Тема 2

1. **Атака, позволяющая перехватить поток передаваемых данных, которыми обмениваются компоненты сетевой ОС называется:**
    a. Подмена доверенного объекта или субъекта распределенной вычислительной сети
    b. Использование ошибок конфигурации сетевого оборудования
    c. Отказ в обслуживании

ПК-27.1. Атака, позволяющая перехватить поток передаваемых данных, которыми обмениваются компоненты сетевой ОС называется: (Множественный выбор / Только один ответ)

---

2. **Атака, результатом осуществления которой может стать нарушение работоспособности соответствующей службы предоставления удаленного доступа на атакуемый хост называется:**
    a. Подмена доверенного объекта или субъекта распределенной вычислительной сети
    b. Удаленный контроль над станцией в сети
    c. Отказ в обслуживании

ПК-27.1. Атака, результатом осуществления которой может стать нарушение работоспособности соответствующей службы предоставления удаленного доступа на атакуемый хост называется: (Множественный выбор / Только один ответ)

---

3. **К внутренним нарушителям информационной безопасности относятся**
    a. Клиенты
    b. Любые лица, находящиеся внутри контролируемой территории
    c. Посетители

ПК-27.1. К внутренним нарушителям информационной безопасности относятся (Множественный выбор / Только один ответ)

---

4. **К этапу определения объектов воздействия, описанной в "Методике оценки угроз безопасности информации", не относят:**
    a. Анализ документации систем и сетей
    b. Инвентаризацию сетей и систем
    c. Оценку способов реализации угроз

ПК-27.1. К этапу определения объектов воздействия, описанной в "Методике оценки угроз безопасности информации", не относят: (Множественный выбор / Только один ответ)

---

5. **Какому аспекту информационной безопасности угрожает чрезмерная интенсивность запросов к информационному ресурсу?**
    a. Целостности
    b. Доступности
    c. Конфиденциальности

ПК-27.1. Какому аспекту информационной безопасности угрожает чрезмерная интенсивность запросов к информационному ресурсу? (Множественный выбор / Только один ответ)

---

6. **На этапе эксплуатации систем и сетей результаты оценки угроз безопасности информации должны быть направлены на оценку:**

a. Эффективности принятых технических мер, в том числе используемых средств защиты информации
b. Стоимости принятых технических мер, в том числе используемых средств защиты информации
c. Времени передачи информации с использованием принятых технических мер, в том числе используемых средств защиты информации

ПК-27.1. На этапе эксплуатации систем и сетей результаты оценки угроз безопасности информации должны быть направлены на оценку: (Множественный выбор / Только один ответ)

---

7. **Основными задачами, решаемыми в ходе оценки угроз безопасности информации, являются**
   a. Определение негативных последствий, которые могут наступить от реализации (возникновения) угроз безопасности информации
   b. Обеспечение заданного уровня криптографического закрытия информации
   c. Обеспечение заданного уровня защиты от помех и контроля помехоустойчивости

ПК-27.1. Основными задачами, решаемыми в ходе оценки угроз безопасности информации, являются: (Множественный выбор / Только один ответ)

---

8. **Оценка угроз безопасности информации в системах и сетях, функционирующих с использованием "облачных технологий" осуществляется:**
   a. С учетом состава и содержания услуг, предоставляемых поставщиком услуг (например, инфраструктура как услуга, платформа как сервис, программное обеспечение как сервис)
   b. Без учета состава и содержания услуг, предоставляемых поставщиком услуг (например, инфраструктура как услуга, платформа как сервис, программное обеспечение как сервис)
   c. С учетом только собственной инфраструктуры

ПК-27.1. Оценка угроз безопасности информации в системах и сетях, функционирующих с использованием "облачных технологий" осуществляется: (Множественный выбор / Только один ответ)

---

9. **По условию начала осуществления воздействия удаленные атаки делятся на:**
   a. Условные и безусловные
   b. Атаки с обратной связью и без обратной связи
   c. Внутрисегментные и межсегментные

ПК-27.1. По условию начала осуществления воздействия удаленные атаки делятся на: (Множественный выбор / Только один ответ)

---

10. **По цели воздействия удаленные атаки делятся на:**
    a. Условные и безусловные
    b. Внутрисегментные и межсегментные
    c. Атаки в зависимости от нарушения конфиденциальности, целостности и доступности

ПК-27.1. По цели воздействия удаленные атаки делятся на: (Множественный выбор / Только один ответ)

Тема 3 :: ПК-27.1. На сколько уровней модель OSI разделяет коммуникационные функции: ::На сколько уровней модель OSI

разделяет коммуникационные функции: {~4 =7 ~8}

1. **С помощью какого безопасного способа клиент может подключиться к внутриполосному устройству с целью удаленного мониторинга и администрирования?**
    a. TELNET
    b. HTTP
    c. SSH
    d. HTTPS

    ПК-27. С помощью какого безопасного способа клиент может подключиться к внутриполосному устройству с целью удаленного мониторинга и администрирования? (Множественный выбор / Только один ответ)

---

2. **Атака почтовая бомба позволяет:**
    a. Определить пароль от почтового ящика
    b. Осуществить фишинговую атаку
    c. Осуществить переполнение почтового ящика

    ПК-27.1 Атака почтовая бомба позволяет: (Множественный выбор / Только один ответ)

---

3. **Атака почтовая бомба позволяет:**
    a. Определить пароль от почтового ящика
    b. Осуществить фишинговую атаку
    c. Осуществить переполнение почтового ящика

    ПК-27.1 Атака почтовая бомба позволяет: (Множественный выбор / Только один ответ)

---

4. **В протоколе FTPS для защиты соединения используется:**
    a. SSL
    b. FTP
    c. SSH

    ПК-27.1 В протоколе FTPS для защиты соединения используется: (Множественный выбор / Только один ответ)

---

5. **В протоколе FTPS для защиты соединения используется:**
    a. SSL
    b. FTP
    c. SSH

    ПК-27.1 В протоколе FTPS для защиты соединения используется: (Множественный выбор / Только один ответ)

---

6. **Для чего используется механизм кэширования страниц?**
    a. Обеспечения целостности
    b. Обеспечения доступности
    c. Обеспечения конфиденциальности

    ПК-27.1 Для чего используется механизм кэширования страниц? (Множественный выбор / Только один ответ)

---

7. Для чего используется механизм кэширования страниц?

a. Обеспечения целостности
b. Обеспечения доступности
c. Обеспечения конфиденциальности

ПК-27.1 Для чего используется механизм кэширования страниц? (Множественный выбор / Только один ответ)

---

8. Для чего необходима синхронизация порядковых номеров во время трехстороннего квитирования TCP?

a. Для идентификации приложения, которое является пунктом назначения сегментов
b. Для учета отправленных и подтвержденных сегментов
c. Для обеспечения информации о пункте назначения для сетевых устройств, через которые проходит маршрут
d. Определения утерянных сегментов, которые необходимо передать повторно

ПК-27.1 Для чего необходима синхронизация порядковых номеров во время трехстороннего квитирования TCP? (Множественный выбор)

---

9. Для чего необходима синхронизация порядковых номеров во время трехстороннего квитирования TCP?

a. Для идентификации приложения, которое является пунктом назначения сегментов
b. Для учета отправленных и подтвержденных сегментов
c. Для обеспечения информации о пункте назначения для сетевых устройств, через которые проходит маршрут
d. Определения утерянных сегментов, которые необходимо передать повторно

ПК-27.1 Для чего необходима синхронизация порядковых номеров во время трехстороннего квитирования TCP? (Множественный выбор)

---

10. Подлинность веб-приложения может быть подтверждена:

a. IP-адресом приложения
b. Доменным именем
c. Цифровым сертификатом

ПК-27.1 Подлинность веб-приложения может быть подтверждена: (Множественный выбор / Только один ответ)

---

11. Подлинность веб-приложения может быть подтверждена:

a. IP-адресом приложения
b. Доменным именем
c. Цифровым сертификатом

ПК-27.1 Подлинность веб-приложения может быть подтверждена: (Множественный выбор / Только один ответ)

---

12. Протокол TLS не использует:

a. Симметричную криптографию для аутентификации
b. Симметричное шифрование для конфиденциальности
c. Коды аутентичности сообщений (имитовставку) для контроля целостности данных

ПК-27.1 Протокол TLS не использует: (Множественный выбор / Только один ответ)

---

13. **Протокол TLS не использует:**
    a. Симметричную криптографию для аутентификации
    b. Симметричное шифрование для конфиденциальности
    c. Коды аутентичности сообщений (имитовставку) для контроля целостности данных

ПК-27.1 Протокол TLS не использует: (Множественный выбор / Только один ответ)

---

14. **Укажите неверное определение:**
    a. HTTPS
    b. HTTP + TLS/SSL
    c. HTTPS обеспечивает защиту от атак, основанных на прослушивании, при условии, что сертификат сервера проверен и используется шифрование.
    d. В отличие от HTTP, для HTTPS по умолчанию используется TCP-порт 80

ПК-27.1 Укажите неверное определение: (Множественный выбор / Только один ответ)

---

15. **Укажите неверное определение:**
    a. HTTPS
    b. HTTP + TLS/SSL
    c. HTTPS обеспечивает защиту от атак, основанных на прослушивании, при условии, что сертификат сервера проверен и используется шифрование.
    d. В отличие от HTTP, для HTTPS по умолчанию используется TCP-порт 80

ПК-27.1 Укажите неверное определение: (Множественный выбор / Только один ответ)

---

16. **HTTPS позволяет осуществлять защиту через шифрованные транспортные механизмы используя протокол:**
    a. SSL/TLS
    b. RIP
    c. IPSec

ПК-27.1 HTTPS позволяет осуществлять защиту через шифрованные транспортные механизмы используя протокол: (Множественный выбор / Только один ответ)

---

17. **HTTPS позволяет осуществлять защиту через шифрованные транспортные механизмы используя протокол:**
    a. SSL/TLS
    b. RIP
    c. IPSec

ПК-27.1 HTTPS позволяет осуществлять защиту через шифрованные транспортные механизмы используя протокол: (Множественный выбор / Только один ответ)

---

18. **MD5, используемый при аутентификации является:**
    a. Хэш-функцией
    b. Алгоритмом общего ключа
    c. Алгоритмом секретного ключа

ПК-27.1 MD5, используемый при аутентификации является: (Множественный выбор / Только один ответ)

---

19. **MD5, используемый при аутентификации является:**

a. Хэш-функцией
b. Алгоритмом общего ключа
c. Алгоритмом секретного ключа

ПК-27.1 MD5, используемый при аутентификации является: (Множественный выбор / Только один ответ)

---

20. В протоколе TCP/IP маршрутизация пакетов по межсетевым соединениям реализуется

a. Сеансовом
b. Сетевом
c. Транспортном

ПК-27.1 В протоколе TCP/IP маршрутизация пакетов по межсетевым соединениям реализуется на уровне: (Множественный выбор / Только один ответ)

---

21. В протоколе TCP/IP маршрутизация пакетов по межсетевым соединениям реализуется

a. Сеансовом
b. Сетевом
c. Транспортном

ПК-27.1 В протоколе TCP/IP маршрутизация пакетов по межсетевым соединениям реализуется на уровне: (Множественный выбор / Только один ответ)

---

22. Какая из атак не реализуется в протоколе TCP?

a. Затопление с Ddos
b. Затопление при перегрузке каналов связи
c. Сканирование с установлением флага FIN, SYN, RST, PSH, URG
d. Навязывание ложного маршрутизатора

ПК-27.1 Какая из атак не реализуется в протоколе TCP? (Множественный выбор / Только один ответ)

---

23. Какая из атак не реализуется в протоколе TCP?

a. Затопление с Ddos
b. Затопление при перегрузке каналов связи
c. Сканирование с установлением флага FIN, SYN, RST, PSH, URG
d. Навязывание ложного маршрутизатора

ПК-27.1 Какая из атак не реализуется в протоколе TCP? (Множественный выбор / Только один ответ)

---

24. Какие атаки возможно осуществлять при динамическом изменении скользящего окна?

a. Атака на увеличение размера окна
b. Атака на срочность передачи данных
c. Атака на повторную передачу данных

ПК-27.1 Какие атаки возможно осуществлять при динамическом изменении скользящего окна? (Множественный выбор)

---

25. Какие атаки возможно осуществлять при динамическом изменении скользящего окна?

a. Атака на увеличение размера окна
b. Атака на срочность передачи данных
c. Атака на повторную передачу данных

ПК-27.1 Какие атаки возможно осуществлять при динамическом изменении скользящего окна? (Множественный выбор)

---

26. Какие протоколы маршрутизации используются в IP-сетях?

a. Протокол IPv4
b. Протокол OSPF
c. Протокол RIP
d. Протокол DHCP
e. Протокол ICMP

ПК-27.1 Какие протоколы маршрутизации используются в IP-сетях? (Множественный выбор)

---

27. Какие протоколы маршрутизации используются в IP-сетях?

