Вопросы по курсу «Математические основы безопасности ИТ»

Лапонина О.Р.

Магистратура, РКТ, 19-20 уч. год

1. Основные понятия и определения, относящиеся к информационной безопасности: атаки, уязвимости, политика безопасности, механизмы и сервисы безопасности; классификация атак.
2. Алгоритмы симметричного шифрования. Понятие стойкости алгоритма, типы операций, используемых в алгоритмах симметричного шифрования. Сеть Фейштеля.
3. Алгоритмы DES и тройной DES.
4. Алгоритмы симметричного шифрования Blowfish, IDEA, ГОСТ 28147.
5. Режимы выполнения алгоритмов симметричного шифрования. Способы создания псевдослучайных чисел.
6. Алгоритм Rijndael. Математические понятия, лежащие в основе алгоритма Rijndael. Структура алгоритма Rijndael.
7. Основные понятия, относящиеся к криптографии с открытым ключом, способы использования алгоритмов с открытым ключом: шифрование, создание и проверка цифровой подписи, обмен ключа.
8. Алгоритм RSA.
9. Алгоритм Диффи-Хеллмана.
10. Требования к криптографическим хэш-функциям. Хэш-функции MD5, SHA-1, SHA-2, SHA-3 и ГОСТ 3411.
11. Обеспечение целостности сообщений.
12. Основные требования к цифровым подписям, стандарты цифровой подписи ГОСТ 3410 и DSS.
13. Криптография с использованием эллиптических кривых.
14. Основные протоколы аутентификации и обмена ключей с использованием третьей доверенной стороны.
15. Аутентификация и обмен ключей в протоколе Kerberos.
16. Инфраструктура открытого ключа. Сертификаты X.509 v3.
17. Инфраструктура открытого ключа. Репозиторий сертификатов. Способы отмены сертификатов.
18. Аутентификация и обмен ключей в протоколе TLS/SSL.
19. Аутентификация и обмен ключей в протоколе SSH.