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=8698880)

История попыток

	Попытка	Время	Оценка
ПОСЛЕДНЯЯ	Попытка 1 (https://685059869.netacad.com/courses/832407/quizzes/7516579/history?version=1)	49 минут(ы)	71,33 из 100

Оценка за эту попытку: **71,33** из 100
Отправлено 18 Май в 17:25
Эта попытка длилась 49 минут(ы).

Вопрос 1 **2 / 2 балла (-ов)**

Назовите две группы лиц, которые относятся к категории внутренних злоумышленников. (Выберите два варианта.)

- ☐ «черные» хакеры
- ☐ кибермастера
- ☐ непрофессионалы
- ☑ бывшие сотрудники

Верно!

- [ ] хактивисты

Верно!

- [x] доверенные партнеры

Refer to curriculum topic: 1.4.1
Угрозы делятся на внешние и внутренние. Специалист по кибербезопасности должен иметь ясное представление о возможных источниках угроз.

Вопрос 2

2 / 2 балла (-ов)

Такие технологии, как IoE и GIS, способствуют накоплению огромных объемов данных. Назовите две причины, в силу которых эти технологии увеличивают спрос на специалистов по кибербезопасности. (Выберите два варианта.)

Верно!

- [x] В системах, созданных на основе этих технологий, хранятся персональные данные.

- [ ] Требуется больше ресурсов для обработки данных.

- [ ] Необходим круглосуточный мониторинг.

Верно!

- [x] С помощью этих технологий ведется сбор конфиденциальной информации.

- [ ] Требуется больше оборудования.

- [ ] Эти технологии усложняют структуру систем.

Refer to curriculum topic: 1.1.1
Растущая необходимость в надежной защите продиктована характером данных, собираемых с помощью этих технологий.

Вопрос 3

0 / 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?

- «черные» хакеры
- то правильный ответ «белые» хакеры
- «серые» хакеры
- Ваш ответ хакеры-дилетанты

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

Вопрос 4

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?

- Ваш ответ Применение виртуальной локальной сети.
- Внедрение систем обнаружения вторжений.
- Применение RAID.
- то правильный ответ Внедрение межсетевого экрана.

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 5

2 / 2 балла (-ов)

Назовите методы, с помощью которых можно внедрить многофакторную аутентификацию.

- системы IDS и IPS
- Верно! пароли и отпечатки пальцев
- токены и хеш-суммы
- сети VPN и VLAN

Refer to curriculum topic: 2.2.1
Специалист по обеспечению кибербезопасности должен знать, какие существуют технологии для поддержки триады «конфиденциальность, целостность, доступность».

Вопрос 6

2 / 2 балла (-ов)

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

- сети переноса данных вручную
- Верно! беспроводные сети
- проводные сети

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 7

2 / 2 балла (-ов)

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

Верно!

- (•) хранимые данные
- ( ) обрабатываемые данные
- ( ) передаваемые 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

0,67 / 2 балла (-ов)

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

- [ ] зашифрованные данные

Верно!

- [x] обрабатываемые данные

то правильный ответ хранимые данные

Ваш ответ

- [x] расшифрованные данные

Верно!

- [x] передаваемые данные
- [ ] удаленные 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 9

0 / 2 балла (-ов)

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

Ваш ответ

- (•) атака через посредника
- ( ) рассылка спама

то правильный ответ подмена

- ( ) прослушивание

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)

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

- [ ] Применение надежных паролей.
- [x] Установка и своевременное обновление антивирусного ПО.

Верно!

- [ ] Применение RAID.
- [ ] Внедрение межсетевых экранов.
- [x] Своевременное обновление операционной системы и остального программного обеспечения.

Верно!

- [ ] Внедрение сети VPN.

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 11

0 / 2 балла (-ов)

Какое из описаний точнее всего соответствует DDoS-атаке?

Ваш ответ

- (•) Злоумышленник посылает огромные объемы данных, которые сервер не в состоянии обработать.
- ( ) Компьютер принимает пакеты данных, используя MAC-адрес другого компьютера.

Злоумышленник отслеживает сетевой трафик, пытаясь обнаружить учетные данные для аутентификации.

то правильный ответ Злоумышленник формирует ботнет из компьютеров-зомби.

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)

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?

близкие отношения

Ваш ответ срочность

доверенные партнеры

то правильный ответ принуждение

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

Вопрос 13

2 / 2 балла (-ов)

К какому типу относится атака, при которой сотрудник подключает к сети организации неавторизованное устройство для отслеживания сетевого трафика?

