Компьютерные вирусы

Под **компьютерным вирусом** принято понимать программы или элементы программ, несанкционированно проникшие в компьютер с целью нанесения вреда, отличительной особенностью которых является способность само тиражирования.

Обязательным свойством компьютерного вируса является способность к размножению (самокопированию) и незаметному для пользователя внедрению в файлы, загрузочные секторы дисков и документы.

Название "вирус" по отношению к компьютерным программам пришло из биологии именно по признаку способности к саморазмножению.

Компьютерные вирусы *являются программами, которые могут "размножаться" и скрытно внедрять свои копии в файлы, загрузочные секторы дисков и документы.*

Активизация компьютерного вируса может вызывать уничтожение программ и данных.

Разнообразны последствия действия вирусов; по величине вредных воздействий вирусы можно разделить на:

- неопасные, влияние которых ограничивается уменьшением свободной памяти на диске, графическими, звуковыми и другими внешними эффектами;
- опасные, которые могут привести к сбоям и зависаниям при работе компьютера;
- очень опасные, активизация которых может привести к потере программ и данных (изменению или удалению файлов и каталогов), форматированию винчестера и так далее.

В настоящее время не существует официальной классификации вирусов, поэтому их можно разделить условно:

- компьютерные вирусы
- сетевые черви
- троянские программы
- зомби
- шпионские программы
- фишинг
- фарминг
- мобильные вирусы
- полезные вирусы
- вредоносные программы
- хакерские атаки

Червь (Worm)- это программа, которая тиражируется на жестком диске, в памяти компьютера и распространяется по сети.

Троянские программы

Троян или троянский конь (Trojans) - это программа, которая находится внутри другой, как правило, абсолютно безобидной программы, при запуске которой в систему инсталлируются программа, написанная только с одной целью - нанести ущерб целевому компьютеру путем выполнения несанкционированных пользователем действий: кражи, порчи или удаления конфиденциальных данных, нарушения работоспособности компьютера или использования его ресурсов в неблаговидных целях.

Зомби

Зомби (Zombie) - это программа-вирус, которая после проникновения в компьютер, подключенный к сети Интернет управляется извне и используется злоумышленниками для организации атак на другие компьютеры.

Шпионские программы

Шпионская программа (Spyware) - это программный продукт, установленный или проникший на компьютер без согласия его владельца, с целью получения практически полного доступа к компьютеру, сбора и отслеживания личной или конфиденциальной информации.

Одной из разновидностей шпионских программ являются фишинг рассылки:

Фишинг (Phishing) - это почтовая рассылка имеющая своей целью получение конфиденциальной финансовой информации.

Фарминг – это замаскированная форма фишинга, заключающаяся в том, что при попытке зайти на официальный сайт интернет банка или коммерческой организации, пользователь автоматически перенаправляется на ложный сайт, который очень трудно отличить от официального сайта.

Мобильные вирусы

Мобильные вирусы – это компьютерные (программные) вирусы, разработанные злоумышленниками специально для распространения через мобильные устройства, такие как смартфоны и КПК.

Чаще всего мобильные вирусы распространяются с помощью SMS и MMS сообщений, а также по каналу Bluetooth.

Вредоносные программы

Вредоносная программа (Malware)
- программное обеспечение, разработанное специально для нанесения вреда компьютеру.

Термин "вредоносная программа" является наиболее общим понятием, которое может применяться к любым вирусам, червям, троянам, шпионским программам и другим компьютерным вирусам.

По "среде обитания" вирусы можно разделить на *файловые, загрузочные, макровирусы* и *сетевые.*

Файловые вирусы

Файловые вирусы различными способами внедряются в исполнимые файлы (программы) и обычно активизируются при их запуске. После запуска зараженной программы вирус находится в оперативной памяти компьютера и является активным (то есть может заражать другие файлы) вплоть до момента выключения компьютера или перезагрузки операционной системы.

При этом файловые вирусы не могут заразить файлы данных (например, файлы, содержащие изображение или звук).

Загрузочные вирусы

Загрузочные вирусы записывают себя в загрузочный сектор диска. При загрузке операционной системы с зараженного диска вирусы внедряются в оперативную память компьютера.

В дальнейшем загрузочный вирус ведет себя так же, как файловый, то есть может заражать файлы при обращении к ним компьютера.

Макровирусы

Макровирусы заражают файлы документов Word и электронных таблиц Excel.

Макровирусы являются фактически макрокомандами (макросами), которые встраиваются в документ.

После загрузки зараженного документа в приложение макровирусы постоянно присутствуют в памяти компьютера и могут заражать другие документы. Угроза заражения прекращается только после закрытия приложения.

Сетевые вирусы

По компьютерной сети могут распространяться и заражать компьютеры любые обычные вирусы. Это может происходить, например, при получении зараженных файлов с серверов файловых архивов.

Интернет-черви (worm) - это вирусы, которые распространяются в компьютерной сети во вложенных в почтовое сообщение файлах.

Автоматическая активизация червя и заражение компьютера могут произойти при обычном просмотре сообщения. Опасность таких вирусов состоит в том, что они по определенным датам активизируются и уничтожают файлы на дисках зараженного компьютера.

Особой разновидностью вирусов являются активные элементы (программы) на языках JavaScript или VBScript, которые могут выполнять разрушительные действия, то есть являться вирусами (*скрипт-вирусами*).

Благодарю за внимание

Презентацию подготовила
преподаватель ГБОУ СПО «Баймакский
сельскохозяйственный техникум»
Мусина Ж.М.