Экзаменационные вопросы по дисциплине «Информационная безопасность»

1. Понятие информационной безопасности. Основные типы угроз информационной безопасности.
2. Законодательные аспекты информационной безопасности.
3. Базовые понятия криптографии. Основные задачи, решаемые с помощью криптографии. Понятия криптоалгоритма и ключа.
4. Криптоанализ. Понятие стойкости алгоритма. Основные разновидности криптоаналитических атак.
5. Классификация алгоритмов классической криптографии. Одноразовые блокноты. Классификация компьютерных криптоалгоритмов.
6. Принципы построения блочных шифров. Сеть Фейстеля.
7. Основные режимы работы блочных шифров.
8. Криптоалгоритм ГОСТ 28147-89. Структура раунда. Базовые циклы зашифрования и расшифрования. Режимы шифрования, определенные стандартом.
9. Криптоалгоритм AES. Характеристики алгоритма и его структура.
10. Криптосистемы с открытым ключом. Принципы построения и отличия от симметричных криптосистем. Алгоритм с открытым ключом RSA.
11. Управление ключами в симметричных и асимметричных криптосистемах. Генерация ключей. Распределение ключей для симметричных криптосистем.
12. Обмен сеансовыми ключами средствами симметричной криптографии и криптографии с открытым ключом. Способы хранения ключей. Время жизни ключей.
13. Алгоритм обмена ключами Диффи-Хеллмана.
14. Однонаправленные хэш-функции. Назначение. Основные требования, предъявляемые к хэш-функциям. Коллизии и их использование в процессе подделки сообщений.
15. Характеристики и общие принципы построения алгоритмов хэширования MD5, SHA-1, 2, 3, ГОСТ Р 34.11-94, 2012.
16. Коды проверки подлинности сообщений (MAC).
17. Электронная подпись (ЭП). Назначение электронной подписи, ее виды. Требования к ЭП. Общие принципы создания ЭП. Стандарты ЭП РФ и США.
18. Протоколы односторонней и двухсторонней аутентификации.
19. Стандарт X.509. Структура сертификата разных версий. Форматы хранения сертификатов.
20. Стандарт X.509. Принципы аутентификации. Отзыв сертификатов.
21. Инфраструктуры открытых ключей.
22. Система защиты электронной почты PGP.
23. Система защиты электронной почты S/MIME.
24. Потоковые шифры A5 и RC4.
25. Защищенный протокол передачи данных IPSec.
26. Защищенный протокол передачи данных SSL/TLS.
27. Стандарты информационной безопасности РФ.