них ошибок. К этому классу также можно отнести вирусы, которые размножаются только один раз. Заразив какой-либо файл, они теряют способность к дальнейшему размножению через него.

**По деструктивным возможностям вирусы разделяются на:**

1. неопасные, влияние которых ограничивается уменьшением свободной памяти на диске, замедлением работы компьютера, графическим и звуковыми эффектами;
2. опасные, которые потенциально могут привести к нарушениям в структуре файлов и сбоям в работе компьютера;
3. очень опасные, в алгоритм которых специально заложены процедуры уничтожения данных и возможность обеспечивать быстрый износ движущихся частей механизмов путем ввода в резонанс и разрушения головок чтения/записи некоторых НЖМД.

Для борьбы с вирусами существуют программы, которые можно разбить на основные группы: мониторы, детекторы, доктора, ревизоры и вакцины.

***Программы-мониторы*** (программы-фильтры) располагаются резидентно в ОП компьютера, перехватывают и сообщают пользователю об обращениях ОС, которые используются вирусами для размножения и нанесения ущерба. Пользователь имеет возможность разрешить или запретить выполнение этих обращений. К преимуществу таких программ относится возможность обнаружения неизвестных вирусов. Использование программ-фильтров позволяет обнаруживать вирусы на ранней стадии заражения компьютера. Недостатками программ являются невозможность отслеживания вирусов, обращающихся непосредственно к BIOS, а также загрузочных вирусов, активизирующихся до запуска антивируса при загрузке DOS, и частая выдача запросов на выполнение операций.

***Программы-детекторы*** проверяют, имеется ли в файлах и на дисках специфическая для данного вируса комбинация байтов. При ее обнаружении выводится соответствующее сообщение. Недостаток — возможность защиты только от известных вирусов.

***Программы-доктора*** восстанавливают зараженные программы путем удаления из них тела вируса. Обычно эти программы рассчитаны на конкретные типы вирусов и основаны на сравнении последовательности кодов, содержащихся в теле вируса, с кодами проверяемых программ. Программы-доктора необходимо периодически обновлять с целью получения новых версий, обнаруживающих новые виды вирусов.

***Программы-ревизоры*** анализируют изменения состояния файлов и системных областей диска. Проверяют состояние загрузочного сектора и таблицы FAT; длину, атрибуты и время создания файлов; контрольную сумму кодов. Пользователю сообщается о выявлении несоответствий.

***Программы-вакцины*** модифицируют программы и риски так, что это не отражается на работе программ, но вирус, от которого производится вакцинация, считает программы или диски уже зараженными. Существующие антивирусные программы в основном относятся к классу гибридных (детекторы-доктора, доктора-ревизоры и пр.).

В России наибольшее распространение получили антивирусные программы Лаборатории Касперского (Anti-IViral Toolkit Pro) и ДиалогНаука (Adinf,Dr.Web). Антивирусный пакет AntiViral Toolkit Pro (AVP) включает AVP Сканер, резидентный сторож AVP Монитор, программу администрирования установленных компонентов. Центр управления и ряд других. AVP Сканер помимо традиционной проверки выполняемых файлов и файлов документов обрабатывает базы данных электронной почты. Использование сканера позволяет выявить вирусы в упакованных и архивированных файлах (не защищенных паролями). Обнаруживает к удаляет макровирусы, полиморфные, стеле, троянские, а также ранее неизвестные вирусы. Это достигается, например, за счет использования эвристических анализаторов. Такие анализаторы моделируют работу процессора и выполняют анализ действий диагностируемого файла. В зависимости от этих действий и принимается решение о наличии вируса.

Монитор контролирует типовые пути проникновения вируса, например операции обращения к файлам и секторам.

AVP Центр управления — сервисная оболочка, предназначенная для установки времени запуска сканера, автоматического обновления компонент пакета и др.

При заражении или при подозрении на заражение компьютера вирусом необходимо:

1. оценить ситуацию и не предпринимать действий, приводящих к .потере информации;
2. перезагрузить ОС компьютера. При этом использовать специальную, заранее созданную и защищенную от записи системную дискету. В результате будет предотвращена активизация загрузочных и резидентных вирусов с жесткого диска компьютера;
3. запустить имеющиеся антивирусные программы, пока не будут обнаружены и удалены все вирусы. В случае невозможности удалить вирус и при наличии в файле ценной информации произвести архивирование файла и подождать выхода новой версии антивируса. После окончания перезагрузить компьютер.