**Вопросы к зачету по дисциплине «Основы информационной безопасности в правоохранительных органах»**

1. Понятие информации, информационной сферы, безопасности информации и

информационной безопасности субъекта.

2. Основные составляющие национальных интересов в информационной сфере.

3. Виды и источники угроз информационной безопасности страны (на примере Российской Федерации).

4. Принципы государственной политики обеспечения информационной безопасности

страны (на примере Российской Федерации).

5. Информационная сфера и информационная безопасность правоохранительных органов.

6. Обеспечение информационной безопасности в процессе деятельности оперативных подразделений органов внутренних дел.

7. Важнейшие составляющие интересов в информационной сфере и основные угрозы информационной безопасности правоохранительных органов.

8. Защита информации. Комплексный подход к защите информации.

9. Классификация методов защиты информации.

10. Понятие и виды каналов утечки информации ограниченного доступа. «Типовые» каналы утечки информации объектов информатизации ПО.

11. «Типовые» каналы утечки информации объектов информатизации ПО. Условия и факторы, способствующие утечке информации ограниченного доступа.

12. Основные угрозы безопасности информации. Общая характеристика технических средств несанкционированного получения информации и технологий их применения.

13. Основные направления инженерно-технической защиты информации: физическая защита, скрытие информации, поиск и нейтрализация источников утечки.

14. Распространённые способы блокирования каналов утечки информации и виды специальных технических средств защиты.

15. Понятие и цели проведения специальных проверок объектов информатизации; основные этапы проведения проверки.

16. Методы и специальные технические средства, используемые в ходе поисковой операции в целях обеспечения защиты информации.

17. Уязвимость компьютерных систем. Понятие несанкционированного доступа. Классы и виды несанкционированного доступа.

18. Уязвимость компьютерных систем. Модель злоумышленника.

19. Понятие «идентификации пользователя». Задача идентификации пользователя. Использование идентификации в защите информационных процессов.

20. Методы и средства защиты данных от несанкционированного доступа.

21. Основные методы НСД при физическом контакте с компьютером.

22. Классический алгоритм поведения злоумышленника при удаленном несанкционированном доступе в компьютерную систему.

23. Основные причины утечки информации с охраняемых объектов.

24. Разграничение доступа к информации. Идентификация и аутентификация.

25. Криптографические методы защиты данных. Электронно-цифровая подпись.

26. Основные угрозы безопасности информации в компьютерных системах.

27. Вредоносные программы и методы борьбы с ними.

28. Угрозы безопасности современных информационно-вычислительных и телекоммуникационных сетей. Классификация угроз безопасности.

29. Методы и средства воздействия на безопасность сетей.

30. Особенности построения защиты информации в телекоммуникационных сетях. Современные технические и программные средства сетевой защиты компьютерной информации.

31. Применение электронно-цифровой подписи для защиты документов.

32. Идентификация электронных и бумажных документов. Реквизиты и свойства документов.

33. Свойства файла и свойства электронного документа.

34. Свойства электронного документа – фиксация в электронном документе и в бумажной форме.

35. Свойства электронного документа – поиск документов по заданному фрагменту текста.

36. Свойства электронного документа – поиск документов по заданным свойствам.

37. Понятие и назначение шаблона процессуальных документов.

38. Создание нового шаблона на основе одного из стандартных шаблонов MS Word.

39. Создание нового шаблона на основе готового электронного документа.

40. Извлечение и использование готовых шаблонов процессуальных документов изстандартных шаблонов MS Word.

41. Сохранение шаблонов и создание на их основе новых документов.

42. Автоматизация заполнения электронных документов. Создание защищенного шаблона

43. Виды и параметры полей форм. Текстовое поле, флажок, список.

44. Понятие и места установки паролей.

45. Современные требования к надежным паролям.

46. Виды атак на пароли и классификация паролей.

47. Правила составления и запоминания надежных (сложных) паролей.

48. Парольная защита документов MS Word. Установка и различные виды парольной защиты.

49. Возможности преодоления и обхода парольной защиты документов MS Word.

50. Приемы скрытия текста и графических объектов в документе.

51. Приемы обнаружения скрытых текстовых и графических объектов в документе.

52. Защита различных объектов в MS Excel: книги, листа, ячейки, выделенного диапазона.

53. Создание защищенной таблицы с редактируемыми областями.

54. Скрытие объектов в Excel: окна Excel, окна книги, листов, ячеек, выделенных диапазонов, формул.

55. Приемы скрытия текста и графических объектов в документе MS Excel.

56. Приемы обнаружения скрытых текстовых и графических объектов в документе MS Excel.

57. Шифрование любых файлов с документами.

58. Добавление текстовой информации в конец графического файла.

59. Запаковка текста внутри графического файла с искажением последнего.

60. Сокрытие текста внутри графического файла без искажения последнего.

61. Понятие и квалификация преступлений в сфере компьютерной информаций