ТЕМА 2.2 КОМПЬЮТЕРНЫЕ ВИРУСЫ. АНТИВИРУСНЫЕ ПРОГРАММЫ

Компьютерный вирус — вид вредоносного программного обеспечения, способного создавать копии самого себя и внедряться в код других программ, системные области памяти, загрузочные секторы, а также распространять свои копии по разнообразным каналам связи с целью нарушения работы программно-аппаратных комплексов, удаления файлов, приведения в негодность структур размещения данных, блокирования работы пользователей или же приведения в негодность аппаратных комплексов компьютера.

Компьютерные вирусы принято классифицировать по следующим признакам:

1. Классификация по среде обитания.

а) Файловые вирусы являются одними из самых распространенных типов компьютерных вирусов.

Их характерной чертой является то, что они инициируются при запуске заражённой программы. Код вируса обычно содержится в исполняемом файле этой программы (файл с расширением .com, .exe или .bat), либо в динамической библиотеке (расширение .dll), используемой программой.

В настоящее время такие вирусы, как правило, представляют собой скрипты, написаны с использованием скриптового языка программирования (JavaScript, к примеру) и могут входить в состав веб-страниц.

Они внедряются в исполняемые файлы, создают дубликаты файлов или используют особенности организации файловой системы для выполнения несанкционированных действий.

б) Загрузочные вирусы записываются в загрузочный сектор диска и запускаются при запуске операционной системы, становясь ее частью.

в) Сетевые вирусы, которые ещё называют сетевыми червями, имеют своим основным местом «проживания» и функционирования локальную сеть. Сетевой вирус, попадая на компьютер пользователя, самостоятельно копирует себя и распространяется по другим компьютерам, входящим в сеть. Они используют для своего распространения электронную почту, системы обмена мгновенными сообщениями (например, ICQ), сети обмена данными, а также недостатки в конфигурации сети и ошибки в работе сетевых протоколов.

г) Макровирусы поражают документы, выполненные в некоторых прикладных программах, имеющих средства для исполнения макрокоманд. К таким документам относятся файлы, созданные с помощью пакета программ **Microsoft Office (Word, Excel, Access),** который поддерживает создание макросов на языке программирования Visual Basic for Application.

2. Классификация по области поражения.

Как правило, каждый вирус заражает файлы одной или нескольких операционных систем: DOS, Windows, Win95/NT, OS/2, Unix. Макровирусы заражают файлы форматов MS Word, MS Excel и других приложений MS Office. Многие загрузочные вирусы также ориентированы на конкретные форматы расположения системных данных в загрузочных секторах дисков.

3. Классификация по особенностям алгоритма.

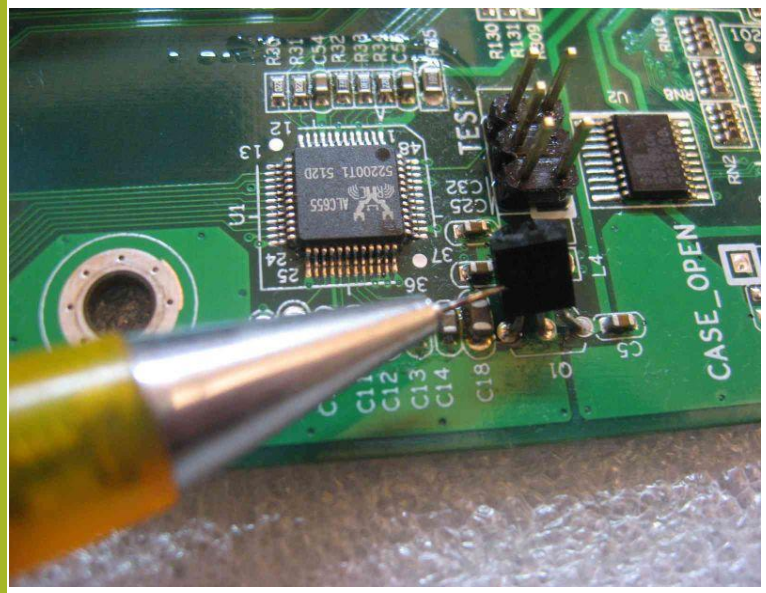
Выделяют резидентные вирусы, стелс-вирусы (steals — *англ,* невидимка), полиморфные и другие вирусы.

Резидентные вирусы способны оставлять свои копии (или части) в операционной памяти, перехватывать обработку событий (например, обращения к файлам или дискам) и вызывать при этом процедуры заражения объектов (файлов и секторов);

Нерезидентные вирусы, напротив, активны довольно непродолжительное время — только в момент запуска зараженной программы;

Стелс-алгоритмы позволяют вирусам полностью или частично скрыть свое присутствие.

Полиморфные вирусы — это трудно выявляемые вирусы, не имеющие постоянного участка кода. *Полиморфность* (самошифрование) используется для усложнения процедуры обнаружения вируса.



4. Классификация по способу заражения

Различают так называемые троянские программы, утилиты скрытого администрирования, Intended-вирусы и пр.

Троянские программы получили свое название по аналогии с троянским конем. Назначение этих программ — имитация каких-либо полезных программ, новых версий популярных утилит или дополнений к ним.

Разновидностью троянских программ являются *утилиты скрытого администрирования* (backdoor).

К *Intended -вирусам* относятся программы, которые не способны размножаться из-за существующих в них ошибок.

5. Классификация по деструктивным возможностям

- *неопасные,* влияние которых ограничивается уменьшением свободной памяти на диске, замедлением работы компьютера, графическими и звуковыми эффектами;

- *опасные,* которые потенциально могут привести к нарушениям в структуре файлов и сбоям в работе компьютера;

- *очень опасные,* в алгоритм работы которых специально заложены процедуры уничтожения данных и, согласно одной из неподтвержденных гипотез, возможность обеспечивать быстрый износ движущихся частей механизмов путем ввода в резонанс и разрушения головок записи/чтения некоторых накопителей на жестких дисках.

Контрольные вопросы:

1. Что такое фишинг?
2. Перечислите пути заражения компьютерными вирусами
3. Перечислите признаки заражения компьютера вирусами
4. Что такое антивирус? Перечислите 5-7 антивирусных программ