Финальный экзамен

Срок Нет срока выполнения **Баллы** 100 **Вопросы** 50
Ограничение времени 60 минут **Разрешенные попытки** 2

Инструкции

Этот тест полностью охватывает содержание курса **Cybersecurity Essentials 1.0.** Он предназначен для проверки знаний и навыков, приобретенных при изучении курса.

Этот тест может содержать задания различных видов.

ПРИМЕЧАНИЕ. В целях содействия обучению в тестах допускается начисление баллов за частично верный ответ по всем типам заданий. **Также при неправильном ответе баллы могут вычитаться.**

Формы 33964 – 33970

Снова принять контрольную работу
(https://685059869.netacad.com/courses/832407/quizzes/7516579/take?user_id=8662160)

История попыток

	Попытка	Время	Оценка
ПОСЛЕДНЯЯ	Попытка 1 (https://685059869.netacad.com/courses/832407/quizzes/7516579/history?version=1)	41 минут(ы)	82 из 100

Оценка за эту попытку: **82** из 100
Отправлено 12 Май в 11:11
Эта попытка длилась 41 минут(ы).

Вопрос 1 **2 / 2 балла (-ов)**

Специалисту по кибербезопасности поручили выявить потенциальных преступников, организовавших атаку на организацию. Какая категория хакеров должна меньше всего интересовать специалиста в такой ситуации?

- «серые» хакеры
- **Верно!** «белые» хакеры
- «черные» хакеры

хакеры-дилетанты

Refer to curriculum topic: 1.2.1
Категории хакеров обозначены цветами, которые соответствуют целям предпринимаемых атак.

Вопрос 2

2 / 2 балла (-ов)

Назовите системы раннего оповещения, которые можно использовать в борьбе с киберпреступниками.

Программа ISO/IEC 27000

Верно!

Проект Honeynet

База данных общих уязвимостей и рисков (CVE)

Infragard

Refer to curriculum topic: 1.2.2
Системы раннего оповещения **помогают** распознать атаки и могут быть эффективным защитным инструментом в руках специалистов по кибербезопасности.

Вопрос 3

2 / 2 балла (-ов)

К какому типу относится атака, при которой злоумышленники формируют пакеты, маскируемые под обычный сетевой трафик, и таким образом вмешиваются в работу сети?

неавторизованная точка доступа Wi-Fi

DNS-подмена

перехватывание пакетов

Верно! подделка пакетов

Refer to curriculum topic: 1.3.1
Специалисты по кибербезопасности должны хорошо понимать механизмы различных видов атак.

Вопрос 4

2 / 2 балла (-ов)

Какая из технологий обеспечивает конфиденциальность данных?

хэширование

Верно! шифрование

RAID

управление идентификационными данными

Refer to curriculum topic: 2.2.1
Специалист по обеспечению кибербезопасности должен быть хорошо знаком с технологиями, реализующими конфиденциальность, целостность и доступность данных.

Вопрос 5

0 / 2 балла (-ов)

К какому типу относятся сети, требующие все больше и больше усилий со стороны специалистов по кибербезопасности из-за распространения концепции BYOD?

то правильный ответ беспроводные сети

проводные сети

сети переноса данных вручную

Ваш ответ

виртуальные сети

Refer to curriculum topic: 2.3.2
Специалист по обеспечению кибербезопасности должен быть осведомлен о видах технологий, которые используются для хранения, передачи и обработки данных.

Вопрос 6

0 / 2 балла (-ов)

К специалисту по безопасности обратились за советом: нужно выбрать механизм безопасности, с помощью которого можно будет исключить доступ неавторизованных хостов в домашнюю сеть сотрудников. Какая мера наиболее эффективна в данном случае?

Применение виртуальной локальной сети.

Ваш ответ

Применение RAID.

то правильный ответ

Внедрение межсетевого экрана.

Внедрение систем обнаружения вторжений.

Refer to curriculum topic: 2.4.1
Для защиты конфиденциальности данных необходимо понимать, какие технологии используются для защиты данных во всех их трех состояниях.

Вопрос 7

2 / 2 балла (-ов)

В каких трех состояниях данные уязвимы для атак? (Выберите три варианта.)

