**КОМПЬЮТЕРНЫЕ ВИРУСЫ**

**1. Компьютерные вирусы, их свойства и классификация**

Вирус – вредоносная программа, обладающая способностью к самовоспроизведению. Такая способность является единственным средством, присущим всем типам вирусов. Но не только вирусы способны к самовоспроизведению. Любая операционная система и еще множество программ способны создавать собственные копии. Копии же вируса не только не обязаны полностью совпадать с оригиналом, но и могут вообще с ним не совпадать!

Вирус не может существовать в "полной изоляции": сегодня нельзя представить себе вирус, который не использует код других программ, информацию о файловой структуре или даже просто имена других программ. Причина понятна: вирус должен каким-нибудь способом обеспечить передачу себе управления.

В настоящее время известно более 5000 программных вирусов, их можно классифицировать по следующим признакам:

* среде обитания
* способу заражения среды обитания
* воздействию
* особенностям алгоритма

В зависимости от среды обитания вирусы можно разделить на сетевые, файловые, загрузочные и файлово-загрузочные.

*Сетевые вирусы* распространяются по различным компьютерным сетям. Файловые вирусы внедряются главным образом в исполняемые модули, т. е. В файлы, имеющие расширения COM и EXE.

*Файловые вирусы* могут внедряться и в другие типы файлов, но, как правило, записанные в таких файлах, они никогда не получают управление и, следовательно, теряют способность к размножению. *Загрузочные вирусы* внедряются в загрузочный сектор диска (Boot-сектор) или в сектор, содержащий программу загрузки системного диска (Master Boot Re-cord).

*Файлово-загрузочные* вирусы заражают как файлы, так и загрузочные сектора дисков.

По способу заражения вирусы делятся на резидентные и нерезидентные.

*Резидентный вирус* при заражении (инфицировании) компьютера оставляет в оперативной памяти свою резидентную часть, которая потом перехватывает обращение операционной системы к объектам заражения (файлам, загрузочным секторам дисков и т. п.) и внедряется в них. Резидентные вирусы находятся в памяти и являются активными вплоть до выключения или перезагрузки компьютера.

*Нерезидентные вирусы* не заражают память компьютера и являются активными ограниченное время.

По степени воздействия вирусы можно разделить на следующие виды:

* + *неопасные*, не мешающие работе компьютера, но уменьшающие объем свободной оперативной памяти и памяти на дисках, действия таких вирусов проявляются в каких-либо графических или звуковых эффектах
  + *опасные* вирусы, которые могут привести к различным нарушениям в работе компьютера
  + *очень опасные*, воздействие которых может привести к потере программ, уничтожению данных, стиранию информации в системных областях диска.

По особенностям алгоритма вирусы классифицируются:

*Простейшие вирусы* – паразитические, они изменяют содержимое файлов и секторов диска и могут быть достаточно легко обнаружены и уничтожены.

*Вирусы-репликаторы* (*червями*) – распространяются по компьютерным сетям, вычисляют адреса сетевых компьютеров и записывают по этим адресам свои копии.

*Вирусы-невидимки* (*стелс-вирусами*) – их трудно обнаружить и обезвредить, так как они перехватывают обращения операционной системы к пораженным файлам и секторам дисков и подставляют вместо своего тела незараженные участки диска.

*Вирусы-мутанты* – содержащие алгоритмы шифровки-расшифровки, благодаря которым копии одного и того же вируса не имеют ни одной повторяющейся цепочки байтов.

*Квазивирусы* (*"троянские"* программы) – маскируются под полезную программу, разрушают загрузочный сектор и файловую систему дисков; они не способны к самораспространению

**2. Основные виды вирусов и схемы их функционирования**

Среди всего разнообразия вирусов можно выделить следующие основные группы:

* загрузочные
* файловые
* файлово-загрузочные

Теперь поподробнее об каждой из этих групп.

**2.1 Загрузочные вирусы**

Рассмотрим схему функционирования очень простого загрузочного вируса, заражающего дискеты.

