**ОПК-9. Способен решать задачи профессиональной деятельности с учетом текущего состояния и тенденций развития информационных технологий, средств технической защиты информации, сетей и систем передачи информации**

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| |  |  |  |  | | --- | --- | --- | --- | | Индикаторы, дескрипторы  достижения компетенций | Комплекс заданий для оценки компетенций  (сквозная нумерация) | Ключи правильных ответов | Критерии  оценки  в баллах | | | | |
| **Дисциплина «Сети и системы передачи информации» Б1.Б.31** | | | |
| **ИОПК -9.2.**  Анализирует и учитывает текущее состояние и тенденции развития информационных сетей передачи информации для обеспечения информационной безопасности в открытых информационных системах.  **Знать:**  теоретические сведения в области информационных систем и основ сетевых технологий  принципы работы сетевых технологий  показатели качества функционирования сетевых технологий  **Уметь:**  обрабатывать и анализировать информацию, характеризующую работу сетевых технологий **Владеть:**  методами и технологиями проектирования сетевых технологий | **1.** Выберите правильный вариант ответа.  В настоящее время применяются следующие виды сетевого кабеля для интернета  1) коаксиальный кабель  2) оптоволоконный кабель  3) витая пара,  По какому из них информация передаётся не электрическим, а световым импульсом? | 2 | Верный ответ –1 неверный – 0. |
| **2.** Выберите правильный вариант ответа.  В сетях Ethernet используется следующий метод организации доступа к передающей среде:   1. маркерный метод, 2. CSMA/CD, 3. CSMA/CA, 4. вставка регистра. | 2 | Верный ответ –1 неверный – 0. |
| **3.** Выберите правильный вариант ответа.  В сетях Ethernet возможно применение следующей топологии:   1. кольцо, 2. звезда, 3. общая шина, 4. все перечисленные варианты топологий. | 4 | Верный ответ –1 неверный – 0. |
| **4.** Выберите правильный вариант ответа.  Мосты работают на определенном уровне модели OSI:   1. физический, 2. сетевой, 3. канальный, 4. транспортный. | 3 | Верный ответ –1 неверный – 0. |
| **5.** Установите соответствие между названием протокола и его назначением:   |  |  |  |  | | --- | --- | --- | --- | | А | RARP | 1 | нахождение оптимального пути для передачи данных | | Б | OSPF | 2 | определение MAC-адреса по IP-адресу | | В | ARP | 3 | определение IP-адреса по МАС-адресу | | |  |  | | --- | --- | | А | 3 | | Б | 1 | | В | 2 | | Верный ответ –1 неверный – 0. |
| **6.** Установите соответствие между функциональной группой задач системы управления сетями и входящими в них задачами:   |  |  |  |  | | --- | --- | --- | --- | | А | управление конфигурацией сети и именованием | 1 | выявление, определение и устранение последствий сбоев и отказов в работе сети | | Б | обработка ошибок | 2 | регистрация времени использования различных ресурсов сети | | В | анализ производительности и надежности | 3 | конфигурирование параметров как отдельных элементов сети, так и всей сети в целом | | Г | Управление безопасностью | 4 | оценка на основе накопленной статистической информации пропускной способности реального либо виртуального канала связи, интенсивность трафика в отдельных сегментах и каналах сети | | Д | Учет работы сети | 5 | контроль доступа к ресурсам сети и сохранение целостности данных при их передаче через сеть | | |  |  | | --- | --- | | А | 3 | | Б | 1 | | В | 4 | | Г | 5 | | Д | 2 | | Верный ответ –1 неверный – 0. |
| **7.** Установите соответствие между названием группы объектов RMON базы данных управляющей информации MIB протокола SNMP и входящими в группу объектами:   |  |  |  |  | | --- | --- | --- | --- | | А | Alarms | 1 | условия регистрации и генерации событий | | Б | Hosts | 2 | пороговые значения статистических показателей, при превышении которых агент RMON посылает сообщение менеджеру | | В | TrafficMatrix | 3 | условия фильтрации пакетов | | Г | Filter | 4 | данные о хостах сети | | Д | Event | 5 | статистика об интенсивности трафика между каждой парой хостов сети, упорядоченная в виде матрицы | | |  |  | | --- | --- | | А | 2 | | Б | 4 | | В | 5 | | Г | 3 | | Д | 1 | | Верный ответ –1 неверный – 0. |
