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=8698891)

История попыток

	Попытка	Время	Оценка
ПОСЛЕДНЯЯ	Попытка 1 (https://685059869.netacad.com/courses/832407/quizzes/7516579/history?version=1)	44 минут(ы)	74,67 из 100

Оценка за эту попытку: **74,67** из 100
Отправлено 21 Май в 12:58
Эта попытка длилась 44 минут(ы).

Вопрос 1 **0 / 2 балла (-ов)**

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

- Программа ISO/IEC 27000
- **Ваш ответ** Infragard
- **то правильный ответ** Проект Honeynet
- База данных общих уязвимостей и рисков (CVE)

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 2

0,67 / 2 балла (-ов)

Специалисту из отдела кадров предложили провести занятия с учащимися государственных школ, чтобы привлечь внимание молодых людей к сфере кибербезопасности. Назовите три темы, которым нужно уделить особое внимание на этих занятиях, чтобы мотивировать учащихся к построению карьеры в этой области? (Выберите три варианта.)

- должность, подразумевающая рутинную повседневную работу
- Верно! высокий спрос на специалистов
- то правильный ответ служение обществу
- необходима докторская степень (PhD)
- Ваш ответ сертификация CompTIA A+ обеспечивает достаточный уровень знаний для начала карьеры
- Верно! высокий доход

Refer to curriculum topic: 1.2.2
Высокий спрос на специалистов по кибербезопасности открывает уникальные карьерные возможности.

Вопрос 3

2 / 2 балла (-ов)

Какое из определений наиболее точно описывает хактивистов?

- Любознательны и осваивают хакерские методы.
- Хотят похвастаться хакерским мастерством.

Верно!

- Входят в протестную группу, действующую ради продвижения некой политической идеи.

- Ищут новые эксплойты.

Refer to curriculum topic: 1.2.1
Для каждой категории киберпреступников характерны определенные мотивы.

Вопрос 4

2 / 2 балла (-ов)

Специалист по кибербезопасности совместно с сотрудниками подразделения ИТ работает над планом информационной безопасности. Какой набор принципов безопасности следует взять за основу при разработке плана информационной безопасности?

- секретность, идентификация, невозможность отказа
- технологии, политики, осведомленность
- шифрование, аутентификация, идентификация

Верно!

- конфиденциальность, целостность, доступность

Refer to curriculum topic: 2.1.1
Конфиденциальность, целостность и доступность берутся за основу при разработке всех систем управления.

Вопрос 5

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?

- RAID
- SHS
- сети VLAN
- Верно! VPN

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 6

2 / 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 RAID.
- Верно! Внедрение межсетевого экрана.
- Внедрение систем обнаружения вторжений.
- Применение виртуальной локальной сети.

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)

Какое состояние данных преобладает в сетевых устройствах хранения данных (NAS) и сетях хранения данных (SAN)?

- передаваемые данные
- Верно! хранимые данные
- обрабатываемые данные
- зашифрованные данные

Refer to curriculum topic: 2.3.1
Специалист по обеспечению кибербезопасности должен быть осведомлен о видах технологий, которые используются для хранения, передачи и обработки данных.

Вопрос 8

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 9

2 / 2 балла (-ов)

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

- рассылка спама
- атака через посредника
- прослушивание

Верно!

- (•) подмена

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 10

2 / 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?

- вирус

Верно!

- (•) 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 11

2 / 2 балла (-ов)

Как называется атака, при которой данные превышают объем памяти, отведенной приложению?

Верно!

переполнение буфера

подмена ОЗУ

внедрение в ОЗУ

внедрение SQL-кода

Refer to curriculum topic: 3.3.3
Специалист по обеспечению кибербезопасности должен быть знаком с особенностями разных видов вредоносного ПО и атак, которые угрожают организации.

Вопрос 12

0 / 2 балла (-ов)

Сотрудники компании получают электронные письма, в которых говорится, что срок действия пароля учетной записи истекает в ближайшее время и поэтому нужно сменить пароль в течение 5 минут. Какое из описаний подходит для такого электронного сообщения?

