Тема:

«Структура антивирусов»

1. Особенности антивирусов.
2. Классификация антивирусных комплексов

1. Особенности антивирусов.

- Для обнаружения вирусов антивирусные программы используют два метода – сигнатурный и эвристический.
- **Сигнатурный метод** основан на сравнении подозрительного файла с сигнатурами известных вирусов. Сигнатура – это некий образец известного вируса, то есть набор характеристик, позволяющих идентифицирс и наличие вируса в файл

- **Эвристический метод** представляет собой совокупность приблизительных методов обнаружения вирусов, основанных на тех или иных предположениях. Выделяют следующие эвристические методы:

1. **поиск вирусов, похожих на известные** (часто именно этот метод называют эвристическим). Метод похож на сигнатурный, только сигнатурный требует точного совпадения; а здесь же файл исследуется на наличие модификаций известных сигнатур, то есть не обязательно полное совпадение. Это помогает обнаруживать гибриды вирусов и модификации уже известных вирусов;

2. аномальный метод (поведенческий анализ) – метод основан на отслеживании аномальных событий в системе и выделении основных вредоносных действий: удаления, запись в определенные области реестра, рассылка писем и пр. Данный метод не обладает вирусной базой и неспособен различать известные / неизвестные вирусы - все подозрительные программы считаются неизвестными вирусами и не пр
лечения.

3. анализ контрольных сумм (ревизор) - это способ отслеживания изменений в объектах компьютерной системы. Сегодня ревизоры изменений утратили свои позиции и используются в антивирусах достаточно редко. Чаще подобные технологии применяются в сканерах при доступе - при первой проверке с файла снимается контрольная сумма и помещается в кэше, перед следующей проверкой того же файла сумма снимается еще раз, сравнивается, и в случае отсутствия изменений файл считается незараженным.

- В состав антивируса входят следующие модули:

1. **<u>модуль обновления</u>** – доставляет обновленные базы сигнатур пользователю антивируса. Модуль обновления обращается к серверам производителя и скачивает обновленные антивирусные базы.
2. **<u>модуль планирования</u>** – предназначен для планирования действий, которые регулярно должен выполнять антивирус. Например, проверять компьютер на наличие вирусов и обновлять антивирусные базы. Пользователь может выбрать расписание выполнения данных действий.

3. модуль управления – предназначен для администраторов крупных сетей, позволяющий удаленно настраивать антивирусы на узлах сети, а также способы ограничения доступа локальных пользователей к настройкам антивируса.

4. модуль карантина – предназначен для изолирования подозрительных файлов в специальное место – карантин. В этих случаях файл помещается в карантин и не может выполнять какие-либо действия оттуда.

2. Классификация антивирусных комплексов.

НА ДОМ!!!