**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?

2. Как маскируются «невидимые» вирусы?

3. Каковы особенности самомодифицирующихся вирусов?

4. Какие методы защиты от компьютерных вирусов можно использовать?

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

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

7. Как действуют программы-детекторы?

8. Что называется сигнатурой?

9. Всегда ли детектор распознает зараженную программу?

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

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

12. Перечислите меры защиты информации от компьютерных вирусов.

13. Каковы современные технологии антивирусной защиты?

1. Дискеты. Самый распространённый канал заражения в 1980—1990-е годы. Сейчас практически отсутствует из-за появления более распространённых и эффективных каналов и отсутствия флоппи-дисководов на многих современных компьютерах.

Флеш-накопители (флешки). В настоящее время USB-флешки заменяют дискеты и повторяют их судьбу — большое количество вирусов распространяется через съёмные накопители, включая цифровые фотоаппараты, цифровые видеокамеры, портативные цифровые плееры, а с 2000-х годов всё большую роль играют мобильные телефоны, особенносмартфоны (появились мобильные вирусы). Использование этого канала ранее было преимущественно обусловлено возможностью создания на накопителе специального файла autorun.inf, в котором можно указать программу, запускаемую Проводником Windows при открытии такого накопителя. В Windows 7 возможность автозапуска файлов с переносных носителей была отключена.

Электронная почта. Обычно вирусы в письмах электронной почты маскируются под безобидные вложения: картинки, документы, музыку, ссылки на сайты. В некоторых письмах могут содержаться действительно только ссылки, то есть в самих письмах может и не быть вредоносного кода, но если открыть такую ссылку, то можно попасть на специально созданный веб-сайт, содержащий вирусный код. Многие почтовые вирусы, попав на компьютер пользователя, затем используют адресную книгу из установленных почтовых клиентов типа Outlook для рассылки самого себя дальше.

Системы обмена мгновенными сообщениями. Здесь также распространена рассылка ссылок на якобы фото, музыку либо программы, в действительности являющиеся вирусами, поICQ и через другие программы мгновенного обмена сообщениями.

Веб-страницы. Возможно также заражение через страницы Интернета ввиду наличия на страницах всемирной паутины различного «активного» содержимого: скриптов, ActiveX-компонент. В этом случае используются уязвимости программного обеспечения, установленного на компьютере пользователя, либо уязвимости в ПО владельца сайта (что опаснее, так как заражению подвергаются добропорядочные сайты с большим потоком посетителей), а ничего не подозревающие пользователи, зайдя на такой сайт, рискуют заразить свой компьютер.

Интернет и локальные сети (черви). Черви — вид вирусов, которые проникают на компьютер-жертву без участия пользователя. Черви используют так называемые «дыры» (уязвимости) в программном обеспечении операционных систем, чтобы проникнуть на компьютер. Уязвимости — это ошибки и недоработки в программном обеспечении, которые позволяют удаленно загрузить и выполнить машинный код, в результате чего вирус-червь попадает в операционную систему и, как правило, начинает действия по заражению других компьютеров через локальную сеть или Интернет. Злоумышленники используют заражённые компьютеры пользователей для рассылки спама или для DDoS-атак.

1. Многие резидентные вирусы (и файловые, и загрузочные) предотвращают свое обнаружение тем, что перехватывают обращения операционной системы (и тем самым прикладных программ) к зараженным файлам и областям диска и выдают их в исходном (незараженном) виде. Такие вирусы называются невидимыми, или stealth (стелс) вирусами. Разумеется, эффект "невидимости" наблюдается толькона зараженном компьютере - на "чистом" компьютере изменения в файлах и загрузочных областях диска можно легко обнаружить
2. Средства антивирусной зашиты
3. Когда в компьютере есть вирусы
4. Детекторы, ревизоры, фильтры, доктора, вакцины.
5. осуществляют поиск компьютерных вирусов в памяти и при обнаружении сообщают об этом пользователю.
6. Классическая вирусная сигнатура — это непрерывная последовательность байтов, характерная для той или иной вредоносной программы. То есть она содержится в этом вредоносном файле и не содержится в чистых файлах
7. Не всегда
8. **Ревизоры** выполняют значительно более сложные действия для обнаружения вирусов. Они запоминают исходное состояние программ, каталогов, системных областей и периодически сравнивают их с текущими значениями. При изменении контролируемых параметров ревизоры сообщают об этом пользователю.

**Фильтры** выполняют выявление подозрительных процедур, например, коррекция исполняемых программ, изменение загрузочных записей диска, изменение атрибутов или размеров файлов. При обнаружении подобных процедур фильтры запрашивают пользователя о правомерности их выполнения.

**Вакцины** — это антивирусные программы, которые так модифицируют файл или диск, что он воспринимается программой-вирусом уже зараженным и поэтому вирус не внедряется.

1. Для защиты следует:

• использовать датчик поиска вирусов для автоматической проверки компьютера на вирусы во время работы;

• использовать датчик описаний вирусов для автоматического обновления описаний вирусов. Это даст уверенность в том, что компьютер будет защищен от самых новейших вирусов;

• приобрести и использовать хорошую программу по обнаружению и удалению вирусов;

• периодически создавать резервные копии жестких дисков