a. Протокол IPv4
b. Протокол OSPF
c. Протокол RIP
d. Протокол DHCP
e. Протокол ICMP

ПК-27.1 Какие протоколы маршрутизации используются в IP-сетях? (Множественный выбор)

---

28. Какие протоколы маршрутизации используются для автономных систем?

a. EGP
b. BGP
c. OSPF
d. RIP

ПК-27.1 Какие протоколы маршрутизации используются для автономных систем? (Множественный выбор)

---

29. Какие протоколы маршрутизации используются для автономных систем?

a. EGP
b. BGP
c. OSPF
d. RIP

ПК-27.1 Какие протоколы маршрутизации используются для автономных систем? (Множественный выбор)

---

30. Каковы преимущества и недостатки статической маршрутизации по сравнению с динамической?

a. Статическая маршрутизация обеспечивает более высокий уровень безопасности
b. Сети, использующие статическую маршрутизацию, плохо масштабируемы
c. Статическая маршрутизация обеспечивает более высокий уровень производительности

ПК-27.1 Каковы преимущества и недостатки статической маршрутизации по сравнению с динамической? (Множественный выбор)

---

31. Каковы преимущества и недостатки статической маршрутизации по сравнению с динамической?

a. Статическая маршрутизация обеспечивает более высокий уровень безопасности
b. Сети, использующие статическую маршрутизацию, плохо масштабируемы
c. Статическая маршрутизация обеспечивает более высокий уровень производительности

ПК-27.1 Каковы преимущества и недостатки статической маршрутизации по сравнению с динамической? (Множественный выбор)

---

32. Какой из протоколов не относится к прикладному уровню?

a. ICMP
b. Telnet
c. SMTP

ПК-27.1 Какой из протоколов не относится к прикладному уровню? (Множественный выбор / Только один ответ)

---

33. Какой из протоколов не относится к прикладному уровню?

a. ICMP
b. Telnet
c. SMTP

ПК-27.1 Какой из протоколов не относится к прикладному уровню? (Множественный выбор / Только один ответ)

---

34. На каком уровне стека TCP/IP используется протокол DNS (служба доменных имен)?

a. Прикладном
b. Транспортном
c. Межсетевого взаимодействия

ПК-27.1 На каком уровне стека TCP/IP используется протокол DNS (служба доменных имен)? (Множественный выбор / Только один ответ)

---

35. На каком уровне стека TCP/IP используется протокол DNS (служба доменных имен)?

a. Прикладном
b. Транспортном
c. Межсетевого взаимодействия

ПК-27.1 На каком уровне стека TCP/IP используется протокол DNS (служба доменных имен)? (Множественный выбор / Только один ответ)

---

36. Назначение службы DNS?

a. Разрешение системных имен и их преобразование в IP адреса
b. Синхронизация времени
c. Поддержка функционирования сети

ПК-27.1 Назначение службы DNS? (Множественный выбор / Только один ответ)

---

37. Назначение службы DNS? :: ПК-27. С помощью какого безопасного способа клиент может подключиться к внутриполосному устройству с целью удаленного

мониторинга и администрирования? ::С помощью какого безопасного способа клиент может подключиться к внутриполосному устройству с целью удаленного мониторинга и администрирования? {~TELNET ~HTTP =SSH ~HTTPS}

a. Разрешение системных имен и их преобразование в IP адреса
b. Синхронизация времени
c. Поддержка функционирования сети

ПК-27.1 Назначение службы DNS? (Множественный выбор / Только один ответ)

---

38. Таймер повторной передачи используется:

a. Если нет подтверждения получения сегмента
b. При длительном простое соединения
c. При проверке работоспособность соединения

ПК-27.1 Таймер повторной передачи используется: (Множественный выбор / Только один ответ)

---

39. Таймер повторной передачи используется:

a. Если нет подтверждения получения сегмента
b. При длительном простое соединения
c. При проверке работоспособность соединения

ПК-27.1 Таймер повторной передачи используется: (Множественный выбор / Только один ответ)

---

40. Укажите, почему HTTP не использует шифрование:

a. Шифрование требует больше вычислительных мощностей и передачу больше данных
b. Шифрование бесполезно, поскольку страницы кэшируются
c. Защита от атак на прикладном уровне труднореализуема, поскольку перехват HTTPS-соединений может быть автоматизирован

ПК-27.1 Укажите, почему HTTP не использует шифрование: (Множественный выбор / Только один ответ)

---

41. Укажите, почему HTTP не использует шифрование:

a. Шифрование требует больше вычислительных мощностей и передачу больше данных
b. Шифрование бесполезно, поскольку страницы кэшируются
c. Защита от атак на прикладном уровне труднореализуема, поскольку перехват HTTPS-соединений может быть автоматизирован

ПК-27.1 Укажите, почему HTTP не использует шифрование: (Множественный выбор / Только один ответ)

---

42. Что не содержит заголовок HTTP запроса?

a. Метод запроса
b. URI
c. Версию протокола
d. MIME-подобное сообщение с модификаторами запроса
e. Ключи шифрования

ПК-27.1 Что не содержит заголовок HTTP запроса? (Множественный выбор / Только один ответ)

---

43. Что не содержит заголовок HTTP запроса?

a. Метод запроса
b. URI
c. Версию протокола
d. MIME-подобное сообщение с модификаторами запроса
e. Ключи шифрования

ПК-27.1 Что не содержит заголовок HTTP запроса? (Множественный выбор / Только один ответ)

---

44. DDoS-атака осуществляет нарушение:

a. Целостности
b. Доступности
c. Конфиденциальности

ПК-27.1. DDoS-атака осуществляет нарушение: (Множественный выбор / Только один ответ)

---

45. DDoS-атака осуществляет нарушение:

a. Целостности
b. Доступности
c. Конфиденциальности

ПК-27.1. DDoS-атака осуществляет нарушение: (Множественный выбор / Только один ответ)

---

46. Атака крошечными фрагментами позволяет осуществить нарушение:

a. Целостности
b. Доступности
c. Конфиденциальности

ПК-27.1. Атака крошечными фрагментами позволяет осуществить нарушение: (Множественный выбор / Только один ответ)

---

47. Атака крошечными фрагментами позволяет осуществить нарушение:

a. Целостности
b. Доступности
c. Конфиденциальности

ПК-27.1. Атака крошечными фрагментами позволяет осуществить нарушение: (Множественный выбор / Только один ответ)

---

48. Атака, которая заключается в навязывании ложного маршрута из-за недостатков в алгоритмах маршрутизации:

a. Подмена доверенного объекта или субъекта распределенной вычислительной сети
b. Анализ сетевого трафика
c. Отказ в обслуживании

ПК-27.1. Атака, которая заключается в навязывании ложного маршрута из-за недостатков в алгоритмах маршрутизации: (Множественный выбор / Только один ответ)

---

49. Атака, которая заключается в навязывании ложного маршрута из-за недостатков в алгоритмах маршрутизации:

a. Подмена доверенного объекта или субъекта распределенной вычислительной сети
b. Анализ сетевого трафика
c. Отказ в обслуживании

ПК-27.1. Атака, которая заключается в навязывании ложного маршрута из-за недостатков в алгоритмах маршрутизации: (Множественный выбор / Только один ответ)

---

50. Атака, которая может быть предпринята, если нет средств аутентификации адреса отправителя и с хоста на атакуемый хост можно передавать бесконечное число анонимных запросов на подключение от имени других хостов называется:

a. Подмена доверенного объекта
b. Ложный объект распределенной вычислительной сети
c. Отказ в обслуживании

ПК-27.1. Атака, которая может быть предпринята, если нет средств аутентификации адреса отправителя и с хоста на атакуемый хост можно передавать бесконечное число анонимных запросов на подключение от имени других хостов называется: (Множественный выбор / Только один ответ)

---

51. Атака, которая может быть предпринята, если нет средств аутентификации адреса отправителя и с хоста на атакуемый хост можно передавать бесконечное число анонимных запросов на подключение от имени других хостов называется:

a. Подмена доверенного объекта
b. Ложный объект распределенной вычислительной сети
c. Отказ в обслуживании

ПК-27.1. Атака, которая может быть предпринята, если нет средств аутентификации адреса отправителя и с хоста на атакуемый хост можно передавать бесконечное число анонимных запросов на подключение от имени других хостов называется: (Множественный выбор / Только один ответ)

---

52. В протоколе UDP маршрутизация пакетов по межсетевым соединениям реализуется на уровне:

a. Прикладном
b. Сетевом
c. Транспортном

ПК-27.1. В протоколе UDP маршрутизация пакетов по межсетевым соединениям реализуется на уровне: (Множественный выбор / Только один ответ)

---

53. В протоколе TCP/IP надежную передачу данных реализует уровень:

a. Прикладной
b. Сетевой
c. Транспортный

ПК-27.1. В протоколе UDP маршрутизация пакетов по межсетевым соединениям реализуется на уровне: (Множественный выбор / Только один ответ)

---

54. В протоколе UDP маршрутизация пакетов по межсетевым соединениям реализуется на уровне:

a. Прикладном
b. Сетевом
c. Транспортном

ПК-27.1. В протоколе UDP маршрутизация пакетов по межсетевым соединениям реализуется на уровне: (Множественный выбор / Только один ответ)

55. В протоколе TCP/IP надежную передачу данных реализует уровень:

a. Прикладной
b. Сетевой
c. Транспортный

ПК-27.1. В протоколе UDP маршрутизация пакетов по межсетевым соединениям реализуется на уровне: (Множественный выбор / Только один ответ)

---

56. Выберите утверждение, касающееся команд ping:

a. Команда ping использует MAC-адреса для проверки взаимодействия двух хостов, подключенных к сети
b. Команда ping отображает результат передачи шифрованного трафика
c. Команда ping использует ip-адреса для проверки взаимодействия двух хостов, подключенных к сети

ПК-27.1. Выберите утверждение, касающееся команд ping: (Множественный выбор / Только один ответ)

---

57. Выберите утверждение, касающееся команд ping:

a. Команда ping использует MAC-адреса для проверки взаимодействия двух хостов, подключенных к сети
b. Команда ping отображает результат передачи шифрованного трафика
c. Команда ping использует ip-адреса для проверки взаимодействия двух хостов, подключенных к сети

ПК-27.1. Выберите утверждение, касающееся команд ping: (Множественный выбор / Только один ответ)

---

58. Выберите утверждение, касающееся команд tracert.

a. Команда tracert отображает каждый участок пути, пройденный от отправителя к получателю.
b. Команда tracert использует MAC-адреса для проверки пути между двумя хостами, подключенными к сети
c. Команда tracert отображает количество хостов, подключенных к сети

ПК-27.1. Выберите утверждение, касающееся команд tracert: (Множественный выбор / Только один ответ)

---

59. Выберите утверждение, касающееся команд tracert.

a. Команда tracert отображает каждый участок пути, пройденный от отправителя к получателю.
b. Команда tracert использует MAC-адреса для проверки пути между двумя хостами, подключенными к сети
c. Команда tracert отображает количество хостов, подключенных к сети

ПК-27.1. Выберите утверждение, касающееся команд tracert: (Множественный выбор / Только один ответ)

---

60. Выбрать правильное расположение уровней модели OSI от 7 до 1

a. Прикладной, канальный, представительский, сеансовый, транспортный, сетевой, физический
b. Прикладной, представительский, сеансовый, транспортный, сетевой, канальный, физический
c. Представительский, прикладной, сеансовый, транспортный, сетевой, канальный, физический

ПК-27.1. Выбрать правильное расположение уровней модели OSI от 7 до 1 (Множественный выбор / Только один ответ)

---

61. Выбрать правильное расположение уровней модели OSI от 7 до 1

a. Прикладной, канальный, представительский, сеансовый, транспортный, сетевой, физический
b. Прикладной, представительский, сеансовый, транспортный, сетевой, канальный, физический
c. Представительский, прикладной, сеансовый, транспортный, сетевой, канальный, физический

ПК-27.1. Выбрать правильное расположение уровней модели OSI от 7 до 1 (Множественный выбор / Только один ответ)

---

62. Гарантированную передачу данных согласно модели OSI обеспечивает:

a. Сетевой уровень
b. Транспортный уровень
c. Уровень представления

ПК-27.1. Гарантированную передачу данных согласно модели OSI обеспечивает: (Множественный выбор / Только один ответ)

---

63. Гарантированную передачу данных согласно модели OSI обеспечивает:

a. Сетевой уровень
b. Транспортный уровень
c. Уровень представления

ПК-27.1. Гарантированную передачу данных согласно модели OSI обеспечивает: (Множественный выбор / Только один ответ)

---

64. Главная функция прикладного уровня

a. Синхронизация взаимодействия прикладных процессов
b. Обеспечение работы с синтаксисом данных
c. Определение структур команд

ПК-27.1. Главная функция прикладного уровня (Множественный выбор / Только один ответ)

---

65. Главная функция прикладного уровня

a. Синхронизация взаимодействия прикладных процессов
b. Обеспечение работы с синтаксисом данных
c. Определение структур команд

ПК-27.1. Главная функция прикладного уровня (Множественный выбор / Только один ответ)

---

66. Для преобразования MAC адресов в IP используют протокол:

a. IP
b. ICMP
c. ARP
d. DCHP

ПК-27.1. Для преобразования MAC адресов в IP используют протокол: (Множественный выбор / Только один ответ)

67. Для преобразования MAC адресов в IP используют протокол:

a. IP
b. ICMP
c. ARP
d. DCHP

ПК-27.1. Для преобразования MAC адресов в IP используют протокол: (Множественный выбор / Только один ответ)

---

68. Для сети с маской 255.255.255.0 соответствующий блок адресного пространства конечных хостов составит…

a. 255
b. 4
c. 600

ПК-27.1. Для сети с маской 255.255.255.0 соответствующий блок адресного пространства конечных хостов составит… (Множественный выбор / Только один ответ)

---

69. Для сети с маской 255.255.255.0 соответствующий блок адресного пространства конечных хостов составит…

a. 255
b. 4
c. 600

ПК-27.1. Для сети с маской 255.255.255.0 соответствующий блок адресного пространства конечных хостов составит… (Множественный выбор / Только один ответ)

---

70. Для сокрытия в сети IP адресов используются механизм:

a. Туннелирования
b. Фрагментации
c. Декапсуляции

ПК-27.1. Для сокрытия в сети IP адресов используются механизм: (Множественный выбор / Только один ответ)

---

71. Для сокрытия в сети IP адресов используются механизм:

a. Туннелирования
b. Фрагментации
c. Декапсуляции

ПК-27.1. Для сокрытия в сети IP адресов используются механизм: (Множественный выбор / Только один ответ)

---

72. Единица данных, которой оперирует прикладной уровень, называется:

a. Пакетом
b. Сообщением
c. Потоком

ПК-27.1. Единица данных, которой оперирует прикладной уровень, называется: (Множественный выбор / Только один ответ)

---

73. Единица данных, которой оперирует прикладной уровень, называется:

a. Пакетом
b. Сообщением
c. Потоком

ПК-27.1. Единица данных, которой оперирует прикладной уровень, называется: (Множественный выбор / Только один ответ)

---

74. Если MTU сети меньше размера пакета, то:

a. Маршрутизатор отбрасывает пакет, получателю отправляется ICMP с кодом ошибки
b. Маршрутизатор буферизирует пакеты для дальнейшей сборки
c. Маршрутизатор пропускает пакет

ПК-27.1. Если MTU сети меньше размера пакета, то: (Множественный выбор / Только один ответ)

---

75. Если MTU сети меньше размера пакета, то:

a. Маршрутизатор отбрасывает пакет, получателю отправляется ICMP с кодом ошибки
b. Маршрутизатор буферизирует пакеты для дальнейшей сборки
c. Маршрутизатор пропускает пакет

ПК-27.1. Если MTU сети меньше размера пакета, то: (Множественный выбор / Только один ответ)

---

76. К командам позволяющим осуществлять сканирования сети относят:

a. ping
b. traceroute
c. ipconfig

ПК-27.1. К командам позволяющим осуществлять сканирования сети относят: (Множественный выбор / Только один ответ)

---

77. К основным функциям ICMP не относят: :: ПК-27.1. К командам позволяющим осуществлять сканирования сети относят: ::К командам позволяющим осуществлять сканирования сети относят: {= ping ~traceroute ~ipconfig}

a. Оповещение об ошибках на сетевом уровне
b. Тестирование работоспособности сети
c. Обеспечение маршрутизации пакетов

ПК-27.1. К основным функциям ICMP не относят: (Множественный выбор / Только один ответ)

---

78. К основным функциям ICMP не относят:

a. Оповещение об ошибках на сетевом уровне
b. Тестирование работоспособности сети
c. Обеспечение маршрутизации пакетов

ПК-27.1. К основным функциям ICMP не относят: (Множественный выбор / Только один ответ)

---

79. К характеристикам функционирования физического и канального уровней модели OSI не относится...

a. Пропускная способность Количество ошибок за единицу времени
b. Использование механизмов принудительной передачи данных

ПК-27.1. К характеристикам функционирования физического и канального уровней модели OSI не относится: (Множественный выбор / Только один ответ)

---

80. К характеристикам функционирования физического и канального уровней модели OSI не относится...

a. Пропускная способность Количество ошибок за единицу времени
b. Использование механизмов принудительной передачи данных

ПК-27.1. К характеристикам функционирования физического и канального уровней модели OSI не относится: (Множественный выбор / Только один ответ)

---

81. Какие транспортные протоколы используют подтверждение доставки пакетов? :: ПК-27.1. Что не относится к сервисам протокола TCP: ::Что не относится к сервисам протокола TCP: {~Нумерация сообщений ~Подтверждение получения сообщения ~Повторная отправка при отсутствии подтверждения =Построение наикратчайшего пути маршрута продвижения пакета}

a. TCP
b. UDP
c. OSPF

ПК-27.1. Какие транспортные протоколы используют подтверждение доставки пакетов? (Множественный выбор / Только один ответ)

---

82. Какие транспортные протоколы используют подтверждение доставки пакетов?

a. TCP
b. UDP
c. OSPF

ПК-27.1. Какие транспортные протоколы используют подтверждение доставки пакетов? (Множественный выбор / Только один ответ)

---

83. Какие три типа сетевых документов должен заполнить специалист, прежде чем проектировать новую сеть?

a. Лист инструкций {
b. Отчет об обследовании объекта
c. Лист стандартов {
d. Карты топологии

ПК-27.1. Какие три типа сетевых документов должен заполнить специалист, прежде чем проектировать новую сеть? (Множественный выбор)

---

84. Какие три типа сетевых документов должен заполнить специалист, прежде чем проектировать новую сеть?

a. Лист инструкций {
b. Отчет об обследовании объекта
c. Лист стандартов {
d. Карты топологии

ПК-27.1. Какие три типа сетевых документов должен заполнить специалист, прежде чем проектировать новую сеть? (Множественный выбор)

---

85. Какие элементы данных можно получить, используя команду ipconfig?

a. IP-адрес
b. Сервер DHCP
c. Сервер DNS
d. Маска подсети

ПК-27.1. Какие элементы данных можно получить, используя команду ipconfig? (Множественный выбор)

---

86. Какие элементы данных можно получить, используя команду ipconfig?

a. IP-адрес
b. Сервер DHCP
c. Сервер DNS
d. Маска подсети

ПК-27.1. Какие элементы данных можно получить, используя команду ipconfig? (Множественный выбор)

---

87. Какова цель присвоения IP-адреса интерфейсу VLAN1 на коммутаторе?

a. Для получения доступа к коммутатору с целью управления и конфигурирования
b. Для создания локальной сети с новым IP на коммутаторе
c. Для продления коммутации с новым IP-адресом

ПК-27.1. Какова цель присвоения IP-адреса интерфейсу VLAN1 на коммутаторе? (Множественный выбор / Только один ответ)

---

88. Какова цель присвоения IP-адреса интерфейсу VLAN1 на коммутаторе?

a. Для получения доступа к коммутатору с целью управления и конфигурирования
b. Для создания локальной сети с новым IP на коммутаторе
c. Для продления коммутации с новым IP-адресом

ПК-27.1. Какова цель присвоения IP-адреса интерфейсу VLAN1 на коммутаторе? (Множественный выбор / Только один ответ)

---

89. Какое утверждение описывает результат ввода команды ip route 0.0.0.0 0.0.0.0 192.168.1.1 в маршрутизаторе?

a. Маршрутизатор не может достичь сети 192.168.1.0
b. Все пакеты, полученные маршрутизатором, отправляются на адрес 192.168.1.1
c. Доступ к удаленной сети 192.168.1.0 можно получить с помощью любого интерфейса
d. Статический маршрутизатор по умолчанию добавляется в таблицу маршрутизации

ПК-27.1. Какое утверждение описывает результат ввода команды ip route 0.0.0.0 0.0.0.0 192.168.1.1 в маршрутизаторе? (Множественный выбор / Только один ответ)

---

90. Какое утверждение описывает результат ввода команды ip route 0.0.0.0 0.0.0.0 192.168.1.1 в маршрутизаторе?

a. Маршрутизатор не может достичь сети 192.168.1.0
b. Все пакеты, полученные маршрутизатором, отправляются на адрес 192.168.1.1
c. Доступ к удаленной сети 192.168.1.0 можно получить с помощью любого интерфейса
d. Статический маршрутизатор по умолчанию добавляется в таблицу маршрутизации

ПК-27.1. Какое утверждение описывает результат ввода команды ip route 0.0.0.0 0.0.0.0 192.168.1.1 в маршрутизаторе? (Множественный выбор / Только один ответ)

---

91. Какое утверждение точно описывают таблицу ARP?

a. Таблица ARP содержит информацию о сетях
b. Таблица ARP содержит информацию об устройствах, подключенных к сетям
c. Таблица ARP содержит информации о отражении адресации канального на сетевой

ПК-27.1. Какое утверждение точно описывают таблицу ARP? (Множественный выбор / Только один ответ)

---

92. Какое утверждение точно описывают таблицу ARP?

a. Таблица ARP содержит информацию о сетях
b. Таблица ARP содержит информацию об устройствах, подключенных к сетям
c. Таблица ARP содержит информации о отражении адресации канального на сетевой

ПК-27.1. Какое утверждение точно описывают таблицу ARP? (Множественный выбор / Только один ответ)

---

93. Какой из представленных адресов является конечным MAC-адресом широковещательного кадра Ethernet?

a. 255.255.255.255
b. AA-AA-AA-AA-AA-AA
c. FF-FF-FF-FF-FF-FF

ПК-27.1. Какой из представленных адресов является конечным MAC-адресом широковещательного кадра Ethernet? (Множественный выбор / Только один ответ)

---

94. Какой из представленных адресов является конечным MAC-адресом широковещательного кадра Ethernet?

a. 255.255.255.255
b. AA-AA-AA-AA-AA-AA
c. FF-FF-FF-FF-FF-FF

ПК-27.1. Какой из представленных адресов является конечным MAC-адресом широковещательного кадра Ethernet? (Множественный выбор / Только один ответ)

---

95. Какой протокол обеспечивает преобразование логических адресов сетевых устройств в физические адрес?

a. ARP
b. DHCP
c. ICMP

ПК-27.1. Какой протокол обеспечивает преобразование логических адресов сетевых устройств в физические адрес? (Множественный выбор / Только один ответ)

---

96. Какой режим маршрутизатора отображает подсказку router/?

a. Режим глобальной конфигурации
b. Привилегированный режим EXEC
c. Режим настройки
d. Пользовательский режим EXEC
e. Режим конфигурации

ПК-27.1. Какой режим маршрутизатора отображает подсказку router/? (Множественный выбор / Только один ответ)

---

97. Какой режим маршрутизатора отображает подсказку router/?

a. Режим глобальной конфигурации
b. Привилегированный режим EXEC
c. Режим настройки
d. Пользовательский режим EXEC
e. Режим конфигурации

ПК-27.1. Какой режим маршрутизатора отображает подсказку router/? (Множественный выбор / Только один ответ)

---

98. Какой уровень обеспечивает контроль логической связи и контроль доступа к среде:

a. Представительский
b. Прикладной
c. Канальный

ПК-27.1. Какой уровень обеспечивает контроль логической связи и контроль доступа к среде: (Множественный выбор / Только один ответ)

---

99. Какой уровень обеспечивает контроль логической связи и контроль доступа к среде:

a. Представительский
b. Прикладной
c. Канальный

ПК-27.1. Какой уровень обеспечивает контроль логической связи и контроль доступа к среде: (Множественный выбор / Только один ответ)

---

100. Какой уровень управляет потоками данных, преобразует логические сетевые адреса и имена в соответствующие им физические:

a. Сетевой
b. Представительский
c. Транспортный

ПК-27.1. Какой уровень управляет потоками данных, преобразует логические сетевые адреса и имена в соответствующие им физические: (Множественный выбор / Только один ответ)

---

101. Какой уровень управляет потоками данных, преобразует логические сетевые адреса и имена в соответствующие им физические:

a. Сетевой
b. Представительский
c. Транспортный

ПК-27.1. Какой уровень управляет потоками данных, преобразует логические сетевые адреса и имена в соответствующие им физические: (Множественный выбор / Только один ответ)

---

102. Максимальное число переходов на пути к адресату назначения протокола RIP равно:

a. 10,
b. 15,
c. 16,
d. 24

ПК-27.1. Максимальное число переходов на пути к адресату назначения протокола RIP равно: (Множественный выбор / Только один ответ)

103. Максимальное число переходов на пути к адресату назначения протокола RIP равно:

a. 10,
b. 15,
c. 16,
d. 24

ПК-27.1. Максимальное число переходов на пути к адресату назначения протокола RIP равно: (Множественный выбор / Только один ответ)

---

104. На каком из уровней реализуется атака ARP Spoofing?

a. Канальном
b. Физическом
c. Прикладном

ПК-27.1. На каком из уровней реализуется атака ARP Spoofing? (Множественный выбор / Только один ответ)

