Файлы и Файловая система

Во всех операционных системах имеющаяся на компьютере информация хранится в виде файлов.

Файл (англ. *file* —папка) – именованная область внешней памяти.

Файл может содержать программу, числовые данные, текст, закодированное изображение и др.

Файловая система — это средство для организации хранения файлов на каком-либо носителе.

Имя файла

Полное имя файла состоит из его имени и типа (расширения), между которыми ставится точка.

Примеры:

abc.txt - текстовый файл;

стихи.doc - текстовый файл

пейзаж.bmp - рисунок;

pr.bas - программа, написанная в паскале;

Quake3.exe - исполняемый файл

mus.wav - звуковой файл

Тип файла характеризует вид информации, хранящейся в файле, назначение файла, определения программы, в которой файл создан или можно его редактировать.

Характеристики файла

- размер файла
- дата и время создания файла
- тип
- значок
- специальные атрибуты файла (только для чтения, скрытый, системный, архивированный).

Папки

Для удобства хранения и поиска файлов они объединены в папки.

Папка (каталог) – именованная часть внешней памяти, хранящая данные о файлах.

Папки могут быть вложены друг в друга, образуя многоуровневую древовидную структуру.

Логические имена устройств

Для логических имен устройств (дисководов) используются латинские буквы:

- A: - дисковод для дискет 3,5 дюйма.
- Начиная с C: (D:, E: …) - разбивается жесткий диск (винчестер) на логические блоки.
- Следующие D: (E: …) - дисководы для лазерных (CD-ROM) дисков, DVD –дисков, записывающих устройств.

Полное имя файла

Полное имя файла состоит из пути к файлу и имени файла.

Путь к файлу представляет собой перечень имен папок, которые нужно последовательно открыть, чтобы спуститься к файлу с самого высокого уровня дерева файлов.

Пример:

C: \ Program Files \ Borland \ Delphi7 \ project.exe

Операции с файлами

- Создание
- Сохранение
- Редактирование
- Переименование
- Перемещение
- Копирование
- Удаление

Компьютерные вирусы и антивирусные программы

Компьютерный вирус

- это программа, которая может копировать себя в другие программы, чтобы продолжать размножение, выполняясь вместе с ними и, возможно, совершать некоторые побочные действия от безобидных шуток до действий, ведущих к потере информации и полной остановке работы компьютера .

Компьютерный вирус – это целенаправленно созданная программа, автоматически приписывающая себя к другим программным продуктам, изменяющая или уничтожающая их.

Первая «эпидемия» компьютерного вируса произошла в 1986 году, когда вирус по имени Brain (англ. «мозг») заражал дискеты персональных компьютеров. В настоящее время известно более 50 тысяч, заражающих компьютеры и распространяющихся по компьютерным сетям.

Аналитики PC Tools уверяют, что по масштабам распространения компьютерных вирусов, вредоносного и шпионского программного обеспечения Россия давно опередила таких "гигантов" в этой области, как Китай и США. По оценкам аналитиков PC Tools - американского производителя средств защиты от нежелательного ПО – на долю РФ приходится 27,89% вредоносных программ в мире, Китая - 26,52%, США - 9,98% Россия вышла в мировые лидеры по распространению компьютерных вирусов

Признаки появления вирусов

- неправильная работа нормально работавших программ;
- медленная работа компьютера;
- невозможность загрузки ОС;
- исчезновение файлов и каталогов;
- изменение размеров файлов;
- неожиданное увеличение количества файлов на диске;
- уменьшение размеров свободной оперативной памяти;
- вывод на экран неожиданных сообщений и изображений;
- подача непредусмотренных звуковых сигналов;
- частые зависания и сбои в работе компьютера.

Авторами вирусов могут быть профессиональные программисты, студенты и даже дети школьного возраста.

Написать работающий вирус не составляет большого труда.

Сама угроза вирусов порождает многомиллиардный рынок соответствующих продуктов.

Сейчас ситуация с вирусами и антивирусами напоминает гонку вооружений недавних времен.

Почти каждый день появляются новые вирусы, а антивирусные компании выпускают дополнения к своим антивирусным базам данных.

Этому не видно конца, но пока никто не придумал ничего лучше, чем регулярное обновление антивирусного ПО.

Свойства программ-вирусов

1) способность к саморазмножению;
2) скрытность;
3) способность нести деструктивные действия.

Классификация вирусов

Вирус может внедрится в файлы трех типов:

1) командные файлы (файлы с расширением BAT);
2) загружаемые драйверы (файлы с расширением SYS или BIN);
3) выполняемые двоичные файлы (файлы с расширениями EXE, COM).

