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

История попыток

	Попытка	Время	Оценка
СОХРАНЕННАЯ	**Попытка 2 (https://685059869.netacad.com/courses/832407/quizzes/7516579/history?version=2)**	41 минут(ы)	80 из 100
ПОСЛЕДНЯЯ	**Попытка 2 (https://685059869.netacad.com/courses/832407/quizzes/7516579/history?version=2)**	41 минут(ы)	80 из 100
	Попытка 1 (https://685059869.netacad.com/courses/832407/quizzes/7516579/history?version=1)	60 минут(ы)	0 из 100

Оценка за эту попытку: **80** из 100
Отправлено 25 Май в 11:10
Эта попытка длилась 41 минут(ы).

Вопрос 1 **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?

- DNS-подмена
- перехватывание пакетов
- неавторизованная точка доступа Wi-Fi

Верно!

- (•) подделка пакетов

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

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] С помощью этих технологий ведется сбор конфиденциальной информации.
- [ ] Требуется больше ресурсов для обработки данных.
- [ ] Необходим круглосуточный мониторинг.
- [ ] Требуется больше оборудования.

Верно!

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

2 / 2 балла (-ов)

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

- База данных общих уязвимостей и рисков (CVE)
- Программа ISO/IEC 27000
- Infragard
- Проект Honeynet

Верно!

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 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?

- конфиденциальность, целостность, доступность
- шифрование, аутентификация, идентификация
- секретность, идентификация, невозможность отказа
- технологии, политики, осведомленность

Верно!

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)

Назовите технологию, с помощью которой можно было бы в принудительном порядке обеспечить соблюдение политики безопасности, согласно которой вычислительное устройство может быть подключено к сети комплекса зданий лишь при условии, что на этом устройстве установлено последнее обновление антивирусного ПО.

- VPN
- сеть хранения данных (SAN)
- NAS
- Верно! NAC

Refer to curriculum topic: 2.4.1
Специалист по кибербезопасности должен быть хорошо знаком с современными технологиями, позволяющими усилить политику безопасности, действующую в его организации.

Вопрос 6

2 / 2 балла (-ов)

Какая из технологий обеспечивает конфиденциальность данных?

- RAID
- хэширование
- Верно! шифрование
- 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 7

2 / 2 балла (-ов)

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

Верно!

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

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.
- ( ) Применение RAID.

Внедрение систем обнаружения вторжений.

Верно!

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 9

2 / 2 балла (-ов)

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

угонщик браузеров

Верно!

злоупотребление поисковой оптимизацией

атака путем подделки DNS

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)

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

Применение RAID.

Применение надежных паролей.

Внедрение межсетевых экранов.

Верно! Установка и своевременное обновление антивирусного ПО.

Верно! Своевременное обновление операционной системы и остального программного обеспечения.

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)

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 системы на наличие вирусов.

Ваш ответ Проверить, нет ли учетных записей без паролей.

то правильный ответ Проверить системы на наличие неавторизованных учетных записей.

Проверить в журнале событий, не было ли изменений в политике.

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 12

2 / 2 балла (-ов)

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

Верно!

- (•) переполнение буфера
- ( ) подмена ОЗУ
- ( ) внедрение SQL-кода
- ( ) внедрение в ОЗУ

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 13

0 / 2 балла (-ов)

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

то правильный ответ

- ( ) прослушивание
- ( ) рассылка спама

Ваш ответ

- (•) подмена

фишинг

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)

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?

спам

вирус

Верно!

интернет-червь

фишинг

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 15

0 / 2 балла (-ов)

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

Ваш ответ

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

Ваш ответ

- [x] Внедрить эффективные межсетевые экраны.

Верно!

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

то правильный ответ

Повысить осведомленность сотрудников относительно действующих политик.

то правильный ответ

Не вводить пароли в окне чата.

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)

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

Верно!