---

105. На каком из уровней реализуется атака ARP Spoofing?

a. Канальном
b. Физическом
c. Прикладном

ПК-27.1. На каком из уровней реализуется атака ARP Spoofing? (Множественный выбор / Только один ответ)

---

106. На каком уровне сетевой модели OSI целесообразно осуществлять контроль помехоустойчивости:

a. Физическом
b. Канальном
c. Прикладном

ПК-27.1. На каком уровне сетевой модели OSI целесообразно осуществлять контроль помехоустойчивости: (Множественный выбор / Только один ответ)

---

107. На каком уровне сетевой модели OSI целесообразно осуществлять контроль помехоустойчивости:

a. Физическом
b. Канальном
c. Прикладном

ПК-27.1. На каком уровне сетевой модели OSI целесообразно осуществлять контроль помехоустойчивости: (Множественный выбор / Только один ответ)

---

108. Назовите характеристики масштабируемой сети:

a. Чувствительность к нагрузкам при увеличении трафика
b. Сеть содержит модульные устройства, делающие возможным расширение
c. Сеть содержит ограниченное количество оборудования

ПК-27.1. Назовите характеристики масштабируемой сети: (Множественный выбор / Только один ответ)

---

109. Назовите характеристики масштабируемой сети:

a. Чувствительность к нагрузкам при увеличении трафика
b. Сеть содержит модульные устройства, делающие возможным расширение
c. Сеть содержит ограниченное количество оборудования

ПК-27.1. Назовите характеристики масштабируемой сети: (Множественный выбор / Только один ответ)

---

110. Неправильное указание смещение фрагмента при фрагментации пакета ведет?

a. Нарушению конфиденциальности и доступности
b. Нарушению доступности и целостности
c. Нарушению конфиденциальности и работоспособности

ПК-27.1. Неправильное указание смещение фрагмента при фрагментации пакета ведет? (Множественный выбор / Только один ответ)

---

111. Неправильное указание смещение фрагмента при фрагментации пакета ведет?

a. Нарушению конфиденциальности и доступности
b. Нарушению доступности и целостности
c. Нарушению конфиденциальности и работоспособности

ПК-27.1. Неправильное указание смещение фрагмента при фрагментации пакета ведет? (Множественный выбор / Только один ответ)

---

112. Определите последствия применения схемы IP-адресации с использованием смежных адресов?

a. Петля уровня 2
b. Петля маршрутизации
c. Брешь в безопасности

ПК-27.1. Определите последствия применения схемы IP-адресации с использованием смежных адресов? (Множественный выбор / Только один ответ)

---

113. Определите последствия применения схемы IP-адресации с использованием смежных адресов?

a. Петля уровня 2
b. Петля маршрутизации
c. Брешь в безопасности

ПК-27.1. Определите последствия применения схемы IP-адресации с использованием смежных адресов? (Множественный выбор / Только один ответ)

---

114. Откуда маршрутизатор получает информацию об оптимальном маршруте для отправки пакета, предназначенного для узла, расположенного в удаленной сети?

a. Из таблицы маршрутизации, сохраненной в оперативной памяти
b. Из файла конфигурации, сохраненного в оперативной памяти
c. Из передаваемого IP-пакета

ПК-27.1. Откуда маршрутизатор получает информацию об оптимальном маршруте для отправки пакета, предназначенного для узла, расположенного в удаленной сети? (Множественный выбор / Только один ответ)

---

115. Откуда маршрутизатор получает информацию об оптимальном маршруте для отправки пакета, предназначенного для узла, расположенного в удаленной сети?

a. Из таблицы маршрутизации, сохраненной в оперативной памяти
b. Из файла конфигурации, сохраненного в оперативной памяти
c. Из передаваемого IP-пакета

ПК-27.1. Откуда маршрутизатор получает информацию об оптимальном маршруте для отправки пакета, предназначенного для узла, расположенного в удаленной сети? (Множественный выбор / Только один ответ)

---

116. Перечислите особенность, не относящуюся к протоколу ICMP:

a. Протокол не требует номера портов для работы;
b. Протокол не посылает сообщение об ошибке в ответ на полученное, тем самым не загружая сеть;
c. Для фрагментированных дейтограмм сообщение протокола посылается только для первого фрагмента ICMP
d. Устанавливает надежное соединение для передачи сообщения об ошибках

ПК-27.1. Перечислите особенность, не относящуюся к протоколу ICMP: (Множественный выбор / Только один ответ)

---

117. Перечислите особенность, не относящуюся к протоколу ICMP:

a. Протокол не требует номера портов для работы;
b. Протокол не посылает сообщение об ошибке в ответ на полученное, тем самым не загружая сеть;
c. Для фрагментированных дейтограмм сообщение протокола посылается только для первого фрагмента ICMP
d. Устанавливает надежное соединение для передачи сообщения об ошибках

ПК-27.1. Перечислите особенность, не относящуюся к протоколу ICMP: (Множественный выбор / Только один ответ)

---

118. Почему во время разработки структурированной кабелепроводки очень важно получить точный поэтажный план?

a. Для проектирования адресации уровня 3
b. Для определения возможных местоположений коммутационных отсеков
c. Для определения необходимого количества хост-устройств
d. Во избежание участков с электрооборудованием или проводкой

ПК-27.1. Почему во время разработки структурированной кабелепроводки очень важно получить точный поэтажный план? (Множественный выбор)

---

119. Почему во время разработки структурированной кабелепроводки очень важно получить точный поэтажный план?

a. Для проектирования адресации уровня 3
b. Для определения возможных местоположений коммутационных отсеков
c. Для определения необходимого количества хост-устройств
d. Во избежание участков с электрооборудованием или проводкой

ПК-27.1. Почему во время разработки структурированной кабелепроводки очень важно получить точный поэтажный план? (Множественный выбор)

---

120. При какой передаче прикладные процессы будут передавать данные, и принимать их одновременно?

a. Дуплексная передача
b. Полудуплексная передача
c. Многоканальное соединение

ПК-27.1. При какой передаче прикладные процессы будут передавать данные, и принимать их одновременно? (Множественный выбор / Только один ответ)

---

121. При какой передаче прикладные процессы будут передавать данные, и принимать их одновременно?

a. Дуплексная передача
b. Полудуплексная передача
c. Многоканальное соединение

ПК-27.1. При какой передаче прикладные процессы будут передавать данные, и принимать их одновременно? (Множественный выбор / Только один ответ)

---

122. Протокол TCP обеспечивает:

a. Дуплексную передачу данных
b. Полудуплексную передачу данных
c. Многоканальное соединение

ПК-27.1. Протокол TCP обеспечивает: (Множественный выбор / Только один ответ)

---

123. Протокол TCP обеспечивает:

a. Дуплексную передачу данных
b. Полудуплексную передачу данных
c. Многоканальное соединение

ПК-27.1. Протокол TCP обеспечивает: (Множественный выбор / Только один ответ)

---

124. С помощью какой команды, введенной на основном маршрутизаторе, можно получить необходимую информацию для определения и регистрации всех сетевых устройств Cisco, присоединенных к главному маршрутизатору? :: ПК-27.1. Какой протокол обеспечивает преобразование логических адресов сетевых устройств в физические адрес? ::Какой протокол обеспечивает преобразование логических адресов сетевых устройств в физические адрес? {=ARP ~DHCP ~ICMP}

a. show version
b. show
c. show tech-support
d. show running-config
e. show cdp neighbors detail

ПК-27.1. С помощью какой команды, введенной на основном маршрутизаторе, можно получить необходимую информацию для определения и регистрации всех сетевых устройств Cisco, присоединенных к главному маршрутизатору? (Множественный выбор / Только один ответ)

---

125. С помощью какой команды, введенной на основном маршрутизаторе, можно получить необходимую информацию для определения и регистрации всех сетевых устройств Cisco, присоединенных к главному маршрутизатору?

a. show version
b. show
c. show tech-support
d. show running-config

e. show cdp neighbors detail

ПК-27.1. С помощью какой команды, введенной на основном маршрутизаторе, можно получить необходимую информацию для определения и регистрации всех сетевых устройств Cisco, присоединенных к главному маршрутизатору? (Множественный выбор / Только один ответ)

---

126. Сетевой уровень модели OSI не обеспечивает…

a. Определение сетевых адресов
b. Маршрутизацию пакетов
c. Фрагментацию пакетов
d. Гарантию доставки пакетов

ПК-27.1. Сетевой уровень модели OSI не обеспечивает… (Множественный выбор / Только один ответ)

---

127. Сетевой уровень модели OSI не обеспечивает…

a. Определение сетевых адресов
b. Маршрутизацию пакетов
c. Фрагментацию пакетов
d. Гарантию доставки пакетов

ПК-27.1. Сетевой уровень модели OSI не обеспечивает… (Множественный выбор / Только один ответ)

---

128. Сканирование портов позволяет:

a. Подменять доверенный объект или субъект распределенной вычислительной сети
b. Осуществлять анализ сетевого трафика
c. Оценить программное обеспечение, установленное на хост

ПК-27.1. Сканирование портов позволяет: (Множественный выбор / Только один ответ)

---

129. Сканирование портов позволяет:

a. Подменять доверенный объект или субъект распределенной вычислительной сети
b. Осуществлять анализ сетевого трафика
c. Оценить программное обеспечение, установленное на хост

ПК-27.1. Сканирование портов позволяет: (Множественный выбор / Только один ответ)

---

130. Укажите команду, которую необходимо выполнить при тестировании соединений между хостами в сети:

a. msconfig
b. ping
c. netstat
d. nslookup

ПК-27.1. Укажите команду, которую необходимо выполнить при тестировании соединений между хостами в сети: (Множественный выбор / Только один ответ)

---

131. Укажите команду, которую необходимо выполнить при тестировании соединений между хостами в сети:

a. msconfig
b. ping
c. netstat

d. nslookup

ПК-27.1. Укажите команду, которую необходимо выполнить при тестировании соединений между хостами в сети: (Множественный выбор / Только один ответ)

---

132. Уничтожение пакета в маршрутизаторе возникает при значении метрики протокола RIP равным:

a. 10,
b. 15,
c. 16,
d. 24

ПК-27.1. Уничтожение пакета в маршрутизаторе возникает при значении метрики протокола RIP равным: (Множественный выбор / Только один ответ)

---

133. Уничтожение пакета в маршрутизаторе возникает при значении метрики протокола RIP равным:

a. 10,
b. 15,
c. 16,
d. 24

ПК-27.1. Уничтожение пакета в маршрутизаторе возникает при значении метрики протокола RIP равным: (Множественный выбор / Только один ответ)

---

134. Что не относится к сервисам протокола TCP:

a. Нумерация сообщений
b. Подтверждение получения сообщения
c. Повторная отправка при отсутствии подтверждения
d. Построение наикратчайшего пути маршрута продвижения пакета

ПК-27.1. Что не относится к сервисам протокола TCP: (Множественный выбор / Только один ответ)

---

135. Что такое горизонт сходимости?

a. Время для настройки маршрутизации администратором
b. Время передачи сообщения от источника узлу назначения
c. Время согласования таблиц маршрутизации при изменении топологии сети
d. Время включения протокола маршрутизации в работу

ПК-27.1. Что такое горизонт сходимости? (Множественный выбор)

---

136. Что такое горизонт сходимости?

a. Время для настройки маршрутизации администратором
b. Время передачи сообщения от источника узлу назначения
c. Время согласования таблиц маршрутизации при изменении топологии сети
d. Время включения протокола маршрутизации в работу

ПК-27.1. Что такое горизонт сходимости? (Множественный выбор)

Тема 8 :: ПК-27.1 Протокол WEP позволяет осуществить защиту соединения, реализованного по технологии: ::Протокол WEP позволяет осуществить защиту соединения, реализованного по технологии: {=Wi-fi ~Ethernet ~Bluetooth}

1. **IV относится к:**
    a. Вектору инициализации
    b. Вектору аутентификации
    c. Вектору кодирования

    ПК-27.1 IV относится к: (Множественный выбор / Только один ответ)

---

2. **MIC в WPA определяет:**
    a. Процесс генерации ключей
    b. Контроль целостности сообщений
    c. Контроль конфиденциальности данных

    ПК-27.1 MIC в WPA определяет: (Множественный выбор / Только один ответ)

---

3. **RC4 относится к:**
    a. Симметричному потоковому шифрованию
    b. Блочному шифрованию
    c. Несимметричному блочному шифрованию

    ПК-27.1 RC4 относится к: (Множественный выбор / Только один ответ)

---

4. **SSID представляет собой атрибут беспроводной сети, позволяющий:**
    a. Отличать станции одной сети друг от друга посредством используемого оборудования
    b. Отличать сети друг от друга
    c. Отличать станции, подключенные к сети

    ПК-27.1 SSID представляет собой атрибут беспроводной сети, позволяющий: (Множественный выбор / Только один ответ)

