Вопрос 1.

1. Понятие информационной безопасности. Компоненты. Категории.
2. Способы обеспечения ИБ. Сервисы безопасности.
3. Средства защиты от несанкционированого доступа. Причины НСД. Каналы утечки информации. Последствия НСД.
4. DLP-системы. Методы функционирования. Компоненты, задачи DLP-систем.
5. VPN.
6. Сложная система. Шкала сложности. Динамическая система.
7. CASE-системы. Типы. Инструменты. Методологии IDEF.
8. DoS-атаки. Эксплойт. Ботнет.
9. Снифферы. Принцип действия. Способы перехвата трафика.
10. Взлом и защита беспроводных сетей. Спутниковая рыбалка.
11. Антивирусы. Сигнатурный метод.
12. Антивирусы. Проактивная защита.
13. Антивирусы. Эвристический анализ.
14. Антивирусы. Эмуляция кода. Песочница. Виртуализация.
15. Межсетевые экраны. Возможности. Проблемы. Бэкдор.
16. Принцип Керкгоффса.
17. Криптостойкость. Абсолютно и достаточно стойкие системы. Оценка криптостойкости.
18. Брутфорс. Устойчивость к атаке.
19. Повышение надёжности криптосистем. Хеширование. Коллизии хеш функций. Атака нахождения прообраза.
20. Криптографические алгоритмы. Алгоритмы симметричного шифрования.
21. Общая схема симметричных криптосистем. Параметры алгоритмов симметричного шифрования. Сравнение с асимметричными системами.
22. Управление ключами. Закрытый ключ. Электронная цифровая подпись.
23. Симметричная схема ЭП. Асимметричная схема ЭП. Виды асимметричных ЭП.
24. Взлом подписей. Слепая подпись.
25. Жизненный цикл ключей. Срок действия.
26. Криптоанализ. Классический и современный криптоанализ.
27. Методы криптоанализа.
28. Технические средства защиты авторских прав.

Вопрос 2.

29. Шифр Вернама.
30. Алгоритм шифрования AES
31. Алгоритм шифрования ГОСТ 28147-89
32. Алгоритм шифрования DES
33. Шифры Ривеста
34. Алгоритм шифрования Blowfish
35. Алгоритм шифрования Twofish
36. Алгоритм шифрования IDEA

37. Алгоритмы шифрования Khufu и Khafre
38. Потоковый алгоритм шифрования RC4
39. Асимметричный алгоритм шифрования RSA