Вопросы по курсу «Введение в криптографию»

Лапонина О.Р.

Магистратура, РКТ, 20-21 уч. год

1. Основные понятия и определения, относящиеся к информационной безопасности: атаки, уязвимости, политика безопасности, классификация атак.
2. Основные сервисы и криптографические механизмы безопасности.
3. Алгоритмы симметричного шифрования. Понятие стойкости алгоритма, области применения, типы операций, используемых в алгоритмах симметричного шифрования.
4. Сеть Фейстеля, SP-сеть.
5. Алгоритмы DES и тройной DES.
6. Алгоритмы симметричного шифрования Blowfish, IDEA, ГОСТ 28147.
7. Алгоритм Rijndael. Математические понятия, лежащие в основе алгоритма Rijndael. Структура алгоритма Rijndael.
8. Алгоритм ГОСТ 34.12-2015 «Кузнечик».
9. Поточные алгоритмы шифрования. Алгоритмы Salsa20 и ChaCha20.
10. Режимы выполнения алгоритмов симметричного шифрования.
11. Способы создания псевдослучайных чисел.
12. Требования к криптографическим хеш-функциям.
13. Структура Меркла — Дамгора. Хеш-функции MD5, SHA-1, SHA-2и ГОСТ 3411.
14. Хеш-функция SHA-3
15. Коды аутентификации сообщений.
16. Основные понятия, относящиеся к криптографии с открытым ключом, способы использования алгоритмов с открытым ключом: шифрование, создание и проверка цифровой подписи, обмен ключа.
17. Алгоритм RSA.
18. Алгоритм Диффи-Хеллмана.
19. Основные требования к цифровым подписям, стандарты цифровой подписи ГОСТ 3410 и DSS.
20. Криптография с использованием эллиптических кривых.
21. Основные протоколы аутентификации и обмена ключей с использованием третьей доверенной стороны.
22. Аутентификация и обмен ключей в протоколе Kerberos.

23. Инфраструктура открытого ключа. Сертификаты X.509 v3.
24. Инфраструктура открытого ключа. Репозиторий сертификатов. Способы отмены сертификатов.
25. Аутентификация и обмен ключей в протоколе TLS.
26. Классификация межсетевых экранов. Пакетные фильтры с поддержкой и без поддержки состояния.
27. Межсетевые экраны прикладного уровня.
28. Политики межсетевого экрана.
29. Межсетевые экраны с возможностями NAT.
30. Понятие DMZ. Различные топологии DMZ сетей с использованием межсетевых экранов разного типа.