- фишинг
- подмена
- рассылка спама
- прослушивание

Верно!

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 14

2 / 2 балла (-ов)

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

- подмена ОЗУ
- переполнение буфера

Верно!

- 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 15

0,67 / 2 балла (-ов)

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

то правильный ответ

- [ ] Не вводить пароли в окне чата.
- [ ] Внедрить эффективные межсетевые экраны.

Верно!

- [x] Повысить осведомленность сотрудников относительно действующих политик.

Ваш ответ

- [x] Внедрить политику, согласно которой сотрудники ИТ-подразделения имеют право передавать информацию по телефону только руководителям.

Верно!

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

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 16

2 / 2 балла (-ов)

Назовите компонент, представляющий наибольшую сложность при разработке криптосистемы.

- обратная разработка
- Верно! управление ключами
- 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 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?

- Верно! административный
- физический
- технологический
- логический

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)

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 19

0 / 2 балла (-ов)

Какой алгоритм применяется в Windows по умолчанию при шифровании файлов и папок на томе NTFS?

то правильный ответ

- AES

Ваш ответ

- (•) RSA
- ( ) DES
- ( ) 3DES

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

Вопрос 20

2 / 2 балла (-ов)

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

- изменение старшего бита
- маскирование данных

Верно!

- изменение младшего бита
- обфускация данных

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

Вопрос 21

2 / 2 балла (-ов)

В какой ситуации требуются средства обнаружения?

Верно!

- в сети организации нужно выявить запрещенную активность
- нужно ликвидировать нанесенный организации ущерб
- нет возможности привлечь сторожевую собаку, поэтому требуется альтернативный вариант

необходимо восстановить нормальное состояние систем после проникновения в сеть организации

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 22

0 / 2 балла (-ов)

Какие средства контроля доступа должны будут применить сотрудники подразделения ИТ, чтобы восстановить нормальное состояние системы?

компенсирующие

Ваш ответ

превентивные

распознавательные

то правильный ответ

корректирующие

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 23

0 / 2 балла (-ов)

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

- ACL
- Обязательное разграничение доступа

то правильный ответ — Избирательный контроль доступа

Ваш ответ — Контроль доступа на основе ролей

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 24

2 / 2 балла (-ов)

Вам поручили внедрить систему обеспечения целостности данных для защиты файлов, загружаемых сотрудниками отдела продаж. Вы намерены применить самый стойкий из всех алгоритмов хеширования, имеющихся в системах вашей организации. Какой алгоритм хеширования вы выберете?

Верно! — SHA-256

- SHA-1
- AES
- MD5

Refer to curriculum topic: 5.1.1
На практике чаще всего применяются алгоритмы хеширования MD5 и SHA. SHA-256 формирует хеш-сумму длиной в 256 бит, тогда как длина хеш-суммы MD5 составляет 128 бит.

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?

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

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

Вопрос 26

2 / 2 балла (-ов)

Какой алгоритм хеширования следует использовать для защиты конфиденциальной несекретной информации?

- MD5
- Верно! SHA-256

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 27

2 / 2 балла (-ов)

Какую технологию следует внедрить, чтобы иметь возможность идентифицировать организацию, выполнить аутентификацию веб-сайта этой организации и установить зашифрованное соединение между клиентом и веб-сайтом?

добавление соли

Верно!

цифровой сертификат

асимметричное шифрование

цифровая подпись

Refer to curriculum topic: 5.2.2
Шифрование — важная технология, предназначенная для защиты конфиденциальности данных. Важно понимать особенности различных методов шифрования.

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».

- мужчина, 25,25 $, ветеран
- 800-900-4560, 4040-2020-8978-0090, 21.01.2013
- 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)

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

- ссылочная целостность
- Определяемая пользователем целостность
- доменная целостность
- Верно! сущностная 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 30

2 / 2 балла (-ов)

В организации только что завершили аудит безопасности. Согласно результатам аудита, в вашем подразделении не обеспечено соответствие требованиям стандарта X.509. Какие средства контроля безопасности нужно проверить в первую очередь?

- операции хеширования
- сети VPN и сервисы шифрования
- правила проверки данных

Верно!

- цифровые сертификаты

Refer to curriculum topic: 5.3.2
Цифровые сертификаты предназначены для защиты участников защищенного информационного обмена.

Вопрос 31

2 / 2 балла (-ов)

К какой технологии обеспечения безопасности относится стандарт X.509?

- надежные пароли

Верно!

