Вопросы

1. Контрольные вопросы для проведения текущего контроля по итогам освоения Раздела 1 – Концептуальные основы защиты информации:

1) История деятельности по защите информации.

2) Проблема защиты информации в обществе.

3) Концептуальные подходы и направления деятельности в области защиты информации.

4) Центры защиты информации.

5) Принципы построения защищенной информационной системы.

6) Предмет защиты информации.

7) Термин информация.

8) Термин защита информации.

9) Термины видов защиты информации.

10) Термины способов защиты информации.

11) Термины замысла защиты информации.

12) Термины объекта защиты информации.

13) Термины угроз безопасности информации.

14) Термины техники защиты информации.

15) Термины способов оценки соответствия требованиям по защите информации.

16) Термины эффективности защиты информации.

17) Государственная система защиты информации.

18) Задачи и функции органов системы защиты информации на предприятии.

19) Лицензирование деятельности в области защиты информации.

20) Сертификация в области защиты информации.

21) Аттестация в области защиты информации.

22) Концептуальное основание защиты информации

23) Стратегия национальной безопасности РФ до 2020 года.

24) Доктрина информационной безопасности РФ.

25) Законодательные акты в области защиты информации.

26) Нормативные правовые акты Президента РФ в области защиты информации.

27) Постановления Правительства РФ в области защиты информации.

28) Национальные стандарты в области защиты информации.

29) Структура нормативно-технических и нормативно-методических документов по защите информации.

30) Нормативные и методические документы по технической защите информации.

31) Органы государственной власти в области защиты информации РФ.

32) Федеральная служба безопасности РФ в области защиты информации РФ.

33) Федеральная служба по техническому и экспортному контролю РФ.

34) Проблема информационной безопасности общества.

35) Информационная безопасность в Доктрине информационной безопасности РФ.

36) Цели и задачи информационной безопасности.

37) Система обеспечения информационной безопасности предприятия.

2. Контрольные вопросы для проведения текущего контроля по итогам освоения Раздела 2 – Методические подходы формирования защищенной информационной системы:

1) Виды информационных ресурсов предприятия, подлежащие защите.

2) Юридическая и финансовая информация предприятия.

3) Информация о работниках предприятия.

4) Общая информация и информация о клиентах предприятия.

5) Коммуникативная информация предприятия.

6) Степени важности информационных ресурсов предприятия.

7) Принципы построения защищенной информационной системы предприятия.

8) Требования к защищенной информационной системе предприятия.

9) Рекомендации к построению защищенной информационной системы предприятия.

10) Составляющие системы защиты информационной системы предприятия.

11) Алгоритм формирования информационной системы предприятия.

12) Внутренние информационные потоки информационной системы предприятия.

13) Внешние информационные потоки информационной системы предприятия.

14) Организационно-распорядительная составляющая защищенной информационной системы предприятия.

15) Политика безопасности защищенной информационной системы предприятия.

16) Техническая составляющая защищенной информационной системы предприятия.

17) Подсистема антивирусной защиты информационной системы предприятия.

18) Подсистема защиты каналов передачи данных информационной системы предприятия.

19) Понятие протокола передачи данных.

20) Принципы организации обмена данными в вычислительных сетях.

21) Транспортный протокол TCP и модель ТСР/IР.

22) Подсистема обнаружения вторжений информационной системы предприятия.

23) Особенности архитектуры при построении подсистемы обнаружения вторжений информационной системы предприятия.

24) Подсистема защиты электронной почты информационной системы предприятия.

25) Особенности архитектуры при построении подсистемы защиты электронной почты информационной системы предприятия.

26) Подсистема управления доступом информационной системы предприятия.

27) Особенности архитектуры при построении подсистемы управления доступом – безопасность закрытых ключей.

28) Особенности архитектуры при построении подсистемы управления доступом – аппаратные хранилища закрытых ключей.

29) Особенности архитектуры при построении подсистемы управления доступом – аппаратные устройства с криптографическими возможностями.

30) Особенности архитектуры при построении подсистемы управления доступом – смарт-карты и USB-ключи.

31) Подсистема резервного копирования и архивирования информационной системы предприятия.

32) Алгоритм внедрения и тестирования подсистем защиты информационной системы предприятия – функции подсистем.