«Презентация подготовлена для конкурса «Интернешка»

«Компьютерные вирусы и антивирусные программы»

Работу выполнил:
Исмагилов Камиль, 8Б класс

Компьютерные вирусы и антивирусные программы

Борьбой с компьютерными вирусами профессионально занимаются сотни (или тысячи) специалистов в десятках компаний.

Компьютерные вирусы были и остаются одной из наиболее распространенных причин потери информации.

Феномен компьютерных вирусов

Наше столетие, несомненно, является одним из поворотных этапов в жизни человечества. Человечество захвачено техникой и уже вряд ли откажется от удобств, предоставляемых ею

(мало кто пожелает поменять

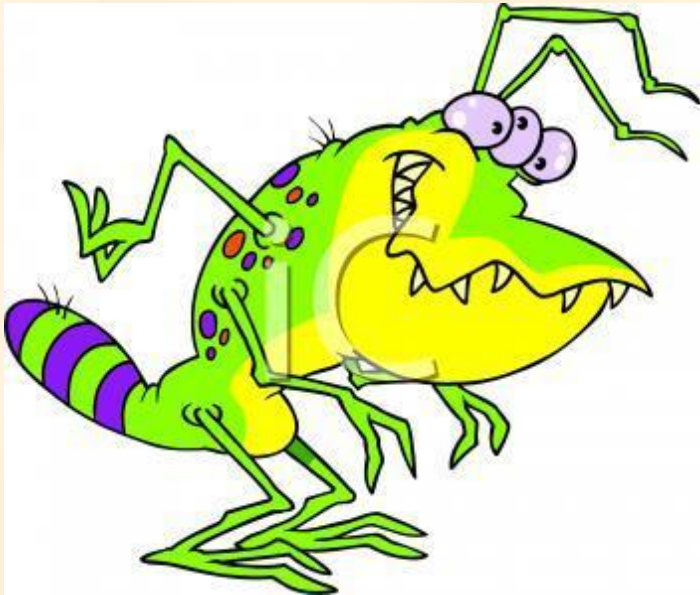
современный автомобиль на гужевую тягу).

Уже забыта обычная почта с ее конвертами и почтальонами - вместо нее пришла электронная почта.

- Сегодня факт возникновения компьютерных вирусов поставлен в один ряд с исследованиями космоса, атомного ядра и развитием электроники.

Что такое компьютерный вирус?

Объяснений, что такое компьютерный вирус, можно привести несколько.



Что такое компьютерный вирус

Объяснение бытовое

Рассмотрим работу клерка, занимающегося исключительно с бумагами (идея такого объяснения принадлежит Д.Н.Лозинскому, одному из известнейших «докторов»). Представим себе аккуратного клерка, который приходит на работу к себе в контору и каждый день обнаруживает у себя на столе стопку листов бумаги со списком заданий, которые он должен выполнить за рабочий день.

Клерк берет верхний лист, читает указания начальства, пунктуально их выполняет, выбрасывает «отработанный» лист в мусорное ведро и переходит к следующему листу.

Предположим, что некий злоумышленник тайком прокрадывается в контору и подкладывает в стопку бумаг лист, на котором написано следующее:….

Вирус «Jerusalem»

Хорошо известен вирус «Jerusalem»

(другое название - «Time»).

Кстати, на примере клерка очень хорошо видно, почему в большинстве случаев нельзя точно определить, откуда в компьютере появился вирус. Все клерки имеют одинаковые (с точностью до почерка) КОПИИ, но оригинал-то с почерком злоумышленника уже давно в корзине!

Научное определение

Первые исследования саморазмножающихся искусственных конструкций проводились в середине нынешнего столетия. В работах фон Неймана, Винера и других авторов дано определение и проведен их математический анализ.

Термин «компьютерный вирус» впервые употребил сотрудник Лехайского университета (США**) Ф.Коэн** в **1984 г.** на 7-й конференции по безопасности информации, проходившей в США.

С тех пор прошло немало времени, однако строгого определения, что же такое компьютерный вирус, так и не дано, несмотря на то, что попытки дать такое определение предпринимались неоднократно.

Компьютерные вирусы

- это класс программ способных к саморазмножению и самомодификации в работающей вычислительной среде и вызывающих нежелательные для пользователей действия.

Действия могут выражаться в нарушении работы программ, выводе на экран посторонних сообщений или изображений, порче записей, файлов, дисков, замедлении работы ЭВМ и др.

Классификация компьютерных вирусов

Вирусы можно разделить на классы по следующим основным признакам:

- среда обитания;
- операционная система (ОС);
- особенности алгоритма работы;
- деструктивные возможности.

По **СРЕДЕ ОБИТАНИЯ** вирусы можно разделить на:

- файловые;
- загрузочные;
- макро;
- сетевые.

- **Файловые вирусы** заражают выполняемые файлы (это наиболее распространенный тип вирусов), либо создают файлы-двойники (компаньон - вирусы), либо используют особенности организации файловой системы (link-вирусы).

- **Загрузочные вирусы** заражают загрузочные сектора дисков (boot-сектор), либо главную загрузочную запись (Master Boot Record), либо меняют указатель на активный boot-сектор.

