Вопросы к экзамену МДК 03.02 БКС 8 семестр группы СА50-1-2-3-20

- Основные понятия информационной безопасности
- Угрозы информационной безопасности.
- Алгоритм RSA.
- Инфраструктура открытых ключей.
- Криптографические хэш-функции.
- Атаки на канальный уровень. Методы защиты от атак.
- Принцип работы протокола 802.1x.
- Протокол SSL/TLS.
- Протокол Netflow.
- Угрозы WI-FI сети. Обеспечение безопасности.
- Классификация компьютерных вирусов.
- Антивирусные программы.
- Определение виртуальной часной сети.
- Виртуальные частные сети канального уровня.
- Технологии туннелирования. GRE-туннель.
- Протоколы IPSec.
- Технологии фильтрации трафика.
- Принцип работы межсетевого экрана.
- Технология инспектирования трафика.
- Технология AAA. Протокол Tacacs+.
- Технология AAA. Протокол RADIUS.
- Системы контроля и учета доступа.
- Утечка информации – это?
- Наиболее эффективное средство для защиты от сетевых атак.
- Политика информационной безопасности — это? RADIUS, серверы TACACS, TACACS + - примеры систем
- Чем отличается протокол HTTPS от HTTP?
- HTTP и HTTPS. Описание, характеристика.
- Каким термином называется способ шифрования, в котором для шифрования и

  расшифровывания применяется один и тот же криптографический ключ?
- Межсетевой экран Cisco ASA. Описание возможностей, характеристика.
- Методы обеспечения безопасного доступа к оборудованию.

- Атаки на беспроводные сети.
- Идентификатор набора служб.
- Усиление защиты беспроводной сети; Стандартные списки доступа.
- Расширенные списки доступа.
- Переполнение CAM-таблицы.
- Атака VLAN-hopping.
- Межсетевые экраны. Виды
- Разница между PAT и NAT?
- Центр сертификации Windows
- Центр сертификации Cisco
- Центр сертификации Linux
- Стандарты с применением RSA
- Симметричное шифрование
- Ассиметричное шифрование
- Цифровая подпись
- Задачи криптографии
- Реализация криптографических протоколов
- Типы криптографических методов
- Технология CBAC. Отличие от списков доступа.
- Site-to-site VPN. Характеристики. Описание.
- Site-to-client VPN. Характеристики. Описание.
- Рефлексивные списки доступа.
- Сертификаты служб и клиента. Атаки с двойным тегированием
- Прокси-сервера. Применение.
- Технология GRE over IPSec.
- Зачем нужны сертификаты? Каким образом они поддерживают безопасность информационных систем?
- Почему на сетевом оборудовании важно указывать актуальные дату и время?