DDoS-атака.

Атака, при которой злоумышленник выдает себя за авторизованную сторону.

то правильный ответ Обман.

Ваш ответ

Атака, при которой злоумышленник проникает в систему, пользуясь действующим подключением авторизованного пользователя.

Refer to curriculum topic: 3.2.2
Методы социальной инженерии включают несколько различных тактик для получения информации от жертв.

Вопрос 13

2 / 2 балла (-ов)

Назовите нетехнический метод, с помощью которого киберпреступники получают конфиденциальную информацию.

программа-вымогатель

Верно!

социальная инженерия

атака через посредника

фарминг

Refer to curriculum topic: 3.2.1
Специалист по обеспечению кибербезопасности должен быть знаком с особенностями разных видов вредоносного ПО и атак, которые угрожают организации.

Вопрос 14

2 / 2 балла (-ов)

Назовите три лучших способа для защиты от атак с использованием социальной инженерии. (Выберите три варианта.)

Верно!

- [x] Повысить осведомленность сотрудников относительно действующих политик.
- [ ] Увеличить число охранников.
- [ ] Внедрить эффективные межсетевые экраны.

Верно!

- [x] Не вводить пароли в окне чата.
- [ ] Внедрить политику, согласно которой сотрудники ИТ-подразделения имеют право передавать информацию по телефону только руководителям.

Верно!

- [x] Не переходить по ссылкам, вызывающим любопытство.

Refer to curriculum topic: 3.2.2
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 15

2 / 2 балла (-ов)

В компании организовали проверку защищенности сети путем тестирования на проникновение. Проверка показала, что в сети присутствует бэкдор. Какие меры следует принять в этой организации, чтобы выяснить, скомпрометирована ли сеть?

- [ ] Проверить в журнале событий, не было ли изменений в политике.

Верно!

- (•) Проверить системы на наличие неавторизованных учетных записей.
- ( ) Проверить системы на наличие вирусов.
- ( ) Проверить, нет ли учетных записей без паролей.

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 16

0 / 2 балла (-ов)

Алиса и Боб обмениваются конфиденциальными сообщениями, пользуясь общим PSK-ключом. Если Боб пожелает отправить сообщение Кэрол, то каким ключом нужно будет зашифровать это сообщение?

- ( ) открытый ключ Боба
- ( ) закрытый ключ Кэрол

то правильный ответ — новый общий PSK-ключ

Ваш ответ

- (•) общий PSK-ключ, которым шифруются сообщения, адресованные Алисе

Refer to curriculum topic: 4.1.2
Шифрование — важная технология, предназначенная для защиты конфиденциальности данных. Важно понимать особенности различных методов шифрования.

Вопрос 17

0 / 2 балла (-ов)

Какое из утверждений относится к блочным шифрам?

- Блочное шифрование сжимают шифруемую информацию.

то правильный ответ

- При блочном шифровании объем зашифрованных данных обычно больше объема исходных данных.

- Алгоритмы блочного шифрования быстрее алгоритмов поточного шифрования.

Ваш ответ

- Алгоритмы блочного шифрования обрабатывают открытый текст по одному биту и формируют из битов блоки.

Refer to curriculum topic: 4.1.2
Шифрование — важная технология, предназначенная для защиты конфиденциальности данных. Важно понимать особенности различных методов шифрования.

Вопрос 18

2 / 2 балла (-ов)

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

- компенсационные средства контроля
- средства обнаружения

Верно!

- средства восстановления
- 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 19

2 / 2 балла (-ов)

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

Верно!

- (•) административный
- ( ) физический
- ( ) логический
- ( ) 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 20

2 / 2 балла (-ов)

В какой ситуации требуются средства обнаружения?

