1. Выберите правильный вариант ответа: Что в контексте кибериммунитета означает «устойчивость по умолчанию»?

2. Выберите правильный вариант ответа: Какую основную функцию выполняет протокол TLS при обеспечении кибериммунитета?

3. Выберите правильный вариант ответа: Какой протокол преимущественно используют для построения защищённых туннелей на сетевом уровне?

4. Выберите правильный вариант ответа: Какой принцип наиболее соответствует архитектуре кибериммунитета?

5. Выберите правильный вариант ответа: Какой протокол аутентификации чаще всего используется совместно с 802.1X для контроля доступа в сети?

6. Выберите правильный вариант ответа: Какая характеристика наилучше описывает кибериммунную систему?

7. Выберите правильный вариант ответа: Какой протокол используют для безопасного управления сетевыми устройствами вместо Telnet?

8. Выберите правильный вариант ответа: Какая задача наиболее характерна для DNSSEC?

9. Выберите правильный вариант ответа: Какой протокол чаще всего используют для защиты маршрутизируемых каналов между площадками организации?

10. Выберите правильный вариант ответа: Какой тип атаки прежде всего снижает кибериммунитет на уровне маршрутизации?

11. Выберите правильный вариант ответа: Какой протокол обеспечивает безопасную передачу веб трафика поверх незащищённой сети?

12. Выберите правильный вариант ответа: Какой механизм чаще всего применяют для криптографической защиты трафика в IPsec?

13. Выберите правильный вариант ответа: Какой протокол предназначен для защищённой передачи файлов по аналогии с FTP?

14. Выберите правильный вариант ответа: Какой принцип управления доступом лучше всего поддерживает кибериммунитет?

15. Выберите правильный вариант ответа: Какой протокол применяют для многофакторной аутентификации и единого входа в доменной инфраструктуре?

16. Выберите правильный вариант ответа: Какой метод защиты трафика наиболее характерен для кибериммунной сети на канальном уровне?

17. Выберите правильный вариант ответа: Какая особенность кибериммунной архитектуры снижает ценность успешной атаки?

18. Выберите правильный вариант ответа: Какой протокол чаще всего применяют для защищённого удалённого администрирования серверов?

19. Выберите правильный вариант ответа: Для чего в кибериммунной сети применяют протоколы синхронизации времени (например, NTP с аутентификацией)?

20. Выберите правильный вариант ответа: Какой тип трафика в первую очередь должен быть защищён при проектировании кибериммунной сети управления технологическим процессом?

21. Выберите правильный вариант ответа: Какой протокол чаще всего используют для безопасного доступа к почтовому ящику пользователя?

22. Выберите правильный вариант ответа: Чем протокол SNMPv3 принципиально отличается от SNMPv1 с точки зрения кибериммунитета?

23. Выберите правильный вариант ответа: Какой механизм чаще всего используют для защиты от подмены маршрута в протоколе BGP?

24. Выберите правильный вариант ответа: Какой протокол чаще всего применяют для защищённой передачи данных датчиков Интернета вещей?

25. Выберите правильный вариант ответа: Какая технология лучше всего поддерживает реализацию принципа «Zero Trust» в корпоративной сети?

26. Выберите все корректные характеристики кибериммунной системы:

27. Какие протоколы относятся к защищённым протоколам удалённого доступа и администрирования?

28. Какие протоколы чаще всего используют для создания VPN туннелей в архитектуре кибериммунной сети?

29. Какие механизмы в первую очередь обеспечивают целостность и подлинность данных в защищённых сетевых протоколах?

30. Какие протоколы непосредственно поддерживают концепцию «защищённого канала связи» между клиентом и сервером?

31. Какие меры следует применить к DNS инфраструктуре для повышения уровня кибериммунитета сети?

32. Какие протоколы и технологии чаще всего применяют для аутентификации устройств и пользователей при доступе в проводную или беспроводную сеть?

33. Какие свойства трафика защищает протокол IPsec в режиме туннелирования при корректной настройке?

34. Какие протоколы можно использовать для безопасной передачи файлов в кибериммунной инфраструктуре?

35. Какие свойства архитектуры сети способствуют кибериммунитету?

36. Какие протоколы или механизмы помогают повысить защищённость маршрутизации в больших сетях?

37. Какие действия относятся к принципам «Zero Trust» в сетевой архитектуре?

38. Какие протоколы используют криптографию с открытым ключом в процессе установления защищённого соединения?

39. Какие дополнительные механизмы усиливают кибериммунитет при использовании протокола HTTPS в веб приложениях?

40. Какие протоколы могут использоваться для защиты трафика промышленных систем управления?

41. Какие меры по управлению ключами критичны для кибериммунных сетевых протоколов?

42. Какие протоколы чаще всего используют для безопасного доступа пользователей к корпоративным приложениям через Интернет?

43. Какие особенности журналирования сетевых событий необходимы для поддержки кибериммунитета?

44. Какие протоколы чаще всего используют для безопасной работы с каталогами пользователей и служб?

45. Какие уровни модели сетевого взаимодействия в наибольшей степени задействованы в реализации защищённых туннелей?

46. Какие элементы архитектуры помогают ограничить распространение атаки внутри кибериммунной сети?

47. Какие протоколы и механизмы можно использовать для защиты беспроводных сетей в концепции кибериммунитета?

48. Какие протоколы и технологии применяют для безопасной интеграции облачных сервисов в кибериммунную архитектуру организации?

49. Какие протоколы и механизмы особенно важны для защиты каналов управления устройствами Интернета вещей?

50. Установите правильную последовательность этапов установления защищённого соединения TLS:

51. Установите правильную последовательность действий при проектировании кибериммунной сетевой архитектуры:

52. Установите правильную последовательность обработки пакета межсетевым экраном с глубокой проверкой:

53. Установите правильную последовательность действий при настройке защищённого удалённого доступа администратора:

54. Установите правильную последовательность этапов реагирования на сетевой инцидент в кибериммунной архитектуре:

55. Установите правильную последовательность внедрения защиты маршрутизации с использованием криптографических механизмов:

56. Установите правильный порядок действий при внедрении 802.1X для доступа в проводную сеть:

57. Установите правильную последовательность этапов построения защищённого VPN канала между двумя площадками:

58. Установите правильную последовательность действий при создании кибериммунной зоны для промышленных систем управления:

59. Установите правильную последовательность этапов управления ключами для защищённых сетевых протоколов:

60. Установите соответствие между протоколом и основной функцией в кибериммунной сети:

61. Установите соответствие между протоколом и типичной областью применения:

62. Установите соответствие между протоколом и уровнем, на котором он преимущественно работает: