**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?**

Вирусы могут заразить программы, диски и дискеты, командные файлы, драйверы, библиотеки, документы с микросхемами, веб страницы со скриптами. Но вирусы не заражают Текст, рисунки, звук, видео, любые данные которые без программного кода.

2. **Как маскируются «невидимые» вирусы?**

Камуфляжные вирусы или невидимки останавливают свое обнаружение через овладевание обращением операционной системы к файлам и дискам и выдают как незараженные .

3. **Каковы особенности самомодифицирующихся вирусов?**

Говоря простым языком, вирус меняет структуру своего тела и код рандомный образом, и получается что их трудно обнаружить.

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

Специальные программы для защиты что то по типу: Антивирусы, Касперский секюрети. Профилактические меры.Общие средства защиты информации.

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

Если я правильно понял, в тех случаях когда в компьютере есть вирусы.

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

**Программы детекторы** – это поиск конкретного вируса по его характеристикам в файлах. Когда обнаруживает выводит сообщение

**Программа доктор** – ну как и говорится в самом названии оно лечит зараженные файлы.

**Программы ревизоры** – запоминает исходную программу и выдает нарушение.

**Вакцины** – судя по названию они как и вакцина предотвращает заражение.

**7. Как действуют программы-детекторы?**

**Программы детекторы** – это поиск конкретного вируса по его характеристикам в файлах. Когда обнаруживает выводит сообщение

**8. Что называется сигнатурой?**

Тут если антивирусная программа обнаружит некоторую последовательность программного кода, специфичная для конкретной вредоносной проги, то посчитает зараженным вирусом и будет удален или будет лечится.

**9. Всегда ли детектор распознает зараженную программу?**

Программа детектор не почти не имеют ошибку второго рода.

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

**Программы ревизоры** – запоминает исходную программу и выдает нарушение.

**Вакцины** – судя по названию они как и вакцина предотвращает заражение.

**Программы фильтры** – перехватывает обращение к операционке, которое использует вирусы.

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

Если говорит про Dr.Web

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 скачивайте программы через пиратские сайты.

2.скачайте антивирус, желательно Касперский.

3.постоянно чистите и обновляйте антивирус.

**13. Каковы современные технологии антивирусной защиты?**

Есть сканирование сигнатур о котором мы уже говорили, еще есть мониторинг операций. Мониторинг операций – как говорит само название, это мониторинг выполняемых программ при запуске.