---

5. **Атака на секретный ключ шифрования WEP реализуется с использованием:**
    a. Определенных фреймов, пассивно собранных в беспроводной локальной сети
    b. Метода перебора ключевой последовательности
    c. Фреймов, собранных только по MAC адресу отправителя

    ПК-27.1 Атака на секретный ключ шифрования WEP реализуется с использованием: (Множественный выбор / Только один ответ)

---

6. **Аутентификация с использованием WEP подвержена:**
    a. Атакам человек посередине

b. Ddos атакам
c. Атакам с использованием механизма WPS

ПК-27.1 Аутентификация с использованием WEP подвержена: (Множественный выбор / Только один ответ)

---

7. Базовый режим точки доступа используется для:
a. Подключения к ней удаленных роутеров
b. Подключения к ней станций
c. Обнаружения соседних беспроводных сетей

ПК-27.1 Базовый режим точки доступа используется для: (Множественный выбор / Только один ответ)

---

8. В сетях 802.11 уровень MAC обеспечивает режимы доступа к разделяемой среде:
a. Режим DCF
b. Режим MCF
c. Режим ECF

ПК-27.1 Базовый режим точки доступа используется для: (Множественный выбор / Только один ответ)

---

9. Большинство беспроводных сетевых технологий использует:
a. Частоту передачи, требующую лицензирования
b. Частоту передачи, не требующую лицензирования
c. Очень узкий промежуток специально зарезервированных лицензированных частот

ПК-27.1 Большинство беспроводных сетевых технологий использует: (Множественный выбор / Только один ответ)

---

10. В каком случае подлинность клиента считается установленной, если в точке доступа включена только фильтрация MAC-адресов?
a. Если клиент предоставляет правильный секретный ключ для точки доступа
b. Если клиент отправляет в точку доступа MAC-адрес
c. Если точка доступа проверяет наличие соответствующего MAC-адреса в таблице MAC-адресов и отправляет клиенту сообщение с подтверждением

ПК-27.1 В каком случае подлинность клиента считается установленной, если в точке доступа включена только фильтрация MAC-адресов? (Множественный выбор / Только один ответ)

---

11. В каком случае подлинность клиента считается установленной, если в точке доступа включена только фильтрация MAC-адресов?
a. Если точка доступа проверяет наличие соответствующего MAC-адреса в таблице MAC-адресов и отправляет клиенту сообщение с подтверждением
b. Если точка доступа отправляет MAC-адрес на сервер и получает уведомление о том, что данный MAC-адрес является действительным
c. Если точка доступа проверяет наличие соответствующего MAC-адреса в таблице MAC-адресов и запрашивает IP адрес пользователя

ПК-27.1 В каком случае подлинность клиента считается установленной, если в точке доступа включена только фильтрация MAC-адресов? (Множественный выбор / Только один ответ)

---

12. В спящем режиме станция не принимает и не передает данные для:
a. Уменьшения атак на станцию

b. Экономии заряда устройства
c. Передачи канала связи другим устройствам

ПК-27.1 В спящем режиме станция не принимает и не передает данные для: (Множественный выбор / Только один ответ)

---

13. Вектор инициализации используется для:
a. Перемешивания исходного сообщения
b. Управления передачей ключей
c. Модификации ключевой последовательности

ПК-27.1 Вектор инициализации используется для: (Множественный выбор / Только один ответ)

---

14. Для борьбы с избыточным покрытием сети целесообразно:
a. Снизить мощность сигнала
b. Переместить оборудование
c. Использовать линейное зашумление сигнала

ПК-27.1 Для борьбы с избыточным покрытием сети целесообразно: (Множественный выбор)

---

15. К недостаткам фрагментации относят:
a. Увеличение производительности беспроводной станции
b. Снижение реальной производительности беспроводной станции
c. Снижение зоны охвата беспроводной станции

ПК-27.1 К недостаткам фрагментации относят: (Множественный выбор / Только один ответ)

---

16. К преимуществам WPA можно отнести:
a. Обязательная аутентификация с использованием EAP.
b. Усовершенствованная схема шифрования RC4
c. Обеспечение защиты от DDos

ПК-27.1 К преимуществам WPA можно отнести: (Множественный выбор)

---

17. Какая из перечисленных сетей имеет наименьший радиус действия?
a. WPAN
b. WLAN
c. WMAN
d. WWAN

ПК-27.1 Какая из перечисленных сетей имеет наименьший радиус действия? (Множественный выбор / Только один ответ)

---

18. Каково преимущество технологии беспроводной связи перед технологией проводных ЛВС?
a. Более низкая стоимость обслуживания
b. Большая дальность передачи
c. Более дешевые хост-адаптеры

ПК-27.1 Каково преимущество технологии беспроводной связи перед технологией проводных ЛВС? (Множественный выбор / Только один ответ)

19. Какое утверждение является истинным в отношении проверки подлинности с использованием предварительных ключей при включенном EAP?

a. Использует ключ для шифрования произвольной строки байтов
b. Требуется вычислительный сервер проверки подлинности, такой как Radius
c. Выполняет только одностороннюю проверку подлинности

ПК-27.1 Какое утверждение является истинным в отношении проверки подлинности с использованием предварительных ключей при включенном EAP? (Множественный выбор / Только один ответ)

---

20. Какой метод обеспечивает защищенное туннелирование через Интернет?

a. Виртуальная частная сеть
b. Публичная точка беспроводного доступа
c. Система обнаружения вторжений
d. Протокол SSH

ПК-27.1 Какой метод обеспечивает защищенное туннелирование через Интернет? (Множественный выбор / Только один ответ)

---

21. Перечислите возможные виды аутентификации в беспроводных сетях

a. Закрытая аутентификация
b. Открытая аутентификация
c. Аутентификация по MAC адресу

ПК-27.1 Перечислите возможные виды аутентификации в беспроводных сетях (Множественный выбор)

---

22. Перечислите возможные виды аутентификации в беспроводных сетях

a. Закрытая аутентификация
b. Открытая аутентификация
c. Аутентификация с использование протокола WEP

ПК-27.1 Перечислите возможные виды аутентификации в беспроводных сетях (Множественный выбор)

---

23. Для борьбы с проблемой «засвеченной» станцией используют:

a. Режим DCF
b. Режим PCF
c. Режим NCF

ПК-27.1 Перечислите возможные виды аутентификации в беспроводных сетях (Множественный выбор / Только один ответ)

---

24. При организации беспроводной связи особое внимание следует обратить на:

a. Обеспечение безопасности передачи данных в связи с большей уязвимостью при прослушивании
b. Необходимость отключать точки доступа, попадающих в зону действия распределенных беспроводных сетей
c. Вероятность прямого физического доступа к беспроводной точке

ПК-27.1 При организации беспроводной связи особое внимание следует обратить на: (Множественный выбор)

---

25. Проблема скрытого терминала заключается если из трех подключенных к сети устройств:

a. Все удалены и не входят в диапазон друг друга
b. Два устройства удалены и не входят в диапазон друг друга, однако оба попадают в зону охвата третьего устройства
c. Одно из устройств не входит в диапазон сигнала других

ПК-27.1 Проблема скрытого терминала заключается если из трех подключенных к сети устройств: (Множественный выбор / Только один ответ)

---

26. Протокол TKIP в WPA определяет:

a. Постоянный протокол целостности ключа
b. Временный протокол целостности ключа
c. Активный блочный протокол анализа ключа

ПК-27.1 Протокол TKIP в WPA определяет: (Множественный выбор / Только один ответ)

---

27. Протокол WPA позволяет осуществить защиту:

a. Локальных вычислительных сетей
b. Глобальных вычислительных сетей
c. Персональных сетей
d. Беспроводных сетей

ПК-27.1 Протокол WPA позволяет осуществить защиту: (Множественный выбор / Только один ответ)

---

28. Укажите нарушение безопасности беспроводной сети, встречающееся наиболее часто:

a. Затопление широковещательной рассылкой
b. Подбор SSID
c. Помехи

ПК-27.1 Укажите нарушение безопасности беспроводной сети, встречающееся наиболее часто: (Множественный выбор / Только один ответ)

---

29. Фрагментация проводится с целью:

a. Понизить скорость передачи данных через беспроводную среду
b. Повысить надежность передачи фреймов через беспроводную среду
c. Снизить количество ошибок

ПК-27.1 Фрагментация проводится с целью: (Множественный выбор / Только один ответ)

---

30. Шифр WEP основан на алгоритме:

a. IV
b. RC4
c. MD5
d. KSA

ПК-27.1 Шифр WEP основан на алгоритме: (Множественный выбор / Только один ответ)

---

31. Шифр WPA2 основан на алгоритме:

a. EAP

b. AES
c. SHA
d. KSA

ПК-27.1 Шифр WPA2 основан на алгоритме: (Множественный выбор / Только один ответ)

---

32. Шифр WPA3 основан на алгоритме:
a. CCMP
b. AES
c. SHA
d. KSA

ПК-27.1 Шифр WPA2 основан на алгоритме: (Множественный выбор / Только один ответ)

Тема 5

1. HTTPS позволяет осуществлять защиту через шифрованные транспортные механизмы используя протокол:
a. SSL/TLS
b. RIP
c. IPsec

ПК-27.1 HTTPS позволяет осуществлять защиту через шифрованные транспортные механизмы используя протокол: (Множественный выбор / Только один ответ)

---

2. В цифровом сертификате используются механизмы:
a. Блочного шифрования
b. Ассиметричного шифрования
c. Поточного шифрования

ПК-27.1 В цифровом сертификате используются механизмы: (Множественный выбор / Только один ответ)

---

3. Заголовок АН добавляется:
a. Перед заголовком IP
b. После заголовка IP
c. Вместо заголовка IP

ПК-27.1 Заголовок АН добавляется: (Множественный выбор / Только один ответ)

---

4. Использование протокола IPSec позволяет осуществить:
a. Аутентификацию пользователя
b. Поверку работоспособности сети
c. Фрагментацию пакетов

ПК-27.1 Использование протокола IPSec позволяет осуществить: (Множественный выбор / Только один ответ)

---

5. Использование протокола Radius позволяет осуществить:
a. Аутентификацию пользователя
b. Туннелирование при передаче данных
c. Фрагментацию пакетов при передаче топологии сети в другую

ПК-27.1 Использование протокола Radius позволяет осуществить: (Множественный выбор / Только один ответ)

---

6. К недостаткам протокола TLS/SSL относят:

a. Снижение производительности приложений
b. Отсутствие аутентификации сторон
c. Применение симметричного шифрования

ПК-27.1 К недостаткам протокола TLS/SSL относят: (Множественный выбор / Только один ответ)

---

7. Какие из следующих протоколов защищены от прослушивания?

a. SFTP
b. HTTP
c. SMTP

ПК-27.1 Какие из следующих протоколов защищены от прослушивания? (Множественный выбор / Только один ответ)

---

8. Механизмы аутентификации протокола Kerberos используют:

a. AS для аутентификации пользователя и выдачи билет на TGS
b. TGS для аутентификации пользователя и выдачи билет на AS
c. AS для аутентификации пользователя и выдачи билет сервер

ПК-27.1 Механизмы аутентификации протокола Kerberos используют: (Множественный выбор / Только один ответ)

---

9. Механизмы аутентификации протокола Kerberos используются один раз на входную сессию клиента с выдачей билета на:

a. TGS
b. на сервер
c. AS

ПК-27.1 Механизмы аутентификации протокола Kerberos используются один раз на входную сессию клиента с выдачей билета на: (Множественный выбор / Только один ответ)

---

10. Протокол CHAP обеспечивает защиту от атак:

a. Путем воспроизведения с помощью возрастающего значения идентификатора
b. За счет динамического распределения ключей
c. За счет использования одноразовых паролей

ПК-27.1 Протокол CHAP обеспечивает защиту от атак: (Множественный выбор / Только один ответ)

---

11. Протокол ESP обеспечивает:

a. Электронную цифровую подпись
b. Шифрование трафика
c. Управление ключами

ПК-27.1 Протокол ESP обеспечивает: (Множественный выбор / Только один ответ)

---

12. Протокол IKE обеспечивает:

a. Туннелирование при передаче данных

b. Управление ключами
c. Фрагментирование больших данных

ПК-27.1 Протокол IKE обеспечивает: (Множественный выбор / Только один ответ)

---

13. Протокол IPSec при передаче данных не использует:

a. Туннельный режим
b. Транспортный режим
c. Сеансовый режим

ПК-27.1 Протокол IPSec при передаче данных не использует: (Множественный выбор / Только один ответ)

---

14. Протокол SSH:

a. Позволяет осуществлять удаленное управление
b. Позволяет осуществлять дефрагментацию пакетов при передаче в разнородных сетях
c. Проверять наличие цифровой подписи у каждого пакета с данными

ПК-27.1 Протокол SSH: (Множественный выбор / Только один ответ)

---

15. Транспортный режим протокола IPSec используется для:

a. Установления соединения между хостами
b. Установления соединения хост-сеть
c. Установление соединения сеть-сеть

ПК-27.1 Транспортный режим протокола IPSec используется для: (Множественный выбор / Только один ответ)

