**Примерные оценочные материалы, применяемые при проведении**

**промежуточной аттестации по дисциплине (модулю)**

**09.04.01 «Защита информации в сетях».**

Примерный перечень тем курсового проекта:

1. Разработка модели малого инновационного предприятия c использованием нотации IDEF0
2. Разработка модели малого инновационного предприятия c использованием нотации BPMN
3. Разработка модели малого инновационного предприятия c использованием UML
4. Разработка модели подразделения учебного заведения с использованием нотации IDEF0
5. Разработка модели подразделения учебного заведения с использованием нотации BPMN
6. Разработка модели подразделения учебного заведения с использованием UML
7. Разработка модели производственного предприятия с использованием нотации IDEF0
8. Разработка модели производственного предприятия с использованием нотации BPMN
9. Разработка модели производственного предприятия с использованием UML
10. Традиционные направления информационной защиты и пути их интеграции.

Уровень знаний определяется оценками ***«отлично», «хорошо», «удовлетворительно», «неудовлетворительно».***

Оценка **«отлично»** - курсовой проект выполнен технически грамотно, в соответствии с заданием. Студент показывает полные и глубокие знания программного материала, логично и аргументировано отвечает на поставленный вопрос, а также дополнительные вопросы, показывает высокий уровень теоретических знаний.

Оценка «хорошо» - курсовой проект выполнен технически грамотно, в соответствии с заданием. Студент показывает глубокие знания программного материала, грамотно его излагает, достаточно полно отвечает на поставленный вопрос и дополнительные вопросы, умело формулирует выводы. В тоже время при ответе допускает несущественные погрешности.

Оценка «удовлетворительно» - курсовой проект выполнен выполнена с небольшими недочетами. Студент показывает достаточные, но не глубокие знания программного материала; при ответе не допускает грубых ошибок или противоречий, однако в формулировании ответа отсутствует должная связь между анализом, аргументацией и выводами. Для получения правильного ответа требуется уточняющие вопросы.

Оценка «неудовлетворительно» - курсовой проект не выполнен или студент показывает недостаточные знания программного материала, не способен аргументировано и последовательно его излагать, допускается грубые ошибки в ответах, неправильно отвечает на поставленный вопрос или затрудняется с ответом.

Примерный перечень вопросов:

