

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=2479295)

История попыток

	Попытка	Время	Оценка
ПОСЛЕДНЯЯ	Попытка 1 (https://685059869.netacad.com/courses/832407/quizzes/7516579/history?version=1)	18 минут(ы)	66 из 100

Оценка за эту попытку: **66** из 100

Отправлено 3 Май в 14:34

Эта попытка длилась 18 минут(ы).

Нет ответа

Вопрос 1

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.)

☐ должность, подразумевающая рутинную повседневную работу

то правильный ответ

служению обществу

то правильный ответ

высокий доход

☐

сертификация CompTIA A+ обеспечивает достаточный уровень знаний для начала карьеры

☐

необходима докторская степень (PhD)

то правильный ответ

высокий спрос на специалистов

Refer to curriculum topic: 1.2.2

Высокий спрос на специалистов по кибербезопасности открывает уникальные карьерные возможности.

Вопрос 2

0 / 2 балла (-ов)

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

☐ Infragard

то правильный ответ

Проект Honeynet

☐ База данных общих уязвимостей и рисков (CVE)

Ваш ответ

☒ Программа ISO/IEC 27000

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 3

0 / 2 балла (-ов)

Какое из определений наиболее точно описывает хактивистов?

☐ Хотят похвастаться хакерским мастерством.

то правильный ответ

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

Ваш ответ

☒ Любознательны и осваивают хакерские методы.

☐ Ищут новые эксплойты.

Refer to curriculum topic: 1.2.1

Для каждой категории киберпреступников характерны определенные мотивы.

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

☐ сеть хранения данных (SAN)

Ваш ответ

☒ VPN

то правильный ответ

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.

Нет ответа

Вопрос 5

0 / 2 балла (-ов)

Какую технологию идентификации можно использовать в составе системы аутентификации сотрудников?

то правильный ответ

считывание смарт-карт

☐ виртуальный отпечаток пальца

☐ тамбур-шлюз

☐ Хеширование SHA-1

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)

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

☐ Модель ISO/OSI

☐ Триада «КЦД»

☐ 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 7

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?

Верно!

☒ беспроводные сети

☐ сети переноса данных вручную

☐ проводные сети

☐ виртуальные сети

Refer to curriculum topic: 2.3.2

Специалист по обеспечению кибербезопасности должен быть осведомлен о видах технологий, которые используются для хранения, передачи и обработки данных.

Вопрос 8

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?

☐ шифрование, аутентификация, идентификация

Верно!

- ☒ конфиденциальность, целостность, доступность
- ☐ секретность, идентификация, невозможность отказа
- ☐ технологии, политики, осведомленность

Refer to curriculum topic: 2.1.1

Конфиденциальность, целостность и доступность берутся за основу при разработке всех систем управления.

Нет ответа

Вопрос 9

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.

☐ Увеличить число охранников.

то правильный ответ

Не вводить пароли в окне чата.

☐ Внедрить эффективные межсетевые экраны.

то правильный ответ

Не переходить по ссылкам, вызывающим любопытство.

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

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 10

2 / 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?

- ☐ подмена пакетов
- ☐ атака через посредника
- ☒ DoS-атака
- ☐ внедрение SQL-кода

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)

Какое из описаний точнее всего соответствует DDoS-атаке?

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



Злоумышленник посылает огромные объемы данных, которые сервер не в состоянии обработать.

Верно!



Злоумышленник формирует ботнет из компьютеров-зомби.



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

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

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.



DoS-атака

Верно!



программа-вымогатель



атака через посредника



троян

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 13

2 / 2 балла (-ов)

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

Верно!



Своевременное обновление операционной системы и остального программного обеспечения.

Верно!



Установка и своевременное обновление антивирусного ПО.



Внедрение сети VPN.



Применение надежных паролей.



Внедрение межсетевых экранов.



Применение RAID.

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 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
- ☐ прослушивание
- ☐ атака через посредника
- ☒ 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 15

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?

- ☐ фишинг
- ☒ интернет-червь
- ☐ спам
- ☐ вирус

Верно!

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 16

0 / 2 балла (-ов)

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

Ваш ответ

☒ авторизация

☐ доступ

☐ идентификация

то правильный ответ

аутентификация

Refer to curriculum topic: 4.2.4

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

Вопрос 17

0 / 2 балла (-ов)

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

☐ административные

то правильный ответ

логические

Ваш ответ

☒ физические

☐ 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.

Вопрос 18

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

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 19

0 / 2 балла (-ов)

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

Ваш ответ

☒ открытый ключ Боба

☐ закрытый ключ Кэрол

☐ общий PSK-ключ, которым шифруются сообщения, адресованные Алисе

то правильный ответ

новый общий PSK-ключ

Refer to curriculum topic: 4.1.2

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

Вопрос 20

2 / 2 балла (-ов)

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

☐ превентивные

☐ компенсирующие

☐ распознавательные

Верно!