Что происходит, когда вы включаете компьютер? Первым делом управление передается программе начальной загрузки, которая хранится в постоянно запоминающем устройстве (ПЗУ). Эта программа тестирует оборудование и при успешном завершении проверок пытается найти дискету в дисководе А:.

Среди секторов есть несколько служебных, используемых операционной системой для собственных нужд (в этих секторах не могут размещаться ваши данные). Среди служебных секторов нас пока интересует один - т.н. сектор начальной загрузки (boot-sector). В секторе начальной загрузки хранится информация о дискете – количество поверхностей, количество дорожек, количество секторов и пр. Но нас сейчас интересует не эта информация, а небольшая программа начальной загрузки (ПНЗ), которая должна загрузить саму операционную систему и передать ей управление. Таким образом, нормальная схема начальной загрузки следующая: ПНЗ (ПЗУ) – ПНЗ (диск) – СИСТЕМА

Теперь рассмотрим вирус. В загрузочных вирусах выделяют две части - т.н. голову и т.н. хвост. Хвост, вообще говоря, может быть пустым. Пусть у вас имеются чистая дискета и зараженный компьютер, под которым мы понимаем компьютер с активным резидентным вирусом. Как только этот вирус обнаружит, что в дисководе появилась подходящая жертва - в нашем случае не защищенная от записи и еще не зараженная дискета, он приступает к заражению. Заражая дискету, вирус производит следующие действия:

* + выделяет некоторую область диска и помечает ее как недоступную операционной системе, это можно сделать по-разному, в простейшем и традиционном случае занятые вирусом секторы помечаются как сбойные (bad)
  + копирует в выделенную область диска свой хвост и оригинальный (здоровый) загрузочный сектор
  + замещает программу начальной загрузки в загрузочном секторе (настоящем) своей головой
  + организует цепочку передачи управления согласно схеме.

Таким образом, голова вируса теперь первой получает управление, вирус устанавливается в память и передает управление оригинальному загрузочному сектору. В цепочке ПНЗ (ПЗУ) - ПНЗ (диск) – СИСТЕМА появляется новое звено: ПНЗ (ПЗУ) - ВИРУС - ПНЗ (диск) – СИСТЕМА

Мы рассмотрели схему функционирования простого бутового вируса, живущего в загрузочных секторах дискет. Как правило, вирусы способны заражать не только загрузочные секторы дискет, но и загрузочные секторы винчестеров. При этом в отличие от дискет на винчестере имеются два типа загрузочных секторов, содержащих программы начальной загрузки, которые получают управление. При загрузке компьютера с винчестера первой берет на себя управление программа начальной загрузки в MBR (Master Boot Record - главная загрузочная запись). Если ваш жесткий диск разбит на несколько разделов, то лишь один из них помечен как загрузочный (boot). Программа начальной загрузки в MBR находит загрузочный раздел винчестера и передает управление на программу начальной загрузки этого раздела. Код последней совпадает с кодом программы начальной загрузки, содержащейся на обычных дискетах, а соответствующие загрузочные секторы отличаются только таблицами параметров. Таким образом, на винчестере имеются два объекта атаки загрузочных вирусов – программа начальной загрузки в MBR и программа начальной загрузки в бут-секторе загрузочного диска.

**2.2. Файловые вирусы**

Файловые вирусы прописывают себя внутрь полезного файла. В отличие от загрузочных вирусов, которые практически всегда резидентны, файловые вирусы совсем не обязательно резидентны. Рассмотрим схему функционирования нерезидентного файлового вируса. Пусть у нас имеется инфицированный исполняемый файл. При запуске такого файла вирус получает управление, производит некоторые действия и передает управление "хозяину".

