



Программные и аппаратные средства информационной безопасности.фип_БАК_МОиАИС

- 1 На ваш компьютер пришло сообщение о необходимости пройти тест по курсу компьютерных сетей. Укажите, в какой последовательности при декапсуляции данных будут анализироваться заголовки уровней модели OSI? Ответ приведите для следующего набора уровней: сетевой, канальный, транспортный.
- 2 Какое(ие) из перечисленных устройств является(ются) устройством(ами) канального уровня модели OSI? Выберите все верные ответы.
- 3 Какое(ие) из перечисленных устройств является(ются) устройством(ами) сетевого уровня модели OSI? Выберите все верные ответы.
- 4 Какое(ие) из перечисленных устройств является(ются) устройством(ами) транспортного уровня модели OSI? Выберите все верные ответы.
- 5 Укажите протоколы транспортного уровня модели OSI. Выберите все верные ответы.
- 6 В каком(их) из перечисленных протоколов блоки данных имеют не только заголовок, но и концевик?
- 7 Укажите, какое количество соединений необходимо для построения полносвязанной топологии из 5 устройств?
- 8 Укажите, какое количество соединений необходимо для построения полносвязанной топологии из 10 устройств?
- 9 Как называется система, которая в одном месте хранит информацию о том, какие сети для каких целей использованы, какие в этих сетях ресурсы, сколько адресов выдано (какой % утилизации адресного пространства в той или иной подсети)?





- 10) Клиент отправляет широковещательно сообщение Discover. Наш роутер, на котором настроена функция X, перехватывает это сообщение, сам его не обрабатывает, а отправляет на адрес сервера. Сервер это сообщение обрабатывает, понимает, из какого сегмента пришел запрос, смотрит пул адресов, который соответствует этому сегменту, и отправляет ответ (то есть происходит стандартная процедура получения IP-адреса). Другими словами, роутер «прикидывается» DHCP-сервером, а в реальности пересылает запрос дальше. Укажите, о какой функции протокола DHCP идет речь
- 11) Может ли роутер (в частности, ваш домашний Wi-Fi роутер) выполнять функции DHCP-сервера? В ответе укажите только да или нет.
- 12) Как может выглядеть MAC-адрес отправителя широковещательного фрейма? Выберите все верные ответы.
- 13) Выберите флаг протокола TCP, указывающий на важность = передаются ли в нашем сегменте какие-то важные данные. Если этот флаг поднят, то мы (принимающая сторона) обращаем внимание на поле Urgent point, которое показывает границы важных данных. Если этот флаг опущен, то на поле Urgent point мы, соответственно, смотреть не будем.
- 14) Выберите флаг протокола TCP, который говорит получателю о том, что принятые данные нужно не хранить в буфере, а как можно быстрее передать приложению.
- 15) Выберите флаг(и) протокола TCP, который(ые) используется(ют) для того, чтобы закрыть TCP-сессию
- 16) Сопоставьте поля заголовков протоколов и протоколы, в которых они используются
- 17) Расположите протоколы в порядке возрастания уровня модели OSI, на котором расположен соответствующий протокол?
- 18) Позволяет ли переход от концентраторов к коммутаторам в локальных сетях полностью избавиться от прослушивания сети злоумышленником?
- 19) Какую информацию может предоставить кабельный тестер?





- 20) Системный администратор подключила свой ноутбук к сетевому устройству с надписью Switch на лицевой панели с помощью прямого патч-корда и увидела, что с помощью Auto MDI/MDIX у неё определились следующие параметры работы среды: 100 FX. Может ли она утверждать, что устройство, к которому она подключилась, - коммутатор? Что на это указывает?
- 21) В процессе своей работы коммутатор обучается (learning) на проходящем трафике. Что используется для заполнения мостовой таблицы?
- 22) Какой механизм позволяет ограничить количество изученных MAC-адресов на порту коммутатора?
- 23) Какой механизм позволяет защититься от атак с использованием rogue DHCP-сервер?
- 24) Что такое native-VLAN (выберите максимально подходящий ответ)?
- 25) На что направлена атака DHCP starvation?
- 26) В чём смысл атаки ARP spoofing?
- 27) В чём смысл атаки ARP flooding?
- 28) С помощью какого механизма DHCP-сервер может узнать, к какому порту какого коммутатора подключен DHCP-клиент?
- 29) С помощью какого протокола злоумышленник может узнать подробную информацию о коммутаторе, к которому подключен?
- 30) С помощью какого протокола злоумышленник может удалить всю информацию о виртуальных сетях (VLAN) с коммутаторов?
- 31) С помощью какого протокола можно провести аутентификацию подключаемого к сети устройства?
- 32) С помощью какого пассивного устройства можно получить копию трафика, передаваемого через оптический канал?
- 33) Какое сообщение используется маршрутизатором в протоколе NDP для сообщения о себе, то есть, например, для объявления о том, что данный маршрутизатор можно использовать для выхода из сегмента сети?
- 34) При проведении атаки DHCP starvation появление какого из перечисленных сообщений протокола DHCP не ожидается: Discover, Offer, Request, Release?





- 35) Упорядочите уровни модели OSI (снизу вверх):
- 36) Поставьте в соответствие названия устройств из левого столбца уровням модели OSI из правого столбца.
- 37) Укажите сообщения протокола DHCP в порядке их появления в сети в процессе стандартного получения хостом IP-адреса:
- 38) Поставьте понятию из левого столбца в соответствие уровень модели OSI из правого столбца.
- 39) Укажите цель, которую преследует злоумышленник при использовании VLAN ID Enumeration.
- 40) Как формируется значение BID коммутатора без использования опции Extended System ID? Ответ запишите в виде x/y, где x – длина Bridge Priority в байтах, а y – длина MAC-адреса коммутатора в байтах.
- 41) Как формируется значение BID коммутатора при использовании опции Extended System ID? Ответ запишите в виде x/y/z, где x – длина Bridge Priority в битах, y – длина Extended System ID в битах, а z – длина MAC-адреса коммутатора в битах.
- 42) Какой виртуальной сети (VLAN ID) соответствует следующее значение BID коммутатора - 8315?
- 43) Какую цель преследует злоумышленник при выполнении атаки Eternal Election Attack?
- 44) Какую цель преследует злоумышленник при выполнении атаки Root Disappearance Attack?
- 45) Какую цель преследует злоумышленник при выполнении атаки Merging-splitting of the trees?
- 46) Злоумышленник подключён к одному порту коммутатора доступа. Что из перечисленного ниже поможет защититься от любых STP-атак с его стороны?
- 47) Что из перечисленного ниже может помочь против атак, связанных с перевыборами корневого коммутатора?
- 48) Как называется BPDU, в котором содержится меньшее значение Rood ID?
- 49) Каково значение таймера forwarding delay по умолчанию в классическом протоколе STP?
- 50) Как влияет событие изменение топологии в протоколе STP на время жизни записей в таблице коммутации?





- 51) На таблицы коммутации каких коммутаторов влияет событие изменения топологии в протоколе STP?
- 52) Какая версия протокола STP позволяет построить несколько деревьев, соответствующих независимым топологиям (обычно больше одного, но меньше количества существующих виртуальных сетей (VLAN))?
- 53) Какая версия протокола STP строит столько деревьев, сколько используется виртуальных сетей (VLAN)?
- 54) Какая версия протокола STP всегда строит одно единственное дерево вне зависимости от количества виртуальных сетей (VLAN)?
- 55) Каково значение hello таймера по умолчанию в классическом протоколе STP?
- 56) Как называется опция, позволяющая заблокировать интерфейс коммутатора, если через него было получено любое сообщение STP BPDU?
- 57) Понятиям, технологиям, оптимизациям в левом столбце поставьте в соответствие протоколу, который указан в правом столбце?
- 58) Ролям портов коммутатора из левого столбца поставьте в соответствие версию протокола STP из правого столбца?
- 59) Коммутатор работает в режиме классического STP 802.1D. Расставьте статусы интерфейса, через которые пройдет порт, в соответствующем порядке, если к нему подключают какое-либо устройство:
- 60) Какова длина ключа для протокола симметричного шифрования DES (в битах)?
- 61) Какая длина блока используется при шифровании с помощью протокола DES?
- 62) В чем содержится «весь секрет» алгоритмов симметричного шифрования?
- 63) Какой параметр алгоритма шифр Цезаря можно назвать ключом шифрования?
- 64) Какая суммарная длина ключей в алгоритме шифрования 3DES (в битах)?
- 65) Какие цели преследует нарушитель, пытаясь взломать алгоритм симметричного шифрования?
- 66) Как называется статистическая зависимость между исходным и зашифрованным сообщением?





