**Примерные оценочные материалы, применяемые при проведении**

**промежуточной аттестации по дисциплине (модулю)**

**«Программно-аппаратные средства защиты информации».**

При проведении промежуточной аттестации обучающемуся предлагается дать ответы на 3 вопроса из нижеприведенного списка.

Примерный перечень вопросов

1. Концепции безопасности. Преимущества применения системы защиты. Компоненты защиты.
2. Защита административных интерфейсов. Усиление парольной защиты.
3. Системы парольной аутентификации. Локальное хранение и сравнение.
4. Этапы формирования системы безопасности и оценка ее состояния.
5. Защита административных интерфейсов с помощью аутентификации и усиление парольной защиты по линиям vty.
6. Системы парольной аутентификации. Централизованное хранение.
7. Виды политик защиты.
8. Многоуровневая система привилегий доступа.
9. Системы парольной аутентификации. CHAP и MS-CHAP.
10. Недостатки системы защиты.
11. Защита связи между маршрутизаторами. Аутентификация протоколов маршрутизации.
12. Системы парольной аутентификации. Kerberos. Управление ключами.
13. Вредоносные программы.
14. Защита конфигурационных файлов маршрутизатора.
15. Системы парольной аутентификации. Этапы аутентификации Kerberos.
16. Типы атак. Разведка и методы противодействия.
17. Управление обновлениями маршрутной информации.
18. Системы с одноразовыми паролями.
19. Типы атак. Несанкционированный доступ и методы противодействия.
20. Настройка локальной аутентификации ААА. Список методов аутентификации.
21. Аутентификация по сертификатам.
22. Типы атак. Блокирование сервиса и методы противодействия.
23. Настройка удаленной аутентификации ААА.
24. Блочное шифрование.
25. Типы атак. Подмена данных сервиса и методы противодействия.
26. Настройка авторизации AAA.
27. Требования к алгоритму шифрования.
28. Защита административного доступа к сетевым устройствам. Защита на уровне физического доступа к устройствам. Защита на уровне административного интерфейса.
29. Настройка аудита ААА.
30. Блочный шифр на основе сетей Фейстеля.
31. Технология защиты ААА. Аутентификация и режимы доступа. Методы аутентификации, авторизации и аудита.
32. Работа и настройка Reflexive IP ACL.
33. Алгоритм DES.
34. Серверы защиты ААА. TACACS+.
35. Работа и настройка Dynamic ACL.
36. Режимы работы алгоритма DES.
37. Серверы защиты ААА. RADIUS.
38. Работа и настройка Time-Based ACL.
39. Тройной DES с двумя ключами.
40. . Классификация вирусов.
41. Задачи и принципы работы CBAC.
42. Преобразования алгоритма Rijndael
43. Особенности алгоритма вирусов.
44. Работа CBAC с TCP и UDP.
45. Алгоритм ГОСТ 28147.
46. Модели обороны.
47. Настройка CBAC.
48. Алгоритм шифрования RSA.
49. Структура защищенной сети.
50. . Этапы настройки IPSec VPN.
51. . Электронная цифровая подпись.
52. Разделение сети на зоны. Элементы зонной структуры.
53. Настройка списка доступа, совместимого с конфигурацией IPSec.
54. Алгоритм DSA.
55. Контроль сервисов TCP/IP.
56. Настройка политики ISAKMP.
57. Шифрование сетевого уровня.
58. Задачи шифрования.
59. Настройка политики ISAKMP. Предустановленные ключи.
60. Принципы работы средств шифрования и применение шифрования.
61. Защита от блокирования сервисов. Защита от синхронных и асинхронных атак.
62. Определение набора преобразований IPSec.
63. Обзор технологии виртуальных частных сетей. Топологии сетей VPN.
64. Создание криптографической карты. Конфигурационные параметры. Правила формирования. Конфигурирование.
65. Протоколы для поддержки VPN.
66. Протоколы IPSec.
67. . Работа IPSec. Начало процесса IPSec Работа IPSec. Первая фаза IKE. Энергичный режим.
68. Работа IPSec. Вторая фаза IKE. Передача данных. Завершение работы туннеля IPSec.