- ( ) нужно ликвидировать нанесенный организации ущерб

необходимо восстановить нормальное состояние систем после проникновения в сеть организации

нет возможности привлечь сторожевую собаку, поэтому требуется альтернативный вариант

Верно!

- (•) в сети организации нужно выявить запрещенную активность

Refer to curriculum topic: 4.2.7
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 21

0 / 2 балла (-ов)

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

то правильный ответ

- 3DES

Ваш ответ

- (•) ECC

- алгоритм Диффи-Хеллмана

- RSA

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

Вопрос 22

2 / 2 балла (-ов)

Подразделению ИТ поручили внедрить систему, которая будет контролировать полномочия пользователей в корпоративной сети. Какое решение следует применить в этом случае?

- наблюдение за всеми сотрудниками
- устройство считывания отпечатков пальцев
- Верно! набор атрибутов, описывающих права доступа пользователя
- аудит входа пользователей в систему

Refer to curriculum topic: 4.2.5
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 23

2 / 2 балла (-ов)

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

- закрытый ключ Алисы
- открытый ключ Алисы
- Верно! открытый ключ Боба
- 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 24

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
- симметричное шифрование
- Верно! цифровые сертификаты
- асимметричное шифрование

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

Вопрос 25

2 / 2 балла (-ов)

Назовите главную особенность криптографической хеш-функции.

- Верно! Хеш-функция необратима.
- Для хеширования необходимы открытый и закрытый ключи.

По выходному значению хеш-функции можно вычислить входное значение.

Выходные значения имеют различную длину.

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 26

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

Верно!

женщина, 9866, 125,50 $

да/нет 345-60-8745, TRF562

мужчина, 25,25 $, ветеран

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 27

2 / 2 балла (-ов)

Какой алгоритм хеширования следует использовать для защиты конфиденциальной несекретной информации?

Верно!

- [x] SHA-256
- [ ] MD5
- [ ] AES-256
- [ ] 3DES

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 28

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?

- [ ] асимметричное шифрование
- [ ] HMAC
- [ ] цифровой сертификат

Верно!

- [x] цифровая подпись

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

Вопрос 29

0 / 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.)

- [ ] Обе системы шифруют пароли перед хешированием.
- [x] **Ваш ответ** В обеих системах применяется алгоритм MD5.
- [ ] **то правильный ответ** В системах применяются различные алгоритмы хеширования.
- [x] **Верно!** В одной системе применяется только хеширование, тогда как в другой системе, помимо хеширования, применяется механизм добавления соли.
- [ ] В одной системе применяется симметричное хеширование, в другой — асимметричное.

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

Вопрос 30

2 / 2 балла (-ов)

Каким видом целостности обладает база данных, если в каждой ее строке имеется уникальный идентификатор, именуемый первичным ключом?

- [ ] доменная целостность
- [x] **Верно!** сущностная целостность

ссылочная целостность

Определяемая пользователем целостность

Refer to curriculum topic: 5.4.1
Целостность данных является одним из трех руководящих принципов обеспечения информационной безопасности. Специалист по кибербезопасности должен быть знаком со средствами и технологиями обеспечения целостности данных.

Вопрос 31

2 / 2 балла (-ов)

Какая технология хеширования подразумевает обмен ключами?

добавление соли

MD5

Верно!

HMAC

AES

Refer to curriculum topic: 5.1.3
Механизм HMAC отличается от обычного хеширования наличием ключей.

Вопрос 32

0 / 2 балла (-ов)

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

то правильный ответ

превентивные

Ваш ответ

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

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

Вопрос 33

2 / 2 балла (-ов)

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

Верно!

- (•) передача риска
- ( ) уклонение от риска
- ( ) снижение риска
- ( ) принятие 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

0 / 2 балла (-ов)

Риск-менеджер вашей организации представил схему, где уровни угрозы для ключевых ресурсов систем информационной безопасности обозначены тремя цветами. Красный, желтый и зеленый цвета

обозначают соответственно высокий, средний и низкий уровень угрозы. Какому виду анализа рисков соответствует такая схема?