☒ корректирующие

Refer to curriculum topic: 4.2.7

Контроль доступа препятствует получению доступа неавторизованным пользователем к конфиденциальным данным и сетевым системам. Существует несколько технологий, с помощью которых реализуются эффективные стратегии контроля доступа.

Вопрос 21

2 / 2 балла (-ов)

В какой ситуации требуются средства обнаружения?

Верно!

- ☒ в сети организации нужно выявить запрещенную активность
- ☐ нужно ликвидировать нанесенный организации ущерб
- ☐ необходимо восстановить нормальное состояние систем после проникновения в сеть организации
- ☐ нет возможности привлечь сторожевую собаку, поэтому требуется альтернативный вариант

Refer to curriculum topic: 4.2.7

Контроль доступа препятствует получению доступа неавторизованным пользователем к конфиденциальным данным и сетевым системам. Существует несколько технологий, с помощью которых реализуются эффективные стратегии контроля доступа.

Вопрос 22

0 / 2 балла (-ов)

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

Ваш ответ

☒ DES

то правильный ответ

AES

- ☐ RSA
- ☐ 3DES

Refer to curriculum topic: 4.1.4

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

Вопрос 23

2 / 2 балла (-ов)

Назовите компонент, представляющий наибольшую сложность при разработке криптосистемы.

- ☐ алгоритм шифрования
- ☐ длина ключа
- ☐ обратная разработка
- ☒ управление ключами

Верно!

Refer to curriculum topic: 4.1.1

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

Вопрос 24

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
- ☒ цифровая подпись
- ☐ цифровой сертификат

Верно!

☐ асимметричное шифрование

Refer to curriculum topic: 5.2.1

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

Вопрос 25

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.)

то правильный ответ

В системах применяются различные алгоритмы хеширования.

☐ Обе системы шифруют пароли перед хешированием.

Верно!



В одной системе применяется только хеширование, тогда как в другой системе, помимо хеширования, применяется механизм добавления соли.

Ваш ответ



В обеих системах применяется алгоритм MD5.



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

Refer to curriculum topic: 5.1.2

Хеширование позволяет обеспечить целостность данных в различных ситуациях.

Вопрос 26

2 / 2 балла (-ов)

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

☐ сети VPN и сервисы шифрования

☐ операции хеширования

☐ правила проверки данных

Верно!

☒ цифровые сертификаты

Refer to curriculum topic: 5.3.2

Цифровые сертификаты предназначены для защиты участников защищенного информационного обмена.

Вопрос 27

0 / 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

Ваш ответ

☒ MD5

☐ AES

то правильный ответ HMAC

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 28

2 / 2 балла (-ов)

К какой технологии обеспечения безопасности относится стандарт X.509?

- ☐ токены безопасности
- ☒ цифровые сертификаты
- ☐ технология биометрической идентификации
- ☐ надежные пароли

Верно!

Refer to curriculum topic: 5.3.2

С помощью цифровых сертификатов обеспечивается безопасность сторон защищенного соединения.

Вопрос 29

2 / 2 балла (-ов)

Назовите метод, с помощью которого можно сгенерировать разные хеш-суммы для одинаковых паролей.

- ☐ HMAC
- ☐ CRC
- ☐ SHA-256

Верно!

- ☒ добавление соли

Refer to curriculum topic: 5.1.2

Целостность данных является одним из трех руководящих принципов обеспечения информационной безопасности.

Специалист по кибербезопасности должен быть знаком со средствами и технологиями обеспечения целостности данных.

Вопрос 30

2 / 2 балла (-ов)

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
- ☐ мужчина, 25,25 \$, ветеран
- ☒ женщина, 9866, 125,50 \$
- ☐ 800-900-4560, 4040-2020-8978-0090, 21.01.2013

Верно!

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 31

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?

☐ асимметричное шифрование

☐ цифровая подпись

Верно!

☒ цифровой сертификат

☐ добавление соли

Refer to curriculum topic: 5.2.2

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

Вопрос 32

2 / 2 балла (-ов)

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

☐ единая точка отказа

☐ бесперебойное обслуживание

Верно!

☒ отказоустойчивость системы

☐ отказоустойчивость

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 33

0 / 2 балла (-ов)

Группа специалистов проводит анализ рисков применительно к сервисам БД. Помимо прочего, специалисты собирают следующую информацию: первоначальная ценность ресурсов; существующие угрозы для этих ресурсов; ущерб, который могут нанести эти угрозы. На основании собранной информации специалисты рассчитывают ожидаемый годовой объем убытков. Какой вид анализа рисков выполняет группа?

☐ анализ защищенности

☐ анализ потерь

☐ качественный анализ

то правильный ответ

количественный анализ

Refer to curriculum topic: 6.2.1

Качественный или количественный анализ рисков используется для определения угроз организации и распределения их по приоритетам.

Вопрос 34

0 / 2 балла (-ов)

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

то правильный ответ

ограничение

☐ упрощение

☐ сокрытие информации

Ваш ответ

☒ 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 35

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?