- 67) Используется ли ключ шифрования при начальной и конечной перестановках (Initial Permission) в алгоритме DES?
- 68) Использует ли алгоритм симметричного шифрования DES классическую сеть Фейстеля? (В ответе укажите только да или нет)
- 69) Как называется «исторический» шифр, в котором каждая буква исходного текста заменялась буквой, стоящей на некоторое фиксированное число мест дальше в алфавите, о применении которого имеются документальные свидетельства?
- 70) Укажите количество раундов в алгоритме симметричного шифрования DES (В ответе укажите только число).
- 71) Что в криптографии называют открытым текстом?
- 72) Укажите, число S-блоков (блоков), используемых в алгоритме симметричного шифрования DES
- 73) Укажите длину ключа раунда для протокола DES в битах
- 74) Сколько ветвей в сети Фейстеля в протоколе DES?
- 75) Требуется ли при шифровании с помощью алгоритмов, использующих сеть Фейстеля, обратимость функции F в сети Фейстеля? (В ответе укажите только да или нет)
- 76) До какой длины (в битах) расширяется во время раунда шифрования правая ветка сети Фейстеля в алгоритме DES?
- 77) Установите соответствие между алгоритмами симметричного шифрования и длинами ключей
- 78) Расположите алгоритмы симметричного шифрования в порядке возрастания их криптографической стойкости
- 79) Изучите структуру функции расширения для алгоритма симметричного шифрования DES. Выпишите номера бит, полученные в первой строке после применения функции расширения (получается таблица из 8 строк, по 6 бит в каждой), если считать, что изначально все биты были занумерованы от 1 до 32. В ответе укажите номера бит без пробелов.
- 80) Какая может быть длина ключа для протокола симметричного шифрования AES (в битах)? Выберите все правильные варианты
- 81) Какая длина блока используется при шифровании с помощью протокола AES?





- 82) В чем содержится «весь секрет» алгоритма симметричного шифрования AES?
- 83) Как называется статистическая зависимость между исходным и зашифрованным сообщением?
- 84) Использует ли алгоритм симметричного шифрования AES классическую сеть Фейстеля? (В ответе укажите только да или нет)
- 85) Укажите количество раундов в алгоритме симметричного шифрования AES при использовании длины ключа и длины блока 128 бит? (В ответе укажите только число).
- 86) Выберите, какие операции используются в алгоритмах симметричного шифрования?
- 87) Требуется ли обратимость преобразований, выполняемых во время раунда в протоколе симметричного шифрования AES? (В ответе укажите только да или нет)
- 88) До какой длины (в битах) расширяется во время раунда шифрования правая ветка сети Фейстеля в алгоритме DES?
- 89) Установите соответствие между алгоритмами симметричного шифрования и длинами ключей
- 90) Расположите функции раунда, используемые в алгоритме в том порядке, в котором они применяются во время раунда шифрования.
- 91) Изучите описание, предложенное ниже и определите, о каком режиме шифрования блоков идет речь. В ответе можно указать аббревиатуру/полное название. Преимущество данного режима заключается в том, что в случае потери пакета при транспорте от отправителя к получателю ничего страшного не произойдет – следующий пакет расшифруется. Однако мы теряем в безопасности, потому что в хвост регистра мы фактически помещаем зашифрованный исходный текст, и можно попытаться перебрать ключи
- 92) Какой алгоритм асимметричного шифрования основан на задаче факторизации числа?
- 93) Верно ли утверждение про алгоритмы асимметричного шифрования: легко вычислить пару (KU, KR). В ответе укажите только да или нет





- 94) Верно ли утверждение про алгоритмы асимметричного шифрования: вычислительно легко зашифровать сообщение, используя открытый ключ (KU). В ответе укажите только да или нет
- 95) Укажите, какой(ие) из предложенных алгоритмов асимметричного шифрования может(гут) использоваться для создания цифровой подписи?
- 96) Верно ли утверждение про алгоритмы асимметричного шифрования: вычислительно легко расшифровать сообщение, используя закрытый ключ (KR). В ответе укажите только да или нет
- 97) Укажите, какой(ие) из предложенных алгоритмов асимметричного шифрования может(гут) использоваться для обмена общим секретом?
- 98) Верно ли утверждение про алгоритмы асимметричного шифрования: вычислительно трудно, зная открытый ключ (KU), найти соответствующий ему закрытый ключ (KR). В ответе укажите только да или нет
- 99) Верно ли утверждение про алгоритмы асимметричного шифрования: вычислительно трудно, зная зашифрованное сообщение (C) и открытый ключ (KU), найти исходное сообщение (M). В ответе укажите только да или нет
- 100) Верно ли утверждение про алгоритмы асимметричного шифрования: трудно вычислить пару (KU, KR). В ответе укажите только да или нет
- 101) Верно ли утверждение про алгоритмы асимметричного шифрования: вычислительно трудно зашифровать сообщение, используя открытый ключ (KU). В ответе укажите только да или нет
- 102) Верно ли утверждение про алгоритмы асимметричного шифрования: вычислительно легко, зная открытый ключ (KU), найти соответствующий ему закрытый ключ (KR). В ответе укажите только да или нет
- 103) Установите соответствие между столбцами слева и справа
- 104) Расположите алгоритмы симметричного шифрования в порядке возрастания их криптографической стойкости
- 105) В алгоритме асимметричного шифрования RSA $p = 5$, $q = 7$. Вычислите значение $\phi(n)$, $n = pq$. В ответе укажите только число.





- 106) Укажите длину хеш-кода для функции MD5 (в битах).
- 107) Укажите, на блоки какой длины разбивается сообщение для хеширования с помощью функции MD5.
- 108) Укажите, на блоки какой длины разбивается сообщение для хеширования с помощью функции SHA-2 [256].
- 109) Укажите, на блоки какой длины разбивается сообщение для хеширования с помощью функции SHA-2 [512].
- 110) Какой может быть длина хеш-кода у функции SHA-2? (Выберите все подходящие варианты)
- 111) Укажите, на блоки какой длины разбивается сообщение для хеширования с помощью функции SHA-2 [384].
- 112) Укажите длину хеш-кода для функции SHA-1 (в битах).
- 113) Какая наименьшая длина хеш-кода может быть у функции SHA-3? (в битах)
- 114) Какая наибольшая длина хеш-кода может быть у функции SHA-3? (в битах)
- 115) Установите соответствие между хеш-функциями и длинами хеш-кодов этих функций
- 116) Расположите хеш-функции в порядке возрастания длины хеш-кода
- 117) Изучите описание, предложенное ниже, и определите, о какой хеш-функции идет речь. В ответе запишите только название хеш-функции, например SHA-1 Алгоритм основан на «принципе губки». Исходное сообщение делится на блоки; используется начальный вектор, который состоит из двух частей r и s . Выполняется XOR r -части с первым блоком, полученный результат и блок с подаются в функцию f и так до тех пор, пока не закончится сообщение. Это так называемая стадия «сжатия». Когда сообщение закончилось, начинается стадия «отжатия»: используется та же функция f , результат выдается до получения хэш-кода нужной длины.
- 118) Как называется протокол, который позволяет спросить у сервера, истек ли сертификат?
- 119) Как называется список недействительных сертификатов, который каждый сертификационный центр выпускает через определенные промежутки времени ΔT (должен быть подписан закрытым ключом CA)?





