1. Вирус находит и заражает другие программы, а также выполняет какие-нибудь вредные действия (например, портит файлы или таблицу размещения файлов на диске, засоряет оперативную память и т.д.).
2. Предотвращают своё обнаружение тем, перехватывают обращения операционной системы (и тем самым прикладных программ) к заражённым файлам и областям диска и выдают их в исходном (незаражённом) виде.
3. Самомодифицирующиеся вирусы (мутанты) изменяют свое тело таким образом, чтобы антивирусная программа не смогла его идентифицировать.
4. 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
5. Специализированные программы защиты от компьютерных вирусов применяются для профилактики , при подозрительном поведении компьютера , долгой загрузки, зависании.
6. Антивирусные программы делятся на: программы-детекторы, программы - доктора, программы-ревизоры, программы-фильтры, программы-вакцины.
7. Программы-детекторы обеспечивают поиск и обнаружение вирусов в оперативной памяти и на внешних носителях.
8. Сигнатура вируса - это уникальная последовательность байтов, принадлежащая вирусу и не встречающаяся в других программах.
9. Зараженная программа будет распознана в случае, если данный вирус входит в актуальную базу антивирусника.
10. Программы -ревизоры -принцип их работы состоит в подсчете контрольных сумм для присутствующих на диске файлов/системных секторов. Программы-вакцины (или иммунизаторы) - резидентные программы, предотвращающие заражение файлов, путем модификации програм.
11. Многоуровневая защита подразумевает использование всех видов антивирусных программ, а так же средств профилактики, таких как резервное копирование.
12. Основными мерами защиты от вирусов считаются: резервирование (копирование, ежедневное ведение архивов измененных файлов); профилактика (раздельное хранение вновь полученных программ и эксплуатирующихся, хранение неиспользуемых программ в архивах, использование специального диска для записи новых программ).
13. Существует четыре основных типа антивирусных программ: сканеры, программы контроля целостности данных, мониторы и гибридные антивирусные средства. Алгоритм работы антивирусного сканера заключается в обнаружении вирусов на базе сигнатур, хранящихся в БД сканера.