

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=8462098)
(https://685059869.netacad.com/courses/832407/quizzes/7516579/take?user_id=8462098)

История попыток

	Попытка	Время	Оценка
ПОСЛЕДНЯЯ	Попытка 1 (https://685059869.netacad.com/courses/832407/quizzes/7516579/history?version=1)	42 минут(ы)	88 из 100

Оценка за эту попытку: **88** из 100

Отправлено 23 Май в 23:27

Эта попытка длилась 42 минут(ы).

Верно!

Вопрос 1

2 / 2 балла (-ов)

Какое из определений наиболее точно описывает хактивистов?

☐ Хотят похвастаться хакерским мастерством.

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

☐ Ищут новые эксплойты.

☐ Любознательны и осваивают хакерские методы.

Refer to curriculum topic: 1.2.1

Для каждой категории киберпреступников характерны определенные мотивы.

Вопрос 2

2 / 2 балла (-ов)

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

☐ хактивисты

Верно!

☒ бывшие сотрудники

Верно!

☒ доверенные партнеры

☐ непрофессионалы

☐ «черные» хакеры

☐ кибермастера

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)

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

☐ Необходим круглосуточный мониторинг.

☐ Требуется больше ресурсов для обработки данных.

Верно!



В системах, созданных на основе этих технологий, хранятся персональные данные.

☐ Требуется больше оборудования.

Верно!



С помощью этих технологий ведется сбор конфиденциальной информации.

☐ 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 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?

Верно!

☒ конфиденциальность, целостность, доступность

☐ секретность, идентификация, невозможность отказа

☐ технологии, политики, осведомленность

☐ шифрование, аутентификация, идентификация

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 методы, с помощью которых можно внедрить многофакторную аутентификацию.

☐ сети VPN и VLAN

Верно!

☒ пароли и отпечатки пальцев

☐ системы IDS и IPS

☐ токены и хеш-суммы

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)

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.

☐ сеть хранения данных (SAN)

☐ NAS

☐ VPN

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 7

2 / 2 балла (-ов)

Какая из технологий обеспечивает конфиденциальность данных?

Верно!

☒ шифрование

☐ RAID

☐ управление идентификационными данными

☐ хэширование

Refer to curriculum topic: 2.2.1

Специалист по обеспечению кибербезопасности должен быть хорошо знаком с технологиями, реализующими конфиденциальность, целостность и доступность данных.

Вопрос 8

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

☐ виртуальные сети

☐ проводные 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 9

2 / 2 балла (-ов)

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

☐ атака через посредника

Верно!

☒ программа-вымогатель

☐ троян

☐ DoS-атака

Refer to curriculum topic: 3.1.1

Специалист по обеспечению кибербезопасности должен быть знаком с особенностями разных видов вредоносного ПО и атак, которые угрожают организации.

Вопрос 10

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 11

2 / 2 балла (-ов)

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

Верно!

☒ прослушивание

☐ подмена

☐ рассылка спама

☐ 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 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

☐ срочность

то правильный ответ принуждение

Ваш ответ

☒ доверенные партнеры

Refer to curriculum topic: 3.2.1

Методы социальной инженерии включают несколько различных тактик для получения информации от жертв.

Вопрос 13

0 / 2 балла (-ов)

Киберпреступник отправляет ряд специально подготовленных некорректных пакетов на сервер базы данных. Сервер безуспешно пытается обработать пакеты, что приводит к его сбою. Какую атаку реализует киберпреступник?

то правильный ответ DoS-атака

☐ внедрение SQL-кода

☐ атака через посредника

Ваш ответ

☒ подмена пакетов

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 злоумышленник выдает себя за авторизованную сторону и пользуется уже существующими доверительными отношениями между двумя системами?

- ☐ рассылка спама
- ☐ атака через посредника
- ☒ подмена
- ☐ 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 15

2 / 2 балла (-ов)

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

- ☐ внедрение в ОЗУ
- ☒ переполнение буфера
- ☐ внедрение SQL-кода

Верно!

☐ подмена 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 16

2 / 2 балла (-ов)

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

Верно!

- ☒ Избирательный контроль доступа
- ☐ ACL
- ☐ Обязательное разграничение доступа
- ☐ 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 17

2 / 2 балла (-ов)

Как называется механизм безопасности, к которому относятся пароли, парольные фразы и PIN-коды?