- 120) Какие значения может принимать поле признак критичности у расширений сертификата X.509?
- 121) Какая версия сертификатов формата X.509 наиболее распространена на сегодняшний день?
- 122) Укажите длину хеш-кода для функции MD5 (в битах).
- 123) Какой формат сертификатов наиболее распространен на сегодняшний день?
- 124) Укажите, на блоки какой длины разбивается сообщение для хеширования с помощью функции SHA-2 [256].
- 125) Укажите, на блоки какой длины разбивается сообщение для хеширования с помощью функции SHA-2 [512].
- 126) Какой может быть длина хеш-кода у функции SHA-2? (Выберите все подходящие варианты)
- 127) Укажите, на блоки какой длины разбивается сообщение для хеширования с помощью функции SHA-2 [384].
- 128) Укажите длину хеш-кода для функции SHA-1 (в битах).
- 129) Какая наименьшая длина хеш-кода может быть у функции SHA-3? (в битах)
- 130) Какая наибольшая длина хеш-кода может быть у функции SHA-3? (в битах)
- 131) Установите соответствие между хеш-функциями и длинами хеш-кодов этих функций
- 132) Расположите хеш-функции в порядке возрастания длины хеш-кода
- 133) Изучите описание, предложенное ниже, и определите, о какой хеш-функции идет речь. В ответе запишите только название хеш-функции, например SHA-1 Алгоритм основан на «принципе губки». Исходное сообщение делится на блоки; используется начальный вектор, который состоит из двух частей g и s . Выполняется XOR g -части с первым блоком, полученный результат и блок s подаются в функцию f и так до тех пор, пока не закончится сообщение. Это так называемая стадия «сжатия». Когда сообщение закончилось, начинается стадия «отжатия»: используется та же функция f , результат выдается до получения хэш-кода нужной длины.
- 134) Какое количество корневых центров сертификации существует на данный момент?





- 135) Каким образом операционная система изначально получает список доверенных корневых центров сертификации?
- 136) Как коротко называется список отозванных сертификатов?
- 137) В чём состоит основной недостаток использования CRL?
- 138) Чей сертификат обычно имеет самый длительный период валидности? Укажите ответ в именительном падеже.
- 139) Может ли сертификат конечного устройства быть заменён раньше окончания срока его действия?
- 140) Может ли электронный сертификат выдаваться строго для определённых целей? Ответ да/нет.
- 141) Для чего используются электронные подписи в сертификате (fingerprints)?
- 142) Может ли маршрутизатор Cisco встраиваться в цепочку доверия с корневым центром сертификации, работающим под управлением операционной системы MS Windows?
- 143) Для чего может использовать сертификаты site-to-site IPSec VPN?
- 144) С помощью какой команды клиентский маршрутизатор Cisco (с настроенным trustpoint) устанавливает отношения доверия с PKI-сервером?
- 145) Какой протокол является альтернативой CRL?
- 146) Для корректного функционирования PKI инфраструктуры критически важно наличие синхронизации времени. По какому протоколу это можно сделать?
- 147) При генерации ключей часто используется опция modulus. За что она отвечает?
- 148) Что выполняет функция grant?
- 149) Какую длину имеет хэш-сумма MD5?
- 150) Какую длину имеет хэш-сумма RSA-1?
- 151) Поставьте в соответствие название хэш-суммы в левом столбце и её длину из правого столбца.





- 152) Запишите в порядке возрастания время жизни следующих сущностей:
- 153) Поставьте в соответствие высказывание из правого столбца методу проверки отозванных сертификатов из левого столбца.
- 154) Между протоколами каких уровней модели OSI располагается заголовок протокола ESP?
- 155) Между протоколами каких уровней модели OSI располагается заголовок протокола AH?
- 156) Целостность каких полей IP-заголовка может проверить протокол AH?
- 157) Между протоколами каких уровней модели OSI может быть расположен заголовок протокола ESP? Выберите все подходящие варианты.
- 158) Между протоколами каких уровней модели OSI может быть расположен заголовок протокола ESP? Выберите все подходящие варианты.
- 159) Целостность каких полей IP-заголовка не может проверить протокол AH?
- 160) Как называется упорядоченный набор записей, в котором содержится действие Action и параметры трафика? В ответе приведите только аббревиатуру данной базы данных на английском языке
- 161) Какой формат сертификатов наиболее распространен на сегодняшний день?
- 162) Какой сервис безопасности может быть обеспечен протоколом ESP и принципиально не обеспечивается протоколом AH?
- 163) Установите соответствие между хеш-функциями и длинами хеш-кодов этих функций
- 164) Расположите хеш-функции в порядке возрастания длины хеш-кода
- 165) Изучите описание, предложенное ниже, и определите, о каком протоколе семейства IPSec идет речь. В ответе запишите только название протокола, например ESP. Данный протокол используется для формирования IPSec SA, проще говоря, согласования работы участников защищенного соединения. Используя этот протокол, участники договариваются, какой алгоритм шифрования будет использоваться, по какому алгоритму будет производиться (и будет ли вообще) проверка целостности, как аутентифицировать друг друга





- 166) Что не является недостатком режима настройки IPSec с использованием криптографических карт?
- 167) В какой фазе установления IPSec соединения используется протокол ISAKMP? Ответ укажите цифрой
- 168) Какова минимальная длина заголовка протокола GRE?
- 169) Какой алгоритм сжатия данных поддерживается в IPSec?
- 170) Какой алгоритм шифрования данных не поддерживается в ISAKMP сессии (на том оборудовании, которое используется в курсе)?
- 171) Для чего в одну криптокарту добавляют несколько записей?
- 172) Что не является преимуществом подхода GRE over IPSec по сравнению с традиционными криптокартами?
- 173) В чём особенность настройки списков доступа (ACL) для отбора «интересного» трафика при использовании криптокарт?
- 174) Чем отличается настройка IPSec VTI от настройки традиционного IPSec с использованием криптокарт?
- 175) В какой ситуации наиболее вероятно использование сертификата для аутентификации, а в какой разделяемого секрета (pre-shared key)?
- 176) Что наиболее точно описывает работу группы Диффи-Хэллмана?
- 177) Что из перечисленного ниже верно описывает разницу между первой и второй версиями протокола IKE?
- 178) Возможно ли АН использовать в туннельном режиме? Ответ да/нет.
- 179) Может ли IPSec с ESP передавать данные открытым? Ответ да/нет.
- 180) Какое минимальное количество байт добавляется к пакету при стандартной GRE инкапсуляции?
- 181) В какой транспортный протокол может инкапсулироваться IPSec?
- 182) Поставьте в соответствие характеристику работы протокола из правого столбца протоколу из левого столбца?
- 183) Запишите алгоритмы шифрования, упорядочив их от самых слабых до наиболее криптостойких: AES, DES, 3DES.





- 184) Запишите режимы настройки IPSec, упорядочив их по времени появления:
- 185) Какой протокол используется для связи между прокси-сервером и сервером антивирусной защиты?
- 186) Корпоративный пользователь просматривает разнообразные ресурсы в Интернет со своего рабочего места. При посещении большинства страниц браузер отображает предупреждение о проблемах с сертификатом сайта. Какова наиболее вероятная причина появления таких предупреждений?
- 187) С помощью какого режима работы ICAP прокси-сервер передает идущий от пользователя в Интернет-трафик на модуль антивирусной защиты?
- 188) С помощью какого режима работы ICAP прокси-сервер передает идущий из сети Интернет в сторону пользователя трафик на модуль антивирусной защиты?
- 189) Что такое межсайтовый скриптинг (XSS-атаки)?
- 190) Что такое атака нулевого дня (zero day)?
- 191) Что из перечисленного ниже является HTTP-запросом?
- 192) Что такое WAF? Напишите расшифровку аббревиатуры.
- 193) Что такое IPS? Напишите расшифровку аббревиатуры.
- 194) Что из перечисленного ниже может рассматриваться в качестве замены (альтернативы) для WAF?
- 195) Как называется атака, при которой злоумышленник внедряет в страницу код, исполняемый в браузере жертвы?
- 196) Как называется атака, при которой злоумышленник вводит код на языке баз данных, исполняемый на стороне сервера?
- 197) Как называется атака, при которой злоумышленник кроме технических средств использует также методы социальной инженерии?
- 198) В каком виде получает информацию WAF, работающий в режиме аудита?
- 199) Выберите модель защиты WAF и правильное описание к ней.





