**Лекция № 6. Защита информации, антивирусная защита.**

**Вирусы. Антивирусное программное обеспечение**

**Компьютерный вирус** - программа способная самопроизвольно внедряться и внедрять свои копии в другие программы, файлы, системные области компьютера и в вычислительные сети, с целью создания всевозможных помех работе на компьютере.

Все действия вируса могут выполняться достаточно быстро и без выдачи каких- либо сообщений, поэтому пользователю очень трудно заметить, что в компьютере происходит что-то необычное.

Признаки заражения:

* прекращение работы или неправильная работа ранее функционировавших программ
* медленная работа компьютера
* невозможность загрузки ОС
* исчезновение файлов и каталогов или искажение их содержимого
* изменение размеров файлов и их времени модификации
* уменьшение размера оперативной памяти
* непредусмотренные сообщения, изображения и звуковые сигналы
* частые сбои и зависания компьютера и др.

Некоторые виды вирусов вначале незаметно заражают большое число программ или дисков, а потом причиняют очень серьезные повреждения, например, форматируют весь жесткий диск на компьютере. Другие вирусы стараются вести себя как можно более незаметно, но понемногу и постепенно портят данные на жестком диске.

Таким образом, если не предпринимать мер по защите от вируса, то последствия заражения компьютера могут быть очень серьезными.

**Классификация компьютерных вирусов**

По среде обитания:

* Сетевые – распространяются по различным компьютерным сетям
* Файловые – внедряются в исполняемые модули (COM, EXE)
* Загрузочные – внедряются в загрузочные сектора диска или сектора, содержащие программу загрузки диска
* Фалово-загрузочные – внедряются и в загрузочные сектора и в исполняемые модули

По способу заражения:

* Резидентные – при заражении оставляет в оперативной памяти компьютера свою резидентную часть, которая потом перехватывает обращения ОС к объектам заражения
* Нерезидентные – не заражают оперативную память и активны ограниченное время

По воздействию:

* Неопасные – не мешают работе компьютера, но уменьшают объем свободной оперативной памяти и памяти на дисках
* Опасные – приводят к различным нарушениям в работе компьютера
* Очень опасные – могут приводить к потере программ, данных, стиранию информации в системных областях дисков

По особенностям алгоритма:

* Паразиты – изменяют содержимое файлов и секторов, легко обнаруживаются
* Черви – вычисляют адреса сетевых компьютеров и отправляют по ним свои копии
* Стелсы – перехватывают обращение ОС к пораженным файлам и секторам и подставляют вместо них чистые области
* Мутанты – содержат алгоритм шифровки-дешифровки, ни одна из копий не похожа на другую
* Трояны – не способны к самораспространению, но маскируясь под полезную, разрушают загрузочный сектор и файловую систему

**Основные меры по защите от вирусов**

* оснастите свой компьютер одной из современных антивирусных программ: Doctor Weber, Norton Antivirus, AVP
* постоянно обновляйте антивирусные базы
* делайте архивные копии ценной для Вас информации (гибкие диски, CD)

# Методы защиты от компьютерных вирусов

Каким бы не был вирус, пользователю необходимо знать основные методы защиты от компьютерных вирусов.

Для защиты от вирусов можно использовать:

* + общие средства защиты информации, которые полезны также и как страховка от физической порчи дисков, неправильно работающих программ или ошибочных действий пользователя;
  + профилактические меры, позволяющие уменьшить вероятность заражения вирусом;
  + специализированные программы для защиты от вирусов.
  + Общие средства защиты информации полезны не только для защиты от вирусов.
* Имеются две основные разновидности этих средств:
  + копирование информации - создание копий файлов и системных областей дисков;
  + разграничение доступа предотвращает несанкционированное использование информации, в частности, защиту от изменений программ и данных вирусами, неправильно работающими программами и ошибочными действиями пользователей.

Несмотря на то, что общие средства защиты информации очень важны для защиты от вирусов, все же их недостаточно. Необходимо и применение специализированных программ для защиты от вирусов. Эти программы можно разделить на несколько видов: детекторы, доктора (фаги), ревизоры, доктора-ревизоры, фильтры и вакцины (иммунизаторы).

**Классификация антивирусного программного обеспечения**

Для обнаружения, удаления и защиты от компьютерных вирусов разработаны специальные антивирусные программы. Различают следующие **виды антивирусных программ**:

* **Программы-детекторы**осуществляют поиск характерной для конкретного вируса сигнатуры в оперативной памяти и в файлах и при обнаружении выдают соответствующее сообщение. Недостатки: могут находить только те вирусы, которые известны разработчикам этой программы, поэтому быстро устаревают и требуют регулярного обновления.
* **Программы-доктора**или**фаги** не только находят зараженные вирусами файлы, но и «лечат» их, т.е. удаляют из файла тело программы-вируса, возвращая файл в исходное состояние. **Полифаги** – программы-доктора, предназначенные для поиска и уничтожения большого количества вирусов. Недостатки те же, что и у программ-детекторов.
* **Программы-ревизоры**относятся к самым надежным средствам защиты. Ревизоры запоминают исходное состояние программ, каталогов и системных областей диска тогда, когда компьютер не заражен вирусом, а затем периодически или по желанию пользователя сравнивают текущее состояние с исходным. Обнаруженные изменения выводятся на экран монитора.
* **Программы-фильтры**или**«сторожа»**представляют собой небольшие резидентные программы, предназначенные для обнаружения подозрительных действий при работе компьютера, характерных для вирусов (попытки коррекции файлов с расширением EXE или COM, изменение атрибутов файла, запись в загрузочные сектора и т.п.). При попытке какой-либо программы произвести указанные действия «сторож» посылает пользователю сообщение и предлагает запретить или разрешить соответствующее действие. Эти программы способны обнаружить вирус на самой ранней стадии его существования до размножения. Однако они не лечат файла и диски. Для уничтожения вируса требуется применить другие программы.
* **Вакцины**или **иммунизаторы** это резидентные программы, предотвращающие заражение файлов. Вакцины применяют, если отсутствуют программы-доктора, лечащие этот вирус. Вакцинация возможна только от известных вирусов. Вакцина модифицирует программу или диск таким образом, чтобы это не отражалось на их работе, а вирус будет воспринимать их зараженными и поэтому не внедрится. Имеют ограниченное применение.