- **Макро-вирусы** - разновидность файловых вирусов встраивающиеся в документы и электронные таблицы популярных редакторов.

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

Заражаемая ОПЕРАЦИОННАЯ СИСТЕМА

вернее, ОС, объекты которой подвержены заражению, является вторым уровнем деления вирусов на классы.

Каждый файловый или сетевой вирус заражает файлы какой-либо одной или нескольких OS - DOS, Windows, Win95/NT, OS/2 и т.д. Макро-вирусы заражают файлы форматов Word, Excel, Office97.

Загрузочные вирусы также ориентированы на конкретные форматы расположения системных данных в загрузочных секторах дисков.

Среди

ОСОБЕННОСТЕЙ АЛГОРИТМА РАБОТЫ

вирусов выделяются следующие пункты:

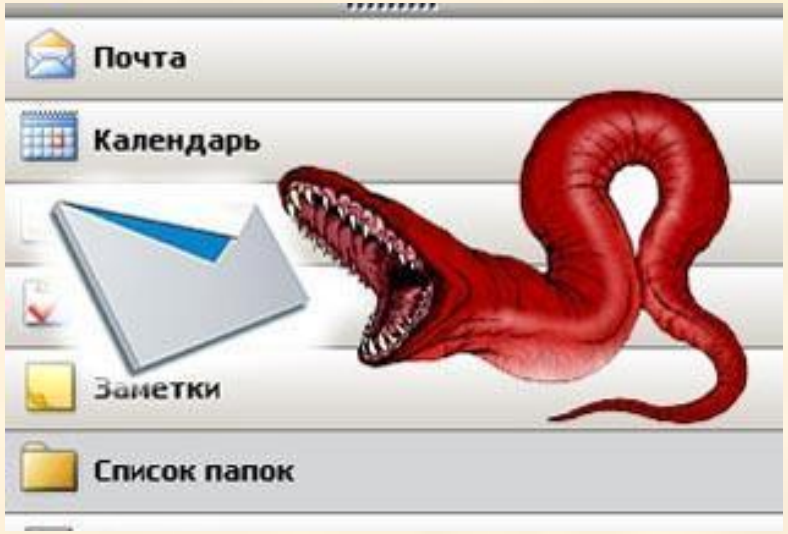
- резидентность;
- использование стелс - алгоритмов;
- самошифрование и полиморфичность;
- использование нестандартных приемов.

По ДЕСТРУКТИВНЫМ ВОЗМОЖНОСТЯМ вирусы можно разделить на

- **безвредные**, т.е. никак не влияющие на работу компьютера (кроме уменьшения свободной памяти на диске в результате своего распространения);
- **неопасные**, влияние которых ограничивается уменьшением свободной памяти на диске и графическими, звуковыми и пр. эффектами;
- **опасные вирусы**, которые могут привести к серьезным сбоям в работе компьютера;
- **очень опасные**, в алгоритм работы которых заведомо заложены процедуры, которые могут привести к потере программ, уничтожить данные, стереть необходимую для работы компьютера информацию, записанную в системных областях памяти

Защита от компьютерных вирусов

Как говорят в медицине болезнь легче предупредить, чем лечить.



Антивирусные программы

- **Антивирусные программы** предназначены для предотвращения заражения компьютера вирусом и ликвидации последствий заражения. В зависимости от назначения и принципа действия различают следующие антивирусные программы:
- **сторожа или детекторы** – предназначены для обнаружения файлов зараженных известными вирусами, или признаков указывающих на возможность заражения.
- **доктора** – предназначены для обнаружения и устранения известных им вирусов, удаляя их из тела программы и возвращая ее в исходное состояние. Наиболее известными представителями являются Dr.Web, AidsTest, Norton Anti Virus.
- **ревизоры** – они контролируют уязвимые и поэтому наиболее атакуемые компоненты компьютера, запоминают состояние служебных областей и файлов, а в случае обнаружения изменений сообщают пользователю.
- **резидентные мониторы или фильтры** – постоянно находятся в памяти компьютера для обнаружения попыток выполнить несанкционированные действия. В случае обнаружения подозрительного действия выводят запрос пользователю на подтверждение операций.
- **вакцины** – имитируют заражение файлов вирусами. Вирус будет воспринимать их зараженными и не будет внедряться.Чаще всего используются Aidstest Лозинского, Drweb, Dr.Solomon.

Полезные советы

1. Применение комплекса антивирусных программ
2. Необходимо периодическое обновление антивирусных программ
3. Проверка информации поступающей из вне.
4. Периодическая проверка всего компьютера.
5. Осторожность с незнакомыми файлами. Их действия могут не соответствовать названию.

Среди антивирусных программных продуктов можно отметить, прежде всего, пакеты:

- **Norton Antivirus (Symantec),**
- **Vims Scan (McAfee),**
- **Dr.Solomon AV Toolkit (S&S IntL),**
- **AntiVirus (IBM),**
- **InocuLAN (Computer Associates)**
- **Лаборатория Касперского.**

Спасибо за внимание