- (200) Что относится к веб-приложениям?
- (201) Чем централизованная антивирусная проверка веб-трафика лучше использования антивирусного ПО, установленного на компьютерах пользователей?
- (202) Расположите устройства в порядке прохождения трафика через них по направлению из Интернет к базе данных:
- (203) Поставьте в соответствие модель защиты WAF и описание.
- (204) Поставьте в соответствие название атаки и её описание.
- (205) Какой протокол используется для передачи электронной почты между почтовыми серверами?
- (206) Какой протокол используется клиентом для получения почты с помощью почтового клиента?
- (207) Какой протокол используется клиентом для доступа к почте с помощью браузера?
- (208) Выберите правильное утверждение.
- (209) Какой тип записи в DNS обычно используется для определения почтовых серверов, отвечающих за домен?
- (210) С помощью какой команды протокола SMTP современный клиент идентифицирует себя?
- (211) Как производится проверка существования домена отправителя электронного письма?
- (212) На чём основана атака SMTP smuggling?
- (213) В чём преимущество для компании, если антивирусная (антифишинговая, антиспам и т.д.) проверка почты выполняется централизованно на шлюзе или SMTP-сервере, а не только средствами антивируса на ПК пользователя?
- (214) Перед вами пример части DKIM-записи из электронного письма сотрудника нашего Университета. С помощью какой команды можно получить открытый ключ для проверки подписи данного письма? DKIM-Signature: v=1; a=rsa-sha256; c=relaxed/simple; d=synergy.ru; s=default; t=1707573465; x=1709387866.





- (215) Вы работаете почтовым администратором в компании. Один из сотрудников обратился к Вам с вопросом о том, что у него не работает отправка почты через наши почтовые сервера и он подозревает, что проблема в том, что во время SMTP-сессии сервер возвращает клиенту код 354. В чём может быть источник проблемы?
- (216) Какой протокол может использоваться для шифрования электронной почты при передаче?
- (217) Какая из команд протокола SMTP может использоваться несколько раз за время отправки клиентом электронного письма?
- (218) Какая команда используется в протоколе SMTP для уведомления противоположной стороны об окончании передачи электронного письма.
- (219) Как называется узел, входящий в цепочку пересылки электронной почты, и не являющийся почтовым сервером?
- (220) С помощью какой команды протокола SMTP отправитель извещает почтовый сервер о начале передачи тела электронного письма?
- (221) Расположите следующие команды в порядке, в котором они появляются в рамках SMTP сессии:
- (222) Вы работаете сетевым администратором в нашем ВУЗе. В логах DNS-сервера, авторитетного для зоны synergy.ru Вы видите запросы с некоторого стороннего сервера электронной почты о TXT-записях для самого домена и некоторых поддоменов. Поставьте в соответствие перечисленные в логах домены и технологии защиты электронной почты, в рамках которых с наибольшей вероятностью производилась проверка.
- (223) Ваш почтовый клиент поддерживает работу нескольких почтовых протоколов. Поставьте в соответствие название протокола и направление передачи почты.
- (224) Что такое пассивный интерфейс в OSPF?
- (225) Какой максимально безопасный метод аутентификации в OSPF?
- (226) В чём суть seq++ атаки на OSPF?
- (227) Что такое unnumbered-интерфейс?
- (228) Какой транспортный протокол используется BGP?





- 229) Что из перечисленного ниже относится к механизмам аутентификации в BGP?
- 230) Какова основная цель использования механизмов TTL-security в BGP?
- 231) С какой целью оператор устанавливает ограничение на количество префиксов, принимаемых от клиента по BGP?
- 232) В чём смысл защиты с использованием IRR?
- 233) В чём смысл атаки LSA flooding?
- 234) Вы снимаете разнообразную статистику с маршрутизаторов в сети. В какой-то момент Вы замечаете, что начался резкий рост счётчика OspfSpfRuns и он продолжается в течение длительного времени. В чём может быть наиболее вероятная причина такого роста?
- 235) С помощью какого механизма можно преодолеть «расщепление горизонта» в BGP?
- 236) Анатолий пытается разобраться в том, как работает TTL Security в BGP и занимается подсчётами вручную. Между двумя BGP-маршрутизаторами находится четыре L3-устройства. Какое максимальное значение поля TTL могут увидеть указанные маршрутизаторы в сообщениях друг от друга?
- 237) Что является этапами внедрения RPKI?
- 238) Укажите номер TCP-порта, который используется для установления соединения.
- 239) В блоки данных какого протокола помещаются сообщения OSPF?
- 240) Какой вспомогательный протокол используется протоколами динамической маршрутизации OSPF и BGP для ускорения детектирования не прямых (indirect) отказов?
- 241) Какие модели внедрения RPKI поддерживает RIPE?
- 242) Сопоставьте термины из правого столбца с протоколами динамической маршрутизации из левого.
- 243) С чем связано ограничение на количество записей IP route records в пакете? Укажите ответ в именительном падеже.
- 244) Какое максимальное количество IP route records может быть в пакете?





- 245) Путь, отображаемый утилитой tracert, ограничен тридцатью хопами. Вы можете написать свою собственную утилиту tracert, сняв ограничение в тридцать хопов. Какое максимальное количество хопов могла бы отображать Ваша утилита, работающая по тому же принципу, что и стандартный tracert (traceroute)?
- 246) Что такое white list?
- 247) Что лежит в основе атаки Ping of Death?
- 248) Что лежит в основе атаки TearDrop?
- 249) Какова наиболее вероятная причина использования злоумышленником маршрутизации от источника?
- 250) Что может стать узлом ботнет?
- 251) Какой тип DDoS атак может быть подавлен непосредственно на площадке заказчика с использованием специализированного оборудования, но без привлечения услуг провайдера или иных компаний?
- 252) В чём суть защиты от атаки SYN flood с помощью SYN cookie?
- 253) Что означает «DNS amplification»?
- 254) При какой атаке рассылается сообщение ICMP echo request на широковещательный адрес подсети?
- 255) При какой атаке злоумышленник отправляет специально подготовленные сегменты TCP, в которых порт отправителя совпадает с портом получателя, а значение IP-адреса получателя совпадает с IP-адресом отправителя?
- 256) Как называется компьютерная сеть, состоящая из некоторого количества хостов с запущенным автономным программным обеспечением. Чаще всего на узлах находится программа, скрытно установленная на устройство жертвы и позволяющая злоумышленнику выполнять некие действия с использованием ресурсов зараженного компьютера?
- 257) Что лежит в основе атак Smurf и Fraggle?
- 258) Каково максимальное смещение фрагмента допустимо в IPv4-сетях?





- 259) Как называется механизм, позволяющий запретить принимать пакеты, если маршрут на отправителя этих пакетов лежит не через тот интерфейс, через который они были получены?
- 260) В заголовке пакета протокола IPv6 отсутствуют опции. Что используется вместо них?
- 261) Поставьте в соответствие название атаки и её описание.
- 262) Расположите протоколы динамической маршрутизации в порядке возрастания AD (с точки зрения Cisco):
- 263) Какое максимальное количество IP route records может быть в пакете?
- 264) Путь, отображаемый утилитой tracert, ограничен тридцатью хопами. Вы можете написать свою собственную утилиту tracert, сняв ограничение в тридцать хопов. Какое максимальное количество хопов могла бы отображать Ваша утилита, работающая по тому же принципу, что и стандартный tracert (traceroute)?
- 265) Что такое white list?
- 266) Что лежит в основе атаки Ping of Death?
- 267) Что лежит в основе атаки TearDrop?
- 268) Какова наиболее вероятная причина использования злоумышленником маршрутизации от источника?
- 269) Что может стать узлом ботнет?
- 270) Какой тип DDoS атак может быть подавлен непосредственно на площадке заказчика с использованием специализированного оборудования, но без привлечения услуг провайдера или иных компаний?
- 271) В чём суть защиты от атаки SYN flood с помощью SYN cookie?
- 272) Что означает «DNS amplification»?
- 273) При какой атаке рассылается сообщение ICMP echo request на широковещательный адрес подсети?
- 274) При какой атаке злоумышленник отправляет специально подготовленные сегменты TCP, в которых порт отправителя совпадает с портом получателя, а значение IP-адреса получателя совпадает с IP-адресом отправителя?