- (•) открытый ключ Боба
- ( ) открытый ключ Алисы
- ( ) закрытый ключ Боба
- ( ) закрытый ключ Алисы

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)

Предположим, некие данные необходимо передать третьей стороне для проведения анализа. Какой метод может быть использован вне среды компании для защиты конфиденциальной информации в передаваемых данных путем ее замены?

- стегоанализ
- Верно! замена данных путем маскирования
- стеганография
- обфускация программного обеспечения

Refer to curriculum topic: 4.3.1
Существуют технологии, помогающие дезориентировать хакеров путем замены и сокрытия исходных данных.

Вопрос 18

0 / 2 балла (-ов)

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

- DES
- Ваш ответ RSA
- 3DES

то правильный ответ AES

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

Вопрос 19

2 / 2 балла (-ов)

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

Верно!

- (•) средства восстановления
- ( ) компенсационные средства контроля
- ( ) сдерживающие средства контроля
- ( ) средства обнаружения

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 20

2 / 2 балла (-ов)

Что происходит по мере увеличения длины ключа шифрования?

- ( ) Пространство ключей экспоненциально уменьшается.

Верно!

- (•) Пространство ключей экспоненциально увеличивается.

Пространство ключей пропорционально увеличивается.

Пространство ключей пропорционально уменьшается.

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)

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

Верно!

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

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 22

0 / 2 балла (-ов)

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

то правильный ответ

изменение младшего бита

обфускация данных

Ваш ответ

изменение старшего бита

маскирование данных

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

Вопрос 23

2 / 2 балла (-ов)

К какому типу средств контроля доступа относятся смарт-карты и системы биометрической идентификации?

технологические

Верно!

логические

административные

физические

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 24

2 / 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.)

Верно!

- [x] В одной системе применяется только хеширование, тогда как в другой системе, помимо хеширования, применяется механизм добавления соли.
- [ ] В обеих системах применяется алгоритм MD5.
- [ ] Обе системы шифруют пароли перед хешированием.
- [ ] В одной системе применяется симметричное хеширование, в другой — асимметричное.

Верно!

- [x] В системах применяются различные алгоритмы хеширования.

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

Вопрос 25

2 / 2 балла (-ов)

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

Верно!

- (•) сущностная целостность
- ( ) Определяемая пользователем целостность
- ( ) ссылочная целостность
- ( ) доменная 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 26

0 / 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
- Ваш ответ: мужчина, 25,25 $, ветеран
- да/нет 345-60-8745, TRF562
- то правильный ответ: женщина, 9866, 125,50 $

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)

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
- ( ) AES
- ( ) MD5
- ( ) SHA-1

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 28

2 / 2 балла (-ов)

В организации будет развернута сеть VPN, через которую пользователи смогут безопасно получать удаленный доступ к корпоративной сети. Назовите компонент, с помощью которого в IPsec производится аутентификация источника каждого пакета для проверки целостности данных.

- ( ) CRC
- ( ) добавление соли

Верно!

- (•) HMAC
- ( ) пароль

Refer to curriculum topic: 5.1.3
Алгоритм HMAC предназначен для аутентификации. Отправитель и получатель пользуются секретным ключом, который совместно с данными применяется для аутентификации источника сообщения и проверки подлинности данных.

Вопрос 29

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?

- цифровая подпись
- добавление соли
- асимметричное шифрование
- Верно! цифровой сертификат

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

Вопрос 30

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?

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

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

Вопрос 31

0 / 2 балла (-ов)

Какой алгоритм хеширования следует использовать для защиты конфиденциальной несекретной информации?

Ваш ответ

- (•) AES-256

то правильный ответ

- SHA-256
- MD5
- 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 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?

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 33

2 / 2 балла (-ов)

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

принятие риска

снижение риска

Верно!

передача риска

уклонение от 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)

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?

