Лекция 8. Информационная безопасность

Компьютерные вирусы - это программные продукты - коды, встроенные в другие программы, или документы, или в определенные области носителя данных и предназначены для выполнения несанкционированных действий на несущем компьютере

В зависимости от *среды обитания* вирусы можно разделить на:

- *Сетевые*
- *Файловые*
- *Загрузочные*
- *Файлово - загрузочные*

- *Сетевые вирусы* распространяются по различным компьютерным сетям.
- *Файловые вирусы* внедряются главным образом в исполняемые модули, то есть в файлы, имеющие расширение **COM и EXE.** Они могут внедряться и в другие типы файлов, но, как правило, записанные в таких файлах, они никогда не получают управление и, следовательно, теряют способность к размножению.
- *Загрузочные вирусы* внедряются в загрузочный сектор диска (Boot- сектор) или в сектор, содержащий программу загрузки системного диска (Master Boot Record).
- *Файлово – загрузочные вирусы* заражают как файлы, так и загрузочные сектора дисков.

По способу заражения вирусы делятся на:

- *Резидентные*
- *Нерезидентные.*
- *Резидентный вирус* при заражении (инфицировании) компьютера оставляет в оперативной памяти свою резидентную часть, которая потом перехватывает обращение операционной системы к объектам заражения (файлам, загрузочным секторам дисков и т.п.) и внедряется в них. Эти вирусы находятся в памяти и являются активными вплоть до выключения или перезагрузки компьютера.
- *Нерезидентные вирусы* не заражают память компьютера и являются активными ограниченное время.

По степени воздействия вирусы можно разделить на:

- *Неопасные*, не мешающие работе компьютера, но уменьшающие объем свободной оперативной памяти и памяти на дисках, действия таких вирусов проявляются в каких-либо графических или звуковых эффектах.

- *Опасные*, могут привести к различным нарушениям в работе компьютера.

- *Очень опасные,* воздействие которых может привести к потере программ, уничтожению данных, стиранию информации в системных областях диска.

По особенностям алгоритма вирусы трудно классифицировать из-за большого разнообразия.

- *Простейшие вирусы – паразитические*, они меняют содержимое файлов и секторов диска и могут быть достаточно легко обнаружены и уничтожены.

- *Вирусы- репликаторы,* называются *червями,* которые распространяются по компьютерным сетям, вычисляют адреса сетевых компьютеров и записывают по этим адресам свои копии.

- *Вирусы – невидимки*, называемые *стелс* - вирусами, которые очень трудно обнаружить и обезвредить, так как они перехватывают обращение ОС к пораженным файлам и секторам дисков и подставляют вместо своего тела незараженные участки диска.

- Наиболее трудно обнаружить *вирусы – мутанты (полиморфные* вирусы), содержащие алгоритмы шифровки-расшифровки, благодаря которым копии одного и того же вируса не имеют ни одной повторяющейся цепочки байтов.

- Имеются так называемые *квазивирусные* или *«троянские»* программы, которые хотя и не способны к самораспространению, но очень опасны, так как, маскируясь под полезные программы, разрушают загрузочный сектор и файловую систему дисков.

Основными типами компьютерных вирусов являются:

- ***1. Программные вирусы.***
- ***2. Загрузочные вирусы.***
- ***3. Макровирусы.***

- *Программные вирусы* - это блоки программного кода, целенаправленно внедренные внутрь других программ. При запуске программы, несущей вирус, происходит запуск имплантированного в нее вирусного кода. Работа его вызывает скрытые от пользователя изменения в файловой системе Жестких дисков и/или в содержании программ.
- *Программные вирусы* попадают на ПК при запуске непроверенных программ, полученных на внешнем носителе (гибкий диск или флэш-карта, или компакт-диск) или принятых из Интернета.

- *Загрузочные вирусы* - отличаются от программных - методом распространения. Они поражают не программы, а определенные системные области магнитных носителей (гибких, жестких дисков, флэш-карт). Кроме того, на включенном ПК они могут временно располагаться в ОП!!!
- *Макровирусы* – это особая разновидность вирусов поражающих документы, при формировании которых использовались прикладные программные средства, называемые макросами. (Например, документы Word с расширением .Doc). Заражение происходит при открытии документа. Антивирусные системы такие файла предлагают использовать только для чтения и отключить макросы.

