**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 antispyware.

**Контрольные вопросы:**

1. **Что могут заразить вирусы?**

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

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

Невидимые вирусы предотвращают обнаружение через овладение обращения ОС к файлам и дискам и выдают как незараженные.

3. **Каковы особенности самомодифицирующихся вирусов?**

Вирус меняет структуру своего тела и код случайным образом, из-за чего их трудно обнаружить.

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

Специальные программы для защиты, антивирусы: Kaspersky security. Проводить профилактические меры.

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

Как правило, при заражении вирусом, проведении проверок на заражение вирусами.

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

Программы-детекторы–поиск конкретного вируса по его характеристикам в файлах. Когда обнаруживает выводит сообщение об обнаружении.

Программа-доктор – лечит зараженные файлы.

Программы-ревизоры – запоминает исходную программу и выдает нарушение.

Вакцины–они как и вакцина предотвращает заражение.

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

Программы-детекторы–поиск конкретного вируса по его характеристикам в файлах.

**8. Что называется сигнатурой?**

Если антивирусная программа обнаружит некоторую последовательность программного кода, характерная для конкретной вредоносной программы, то она посчитает ее зараженным вирусом и удалит или будет лечить.

**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– запоминает исходную программу и выдает нарушение.

Вакцины–они как и вакцина предотвращает заражение.

Программы-фильтры– перехватывают обращение к ОС, которое использует вирусы.

**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.