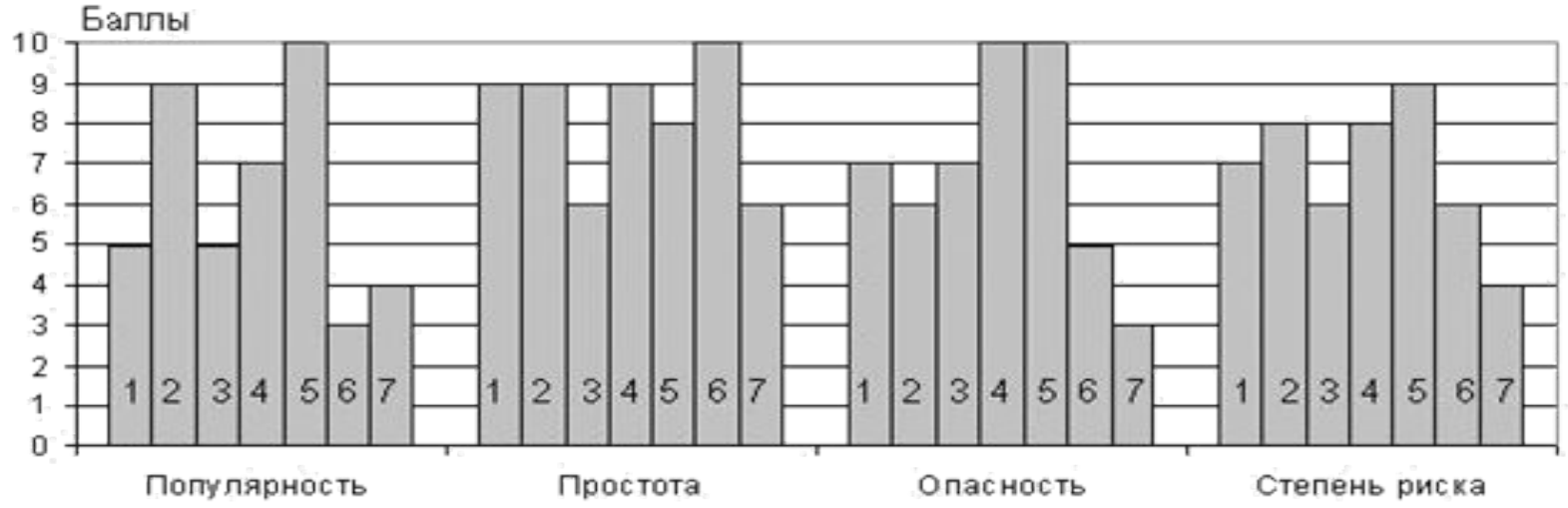
Лекция 7. Методы и средства обеспечения ИБ компьютерных систем.

1. Компьютерная система как объект ИБ. Каналы несанкционированного получения информации.
2. Неформальная модель нарушителя компьютерных систем.
3. Методы обеспечения ИБ: организационно - правовые, технические, криптографичес-кие. Их характеристика.
4. Средства обеспечения ИБ компьютерных систем.

1. Компьютерная система как объект ИБ. Каналы несанкционированного получения информации.

1). **Класс каналов от источников информации путем НСД к ним.**

1.Хищение носителей информации.
2.Копирование информации с носителей.
3.Подслушивание разговоров (в том числе их аудиозапись).
4.Установка закладных устройств в помещение и съем информации.
5.Выведывание информации обслуживающего персонала на объекте.
6.Фотографирование или видеосъемка носителей информации.



1 – рабочее место; 2 – разгребание мусора; 3 – поиск информации о сети; 4 – доступ к консоли; 5 – кража компьютеров; 6 – загрузка альтернативной ОС; 7 – взлом BIOS

2) Класс каналов от средств обработки информации путем НСД к ним.

1.Снятие информации с устройств электронной памяти.

2.Установка закладных устройств в СОИ.

3.Ввод программных продуктов получения информации.

4.Копирование информации с технических устройств отображения (фотографирование с мониторов и др.).

3). Класс каналов от источников информации без НСД к ним.

1.Получение информации по акустическим каналам (в системах венти-ляции, теплоснабжения, а также с помощью направленных микрофо-нов).

2.Получение информации по виброакустическим каналам (с использо-ванием акустических датчиков, лазерных устройств).

3.Использование технических средств оптической разведки (биноклей, подзорных труб и т. д.).

4.Использование технических средств оптико-электронной разведки (внешних телекамер, приборов ночного видения и т. д.).

5.Осмотр отходов и мусора..

6.Выведывание информации у обслуживающего персонала за преде-лами объекта.

7.Изучение выходящей за пределы объекта открытой информации (публикаций, рекламных проспектов и т. д.).

4) Класс каналов со средств обработки информации без НСД к ним.

