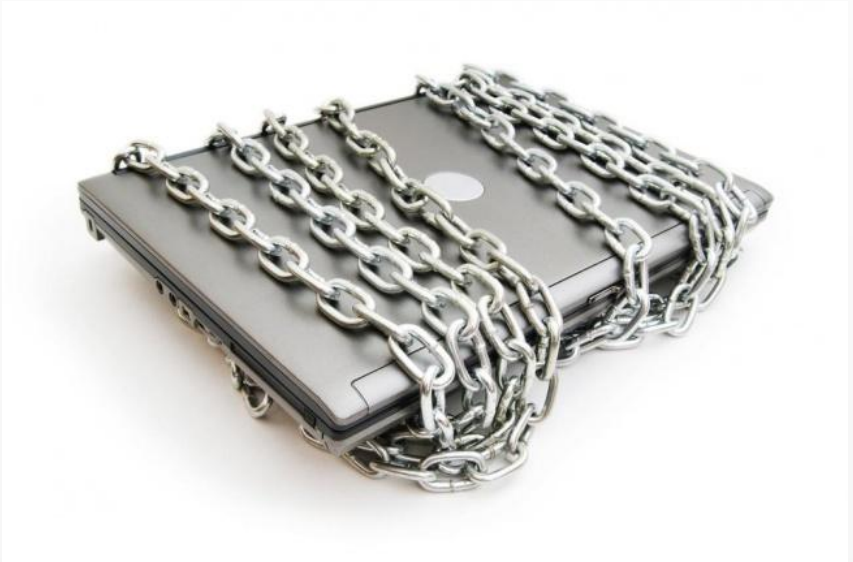
Безопасность

Существуют три вида угроз безопасности компьютерной системы организации:

- угроза нарушения режима конфиденциальности обрабатываемой информации;
- угроза нарушения целостности обрабатываемой информации;
- угроза нарушения работоспособности системы (отказ в обслуживании).



Источниками этих угроз являются:

- частичная или полная «поломка» оборудования
- кражи
- «логические бомбы»
- «троянский конь»
- «сбор мусора»
- сетевые анализаторы
- суперзаппинг
- «маскарад»

Частичная или полная «поломка» оборудования

Причинами этого явления могут быть:

- ошибки и намеренные действия персонала организации и посторонних лиц;
- активные эксперименты с различными вариантами настройки программного обеспечения, используемого в компьютерной системе организации, которые могут закончиться сбоями в работе компьютерной системы организации и/или потерей информации.

Наиболее распространенными причинами являются:

- атаки хакеров. Арсенал используемых средств достаточно широк. Атаки хакеров могут привести к разглашению конфиденциальной информации, а также к ее частичной модификации или полному уничтожению;
- побочные электромагнитные излучения (ПЭМИН). Одним из побочных факторов работы компьютера является электромагнитное излучение;
- диверсии, то есть умышленное нанесение физического повреждения компьютерной системе организации или логического повреждения информации и программному обеспечению. Если противник имеет физический доступ к оборудованию, то он может нанести ущерб;

Кражи

Они делятся на три вида:

- кражи оборудования. Особенно опасны кражи носителей конфиденциальной информации;
- кража информации. Утечка данных означает несанкционированное копирование конфиденциальной информации или программного обеспечения сотрудниками и тайный вынос носителей со скопированными данными за территорию организации;
- кража ресурсов компьютерной системы организации. Спектр угроз велик. Начиная от незаконного предоставления посторонним лицам доступа к автоматизированным базам данных, обычный доступ к которым происходит на коммерческой основе, и заканчивая использованием принтеров для распечатки материалов для личных нужд;

«Логические бомбы»

- для организации хищений, когда, например, программа производит начисление некоторой денежной суммы на заранее указанный счет;
- для удаления файлов после наступления определенных условий;
- для изменения случайным образом всех данных (диверсия);