---

16. Туннельный режим протокола IPSec используется для:

a. Установления соединения между хостами
b. Установления соединения хост-сеть
c. Установление соединения сеть-сеть

ПК-27.1 Туннельный режим протокола IPSec используется для: (Множественный выбор)

---

17. Укажите какие компоненты входят в IPSec:

a. **(30%)** AH
b. **(30%)** ESP
c. **(40%)** IKE
d. AM

ПК-27.1 Укажите какие компоненты входят в IPSec: (Множественный выбор)

---

18. Цепочка сертификатов – это последовательность сертификатов:

a. Позволяющая определить действительность сертификата конечного участника
b. Выпущенных распределённом сертификационным центром
c. Множество сертификатов некоторого конечного участника

ПК-27.1 Цепочка сертификатов – это последовательность сертификатов: (Множественный выбор / Только один ответ)

19. Что не входит в протокол L2TP?

a. L2F
b. PPTP
c. ESP

ПК-27.1 Что не входит в протокол L2TP? (Множественный выбор / Только один ответ)

---

20. Электронно-цифровая подпись (ЭЦП) документа формируется на основе:

a. Сторонних данных
b. Перестановки элементов ключа
c. Самого документа

ПК-27.1 Электронно-цифровая подпись (ЭЦП) документа формируется на основе: (Множественный выбор / Только один ответ)

---

21. VPN, основная цель которой состоит в организации виртуальной подсети внутри защищённой сети, называется:

a. Надёжной
b. Доверительной
c. Комплексной

ПК-27.1. VPN, основная цель которой состоит в организации виртуальной подсети внутри защищённой сети, называется: (Множественный выбор / Только один ответ)

---

22. Какие проблемы возникают при использовании VPN?

a. Высокие требования к обеспечению безопасности при распределении ключей по
b. Сравнению с выделенными каналами Дополнительная нагрузка трафика
c. Проблем при фрагментации трафика

ПК-27.1. Какие проблемы возникают при использовании VPN? (Множественный выбор)

---

23. Какими характеристиками не обладают VPN?

a. Трафик шифруется для обеспечения защиты от прослушивания
b. Трафик фрагментируется для обеспечения защиты от прослушивания
c. Осуществляется аутентификация удаленного пользователя
d. Виртуальные частные сети обеспечивают поддержку множества протоколов

ПК-27.1. Какими характеристиками не обладают VPN? (Множественный выбор / Только один ответ)

---

24. Какой из указанных протоколов не обеспечивает защищенную передачу данных в VPN?

a. IPSec
b. PPTP
c. IMAP

ПК-27.1. Какой из указанных протоколов не обеспечивает защищенную передачу данных в VPN? (Множественный выбор / Только один ответ)

---

25. Какой механизм обеспечивает конфиденциальность данных в сети VPN?

a. Хэширование
b. Туннелирование
c. Шифрование
d. Инкапсуляция

ПК-27.1. Какой механизм обеспечивает конфиденциальность данных в сети VPN? (Множественный выбор / Только один ответ)

---

26. Какой этап не входит в установление соединения по протоколу PPTP?

a. Автоматическое создание ключей
b. Инкапсуляция пакетов IP для передачи по IP-сети
c. Создание соединения для пересылки данных по туннелю

ПК-27.1. Какой этап не входит в установление соединения по протоколу PPTP? (Множественный выбор / Только один ответ)

---

27. Логический путь передвижения инкапсулированных пакетов в транзитной сети называется:

a. Туннель;
b. Шлюз;
c. Магистраль

ПК-27.1. Логический путь передвижения инкапсулированных пакетов в транзитной сети называется: (Множественный выбор / Только один ответ)

---

28. На каком оборудовании нельзя организовать VPN?

a. Конечный хост
b. Концентратор
c. Маршрутизатор

ПК-27.1. На каком оборудовании нельзя организовать VPN? (Множественный выбор / Только один ответ)

---

29. Назовите протокол, использующийся при построении VPN

a. L2TP
b. ARP
c. P2P

ПК-27.1. Назовите протокол, использующийся при построении VPN (Множественный выбор / Только один ответ)

---

30. Назовите протокол, не использующийся при построении VPN:

a. L2TP
b. P2P
c. PPTP
d. L2TP/IPsec

ПК-27.1. Назовите протокол, не использующийся при построении VPN: (Множественный выбор / Только один ответ)

---

31. Перечислите преимущества узловых VPN:

a. Использование выделенной линии связи
b. Возможность использование традиционной инфраструктурой сети
c. Скорость передачи данных

ПК-27.1. Перечислите преимущества узловых VPN: (Множественный выбор / Только один ответ)

---

32. Перечислите преимущества узловых VPN?

a. Использование выделенной линии связи
b. Возможность использование традиционной инфраструктурой сети
c. Скорость передачи данных

ПК-27.1. Перечислите преимущества узловых VPN? (Множественный выбор / Только один ответ)

---

33. При установлении несколько соединений VPN, что происходит с трафиком?

a. Трафик разделяется посредством шифрования с различными ключами
b. Трафик шифруется одним ключом
c. Трафик не разделяется

ПК-27.1. При установлении несколько соединений VPN, что происходит с трафиком? (Множественный выбор / Только один ответ)

---

34. Укажите какие протоколы использует IPsec при шифровании всего IP-пакет:

a. Authentication Header (AH);
b. Encapsulating Security Protocol (ESP);
c. SSH

ПК-27.1. Укажите какие протоколы использует IPsec при шифровании всего IP-пакет: (Множественный выбор)

Тема 7

1. DDos атака характеризуется:

a. Увеличением пакетов, содержащих флаг SYN
b. Уменьшением пакетов, содержащих флаг RST
c. Одинаковым количеством пакетов, содержащих флаг SYN+RST

ПК-27.1 DDos атака характеризуется: (Множественный выбор / Только один ответ)

---

2. Honeypot позволяет:

a. Изучить стратегию злоумышленника
b. Определить структуру сети
c. Осуществить формирование динамических правил фильтрации трафика

ПК-27.1 Honeypot позволяет: (Множественный выбор / Только один ответ)

---

3. Honeypot позволяет:

a. Определить перечень средств, с помощью которых могут быть нанесены удары
b. Осуществить формирование динамических правил фильтрации трафика
c. Определить сетевую структуру

ПК-27.1 Honeypot позволяет: (Множественный выбор / Только один ответ)

---

4. Honeypot это:

a. Ресурс, представляющий собой приманку для злоумышленников
b. СОВ системного уровня
c. Модуль прогнозирования сетевого трафика

ПК-27.1 Honeypot это: (Множественный выбор / Только один ответ)

---

5. Snort относится к:
a. Анализаторам системного уровня
b. Анализаторам сетевого уровня
c. Хостовым СОВ

ПК-27.1 Snort относится к: (Множественный выбор / Только один ответ)

---

6. Агент, фиксирующий изменения журналов, называется:
a. Анализатор журналов
b. Контроллер целостности файлов
c. Анализатор поведения приложений

ПК-27.1 Агент, фиксирующий изменения журналов, называется: (Множественный выбор / Только один ответ)

---

7. В SIEM-системы первого поколения не входят средства:
a. Нормализации
b. Фильтрации,
c. Визуализации

ПК-27.1 В SIEM-системы первого поколения не входят средства: (Множественный выбор / Только один ответ)

---

8. В режиме анализа пакетов Snort действует как:
a. IDS сетевого уровня
b. IDS системного уровня
c. Сетевой анализатор

ПК-27.1 В режиме анализа пакетов Snort действует как: (Множественный выбор / Только один ответ)

---

9. Для повышения эффективности защиты общедоступных серверов, целесообразно:
a. Разместить сенсоры СОВ в демилитаризованной зоне
b. Увеличить число сигнатур, для обнаружения любой подозрительной активности
c. Разместить в ДМЗ сервер AAA

ПК-27.1 Для повышения эффективности защиты общедоступных серверов, целесообразно: (Множественный выбор / Только один ответ)

---

10. Для увеличения эффективным средств защиты общедоступных серверов, целесообразно:
a. Включить в периметр ДМЗ honeypot
b. Не реагировать на такую активность, как сканирование портов
c. Разместить сенсоры сетевой системы обнаружения вторжений в локальной сети

ПК-27.1 Для увеличения эффективным средств защиты общедоступных серверов, целесообразно: (Множественный выбор / Только один ответ)

11. Для уменьшения числа ложных срабатываний СОВ следует:

a. Построить профиль сетевой активности
b. Использовать настройки сетевого оборудования «по умолчанию»
c. Минимизировать число настраиваемых параметров

ПК-27.1 Для уменьшения числа ложных срабатываний СОВ следует: (Множественный выбор / Только один ответ)

---

12. К достоинствам методов обнаружения вторжений, основанных на нейронных сетях, можно отнести:

a. Способность обобщать неструктурированные неполные данные
b. Отсутствие необходимости в - экспертных знаниях
c. Возможность переобучения

ПК-27.1 К достоинствам методов обнаружения вторжений, основанных на нейронных сетях, можно отнести: (Множественный выбор)

---

13. К недостатку метода обнаружения вторжений, основанного на методе сингулярного спектрального разложения, можно отнести:

a. Использование подмножество обучающих точек в функции принятия решений
b. Использование матричных вычислений
c. Использование оценок согласованности

ПК-27.1 К недостатку метода обнаружения вторжений, основанного на методе опорных векторов, можно отнести: (Множественный выбор / Только один ответ)

---

14. К основным видам систем обнаружения вторжений не относятся:

a. Сетевые
b. Хостовые
c. Гибридные
d. Локальные

ПК-27.1 К основным видам систем обнаружения вторжений не относятся: (Множественный выбор / Только один ответ)

---

15. К сигнатурным методам обнаружения вторжений можно отнести:

a. Модель Гаусса
b. Построение графа атак
c. Спектральное разложение

ПК-27.1 К сигнатурным методам обнаружения вторжений можно отнести: (Множественный выбор / Только один ответ)

---

16. К сигнатурным методам обнаружения вторжений относят:

a. Методы оценки превышения порогового значения
b. Следование по пути графа атаки
c. Выделение кластером

ПК-27.1 К сигнатурным методам обнаружения вторжений относят: (Множественный выбор / Только один ответ)

---

17. **К числу недостатков размещения СОВ между поставщиком Интернет-услуг и межсетевым экраном относят:**
    a. Требование постоянного обновления сигнатур
    b. Наличие одиночной точкой отказа для сетевого трафика
    c. Необходимость постоянной фильтрации трафика

ПК-27.1 К числу недостатков размещения СОВ между поставщиком Интернет-услуг и межсетевым экраном относят: (Множественный выбор / Только один ответ)

---

18. **К числу типичных причин ложных срабатываний СОВ принадлежат:**
    a. Активное администрирование баз данных
    b. Применение длинных и сложных паролей
    c. Изменения правил фильтрации трафика

ПК-27.1 К числу типичных причин ложных срабатываний СОВ принадлежат: (Множественный выбор / Только один ответ)

---

19. **К числу типичных причин ложных срабатываний СОВ принадлежат:**
    a. Применение длинных и сложных паролей
    b. Изменения правил фильтрации трафика
    c. Длинные базовые цепочки аутентификации

ПК-27.1 К числу типичных причин ложных срабатываний СОВ принадлежат: (Множественный выбор / Только один ответ)

---

20. **Какая система не относится к обеспечения сетевой безопасности:**
    a. IDS
    b. SIEM
    c. ERP
    d. DLP

ПК-27.1 Какая система не относится к обеспечения сетевой безопасности: (Множественный выбор / Только один ответ)

---

21. **Какое основное сетевое оборудование используется при луковой маршрутизации**
    a. Анонимный маршрутизатор
    b. Анонимный прокси-сервер
    c. Анонимный межсетевой экран

ПК-27.1 Какое основное сетевое оборудование используется при луковой маршрутизации (Множественный выбор / Только один ответ)

---

22. **Какой протокол передачи используют в своей работе СОВ, использующие протокол SNMP?**
    a. TCP
    b. UDP
    c. ICMP

ПК-27.1 Какой протокол передачи используют в своей работе СОВ, использующие протокол SNMP? (Множественный выбор / Только один ответ)

---

23. Какой протокол участвует в построении СОВ:

a. SNMP
b. BGP
c. OSPF

ПК-27.1 Какой протокол участвует в построении СОВ: (Множественный выбор / Только один ответ)

---

24. Какой элемент отсутствуют в архитектуре SNMP?

a. Менеджер
b. Агент
c. Модуль прогноза

ПК-27.1 Какой элемент отсутствуют в архитектуре SNMP? (Множественный выбор / Только один ответ)

---

25. Кластерный анализ сетевого трафика позволяет:

a. Собирать события в отдельные группы
b. Устанавливать пороговые значения
c. Формировать профиль устройства

ПК-27.1 Кластерный анализ сетевого трафика позволяет: (Множественный выбор / Только один ответ)

