Вопросы к зачёту

1. Прогресс информационных технологий и необходимость обеспечения информационной безопасности.

2. Основные понятия информационной безопасности.

3. Структура понятия информационная безопасность.

4. Система защиты информации и ее структура.

5. Экономическая информация как товар и объект безопасности.

6. Профессиональные тайны, их виды. Объекты коммерческой тайны на предприятии.

7. Персональные данные и их защита.

8. Информационные угрозы, их виды и причины возникновения.

9. Информационные угрозы для государства.

10. Информационные угрозы для компании.

11. Информационные угрозы для личности (физического лица).

12. Действия и события, нарушающие информационную безопасность.

13. Личностно-профессиональные характеристики и действия сотрудников, способствующих

реализации информационных угроз.

14. Способы воздействия информационных угроз на объекты.

15. Внешние и внутренние субъекты информационных угроз.

16. Компьютерные преступления и их классификация.

17. Исторические аспекты компьютерных преступлений и современность.

18. Субъекты и причины совершения компьютерных преступлений.

19. Вредоносные программы, их виды.

20. История компьютерных вирусов и современность.

21. Государственное регулирование информационной безопасности.

22. Деятельность международных организаций в сфере информационной безопасности.

23. Нормативно-правовые аспекты в области информационной безопасности в Российской

Федерации.

24. Доктрина информационной безопасности России.

25. Уголовно-правовой контроль над компьютерной преступностью в России.

26. Федеральные законы по ИБ в РФ.

27. Политика безопасности и ее принципы.

28. Фрагментарный и системный подход к защите информации.

29. Методы и средства защиты информации.

30. Организационное обеспечение ИБ.

31. Организация конфиденциального делопроизводства.

32. Комплекс организационно-технических мероприятий по обеспечению защиты

информации.

33. Инженерно-техническое обеспечение компьютерной безопасности.

34. Организационно-правовой статус службы безопасности.

35. Защита информации в Интернете.

36. Электронная почта и ее защита.

37. Защита от компьютерных вирусов.

38. «Больные» мобильники и их «лечение».

39. Популярные антивирусные программы и их классификация.

40. Организация системы защиты информации экономических объектов.

41. Криптографические методы защиты информации.

42. Этапы построения системы защиты информации.

43. Оценка эффективности инвестиций в информационную безопасность.

44. План обеспечения непрерывной работы и восстановления функционирования

автоматизированной информационной системы.

45. Управление информационной безопасности на государственном уровне.

46. Аудит ИБ автоматизированных банковских систем.

47. Электронная коммерция и ее защита.

48. Менеджмент и аудит информационной безопасности на уровне предприятия.

49. Информационная безопасность предпринимательской деятельности.

50. Обеспечение информационной безопасности должностных лиц и представителей деловых

кругов.

51. Основные определения информационной безопасности

52. Информация как предмет защиты, жизненный цикл информации и вопросы безопасности

53. Составляющие безопасности. Комплексная защита информации. Понятие и задачи.

54. Принципы организации систем обеспечения информационной безопасности

55. Классификация угроз информационной безопасности (с примерами).

56. Способы и средства защиты информации.

57. Управление доступом. Матричная и многоуровневая модели управления доступом.

58. Основы шифрования. Симметричная и асимметричная криптосистемы. Хеш-функции.

59. Электронная цифровая подпись.

60. Аутентификация. Способы аутентификации. Проблемы парольной защиты.

61. Аутентификация при помощи цифровых сертификатов. Сертифицирующие центры

62. Вредоносное программное обеспечение. Жизненный цикл вируса.