**Тема 3-4 Современные компьютерные угрозы и методы борьбы с ними**

1. Вирусы заражают компьютеры и переносные носители.
2. Антивирусы перехватывают обращения системы к заражённым файлам и выдают их за чистые.
3. Самомодифицирующиеся вирусы способны менять параметры своей кодировки, что значительно затрудняет определение механизмов их работы.
4. Использовать программы-детекторы, программы-фильтры, программы-вакцины, программы-ревизоры, антивирусы, блокировка всплывающих окон браузеров и писем не известных отправителей, мониторинг целостности файлов и, чтобы наверняка, перейти на Linux
5. Для полноценной защиты данными программами следует пользоваться на постоянной основе.
6. Программы-детекторы, программы-фильтры, программы-вакцины, программы-ревизоры, антивирусы.
7. Проверяют файлы на наличие сигнатур.
8. Специфических для вируса комбинация байтов.
9. Нет, она обнаруживает вирусы только с уже знакомой сигнатурой

* Программа-ревизор сканируют и запоминают исходное состояние файлов и, при повторном сканировании, обнаруживают угрозу.
* Программы-вакцины заставляют верить вирус в то, что вакцинированная программа уже заражена.
* Программы-фильтры мониторят происходящие в системе действия и перемещения файлов, что позволяет отслеживать вирусы.

1. На переднем плане работают программы-детекторы, за ними программы-фильтры, программы-ревизоры, программы-доктора и последняя линия обороны – разграничение доступа.

* Архивирование данных
* Систематические проверки
* Использование лицензионного ПО
* Не пользоваться не проверенными переносными накопителями
* Контроль файлов, получаемых из сети
* Сканеры, работающие в реальном времени
* Фильтры сетевого потока с отображением подробных данных
* Программы-ревизоры, регулярно проверяющих файлы системы