то правильный ответ — качественный анализ

- количественный анализ

Ваш ответ

- анализ степени уязвимости к угрозам

- анализ потерь

Refer to curriculum topic: 6.2.1
Качественный или количественный анализ рисков используется для определения угроз организации и распределения их по приоритетам.

Вопрос 35

2 / 2 балла (-ов)

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

- анализ рисков и высокая доступность

Верно!

- изоляция и восстановление

- предотвращение и изоляция

- устранение угроз и принятие

Верно!

- обнаружение и анализ

- конфиденциальность и ликвидация

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 36

0 / 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
- то правильный ответ стандартизация ресурсов
- идентификация ресурсов
- Ваш ответ 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 37

2 / 2 балла (-ов)

Какие две величины необходимы для расчета ожидаемого годового объема убытков? (Выберите два варианта.)

Верно!
- [x] количество реализаций угрозы в год
- [ ] ценность ресурса

Верно!
- [x] ожидаемый ущерб в результате реализации единичной угрозы
- [ ] мера уязвимости ресурса к угрозе
- [ ] количественная величина убытков
- [ ] коэффициент частоты

Refer to curriculum topic: 6.2.1
При количественном анализе рисков используются следующие величины: ожидаемый ущерб в результате реализации единичной угрозы; количество реализаций угрозы в годовом исчислении; ожидаемый объем убытков в годовом исчислении.

Вопрос 38

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?

- [ ] ограничение доступа к данным в этих системах

Верно!
- [x] повышение надежности и эксплуатационной готовности серверов
- [ ] повышение надежности шифрования
- [ ] 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 39

2 / 2 балла (-ов)

Какому из принципов высокой доступности соответствует формулировка «сохранение доступности в аварийных ситуациях»?

- отказоустойчивость
- бесперебойное обслуживание
- отказоустойчивость системы

Верно!

- единая точка отказа

Refer to curriculum topic: 6.1.1
Высокая доступность достигается следующими методами: полное или частичное исключение ситуаций, при которых отказ единичного компонента влечет за собой отказ всей системы; повышение отказоустойчивости системы в целом; проектирование системы с учетом требований к отказоустойчивости.

Вопрос 40

0 / 2 балла (-ов)

Группа специалистов проводит анализ рисков применительно к сервисам БД. Помимо прочего, специалисты собирают следующую информацию: первоначальная ценность ресурсов; существующие угрозы для этих ресурсов; ущерб, который могут нанести эти угрозы. На основании собранной информации специалисты рассчитывают

ожидаемый годовой объем убытков. Какой вид анализа рисков выполняет группа?

- анализ защищенности
- то правильный ответ: количественный анализ
- Ваш ответ: анализ потерь
- качественный анализ

Refer to curriculum topic: 6.2.1
Качественный или количественный анализ рисков используется для определения угроз организации и распределения их по приоритетам.

Вопрос 41

0 / 2 балла (-ов)

Какой инструмент Windows следует использовать для настройки политики паролей и политики блокировки учетных записей в системе, которая не входит в домен?

- Журнал безопасности в средстве просмотра событий
- Управление компьютером
- Ваш ответ: Инструмент «Безопасность Active Directory»
- то правильный ответ: Оснастка «Локальная политика безопасности»

Refer to curriculum topic: 7.2.2
Специалист по обеспечению кибербезопасности должен знать, какие существуют технологии и средства, которые используются в качестве контрмер для защиты организации от угроз и нейтрализации уязвимостей. Параметры безопасности настраиваются в оснастках Windows «Локальная политика безопасности», «Просмотр событий» и «Управление компьютером».

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
- степень неприемлемости и количество ложноотрицательных срабатываний

Верно!

- количество ложноотрицательных результатов и количество ложноположительных результатов

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)

Какое из перечисленных утверждений точнее всего соответствует забору высотой в 1 метр?

