Перечень вопросов для дифференцированного зачёта
ПМ.02 «Применение программно-аппаратных средств обеспечения информационной безопасности в автоматизированных системах»
МДК.02.02 «Криптографические средства и методы защиты информации»

1. Криптология. Определение. Виды дисциплин;
2. Криптография. Определение. Терминология;
3. Юридические аспекты криптологии на территории РФ;
4. Криптографический ключ. Определение. Назначение. Длина ключа. Классификации ключа;
5. История появления дисциплины «Криптография»;
6. Криптографические протоколы. Определение. Функции. Классификации;
7. Системы счисления. Определение. Виды. Переводы систем счисления. Арифметические операции с системами счисления;
8. Симметричные криптосистемы. Определение. Достоинства и недостатки. Основные алгоритмы шифрования;
9. Алгоритм DES. Определение. Блочный шифр. Принцип шифрования;
10. Алгоритм AES. Определение. Принцип шифрования;
11. Алгоритм IDEA. Определение. Принцип шифрования;
12. Криптосистемы с открытым ключом. Определение. Достоинства и недостатки. Основные принципы построения криптосистем с открытым ключом;
13. Алгоритм RSA. Определение. Применение. Принцип работы;
14. Хеширование. Определение. Виды хеш-функций;
15. Алгоритм MD4. Определение. Принцип работы;
16. Алгоритм MD5. Определение. Принцип работы;
17. Алгоритм MD6. Определение. Принцип работы;
18. Алгоритм криптографического хеширования SHA-1. Определение. Назначение. Принцип работы;
19. Алгоритм криптографического хеширования SHA-2. Определение. Назначение. Принцип работы;
20. Алгоритм WEP. Определение. Назначение. Принцип работы;
21. Алгоритм WPA. Определение. Назначение. Принцип работы;
22. Цифровая подпись. Определение. Назначение. Принцип работы. Привести примеры применения;
23. Криптографический протокол SSL. Определение. Назначение. Принцип работы;
24. Протокол защиты транспортного уровня TLS. Определение. Назначение. Принцип работы;
25. Управление ключами. Цели управления ключами. Политика безопасности;
26. Криптоанализ. Определение. История криптоанализа;
27. Криптоанализ. Определение. Основные и дополнительные методы криптоанализа;
28. Стенография. Определение. История появления. Виды. Применение;
29. Стеганография. Определение. История появления. Классификации;
30. Квантовая криптография. Определение. История возникновения. Физические и практические реализации систем.