Каналы распространения

- Флеш-накопители (флешки)
- Электронная почта. Обычно вирусы в письмах электронной почты маскируются под безобидные вложения: картинки, документы, музыку, ссылки на сайты.
- Системы обмена мгновенными сообщениями. Здесь также распространена рассылка ссылок на якобы фото, музыку либо программы, в действительности являющиеся вирусами, по ICQ и через другие программы мгновенного обмена сообщениями.
- Веб-страницы. Возможно также заражение через страницы Интернета ввиду наличия на страницах всемирной паутины различного «активного» содержимого: скриптов, ActiveX-компонентов.
- Интернет и локальные сети (черви). Черви – вид вирусов, которые проникают на компьютер-жертву без участия пользователя. Черви используют так называемые «дыры» (уязвимости) в программном обеспечении операционных систем, чтобы проникнуть на компьютер.

Методы защиты

Существует три *рубежа* защиты от компьютерных вирусов:

1) Предотвращение поступления вирусов.

2) Предотвращение вирусной атаки, если вирус поступил на ПК.

3) Предотвращение разрушительных последствий вирусной атаки, если она произошла.

Существует три *метода* реализации защиты:

1) Программные методы защиты.

2) Аппаратные методы защиты.

3) Организационные методы защиты.

- Основным средством защиты информации является *резервное копирование* наиболее ценной информации.

Антивирусные программы

- *программы- детекторы*, осуществляющие поиск характерной для конкретного вируса сигнатуры в оперативной памяти и в файлах и при обнаружении выдают соответствующее сообщение. Недостаток – они находят только те вирусы, которые известны разработчикам таких программ;

- *программы- доктора или фаги,* а также *программы- вакцины* не только находят зараженные вирусами файлы, но и «лечат» их, т.е. удаляют из файла тело программы-вируса, возвращая файлы в исходное состояние. В начале своей работы они ищут и уничтожают вирусы из оперативной памяти, и только потом переходят к лечению файлов. Наиболее известные из них:

Aidstest, Scan, Norton Anti Virus, Doctor Web.

- *программы-ревизоры* относятся к самым надежным средствам защиты от вирусов. Ревизоры запоминают исходное состояние программ, каталогов и системных областей диска, когда компьютер не заражен вирусом, а затем периодически или по желанию пользователя сравнивают текущее и исходное состояние.

Adinf

- *программы-фильтры или сторожа* представляют собой небольшие резидентные программы, предназначенные для обнаружения подозрительных действий при работе компьютера, характерных для вирусов.

- *вакцины – иммунизаторы* – это резидентные программы, предотвращающие заражение файлов. Вакцины применяют, если нет программы «лечащей» этот вирус. Вакцина модифицирует программу или диск таким образом, чтобы это не отражалось нм работе, а вирус воспринимал их зараженными и поэтому не внедрялся.

Почти все антивирусные программы имеют следующие подпрограммы:

- *1. Эвристический модуль* – необходимый для детектирования неизвестных вирусов.

- *2. Резидентный сторож* (называемый *монитором, резидентом*), находясь в ОП компьютера, постоянно контролирует вирусоподобные ситуации, производимые различными программами с диском и памятью.

- *3. Планировщик* – позволяет производить запуск антивирусных программ и проверку устройств хранения информации, а также осуществлять обновление вирусных баз и компонентов программы по графику, задаваемому пользователем.

- *4. Почтовая программа* – проверяет электронную почту.
- *5. Программа сканер* (*полифаг* и др.) – проверяет, обнаруживает и удаляет фиксированный набор известных вирусов в памяти, файлах и системной области дисков компьютера по заданию пользователя.
- *6. Программа – сетевой экран* – организует защиту от хакерских атак, но эту подпрограмму имеют не все антивирусные комплексы.
- *7. Программа базы данных* – по известным вирусам, которую необходимо постоянно обновлять.

Профилактика и лечение

- 1. Не работать под привилегированными учётными записями без крайней необходимости.
- 2. Не запускать незнакомые программы из сомнительных источников.
- 3. Стараться блокировать возможность несанкционированного изменения системных файлов.
- 4. Отключать потенциально опасный функционал системы (например, autorun носителей в MS Windows, сокрытие файлов, их расширений и пр.).

- 5. Не заходить на подозрительные сайты, обращать внимание на адрес в адресной строке обозревателя.
- 6. Пользоваться только доверенными дистрибутивами.
- 7. Постоянно делать резервные копии важных данных и иметь образ системы со всеми настройками для быстрого развёртывания.
- 8. Выполнять регулярные обновления часто используемых программ, особенно, обеспечивающих безопасность системы.