- 275) Как называется компьютерная сеть, состоящая из некоторого количества хостов с запущенным автономным программным обеспечением. Чаще всего на узлах находится программа, скрытно установленная на устройство жертвы и позволяющая злоумышленнику выполнять некие действия с использованием ресурсов зараженного компьютера?
- 276) Что лежит в основе атак Smurf и Fraggle?
- 277) Каково максимальное смещение фрагмента допустимо в IPv4-сетях?
- 278) Как называется механизм, позволяющий запретить принимать пакеты, если маршрут на отправителя этих пакетов лежит не через тот интерфейс, через который они были получены?
- 279) Для чего брандмауэры выполняют сборку пакетов из фрагментов?
- 280) Кто такие скрипт-кидди (script kiddie)?
- 281) В заголовке пакета протокола IPv6 отсутствуют опции. Что используется вместо них?
- 282) Что такое BGP FlowSpec?
- 283) Что (как и BGP FlowSpec) используется для фильтрации трафика в сети оператора?
- 284) Поставьте в соответствие название атаки и ее описание.
- 285) Расположите протоколы динамической маршрутизации в порядке возрастания AD (с точки зрения Cisco):
- 286) Что такое пассивный интерфейс в OSPF?
- 287) Какой максимально безопасный метод аутентификации в OSPF?
- 288) В чём суть seq++ атаки на OSPF?
- 289) Что такое unnumbered-интерфейс?
- 290) Какой транспортный протокол используется BGP?
- 291) Что из перечисленного ниже относится к механизмам аутентификации в BGP?





- (292) Какова основная цель использования механизмов TTL-security в BGP?
- (293) С какой целью оператор устанавливает ограничение на количество префиксов, принимаемых от клиента по BGP?
- (294) В чём смысл защиты с использованием IRR?
- (295) В чём смысл атаки LSA flooding?
- (296) Вы снимаете разнообразную статистику с маршрутизаторов в сети. В какой-то момент Вы замечаете, что начался резкий рост счётчика OspfSpfRuns и он продолжается в течение длительного времени. В чём может быть наиболее вероятная причина такого роста?
- (297) С помощью какого механизма можно преодолеть «расщепление горизонта» в BGP?
- (298) Как работает механизм uRPF?
- (299) В некотором OSPF домене ABR настроен таким образом, что в магистральную зону отдаёт единственный агрегированный префикс (вместо множества мелких). В чём преимущество такого подхода?
- (300) С какой целью используют списки доступа (ACL), разрешающие подключение к порту TCP-179 только с определённых IP-адресов, если сам BGP-протокол не позволит установить BGP-сессию с произвольным адресом?
- (301) От каких атак может защитить использование RPKI совместно с BGP?
- (302) Анатолий пытается разобраться в том, как работает TTL Security в BGP и занимается подсчётами вручную. Между двумя BGP-маршрутизаторами находится четыре L3-устройства. Какое максимальное значение поля TTL могут увидеть указанные маршрутизаторы в сообщениях друг от друга?
- (303) Что является этапами внедрения RPKI?
- (304) Укажите номер TCP-порта, который используется для установления соединения.
- (305) Какой вспомогательный протокол используется протоколами динамической маршрутизации OSPF и BGP для ускорения детектирования не прямых (indirect) отказов?





- 306 Какие модели внедрения RPKI поддерживает RIPE?
- 307 Что из перечисленного ниже должно выполняться при валидации ROA?
- 308 В каком статусе может оказаться префикс в результате проверки?
- 309 Сопоставьте термины из левого столбца с протоколами динамической маршрутизации из правого.
- 310 Запишите в порядке возрастания значений AD следующие протоколы динамической маршрутизации (значения AD считать по принятым в Cisco):
- 311 Запишите в порядке возрастания безопасности методы аутентификации в OSPF:
- 312 Какое количество корневых центров сертификации существует на данный момент?
- 313 Каким образом операционная система изначально получает список доверенных корневых центров сертификации?
- 314 Как коротко называется список отозванных сертификатов?
- 315 В чём состоит основной недостаток использования CRL?
- 316 Чей сертификат обычно имеет самый длительный период валидности? Укажите ответ в именительном падеже.
- 317 Может ли сертификат конечного устройства быть заменён раньше окончания срока его действия?
- 318 Может ли электронный сертификат выдаваться строго для определённых целей? Ответ да/нет.
- 319 Для чего используются электронные подписи в сертификате (fingerprints)?
- 320 Может ли маршрутизатор Cisco встраиваться в цепочку доверия с корневым центром сертификации, работающим под управлением операционной системы MS Windows?
- 321 Для чего может использовать сертификаты site-to-site IPSec VPN?
- 322 С помощью какой команды клиентский маршрутизатор Cisco (с настроенным trustpoint) устанавливает отношения доверия с PKI-сервером?





- 323 Какой протокол является альтернативой CRL?
- 324 Для корректного функционирования PKI инфраструктуры критически важно наличие синхронизации времени. По какому протоколу это можно сделать?
- 325 При генерации ключей часто используется опция modulus. За что она отвечает?
- 326 Что выполняет функция grant?
- 327 Какой вариант детализации при заполнении базы выданных сертификатов отсутствует в настройках PKI-сервера на маршрутизаторе Cisco?
- 328 Какая информация сохраняется в базе сервера PKI при выборе режима детализации «names»?
- 329 Вы добавляете новый маршрутизатор (с рекомендованным в данном курсе ПО) в существующую PKI инфраструктуру. При выполнении процедуры authenticate отображаются две контрольные суммы для валидации сервера PKI. Какой из перечисленных ниже алгоритмов расчёта контрольных сумм входит в указанную пару?
- 330 Какую длину имеет хэш-сумма MD5?
- 331 Какую длину имеет хэш-сумма RSA-1?
- 332 Поставьте в соответствие название хэш-суммы в левом столбце и её длину из правого столбца.
- 333 Запишите в порядке возрастания время жизни следующих сущностей:
- 334 Поставьте в соответствие высказывание из левого столбца методу проверки отозванных сертификатов из правого столбца.
- 335 Что не является недостатком режима настройки IPSec с использованием криптографических карт?
- 336 Какой алгоритм шифрования данных не поддерживается в ISAKMP сессии (на том оборудовании, которое используется в курсе)?
- 337 Для чего в одну криптокарту добавляют несколько записей?
- 338 Что не является преимуществом подхода GRE over IPSec по сравнению с традиционными криптокартами?





- 339 В чём особенность настройки списков доступа (ACL) для отбора «интересного» трафика при использовании криптокарт?
- 340 Чем отличается настройка IPSec VTI от настройки традиционного IPSec с использованием криптокарт?
- 341 В какой ситуации наиболее вероятно использование сертификата для аутентификации, а в какой разделяемого секрета (pre-shared key)?
- 342 Что наиболее точно описывает работу группы Диффи-Хэллмана?
- 343 Что из перечисленного ниже верно описывает разницу между первой и второй версиями протокола IKE?
- 344 Что из перечисленного ниже не является компонентом IPSec?
- 345 Возможно ли АН использовать в туннельном режиме? Ответ да/нет.
- 346 Может ли IPSec с ESP передавать данные открытым? Ответ да/нет.
- 347 Какое минимальное количество байт добавляется к пакету при стандартной GRE инкапсуляции?
- 348 В какой транспортный протокол может инкапсулироваться IPSec?
- 349 Что относят к недостаткам IPSec?
- 350 Что из перечисленного ниже не является задачей, решаемой семейством протоколов IPSec?
- 351 Поставьте в соответствие характеристику работы протокола из левого столбца протоколу из правого столбца?
- 352 Запишите алгоритмы шифрования, упорядочив их от самых слабых до наиболее криптостойких:
- 353 Запишите режимы настройки IPSec, упорядочив их по времени появления:
- 354 Какой протокол используется для связи между прокси-сервером и сервером антивирусной защиты?
- 355 Корпоративный пользователь просматривает разнообразные ресурсы в Интернет со своего рабочего места. При посещении большинства страниц браузер отображает предупреждение о проблемах с сертификатом сайта. Какова наиболее вероятная причина появления таких предупреждений?





- 356 С помощью какого режима работы ICAP прокси-сервер передает идущий от пользователя в Интернет-трафик на модуль антивирусной защиты?
- 357 С помощью какого режима работы ICAP прокси-сервер передает идущий из сети Интернет в сторону пользователя трафик на модуль антивирусной защиты?
- 358 Что такое межсайтовый скриптинг (XSS-атаки)?
- 359 Что такое атака нулевого дня (zero day)?
- 360 Что из перечисленного ниже является HTTP-запросом?
- 361 Что такое WAF? Напишите расшифровку аббревиатуры.
- 362 Что такое IPS? Напишите расшифровку аббревиатуры.
- 363 Что из перечисленного ниже может рассматриваться в качестве замены (альтернативы) для WAF?
- 364 Какой компонент присутствует в модели доступа 3 Tире, но отсутствует в модели доступа 2 Tире?
- 365 Как называется атака, при которой злоумышленник внедряет в страницу код, исполняемый в браузере жертвы?
- 366 Как называется атака, при которой злоумышленник вводит код на языке баз данных, исполняемый на стороне сервера?
- 367 Как называется атака, при которой злоумышленник кроме технических средств использует также методы социальной инженерии?
- 368 В каком виде получает информацию WAF, работающий в режиме аудита?
- 369 Выберите модель защиты WAF и правильное описание к ней.
- 370 Что относится к веб-приложениям?
- 371 Чем централизованная антивирусная проверка веб-трафика лучше использования антивирусного ПО, установленного на компьютерах пользователей?
- 372 Где обычно располагают WAF в корпоративной сети при использовании on-premise подхода?





