*****ВОПРОСЫ ПО БЕЗОПАСНОСТИ СЕТЕЙ И *****
*****КАНАЛОВ ПЕРЕДАЧИ ДАННЫХ (ЗРИ-311КЛ)*****

1. **Основы теории информации**
 - определение информации Г. Кастлера
 - количество информации К. Шеннона
 - взаимная информация двух причинно связанных событий
 - виды источников информации

2. Кодирование
 - свойства кодов (неравенства Крафта-Макмиллана, кодовое дерево)
 - минимальная разрядность, избыточность и эффективность кодов
 - четыре типа кодирования

3. Оцифровка аналогового сигнала
 - точность квантования и порождаемые им шумы
 - ряды Фурье и частота дискретизации (скорость выборки)
 - четыре типа кодирования

4. Кодирование источников без памяти
 - кодирование Шеннона-Фано
 - кодирование Хаффмана
 - четыре типа кодирования

5. Кодирование источников с памятью
 -подавление нулей
 - групповое кодирование
 - подстановка образцов
 -дифференциальное сжатие
 - сжатие на основе преобразований
 - векторное квантование

6. Примеры сжатия
 -факс
 - текст
 - речь
 -изображения (gif, jpeg, mpeg)

7. Криптографические типы
 - рассеивание
 - перемешивание

8. Криптографические сценарии
 - только зашифрованный текст
 - известный открытый текст
 - выбранный открытый текст
 - выбранный зашифрованный текст

9. Системы с частными ключами
 - перестановочные шифры
 - трансформационные шифры (моноалфавитный, полиалфавитный
 - одноразовое заполнение
 - кодировщики со сдвигом регистра

10. Продукционные и поточные шифры
- стандарт шифрования DES
- расширенный стандарт шифрования AES
- поточные шифры (автоключ Виженера)
- DES-операция сцепления блоков шифра

11. Криптосистемы с общим ключом
- проблема распределения ключей
- односторонние функции (ключевой обмен Диффи-Хеллмана, RSA, knapsack, эллиптические кривые, коды с исправлением ошибок)

12. Криптографический протокол на целостность информации

13. Криптографический протокол на индентификацию (аутентичность)

14. Криптографический протокол «удаленное бросание монеты»

15. Криптографический протокол «неосознанная передача полномочий»

16. Критерии практической целесообразности и эффективности проектируемого уровня защиты
- факторы определяющие уровень защиты
-проверка полномочий
- аварийные ситуации
- человеческий фактор

I. На зачете будет приветствоваться ИНИЦИАТИВА: найденный (в интернете, книгах и т.д.) и представленный (изложенный) Вами дополнительный материал по выбранному вопросу.

II. Минимальная информация по всем вопросам есть в книге (гл. 2-3): Дж. Ирвин, Д. Харль Передача данных в сетях: инженерный подход. Санкт-Петербург. 2003.

III. Книга доступна бесплатно в интернете по URL: http://www.twirpx.com/file/378267/