Классификация вирусов по их алгоритмам

- Вирусы-спутники
- Вирусы-черви
- Паразитические
- Студенческие
- Стелс-вирусы (вирусы-невидимки)
- Вирусы-призраки (полиморфные)

Вирусы-спутники

Это вирусы, не изменяющие файлы.

Алгоритм работы этих вирусов состоит в том, что они создают для EXE файлов файлы-спутники, имеющие такое же имя, но с расширением COM.

Вирус записывается в COM файл и никак не изменяет EXE файл.

При запуске такого файла операционная система первым обнаружит и выполнит COM файл то есть вирус, который затем запустит и EXE файл.

Вирусы-черви

Это вирусы, которые распространяются в компьютерной сети и, так же как и вирусы спутники, не изменяют файлы или сектора на дисках.

Они проникают в память компьютера из компьютерной сети, вычисляют сетевые адреса других компьютеров и рассылают по этим адресам свои копии.

Паразитические вирусы

Это все вирусы, которые при распространении своих копий обязательно изменяют содержимое дисковых секторов или файлов.

В эту группу попадают все вирусы, которые не являются червями или спутниками.

Вирусы-невидимки

Вирусы невидимки (Stealth) представляют собой весьма совершенные программы, которые перехватывают обращения операционных систем к зараженным файлам или секторам и подставляют вместо себя незараженные участки информации.

Такие вирусы, использующие приемы маскировки, нельзя увидеть средствами операционной системы.

Например, если просмотреть зараженный файл, нажав клавишу F3 в системе Norton Commander, то на экране будет показан файл, не содержащий вируса.

Это происходит потому, что вирус, активно работающий вместе с операционной системой, при открытии файла на чтение немедленно удалил свое тело из зараженного файла, а при закрытии файла заразил его опять.

Полиморфные вирусы

Полиморфные вирусы или вирусы -"призраки".

Достаточно трудно обнаруживаемые вирусы, не имеющие постоянных сигнатур (масок), т.е. не содержащие ни одного постоянного участка кода.

В большинстве случаев два образца одного и того же вируса-призрака не будут иметь ни одного совпадения.

Это достигается шифрованием основного тела вируса и модификациями программы-расшифровщика.

«Троянские кони»

«Троянские кони» — программы, предназначенные для перехвата данных на чужом компьютере или получения контроля над ним.

Троянские программы, попав на компьютер, глубоко проникают в систему, маскируются и ведут себя не совсем так, как другие типы вирусов.

Как правило, троянца сложнее обнаружить и удалить.

Виды антивирусных программ

программы – детекторы;

программы- доктора;

программы – ревизоры;

программы – фильтры;

программы - иммунизаторы

Наиболее популярными в настоящее время считаются – антивирус Касперского и Doctor Web.

ПРОГРАММЫ-ДЕТЕКТОРЫ позволяют обнаруживать файлы, зараженные одним из нескольких известных вирусов. Эти программы проверяют, имеется ли в файлах на указанном пользователем диске специфическая для данного вируса комбинация байтов. При ее обнаружении в каком-либо файле на экран выводится соответствующее сообщение. Многие детекторы имеют режимы лечения или уничтожения зараженных файлов. Программы-детекторы могут обнаруживать только те вирусы, которые ей "известны".

ПРОГРАММЫ-РЕВИЗОРЫ позволяют своевременно обнаруживать заражение компьютера практически любым их существующих сейчас вирусов, не допуская развития эпидемии, а современные действия ревизора удаляют большинство даже ранее незнакомых им вирусов

ПРОГРАММЫ-ФИЛЬТРЫ, которые располагаются резидентно в оперативной памяти компьютера и перехватывают те обращения к операционной системе, которые используются вирусами для размножения и нанесения вреда, и сообщают о них пользователя. Пользователь может разрешить или запретить выполнение соответствующей операции.

Некоторые программы-фильтры не "ловят" подозрительные действия, а проверяют вызываемые на выполнение программы на наличие вирусов. Это вызывает замедление работы компьютера.

Однако преимущества использования программ-фильтров весьма значительны — они позволяют обнаружить многие вирусы на самой ранней стадии, когда вирус еще не успел размножиться и что-либо испортить. Тем самым можно свести убытки от вируса к минимуму.

ПРОГРАММЫ-ВАКЦИНЫ, или **ИММУНИЗАТОРЫ**, модифицируют программы и диски таким образом, что это не отражается на работе программ, но тот вирус, от которого производится вакцинация, считает эти программы или диски уже зараженными. Эти программы редко используются, т.к ориентированы на конкретные вирусы.

