**Вопросы на зачет**

1. Понятия «информационная безопасность» и «защита информации». Основные составляющие информационной безопасности.
2. Объекты защиты. Категории и носители информации.
3. Средства защиты информации.
4. Криптография. Основные термины и определения.
5. Классификация криптографических систем.
6. Шифры замены. Классификация и основные методы шифрования.
7. Шифры перестановки. Классификация и основные методы шифрования.
8. Шифры гаммирования. Классификация и основные методы шифрования.
9. Шифры гаммирования. Способы генерации гаммы. Генераторы гамм.
10. Схема режима шифрования DES-ECB.
11. Схема режима шифрования DES-CBC.
12. Схема режима шифрования DES-CPB и DES-OFB.
13. Тройной DES. Сферы применения различных режимов DES.
14. ГОСТ 28147-89. Схема режима шифрования простой замены.
15. AES. Краткая характеристика основных этапов зашифрования/расшифрования.
16. ГОСТ 34.12-2015. Схема шифрования блочного шифра "Кузнечик".
17. Шифрование с открытым ключом. Основные понятия.
18. Алгоритм шифрования RSA.
19. Алгоритм шифрования Эль-Гамаля.
20. Алгоритм шифрования на основе задачи об укладке ранца.
21. Эллиптические кривые. Основные понятия. Сложение и умножение точки.
22. Алгоритм шифрования на основе эллиптических кривых.
23. Хэш-функции. Основные понятия и разновидности.
24. Хэш-функция. MD5.