Какие же действия выполняет вирус? Он ищет новый объект для заражения – подходящий по типу файл, который еще не заражен. Заражая файл, вирус внедряется в его код, чтобы получить управление при запуске этого файла. Кроме своей основной функции – размножения, вирус вполне может сделать что-нибудь другое – это уже зависит от фантазии автора вируса. Если файловый вирус резидентный, то он установится в память и получит возможность заражать файлы и проявлять прочие способности не только во время работы зараженного файла. Заражая исполняемый файл, вирус всегда изменяет его код – следовательно, заражение исполняемого файла всегда можно обнаружить. Но, изменяя код файла, вирус не обязательно вносит другие изменения:

* он не обязан менять длину файла
* неиспользуемые участки кода
* не обязан менять начало файла

К файловым вирусам часто относят вирусы, которые "имеют некоторое отношение к файлам", но не обязаны внедряться в их код. Рассмотрим модель, на которой ясно видна основная идея вируса. Информация о файлах хранится в каталогах. Каждая запись каталога включает в себя имя файла, дату и время создания, некоторую дополнительную информацию, номер первого кластера файла и т.н. резервные байты. При запуске исполняемых файлов система считывает из записи в каталоге первый кластер файла и далее все остальные кластеры. Вирусы семейства Dir-II производят следующую "реорганизацию" файловой системы: сам вирус записывается в некоторые свободные секторы диска, которые он помечает как сбойные. Кроме того, он сохраняет информацию о первых кластерах исполняемых файлов в резервных битах, а на место этой информации записывает ссылки на себя. Таким образом, при запуске любого файла вирус получает управление (операционная система запускает его сама), резидентно устанавливается в память и передает управление вызванному файлу.

**2.3 Загрузочно-файловые вирусы**

Примером загрузочно-файлового вируса является OneHalf. Он заражает главный загрузочный сектор (MBR) и исполняемые файлы. Основное разрушительное действие – шифрование секторов винчестера. При каждом запуске вирус шифрует очередную порцию секторов, а зашифровав половину жесткого диска, радостно сообщает об этом. Основная проблема при лечении данного вируса состоит в том, что недостаточно просто удалить вирус из MBR и файлов, надо расшифровать зашифрованную им информацию. Наиболее "смертельное" действие – просто переписать новый здоровый MBR.

**2.4 Полиморфные вирусы**

Полиморфные вирусы – вирусы, модифицирующие свой код в зараженных программах таким образом, что два экземпляра одного и того же вируса могут не совпадать ни в одном бите. Такие вирусы не только шифруют свой код, используя различные пути шифрования, но и содержат код генерации шифровщика и расшифровщика, т.е. это вирусы с самомодифицирующимися расшифровщиками. Цель такого шифрования: имея зараженный и оригинальный файлы не возможно проанализировать его код с помощью обычного дизассемблирования. Этот код зашифрован и представляет собой бессмысленный набор команд. Расшифровка производится самим вирусом уже непосредственно во время выполнения. При этом возможны варианты: он может расшифровать себя всего сразу, а может выполнить такую расшифровку "по ходу дела", может вновь шифровать уже отработавшие участки. Все это делается ради затруднения анализа кода вируса.

**3. Пути проникновения вирусов в компьютер и механизм распределения вирусных программ**

Основными путями проникновения вирусов в компьютер являются съемные диски (гибкие, флешки и лазерные), а также компьютерные сети. Заражение жесткого диска вирусами может произойти при загрузке программы с дискеты (флешки), содержащей вирус. Такое заражение может быть и случайным, На съемный диск вирус может попасть, даже если его просто вставили в зараженный компьютер

Вирус, как правило, внедряется в рабочую программу таким образом, чтобы при ее запуске управление сначала передалось ему и только после выполнения всех его команд снова вернулось к рабочей программе. Получив доступ к управлению, вирус прежде всего переписывает сам себя в другую рабочую программу и заражает ее. После запуска программы, содержащей вирус, становится возможным заражение других файлов. Наиболее часто вирусом заражаются загрузочный сектор диска и исполняемые файлы, имеющие расширения EXE, COM, SYS, BAT. Крайне редко заражаются текстовые файлы.