Верно!

- ☒ аутентификация

☐ идентификация

☐ доступ

☐ авторизация

Refer to curriculum topic: 4.2.4

Для усиления систем контроля доступа применяются различные методы аутентификации. Нужно понимать особенности каждого из этих методов.

Вопрос 18

2 / 2 балла (-ов)

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

☐ 3DES

Верно!

☒ AES

☐ DES

☐ RSA

Refer to curriculum topic: 4.1.4

Шифрование — важная технология, предназначенная для защиты конфиденциальности данных. Важно понимать особенности различных методов шифрования.

Вопрос 19

0 / 2 балла (-ов)

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

Ваш ответ

☒ технологические

то правильный ответ

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 20

2 / 2 балла (-ов)

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

☐ изменение старшего бита

Верно!

☒ изменение младшего бита

☐ обфускация данных

☐ маскирование 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)

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

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

Верно!

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

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?

- ☒ замена данных путем маскирования
- ☐ обфускация программного обеспечения
- ☐ стеганография
- ☐ стегоанализ

Верно!

Refer to curriculum topic: 4.3.1

Существуют технологии, помогающие дезориентировать хакеров путем замены и сокрытия исходных данных.

Вопрос 23

2 / 2 балла (-ов)

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

- ☐ превентивные
- ☒ корректирующие
- ☐ компенсирующие
- ☐ распознавательные

Верно!

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 24

0 / 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

то правильный ответ

цифровая подпись

☐ цифровой сертификат

Ваш ответ

☒ HMAC

Refer to curriculum topic: 5.2.1

Цифровая подпись позволяет гарантировать подлинность, целостность и невозможность отказа от авторства.

Вопрос 25

2 / 2 балла (-ов)

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

Верно!

☒ закрытый ключ Алисы

☐ открытый ключ Боба

☐ закрытый ключ Боба

☐ имя пользователя и пароль Алисы

Refer to curriculum topic: 5.2.2

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

Вопрос 26

2 / 2 балла (-ов)

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

☐ Определяемая пользователем целостность

☐ ссылочная целостность

Верно!

☒ сущностная 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 27

2 / 2 балла (-ов)

К какой технологии обеспечения безопасности относится стандарт X.509?

☐ технология биометрической идентификации

Верно!

☒ цифровые сертификаты

☐ токены безопасности

☐ надежные пароли

Refer to curriculum topic: 5.3.2

С помощью цифровых сертификатов обеспечивается безопасность сторон защищенного соединения.

Вопрос 28

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?

☐ MD5

☐ AES

☒ SHA-256

☐ SHA-1

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 29

0 / 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?

☐ правила проверки данных

☒ операции хеширования

Ваш ответ

то правильный ответ

цифровые сертификаты

☐ сети VPN и сервисы шифрования

Refer to curriculum topic: 5.3.2

Цифровые сертификаты предназначены для защиты участников защищенного информационного обмена.

Вопрос 30

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?

Верно!

- ☒ цифровые сертификаты
- ☐ хеширование данных
- ☐ симметричное шифрование
- ☐ асимметричное шифрование

Refer to curriculum topic: 5.3.1

Цифровые сертификаты предназначены для защиты участников защищенного информационного обмена.

Вопрос 31

2 / 2 балла (-ов)

Назовите технологию, с помощью которой можно предотвратить атаку, реализуемую методом перебора по словарю или методом грубой силы с использованием хеш-суммы?

- ☐ радужные таблицы

Верно!

- ☒ HMAC

☐ MD5

☐ AES

Refer to curriculum topic: 5.1.3

В HMAC используется дополнительный секретный ключ, который принимает хэш-функция. Таким образом, помимо хеширования, присутствует дополнительный уровень безопасности, что позволяет нейтрализовать атаку через посредника (MitM) и обеспечить аутентификацию источника данных.

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?

Ваш ответ

☒ анализ потерь

то правильный ответ

количественный анализ

☐ 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 33**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?

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

Верно!

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 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?

- ☐ стандартизация ресурсов
- ☐ идентификация ресурсов
- ☐ доступность ресурсов
- ☒ классификация ресурсов

Верно!