- 373 Могут ли функции WAF и балансировщика трафика быть совмещены на одном устройстве?
- 374 Могут ли функции WAF и SSL decrypt быть совмещены на одном устройстве?
- 375 Какова основная причина успешности атак SQL injection?
- 376 Что такое фишинговая ссылка?
- 377 Что из перечисленного ниже позволит снизить необходимость в использовании WAF?
- 378 Расположите устройства в порядке прохождения трафика через них по направлению из Интернет к базе данных:
- 379 Поставьте в соответствие модель защиты WAF и описание.
- 380 Поставьте в соответствие название атаки и ее описание.
- 381 Какой протокол используется для передачи электронной почты между почтовыми серверами?
- 382 Какой протокол используется клиентом для получения почты с помощью почтового клиента?
- 383 Какой протокол используется клиентом для доступа к почте с помощью браузера?
- 384 Выберите правильное утверждение.
- 385 Какой тип записи в DNS обычно используется для определения почтовых серверов, отвечающих за домен?
- 386 С помощью какой команды протокола SMTP современный клиент идентифицирует себя?
- 387 Как производится проверка существования домена отправителя электронного письма?
- 388 К DNS записи какого типа необходимо обратиться при выполнении проверки SPF?
- 389 К DNS записи какого типа необходимо обратиться при выполнении проверки DKIM?
- 390 На чём основана атака SMTP smuggling?





- 391) В чём преимущество для компании, если антивирусная (антифишинговая, антиспам и т.д.) проверка почты выполняется централизованно на шлюзе или SMTP-сервере, а не только средствами антивируса на ПК пользователя?
- 392) Перед вами пример части DKIM-записи из электронного письма сотрудника нашего Университета. С помощью какой команды можно получить открытый ключ для проверки подписи данного письма? DKIM-Signature: v=1; a=rsa-sha256; c=relaxed/simple; d=synergy.ru; s=default; t=1707573465; x=1709387866.
- 393) Вы работаете почтовым администратором в компании. Один из сотрудников обратился к Вам с вопросом о том, что у него не работает отправка почты через наши почтовые сервера и он подозревает, что проблема в том, что во время SMTP-сессии сервер возвращает клиенту код 354. В чём может быть источник проблемы?
- 394) Какой протокол может использоваться для шифрования электронной почты при передаче?
- 395) Вы получили письмо от ректора. Какой из перечисленных ниже адресов отправителя вызывает меньше всего доверия как принадлежащий ректору нашего Университета?
- 396) Для чего используется бесплатный сервис DNSBL?
- 397) Что из перечисленного ниже не является политикой DMARC?
- 398) Какая из команд протокола SMTP может использоваться несколько раз за время отправки клиентом электронного письма?
- 399) В каком виде можно указывать разрешённые сервера в SPF-записи?
- 400) Системы защиты электронной почты проверяют не только входящие письма, но и исходящие. Какова наиболее вероятная цель такой проверки?
- 401) Как называется узел, входящий в цепочку пересылки электронной почты, и не являющийся почтовым сервером?
- 402) С помощью какой команды протокола SMTP отправитель извещает почтовый сервер о начале передачи тела электронного письма?
- 403) Расположите следующие команды в порядке, в котором они появляются в рамках SMTP сессии:





- 404 Вы работаете сетевым администратором в нашем ВУЗе. В логах DNS-сервера, авторитетного для зоны synergy.ru Вы видите запросы с некоторого стороннего сервера электронной почты о TXT-записях для самого домена и некоторых поддоменов. Поставьте в соответствие перечисленные в логах домены и технологии защиты электронной почты, в рамках которых с наибольшей вероятностью производилась проверка.
- 405 Укажите цель, которую преследует злоумышленник при использовании VLAN ID Enumeration.
- 406 Какой виртуальной сети (VLAN ID) соответствует следующее значение BID коммутатора - 8315?
- 407 Какую цель преследует злоумышленник при выполнении атаки Eternal Election Attack?
- 408 Какую цель преследует злоумышленник при выполнении атаки Root Disappearance Attack?
- 409 Какую цель преследует злоумышленник при выполнении атаки Merging-splitting of the trees?
- 410 Злоумышленник подключен к одному порту коммутатора доступа. Что из перечисленного ниже поможет защититься от любых STP-атак с его стороны?
- 411 Что из перечисленного ниже может помочь против атак, связанных с перевыборами корневого коммутатора?
- 412 Как называется BPDU, в котором содержится меньшее значение Rood ID?
- 413 Каково значение таймера forwarding delay по умолчанию в классическом протоколе STP?
- 414 Как влияет событие изменение топологии в протоколе STP на время жизни записей в таблице коммутации?
- 415 На таблицы коммутации каких коммутаторов влияет событие изменения топологии в протоколе STP?
- 416 Какая версия протокола STP позволяет построить несколько деревьев, соответствующих независимым топологиям (обычно больше одного, но меньше количества существующих виртуальных сетей (VLAN))?
- 417 Какая версия протокола STP всегда строит одно единственное дерево вне зависимости от количества виртуальных сетей (VLAN)?
- 418 Каково значение hello таймера по умолчанию в классическом протоколе STP?





- 419) Как называется опция, позволяющая заблокировать передачу или приём STP BPDU через определённый интерфейс коммутатора?
- 420) Как называется опция, позволяющая заблокировать интерфейс коммутатора, если через него было получено любое сообщение STP BPDU?
- 421) Как называется опция, позволяющая заблокировать интерфейс коммутатора, если через него было получено superior сообщение STP BPDU?
- 422) Понятиям, технологиям, оптимизациям в левом столбце поставьте в соответствие протоколу, который указан в правом столбце?
- 423) Ролям портов коммутатора из левого столбца поставьте в соответствие версию протокола STP из правого столбца?
- 424) Коммутатор работает в режиме классического STP 802.1D. Расставьте статусы интерфейса, через которые пройдёт порт, в соответствующем порядке, если к нему подключают какое-либо устройство:
- 425) Позволяет ли переход от концентраторов к коммутаторам в локальных сетях полностью избавиться от прослушивания сети злоумышленником?
- 426) Какую информацию может предоставить кабельный тестер?
- 427) Системный администратор подключила свой ноутбук к сетевому устройству с надписью Switch на лицевой панели с помощью прямого патч-корда и увидела, что с помощью Auto MDI/MDIX у неё определились следующие параметры работы среды: 100 FX. Может ли она утверждать, что устройство, к которому она подключилась, - коммутатор? Что на это указывает?
- 428) В процессе своей работы коммутатор обучается (learning) на проходящем трафике. Что используется для заполнения мостовой таблицы?
- 429) Какой механизм позволяет ограничить количество изученных MAC-адресов на порту коммутатора?
- 430) Какой механизм позволяет защититься от атак с использованием rogue DHCP-сервер?
- 431) Что такое native-VLAN (выберите максимально подходящий ответ)?
- 432) На что направлена атака DHCP starvation?





