КОМПЬЮТЕРНЫЕ ВИРУСЫ И АНТИВИРУСНЫЕ ПРОГРАММЫ

ЛЕКЦИЯ ПО ДИСЦИПЛИНЕ ИНФОРМАТИКА

Подготовили ученики группы ТАВХ-211

Зверев А.А. Бурда Д.А.

КОМПЬЮТЕРНЫЙ ВИРУС — ЭТО СПЕЦИАЛЬНО НАПИСАННАЯ НЕБОЛЬШАЯ ПО РАЗМЕРАМ ПРОГРАММА, КОТОРАЯ МОЖЕТ "ПРИПИСЫВАТЬ" СЕБЯ К ДРУГИМ ПРОГРАММАМ ДЛЯ ВЫПОЛНЕНИЯ КАКИХ-ЛИБО ВРЕДНЫХ ДЕЙСТВИЙ — ПОРТИТ ФАЙЛЫ, "ЗАСОРЯЕТ" ОПЕРАТИВНУЮ ПАМЯТЬ И Т.Д.

Существует очень много разных вирусов. Условно их можно классифицировать следующим образом:

1) загрузочные вирусы или BOOT-вирусы заражают boot-секторы дисков. Очень опасные, могут привести к полной потере всей информации, хранящейся на диске;

2) файловые вирусы заражают файлы. Делятся на:

вирусы, заражающие программы (файлы с расширением .EXE и .COM);

макровирусы вирусы, заражающие файлы данных, например, документы Word или рабочие книги Excel;

вирусы-спутники используют имена других файлов;

вирусы семейства DIR искажают системную информацию о файловых структурах;

3) загрузочно-файловые вирусы способные поражать как код boot-секторов, так и код файлов;

4) вирусы-невидимки или STEALTH-вирусы фальсифицируют информацию прочитанную из диска так, что программа, какой предназначена эта информация получает неверные данные. Эта технология, которую, иногда, так и называют Stealth-технологией, может использоваться как в BOOT-вирусах, так и в файловых вирусах;

5) ретровирусы заражают антивирусные программы, стараясь уничтожить их или сделать нетрудоспособными;

6) вирусы-черви снабжают небольшие сообщения электронной почты, так называемым заголовком, который по своей сути есть Web-адресом местонахождения самого вируса. При попытке прочитать такое сообщение вирус начинает считывать через глобальную сеть Internet свое 'тело' и после загрузки начинает деструктивное действие. Очень опасные, так как обнаружить их очень тяжело, в связи с тем, что зараженный файл фактически не содержит кода вируса.

Если не принимать меры для защиты от компьютерных вирусов, то следствия заражения могут быть очень серьезными. В ряде стран уголовное законодательство предусматривает ответственность за компьютерные преступления, в том числе за внедрение вирусов. Для защиты информации от вирусов используются общие и программные средства.

К программным средствам защиты относят разные антивирусные программы (антивирусы). Антивирус - это программа, выявляющая и обезвреживающая компьютерные вирусы. Следует заметить, что вирусы в своем развитии опережают антивирусные программы, поэтому даже в случае регулярного пользования антивирусов, нет 100% гарантии безопасности. Антивирусные программы могут выявлять и уничтожать лишь известные вирусы, при появлении нового компьютерного вируса защиты от него не существует до тех пор, пока для него не будет разработан свой антивирус. Однако, много современных антивирусных пакетов имеют в своем составе специальный программный модуль, называемый эвристическим анализатором, который способен исследовать содержимое файлов на наличие кода, характерного для компьютерных вирусов. Это дает возможность своевременно выявлять и предупреждать об опасности заражения новым вирусом.

РАЗЛИЧАЮТ ТАКИЕ ТИПЫ АНТИВИРУСНЫХ ПРОГРАММ:

- 1) программы-детекторы: предназначены для нахождения зараженных файлов одним из известных вирусов. Некоторые программы-детекторы могут также лечить файлы от вирусов или уничтожать зараженные файлы. Существуют специализированные, то есть предназначенные для борьбы с одним вирусом детекторы и полифаги, которые могут бороться с многими вирусами;
- 2) программы-лекари: предназначены для лечения зараженных дисков и программ. Лечение программы состоит в изъятии из зараженной программы тела вируса. Также могут быть как полифагами, так и специализированными;
- 3) программы-ревизоры: предназначены для выявления заражения вирусом файлов, а также нахождение поврежденных файлов. Эти программы запоминают данные о состоянии программы и системных областей дисков в нормальном состоянии (до заражения) и сравнивают эти данные в процессе работы компьютера. В случае несоответствия данных выводится сообщение о возможности заражения;
- 4) лекари-ревизоры: предназначены для выявления изменений в файлах и системных областях дисков и, в случае изменений, возвращают их в начальное состояние.
- 5) программы-фильтры: предназначены для перехвата обращений к операционной системе, которые используются вирусами для размножения и сообщают об этом пользователя. Пользователь может разрешить или запретить выполнение соответствующей операции. Такие программы являются резидентными, то есть они находятся в оперативной памяти компьютера.
- 6) программы-вакцины: используются для обработки файлов и boot-секторов с целью предупреждения заражения известными вирусами (в последнее время этот метод используется все чаще).