Верно! ☑ передаваемые данные

Верно! ☑ обрабатываемые данные

Верно! ☑ хранимые данные

☐ удаленные данные

☐ расшифрованные данные

☐ зашифрованные данные

Refer to curriculum topic: 2.3.1
Чтобы обеспечить эффективную защиту данных, специалист по кибербезопасности должен понимать суть каждого из трех ключевых состояний. Удаленные данные ранее находились в состоянии хранения. Зашифрованные и расшифрованные данные могут находиться в любом из трех ключевых состояний.

Вопрос 8

2 / 2 балла (-ов)

Два дня в неделю сотрудники организации имеют право работать удаленно, находясь дома. Необходимо обеспечить конфиденциальность передаваемых данных. Какую технологию следует применить в данном случае?

○ сети VLAN

○ RAID

Верно! ◉ VPN

○ SHS

Refer to curriculum topic: 2.4.1
Для защиты конфиденциальности данных необходимо понимать, какие технологии используются для защиты данных во всех их трех состояниях.

Вопрос 9

2 / 2 балла (-ов)

К какому типу относится атака, при которой мошеннические веб-сайты размещаются на высоких позициях в списках результатов веб-поиска?

- атака путем подделки DNS
- Верно! злоупотребление поисковой оптимизацией
- угонщик браузеров
- спам

Refer to curriculum topic: 3.1.2
Специалист по обеспечению кибербезопасности должен быть знаком с особенностями разных видов вредоносного ПО и атак, которые угрожают организации.

Вопрос 10

2 / 2 балла (-ов)

Пользователи не могут получить доступ к базе данных на главном сервере. Администратор базы данных изучает ситуацию и видит, что файл базы данных оказался зашифрован. Затем поступает электронное сообщение с угрозой и требованием выплатить определенную денежную сумму за расшифровку файла базы данных. Назовите тип этой атаки.

- троян

Верно!

- (•) программа-вымогатель
- ( ) атака через посредника
- ( ) DoS-атака

Refer to curriculum topic: 3.1.1
Специалист по обеспечению кибербезопасности должен быть знаком с особенностями разных видов вредоносного ПО и атак, которые угрожают организации.

Вопрос 11

2 / 2 балла (-ов)

Какое из описаний точнее всего соответствует DDoS-атаке?

- ( ) Компьютер принимает пакеты данных, используя MAC-адрес другого компьютера.

Верно!

- (•) Злоумышленник формирует ботнет из компьютеров-зомби.
- ( ) Злоумышленник посылает огромные объемы данных, которые сервер не в состоянии обработать.
- ( ) Злоумышленник отслеживает сетевой трафик, пытаясь обнаружить учетные данные для аутентификации.

Refer to curriculum topic: 3.3.1
Специалист по обеспечению кибербезопасности должен быть знаком с особенностями разных видов вредоносного ПО и атак, которые угрожают организации.

Вопрос 12

0 / 2 балла (-ов)

Пользователи жалуются на низкую скорость доступа в сеть. Опросив сотрудников, сетевой администратор выяснил, что один из них загрузил стороннюю программу сканирования для МФУ. К какой категории относится вредоносное ПО, снижающее производительность сети?

Ваш ответ

- вирус

то правильный ответ

- интернет-червь
- фишинг
- спам

Refer to curriculum topic: 3.1.1
Специалист по обеспечению кибербезопасности должен быть знаком с особенностями разных видов вредоносного ПО и атак, которые угрожают организации.

Вопрос 13

1 / 2 балла (-ов)

Назовите два наиболее эффективных метода защиты от вредоносного ПО. (Выберите два варианта.)

то правильный ответ

- установка и своевременное обновление антивирусного ПО.
- Применение RAID.
- Внедрение межсетевых экранов.
- Внедрение сети VPN.

Верно!

- Своевременное обновление операционной системы и остального программного обеспечения.

Применение надежных паролей.

Refer to curriculum topic: 3.1.1
Специалист по обеспечению кибербезопасности должен знать, какие существуют технологии и средства, которые используются в качестве контрмер для защиты организации от угроз и нейтрализации уязвимостей.

