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
ПОСЛЕДНЯЯ	Попытка 2 (https://685059869.netacad.com/courses/832407/quizzes/7516579/history?version=2)	60 минут(ы)	0 из 100
	Попытка 1 (https://685059869.netacad.com/courses/832407/quizzes/7516579/history?version=1)	60 минут(ы)	4,67 из 100

Оценка за эту попытку: **0** из 100
Отправлено 22 Май в 1:49
Эта попытка длилась 60 минут(ы).

Нет ответа

Вопрос 1

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?

- «серые» хакеры
- хакеры-дилетанты
- «черные» хакеры

то правильный ответ «белые» хакеры

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

Нет ответа

Вопрос 2

0 / 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.)

то правильный ответ служение обществу

то правильный ответ высокий доход

- необходима докторская степень (PhD)
- должность, подразумевающая рутинную повседневную работу

то правильный ответ высокий спрос на специалистов

- 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.

Нет ответа

Вопрос 3

0 / 2 балла (-ов)

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

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

то правильный ответ Проект Honeynet

Refer to curriculum topic: 1.2.2
Системы раннего оповещения **помогают** распознать атаки и могут быть эффективным защитным инструментом в руках специалистов по кибербезопасности.

Нет ответа

Вопрос 4

0 / 2 балла (-ов)

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

- Модель ISO/OSI
- Триада «КЦД»

то правильный ответ ISO/IEC 27000

- Архитектура NIST/NICE

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

Нет ответа

Вопрос 5

0 / 2 балла (-ов)

Два дня в неделю сотрудники организации имеют право работать удаленно, находясь дома. Необходимо обеспечить конфиденциальность передаваемых данных. Какую технологию следует применить в данном случае?

то правильный ответ

- VPN
- сети VLAN
- SHS
- RAID

Refer to curriculum topic: 2.4.1
Для защиты конфиденциальности данных необходимо понимать, какие технологии используются для защиты данных во всех их трех состояниях.

Нет ответа

Вопрос 6

0 / 2 балла (-ов)

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

то правильный ответ

- хранимые данные
- расшифрованные данные
- удаленные данные
- зашифрованные данные

то правильный ответ

- обрабатываемые данные

то правильный ответ

- передаваемые 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.

Нет ответа

Вопрос 7

0 / 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?

- технологии, политики, осведомленность
- шифрование, аутентификация, идентификация

то правильный ответ

- конфиденциальность, целостность, доступность
- секретность, идентификация, невозможность отказа

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

Нет ответа

Вопрос 8

0 / 2 балла (-ов)

Назовите методы, с помощью которых можно внедрить многофакторную аутентификацию.

- системы IDS и IPS

то правильный ответ

- пароли и отпечатки пальцев

сети VPN и VLAN

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».

Нет ответа

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?

рассылка спама

атака через посредника

прослушивание

то правильный ответ

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.

Нет ответа

Вопрос 10

0 / 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
- троян

то правильный ответ

- программа-вымогатель
- 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.

Нет ответа

Вопрос 11

0 / 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

то правильный ответ

- 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.

Нет ответа

Вопрос 12

0 / 2 балла (-ов)

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

- внедрение в ОЗУ
- подмена ОЗУ
- внедрение SQL-кода

то правильный ответ переполнение буфера

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.

Нет ответа

Вопрос 13

0 / 2 балла (-ов)

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

то правильный ответ Повысить осведомленность сотрудников относительно действующих политик.

то правильный ответ Не переходить по ссылкам, вызывающим любопытство.

то правильный ответ Не вводить пароли в окне чата.

- Внедрить эффективные межсетевые экраны.
- Внедрить политику, согласно которой сотрудники ИТ-подразделения имеют право передавать информацию по телефону только руководителям.

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.

Нет ответа

Вопрос 14

0 / 2 балла (-ов)

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

то правильный ответ

- социальная инженерия
- атака через посредника
- фарминг
- программа-вымогатель

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.

Нет ответа

Вопрос 15

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.

Проверить, нет ли учетных записей без паролей.

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

то правильный ответ Проверить системы на наличие неавторизованных учетных записей.

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.

Нет ответа

Вопрос 16

0 / 2 балла (-ов)

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

физические

административные

то правильный ответ логические

технологические

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.

Нет ответа

Вопрос 17

0 / 2 балла (-ов)

Что происходит по мере увеличения длины ключа шифрования?

то правильный ответ

- Пространство ключей экспоненциально увеличивается.
- Пространство ключей пропорционально увеличивается.
- Пространство ключей экспоненциально уменьшается.
- 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.