После заражения программы вирус может выполнить какую-нибудь диверсию, не слишком серьезную, чтобы не привлечь внимания. И наконец, не забывает возвратить управление той программе, из которой был запущен. Каждое выполнение зараженной программы переносит вирус в следующую. Таким образом, заразится все программное обеспечение.

**4. Признаки появления вирусов**

Основные признаком проявления вирусов. К ним можно отнести следующие:

* прекращение работы или неправильная работа ранее успешно функционировавших программ
* медленная работа компьютера
* невозможность загрузки операционной системы
* исчезновение файлов и каталогов или искажение их содержимого
* изменение даты и времени модификации файлов
* изменение размеров файлов
* неожиданное значительное увеличение количества файлов на диске
* существенное уменьшение размера свободной оперативной памяти
* вывод на экран непредусмотренных сообщений или изображений
* подача непредусмотренных звуковых сигналов
* частые зависания и сбои в работе компьютера

Следует отметить, что вышеперечисленные явления необязательно вызываются присутствием вируса, а могут быть следствием других причин. Поэтому всегда затруднена правильная диагностика состояния компьютера.

**5. Обнаружение вирусов и меры по защите и профилактике**

**6.1 Традиционный подход обнаружения вируса**

Итак, некий вирусописатель создает вирус и запускает его в"жизнь". Некоторое время он, возможно остается необнаруженным. Как правило, вирусы обнаруживают обычные пользователи, которые замечают те или иные аномалии в поведении компьютера. Они, в большинстве случаев, не способны самостоятельно справиться с заразой, но этого от них и не требуется.

Необходимо лишь, чтобы как можно скорее вирус попал в руки специалистов. Профессионалы будут его изучать, выяснять, "что он делает", "как он делает", "когда он делает" и пр. В процессе такой работы собирается вся необходимая информация о данном вирусе, в частности, выделяется сигнатура вируса – последовательность байтов, которая вполне определенно его характеризует. Для построения сигнатуры обычно берутся наиболее важные и характерные участки кода вируса. Одновременно становятся ясны механизмы работы вируса, например, в случае загрузочного вируса важно знать, где он прячет свой хвост, где находится оригинальный загрузочный сектор, а в случае файлового – способ заражения файла. Полученная информация позволяет выяснить:

* как обнаружить вирус, для этого уточняются методы поиска сигнатур в потенциальных объектах вирусной атаки - файлах и \ или загрузочных секторах
* как обезвредить вирус, если это возможно, разрабатываются алгоритмы удаления вирусного кода из пораженных объектов

**6.2 Программы обнаружения и защиты от вирусов**

Для обнаружения, удаления и защиты от компьютерных вирусов разработано несколько видов специальных программ, которые позволяют обнаруживать и уничтожать вирусы. Такие программы называются *антивирусными.* Различают следующие виды антивирусных программ:

* программы-детекторы
* программы-доктора или фаги
* программы-ревизоры
* программы-фильтры
* программы-вакцины или иммунизаторы.

*Программы-детекторы* осуществляют поиск характерной для конкретного вируса сигнатуры в оперативной памяти и в файлах и при обнаружении выдают соответствующее сообщение. Недостатком таких антивирусных программ является то, что они могут находить только те вирусы, которые известны разработчикам таких программ.

*Программы-доктора* или *фаги*, а также *программы-вакцины* не только находят зараженные вирусами файлы, но и "лечат" их, т.е. удаляют из файла тело программы-вируса, возвращая файлы в исходное состояние. В начале своей работы фаги ищут вирусы в оперативной памяти, уничтожая их, и только затем переходят к "лечению" файлов. Среди фагов выделяют полифаги, т.е. программы-доктора, предназначенные для поиска и уничтожения большого количества вирусов. Наиболее известные из них: Aidstest, Scan, Norton AntiVirus, Doctor Web. Учитывая, что постоянно появляются новые вирусы, программы-детекторы и программы-доктора быстро устаревают, и требуется регулярное обновление версий.