Ваш ответ

☒ идентификация ресурсов

то правильный ответ

стандартизация ресурсов

☐ доступность ресурсов

☐ классификация ресурсов

Refer to curriculum topic: 6.2.1

Организации необходимо знать, какое аппаратное обеспечение и какие программы имеются в наличии, чтобы знать, какими должны быть параметры конфигурации. Управление ресурсами охватывает все имеющееся аппаратное и программное обеспечение. В стандартах ресурсов определены все отдельные продукты аппаратного и программного обеспечения, которые использует и поддерживает организация. В случае сбоя оперативные действия помогут сохранить доступность и безопасность.

Вопрос 36

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?

- ☐ ограничение доступа к данным в этих системах
- ☐ обеспечение удаленного доступа для тысяч внешних пользователей
- ☐ 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 37

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?

Ваш ответ

- ☒ анализ степени уязвимости к угрозам

то правильный ответ

качественный анализ

- ☐ анализ потерь
- ☐ количественный анализ

Refer to curriculum topic: 6.2.1

Качественный или количественный анализ рисков используется для определения угроз организации и распределения их по приоритетам.

Вопрос 38

2 / 2 балла (-ов)

Какую технологию следует внедрить, чтобы обеспечить высокую доступность систем хранения данных?

Верно!

- ☒ RAID
- ☐ горячий резерв
- ☐ N+1
- ☐ обновление ПО

Refer to curriculum topic: 6.2.3

Обеспечение доступности систем и данных составляет особо важную обязанность специалиста по кибербезопасности. Необходимо иметь ясное представление о технологиях, процессах и средствах контроля, обеспечивающих резервирование.

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?

- ☐ магазины в местном торговом центре

Верно!

- ☒ Нью-Йоркская фондовая биржа
- ☐ офис спортивной команды высшей лиги
- ☐ Министерство образования США

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 достигается наиболее полная защита благодаря слаженной работе нескольких механизмов безопасности, предотвращающих атаки?

- ☐ ограничение
- ☐ разнообразие

Верно!

- ☒ многоуровневый подход
- ☐ сокрытие информации

Refer to curriculum topic: 6.2.2

Многоуровневая защита подразумевает несколько уровней безопасности.

Вопрос 41

2 / 2 балла (-ов)

Какую технологию можно использовать для защиты от несанкционированного прослушивания голосового трафика,

передаваемого с помощью VoIP-соединений?

Верно!

- ☒ шифрование голосового трафика
- ☐ ARP
- ☐ сильная аутентификация
- ☐ SSH

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)

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 43

2 / 2 балла (-ов)

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

Верно!

☒ ARP

☐ IP

☐ WPA2

☐ RIP

Верно!

☒ STP

☐ ICMP

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 44

2 / 2 балла (-ов)

Какие атаки можно предотвратить с помощью взаимной аутентификации?

☐ беспроводной спам

☐ анализ беспроводного трафика

☐ подмена IP-адреса отправителя в беспроводных сетях

Верно!

☒ атака через посредника

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.

☐ WPA

☒ WPA2

☐ WEP2

☐ WEP

Верно!

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

2 / 2 балла (-ов)

Какая из утилит использует протокол ICMP?

☐ DNS

☒ ping

☐ NTP

Верно!

☐ RIP

Refer to curriculum topic: 7.3.1

С помощью протокола ICMP сетевые устройства передают сообщения об ошибках.

Вопрос 47

0 / 2 балла (-ов)

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

Ваш ответ

☒ MS Baseliner

☐ CVE Baseline Analyzer

то правильный ответ

Microsoft Security Baseline Analyzer

☐ SANS Baselining System (SBS)

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)

В компании, которая обрабатывает информацию о кредитных картах, происходит нарушение безопасности. Какой отраслевой закон регулирует защиту данных кредитной карты?

☐ Закон Сарбейнса — Оксли (SOX)

☐ Закон Грэмма — Лича — Блайли (GLBA)

Верно!

☒ Стандарт безопасности данных индустрии платежных карт (PCI DSS)

☐ Закон о тайне обмена электронной информацией (ЕСРА)

Refer to curriculum topic: 8.2.2

Стандарт безопасности данных индустрии платежных карт (PCI DSS) представляет собой набор правил для защиты данных кредитных карт, которыми обмениваются банки и продавцы при совершении транзакции.

Вопрос 49

2 / 2 балла (-ов)

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

Верно!

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

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

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

☐ Он может использоваться для перехвата и регистрации сетевого трафика.

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)

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

Верно!



Информация, касающаяся национальной безопасности и внешней политики



Общедоступная информация финансовых учреждений



Информация, не защищенная специальными законами



Негеологическая информация о скважинах

Верно!



Конфиденциальная коммерческая информация

Верно!



Документация правоохранительных органов, попадающая под перечисленные исключения

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: **66** из 100