- цифровые сертификаты

токены безопасности

технология биометрической идентификации

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

Вопрос 32

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

качественный анализ

то правильный ответ количественный анализ

Ваш ответ

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 33

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

Ваш ответ

- (•) анализ степени уязвимости к угрозам
- ( ) анализ потерь
- ( ) количественный анализ

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

Вопрос 34

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?

Верно!

- (•) классификация ресурсов
- ( ) идентификация ресурсов
- ( ) доступность ресурсов
- ( ) стандартизация ресурсов

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

Вопрос 35

2 / 2 балла (-ов)

Понимание и выявление уязвимостей относятся к числу важнейших задач специалиста по кибербезопасности. Назовите ресурсы, с помощью которых можно получить подробную информацию об уязвимостях.

- Архитектура NIST/NICE
- Верно! Национальная база данных общих уязвимостей и рисков (CVE)
- Infragard
- Модель ISO/IEC 27000

Refer to curriculum topic: 6.2.1
Специалист по кибербезопасности должен быть знаком с такими ресурсами, как База данных общих уязвимостей и рисков (CVE), Infragard и классификация NIST/NISE Framework. Эти ресурсы облегчают задачу планирования и внедрения эффективной системы управления информационной безопасностью.

Вопрос 36

2 / 2 балла (-ов)

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

- единая точка отказа
- отказоустойчивость

- бесперебойное обслуживание

Верно!

- отказоустойчивость системы

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 37

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?

Верно!

- стандартизация ресурсов
- идентификация ресурсов
- доступность ресурсов
- классификация 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 38

2 / 2 балла (-ов)

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

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

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 39

2 / 2 балла (-ов)

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

- принятие риска
- Верно! передача риска
- уклонение от риска
- снижение 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 40

2 / 2 балла (-ов)

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

- распознавательные
- корректирующие
- административные
- Верно! превентивные

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

Вопрос 41

0 / 2 балла (-ов)

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

- SCP
- то правильный ответ SSH
- Ваш ответ WPA
- Telnet

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 42

2 / 2 балла (-ов)

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

- сильная аутентификация
- ARP
- Верно! шифрование голосового трафика
- SSH

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

Вопрос 43

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?

то правильный ответ

- Оснастка «Локальная политика безопасности»
- Журнал безопасности в средстве просмотра событий
- Управление компьютером

Ваш ответ

- Инструмент «Безопасность Active Directory»

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 44

0 / 2 балла (-ов)

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

Забор сможет противостоять нарушителю, намеренно проникающему на территорию.

Забор ненадолго задержит нарушителя, намеренно проникающего на территорию.

Ваш ответ

Забор ограждает территорию от случайных прохожих благодаря своей высоте.

то правильный ответ Забор сдерживает только случайных прохожих.

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 45

2 / 2 балла (-ов)

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

802.11q

WEP

Верно! 802.11i

Верно! WPA2

Верно! WPA

TKIP

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)

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 47

2 / 2 балла (-ов)

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

- WEP2
- WPA
- Верно! WPA2

WEP

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 48

2 / 2 балла (-ов)

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

Верно! ☑ Открытый доступ к сетевому оборудованию

☐ Сложные пароли

Верно! ☑ Неправильно настроенный межсетевой экран

Верно! ☑ Несанкционированное сканирование портов и зондирования сети

☐ Политика допустимого использования

☐ Закрытый доступ к системам

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 49

2 / 2 балла (-ов)

Компания пытается снизить затраты на развертывание коммерческого программного обеспечения и рассматривает возможность использования облачных служб. Какая облачная служба будет наилучшей для размещения программного обеспечения?

- Платформа как услуга (PaaS)
- Инфраструктура как услуга (IaaS)

Верно!

- ПО как услуга (SaaS)
- Восстановление как услуга (RaaS)

Refer to curriculum topic: 8.1.5
Программное обеспечение как услуга (SaaS) обеспечивает пользователям доступ к централизованно размещенному в облаке программному обеспечению через веб-обозреватель.

Вопрос 50

2 / 2 балла (-ов)

Специалисту по безопасности предлагают выполнить анализ текущего состояния сети компании. Какой инструмент будет использовать специалист по безопасности для сканирования сети исключительно в целях выявления угроз безопасности?

- Вредоносное ПО
- Анализатор пакетов
- Испытание на проникновение

Верно!

- Сканер уязвимостей

Refer to curriculum topic: 8.2.4
Сканеры уязвимостей обычно используются для выявления:

- использования паролей по умолчанию или распространенных паролей;
- неустановленных исправлений;
- открытых портов;
- неправильной настройки операционных систем и ПО;
- активных IP-адресов.

Оценка контрольной работы: **71,33** из 100