Вопросы для промежуточной аттестации:

1. Понятие программно-аппаратных средств защиты информации. Объект защиты информации. Политика безопасности.

2. Политика безопасности: понятие, виды. Достоверная вычислительная база. Принципы реализации политики безопасности.

3. Понятие и назначение модели безопасности. Модель дискреционного доступа. Модель безопасности Белла-ЛаПадулы.

4. Понятие и назначение модели безопасности. Ролевая модель контроля доступа. Системы разграничения доступа: назначение и примеры.

5. Роль парольной защиты в обеспечении безопасности. Характеристики парольной защиты. Методы обхода парольной защиты.

6. Классификация систем идентификации и аутентификации. Электронные идентификаторы: виды и особенности.

7. Классификация систем идентификации и аутентификации. Биометрические идентификаторы: виды и особенности.

8. Классификация систем идентификации и аутентификации. Особенности комбинированных систем идентификации и аутентификации.

9. Классификация и особенности программно-аппаратных средств криптографической защиты информации. Симметричное шифрование: алгоритмы, стандарты, особенности. Примеры средств шифрования информации.

10. Классификация и особенности программно-аппаратных средств криптографической защиты информации. Асимметричное шифрование: алгоритмы, стандарты, особенности. Примеры средств шифрования информации.

11. Особенности применения электронной подписи (ЭП). Алгоритмы ЭП. Сертификаты ЭП. Примеры криптопровайдеров.

12. Классификация, функции и особенности технологии межсетевых экранов.

13. Схема сетевой защиты на базе межсетевых экранов. Известные методы обхода межсетевых экранов.

14. Персональные и распределенные межсетевые экраны.

15. Показатели защищенности межсетевых экранов.

16. Классификация систем обнаружения вторжений. Обнаружение сигнатур и аномалий.

17. Требования к системам обнаружения вторжений.

18. Система обнаружения вторжений SNORT: особенности применения, настройки и управления.

19. Вредоносные программы: понятие и классификация.

20. Компьютерные вирусы: файловые вирусы, макровирусы, загрузочные вирусы.

21. Классификация и особенности троянских программ (троянов).

22. Особенности сетевых червей, типы червей, наименования.

23. Методы обнаружения вредоносных программ.

24. Виды и особенности антивирусных компьютерных программ.

25. Классификация защищенности средств антивирусной защиты информации.