Защита информации. Компьютерные вирусы и антивирусные программы

- Компьютерный вирус – это целенаправленно созданная программа, автоматически приписывающая себя к другим программным продуктам, изменяющая или уничтожающая их.
- Компьютерным вирусом называется программа, способная выполнить на компьютере несанкционированные действия.
- Компьютерный вирус – это программный код, встроенный в другую программу, или в документ, или в определенные области носителя данных и предназначенный для несанкционированных действий на компьютере.
- Компьютерный вирус – это программа, способная создавать свои копии, внедрять их в различные объекты или ресурсы компьютерных систем и сетей и производить определенные действия без ведома пользователя.

Таким образом, вирус

1. специально созданная программа
2. самопроизвольно присоединяется к другим программам
3. создает свои копии
4. приводит к порче и потере информации

Компьютерный вирус – специально созданная компьютерная программа, способная самопроизвольно присоединяться к другим программам, создавать свои копии, внедрять их в файлы с целью нарушения работы других программ, порчи файлов и каталогов.

Компьютерные вирусы могут распространяться через

- *исполняемые файлы*
- *документы Word, Excel*
- *Web-страницы*
- *файлы из Интернета*
- *письма e-mail*
- *компакт-диски*

и flash-носители

Механизм воздействия вируса

- **При запуске инфицированной программы** или **при обращении к носителю**, имеющему **вредоносный вирусный код** в системной области, происходит **заражение**.
- При каждой загрузке инфицированной программы в оперативную память происходит **размножение**.
- Последняя фаза развития вируса – **активизация** или **вирусная атака**.

Признаки заражения. Вас должны насторожить:

- неправильная работа программ
- медленная работа компьютера
- невозможность загрузки операционной системы
- исчезновение файлов и каталогов
- изменение даты, времени создания файла или его размера
- 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

***Биологический вирус* не** может существовать вне клетки.

***Компьютерный вирус* не** может содержаться в ASCII-текстах, графических или звуковых файлах, так как он является программой и требует исполнение своего кода.

Основание классификации – *степень вредных воздействий*

группа вирусов	*характеристика вирусов*
Безвредные	Уменьшают свободную память на диске за счет своего «размножения»
Неопасные	Уменьшают свободную память на диске. Вызывают появление графических, звуковых и др. внешних эффектов
Опасные	Могут привести к сбоям и зависаниям при работе компьютера
Очень опасные	Потеря программ и данных (изменение, удаление файлов и каталогов), форматирование винчестера и т.п.

Основание классификации – *среда обитания*

группа вирусов	*характеристика вирусов*
Файловые	Внедряются в исполняемые файлы (программы) и активизируются при их запуске. Находятся в ОЗУ до выключения компьютера.
Загрузочные	Записывают себя в загрузочный сектор диска (в программу – загрузчик ОС). При загрузке ОС с зараженного диска внедряются в ОЗУ и ведут себя как файловые вирусы.
Макровирусы	Являются макрокомандами, которые заражают файлы документов Word, Excel. Находятся в ОЗУ до закрытия приложения.
Драйверные	Заражают драйверы устройств компьютера или запускают себя путем включения в файл конфигурации дополнительной строки.
Сетевые	Заражают компьютер после открытия вложенного файла (вируса) в почтовое сообщение. Похищают пароли пользователей. Рассылают себя по электронным адресам.

Основание классификации – ***особенности алгоритма***

группа вирусов	*характеристика вирусов*
компаньоны (спутники)	не изменяют файлы, а создают для исполняемых программ (.exe) одноименные командные программы (.com), которые при выполнении исходной программы запускаются первыми, а затем передают управление исходной программе
репликаторы (черви)	распространяются по компьютерным сетям, вычисляют адреса сетевых компьютеров и записывают по этим адресам свои копии, не изменяют файлы или сектора на дисках
паразиты	изменяют содержимое файлов и секторов диска, легко обнаруживаются и уничтожаются
троянские (квазивирусы)	маскируясь под полезную программу, разрушают загрузочный сектор и файловую систему дисков, передают конфиденциальную информацию, модифицируют программы систем защиты
невидимки (стелс)	перехватывают обращения операционной системы к пораженным файлам и подставляют вместо своего тела незараженные участки
мутанты (призраки)	не содержат одинаковых фрагментов, хранят свое тело в закодированном виде, постоянно меняя параметры этой кодировки

Основание классификации – способ заражения

группа вирусов	*характеристика вирусов*
резидентные	записывают в оперативную память свою часть, которая потом перехватывает обращения ОС к любым объектам, активны до выключения или перезагрузки компьютера
нерезидентные	не заражают память компьютера, активны ограниченное время, активизируются в определенные моменты

Основание классификации – целостность

группа вирусов	*характеристика вирусов*
монолитные	внедряются в программы нераздельно
распределенные	части вредоносного кода внедряются в различные места кода программ

Предотвращение разрушительных последствий, если атака произошла

- осуществлять резервное копирование особо ценной информации
- хранить дистрибутивные диски всех программ, установленных на компьютере
- не сохранять на персональном компьютере регистрационные и парольные данные для доступа в Интернет и адреса
- обязательно создать системный загрузочный диск компьютера, заранее проверить его работоспособность и хранить в надежном месте

Антивирусные программы

Наименование	Описание	Плюсы	Минусы
Полифаги	В файлах, загрузочных секторах дисков и ОП поиск известных масок вирусов (постоянной последовательности программного кода, специфичного для этого вируса) и поиск «подозрительной» последовательности команд. Могут проверять файлы в процессе их загрузки в ОП (мониторы)	Универсальность	Большие размеры используемых баз данных, невысокая скорость работы
Ревизоры	Подсчет контрольных сумм для присутствующих на диске файлов и сохранения их, длины файлов, даты последней модификации в базе данных антивируса. При запуске сверяются данные ревизора с реальными значениями	Оперативность	Не может определить вирус в новых файлах (при разархивировании, почтовых)
Блокировщики (сторожа)	Программы, перехватывающие вирусоопасные ситуации и сообщающие об этом поль зователю (например, запись в загрузочный сектор диска).	Остановка вируса на ранней стадии	Нет универсальности

Примеры антивирусных программ

- *программы-полифаги*
  - **Norton AntiVirus**
  - **DoctorWeb**
  - **Aidstest**
  - **AntiViral Toolkit Pro**
  - **Symantec**
  - **Not32**
- *программы-блокировщики (сторожа)*
  - **AntiViral Toolkit Pro Monitor**
  - **Avast**