**Экзаменационные вопросы по дисциплине МДК.03.01 Эксплуатация объектов сетевой инфраструктуры на 8 семестр.**

**Группы: СА50-1-21, СА50-2-21**

1. Пассивное оборудование
2. Активное оборудование
3. Элементы СКС Назначение
4. Профилактика работы периферийного оборудования
5. Профилактика работы ПК
6. Профилактика работы сетевого оборудования
7. Система мониторинга. Функции и задачи
8. Виртуализация и её виды
9. Виртуализация Docker образы
10. Виртуализация Docker. Контейнер
11. Журналирование Syslog
12. Протоколы централизованного управления сетью
13. Протоколы децентрализованного управления сетью
14. Методология поиска неисправностей
15. Поиск неисправностей на физическом уровне
16. Поиск неисправностей на сетевом уровне
17. Централизованное и децентрализованное управление сетью
18. Понятие гипервизора. Примеры
19. Система Proxmox VE
20. Понятие СХД и способы его реализации
21. Протоколы сбора статистики в сети Syslog
22. Системы мониторинга Zabbix
23. Системы мониторинга Wireshark
24. Система виртуализации Hyper-V
25. Понятие объектов сетевой инфраструктуры
26. Понятие и проведение профилактических работ. Особенности профилактических работ с разными типами устройств
27. Система виртуализации Vmware ESXI
28. Программная виртуализации Особенности программной виртуализации
29. Протокол NTP Принцип работы, иерархия NTP-серверов
30. Разработка плана модернизации сети Требования и этапы
31. Система виртуализации Vmware ESXI
32. Управление сетью с помощью SNMP
33. Задачи центра управления NOC
34. Парольные политики Определение, назначение
35. Системы мониторинга Определение, основные задачи
36. Резервное копирование и восстановление.
37. Аппаратная виртуализация. Особенности аппаратной виртуализации
38. Возможные проблемы производительности сети и методы устранения
39. Задачи центра управления сетью
40. Возможные проблемы производительности сети и методы устранения
41. Задачи центра управления сетью
42. Назначение и настройка протокола PPP
43. Назначение и настройка протокола PPPoE
44. Назначение и настройка Multilink
45. Назначение и настройка IP SLA
46. Веб-сервера IIS, основные свойства
47. Способы развертывания веб-сервиса на IIS
48. Основные понятия информационной безопасности.
49. Угрозы информационой безопасности.
50. Алгоритм DES.
51. Алгоритм AES.
52. Алгоритм RSA.
53. Алгоритм обмена ключами Диффи-Хеллмана.
54. Инфраструктура открытых ключей.
55. Криптографические хэш-функции.
56. Атаки на канальный уровень. Методы защиты от атак.
57. Атака на протокол ARP. Способы защиты.
58. Принцип работы протокола 802.1x.
59. Протокол SSL/TLS.
60. Протокол Netflow.
61. Угрозы WI-FI сети. Обеспечение безопасности.
62. Алгоритм WI-FI сети WEP.
63. Алгоритмы WI-FI сети WPA, WPA2.
64. Компьютерные вирусы. Классификация компьютерных вирусов.
65. Антивирусные программы. Классификация антивирусных программ.
66. Определение виртуальной часной сети.
67. Виртуальные частные сети канального уровня.
68. Технологии туннелирования. GRE-туннель.
69. Описание технологии DMVPN.
70. Протоколы IPSec.
71. Технологии фильтрации трафика.
72. Принцип работы межсетевого экрана.
73. Технология инспектирования трафика.
74. Принцип работы системы IPS/IDS.
75. Технология AAA. Протокол Tacacs+.
76. Системы IP-видеонаблюдения.
77. Системы контроля и учета доступа.
78. Утечка информации – это?
79. Наиболее эффективное средство для защиты от сетевых атак
80. Наиболее эффективное средство для защиты от сетевых атак
81. Длина исходного ключа у алгоритма шифрования DES (бит)
82. Политика информационной безопасности — это?
83. Брандмауэры первого поколения представляли собой
84. Удачная криптоатака называется
85. RADIUS, серверы TACACS, TACACS + - примеры систем
86. Чем отличается протокол HTTPS от HTTP?
87. Каким термином называется способ шифрования, в котором для шифрования и расшифровывания применяется один и тот же криптографический ключ?
88. Чем отличается симметричное шифрование от асимметричного?
89. Что такое атака «человек посередине» (MITM)? Примеры и методы защиты.
90. Что такое фишинг и какие существуют методы его предотвращения?
91. Как работает двухфакторная аутентификация и в чём её преимущество?
92. В чём разница между IDS и IPS системами обнаружения атак?
93. Какие существуют уровни модели OSI и где на них реализуется безопасность?
94. Что такое социальная инженерия и как противостоять её приёмам?
95. Какие угрозы связаны с использованием облачных технологий?
96. Что представляет собой политика управления паролями в рамках ИБ?
97. Примеры современных угроз нулевого дня (zero-day) и способы их выявления.