- Забор ненадолго задержит нарушителя, намеренно проникающего на территорию.

Верно!

- Забор сдерживает только случайных прохожих.

- Забор ограждает территорию от случайных прохожих благодаря своей высоте.

- Забор сможет противостоять нарушителю, намеренно проникающему на территорию.

Refer to curriculum topic: 7.4.1
Существуют стандарты безопасности, помогающие внедрить адекватные средства контроля доступа в организациях для устранения потенциальных угроз. Эффективность защиты территории от проникновения посторонних определяется высотой забора.

Вопрос 44

2 / 2 балла (-ов)

Какие атаки можно предотвратить с помощью взаимной аутентификации?

- анализ беспроводного трафика

- беспроводной спам

Верно!

- атака через посредника

- подмена IP-адреса отправителя в беспроводных сетях

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 45

2 / 2 балла (-ов)

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

- [x] WPA2 — Верно!
- [x] WPA — Верно!
- [ ] TKIP
- [ ] 802.11q
- [ ] WEP
- [x] 802.11i — Верно!

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

Вопрос 46

2 / 2 балла (-ов)

Какую технологию можно использовать для защиты от несанкционированного прослушивания голосового трафика, передаваемого с помощью VoIP-соединений?

сильная аутентификация

SSH

ARP

Верно!

шифрование голосового трафика

Refer to curriculum topic: 7.3.2
Многие передовые технологии, включая VoIP, передачу потокового видео и конференц-связь, требуют соответствующих мер безопасности.

Вопрос 47

0 / 2 балла (-ов)

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

то правильный ответ

Microsoft Security Baseline Analyzer

MS Baseliner

Ваш ответ

CVE Baseline Analyzer

SANS Baselining System (SBS)

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

Вопрос 48

2 / 2 балла (-ов)

В компании, которая обрабатывает информацию о кредитных картах, происходит нарушение безопасности. Какой отраслевой закон регулирует защиту данных кредитной карты?

Верно!

- (•) Стандарт безопасности данных индустрии платежных карт (PCI DSS)
- ( ) Закон Грэмма — Лича — Блайли (GLBA)
- ( ) Закон Сарбейнса — Оксли (SOX)
- ( ) Закон о тайне обмена электронной информацией (ECPA)

Refer to curriculum topic: 8.2.2
Стандарт безопасности данных индустрии платежных карт (PCI DSS) представляет собой набор правил для защиты данных кредитных карт, которыми обмениваются банки и продавцы при совершении транзакции.

Вопрос 49

2 / 2 балла (-ов)

Аудитору предлагают оценить потенциальные угрозы для локальной сети компании. Какие три потенциальные угрозы может отметить аудитор? (Выберите три варианта.)

Верно!

- [x] Неправильно настроенный межсетевой экран
- [ ] Политика допустимого использования

Верно!

- [x] Несанкционированное сканирование портов и зондирования сети

Верно!

- [x] Открытый доступ к сетевому оборудованию
- [ ] Закрытый доступ к системам
- [ ] Сложные пароли

Refer to curriculum topic: 8.1.3
К локальной сети может быть подключено множество оконечных устройств. Анализ сетевых и подключенных оконечных устройств важен для определения угроз.

Вопрос 50

2 / 2 балла (-ов)

Каковы две потенциальные угрозы для приложений? (Выберите два варианта.)

Верно! ☑ несанкционированный доступ

Верно! ☑ потеря данных

☐ Перебои питания

☐ социальная инженерия

Refer to curriculum topic: 8.1.7
Угрозы для приложений могут включать:

- несанкционированный доступ к центрам обработки данных, машинным залам и коммутационным шкафам;
- остановку сервера для технического обслуживания;
- уязвимость ПО сетевой операционной системы;
- несанкционированный доступ к системам;
- потерю данных;
- продолжительный простой информационных систем;
- уязвимости, возникающие при разработке клиентских, серверных и веб-приложений.

Оценка контрольной работы: **74,67** из 100