Вопросы для подготовки к экзамену по дисциплине «Защита информации».

1. Проблема защиты информации и подходы к ее решению.

2. Основные понятия защиты информации.

3. Угрозы информационной безопасности и каналы утечки информации.

4. Организационная защита информации.

5. Правовое обеспечение защиты информации.

6. Инженерно-техническая защита информации.

7. Криптографическая защита информации.

8. Программно-аппаратная защита информации.

9. Способы несанкционированного доступа и защиты от него в компьютерных системах.

10. Организация базы учетных записей пользователей в ОС Unix.

11. Организация базы учетных записей пользователей в ОС Windows.

12. Способы аутентификации пользователей.

13. Аутентификация пользователей на основе паролей.

14. Аутентификация пользователей на основе модели «рукопожатия».

15. Программно-аппаратная защита от локального несанкционированного доступа.

16. Аутентификация пользователей на основе их биометрических характеристик.

17. Протокол S/Key.

18. Протокол CHAP.

19. Протокол RADIUS.

20. Протокол Kerberos.

21. Протокол IPSec и виртуальные частные сети.

22. Защита от несанкционированной загрузки ОС.

23. Разграничение прав пользователей в ОС Windows.

24. Дискреционное, мандатное и ролевое разграничение доступа к объектам.

25. Подсистема безопасности ОС Windows.

26. Разграничение доступа к объектам в ОС Windows.

27. Разграничение прав пользователей в ОС Unix.

28. Разграничение доступа к объектам в ОС Unix.

29. Аудит событий безопасности в ОС Windows и Unix.

30. Средства защиты информации в глобальных компьютерных сетях.

31. Стандарты оценки безопасности компьютерных систем и информационных

32. Элементы теории чисел.

33. Способы симметричного шифрования.

34. Абсолютно стойкий шифр. Генерация, хранение и распространение ключей.

35. Криптографическая система DES и ее модификации.

36. Криптографическая система ГОСТ 28147-89.

37. Применение и обзор современных симметричных криптосистем.

38. Принципы построения и свойства асимметричных криптосистем.

39. Криптографическая система RSA.

40. Криптографические системы Диффи-Хеллмана, Эль-Гамаля и эллиптических

41. Электронная цифровая подпись и ее применение. Функции хеширования.

42. Протокол SSL.

43. Криптографический интерфейс приложений ОС Windows.

44. Файловая система с шифрованием в ОС Windows.

45. Компьютерная стеганография и ее применение.

46. Вредоносные программы и их классификация.

47. Методы обнаружения и удаления вредоносных программ.

48. Принципы построения и состав систем защиты от копирования.