- 433 В чём смысл атаки ARP spoofing?
- 434 В чём смысл атаки ARP flooding?
- 435 С помощью какого механизма DHCP-сервер может узнать, к какому порту какого коммутатора подключен DHCP-клиент?
- 436 С помощью какого протокола злоумышленник может узнать подробную информацию о коммутаторе, к которому подключен?
- 437 С помощью какого протокола злоумышленник может удалить всю информацию о виртуальных сетях (VLAN) с коммутаторов?
- 438 С помощью какого протокола можно провести аутентификацию подключаемого к сети устройства?
- 439 С помощью какого пассивного устройства можно получить копию трафика, передаваемого через оптический канал?
- 440 Какое сообщение используется маршрутизатором в протоколе NDP для сообщения о себе, то есть, например, для объявления о том, что данный маршрутизатор можно использовать для выхода из сегмента сети?
- 441 При проведении атаки DHCP starvation появление какого из перечисленных сообщений протокола DHCP не ожидается: Discover, Offer, Request, Release?
- 442 Какой механизм может использоваться для подавления атаки ARP flooding?
- 443 Для подавления какой атаки может использоваться механизм uRPF?
- 444 Какое устройство вставляет опцию №82 в сообщение протокола DHCP?
- 445 Упорядочите уровни модели OSI (снизу вверх):
- 446 Поставьте в соответствие названия устройств из левого столбца уровням модели OSI из правого столбца.
- 447 Укажите сообщения протокола DHCP в порядке их появления в сети в процессе стандартного получения хостом IP-адреса:
- 448 Поставьте понятию из левого столбца в соответствие уровень модели OSI из правого столбца.





- 449) На ваш компьютер пришло сообщение о необходимости пройти тест по курсу компьютерных сетей. Укажите, в какой последовательности при декапсуляции данных будут анализироваться заголовки уровней модели OSI? Ответ приведите для следующего набора уровней:
- 450) Какое(ие) из перечисленных устройств является(ются) устройством(ами) канального уровня модели OSI? Выберите все верные ответы.
- 451) Какое(ие) из перечисленных устройств является(ются) устройством(ами) сетевого уровня модели OSI? Выберите все верные ответы.
- 452) Какое(ие) из перечисленных устройств является(ются) устройством(ами) транспортного уровня модели OSI? Выберите все верные ответы.
- 453) Укажите протоколы транспортного уровня модели OSI. Выберите все верные ответы.
- 454) В каком(их) из перечисленных протоколов блоки данных имеют не только заголовок, но и концевик?
- 455) Укажите, какое количество соединений необходимо для построения полносвязанной топологии из 5 устройств?
- 456) Укажите, какое количество соединений необходимо для построения полносвязанной топологии из 10 устройств?
- 457) Как называется система, которая в одном месте хранит информацию о том, какие сети для каких целей использованы, какие в этих сетях ресурсы, сколько адресов выдано (какой % утилизации адресного пространства в той или иной подсети)?
- 458) Клиент отправляет широковещательно сообщение Discover. Наш роутер, на котором настроена функция X, перехватывает это сообщение, сам его не обрабатывает, а отправляет на адрес сервера. Сервер это сообщение обрабатывает, понимает, из какого сегмента пришел запрос, смотрит пул адресов, который соответствует этому сегменту, и отправляет ответ (то есть происходит стандартная процедура получения IP-адреса). Другими словами, роутер «прикидывается» DHCP-сервером, а в реальности пересылает запрос дальше. Укажите, о какой функции протокола DHCP идет речь
- 459) Может ли роутер (в частности, ваш домашний Wi-Fi роутер) выполнять функции DHCP-сервера? В ответе укажите только да или нет.





- 460) Как может выглядеть MAC-адрес отправителя широковещательного фрейма? Выберите все верные ответы.
- 461) Выберите флаг протокола TCP, указывающий на важность = передаются ли в нашем сегменте какие-то важные данные. Если этот флаг поднят, то мы (принимающая сторона) обращаем внимание на поле Urgent point, которое показывает границы важных данных. Если этот флаг опущен, то на поле Urgent point мы, соответственно, смотреть не будем.
- 462) Выберите флаг протокола TCP, который говорит получателю о том, что принятые данные нужно не хранить в буфере, а как можно быстрее передать приложению.
- 463) Выберите флаг(и) протокола TCP, который(ые) используется(ют) для того, чтобы закрыть TCP-сессию
- 464) Сопоставьте поля заголовков протоколов и протоколы, в которых они используются
- 465) Расположите протоколы в порядке возрастания уровня модели OSI, на котором расположен соответствующий протокол?
- 466) Какова длина ключа для протокола симметричного шифрования DES (в битах)?
- 467) Какая длина блока используется при шифровании с помощью протокола DES?
- 468) В чем содержится «весь секрет» алгоритмов симметричного шифрования?
- 469) Какой параметр алгоритма шифр Цезаря можно назвать ключом шифрования?
- 470) Какая суммарная длина ключей в алгоритме шифрования 3DES (в битах)?
- 471) Какие цели преследует нарушитель, пытаясь взломать алгоритм симметричного шифрования?
- 472) Как называется статистическая зависимость между исходным и зашифрованным сообщением?
- 473) Используется ли ключ шифрования при начальной и конечной перестановках (Initial Permutation) в алгоритме DES?
- 474) Использует ли алгоритм симметричного шифрования DES классическую сеть Фейштеля? (В ответе укажите только да или нет)





- 475) Как называется «исторический» шифр, в котором каждая буква исходного текста заменялась буквой, стоящей на некоторое фиксированное число мест дальше в алфавите, о применении которого имеются документальные свидетельства?
- 476) Укажите количество раундов в алгоритме симметричного шифрования DES (В ответе укажите только число).
- 477) Что в криптографии называют открытым текстом?
- 478) Укажите, число S-блоков (блоков), используемых в алгоритме симметричного шифрования DES
- 479) Укажите длину ключа раунда для протокола DES в битах
- 480) Сколько ветвей в сети Фейстеля в протоколе DES?
- 481) Требуется ли при шифровании с помощью алгоритмов, использующих сеть Фейстеля, обратимость функции F в сети Фейстеля? (В ответе укажите только да или нет)
- 482) До какой длины (в битах) расширяется во время раунда шифрования правая ветка сети Фейстеля в алгоритме DES?
- 483) Установите соответствие между алгоритмами симметричного шифрования и длинами ключей
- 484) Расположите алгоритмы симметричного шифрования в порядке возрастания их криптографической стойкости
- 485) Изучите структуру функции расширения для алгоритма симметричного шифрования DES. Выпишите номера бит, полученные в первой строке после применения функции расширения (получается таблица из 8 строк, по 6 бит в каждой), если считать, что изначально все биты были занумерованы от 1 до 32. В ответе укажите номера бит без пробелов.
- 486) Какая может быть длина ключа для протокола симметричного шифрования AES (в битах)? Выберите все правильные варианты
- 487) Какая длина блока используется при шифровании с помощью протокола AES?
- 488) В чем содержится «весь секрет» алгоритма симметричного шифрования AES?
- 489) Использует ли алгоритм симметричного шифрования AES классическую сеть Фейстеля? (В ответе укажите только да или нет)





- 490) Укажите количество раундов в алгоритме симметричного шифрования AES при использовании длины ключа и длины блока 128 бит? (В ответе укажите только число).
- 491) Выберите, какие операции используются в алгоритмах симметричного шифрования?
- 492) Требуется ли обратимость преобразований, выполняемых во время раунда в протоколе симметричного шифрования AES? (В ответе укажите только да или нет)
- 493) Расположите функции раунда, используемые в алгоритме в том порядке, в котором они применяются во время раунда шифрования.
- 494) Изучите описание, предложенное ниже и определите, о каком режиме шифрования блоков идет речь. В ответе можно указать аббревиатуру/полное название. Преимущество данного режима заключается в том, что в случае потери пакета при транспорте от отправителя к получателю ничего страшного не произойдет – следующий пакет расшифруется. Однако мы теряем в безопасности, потому что в хвост регистра мы фактически помещаем зашифрованный исходный текст, и можно попытаться перебрать ключи
- 495) Какой алгоритм асимметричного шифрования основан на задаче факторизации числа?
- 496) Верно ли утверждение про алгоритмы асимметричного шифрования: легко вычислить пару (KU, KR). В ответе укажите только да или нет
- 497) Верно ли утверждение про алгоритмы асимметричного шифрования: вычислительно легко зашифровать сообщение, используя открытый ключ (KU). В ответе укажите только да или нет
- 498) Укажите, какой(ие) из предложенных алгоритмов асимметричного шифрования может(гут) использоваться для создания цифровой подписи?
- 499) Верно ли утверждение про алгоритмы асимметричного шифрования: вычислительно легко расшифровать сообщение, используя закрытый ключ (KR). В ответе укажите только да или нет
- 500) Укажите, какой(ие) из предложенных алгоритмов асимметричного шифрования может(гут) использоваться для обмена общим секретом?