Вопрос 14

2 / 2 балла (-ов)

Руководящий сотрудник компании отправился на важную встречу. Через некоторое время его секретарю звонят и сообщают, что руководитель будет вести важную презентацию, но файлы этой презентации повреждены. Звонящий настойчиво просит секретаря немедленно переслать презентацию на личный адрес электронной почты. Неизвестный также утверждает, что руководитель возлагает ответственность за успех презентации непосредственно на секретаря. К какому типу относится такая тактика социальной инженерии?

- срочность
- доверенные партнеры
- принуждение

Верно!

- близкие отношения

Refer to curriculum topic: 3.2.1
Методы социальной инженерии включают несколько различных тактик для получения информации от жертв.

Вопрос 15

2 / 2 балла (-ов)

Как называется атака, при которой злоумышленник выдает себя за авторизованную сторону и пользуется уже существующими доверительными отношениями между двумя системами?

- прослушивание
- Верно! подмена
- атака через посредника
- рассылка спама

Refer to curriculum topic: 3.3.1
Специалист по обеспечению кибербезопасности должен быть знаком с особенностями разных видов вредоносного ПО и атак, которые угрожают организации.

Вопрос 16

2 / 2 балла (-ов)

Алиса и Боб обмениваются сообщениями, применяя шифрование с открытым ключом. Каким ключом Алиса должна зашифровать сообщение, адресованное Бобу?

- открытый ключ Алисы
- Верно! открытый ключ Боба
- закрытый ключ Алисы
- закрытый ключ Боба

Refer to curriculum topic: 4.1.3
Шифрование — важная технология, предназначенная для защиты конфиденциальности данных. Важно понимать особенности различных методов шифрования.

Вопрос 17

2 / 2 балла (-ов)

В организации планируют провести тренинг по обучению всех сотрудников действующим политикам безопасности. Какой тип контроля доступа стараются применить в организации?

- физический
- логический
- Верно! административный
- технологический

Refer to curriculum topic: 4.2.1
Контроль доступа препятствует получению доступа неавторизованным пользователем к конфиденциальным данным и сетевым системам. Существует несколько технологий, с помощью которых реализуются эффективные стратегии контроля доступа.

Вопрос 18

2 / 2 балла (-ов)

Назовите стратегию контроля доступа, при которой владелец может разрешать или запрещать доступ к конкретному объекту.

- Обязательное разграничение доступа
- Контроль доступа на основе ролей
- Верно! Избирательный контроль доступа
- ACL

Refer to curriculum topic: 4.2.2
Контроль доступа препятствует получению доступа неавторизованным пользователем к конфиденциальным данным и сетевым системам. Существует несколько технологий, с помощью которых реализуются эффективные стратегии контроля доступа.

Вопрос 19

2 / 2 балла (-ов)

Что происходит по мере увеличения длины ключа шифрования?

- Пространство ключей пропорционально уменьшается.
- Пространство ключей пропорционально увеличивается.
- Пространство ключей экспоненциально уменьшается.

Верно!

- Пространство ключей экспоненциально увеличивается.

Refer to curriculum topic: 4.1.4
Шифрование — важная технология, предназначенная для защиты конфиденциальности данных. Важно понимать особенности различных методов шифрования.

Вопрос 20

0 / 2 балла (-ов)

Пользователь хранит большой объем конфиденциальных данных, которые необходимо защитить. Какой алгоритм лучше подходит для решения этой задачи?

- ECC

Ваш ответ

- RSA

то правильный ответ

- 3DES
- алгоритм Диффи-Хеллмана

Refer to curriculum topic: 4.1.4
Шифрование — важная технология, предназначенная для защиты конфиденциальности данных. Важно понимать особенности различных методов шифрования.

Вопрос 21

2 / 2 балла (-ов)

Какой метод применяется в стеганографии для сокрытия текста внутри файла изображения?

- обфускация данных
- маскирование данных
- изменение старшего бита

Верно!

- (•) изменение младшего бита

Refer to curriculum topic: 4.3.2
Шифрование — важная технология, предназначенная для защиты конфиденциальности данных. Важно понимать особенности различных методов шифрования.

Вопрос 22

2 / 2 балла (-ов)

Назовите компонент, представляющий наибольшую сложность при разработке криптосистемы.

Верно!

