Финальный экзамен Результаты для Yevhen Bodnia

Оценка за эту попытку: **76** из 100
Отправлено 17 Май в 20:13
Эта попытка длилась 36 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?

- перехватывание пакетов
- Верно! подделка пакетов
- неавторизованная точка доступа Wi-Fi
- DNS-подмена

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

Вопрос 2

2 / 2 балла (-ов)

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

- хактивисты
- «черные» хакеры
- Верно! доверенные партнеры
- кибермастера
- непрофессионалы

Верно!

- [x] бывшие сотрудники

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 3

2 / 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!

- [x] служение обществу

Верно!

- [x] высокий доход

Верно!

- [x] высокий спрос на специалистов
- [ ] необходима докторская степень (PhD)
- [ ] сертификация CompTIA A+ обеспечивает достаточный уровень знаний для начала карьеры

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

Вопрос 4

0 / 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.

- NAS
- **Ваш ответ** VPN
- сеть хранения данных (SAN)
- **то правильный ответ** IAC

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 5

2 / 2 балла (-ов)

Что следует рекомендовать в качестве основы для создания комплексной системы управления информационной безопасностью в организации?

- Триада «КЦД»
- Модель ISO/OSI
- Архитектура NIST/NICE
- **Верно!** ISO/IEC 27000

Refer to curriculum topic: 2.5.1
Специалист по кибербезопасности должен быть знаком с различными стандартами, архитектурами и моделями управления информационной безопасностью.

Вопрос 6

2 / 2 балла (-ов)

Какая из технологий обеспечивает конфиденциальность данных?

- RAID
- шифрование

Верно!

- хэширование
- 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

0 / 2 балла (-ов)

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

то правильный ответ

- ранимые данные
- передаваемые данные
- обрабатываемые данные

Ваш ответ

- 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)

Какую технологию идентификации можно использовать в составе системы аутентификации сотрудников?

- тамбур-шлюз
- Хеширование SHA-1
- виртуальный отпечаток пальца
- считывание смарт-карт

Верно!

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

Вопрос 9

0 / 2 балла (-ов)

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

- программа-вымогатель
- атака через посредника
- фарминг

Ваш ответ

то правильный ответ оциальная инженерия

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 10

2 / 2 балла (-ов)

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

- атака через посредника
- рассылка спама
- прослушивание
- подмена

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 11

2 / 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?

Атака, при которой злоумышленник выдает себя за авторизованную сторону.

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

DDoS-атака.

Верно! Обман.

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

Вопрос 12

0 / 2 балла (-ов)

Какое из описаний точнее всего соответствует DDoS-атаке?

то правильный ответ Злоумышленник формирует ботнет из компьютеров-зомби.

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

Ваш ответ 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 13

2 / 2 балла (-ов)

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

- [ ] Внедрить эффективные межсетевые экраны.
- [x] Повысить осведомленность сотрудников относительно действующих политик. — Верно!
- [x] Не переходить по ссылкам, вызывающим любопытство. — Верно!
- [ ] Внедрить политику, согласно которой сотрудники ИТ-подразделения имеют право передавать информацию по телефону только руководителям.
- [x] Не вводить пароли в окне чата. — Верно!
- [ ] 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 14

2 / 2 балла (-ов)

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

Верно!

- прослушивание
- фишинг
- рассылка спама
- 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 15

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?

- доверенные партнеры

Ваш ответ

- срочность

- близкие отношения

то правильный ответ ринуждение

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

Вопрос 16

0 / 2 балла (-ов)

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

Ваш ответ

- RSA

то правильный ответ

- DES
- ECC
- 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 17

2 / 2 балла (-ов)

В какой ситуации требуются средства обнаружения?

- нет возможности привлечь сторожевую собаку, поэтому требуется альтернативный вариант
- нужно ликвидировать нанесенный организации ущерб

Верно!

- (•) в сети организации нужно выявить запрещенную активность
- ( ) 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 18

2 / 2 балла (-ов)

Какое из утверждений относится к блочным шифрам?

- ( ) Блочное шифрование сжимают шифруемую информацию.

Верно!

- (•) При блочном шифровании объем зашифрованных данных обычно больше объема исходных данных.
- ( ) Алгоритмы блочного шифрования быстрее алгоритмов поточного шифрования.
- ( ) 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 19

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
- закрытый ключ Алисы
- закрытый ключ Боба
- открытый ключ Боба

Верно!

Refer to curriculum topic: 4.1.3
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
- изменение младшего бита
- обфускация данных

Верно!

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

Вопрос 21

0 / 2 балла (-ов)

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

- распознавательные
- Ваш ответ: компенсирующие
- то правильный ответ: орректирующие
- превентивные

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

2 / 2 балла (-ов)

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

- Верно! средства восстановления
- сдерживающие средства контроля

- средства обнаружения
- компенсационные 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 23

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 24

0 / 2 балла (-ов)

Какая технология хеширования подразумевает обмен ключами?

- AES

добавление соли

то правильный ответ !MAC

Ваш ответ

MD5

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

Вопрос 25

2 / 2 балла (-ов)

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

Определяемая пользователем целостность

доменная целостность

Верно!

сущностная целостность

ссылочная 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)

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.)