*Программы-ревизоры* относятся к самым надежным средствам защиты от вирусов. Ревизоры запоминают исходное состояние программ, каталогов и системных областей диска тогда, когда компьютер не заражен вирусом, а затем периодически или по желанию пользователя сравнивают текущее состояние с исходным. Обнаруженные изменения выводятся на экран монитора. Как правило, сравнение состояний производят сразу после загрузки операционной системы. При сравнении проверяются длина файла, код циклического контроля (контрольная сумма файла), дата и время модификации, другие параметры. Программы-ревизоры имеют достаточно развитые алгоритмы, обнаруживают стелс-вирусы и могут даже очистить изменения версии проверяемой программы от изменений, внесенных вирусом. К числу программ-ревизоров относится широко распространенная в России программа Adinf.

*Программы-фильтры* или *"сторожа"* представляют собой небольшие резидентные программы, предназначенные для обнаружения подозрительных действий при работе компьютера, характерных для вирусов. Такими действиями могут являться:

* попытки коррекции файлов с расширениями COM, EXE
* изменение атрибутов файла
* прямая запись на диск по абсолютному адресу
* запись в загрузочные сектора диска
* загрузка резидентной программы

При попытке какой-либо программы произвести указанные действия "сторож" посылает пользователю сообщение и предлагает запретить или разрешить соответствующее действие. Программы-фильтры весьма полезны, так как способны обнаружить вирус на самой ранней стадии его существования до размножения. Однако, они не "лечат" файлы и диски. Для уничтожения вирусов требуется применить другие программы, например фаги. К недостаткам программ-сторожей можно отнести их "назойливость"(например, они постоянно выдают предупреждение о любой попытке копирования исполняемого файла), а также возможные конфликты с другим программным обеспечением.

*Вакцины* или *иммунизаторы* – это резидентные программы, предотвращающие заражение файлов. Вакцины применяют, если отсутствуют программы-доктора, "лечащие" этот вирус. Вакцинация возможна только от известных вирусов. Вакцина модифицирует программу или диск таким образом, чтобы это не отражалось на их работе, а вирус будет воспринимать их зараженными и поэтому не внедрится. В настоящее время программы-вакцины имеют ограниченное применение.

Своевременное обнаружение зараженных вирусами файлов и дисков, полное уничтожение обнаруженных вирусов на каждом компьютере позволяют избежать распространения вирусной эпидемии на другие компьютеры.

**6.3 Основные меры по защите от вирусов**

Для того, чтобы не подвергнуть компьютер заражению вирусами и обеспечить надежное хранение информации на дисках, необходимо соблюдать следующие правила:

* оснастите свой компьютер современными антивирусными программами, например Aidstest, Doctor Web, и постоянно возобновляйте их версии
* перед считыванием с дискет информации, записанной на других компьютерах, всегда проверяйте эти дискеты на наличие вирусов, запуская антивирусные программы своего компьютера
* при переносе на свой компьютер файлов в архивированном виде проверяйте их сразу же после разархивации на жестком диске, ограничивая область проверки только вновь записанными файлами
* периодически проверяйте на наличие вирусов жесткие диски компьютера, запуская антивирусные программы для тестирования файлов, памяти и системных областей дисков с защищенной от записи дискеты, предварительно загрузив операционную систему с защищенной от записи системной дискеты
* всегда защищайте свои дискеты от записи при работе на других компьютерах, если на них не будет производится запись информации
* обязательно делайте архивные копии на дискетах ценной для вас информации
* не оставляйте в кармане дисковода А дискеты при включении или перезагрузке операционной системы, чтобы исключить заражение компьютера загрузочными вирусами
* используйте антивирусные программы для входного контроля всех исполняемых файлов, получаемых из компьютерных сетей
* для обеспечения большей безопасности применения Aidstest и Doctor Web необходимо сочетать с повседневным использованием ревизора диска Adinf