Нет ответа

Вопрос 18

0 / 2 балла (-ов)

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

- открытый ключ Боба

то правильный ответ

- новый общий PSK-ключ
- закрытый ключ Кэрол
- общий PSK-ключ, которым шифруются сообщения, адресованные Алисе

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

Нет ответа

Вопрос 19

0 / 2 балла (-ов)

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

то правильный ответ

- аутентификация
- авторизация
- доступ
- идентификация

Refer to curriculum topic: 4.2.4
Для усиления систем контроля доступа применяются различные методы аутентификации. Нужно понимать особенности каждого из этих методов.

Нет ответа

Вопрос 20

0 / 2 балла (-ов)

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

- превентивные
- компенсирующие
- 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.

Нет ответа

Вопрос 21

0 / 2 балла (-ов)

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

- закрытый ключ Алисы
- открытый ключ Алисы

то правильный ответ

- открытый ключ Боба
- закрытый ключ Боба

Refer to curriculum topic: 4.1.3
Шифрование — важная технология, предназначенная для защиты конфиденциальности данных. Важно понимать особенности различных методов шифрования.

Нет ответа

Вопрос 22

0 / 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?

- стеганография

стегоанализ

обфускация программного обеспечения

то правильный ответ замена данных путем маскирования

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

Нет ответа

Вопрос 23

0 / 2 балла (-ов)

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

средства обнаружения

то правильный ответ средства восстановления

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.

Нет ответа

Вопрос 24

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

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

Нет ответа

Вопрос 25

0 / 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?

- [x] то правильный ответ SHA-256
- [ ] MD5
- [ ] SHA-1
- [ ] AES

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.

Нет ответа

Вопрос 26

0 / 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.)

- таблицы алгоритмов
- то правильный ответ таблицы поиска
- хеш-суммы паролей
- то правильный ответ реверсивные таблицы поиска
- неавторизованные точки доступа
- то правильный ответ радужные таблицы

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

Нет ответа

Вопрос 27

0 / 2 балла (-ов)

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

доменная целостность

ссылочная целостность

то правильный ответ сущностная целостность

Определяемая пользователем целостность

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

Нет ответа

Вопрос 28

0 / 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?

то правильный ответ цифровые сертификаты

асимметричное шифрование

симметричное шифрование

хеширование данных

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

Нет ответа

Вопрос 29

0 / 2 балла (-ов)

Какая технология хеширования подразумевает обмен ключами?

- MD5
- AES
- добавление соли

то правильный ответ HMAC

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

Нет ответа

Вопрос 30

0 / 2 балла (-ов)

К какой технологии обеспечения безопасности относится стандарт X.509?

- надежные пароли
- технология биометрической идентификации

то правильный ответ цифровые сертификаты

- токены безопасности

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

Нет ответа

Вопрос 31

0 / 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.

- пароль
- CRC
- добавление соли

то правильный ответ HMAC

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.

Нет ответа

Вопрос 32

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.

- Модель ISO/IEC 27000
- Infragard

то правильный ответ Национальная база данных общих уязвимостей и рисков (CVE)

- 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.

Нет ответа

Вопрос 33

0 / 2 балла (-ов)

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

- разнообразие
- то правильный ответ многоуровневый подход
- ограничение
- сокрытие информации

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

Нет ответа

Вопрос 34

0 / 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?

- идентификация ресурсов
- то правильный ответ классификация ресурсов

доступность ресурсов

стандартизация ресурсов

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

Нет ответа

Вопрос 35

0 / 2 балла (-ов)

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

коэффициент частоты

мера уязвимости ресурса к угрозе

то правильный ответ

количество реализаций угрозы в год

количественная величина убытков

то правильный ответ

ожидаемый ущерб в результате реализации единичной угрозы

ценность ресурса

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.

Нет ответа

Вопрос 36

0 / 2 балла (-ов)

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

то правильный ответ изоляция и восстановление

устранение угроз и принятие

конфиденциальность и ликвидация

предотвращение и изоляция

то правильный ответ обнаружение и анализ

анализ рисков и высокая доступность

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.

Нет ответа

Вопрос 37

0 / 2 балла (-ов)

В организации устанавливают только те приложения, которые соответствуют внутренним нормам. Все остальные приложения удаляются администраторами в целях усиления безопасности. Как называется этот метод?

идентификация ресурсов

доступность ресурсов

то правильный ответ 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.

Нет ответа

Вопрос 38

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?

то правильный ответ

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

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.

