ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ И ЗАЩИТА ИНФОРМАЦИИ

1. Виды угроз информационной безопасности.

2. Методы и средства реализации угроз информационной безопасности.

3. Методы и средства защиты информационных систем.

Защита компьютера от вирусов – это задача, решать которую приходится пользователям, кто активно пользуется Интернетом или работает в локальной сети.

Информационная среда – это совокупность условий, средств и методов на базе компьютерных систем, предназначенных для создания и использования информационных ресурсов.

Информационная безопасность – совокупность мер по защите информационной среды общества и человека.

Цели информационной безопасности:

- ✔защита национальных интересов;
- ✔обеспечение человека и общества достоверной и полной информацией;
- ✔правовая защита человека и общества при получении, распространении и использовании информации.

Объекты обеспечения информационной безопасности:

- ✔ информационные ресурсы;
- ✔ система создания, распространения и использования информационных ресурсов;
- ✔ информационная инфраструктура общества *(информационные коммуникации, сети связи, центры анализа и обработки данных, системы и средства защиты информации)*;

- ✔ средства массовой информации;
- ✔ права человека и государства на получение, распространение и использование информации;
- ✔ защита интеллектуальной собственности и конфиденциальной информации.

Информационные угрозы – совокупность факторов, представляющих опасность для функционирования информационной среды.

Виды угроз *информационной безопасности*:

1. Внешние.
2. Внутренние.

1.Виды угроз информационной безопасности

1. *Внешние возникают, когда компьютерная сеть или отдельные компьютеры предприятия имеют выход в Интернет:*

- отказ в обслуживании;
- взлом системы безопасности.

1.Виды угроз информационной безопасности

2. *Внутренние угрозы исходят от компьютеров, находящихся в локальной сети предприятия.*

Они вызываются преднамеренными и непреднамеренными действиями пользователей.

- нарушение конфиденциальности;
- ошибки пользователей.

2. Методы и средства реализации угроз информационной безопасности

Мотивы реализации угроз информационной безопасности:

- самоутверждение отдельных личностей;
- получение экономической выгоды путем шантажа и кражи;
- нанесение ущерба конкуренту.

2. Методы и средства реализации угроз информационной безопасности

Способы реализации угроз:

1. Простой – *это кража носителя с данными и копирование конфиденциальных данных на съемный носитель.*
2. Сложный – *использование специального шпионского оборудования.*
3. Использование вредоносного программного обеспечения.

2. Методы и средства реализации угроз информационной безопасности

Группы вредоносного программного обеспечения:

1.Вирусы.

2. Хакерское ПО.

3. Спам.

2. Методы и средства реализации угроз информационной безопасности

1. Компьютерный вирус – это *небольшая* программа, написанная программистом высокой квалификации, способная к саморазмножению и выполнению разных вредоносных действий.

2. Методы и средства реализации угроз информационной безопасности

Активизация вируса *может быть* связана с *различными событиями:*

- ✔наступлением определённой даты или дня недели;
- ✔запуском программы;
- ✔открытием документа.

Признаки заражения:

- ✔общее замедление работы компьютера и уменьшение размера свободной оперативной памяти;
- ✔некоторые программы перестают работать или появляются различные ошибки в программах;
- ✔на экран выводятся посторонние символы и сообщения, появляются различные звуковые и видеоэффекты;

- размер некоторых исполнимых файлов и время их создания изменяются;
- некоторые файлы и диски оказываются испорченными;
- компьютер перестает загружаться с жесткого диска.

Вредоносное действие вируса:

1. Появление в процессе работы компьютера неожиданных эффектов.
2. Замедление работы компьютера.
3. Сбои и отказы в работе прикладных программ.
4. Порча и исчезновение файлов с магнитного диска.

5. Вывод из строя операционной системы, т.е. компьютер перестает загружаться.
6. Разрушение файловой системы компьютера.
7. Вывод из строя аппаратуры компьютера.

Классификация компьютерных вирусов

1. Среда обитания.
2. Особенности алгоритма работы.
3. Операционная система.
4. Деструктивные возможности.

Среда обитания

Файловые	**Загрузочные**	**Макровирусы**	**Сетевые**
Перезаписывающие вирусы			Сетевые черви
Файловые черви			Троянские программы
Вирусы-компаньоны			Вредоносные программы
Вирусы-звенья			
Паразитические вирусы			
Вирусы, поражающие исходный код программы			

Особенности алгоритма работы

- ✔ резидентный вирус;
- ✔ стел-алгоритмы;
- ✔ самошифрование и полиморфичность;
- ✔ полиморфик-вирусы.

Деструктивные возможности

- ✔безвредные;
- ✔неопасные;
- ✔опасные;
- ✔очень опасные.

Пути проникновения вирусов:

- ✔глобальная сеть Internet;
- ✔электронная почта;
- ✔локальная сеть;
- ✔компьютеры «Общего назначения»;
- ✔пиратское программное обеспечение,
- ✔ремонтные службы,
- ✔съемные накопители.

2. Хакерское ПО – это инструмент для взлома и хищения конфиденциальных данных:

- ✔для сканирования сети,
- ✔для взлома компьютеров и сетей.

3. Спам .

Метод фишинга используется для того, чтобы «выудить» у пользователя сведения для доступа к каким-либо ресурсам.

2. Методы и средства реализации угроз информационной безопасности

В заключение:

1. Снижение количества крупных всеобщих вирусных эпидемий и увеличение количества целенаправленных атак.
2. Появление организованной киберпреступности.
3. Увеличение количества взломов сайтов для размещения вредоносных кодов *вместо распространения вирусов на почту и червей к сайтам.*

3. Методы и средства защиты информационных систем

При разработке методов защиты информации в информационной среде следует учесть *следующие важные* факторы и условия:

- ✔расширение областей использования компьютеров и увеличение темпа роста компьютерного парка;

- ✔высокая степень концентрации информации в центрах ее обработки *и, как следствие*, появление централизованных баз данных, *предназначенных для коллективного пользования*;
- ✔расширение доступа пользователя к мировым информационным ресурсам;
- ✔усложнение программного обеспечения вычислительного процесса на компьютере.

3. Методы и средства защиты информационных систем

Методы и средства:

- организационно-технические;
- административно-правовые;
- программно-технические.

3. Методы и средства защиты информационных систем

Организационно-технические подразумевают:

- ✔создание на предприятии специальных помещений для размещения компьютеров с ценной информацией;
- ✔выполнение работ по защите помещений от электромагнитного излучения.

3. Методы и средства защиты информационных систем

Административно-правовые средства включают разработку различных правил по эксплуатации информационных систем, внутренних положений, должностных инструкций и мер административного воздействия на нарушителей.

3. Методы и средства защиты информационных систем

Программно-технические средства предназначены для предотвращения нарушения конфиденциальности и целостности данных, хранимых и обрабатываемых в информационной системе.

Группы программно-технических средств защиты:

1. Антивирусное ПО (**Сканеры, CRC-сканеры, блокировщики, иммунизаторы**).

   Антивирусные программы: Dr. Web, AVP, McAfee Virus Scan, Norton Antivirus 2000, Adinf.

2.Средства шифрования (**антивирусные программы, брандмауэры или файрволы, антишпионы**).

3. Средства защиты компьютерных сетей (**межсетевой экран: фильтрующий маршрутизатор, шлюз сетевого уровня, шлюз прикладного уровня**).

3. Методы и средства защиты информационных систем

Интегральной безопасности информационных систем:

1. Физическая безопасность.
2. Безопасность сетей и телекоммуникационных устройств.
3. Безопасность ПО.
4. Безопасность данных.

Спасибо за внимание.