- (•) управление ключами

обратная разработка

алгоритм шифрования

длина ключа

Refer to curriculum topic: 4.1.1
Шифрование — важная технология, предназначенная для защиты конфиденциальности данных. Важно понимать особенности различных методов шифрования.

Вопрос 23

2 / 2 балла (-ов)

В организации внедрили антивирусное ПО. К какому типу относится это средство контроля безопасности?

Верно!

средства восстановления

средства обнаружения

компенсационные средства контроля

сдерживающие средства контроля

Refer to curriculum topic: 4.2.7
Специалист по обеспечению кибербезопасности должен знать, какие существуют технологии и средства, которые используются в качестве контрмер для защиты организации от угроз и нейтрализации уязвимостей.

Вопрос 24

2 / 2 балла (-ов)

Какую технологию следует внедрить, чтобы пользователь, поставивший подпись под документом, не смог в дальнейшем заявить о том, что не

подписывал этот документ?

- HMAC
- цифровой сертификат
- Верно! цифровая подпись
- асимметричное шифрование

Refer to curriculum topic: 5.2.1
Цифровая подпись позволяет гарантировать подлинность, целостность и невозможность отказа от авторства.

Вопрос 25

2 / 2 балла (-ов)

Ваша организация будет обрабатывать информацию о рыночных сделках. Необходимо будет идентифицировать каждого заказчика, выполняющего транзакцию. Какую технологию следует внедрить, чтобы обеспечить аутентификацию и проверку электронных транзакций заказчиков?

- хеширование данных
- асимметричное шифрование
- Верно! цифровые сертификаты
- симметричное шифрование

Refer to curriculum topic: 5.3.1
Цифровые сертификаты предназначены для защиты участников защищенного информационного обмена.

Вопрос 26

2 / 2 балла (-ов)

Выяснилось, что один из сотрудников организации взламывает пароли административных учетных записей, чтобы получить доступ к конфиденциальной информации о заработной плате. Что следует искать в операционной системе этого сотрудника? (Выберите три варианта.)

- [ ] таблицы алгоритмов
- [ ] хеш-суммы паролей
- [ ] неавторизованные точки доступа
- [x] реверсивные таблицы поиска — Верно!
- [x] радужные таблицы — Верно!
- [x] таблицы поиска — Верно!

Refer to curriculum topic: 5.1.2
Пароли взламываются с помощью таблиц с возможными вариантами паролей.

Вопрос 27

1 / 2 балла (-ов)

Технические специалисты проверяют безопасность системы аутентификации, где применяются пароли. Проверяя таблицы паролей, один из специалистов видит, что пароли сохранены в виде хеш-сумм. Сравнив хеш-сумму простого пароля с хеш-суммой того же пароля из другой системы, специалист обнаруживает, что хеш-суммы не совпадают. Назовите две вероятные причины такого несовпадения. (Выберите два варианта.)

- [x] В системах применяются различные алгоритмы хеширования. — то правильный ответ
- [ ] Обе системы шифруют пароли перед хешированием.

В одной системе применяется симметричное хеширование, в другой — асимметричное.

Верно!

В одной системе применяется только хеширование, тогда как в другой системе, помимо хеширования, применяется механизм добавления соли.

В обеих системах применяется алгоритм MD5.

Refer to curriculum topic: 5.1.2
Хеширование позволяет обеспечить целостность данных в различных ситуациях.

Вопрос 28

2 / 2 балла (-ов)

Вам поручили разъяснить суть механизма проверки данных сотрудникам отдела дебиторской задолженности, выполняющим ввод данных. Выберите наилучший пример для иллюстрации типов данных «строка», «целое число», «десятичная дробь».

800-900-4560, 4040-2020-8978-0090, 21.01.2013

мужчина, 25,25 $, ветеран

Верно!

женщина, 9866, 125,50 $

да/нет 345-60-8745, TRF562

Refer to curriculum topic: 5.4.2
Строка — это набор букв, цифр и специальных символов. Целое число — это число без дробной части. Десятичная дробь — это дробное число в десятичной форме.

Вопрос 29

2 / 2 балла (-ов)

К какой технологии обеспечения безопасности относится стандарт X.509?

- токены безопасности
- технология биометрической идентификации

Верно!