Нет ответа

Вопрос 39

0 / 2 балла (-ов)

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

- отказоустойчивость
- бесперебойное обслуживание

то правильный ответ

- отказоустойчивость системы
- единая точка отказа

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

Нет ответа

Вопрос 40

0 / 2 балла (-ов)

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

то правильный ответ

- ограничение
- многоуровневый подход
- упрощение
- 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.

Нет ответа

Вопрос 41

0 / 2 балла (-ов)

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

- [ ] IP
- [ ] WPA2
- [ ] ICMP
- [ ] RIP

то правильный ответ

- [ ] STP

то правильный ответ

- [ ] ARP

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.

Нет ответа

Вопрос 42

0 / 2 балла (-ов)

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

CVE Baseline Analyzer

MS Baseliner

SANS Baselining System (SBS)

то правильный ответ Microsoft Security Baseline Analyzer

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

Нет ответа

Вопрос 43

0 / 2 балла (-ов)

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

SSH

ARP

то правильный ответ шифрование голосового трафика

сильная аутентификация

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

Нет ответа

Вопрос 44

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?

- Инструмент «Безопасность Active Directory»
- Журнал безопасности в средстве просмотра событий
- Управление компьютером

то правильный ответ Оснастка «Локальная политика безопасности»

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

Нет ответа

Вопрос 45

0 / 2 балла (-ов)

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

то правильный ответ 802.11i

то правильный ответ WPA2

- 802.11q
- WEP
- TKIP

то правильный ответ WPA

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

Нет ответа

Вопрос 46

0 / 2 балла (-ов)

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

- WEP2
- WEP
- WPA

то правильный ответ WPA2

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.

Нет ответа

Вопрос 47

0 / 2 балла (-ов)

Какая из утилит использует протокол ICMP?

- DNS

то правильный ответ ping

- RIP

NTP

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

Нет ответа

Вопрос 48

0 / 2 балла (-ов)

В рамках кадровой политики компании физическое лицо может отказаться предоставлять информацию любой третьей стороне, кроме работодателя. Какой закон защищает конфиденциальность предоставленной личной информации?

Стандарт безопасности данных индустрии платежных карт (PCI)

Закон о правах семьи на образование и неприкосновенность частной жизни (FERPA)

то правильный ответ

Закон Грэмма — Лича — Блайли (GLBA)

Закон Сарбейнса — Оксли (SOX)

Refer to curriculum topic: 8.2.2
Закон Грэмма — Лича — Блайли (GLBA) включает положения о конфиденциальности для отдельных лиц и способы ограничения предоставления информации сторонним организациям.

Нет ответа

Вопрос 49

0 / 2 балла (-ов)

Если лицо сознательно получает доступ к компьютеру, который связан с правительством, без разрешения, какие федеральные законы на него распространяются?

Закон Сарбейнса — Оксли (SOX)

то правильный ответ Закон о компьютерном мошенничестве (CFAA)

Закон Грэмма — Лича — Блайли (GLBA)

Закон о тайне обмена электронной информацией (ECPA)

Refer to curriculum topic: 8.2.2
Закон о компьютерном мошенничестве (CFAA) лежит в основе законодательства США, рассматривающего несанкционированный доступ к компьютерным системам как уголовное преступление.

Нет ответа

Вопрос 50

0 / 2 балла (-ов)

Какие три исключения из правил по обязательному предоставлению информации предусмотрены Законом о свободе информации (FOIA)? (Выберите три варианта.)

Общедоступная информация финансовых учреждений

то правильный ответ Конфиденциальная коммерческая информация

то правильный ответ Информация, касающаяся национальной безопасности и внешней политики

Информация, не защищенная специальными законами

то правильный ответ Документация правоохранительных органов, попадающая под перечисленные исключения

Негеологическая информация о скважинах

Refer to curriculum topic: 8.2.2
Закон о свободе информации (FOIA) предусматривает следующие исключения:

1. Информация, касающаяся национальной безопасности и внешней политики
2. Внутренние правила и практики для сотрудников государственных органов
3. Информация, защищенная специальными законами
4. Конфиденциальная коммерческая информация
5. Сведения, передаваемые внутри органов или между ними и попадающие под адвокатскую тайну (в связи с совещательными процессами, судебными разбирательствами и т. д.)
6. Информация, которая в случае раскрытия может расцениваться как явное незаконное вторжение в личную жизнь
7. Документация правоохранительных органов, попадающая под перечисленные исключения
8. Данные государственных органов, полученные от финансовых учреждений
9. Геологическая и геофизическая информация о скважинах

Оценка контрольной работы: **0** из 100