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

то правильный ответ — системах применяются различные алгоритмы хеширования.

Ваш ответ

- [x] В обеих системах применяется алгоритм MD5.

Верно!

- [x] В одной системе применяется только хеширование, тогда как в другой системе, помимо хеширования, применяется механизм добавления соли.
- Обе системы шифруют пароли перед хешированием.

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

Вопрос 27

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».

- да/нет 345-60-8745, TRF562

Верно!

- (•) женщина, 9866, 125,50 $
- мужчина, 25,25 $, ветеран
- 800-900-4560, 4040-2020-8978-0090, 21.01.2013

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 28

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.)

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

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

Вопрос 29

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?

- SHA-1
- AES
- MD5
- SHA-256

Верно!

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 30

2 / 2 балла (-ов)

Назовите главную особенность криптографической хеш-функции.

Верно!

- Хеш-функция необратима.
- Выходные значения имеют различную длину.
- По выходному значению хеш-функции можно вычислить входное значение.
- Для хеширования необходимы открытый и закрытый ключи.

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)

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

- HMAC
- асимметричное шифрование
- цифровой сертификат
- цифровая подпись

Верно!

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

Вопрос 32

2 / 2 балла (-ов)

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

- анализ рисков и высокая доступность
- устранение угроз и принятие
- предотвращение и изоляция
- обнаружение и анализ

Верно!

- изоляция и восстановление

Верно!

- 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 33

2 / 2 балла (-ов)

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

- снижение риска
- передача риска

Верно!

- принятие 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

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?

- количественный анализ
- анализ потерь

Ваш ответ

- анализ степени уязвимости к угрозам

то правильный ответ

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 35

2 / 2 балла (-ов)

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

- упрощение
- сокрытие информации

Верно!

- 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 36

2 / 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 потерь
- качественный анализ
- анализ защищенности

Верно!

- 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 37

0 / 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.

то правильный ответ

- Национальная база данных общих уязвимостей и рисков (CVE)
- Infragard

Ваш ответ

- Модель ISO/IEC 27000
- Архитектура NIST/NICE

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 38

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
- ( ) доступность ресурсов
- ( ) стандартизация ресурсов
- ( ) идентификация ресурсов

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

Вопрос 39

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 40

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

обеспечение удаленного доступа для тысяч внешних пользователей

Верно!

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)

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

Верно!

- (•) количество ложноотрицательных результатов и количество ложноположительных результатов
- ( ) количество ложноположительных срабатываний и степень приемлемости
- ( ) степень приемлемости и количество ложноотрицательных срабатываний
- ( ) 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 42

2 / 2 балла (-ов)

Какая из утилит использует протокол ICMP?

- ( ) NTP
- ( ) RIP

Верно!

- (•) ping
- ( ) DNS

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

Вопрос 43

2 / 2 балла (-ов)

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

Верно! ☑ WPA

Верно! ☑ 802.11i

☐ WEP

☐ TKIP

Верно! ☑ WPA2

☐ 802.11q

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)

Какие атаки можно предотвратить с помощью взаимной аутентификации?

○ анализ беспроводного трафика

Верно! ◉ атака через посредника

○ подмена IP-адреса отправителя в беспроводных сетях

○ беспроводной спам

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

Верно!

- (•) WPA2
- ( ) WPA
- ( ) WEP2
- ( ) 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 46

0 / 2 балла (-ов)

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

то правильный ответ

абор сдерживает только случайных прохожих.

Забор сможет противостоять нарушителю, намеренно проникающему на территорию.

Забор ограждает территорию от случайных прохожих благодаря своей высоте.

Ваш ответ

Забор ненадолго задержит нарушителя, намеренно проникающего 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 47

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 48

2 / 2 балла (-ов)

Специалист по безопасности может иметь доступ к конфиденциальным данным и ресурсам. Что из следующего должен понимать специалист по безопасности для принятия обоснованных, этических решений (выбрать один пункт)?

- Возможный бонус
- Поставщики облачных услуг
- Законы, регулирующие обработку данных

Верно!

- Потенциальная выгода
- Партнерства

Refer to curriculum topic: 8.2.1
Этика чрезвычайно важна для специалистов по безопасности в связи с доступом к важным данным и ресурсам. Соответствие нормативным требованиям государственных органов необходимо для принятия разумных решений.

Вопрос 49

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.

Вопрос 50

2 / 2 балла (-ов)

В компании произошло несколько инцидентов, когда пользователи загружали несанкционированное ПО, использовали запрещенные веб-сайты и личные USB-накопители. ИТ-директор хочет внедрить схему управления угрозами, исходящими от пользователей. Какие три меры могли бы использоваться для управления угрозами? (Выберите три варианта.)

Верно!

- [x] Проведение обучения по вопросам безопасности
- [ ] Дисциплинарное взыскание

Верно!

- [x] Фильтрация содержимого
- [ ] Переход на тонкие клиенты
- [ ] Отслеживание всех действий пользователей

Верно!

- [x] Отключение доступа к CD и USB

Refer to curriculum topic: 8.1.1
Пользователи могут не знать о последствиях своих действий, если им не рассказать о возможных проблемах. Внедрение ряда технических и организационных практик может уменьшить угрозы.

Оценка контрольной работы: **76** из 100