Контрольные вопросы 3-4

1.Что могут заразить вирусы?

Есть несколько разновидностей распространения компьютерных вирусов.К ним относятся: письма со спамом ,вредоносные office макрос ,зараженные съемные носители ,вместе с по и многие другие способы.

По способу воздействия (особенностям алгоритма) вирусы отличаются большим разнообразием. Известны вирусы-паразиты, вирусы-черви, вирусы-невидимки (стелс-вирусы), вирусы-призраки (вирусы-мутанты), компаньон-вирусы, троянские кони и др.

Чаще всего встречаются вирусы, заражающие исполнимые файлы. Некоторые вирусы заражают и файлы, и загрузочные области дисков.

2. Как маскируются «невидимые» вирусы?

"Невидимые" вирусы. Многие резидентные вирусы предотвращают свое обнаружение тем, что перехватывают обращения операционной системы к зараженным файлам и областям диска и выдают их в исходном виде. Разумеется, этот эффект наблюдается только на зараженном компьютере - на "чистом" компьютере изменения в файлах и загрузочных областях диска можно легко обнаружить.

3. Каковы особенности самомодифицирующихся вирусов?

Самомодифицирующиеся вирусы применяют модификацию 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. Регулярное архивирование информации
2. Использование только лицензионных дистрибутивных копий программных продуктов.
3. Систематическая проверка компьютера на наличие вирусов. Компьютер должен быть оснащен эффективным регулярно используемым и постоянно обновляемым пакетом антивирусных программ. Для обеспечения большей безопасности следует применять параллельно несколько антивирусных программ.
4. Осуществление входного контроля нового программного обеспечения, поступивших дискет. При переносе на компьютер файлов в архивированном виде после распаковки их также необходимо проверять.
5. При работе на других компьютерах всегда нужно защищать свои дискеты от записи в тех случаях, когда на них не планируется запись информации.
6. При поиске вирусов следует использовать заведомо чистую операционную систему, загруженную с дискеты.
7. При работе в сети необходимо использовать антивирусные программы для входного контроля всех файлов, получаемых из компьютерных сетей. Никогда не следует запускать непроверенные файлы, полученные по компьютерным сетям.

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

В случае угрозы компьютера и его данных.

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

Программы-детекторы, программы-ревизоры, программы фильтры, программы-доктора и доктора-ревизоры.

7.Как действуют программы-детекторы?

Программы-детекторы позволяют обнаруживать файлы, зараженные одним из нескольких известных вирусов. Эти программы проверяют, имеется ли в файлах на указанном пользователем диске специфическая для данного вируса комбинация байтов. Такая комбинация называется сигнатурой. При ее обнаружении в каком-либо файле на экран выводится соответствующее сообщение. Многие детекторы имеют режимы лечения или уничтожения зараженных файлов. Следует подчеркнуть, что программы-детекторы могут обнаруживать только те вирусы, которые ей "известны".

8.Что называется сигнатурой?

Программы которые обнаруживают файлы зараженным одним из известных файлов, затем проверяют, имеется ли в файлах на указанном пользователем диске специфическая для данного вируса комбинация байтов.

9.Всегда ли детектор распознает зараженную программу?

Нет, программа способна распознавать вирусы которые ей известны. В случае заражения файлом нового или видоизмененного вируса , то файл будет определен как «чистый»

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

Программы-ревизоры имеют две стадии работы. Сначала они запоминают сведения о состоянии программ и системных областей дисков.Далее они сравнивают полученные сведения с исходными и сообщают о не соответствиях. Программы-фильтры, которые располагаются в оперативной памяти компьютера и перехватывают те обращения к операционной системе, которые используются вирусами для размножения и нанесения вреда, и сообщают о них пользователю. Программы-вакцины деформируют программы и диски таким образом, что это не отражается на работе программ, но тот вирус, от которого производится вакцинация, считает эти программы или диски уже зараженными.

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

Уровни защиты включают в себя 4 пункта:

1.Внимательность и информирование пользователей о возможных нарушениях и опасностей.

2.Защита компьютера, данный пункт подразумевает собой использование антивирусных программ.

3.Предварительные меры, такие как обработка конфиденциальной информации и надежное хранение полученной информации.

12. Перечислите меры защиты информации от компьютерных вирусов.

1)копирование информации - создание копий файлов и системных областей дисков;

2)разграничение доступа предотвращает несанкционированное использование информации, в частности, защиту от изменений программ и данных вирусами, неправильно работающими программами и ошибочными действиями пользователей.

13. Каковы современные технологии антивирусной защиты?

Современные технологии антивирусной защиты позволяют защитить от вируса файловые сервера, почтовые сервера и сервера приложений. Например, антивирус Касперского для защиты файловых серверов позволяет обнаружить и нейтрализовать все типы вредоносных программ на файловых серверах и серверах приложений, работающих под управлением ОС Solaris, включая "троянские" программы, Java и ActiveX – апплеты.