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

**Цель:** Изучить существующие компьютерные угрозы и основные методы противодействия угрозам

**Вопросы практического занятия:**

*Компьютерные вирусы. Классификация компьютерных вирусов. Методы построения и внедрения шпионов. Профилактика и лечение информационных инфекций. Программы обнаружения и защиты от вирусов и вредоносные программные средства. Устройство, принципы внедрения и действий компьютерных вирусов и вредоносных программных средств.*

**Задания практического занятия:**

1 Подготовьте конспект по вопросам практического занятия

2 Ответьте на контрольные вопросы. Обоснуйте свои ответы.

3 Дискуссия на темы(устный доклад):

5.1 Типы шпионов. Отличие от «классических» вирусов.

5.2 Жизненный цикл шпиона.

5.3 Методы построения и внедрения шпионов.

5.4 Обзор некоторых представителей шпионского ПО.

5.5 Методы борьбы со шпионами. Пример anti spyware.

**Контрольные вопросы:**

1. Что могут заразить вирусы?

**Программы, сайт, файл, системный файл, драйвера**

1. Как маскируются «невидимые» вирусы?

**Предотаращают свое обнаружение, тем, что перехватывают обращения операционной системы к зараженным файлам и областям диска и выдают их в исходном виде.**

1. Каковы особенности самомодифицирующихся вирусов?

**Кодируют большую часть своего тела, чтобы нельзя было разобраться в механизме их работы**

1. Какие методы защиты от компьютерных вирусов можно использовать?

**Сканирование, эвристический анализ, использование антивирусных мониторов, обнаружение изменений**

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

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

**Детекторы, ревизоры, фильтры, вакцины**

7. Как действуют программы-детекторы?

**Программы-детекторы позволяют обнаруживать файлы, зараженные одним из нескольких известных вирусов.**

8. Что называется сигнатурой?

**Специфическая для вируса комбинация байтов.**

9. Всегда ли детектор распознает зараженную программу?

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

**Программы-ревизоры - сначала они запоминают сведения о состоянии программ и системных областей дисков. После этого с помощью программы-ревизора можно в любой момент сравнить состояние программ и системных областей дисков с исходным.**

**Программы-фильтры - располагаются резидентно 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 - модифицируют 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?

**На первом уровне защиты** находятся резидентные программы для защиты от вируса. Эти программы могут первыми сообщить о вирусной атаке и предотвратить заражение программ и диска.

**Второй уровень защиты** составляют программы-ревизоры, программы-доктора и доктора-ревизоры. Ревизоры обнаруживают нападение тогда, когда вирус сумел пройти сквозь первый уровень. Программы-доктора применяются для восстановления зараженных программ, если ее копий нет в архиве, но они не всегда лечат правильно. Доктора-ревизоры обнаруживают нападение вируса и лечат зараженные файлы, причем контролируют правильность лечения.

**Третий уровень защиты** - это средства разграничения доступа. Они не позволяют вирусам и неверно работающим программам, даже если они проникли в компьютер, испортить важные данные.

12. Перечислите меры защиты информации от компьютерных вирусов.

**Оснащение ЭВМ современными антивирусными программами и регулярное обновление их версий. Проверка накопителей на наличие вирусов перед считыванием с них информации. При переносе на свой ПК файлов в архивированном виде проверка их сразу после разархивации. Защита своих дисков от записи при работе на других ПК. Создание архивных копий ценной информации на других носителях информации.**

13. Каковы современные технологии антивирусной защиты?