- 501) Верно ли утверждение про алгоритмы асимметричного шифрования: вычислительно трудно, зная открытый ключ (KU), найти соответствующий ему закрытый ключ (KR). В ответе укажите только да или нет
- 502) Верно ли утверждение про алгоритмы асимметричного шифрования: вычислительно трудно, зная зашифрованное сообщение (C) и открытый ключ (KU), найти исходное сообщение (M). В ответе укажите только да или нет
- 503) Верно ли утверждение про алгоритмы асимметричного шифрования: трудно вычислить пару (KU, KR). В ответе укажите только да или нет
- 504) Верно ли утверждение про алгоритмы асимметричного шифрования: вычислительно трудно зашифровать сообщение, используя открытый ключ (KU). В ответе укажите только да или нет
- 505) Верно ли утверждение про алгоритмы асимметричного шифрования: вычислительно легко, зная открытый ключ (KU), найти соответствующий ему закрытый ключ (KR). В ответе укажите только да или нет
- 506) Установите соответствие между столбцами слева и справа
- 507) Расположите алгоритмы симметричного шифрования в порядке возрастания их криптографической стойкости
- 508) В алгоритме асимметричного шифрования RSA $p = 5$, $q = 7$. Вычислите значение $\phi(n)$, $n = pq$. В ответе укажите только число.
- 509) Укажите длину хеш-кода для функции MD5 (в битах).
- 510) Укажите, на блоки какой длины разбивается сообщение для хеширования с помощью функции MD5.
- 511) Укажите, на блоки какой длины разбивается сообщение для хеширования с помощью функции SHA-2 [256].
- 512) Укажите длины блоков, на которые разбивается сообщение для хеширования с помощью функции SHA-2 [512].
- 513) Укажите варианты длины хеш-кода для функции SHA-2 (Выберите все подходящие варианты)
- 514) Укажите длины блоков, на которые разбивается сообщение для хеширования с помощью функции SHA-2 [384].
- 515) Какая длина хеш-кода у функции SHA-1? (в битах).





- 516 Укажите наименьшую длину хеш-кода функции SHA-3? (в битах)
- 517 Укажите наибольшую длину хеш-кода для функции SHA-3 (в битах)
- 518 Установите соответствие между хеш-функциями и длинами хеш-кодов этих функций
- 519 Расположите хеш-функции в порядке возрастания длины хеш-кода
- 520 Изучите описание, предложенное ниже, и определите, о какой хеш-функции идет речь. В ответе запишите только название хеш-функции, например SHA-1 Алгоритм основан на «принципе губки». Исходное сообщение делится на блоки; используется начальный вектор, который состоит из двух частей g и s . Выполняется XOR g -части с первым блоком, полученный результат и блок с подаются в функцию f и так до тех пор, пока не закончится сообщение. Это так называемая стадия «сжатия». Когда сообщение закончилось, начинается стадия «отжатия»: используется та же функция f , результат выдается до получения хэш-кода нужной длины.
- 521 Между какими уровнями модели OSI располагается заголовок протокола ESP?
- 522 Между какими уровнями модели OSI располагается заголовок протокола AH?
- 523 Целостность каких полей IP-заголовка может проверить протокол AH?
- 524 Укажите, между какими протоколами может быть расположен заголовок протокола ESP? Выберите все подходящие варианты.
- 525 Укажите, между какими протоколами может быть расположен заголовок протокола ESP? Выберите все варианты, которые могут быть использованы в разобранных на занятиях ситуациях
- 526 Укажите поля IP-заголовка, целостность которых не может проверить протокол AH?
- 527 Как называется упорядоченный набор записей, в котором содержится действие Action и параметры трафика? В ответе приведите только аббревиатуру данной базы данных на английском языке
- 528 Выберите стандарт формата сертификатов, который наиболее распространен на сегодняшний день?





- 529) Какой сервис безопасности может быть обеспечен протоколом ESP и принципиально не обеспечивается протоколом AH?
- 530) Изучите описание, предложенное ниже, и определите протокол семейства IPSec, о котором идет речь. В ответе запишите только название протокола, например, ESP. Данный протокол используется для формирования IPSec SA, проще говоря, согласования работы участников защищенного соединения. Используя этот протокол, участники договариваются, какой алгоритм шифрования будет использоваться, по какому алгоритму будет производиться (и будет ли вообще) проверка целостности, как аутентифицировать друг друга
- 531) Укажите, над протоколами какого уровня модели TCP/IP расположен протокол Записи технологии SSL/TLS?
- 532) Укажите уровни модели TCP/IP, между которыми располагаются протоколы технологии SSL/TLS?
- 533) Конфиденциальность какого протокола можно обеспечить средствами технологии SSL/TLS?
- 534) Конфиденциальность какого протокола можно обеспечить средствами технологии SSL/TLS?
- 535) Конфиденциальность какого протокола можно обеспечить средствами технологии SSL/TLS?
- 536) Выберите протокол, конфиденциальность которого можно обеспечить средствами технологии SSL/TLS
- 537) Как называется упорядоченный набор записей, в котором содержится действие (Action) + параметры трафика? В ответе необходимо привести только аббревиатуру данной базы данных на английском языке
- 538) Выберите протокол, конфиденциальность которого обеспечить средствами технологии SSL/TLS
- 539) Укажите протокол асимметричного шифрования для формирования pre-master secret, который был исключен из технологии TLS 1.3 по сравнению с более ранней версией
- 540) Какое сообщение отправляется первым при установлении соединения между клиентом и сервером по технологии TLS?
- 541) Обязателен ли сертификат со стороны клиента при установке соединения по протоколу TLS? В ответе укажите только да или нет
- 542) Сколько раундов шифрования предусмотрено в алгоритме симметричного шифрования DES? (В ответе укажите только число).





- 543) Что в криптографии понимают под термином «открытый текст»?
- 544) Какое количество S-боксов (блоков), используется в алгоритме симметричного шифрования DES? (В ответе укажите только число)
- 545) Какова длина ключа раунда для протокола DES(ответ приведите в битах)
- 546) Укажите количество ветвей в сети Фейстеля в протоколе DES?
- 547) Какой размер (в битах) достигает правая половина блока данных в процессе одного раунда шифрования в алгоритме DES, когда она расширяется в сети Фейстеля?
- 548) Установите соответствие между версиями протокола TLS и состояниями данных версий
- 549) Над протоколами какого уровня модели TCP/IP располагается протокол Записи технологии SSL/TLS?
- 550) Между протоколами каких уровней модели TCP/IP располагаются протоколы технологии SSL/TLS?
- 551) Как называется упорядоченный набор записей, в котором содержится действие Action и параметры трафика? В ответе приведите только аббревиатуру данной базы данных на английском языке
- 552) Конфиденциальность какого протокола можно обеспечить средствами технологии SSL/TLS?
- 553) Какой протокол асимметричного шифрования для формирования pre-master secret был исключен из технологии TLS 1.3 по сравнению с предыдущей версией?
- 554) С какого сообщения начинается установление соединения между клиентом и сервером по технологии TLS?
- 555) Является ли предоставление сертификата клиента обязательным при установке соединения по протоколу TLS? В ответе укажите только да или нет
- 556) Укажите количество раундов в алгоритме симметричного шифрования DES (В ответе укажите только число).
- 557) Что в криптографии называют открытым текстом?
- 558) Укажите, число S-боксов (блоков), используемых в алгоритме симметричного шифрования DES





- 559) Укажите длину ключа раунда для протокола DES в битах
- 560) Сколько ветвей в сети Фейстеля в протоколе DES?
- 561) Требуется ли при шифровании с помощью алгоритмов, использующих сеть Фейстеля, обратимость функции F в сети Фейстеля? (В ответе укажите только да или нет)
- 562) До какой длины (в битах) расширяется во время раунда шифрования правая ветка сети Фейстеля в алгоритме DES?
- 563) Установите соответствие между версиями протокола TLS и состояниями данных версий
- 564) Расположите хеш-функции в порядке возрастания длины хеш-кода
- 565) Изучите описание, предложенное ниже, и определите, о каком протоколе семейства IPSec идет речь. В ответе запишите только название протокола, например ESP. Данный протокол используется для формирования IPSec SA, проще говоря, согласования работы участников защищенного соединения. Используя этот протокол, участники договариваются, какой алгоритм шифрования будет использоваться, по какому алгоритму будет производиться (и будет ли вообще) проверка целостности, как аутентифицировать друг друга