Refer to curriculum topic: 6.2.1

Одна из важнейших составляющих управления рисками — классификация ресурсов.

Вопрос 35

2 / 2 балла (-ов)

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

Верно!

- ☒ превентивные
- ☐ распознавательные
- ☐ административные
- ☐ корректирующие

Refer to curriculum topic: 6.4.1

План аварийного восстановления помогает подготовить организацию к потенциальным аварийным ситуациям и минимизировать время простоя.

Вопрос 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
- ☐ сокрытие информации
- ☐ разнообразие

☐ ограничение

Refer to curriculum topic: 6.2.2

Многоуровневая защита подразумевает несколько уровней безопасности.

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?

☐ доступность ресурсов

☐ идентификация ресурсов

Верно!

☒ стандартизация 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)

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

☐ Infragard

☐ Модель ISO/IEC 27000

Верно!

☒ Национальная база данных общих уязвимостей и рисков (CVE)

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 39

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

Верно!

☒ Нью-Йоркская фондовая биржа

☐ офис спортивной команды высшей лиги

☐ магазины в местном торговом центре

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 40

2 / 2 балла (-ов)

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

- ☐ сокрытие информации
- ☐ многоуровневый подход
- ☒ ограничение
- ☐ упрощение

Верно!

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 41

2 / 2 балла (-ов)

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

- ☐ RIP
- ☐ ICMP

☐ IP

☐ WPA2

Верно!

☒ ARP

Верно!

☒ STP

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 42

2 / 2 балла (-ов)

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

☐ сильная аутентификация

☐ SSH

Верно!

☒ шифрование голосового трафика

☐ ARP

Refer to curriculum topic: 7.3.2

Многие передовые технологии, включая VoIP, передачу потокового видео и конференц-связь, требуют соответствующих мер безопасности.

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)

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 неприемлемости и количество ложноотрицательных срабатываний



степень приемлемости 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 45

2 / 2 балла (-ов)

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

Верно!

☒ SSH

☐ WPA

☐ SCP

☐ 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 46

2 / 2 балла (-ов)

Какая из утилит использует протокол ICMP?

☐ DNS

☐ NTP

Верно!

☒ ping

☐ RIP

Refer to curriculum topic: 7.3.1

С помощью протокола ICMP сетевые устройства передают сообщения об ошибках.

Вопрос 47

2 / 2 балла (-ов)

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

Верно!

☒ Microsoft Security Baseline Analyzer

☐ MS Baseliner

☐ SANS Baselining System (SBS)

☐ CVE Baseline Analyzer

Refer to curriculum topic: 7.1.1

Существует множество инструментов, с помощью которых специалист по кибербезопасности оценивает потенциальные уязвимости организации.

Вопрос 48

2 / 2 балла (-ов)

Для сбора рекомендаций по защите устройств от угроз компания наняла консультанта. Какие три общие рекомендации можно выявить?

(Выберите три варианта.)

Верно!

☒ Включение блокировки экрана

☐ Отмена фильтрации содержимого

Верно!

☒ Отмена административных прав для пользователей

Верно!

☒ Включение автоматического антивирусного сканирования

☐ Соблюдение строгой кадровой политики

☐ Разрешение съемных носителей информации

Refer to curriculum topic: 8.1.2

Защитить рабочие станции можно путем отмены прав, в которых нет необходимости, автоматизации процессов и включения функций безопасности.

Вопрос 49

2 / 2 балла (-ов)

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

Верно!

☒ Отключение ping-запросов, зондирования и сканирования портов

☐ Предоставление административных прав

Верно!

☒ Установка на устройства последних исправлений и обновлений для системы безопасности

Верно!

☒ Проверка входящего и исходящего трафика

☐ Наем консультанта

☐ Отключение межсетевых экранов

Refer to curriculum topic: 8.1.4

Организации могут управлять угрозами для частного облака следующими способами:

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

Вопрос 50

2 / 2 балла (-ов)

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)?

- ☐ Партнерства
- ☐ Потенциальная выгода
- ☐ Поставщики облачных услуг
- ☐ Возможный бонус
- ☒ Законы, регулирующие обработку данных

Верно!

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.

Оценка контрольной работы: **88** из 100