| 8. Пропускная способность канала передачи информации **не** измеряется в**: бит/с; Мбит/с; Мбит; Кбайт/с.** Введите ответ. | **Мбит** | Верный ответ –1 неверный – 0. |
| **9.** Задан адрес электронной почты в сети Интернет: [username@mtu-net.ru](mailto:username@mtu-net.ru)  Каково имя владельца этого электронного адреса:ru; mtu-net.ru; Username; mtu-net  Введите ответ. | **ru** | Верный ответ –1 неверный – 0. |
| **10.** Установите соответствие между названиями команд и их назначением:  1. ping  2. Traceroute  3. tcpdump  а. Позволяет просматривать все входящие и исходящие из определенного интерфейса пакеты.  б. Для проверки соединения и работы с удаленным хостом.  в. Позволяет отследить маршрут до удаленного хоста. | 1-б  2-в  3-а | Верный ответ – 1 неверный – 0. |
| **11.** Установите правильную последовательность шагов алгоритма работы моста (bridge):  1) очистка буфера (если адресат находится в том же сегменте, что и отправитель);  2) мост проверяет адрес назначения пакета и сравнивает его с адресами узлов, закрепленных за портами;  3) мост осуществляет процедуру доступа к передающей среде и передает кадр в этой среде (если адресат находится в другом сегменте);  4) мост принимает любой пакет, имеющийся на входе порта, и помещает его в буферную память. | 4, 2, 1, 3 | Верный ответ – 1 неверный – 0. |
| **12.** Впишите число.  Эталонная модель взаимосвязи открытых систем OSI включает в себя…уровней. | 7 | Верный ответ – 1 неверный – 0. |
| **13.**Впишите ответ с маленькой буквы.  В манчестерском коде для кодирования единиц и нулей используется… потенциала. | перепад | Верный ответ – 1 неверный – 0. |
| **14.** Впишите ответ с маленькой буквы.  В потенциальных кодах бит кодируется… значением физической величины. | постоянным | Верный ответ – 1 неверный – 0. |
| **15.** Впишите ответ с маленькой буквы.  Протокол IGRP работает по алгоритму… расстояния. | вектора | Верный ответ – 1 неверный – 0. |
| **Дисциплина «Защита информации от утечек по техническим каналам» (Б1.Б.34)** | | | |
| ИОПК-9.1. Анализирует и учитывает текущее состояние и тенденции развития технических средств защиты информации для обеспечения информационной безопасности в открытых информационных системах  **Знать:**  − технические средства обеспечения информационной безопасности (ИОПК-9.1) − особенности применения технических средств защиты информации в открытых информационных системах (ИОПК -9.1 )  − основные категории требований к техническим средствам обеспечения информационной безопасности (ИОПК-9.1) − методы оценки угрозы технического добывания информации (ИОПК-9.1) − основные принципы организации и методы реализации технической защиты информации (ИОПК-9.1)  − основные руководящие и нормативные документы в сфере технической защиты информации (ИОПК - 9.1)  − методику организации технической защиты информации (ИОПК-9.1)  − задачи и технологии сертификации технических средств на соответствие требованиям информационной безопасности (ИОПК-9.1) **Уметь:**  − проводить выбор технических средств обеспечения информационной безопасности для обеспечения требуемого уровня защищенности открытой информационной системы (ИОПК-9.1)  − использовать основные руководящие и нормативные документы в сфере технической защиты информации (ИОПК-9.1)  − выполнять работы по сертификации технических средств защиты информации открытых информационных систем (ИОПК-9.1)  **Владеть:**  − навыками разработки архитектуры системы защиты информации открытой информационной системы (ИОПК-9.1)  − методами и навыками моделирования систем технической защиты информации (ИОПК-9.1) | **1. Что такое утечка информации?**  1. Несанкционированное получение информации третьими лицами  2. Перемещение файлов между устройствами  3. Удаление данных с устройства | 1 | Верный ответ – 1 неверный – 0. |