* 1. Атаки на протоколы и службы Интернет. Методы и средства защиты.
  2. Понятие межсетевых экранов. Компоненты межсетевого экрана. Политика сетевой безопасности.
  3. Критерии фильтрации пакетов. Основные схемы сетевой защиты на базе межсетевых экранов.
  4. Создание защищенных сегментов сетей с использованием межсетевых экранов.
  5. Конфигурирование сетевых фильтров на базе настроек безопасности протокола TCP/IP в ОС Windows XP.
  6. Защита рабочих станций с использованием персональных сетевых фильтров.
  7. Организация VPN-сетей. Задачи, решаемые VPN. Туннелирование в VPN.
  8. Электронные сертификаты. Понятие инфраструктуры открытых ключей.
  9. Протоколы и средства организации VPN на сетевом уровне. Назначение, область применения, аутентификация и шифрование данных в протоколах SKIP и IPSec.
  10. Протоколы PPTP, SSL. Назначение, область применения, аутентификация и шифрование данных.
  11. Преимущества технологии терминального доступа. Обеспечение безопасности.
  12. Назначение систем обнаружения атак. Классификация систем обнаружения атак.
  13. Службы каталогов. Общие сведения о службах каталогов. Структура каталога LDAP.
  14. Система единого входа в сеть на основе протокола Kerberos. Создание единого пространства безопасности на базе Active Directory.
  15. Осуществите криптографическую защиту сетевого трафика средствами протокола IPSec в ОС Windows XP. Перехватите в локальной сети пакеты, убедитесь в шифровании трафика.
  16. Осуществите криптографическую защиту сетевого трафика средствами СКЗИ StrongNet. Перехватите в локальной сети пакеты, убедитесь в шифровании трафика. 18. Орг
  17. Оргаанизовать защищенный обмен почтовой информацией между двумя пользователями. Шифрование почтовых сообщений выполнить с помощью алгоритма ГОСТ 28147-89, реализуемого средствами СКЗИ КриптоПро CSP. Выполнить с использованием образов ОС Windows Server 2003 и Windows 2000.
  18. Разработайте файл конфигурации и настройте СОА Snort на обнаружение тестирования внутренней структуры сети ICMP-запросами.
  19. Разработайте файл конфигурации и настройте СОА Snort на обнаружение ICMPпакетов большой длины.
  20. Разработайте файл конфигурации и настройте СОА Snort на обнаружение устанавливаемых из внешней сети TCP-соединений.
  21. Установить службу терминального доступа. Выполнить настройки службы MSTS, разрешающие доступ к ресурсам терминального сервера только для учетных записей, зарегистрированных в созданной по умолчанию группе «Remote Desktop Users».
  22. Установить службу терминального доступа. Выполнить настройки протокола RDP, запрещающие использование ресурсов рабочей станции, включая буфер обмена, принтеры и накопители.
  23. Выявите сетевые узлы в локальном сетевом сегменте с использованием: утилиты fping; утилиты ping и широковещательной ICMP-посылки; утилиты icmpush (тип ICMPпакетов13 и 17); утилиты ping и многоадресной рассылки; утилиты arping; утилиты hping3 и методов TCP- и UDP-разведки; утилиты Ethereal и метода прослушивания сети.
  24. Разработайте политику для пакетного фильтра, разрешающего только получение информации с FTP-серверов. Реализуйте политику средствами сетевых фильтров.
  25. Разработайте политику для пакетного фильтра, разрешающего только получение и отправку электронной почты. Реализуйте политику средствами сетевых фильтров.
  26. Разработайте и реализуйте политику для пакетного фильтра, запрещающего сканирование внутренней структуры сети. Реализуйте политику средствами сетевых фильтров.
  27. Разработайте и реализуйте политику для пакетного фильтра, запрещающего получение извне доступа к ресурсам компьютера за исключением двух доверенных узлов. Реализуйте политику средствами сетевых фильтров.
  28. Разработайте и реализуйте политику для пакетного фильтра, запрещающего получение доступа к Web-ресурсам определенного узла. Реализуйте политику средствами сетевых фильтров.
  29. Разработайте и реализуйте политику для пакетного фильтра, разрешающего только получение доступа к Web-ресурсам двух определенных узлов. Реализуйте политику средствами сетевых фильтров.
  30. Разработайте и реализуйте политику для пакетного фильтра, разрешающего только просмотр Web-ресурсов. Реализуйте политику средствами сетевых фильтров.
  31. Разработайте политику для пакетного фильтра, разрешающего только получение информации с FTP-серверов. Реализуйте политику средствами протокола IPSec.
  32. Разработайте политику для пакетного фильтра, разрешающего только получение и отправку электронной почты. Реализуйте политику средствами протокола IPSec. Разработайте и реализуйте политику для пакетного фильтра, разрешающего только просмотр Web-ресурсов. Реализуйте политику средствами протокола IPSec.
  33. С использованием программы «Брандмауэр Windows» (Windows Firewall) выполнить настройки, запрещающие использование всех портов защищаемого узла за исключением TCP-порта 3389.
  34. Разработайте и реализуйте политику для пакетного фильтра, запрещающего сканирование внутренней структуры сети. Реализуйте политику средствами протокола IPSec.
  35. Сгенерируйте и получите в виде файла сертификат открытого ключа с использованием образа ОС Windows Server 2003.
  36. Настройте Web-сервер для организации защищенного доступа к Web-странице с использованием протокола SSL. Выполнить с использованием образа ОС Windows Server 2003. Файл-сертификат открытого ключа прилагается.
  37. Настройте входящее подключение VPN с использованием протокола PPTP. Настроить и установить подключение клиентского узла. Выполнить с использованием образа ОС Windows Server 2003.