Вопросы на сессию

Методы обеспечения целостности информации

КБ-3/ИКБ

1. Основные понятия, обозначения и задачи криптографии.
2. Основные принципы криптографической защиты.
3. Актуальность проблематики защиты информации.
4. Защита целостности информации при хранении. Рассмотреть организационные меры.
5. Защита целостности при транспортировке информации
6. Защита целостности при обработке информации
7. Защита от угрозы нарушения целостности информации на уровне содержания
8. Протоколы контроля целостности. Проверка четности.
9. Протоколы контроля целостности. Использование контрольных цифр.
10. Протоколы контроля целостности. Использование контрольных сумм.
11. Защита целостности информации при хранении. Рассмотреть технологические меры.
12. Защита целостности при обработке информации. Рассмотреть интегрированный подход.
13. В чем заключается управление передачей привилегий.
14. Перечислить и охарактеризовать принципы контроля целостности.
15. Рассмотреть принцип разграничения функциональных обязанностей
16. Рассмотреть принцип корректность транзакций
17. Раскрыть суть принципа аутентификации пользователей
18. Рассмотреть принцип минимизация привилегий.

19 Блочные и поточные шифры.

20 Односторонние функции. Функции с секретом.

21 Сеть Фейстеля.

22 Стандарт симметричной криптосистемы США – DES.

23 Симметричные системы шифрования: поточные и блочные шифры.

24 Стандарт шифрования DES. Режимы использования.

25 Стандарт симметричной криптосистемы России – ГОСТ 28147-89.

26 Сравнительный анализ блочных шифров DES и ГОСТ 28147-89.

27 Методы проверки чисел на простоту. Примеры.

28 Особенности и типы асимметричных криптосистем

29 Системы защиты с открытым ключом. Алгоритм Эвклида.

30 Системы защиты с открытым ключом. Малая теорема Ферма.

31 Системы защиты с открытым ключом. Функция Эйлера.

32 Электронная подпись. Хеш-функция.

33 Аутентификация на основе хэш-функций. Алгоритмы хэширования SHA и MD5.

34 Применение систем симметричного и асимметричного шифрования

35 Алгоритм цифровой подписи RSA.

36 Схема RSA: алгоритм шифрования, его обратимость, вопросы стойкости. Алгоритмы разложения чисел на простые сомножители.

37 Алгоритм цифровой подписи DSA.

38 Генерация и проверка цифровой подписи на основе криптосистемы Эль-Гамаля.

39 Оценки надежности электронной подписи.

40 Сравнение систем симметричного и асимметричного шифрования.

41 Электронная цифровая подпись. Определение. Способы построения и проверки.

42 Функции дискретного логарифмирования и основанные на ней алгоритмы Диффи-Хеллмана и Эль-Гамаля.

43 Понятие, назначение и способы вычисления хеш-функции.

44 Что такое криптографические протоколы? Сформулировать доказательство с нулевым разглашением.

45 Криптографические протоколы. Протокол подбрасывание монеты по телефону

46 Криптографические протоколы. Протокол ЭЦП.

47 Стандарт цифровой подписи ГОСТ Р34.10-94

48 Криптографические протоколы. Протокол электронные торги.

49 Протокол электронного голосования.

50 Протокол контроля целостности на основе алгоритма Луна.

51 Протокол контроля целостности на основании использования контрольных сумм.