- цифровые сертификаты
- надежные пароли

Refer to curriculum topic: 5.3.2
С помощью цифровых сертификатов обеспечивается безопасность сторон защищенного соединения.

Вопрос 30

2 / 2 балла (-ов)

Какой алгоритм хеширования следует использовать для защиты конфиденциальной несекретной информации?

- 3DES
- MD5

Верно!

- SHA-256
- AES-256

Refer to curriculum topic: 5.1.1
Целостность данных является одним из трех руководящих принципов обеспечения информационной безопасности. Специалист по обеспечению кибербезопасности должен быть знаком со средствами и технологиями, предназначенными для обеспечения целостности данных.

Вопрос 31

2 / 2 балла (-ов)

Алиса и Боб подписывают документы, пользуясь технологией цифровой подписи. Каким ключом Алиса должна подписать документ, чтобы Боб смог удостовериться в том, что этот документ действительно поступил от Алисы?

- закрытый ключ Боба
- **Верно!** закрытый ключ Алисы
- имя пользователя и пароль Алисы
- открытый ключ Боба

Refer to curriculum topic: 5.2.2
На примере Алисы и Боба показан механизм асимметричной криптографии, лежащий в основе технологии цифровой подписи. Алиса шифрует хеш-сумму документа закрытым ключом.
На основе сообщения, зашифрованной хеш-суммы и открытого ключа формируется подписанный документ, который затем отправляется получателю.

Вопрос 32

2 / 2 балла (-ов)

В организации намерены ввести систему маркировки, которая будет отражать ценность, конфиденциальность и важность информации. Какой компонент управления рисками рекомендуется в данном случае?

доступность ресурсов

Верно!

классификация ресурсов

стандартизация ресурсов

идентификация ресурсов

Refer to curriculum topic: 6.2.1
Одна из важнейших составляющих управления рисками — классификация ресурсов.

Вопрос 33

2 / 2 балла (-ов)

К какому типу стратегий снижения рисков относятся такие меры, как приобретение страховки и привлечение сторонних поставщиков услуг?

снижение риска

уклонение от риска

принятие риска

Верно!

передача риска

Refer to curriculum topic: 6.2.1
Меры по снижению рисков уменьшают степень уязвимости организации к угрозам, что достигается за счет передачи, принятия или снижения риска, а также уклонения от него.

Вопрос 34

2 / 2 балла (-ов)

В организации недавно внедрили программу по обеспечению доступности на уровне «пять девяток», которая охватывает два

критически важных сервера баз данных. Какие меры потребуются для реализации этой программы?

- повышение надежности шифрования
- ограничение доступа к данным в этих системах
- Верно! повышение надежности и эксплуатационной готовности серверов
- обеспечение удаленного доступа для тысяч внешних пользователей

Refer to curriculum topic: 6.1.1
Обеспечение доступности систем и данных относится к числу важнейших задач специалистов по кибербезопасности. Необходимо иметь ясное представление о технологиях, процессах и средствах контроля, обеспечивающих высокую доступность.

Вопрос 35

2 / 2 балла (-ов)

В организации устанавливают только те приложения, которые соответствуют внутренним нормам. Все остальные приложения удаляются администраторами в целях усиления безопасности. Как называется этот метод?

- классификация ресурсов
- Верно! стандартизация ресурсов
- идентификация ресурсов
- доступность ресурсов

Refer to curriculum topic: 6.2.1
Организации необходимо знать, какое аппаратное обеспечение и какие программы имеются в наличии, чтобы знать, какими должны быть параметры конфигурации. Управление ресурсами охватывает все имеющееся аппаратное и программное обеспечение. В стандартах ресурсов определены все отдельные продукты аппаратного и программного обеспечения, которые использует и поддерживает организация. В случае сбоя оперативные действия помогут сохранить доступность и безопасность.

Вопрос 36

0 / 2 балла (-ов)

Назовите подход к обеспечению доступности, при котором используются разрешения на доступ к файлам?

Ваш ответ

- (•) сокрытие информации
- ( ) упрощение

то правильный ответ

- ( ) ограничение
- ( ) многоуровневый подход

Refer to curriculum topic: 6.2.2
Обеспечение доступности систем и данных составляет особо важную обязанность специалиста по кибербезопасности. Важно понимать технологии, процессы и средства контроля, с помощью которых обеспечивается высокая доступность.

