**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?

**исполняемые программы, загрузочные секторы дисков, пакетные командные файлы, драйверы, библиотеки динамической загрузки, документы c макросами (Вирусы НЕ заражают файлы с данными: тексты, рисунки, звук, видео!) веб-страницы.**

1. Как маскируются «невидимые» вирусы?

**Маскируется путем подмены вредоносного кода полезным во время сканирования**

1. Каковы особенности самомодифицирующихся вирусов?

**Самомодифицирующиеся вирусы (мутанты) изменяют свое тело таким образом, чтобы антивирусная программа не смогла его идентифицировать.**

1. Какие методы защиты от компьютерных вирусов можно использовать?

**Резервное копирование, ограничение доступа к компьютеру, включение антивируса, использование только лицензионного ПО, проверка всей поступающей извне информации**

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

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

**Антивирусные программы делятся на: программы-детекторы, программы - доктора, программы-ревизоры, программы-фильтры, программы-вакцины.**

7. Как действуют программы-детекторы?

**Программы-детекторы обеспечивают поиск и обнаружение вирусов в оперативной памяти и на внешних носителях, и при обнаружении выдают соответствующее сообщение.**

8. Что называется сигнатурой?

Сигнатура- обозначает фрагмент кода или функцию, характерные для определенного типа вирусов

9. Всегда ли детектор распознает зараженную программу?

**Программа детектор почти не имеют ошибку второго рода.**

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

**Программы-ревизоры (инспектора) относятся к самым надежным средствам защиты от вирусов.**

**Ревизоры (инспектора) проверяют данные на диске на предмет вирусов-невидимок, изучают, не забрался ли вирус в файлы, нет ли посторонних в загрузочном секторе жесткого диска, нет ли несанкционированных изменений реестра Windows.**

**Программы-фильтры (мониторы) или «сторожа» представляют собой небольшие резидентные программы, предназначенные для обнаружения подозрительных действий при работе компьютера, характерных для вирусов.**

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

**1.Проверка интернет трафика.**

**2.Проверка почтовых сообщений**

**3.Проверка файлов.**

**4.Защита от рекламных программ.**

**5.Защита от червей, троянов, вирусов.**

12. Перечислите меры защиты информации от компьютерных вирусов.

**1. Не стоит скачивать программы через пиратские сайты.**

**2.Скачать антивирус.**

**3.Постоянно очищать и обновлять антивирус.**

13. Каковы современные технологии антивирусной защиты?

**Существует сканирование сигнатур, также есть мониторинг операций. Мониторинг операций– это мониторинг выполняемых программ при запуске.**