---

26. Ложное срабатывание сетевой системы обнаружения вторжений характеризуется:

a. Генерацией сигнала тревоги при нормальном поведении сетевой активности
b. Пропуском неизвестной атаки
c. «Запаздывание» в анализе трафика для реального масштаба времени

ПК-27.1 Ложное срабатывание сетевой системы обнаружения вторжений характеризуется: (Множественный выбор / Только один ответ)

---

27. Метод обнаружения вторжений, основанный на анализе состояний, можно отнести к системам:

a. ERP
b. DLP
c. SAP

ПК-27.1 Метод обнаружения вторжений, основанный на анализе состояний, можно отнести к системам: (Множественный выбор / Только один ответ)

---

28. Определение порогового значения используется в методах:

a. Статистического анализ
b. Сигнатурного анализа
c. Спектрального разложения

ПК-27.1 Определение порогового значения используется в методах: (Множественный выбор / Только один ответ)

---

29. Основными достоинствами систем обнаружения вторжений на основе выявления аномальной активности являются:

a. Возможность обнаружения неизвестных ранее видов атак
b. Отсутствие ложных срабатываний
c. Отсутствие необходимости постоянного обновления сигнатур

ПК-27.1 Основными достоинствами систем обнаружения вторжений на основе выявления аномальной активности являются: (Множественный выбор)

---

30. Основными недостатками статистическим методов выявления атак являются:

a. Высокое число ложных срабатываний
b. Длительность и сложность определения профилей нормальной активности
c. Пропуск атак, статистические характеристики которых близки к нормальным

ПК-27.1 Основными недостатками статистическим методов выявления атак являются: (Множественный выбор)

---

31. Отличие SIEM-систем от IDS заключается в наличии средств:

a. Анализа событий
b. Агрегации
c. Аналитики рисков

ПК-27.1 Отличие SIEM-систем от IDS заключается в наличии средств: (Множественный выбор / Только один ответ)

---

32. Прогнозирование сетевого трафика возможно осуществлять с помощью:

a. Метода скользящей средней
b. Марковской цепи
c. Используя методы вейвлет анализа

ПК-27.1 Прогнозирование сетевого трафика возможно осуществлять с помощью: (Множественный выбор)

---

33. Прогнозирование сетевого трафика позволяет:

a. Осуществить балансировку нагрузки на сеть
b. Сформировать новые правила фильтрации
c. Выявить атаки нулевого дня

ПК-27.1 Прогнозирование сетевого трафика позволяет: (Множественный выбор / Только один ответ)

---

34. К статистическим методам обнаружения вторжений можно отнести:

a. Модель Гаусса
b. Построение графа атак
c. Спектральное разложение

ПК-27.1 Прогнозирование сетевого трафика позволяет: (Множественный выбор / Только один ответ)

---

35. Размещение СОВ в ДМЗ позволяет отслеживать активность внешних пользователей по отношению:

a. К общедоступным серверам
b. К межсетевому экрану
c. По отношению к локальной сети

ПК-27.1 Размещение СОВ в ДМЗ позволяет отслеживать активность внешних пользователей по отношению: (Множественный выбор / Только один ответ)

---

36. Размещение СОВ позади ДМЗ позволяет:

a. Обнаружить вторжение, проникшее во внутреннюю сеть

b. Предотвратить внешние атаки на внутреннюю сеть
c. Обеспечить тестирование сети путем анализа пропускаемого им трафика

ПК-27.1 Размещение СОВ позади ДМЗ позволяет: (Множественный выбор)

---

37. Размещение СОВ позади межсетевого экрана обеспечивает:

a. Дополнительную поддержку защиты от атак
b. Защиту от внешних атак на межсетевой экран
c. Повышение собственной защищенности межсетевого экрана

ПК-27.1 Размещение СОВ позади межсетевого экрана обеспечивает: (Множественный выбор / Только один ответ)

---

38. Сетевые системы обнаружения вторжений целесообразно использовать на:

a. Группе специально выделенных хостов
b. Межсетевом экране
c. Специально выделенном хосте

ПК-27.1 Сетевые системы обнаружения вторжений целесообразно использовать на: (Множественный выбор / Только один ответ)

---

39. Сигнатурные методы анализа защищенности помогают предотвратить:

a. Известные атаки
b. Новые виды атак
c. Нетипичное поведение пользователей

ПК-27.1 Сигнатурные методы анализа защищенности помогают предотвратить: (Множественный выбор / Только один ответ)

---

40. Статистические методы анализа защищенности помогают предотвратить:

a. Известные атаки
b. Новые виды атак
c. Нетипичное поведение пользователей

ПК-27.1 Статистические методы анализа защищенности помогают предотвратить: (Множественный выбор / Только один ответ)

---

41. Укажите, какие компоненты не входят в SIEM:

a. Модули сбора событий
b. Модули обработки сетевого трафика
c. Модули хранения
d. Модули построения профиля злоумышленников

ПК-27.1 Укажите, какие компоненты не входят в SIEM: (Множественный выбор / Только один ответ)

---

42. Шаблон вредоносной активности называется:

a. Идентификационной меткой
b. Профилем
c. Сигнатурой
d. Цифровым отпечатком

ПК-27.1 Шаблон вредоносной активности называется: (Множественный выбор / Только один ответ)

43. Выявление взаимосвязи между разнородными событиями безопасности называется

- корреляция
- корреляцией

ПК-27.1 Выявление взаимосвязи между разнородными событиями безопасности называется (Короткий ответ)

---

44. Объединение событий безопасности, схожих по определенным признакам называется

- агрегация
- агрегацией

ПК-27.1 Объединение событий безопасности, схожих по определенным признакам называется (Короткий ответ)

---

45. Определение значимости и критичности событий безопасности на основании правил, определенных в системе, называется

- приоритезация
- приоритезацией

ПК-27.1 Определение значимости и критичности событий безопасности на основании правил, определенных в системе, называется (Короткий ответ)

---

46. Представление данных в графическом виде, характеризующим результаты анализа событий безопасности и состояние защищаемой системы и ее элементов называется

- визуализация
- визуализацией

ПК-27.1 Представление данных в графическом виде, характеризующим результаты анализа событий безопасности и состояние защищаемой системы и ее элементов называется (Короткий ответ)

---

47. Приведение форматов записей журналов событий безопасности, собранных из различных источников, к единому внутреннему формату называется

- нормализация
- нормализацией

ПК-27.1 Приведение форматов записей журналов событий безопасности, собранных из различных источников, к единому внутреннему формату называется (Короткий ответ)

---

48. **Технология анонимного обмена информацией через компьютерную сеть, при котором сообщения неоднократно шифруются и потом отсылаются через несколько сетевых узлов, называется**
    - луковая маршрутизация
    - Луковой маршрутизацией
    - луковой маршрутизацией

ПК-27.1 Технология анонимного обмена информацией через компьютерную сеть, при котором сообщения неоднократно шифруются и потом отсылаются через несколько сетевых узлов, называется (Короткий ответ)

---

49. **Удалении избыточных данных о событиях безопасности поступающих в систему потоков называется**
    - фильтрация
    - фильтрацией

ПК-27.1 Удалении избыточных данных о событиях безопасности поступающих в систему потоков называется (Короткий ответ)

---

50. **Установление принадлежности определенных классов для атрибутов событий безопасности называется**
    - классификация
    - классификацией

ПК-27.1 Установление принадлежности определенных классов для атрибутов событий безопасности называется (Короткий ответ)

---

51. **Характерные признаки компьютерной атаки, используемые для ее обнаружения, называются**
    - сигнатурой
    - сигнатура

ПК-27.1 Характерные признаки компьютерной атаки, используемые для ее обнаружения, называются (Короткий ответ)

Тема 6 :: ПК-27.1. Для аутентификации пользователя используют протокол: ::Для аутентификации пользователя используют протокол: {=RADIUS ~SNMP ~SMTP}

1. **NAS это:**
    a. Сервер для хранения данных на файловом уровне
    b. Интеллектуальный коммутатор
    c. Сервер распределения ключей

ПК-27.1. NAS это (Множественный выбор / Только один ответ)

---

2. Для какого протокола характерно шифрование пароля пользователя на основе случайного числа, полученного от сервера:

a. CHAP
b. SMTP
c. PAP

ПК-27.1. Для какого протокола характерно шифрование пароля пользователя на основе случайного числа, полученного от сервера: (Множественный выбор / Только один ответ)

---

3. К протоколу аутентификации с косвенным согласованием относят:

a. CHAP
b. Kerberos
c. PAP

ПК-27.1. К протоколу аутентификации с косвенным согласованием относят: (Множественный выбор / Только один ответ)

---

4. Какой алгоритм в качестве хэш-функции определен в CHAP?

a. MD5
b. SHA
c. HAVAL

ПК-27.1. Какой алгоритм в качестве хэш-функции определен в CHAP? (Множественный выбор / Только один ответ)

---

5. Основные достоинства парольной аутентификации:

a. Высокая надежность
b. Низкая стоимость внедрения
c. Простота реализации

ПК-27.1. Основные достоинства парольной аутентификации: (Множественный выбор)

---

6. Основные принципы функционирования RADIUS

a. Клиент-серверная модель функционирования
b. Транзакции между NAS и сервером RADIUS аутентифицированы с помощью общего секрета, который никогда не посылается по сети
c. Транзакции между NAS и сервером RADIUS зашифрованы алгоритмом симметричного шифрования

ПК-27.1. Основные принципы функционирования RADIUS (Множественный выбор / Только один ответ)

---

7. Перечислите основные функции сервера RADIUS

a. **(30%)** Обеспечение аутентификации
b. **(30%)** Обеспечение авторизации
c. **(40%)** Обеспечение аккаунтинга
d. Обеспечение шифрование

ПК-27.1. Перечислите основные функции сервера RADIUS (Множественный выбор)

---

8. **При использовании протокола RADIUS в запросе Access-Request присутствует аутентификационные данные пользователя, которые закрыты методом основанным на алгоритме:**
    a. MD5
    b. DES
    c. RSA

ПК-27.1. При использовании протокола RADIUS в запросе Access-Request присутствует аутентификационные данные пользователя, которые закрыты методом основанным на алгоритме: (Множественный выбор / Только один ответ)

---

9. **Протокол PAP используется**
    a. Для генерации ключей
    b. Для распределения ключей
    c. Для аутентификации маршрутизаторов

ПК-27.1. Протокол PAP используется (Множественный выбор / Только один ответ)

Тема 1

1. **Для первичного сбора информации о системе целесообразно использовать:**
    a. Устав организации
    b. Данные бухгалтерского учета
    c. Кадровую политику предприятия

ПК-27.1. Для первичного сбора информации о системе целесообразно использовать: (Множественный выбор / Только один ответ)

---

2. **К формальным методам защиты информации можно отнести:**
    a. Криптографические методы защиты информации
    b. Организационные методы защиты
    c. Морально-этические методы защиты

ПК-27.1. К формальным методам защиты информации можно отнести: (Множественный выбор / Только один ответ)

---

3. **Наиболее важным при реализации защитных мер политики безопасности является следующее**
    a. Аудит, анализ затрат на проведение защитных мер
    b. Аудит, анализ безопасности
    c. Аудит, анализ уязвимостей, риск-ситуаций

ПК-27.1. Наиболее важным при реализации защитных мер политики безопасности является следующее (Множественный выбор / Только один ответ)

---

4. **Перечень каких систем необходимо учитывать при категорировании объектов, подлежащих защите при передаче данных?**
    a. Реализующие управленческие процессы
    b. Реализующие образовательные процессы
    c. Реализующие оптимизационные процессы

ПК-27.1. Перечень каких систем необходимо учитывать при категорировании объектов, подлежащих защите при передаче данных? (Множественный выбор / Только один ответ)

---

5. **Предварительные испытания сетевого оборудования и подсистемы безопасности не предусматривают наличие документации по**
    a. Программе и методике предварительных испытаний работоспособности подсистемы безопасности сети
    b. Актам (протокол) оценки влияния подсистемы безопасности на функционирование сетевой инфраструктуры
    c. Проверке знаний и умений пользователей и администраторов, необходимых для эксплуатации сетевого оборудования

ПК-27.1. Предварительные испытания сетевого оборудования и подсистемы безопасности не предусматривают наличие документации по (Множественный выбор / Только один ответ)

---

6. **При определении критичности сетевой инфраструктуры, какой временной диапазон необходимо взять для оценки ущерба?**
    a. Максимальный период времени, требуемый на восстановление штатных (проектных) параметров работы сети
    b. Минимальный период времени, требуемый на восстановление штатных (проектных) параметров работы сети
    c. Средний период времени, требуемый на восстановление штатных (проектных) параметров работы сети

ПК-27.1. При определении критичности сетевой инфраструктуры, какой временной диапазон необходимо взять для оценки ущерба? (Множественный выбор / Только один ответ)

---

7. **При оценке объектов ИС в соответствии с показателями критериев значимости, наибольший ущерб присваивается**
    a. Первой категории значимости
    b. Второй категории значимости
    c. Третьей категории значимости

ПК-27.1. При оценке объектов ИС в соответствии с показателями критериев значимости, наибольший ущерб присваивается (Множественный выбор / Только один ответ)