| **2. Какие существуют виды утечки информации?**  1. Технические, организационные, программные  2. Только технические  3. Только внешние | 1 | Верный ответ – 1 неверный – 0. |
| **3. Что такое технический канал утечки информации?**  1. Канал передачи данных между компьютерами  2. Способ утечки информации через физические средства или устройства  3. Ошибка в программном коде | 2 | Верный ответ – 1 неверный – 0. |
| **4. Что относится к техническим каналам утечки?**  1. Электромагнитное излучение, акустические каналы, оптические каналы  2. Только электромагнитные каналы  3. Организационные ошибки | 1 | Верный ответ – 1 неверный – 0. |
| 5. Что такое пассивный канал утечки?  1. Канал, использующий программные методы  2. Канал, при котором злоумышленник не влияет на источник информации  3. Средство защиты данных | 2 | Верный ответ – 1 неверный – 0. |
| **6. Что относится к электромагнитным каналам утечки?**  1. Только радиоволны  2. Неразрешенное излучение от электронных устройств, токопроводящих кабелей  3. Шумы на линии связи | 2 | Верный ответ – 1 неверный – 0. |
| **7. Как защититься от утечки через электромагнитное излучение?**  1. Отключить интернет  2. Экранирование помещений и оборудования  3. Установить пароль на компьютер | 2 | Верный ответ – 1 неверный – 0. |
| **8. Какое оборудование используется для перехвата электромагнитных излучений?**  1. Сканеры текста  2. Антенны, радиоприемники, анализаторы спектра  3. Микрофоны | 2 | Верный ответ – 1 неверный – 0. |
| **9. Что такое TEMPEST?**  1. Метод кодирования данных  2. Стандарт защиты от перехвата электромагнитного излучения  3. Алгоритм шифрования | 2 | Верный ответ – 1 неверный – 0. |
| **10. Какие документы регламентируют защиту от электромагнитных излучений в России?**  1. ГОСТы и стандарты Минобороны РФ  2. Только федеральные законы  3. Постановления судов | 1 | Верный ответ – 1 неверный – 0. |
| **11. Что такое акустический канал утечки информации?**  1. Передача звука через интернет  2. Утечка через звуки, издаваемые устройствами или людьми  3. Утечка через световые сигналы | 2 | Верный ответ – 1 неверный – 0. |
| **12. Какие устройства используют для акустического перехвата?**  1. Микрофоны, лазерные микрофоны, диктофоны  2. Радиопередатчики  3. Анализаторы кода | 1 | Верный ответ – 1 неверный – 0. |
| **13. Как защитить помещение от акустической утечки?**  1. Установить сигнализацию  2. Шумогенераторы, звукоизоляция стен и окон  3. Использовать камеры видеонаблюдения | 2 | Верный ответ – 1 неверный – 0. |
| **14. Что такое виброакустический канал утечки?**  1. Передача звука по проводам  2. Передача информации через вибрации твердых тел  3. Радиоволновый перехват | 2 | Верный ответ – 1 неверный – 0. |
| **15. Какие меры снижают риск виброакустической утечки?**  1. Использование интернета  2. Амортизация столов, снижение вибраций оборудования  3. Усиление сигнала связи | 2 | Верный ответ – 1 неверный – 0. |
| **16. Что относится к оптическим каналам утечки?**  1. Утечка через файлы  2. Передача данных через световые сигналы или отображения на экране  3. Аудиозаписи | 2 | Верный ответ – 1 неверный – 0. |
| **17. Как осуществляется перехват информации через оптические каналы?**  1. С помощью оптических приборов, камер, лазеров  2. Через радиоволны  3. Через сетевые подключения | 1 | Верный ответ – 1 неверный – 0. |
| **18. Какие меры защищают от оптической утечки?**  1. Установить антивирус  2. Закрыть окна жалюзи, использовать светозащитные экраны  3. Отключить монитор | 2 | Верный ответ – 1 неверный – 0. |
| **19. Что такое визуальная утечка информации?**  1. Передача данных через интернет  2. Получение информации путём наблюдения за экраном или документами  3. Снятие информации через микрофон | 2 | Верный ответ – 1 неверный – 0. |
| **20. Как снизить риск визуальной утечки?**  1. Использовать экраны с защитой от обзора, избегать работы в общественных местах  2. Установить межсетевой экран  3. Включить режим энергосбережения | 2 | Верный ответ – 1 неверный – 0. |