Правила защиты от компьютерных вирусов

- Регулярно тестируйте компьютер на наличие вирусов с помощью антивирусных программ.
- Перед считыванием информации с дискет проверяйте их на наличие вирусов.
- Всегда защищайте свои дискеты и др.носителей от записи при работе на других компьютерах.
- Делайте архивные копии ценной для вас информации.
- Не оставляйте дискету в дисководе.
- Не используйте программы, поведение которых непонятно.
- Регулярно обновляйте антивирусные программы

ДЕЙСТВИЯ ПРИ ЗАРАЖЕНИИ ВИРУСОМ

При заражении компьютера вирусом (или при подозрении на это) важно соблюдать правила:

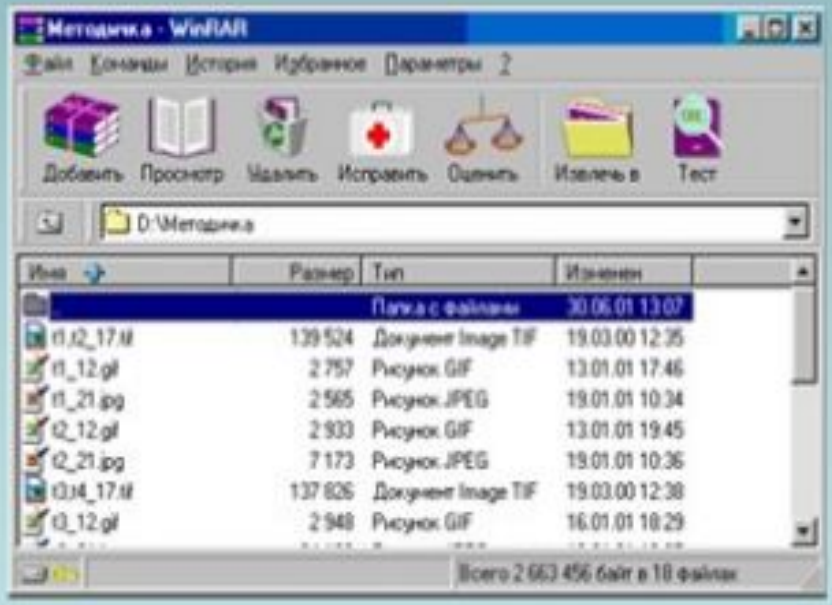
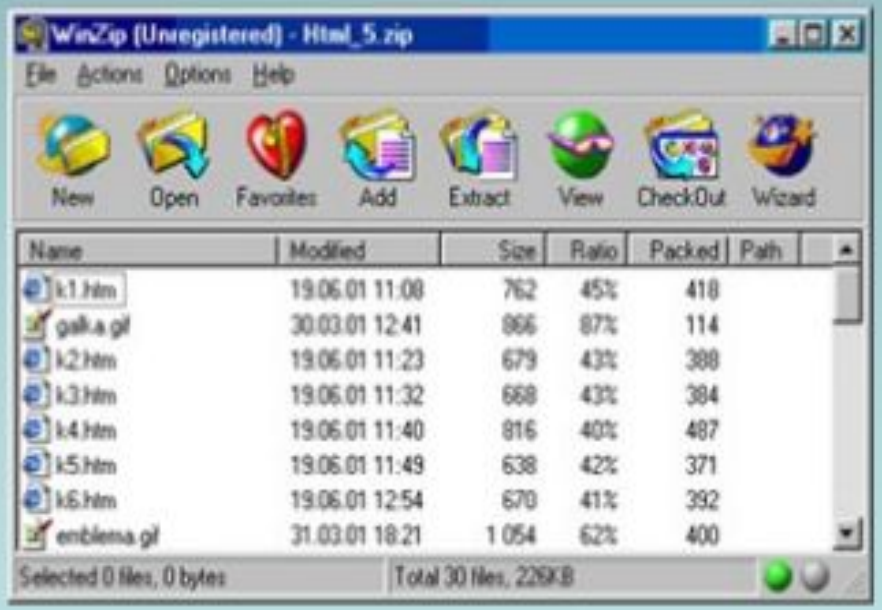
1) Прежде всего не надо торопиться и принимать опрометчивых решений. Непродуманные действия могут привести не только к потери части файлов, но к повторному заражению компьютера.

2) Надо немедленно выключить компьютер, чтобы вирус не продолжал своих разрушительных действий.

3) Все действия по обнаружению вида заражения и лечению компьютера следует выполнять при загрузке компьютера с защищенной от записи дискеты с ОС(обязательное правило).

4) Если Вы не обладаете достаточными знаниями и опытом для лечения компьютера, попросите помочь более опытных коллег.

Архиваторы

Архиватор - специальная компьютерная программа, позволяющая **архивировать** файлы сжатием хранимой в них информации.

Применяются для размещение информации на носителях внешней памяти в более компактном виде, что требует меньших объёмов памяти.