**Контрольные вопросы:**

* Что могут заразить вирусы?

Вирусы могут заразить устройства, такие как компьютер, сервер, смартфон и тп. По сути, вирус - это вредоносное по, которое выполняет какие-либо действия на вашем пк, либо мешает правильному функционированию зараженного устройства

* Как маскируются «невидимые» вирусы?

STEALTH - вирусы

Авторы вирусов заменяют некоторые компоненты операционной системы, например, прерывания, драйверы так, что программа-вирус становится невидимой для других программ. Такие вирусы называются вирусами-невидимками, или стелс-вирусами (Stealth - невидимка ).

Stealth-вирусы всегда резидентны. Резидентный модуль перехватывает обращение операционной системы к пораженным файлам или секторам дисков и “подставляет” вместо них исходные объекты. Так Stealth-вирусы скрываются от опытного пользователя и многих антивирусных средств, которые осуществляют ранний поиск вирусов по изменениям длин файлов контрольных сумм и содержимого загрузочных секторов. Необходимо заметить, что Stealth-вирус невидим только тогда, когда его резидентный модуль находится в оперативной памяти компьютера.

* 3. Каковы особенности самомодифицирующихся вирусов?

САМОМОДИФИЦИРУЮЩИЕСЯ вирусы. Другой способ, применяемый вирусами для

того, чтобы укрыться от обнаружения, - модификация своего тела. Многие

вирусы хранят большую часть своего тела в закодированном виде, чтобы с

помощью дизассемблеров нельзя было разобраться в механизме их работы.

Самомодифицирующиеся вирусы используют этот прием и часто меняют параметры

этой кодировки, а кроме того, изменяют и свою стартовую часть, которая

служит для раскодировки остальных команд вируса. Таким образом, в теле

подобного вируса не имеется ни одной постоянной цепочки байтов, по которой

можно было бы идентифицировать вирус. Это, естественно, затрудняет

нахождение таких вирусов программами-детекторами.

* 4. Какие методы защиты от компьютерных вирусов можно использовать?

1) Скачивать лицензионные программы, и посещать проверенные ссылки. 2) использовать несколько различных антивирусов., с разными базами.

обновлять свои программы и ПО до последних версий

* 5. В каких случаях применяют специализированные программы защиты от компьютерных вирусов?

антивирусы применяют тогда, когда необходимо восстановить поврежденные вирусами данные, когда не известен тип вируса, и момент заражения. для профилактики системы.

* 6. На какие виды можно подразделить программы защиты от компьютерных вирусов?

Во-первых, антивирусы можно подразделить на две категории:

программы, которые непрерывно сканируют потоки данных, например, интернет-трафика, принудительно запускаемые программы с целью сканирования определенных, указанных объектов. Во-вторых, антивирусные программы различаются по виду (способу) защиты от вирусов. Тут можно выделить следующие: Программы-детекторы, или сканеры, находят вирусы в оперативной памяти и на внешних носителях, выводя сообщение при обнаружении вируса. Программы-доктора, (фаги, программы-вакцины) находят зараженные файлы и "лечат" их. Среди этого вида программ существуют полифаги, которые способны удалять разнообразные виды вирусов, самые известные из антивирусов-полифагов Norton AntiVirus, Doctor Web, Kaspersky Antivirus. Программы-ревизоры являются наиболее надежными в плане защиты от вирусов. Ревизоры запоминают исходное состояние программ, каталогов, системных областей диска до момента инфицирования компьютера, затем сравнивают текущее состояние с первоначальным, выводя найденные изменения на дисплей. Программы-мониторы (файерволы, брандмауэры) начинают свою работу при запуске операционной системы, постоянно находятся в памяти компьютера и осуществляют автоматическую проверку файлов по принципу "здесь и сейчас". Программы-фильтры (сторожа) обнаруживают вирус на ранней стадии, пока он не начал размножаться. Программы-сторожа - небольшие резидентные программы, целью которых является обнаружение действий, характерных для вирусов.

* 7. Как действуют программы-детекторы?

Программы-детекторы, или сканеры, находят вирусы в оперативной памяти и на внешних носителях, выводя сообщение при обнаружении вируса.

* 8. Что называется сигнатурой?

Сигнатура функции — характеристическая часть определения функции в программировании. Сигнатура атаки — характеристические особенности компьютерного вируса. Сигнатура файла — набор байтов, обеспечивающий идентификацию типа файла.

* 9. Всегда ли детектор распознает зараженную программу?

Универсальные детекторы в своей работе используют проверку неизменности файлов путем подсчета и сравнения с эталоном контрольной суммы. Недостаток универсальных детекторов связан с невозможностью определения причин искажения файлов.

Специализированные детекторы выполняют поиск известных вирусов по их сигнатуре (повторяющемуся участку кода). Недостаток таких детекторов состоит в том, что они неспособны обнаруживать все известные вирусы.

Детектор, позволяющий обнаруживать несколько вирусов, называют полидетектором.

Недостатком таких антивирусных про грамм является то, что они могут находить только те вирусы, которые известны разработчикам таких программ.

* 10. Каков принцип действия программ-ревизоров, программ-фильтров, программ-вакцин?

Программы-доктора (фаги), не только находят зараженные вирусами файлы, но и "лечат" их, т.е. удаляют из файла тело программы вируса, возвращая файлы в исходное состояние. В начале своей работы фаги ищут вирусы в оперативной памяти, уничтожая их, и только затем переходят к "лечению" файлов. Среди фагов выделяют полифаги, т.е. программы-доктора, предназначенные для поиска и уничтожения большого количества вирусов.

Программы-ревизоры относятся к самым надежным средствам защиты от вирусов. 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 видеомонитора. Как правило, сравнение состояний производят сразу после загрузки операционной системы. При сравнении проверяются длина файла, код циклического контроля (контрольная сумма файла), дата и время модификации, другие параметры.

Программы-фильтры (сторожа) представляют собой небольшие резидентные программы, предназначенные для обнаружения подозрительных действий при работе компьютера, характерных для вирусов. Такими действиями могут являться:

Попытки коррекции файлов с расширениями СОМ и ЕХЕ;

Изменение атрибутов файлов;

Прямая запись на диск по абсолютному адресу;

При попытке какой-либо программы произвести указанные действия "сторож" посылает пользователю сообщение н предлагает запретить или разрешить соответствующее действие. Программы-фильтры весьма полезны, так как способны обнаружить вирус на самой ранней стадии его существования до размножения.

* 11.Как выглядит многоуровневая защита от компьютерных вирусов с помощью антивирусных программ?

сочетает в себе различные типы защитных программ

* 12. Перечислите меры защиты информации от компьютерных вирусов.

1.Оснащение ЭВМ современными антивирусными программами и регулярное обновление их версий.

2.Установка программы-фильтра при работе в глобальной сети.

3.Проверка накопителей на наличие вирусов перед считыванием с них информации, записанной на других ЭВМ.

4.При переносе на свой ПК файлов в архивированном виде проверка их сразу после разархивации.

5.Защита своих дисков от записи при работе на других ПК.

6.Создание архивных копий ценной информации на других носителях информации.

7.При установке большого программного продукта проверка всех дистрибутивных файлов, а после инсталляции продукта повторный контроль наличия вирусов.