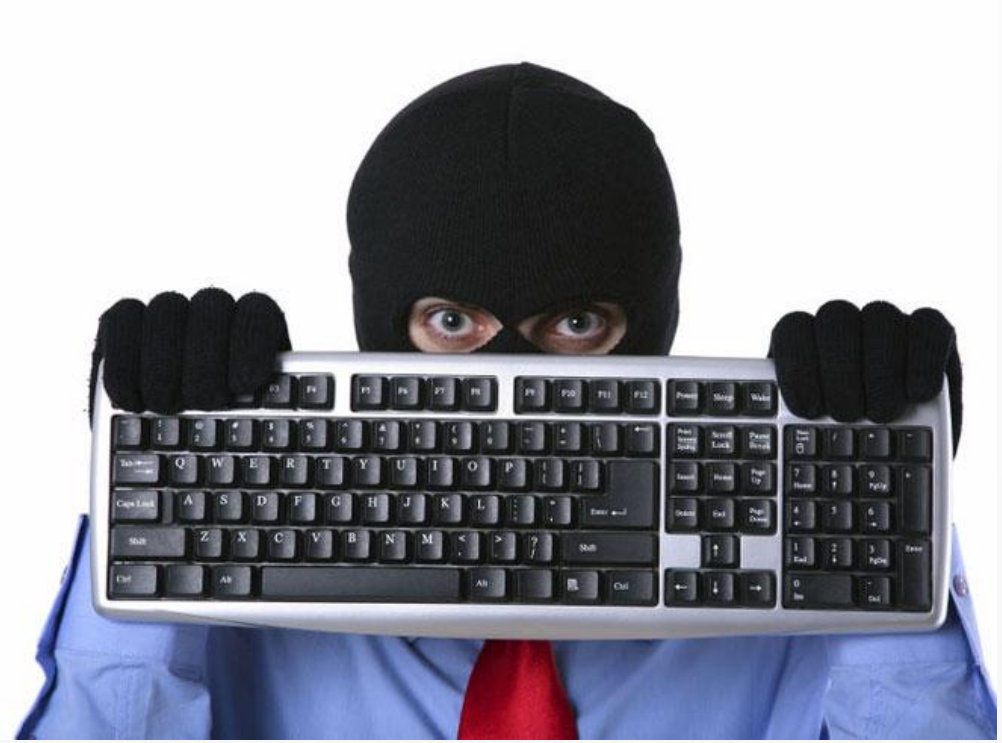
«Троянский конь»

Задачи:

- нарушение работы других программ (вплоть до повисания компьютера, решаемого лишь перезагрузкой, и невозможности их запуска);
- настойчивое, независимое от владельца предложение в качестве стартовой страницы спам-ссылок, рекламы или порно сайтов;
- распространение по компьютеру пользователя порнографии;
- превращение языка текстовых документов в бинарный код;
- мошенничество (например, при открывании определённого сайта пользователь может увидеть окно, в котором ему предлагают сделать определённое действие, иначе произойдёт что-то трудно поправимое — бессрочная блокировка пользователя со стороны сайта, потеря банковского счета и т.п., иногда за деньги, получение доступа к управлению компьютером и установки вредоносного ПО);

Источниками этих угроз являются:

- частичная или полная «поломка» оборудования
- кражи
- «логические бомбы»
- «троянский конь»
- **«сбор мусора»**
- **сетевые анализаторы**
- **суперзаппинг**
- **«маскарад»**



Социальная инженерия

метод несанкционированного доступа к информационным ресурсам, основанный на особенностях психологии человека

Техники:

- Претекстинг
- Фишинг
- Плечевой серфинг
- Квид про кво
- Троянский конь
- Сбор информации из открытых источников
- «Дорожное яблоко»
- Обратная социальная инженерия

Модуль 1

1. Основные узлы компьютера и их взаимодействие
2. Загрузка ПК. Знакомство с операционной системой Windows 8
3. Настройка операционной системы
4. Персонализация системы. Учетные записи пользователей. Системные папки
5. Прикладное ПО компьютера. Командная строка и командные файлы
6. Подключение компьютера к сети передачи данных
7. Организация работы локальной сети. Стек TCP/IP
8. Работа в глобальной сети. Серверы и маршрутизация
9. Работа в глобальной сети. Маршрутизаторы и WiFi. Сети в быту
10. Безопасная работа на компьютере
11. Сервисное обслуживание ПК и сети. Общие сетевые ресурсы. Резервное копирование
12. Сервисное обслуживание ПК и сети. Поиск и устранение неполадок в работе оборудования