---

8. **Проектирование подсистемы безопасности сети не предусматривает**
    a. Техническое задание (частное техническое задание)
    b. Технический проект
    c. Акт установки средств защиты

ПК-27.1. Проектирование подсистемы безопасности сети не предусматривает (Множественный выбор / Только один ответ)

---

9. **Средства ликвидации последствий должны обладать следующими функциями:**
    a. Управление процессами реагирования на компьютерные и инциденты и ликвидации последствий компьютерных атак
    b. Оценке причиненного ущерба
    c. Построения профиля злоумышленника

ПК-27.1. Средства ликвидации последствий должны обладать следующими функциями: (Множественный выбор / Только один ответ)

---

10. **Установление соответствия объекта инфраструктуры критериям значимости и показателям их значений называется**
    a. Категорированием объектов
    b. Планированием сетевой инфраструктуры

c. Формированием требований к безопасности

ПК-27.1. Установление соответствия объекта инфраструктуры критериям значимости и показателям их значений называется (Множественный выбор / Только один ответ)

---

11. Является ли страховая компания субъектом критической инфраструктуры?

a. является
b. не является
c. является, если осуществляет обработку персональных данных

ПК-27.1. Является ли страховая компания субъектом критической инфраструктуры? (Множественный выбор / Только один ответ)

Тема 4

1. Запись в списке доступа Router_A(config-ext-nac1) permit tcp host 192.168.30.11 host 192.168.10.25 eq 8080 означает:

a. Узлу 192.168.30.11 разрешен доступ к узлу 192.168.10.25 по Telnet
b. Узлу 192.168.30.11 запрещен доступ к узлу 192.168.10.25 по http
c. Узлу 192.168.10.25 разрешен доступ к узлу 192.168.30.11 по протоколу 8080
d. Узлу 192.168.10.25 запрещен доступ к узлу 192.168.30.11 по протоколу 8080
e. Узлу 192.168.30.11 разрешен доступ к узлу 192.168.10.25 по порту 8080

ПК-27.1 Запись в списке доступа Router_A(config-ext-nac1) permit tcp host 192.168.30.11 host 192.168.0.25 eq 8080 означает: (Множественный выбор / Только один ответ)

---

2. Запись в списке доступа Router(config) access-list 11 permit 192.168.28.11 0.0.0.0

a. Разрешает доступ к конечному узлу 192.168.28.11 защищаемой сети
b. Запрещает доступ к конечному узлу 192.168.28.11 защищаемой сети
c. Разрешает доступ конечному узлу 192.168.30.11 к защищаемой сети
d. Запрещает доступ конечному узлу 192.168.28.11 к защищаемой сети

ПК-27.1 Запись в списке доступа Router(config) access-list 11 permit 192.168.28.11 0.0.0.0 (Множественный выбор / Только один ответ)

---

3. Расширенный список доступа осуществляет фильтрацию по следующим параметрам

a. IP-адреса источника и назначения
b. MAC-адрес источника и назначения
c. Протокол
d. Номер порта
e. Маску подсети

ПК-27.1 Расширенный список доступа осуществляет фильтрацию по следующим параметрам (Множественный выбор)

---

4. Сколько интерфейсов у межсетевого экрана прикладного уровня?

a. 1
b. 2
c. По количеству подключенных интерфейсов

ПК-27.1 Сколько интерфейсов у межсетевого экрана прикладного уровня? (Множественный выбор / Только один ответ)

5. **К числу достоинств размещения СОВ между поставщиком Интернет-услуг и межсетевым экраном принадлежат:**
    a. Возможность защитить межсетевой экран от внешних атак
    b. Возможность защитить межсетевой экран от внутренних атак
    c. Возможность перехватывать весь трафик

ПК-27.1 К числу достоинств размещения СОВ между поставщиком Интернет-услуг и межсетевым экраном принадлежат: (Множественный выбор / Только один ответ)

---

6. **К числу недостатков размещения СОВ между поставщиком Интернет-услуг и межсетевым экраном принадлежат:**
    a. Невозможность наблюдать внутренний трафик в ЛВС
    b. Невозможность контролировать работу межсетевого экрана
    c. Сложность работы в реальном масштабе времени

ПК-27.1 К числу достоинств размещения СОВ между поставщиком Интернет-услуг и межсетевым экраном принадлежат: (Множественный выбор / Только один ответ)

---

7. **Какие из перечисленных задач выполняются протоколами маршрутизации?**
    a. **(40%)** Формирование доступных маршрутов во все пункты назначения
    Обеспечение схемы адресации для идентификации сетей
    b. **(30%)** Размещение лучшего маршрута в таблице маршрутизации
    c. **(30%)** Удаление маршрутов из таблицы маршрутизации по истечении срока действия

ПК-27.1 Какие из перечисленных задач выполняются протоколами маршрутизации? (Множественный выбор)

---

8. **Какие сетевые устройства используются для маршрутизации трафика между автономными системами?**
    a. Маршрутизаторы пограничного шлюза
    b. Внутренние маршрутизаторы
    c. Коммутаторы поставщика услуг
    d. Маршруты широковещательной рассылки

ПК-27.1 Какие сетевые устройства используются для маршрутизации трафика между автономными системами? (Множественный выбор / Только один ответ)

---

9. **Каковы преимущества NAT?**
    a. Транслирует локальные IP зарегистрированных пользователей общие IP-адреса
    b. Осуществляет фильтрацию трафика
    c. Повышает производительность маршрутизаторов

ПК-27.1 Каковы преимущества NAT? (Множественный выбор / Только один ответ)

---

10. **Каковы преимущества NAT?**
    a. Создает частную адресацию ЛВС недоступную для сети Интернет
    b. Позволяет расширять ЛВС без дополнительных общих ip-адресов
    c. Формирует ДМЗ

ПК-27.1 Каковы преимущества NAT? (Множественный выбор / Только один ответ)

11. Какой вид трансляции допускается при возникновении необходимости обеспечения доступа к Веб-серверу из сети Интернет для внешних хостов?

a. Динамический, с использованием пула NAT
b. Статический
c. Динамическая маршрутизация

ПК-27.1 Какой вид трансляции допускается при возникновении необходимости обеспечения доступа к Веб-серверу из сети Интернет для внешних хостов? (Множественный выбор / Только один ответ)

---

12. Наличие какого элемента обязательно для всех архитектур DMZ?

a. Сервер
b. DNS
c. NTP
d. Межсетевой экран

ПК-27.1 Наличие какого элемента обязательно для всех архитектур DMZ? (Множественный выбор / Только один ответ)

---

13. Прокси-сервер может выполнять:

a. Конфигурирование маршрутизаторов
b. Фильтрацию запросов
c. Распределение ключей

ПК-27.1 Прокси-сервер может выполнять: (Множественный выбор / Только один ответ)

---

14. Стандартный список доступа осуществляет фильтрацию по следующим параметрам:

a. IP-адрес источника
b. Номер порта верхнего уровня
c. MAC-адрес источника и назначения

ПК-27.1 Стандартный список доступа осуществляет фильтрацию по следующим параметрам: (Множественный выбор / Только один ответ)

---

15. Узлы, между которыми устанавливается защищённый канал, называются:

a. Контрольными точками
b. Точками доступа
c. Шлюзами безопасности

ПК-27.1 Узлы, между которыми устанавливается защищённый канал, называются: (Множественный выбор / Только один ответ)

---

16. Экранирование на сетевом уровне может обеспечить:

a. Разграничение доступа по сетевым адресам
b. Выборочное выполнение команд прикладного протокола
c. Контроль надежной передачи данных, переданных по TCP-соединению

ПК-27.1 Экранирование на сетевом уровне может обеспечить: (Множественный выбор / Только один ответ)

---

17. Запрет приема межсетевым экраном пакетов с установленным флагом SYN из внешней сети позволяет:

a. Предотвратить нарушение доступности
b. Предотвратить нарушение целостности
c. Предотвратить нарушение конфиденциальности

ПК-27.1. Запрет приема межсетевым экраном пакетов с установленным флагом SYN из внешней сети позволяет: (Множественный выбор / Только один ответ)

---

18. Какие два элемента информации можно извлечь из IP-адреса 192.168.42.135/24?

a. Маска подсети
b. Класс сети
c. Класс обслуживаемого устройства
d. Номер шлюза по умолчанию

ПК-27.1. Какие два элемента информации можно извлечь из IP-адреса 192.168.42.135/24? (Множественный выбор)

---

19. Какие действия осуществляет маршрутизатор, получив пакет «по умолчанию»?

a. Отбрасывает
b. Передает на следующий фильтр
c. Пропускает во внутреннюю сеть

ПК-27.1. Какие действия осуществляет маршрутизатор, получив пакет «по умолчанию»? (Множественный выбор / Только один ответ)

---

20. Какие функции выполняет PAT?

a. PAT получает IP-адрес и преобразует его в адрес шлюза, используемого по умолчанию
b. PAT получает локальный IP-адрес и преобразует его во внутренний исходный IP-адрес
c. PAT получает внутренний исходный IP-адрес и преобразует его в глобальный IP-адрес

ПК-27.1. Какие функции выполняет PAT? (Множественный выбор / Только один ответ)

---

21. Межсетевой экран позволяет разделить сеть на части и:

a. Реализовать набор правил прохождения пакетов с данными через границу
b. Проверять наличие цифровой подписи у каждого пакета с данными, проходящего через границу
c. Прогнозировать прохождение трафика через сеть

ПК-27.1. Межсетевой экран позволяет разделить сеть на части и: (Множественный выбор / Только один ответ)

---

22. Принципиальным отличием межсетевых экранов от систем обнаружения атак является то, что:

a. МЭ были разработаны для пассивной защиты
b. МЭ работают только на сетевом уровне, а СОВ – еще и на физическом
c. МЭ были разработаны для активного или пассивного обнаружения, а СОВ – для активной или пассивной защиты

ПК-27.1. Принципиальным отличием межсетевых экранов от систем обнаружения атак является то, что: (Множественный выбор / Только один ответ)

23. Прокси-сервер:

a. Обнаруживает вирусы
b. Содержит аутентификационные данные
c. Выполняет функцию посредника между клиентом и сервером

ПК-27.1. Прокси-сервер (Множественный выбор / Только один ответ)

---

24. Прокси-сервер не может:

a. Транслировать IP-адреса
b. Проверять подлинность ресурсов внешней сети
c. Позволить пользователям осуществлять анонимный доступ

ПК-27.1. Прокси-сервер не может: (Множественный выбор / Только один ответ)

---

25. Прокси-сервер, который может анализировать содержимое HTTP-запросов, относится к:

a. Прикладному уровню
b. Уровню соединений
c. Сетевому уровню

ПК-27.1. Прокси-сервер, который может анализировать содержимое HTTP-запросов, относится к: (Множественный выбор / Только один ответ)

---

26. Трансляция IP адресов используемая при межсетевом экранировании позволяет:

a. Сокрыть номера используемых портов
b. Осуществить сокрытие структуры внутренней сети
c. Ускорить работу межсетевого экрана

ПК-27.1. Трансляция IP адресов используемая при межсетевом экранировании позволяет: (Множественный выбор / Только один ответ)

---

27. Узел А сконфигурирован с IP-адресом 192.168.75.34, а узел В сконфигурирован с IP-адресом 192.168.75.50. Оба узла используют одну и ту же маску подсети 255.255.255.240, но не могут направлять друг другу эхо-запрос. Какое сетевое устройство необходимо для того, чтобы эти два узла могли взаимодействовать?

a. Маршрутизатор
b. Концентратор
c. Хаб

ПК-27.1. Узел А сконфигурирован с IP-адресом 192.168.75.34, а узел В сконфигурирован с IP-адресом 192.168.75.50. Оба узла используют одну и ту же маску подсети 255.255.255.240, но не могут направлять друг другу эхо-запрос. Какое сетевое устройство ... (Множественный выбор / Только один ответ)

---

28. Укажите цель ДМЗ?

a. Преобразование внутренних частных адресов во внешние общие адреса
b. Предотвращение или отказ в доступе к сетевому устройству на основе типа используемого приложения
c. Создание среды, в которой сетевые ресурсы могут совместно использоваться внутренними и внешними пользователями

ПК-27.1. Укажите цель ДМЗ? (Множественный выбор / Только один ответ)

29. Шлюзы сеансового уровня осуществляют защиту:

a. Путем фильтрации пакетов согласно правилам на сетевом уровне
b. Используя модули-посредники
c. Путем трансляции IP-адресов

ПК-27.1. Шлюзы сеансового уровня осуществляют защиту: (Множественный выбор / Только один ответ)

---

30. Экранирующий маршрутизатор (пакетный фильтр) осуществляет защиту:

a. Путем фильтрации пакетов согласно правилам на сетевом уровне
b. Используя модули-посредники
c. Путем трансляции IP-адресов

ПК-27.1. Экранирующий маршрутизатор (пакетный фильтр) осуществляет защиту: (Множественный выбор / Только один ответ)
