Вопросы на экзамен

1. Основные составляющие информационной безопасности. Категории и носители информации.
2. Объекты и средства защиты информации в информационных системах.
3. Криптография. Основные термины и определения. Классификация криптографических систем.
4. Шифры гаммирования. Классификация и основные методы шифрования.
5. Режимы шифрования DES. Сферы применения различных режимов DES.
6. AES. Краткая характеристика основных этапов зашифрования/расшифрования.
7. Шифрование с открытым ключом. Основные понятия.
8. Алгоритм шифрования RSA.
9. Алгоритм шифрования Эль-Гамаля.
10. Алгоритм шифрования на основе эллиптических кривых.
11. Хэш-функции. Основные понятия и разновидности. Хэш-функция. MD5.
12. Криптографические протоколы. Основные понятия.
13. Протоколы обмена ключами.
14. Парольная идентификация/аутентификация.
15. Протокол идентификации/аутентификации на основе шифрования с открытым ключом.
16. Сервер аутентификации Kerberos.
17. Идентификация/аутентификация с помощью биометрических данных.
18. Идентификационные карты (ID-cards) и электронные ключи.
19. Электронная цифровая подпись. Общие сведения и разновидности ЭЦП.
20. ЭЦП на базе алгоритма RSA и алгоритмы цифровой подписи ГОСТ 34.10-94 и ГОСТ 34.10-2001.
21. Протоколы контроля целостности: Биты четности, контрольные цифры и числа.
22. Протоколы контроля целостности: Использование ЭЦП и MAC-кодов.
23. Протоколы контроля целостности: Коды Хэмминга и ECC.
24. Электронные платежи. Разновидности и краткая характеристика.
25. Протоколы разбиения и разделения секрета.
26. Тайные многосторонние вычисления.
27. Основные сведения о криптоанализе и атаки на криптосистемы.
28. Компьютерная стеганография.
29. Общедоступные кодовые системы.
30. Секретные кодовые системы.