Вопрос 37

2 / 2 балла (-ов)

Назовите подход к обеспечению доступности, при котором достигается наиболее полная защита благодаря слаженной работе нескольких

механизмов безопасности, предотвращающих атаки?

- ограничение
- Верно! многоуровневый подход
- разнообразие
- сокрытие информации

Refer to curriculum topic: 6.2.2
Многоуровневая защита подразумевает несколько уровней безопасности.

Вопрос 38

0 / 2 балла (-ов)

Доступность на уровне «пять девяток» требуется во многих случаях, однако расходы на ее обеспечение иногда превышают допустимые пределы. В каком случае доступность на уровне «пять девяток» может быть реализована, несмотря на высокие расходы?

- то правильный ответ Нью-Йоркская фондовая биржа
- магазины в местном торговом центре
- Министерство образования США
- Ваш ответ офис спортивной команды высшей лиги

Refer to curriculum topic: 6.1.1
Обеспечение доступности систем и данных составляет особо важную обязанность специалиста по кибербезопасности. Важно понимать технологии, процессы и средства контроля, с помощью которых обеспечивается высокая доступность.

Вопрос 39

2 / 2 балла (-ов)

К какой категории методов аварийного восстановления относится размещение резервных копий на удаленной площадке?

Верно!

- (•) превентивные
- ( ) распознавательные
- ( ) административные
- ( ) корректирующие

Refer to curriculum topic: 6.4.1
План аварийного восстановления помогает подготовить организацию к потенциальным аварийным ситуациям и минимизировать время простоя.

Вопрос 40

1 / 2 балла (-ов)

Назовите два этапа реагирования на инциденты. (Выберите два варианта.)

- [ ] анализ рисков и высокая доступность
- [ ] конфиденциальность и ликвидация
- [ ] предотвращение и изоляция
- [ ] устранение угроз и принятие

то правильный ответ

- [ ] обнаружение и анализ

Верно!

- [x] изоляция и восстановление

Refer to curriculum topic: 6.3.1
Организация должна знать, как реагировать на произошедший инцидент. Необходимо разработать и применять план реагирования на инциденты, включающий несколько этапов.

Вопрос 41

2 / 2 балла (-ов)

Какой из перечисленных инструментов лучше подходит для создания снимка базового состояния операционной системы?

Верно!

- (•) Microsoft Security Baseline Analyzer
- ( ) MS Baseliner
- ( ) SANS Baselining System (SBS)
- ( ) CVE Baseline Analyzer

Refer to curriculum topic: 7.1.1
Существует множество инструментов, с помощью которых специалист по кибербезопасности оценивает потенциальные уязвимости организации.

Вопрос 42

2 / 2 балла (-ов)

Что означает термин «точка баланса вероятностей ошибок», если речь идет о сравнении биометрических систем?

- ( )
количество ложноположительных срабатываний и степень приемлемости
- ( )
степень приемлемости и количество ложноотрицательных срабатываний

Верно!

- (•) количество ложноотрицательных результатов и количество ложноположительных результатов
- ( ) степень неприемлемости и количество ложноотрицательных срабатываний

Refer to curriculum topic: 7.4.1
При сравнении биометрических систем следует учитывать ряд важных факторов, включая точность, скорость (пропускную способность) и степень приемлемости для пользователей.

Вопрос 43

2 / 2 балла (-ов)

Назовите три протокола, допускающие использование симметричного алгоритма блочного шифрования (AES). (Выберите три варианта.)

Верно!

- [x] WPA2
- [ ] 802.11q
- [ ] TKIP
- [ ] WEP

Верно!

- [x] WPA

Верно!

- [x] 802.11i

Refer to curriculum topic: 7.3.1
Защищенную систему связи можно организовать с помощью различных протоколов. Алгоритм AES является наиболее стойким алгоритмом шифрования.

Вопрос 44

2 / 2 балла (-ов)

Назовите стандарт безопасности беспроводных сетей, начиная с которого использование AES и CCM стало обязательным.

