1. Информационная безопасность компьютерных систем. Основные понятия и определения.
2. Анализ угроз информационной безопасности.
3. Модель сетевой безопасности.
4. Обеспечение безопасности АСОИ.
5. Криптографическая защита информации. Основные понятия и определения.
6. Понятие стойкости шифра. Классификация криптоалгоритмов и типы криптоатак.
7. Современные приложения криптографии. Скремблирование.
8. Алгоритмы симметричного шифрования. Основные понятия и определения.
9. Сеть Фейштеля.
10. Алгоритм DES.
11. Алгоритм Blowfish.
12. Алгоритм IDEA.
13. Алгоритм ГОСТ 28147.
14. Режимы выполнения алгоритмов симметричного шифрования.
15. Способы создания псевдослучайных чисел.
16. Алгоритм AES.
17. Криптография с открытым ключом Основные требования к алгоритмам асимметричного шифрования.
18. Криптоанализ алгоритмов с открытым ключом.
19. Алгоритм RSA.
20. Алгоритм Диффи-Хеллмана.
21. Хэш-функции. Требования к хэш-функциям.
22. Простые хэш-функции. Парадокс дня рождения.
23. Использование цепочки зашифрованных блоков.
24. Хэш-функция MD5.
25. Хэш-функция SHA-1.
26. Хэш-функция SHA-2.
27. Хэш-функции ГОСТ 3411
28. Коды аутентификации сообщений – MAC. Требования к MAC.
29. MAC на основе алгоритма симметричного шифрования.
30. MAC на основе хэш-функции.
31. Цифровая подпись. Требования к цифровой подписи.
32. Прямая и арбитражная цифровые подписи.
33. Стандарт цифровой подписи DSS.
34. Отечественный стандарт цифровой подписи ГОСТ 3410.
35. Криптография с использованием эллиптических кривых. Математические понятия.
36. Аналог алгоритма Диффи-Хеллмана обмена ключами.
37. Алгоритм цифровой подписи на основе эллиптических кривых ECDSA.
38. Шифрование/дешифрование с использованием эллиптических кривых.
39. Алгоритмы обмена ключей и протоколы аутентификации.
40. Алгоритмы распределения ключей с использованием третьей доверенной стороны.
41. Взаимная аутентификация.