**Лекция 24**

Компьютерные вирусы и антивирусные средства

Компьютерный вирус – это программа, способная создавать свои копии, (не обязательно полностью совпадающие с оригиналом), внедрять их в различные объекты систем и сетей и производить определенные действия без ведома пользователя.

Программа, внутри которой находится вирус, называется зараженной или инфицированной. Когда инфицированная программа начинает работу, то сначала управление получает вирус. Вирус заражает другие программы и выполняет запланированные действия. После этого передает управление той программе, в которой он находится. В среднем в месяц появляется около 300 новых разновидностей вирусов.

**Симптомы вирусного заражения компьютера:**

1. Замедление работы некоторых программ.
2. Увеличение размеров файлов, особенно исполняемых.
3. Произвольное появление не существовавших ранее файлов.
4. Уменьшение объема доступной ОП, по сравнению с обычным режимом работы.
5. Внезапные видео и звуковые эффекты.
6. Зависание ОС.
7. Запись на диск в непредусмотренный момент времени.
8. Прекращение работы ранее нормально функционировавших программ.

Классификация вирусов

* 1. По способу заражения:

Вирусы делятся на резидентные и нерезидентные/

**Резидентные** – оставляют в ОП свою резидентную часть, которая затем перехватывает обращения неинфицированных программ к ОС и внедряется в них.

**Нерезидентные** – не заражают ОП, проявляют свою активность однократно при запуске инфицированной программы.

* 1. По особенностям алгоритма.

1**. Вирусы – компаньоны.**

Создают для файлов с расширением EXE новые зараженные файлы с тем же именем, но с расширением COM. При запуске программ ОС запускает сначала файлы с расширением COM, затем - с расширением EXE. В результате зараженный файл будет запускаться первым и заражать остальные программы.

1. **Паразитические вирусы**.

Изменяют содержимое дисковых секторов или файлов. В эту группу входят все вирусы, не являющиеся компаньонами или червями.

1. **Черви.**

Это вирусы, которые распространяются в сети, проникают в память, находят сетевые адреса и рассылают по этим адресам свои копии. Черви уменьшают пропускную способность сети, замедляют работу серверов.

Например, почтовый вирус **Melissa** стал причиной массовых сбоев в работе почтовых служб во многих странах. Этот вирус маскируется под сообщение электронной почты и при открытии пользователем посылает аналогичные сообщения по первым 50 адресам его адресной книги.

1. Вирусы типа «**троянский конь**» (**BackDoor-G).**

Маскируются под полезную программу. Выполняют разрушительную работу, например, стирают FAT таблицу.

Аналогичными вирусами являются **Armageddon, BackOrifice** и **NetBus**, они характерны тем, что представляют собой смесь вирусов и средств взлома защиты компьютерных программ.

1. **Макровирусы**.

Используют возможности макроязыков, встроенных в текстовые редакторы и электронные таблицы.

1. Вирусы, **разрушающие “компьютерное железо**”.

**CIH** или “**Чернобыль”**, срабатывающий 26 апреля (в годовщину чернобыльской катастрофы). Другая версия вируса проявляет свои разрушительные свойства по 26 числам каждого месяца. Написанный программистом с Тайваня «Чернобыль» портит данные на жестком диске и разрушает базовую систему ввода/вывода (BIOS), что делает невозможным загрузку компьютера, что в итоге приводит к необходимости замены микросхемы ПЗУ. Переносчиком вируса является CD-ROM с пиратским ПО.

В июне этого года появился созданный в Израиле вирус **Worm.ExploreZip**, сочетающий плодовитость «червя» **Melissa** с разрушительной силой «**Чернобыля**». Этот вирус также распространяется по электронной почте, но приходит в ответ на реальные сообщения, поэтому не вызывает у пользователя особых подозрений. Вирусное послание содержит файлы, упакованные программой-архиватором ZIP. При попытке разархивирования вирус выдает сообщение об ошибке и заражает компьютер, после чего стирает с жесткого диска все данные.

Антивирусные программы

Эти программы могут обнаруживать только те вирусы, сигнатуры (портреты) которых им известны - помещены в библиотеку программы.

Антивирусные программы подразделяются на:

* сканеры;
* программы – доктора;
* ревизоры;
* фильтры;
* иммунизаторы.

**Сканеры** сканируют ОП, диски, выполняя поиск зараженных файлов.

**Программы – доктора** не только находят зараженные файлы, но и лечат, удаляя из файла тело программы – вируса.

Наиболее известные программы – доктора:

AVP – автор Касперский.

AidTest – автор Лозинский.

DoctorWeb – автор Данилов и др.

AntiVirXP

ADinf – автор Мостовой. Программа не использует сигнатуры вирусов, поэтому эффективна против новых вирусов..

**Ревизоры** – программы, которые анализируют текущее состояние файлов и системных областей диска, а также сравнивают его с информацией, сохраненной ранее в одном из файлов ревизора. При этом проверяется состояние FAT таблицы, длина файлов, время создания, атрибуты, контрольные суммы.

Фильтры – это резидентные программы (сторожа), которые оповещают пользователя обо всех попытках какой-либо программы выполнить подозрительные действия. Фильтры контролируют:

* обновление программных файлов и системной области диска;
* форматирование диска;
* резидентное размещение программ в ОП.

Программы – фильтры должны быть установлены при работе в сети Интернет.

Пример: программа VSafe.

**Рекомендации.**

1. Перед считывание с носителей информации проверять носитель на вирусы.
2. Проверять файлы сразу после разархивации.
3. Не оставлять носители в разъемах при включении и перезагрузки ПК, т.к. это может привести к заражению загрузочными вирусами.
4. Получив электронное письмо, к которому приложен исполняемый файл, не запускать этот файл без предварительной проверки.
5. При установке большого программного продукта проверить все дистрибутивные файлы, а после инсталляции повторно произвести проверку на вирус.
6. Обновлять базы антивирусных программ.