- WPA
- WEP
- WEP2
- Верно! WPA2

Refer to curriculum topic: 7.1.2
Безопасность беспроводных сетей определяется соответствующими стандартами, которые постепенно становятся все более и более надежными. На смену WEP пришел стандарт WPA, который уступил место WPA2.

Вопрос 45

2 / 2 балла (-ов)

Какой протокол следует применить, чтобы обеспечить безопасный удаленный доступ для сотрудников, находящихся дома?

- Telnet
- SCP
- Верно! SSH
- WPA

Refer to curriculum topic: 7.2.1
Для организации обмена данными между системами используются различные протоколы уровня приложений. Защищенный протокол позволяет установить защищенное соединение в незащищенной сети.

Вопрос 46

0 / 2 балла (-ов)

Какие атаки можно предотвратить с помощью взаимной аутентификации?

- анализ беспроводного трафика
- беспроводной спам
- подмена IP-адреса отправителя в беспроводных сетях

Ваш ответ

то правильный ответ

- атака через посредника

Refer to curriculum topic: 7.1.2
Специалист по обеспечению кибербезопасности должен знать, какие существуют технологии и средства, которые используются в качестве контрмер для защиты организации от угроз и нейтрализации уязвимостей.

Вопрос 47

2 / 2 балла (-ов)

Какая из утилит использует протокол ICMP?

- DNS
- RIP
- NTP

Верно!

- (•) ping

Refer to curriculum topic: 7.3.1
С помощью протокола ICMP сетевые устройства передают сообщения об ошибках.

Вопрос 48

1 / 2 балла (-ов)

Несанкционированные посетители вошли в офис компании и ходят по зданию. Какие две меры могут предотвратить доступ несанкционированных посетителей в здание? (Выберите два варианта.)

Верно!

- [x] Определение правил и процедур для гостей, посещающих здание
- [ ] Замки на шкафах

то правильный ответ

- [x] Регулярное проведение обучения по вопросам безопасности
- [ ] Запрет на выход из здания в рабочее время

Refer to curriculum topic: 8.1.6
Любое несанкционированное лицо, входящее на объект, может представлять потенциальную угрозу. Общие меры для повышения физической безопасности включают:

- управление доступом и установку средств видеонаблюдения у каждого входа;
- определение правил и процедур для гостей, посещающих объект;
- проверку безопасности здания с помощью физических средств, используемых для тайного получения доступа;
- шифрование пропусков для доступа;
- регулярное проведение обучения по вопросам безопасности;
- внедрение системы маркировки ресурсов.

Вопрос 49

2 / 2 балла (-ов)

Организация внедрила инфраструктуру частного облака. Администратору системы безопасности поручают защитить инфраструктуру от потенциальных угроз. Какие три тактики можно использовать для защиты частного облака? (Выберите три варианта.)

- [ ] Наем консультанта
- [x] Проверка входящего и исходящего трафика — Верно!
- [ ] Предоставление административных прав
- [x] Отключение ping-запросов, зондирования и сканирования портов — Верно!
- [ ] Отключение межсетевых экранов
- [x] Установка на устройства последних исправлений и обновлений для системы безопасности — Верно!

Refer to curriculum topic: 8.1.4
Организации могут управлять угрозами для частного облака следующими способами:

- Отключение ping-запросов, зондирования и сканирования портов.
- Развертывание систем обнаружения и предотвращения вторжений.
- Мониторинг входящего IP-трафика для выявления аномалий.
- Установка на устройства последних исправлений и обновлений для системы безопасности.
- Тест на проникновение после установки настроек.
- Проверка входящего и исходящего трафика.
- Внедрение стандарта классификации данных.
- Отслеживание передаваемых файлов и сканирование для выявления неизвестных типов файлов.

Вопрос 50

2 / 2 балла (-ов)

Что можно использовать для балльной оценки серьезности угроз в целях определения важных уязвимостей?

- Центр реагирования на компьютерные инциденты (CERT)
- ACSC
- Верно! Национальная база данных об уязвимостях (NVD)
- ISC

Refer to curriculum topic: 8.2.3
Национальная база данных об уязвимостях (NVD) используется для оценки серьезности уязвимостей и используется организациями для балльной оценки критичности уязвимостей, обнаруженных в сети.

Оценка контрольной работы: **82** из 100