- Министерство образования США
- магазины в местном торговом центре
- Верно! Нью-Йоркская фондовая биржа
- 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 35

2 / 2 балла (-ов)

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

- предотвращение и изоляция
- устранение угроз и принятие
- конфиденциальность и ликвидация
- анализ рисков и высокая доступность
- Верно! обнаружение и анализ
- Верно! 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 36

2 / 2 балла (-ов)

Назовите подход к обеспечению доступности, при котором достигается наиболее полная защита благодаря слаженной работе нескольких механизмов безопасности, предотвращающих атаки?

Верно!

- (•) многоуровневый подход
- ( ) разнообразие
- ( ) ограничение
- ( ) сокрытие информации

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

Вопрос 37

2 / 2 балла (-ов)

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

- ( ) многоуровневый подход
- ( ) упрощение

Верно!

- (•) ограничение
- ( ) сокрытие информации

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 38

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?

то правильный ответ — количественный анализ

- анализ потерь
- Ваш ответ — качественный анализ
- анализ защищенности

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

Вопрос 39

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
- ( ) доступность ресурсов
- ( ) идентификация 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 40

0 / 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
- ( ) обеспечение удаленного доступа для тысяч внешних пользователей

Ваш ответ

- (•) повышение надежности шифрования

то правильный ответ

повышение надежности и эксплуатационной готовности серверов

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 41

2 / 2 балла (-ов)

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

- SSH
- ARP
- сильная аутентификация
- **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 42

2 / 2 балла (-ов)

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

- 802.11q
- TKIP

Верно! ☑ 802.11i

Верно! ☑ WPA

☐ WEP

Верно! ☑ WPA2

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

Вопрос 43

2 / 2 балла (-ов)

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

Верно! ◉ SSH

○ Telnet

○ WPA

○ SCP

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 44

2 / 2 балла (-ов)

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

- WEP
- Верно! WPA2
- WPA
- WEP2

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

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

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

Вопрос 46

2 / 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
- Верно! Оснастка «Локальная политика безопасности»
- Инструмент «Безопасность Active Directory»
- Управление компьютером

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 47

2 / 2 балла (-ов)

Назовите два протокола, которые могут представлять угрозу для коммутируемой среды. (Выберите два варианта.)

- ICMP
- Верно! ARP
- Верно! STP
- WPA2
- RIP

IP

Refer to curriculum topic: 7.3.1
Ядро современной сетевой инфраструктуры передачи данных составляют сетевые коммутаторы. Сетевые коммутаторы подвержены таким угрозам, как кража, взлом, удаленный доступ и атаки с использованием сетевых протоколов.

Вопрос 48

0 / 2 балла (-ов)

Какие два вида информации можно найти на веб-сайте Internet Storm Center? (Выберите два варианта.)

Архивные данные

Ваш ответ

Действующие законы

то правильный ответ

Вакансии InfoSec

Верно!

Отчеты InfoSec

Refer to curriculum topic: 8.2.3
Веб-сайт Internet Storm Center предоставляет различную информацию, в том числе ежедневный блог InfoSec, инструменты InfoSec и новости.

Вопрос 49

2 / 2 балла (-ов)

Почему для тестирования безопасности сети организации часто выбирают дистрибутив Kali Linux?

Это инструмент сканирования сети, который определяет приоритеты для угроз безопасности.

Он может использоваться для перехвата и регистрации сетевого трафика.

Он может использоваться для проверки слабых мест только с помощью вредоносного ПО.

Верно!

Это дистрибутив Linux с открытым исходным кодом, включающий в себя более 300 инструментов для защиты.

Refer to curriculum topic: 8.2.4
Kali — это дистрибутив Linux с открытым исходным кодом, используемый многими ИТ-специалистами для тестирования безопасности сетей.

Вопрос 50

2 / 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.)

Запрет на выход из здания в рабочее время

Верно!

Определение правил и процедур для гостей, посещающих здание

Верно!

Регулярное проведение обучения по вопросам безопасности

Замки на шкафах

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.

Оценка контрольной работы: **80** из 100