1.Электромагнитные излучения СОИ (ПЭМИ, паразитная генерация уси-лительных каскадов, паразитная модуляция высокочастотных генерато-ров низкочастотным сигналом, содержащим конфиденциальную информацию).

2.Электромагнитные излучения линий связи.

3.Подключения к линиям связи.

4.Снятие наводок электрических сигналов с линий связи.

5.Снятие наводок с системы питания.

6.Снятие наводок с системы заземления.

7.Снятие наводок с системы теплоснабжения.

8.Использование высокочастотного навязывания.

9. Снятие с линий, выходящих за пределы объекта, сигналов, образован-ных на технических средствах за счет акустоэлектрических преобразова-ний.

10. Снятие излучений оптоволоконных линий связи.

11. Подключение к базам данных и ПЭВМ по компьютерным сетям.


Угрозы безопасности информации
По цели воздействия
По характеру воздействия
По характеру возникновения
Нарушения конфиденциальности
Нарушения целостности
Нарушения работоспособности
Активные
Пассивные
Случайные
Преднамеренные

2.Неформальная модель нарушителя компьютерных систем.

1) Нарушитель - лицо – носитель угроз информации. Лицо высшей квалификации.

2) Оценка технических возможностей нарушителя:

- может без помех открыто заниматься перехватом информации за пределами контролируемой зоны;
- как сотрудник предприятия или клиент может проникнуть на территорию объекта.
- Имеет возможность временного использования либо стацио-нарно установленных технических средств шпионажа, получе-ния ряда априорных данных, которые могут облегчить восста-новление недостающей информации.

3) Оценка технического оснащения нарушителя ИБ

Может применять специальные автономные излучающие устрой-ства (микропередатчики) акустического контроля помещений объектов по радиоканалу.

ТТД технических средств:

- модуляция: преимущественно частотная;
- рабочий диапазон, МГц: 75-180, 130-300, 370-400;
- усредненные размеры: от “рисового зернышка” до 58х40х20 мм;
- мощность излучения, мВт: от 5 до 20;
- дальность действия на передачу: минимальная - 80-100 до 400-600 м;
- дальность действия на прием: 20-50 м;
- время непрерывной работы: от 40-100 до 1000 ч;
- питание: автономное, от 1,5 до 9 В.

4. Тактика применения и особые свойства микропередатчиков

Неотъемлемой частью этих устройств является антенна, выполненная в виде отрезка провода длиной 10-30 см, который легко спрятать в щель, замаскировать под нитку или шнур. Обычно микропередатчики устанавливаются в местах, на которые человек редко обращает внимание.

3. Методы обеспечения ИБ: организационно - правовые, технические, криптографические. Их характеристика.

- **Правовые методы обеспечения ИБ РФ** : разработка нормативных правовых актов, регламентирующих отношения в информационной сфере, и нормативных методических документов по вопросам обеспечения ИБ РФ.
- **Организационно-техническими методы обеспечения ИБ РФ:**

1) создание систем и средств предотвращения НСД к обрабаты-ваемой информации и специальных воздействий, вызывающих разрушение, уничтожение, искажение информации, а также изме-нение штатных режимов функционирования систем и средств информатизации и связи;

2) выявление технических устройств и программ, представляю-щих опасность для нормального функционирования информаци-онно-телекоммуникационных систем, предотвращение перехвата информации по техническим каналам, применение криптографи-ческих средств ЗИ при ее хранении, обработке

4. Криптографические методы: обеспечение зашифрования данных перед их передачей по открытым каналам связи и дешифрования их после приема.

5. Экономические методы:

- разработку программ обеспечения ИБ РФ и определение порядка их финансирования;
- совершенствование системы финансирования работ, связанных с реализацией правовых и организационно-технических методов защиты информации, создание системы страхования информационных физических и юридических лиц.

4. **Средства обеспечения ИБ компьютерных систем.**

- Средства защиты от НСД:
  - Средства авторизации;
  - Мандатное управление доступом;
  - Управление доступом на основе ролей;
  - Журналирование (так же называется Аудит).
- Системы анализа и моделирования информационных потоков (CASE-системы).
- Системы мониторинга сетей:
  - Системы обнаружения и предотвращения вторжений (IDS/IPS).
  - Системы предотвращения утечек конфиденциальной инфор- мации (DLP-системы).
- Анализаторы протоколов.
- Антивирусные средства.
- Межсетевые экраны.
- Криптографические средства:
  - Шифрование;
  - Цифровая подпись.

- Системы резервного копирования.
- Системы бесперебойного питания:
  Источники бесперебойного питания;
  Резервирование нагрузки;
  Генераторы напряжения.
- Системы аутентификации:
  Пароль;
  Ключ доступа (физический или электронный);
  Сертификат;
  Биометрия.
- Средства предотвращения взлома корпусов и краж оборудования.
- Средства контроля доступа в помещения.
- Инструментальные средства анализа систем защиты:
  Мониторинговый программный продукт.

КОНЕЦ