

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=5504831)

(https://685059869.netacad.com/courses/832407/quizzes/7516579/take?user_id=5504831)

Оценка за эту попытку: **74** из 100

Отправлено 11 Май в 19:41

Эта попытка длилась 14 минут(ы).

Вопрос 1

2 / 2 балла (-ов)

Назовите категорию, к которой относятся киберпреступники, создающие вредоносное ПО для компрометации компаний посредством кражи данных кредитных карт?

☐ «серые» хакеры

☒ «черные» хакеры

☐ «белые» хакеры

☐ хакеры-дилетанты

Верно!

Refer to curriculum topic: 1.2.1

Хакеры определенных категорий похищают информацию с помощью вредоносного ПО.

Вопрос 2

2 / 2 балла (-ов)

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

Верно!

- ☒ Проект Honeynet
- ☐ База данных общих уязвимостей и рисков (CVE)
- ☐ Infragard
- ☐ 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.

Нет ответа

Вопрос 3

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?

то правильный ответ

«белые» хакеры

- ☐ хакеры-дилетанты
- ☐ «серые» хакеры

☐ «черные» хакеры

Refer to curriculum topic: 1.2.1

Категории хакеров обозначены цветами, которые соответствуют целям предпринимаемых атак.

Вопрос 4

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?

- ☐ проводные сети
- ☐ виртуальные сети
- ☐ сети переноса данных вручную

Верно!

☒ беспроводные 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 5

2 / 2 балла (-ов)

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

Верно!

☒ ISO/IEC 27000

☐ Триада «КЦД»

☐ Архитектура NIST/NICE

☐ Модель ISO/OSI

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 6

0 / 2 балла (-ов)

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

то правильный ответ

☒ передаваемые данные

☐ зашифрованные данные

☐ расшифрованные данные

то правильный ответ

☒ хранимые данные

то правильный ответ

☒ обрабатываемые данные

☐ удаленные 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.

Вопрос 7

2 / 2 балла (-ов)

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

☐ обрабатываемые данные

Верно!

☒ хранимые данные

☐ зашифрованные данные

☐ передаваемые данные

Refer to curriculum topic: 2.3.1

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

Вопрос 8

2 / 2 балла (-ов)

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?

☐ секретность, идентификация, невозможность отказа

Верно!

☒ конфиденциальность, целостность, доступность

☐ 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.

Нет ответа

Вопрос 9

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?

то правильный ответ

принуждение

- ☐ срочность
- ☐ близкие отношения
- ☐ доверенные партнеры

Refer to curriculum topic: 3.2.1

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

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
- ☒ подмена
- ☐ прослушивание
- ☐ рассылка спама

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?

Верно!

- ☒ Злоумышленник формирует ботнет из компьютеров-зомби.
- ☐ Компьютер принимает пакеты данных, используя MAC-адрес другого компьютера.
- ☐ Злоумышленник отслеживает сетевой трафик, пытаясь обнаружить учетные данные для аутентификации.
- ☐ Злоумышленник посылает огромные объемы данных, которые сервер не в состоянии обработать.

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)

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?

☐ атака через посредника

☐ подмена пакетов

Верно!

☒ DoS-атака

☐ внедрение SQL-кода

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)

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.

Нет ответа

Вопрос 14

0 / 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?

☐ DDoS-атака.

то правильный ответ

Обман.

☐

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

☐

Атака, при которой злоумышленник выдает себя за авторизованную сторону.

Refer to curriculum topic: 3.2.2

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

Вопрос 15

2 / 2 балла (-ов)

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

☐ Применение надежных паролей.

☐ Внедрение межсетевых экранов.

Верно!

☒

Своевременное обновление операционной системы и остального программного обеспечения.

Верно!

☒

Установка и своевременное обновление антивирусного ПО.

☐ Внедрение сети VPN.

☐ 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 16

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

☐ аудит входа пользователей в систему

☐ наблюдение за всеми сотрудниками

Верно!

☒ набор атрибутов, описывающих права доступа пользователя

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 17

2 / 2 балла (-ов)

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

☐ компенсационные средства контроля

Верно!

☒ средства восстановления

☐ средства обнаружения

☐ 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.

Вопрос 18

2 / 2 балла (-ов)

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

☐ стегоанализ

☐ обфускация программного обеспечения

Верно!

☒ замена данных путем маскирования

☐ стеганография

Refer to curriculum topic: 4.3.1

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

Вопрос 19

2 / 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?

- ☐ закрытый ключ Кэрол
- ☐ общий PSK-ключ, которым шифруются сообщения, адресованные Алисе
- ☐ открытый ключ Боба
- ☒ новый общий PSK-ключ

Верно!

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)

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

- ☐ изменение старшего бита
- ☐ маскирование данных
- ☐ обфускация данных
- ☒ изменение младшего бита

Верно!

Refer to curriculum topic: 4.3.2

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

Нет ответа

Вопрос 21

0 / 2 балла (-ов)

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

- ☐ технологические
- ☐ физические
- ☐ административные

то правильный ответ

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 22

0 / 2 балла (-ов)

Какое из утверждений относится к блочным шифрам?

- ☐ Алгоритмы блочного шифрования быстрее алгоритмов поточного шифрования.
- ☐ Блочное шифрование сжимают шифруемую информацию.

то правильный ответ

При блочном шифровании объем зашифрованных данных обычно больше объема исходных данных.



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 23

2 / 2 балла (-ов)

В какой ситуации требуются средства обнаружения?

Верно!



в сети организации нужно выявить запрещенную активность



нет возможности привлечь сторожевую собаку, поэтому требуется альтернативный вариант



нужно ликвидировать нанесенный организации ущерб



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.

Нет ответа

Вопрос 24

0 / 2 балла (-ов)

Вам поручили провести работу с сотрудниками, отвечающими за сбор и ввод данных в вашей организации: нужно улучшить контроль целостности данных при вводе и модификации. Некоторые сотрудники просят объяснить, с какой целью в новых формах для ввода данных введены ограничения по типу и длине вводимых значений. Что из перечисленного можно назвать новым средством контроля целостности данных?

то правильный ответ

☒ правило проверки ввода, гарантирующее полноту, точность и непротиворечивость данных

☐ шифрование данных, благодаря которому доступ к конфиденциальным данным имеют только авторизованные пользователи

☐ ограничение, согласно которому ввод конфиденциальных данных могут выполнять только авторизованные сотрудники

☐ средства контроля ввода, допускающие лишь просмотр текущих данных

Refer to curriculum topic: 5.4.2

Целостность данных обеспечивается путем их проверки.

Вопрос 25

2 / 2 балла (-ов)

Какая технология хеширования подразумевает обмен ключами?

☐ добавление соли

Верно!

☒ HMAC

☐ AES

☐ MD5

Refer to curriculum topic: 5.1.3

Механизм HMAC отличается от обычного хеширования наличием ключей.

Нет ответа

Вопрос 26

0 / 2 балла (-ов)

Назовите главную особенность криптографической хеш-функции.

то правильный ответ

Хеш-функция необратима.

☐

По выходному значению хеш-функции можно вычислить входное значение.

☐

Выходные значения имеют различную длину.

☐

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 27

2 / 2 балла (-ов)

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

- ☐ доменная целостность
- ☐ Определяемая пользователем целостность
- ☒ сущностная целостность
- ☐ ссылочная целостность

Верно!

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)

К какой технологии обеспечения безопасности относится стандарт X.509?

то правильный ответ

цифровые сертификаты

- ☐ надежные пароли
- ☐ технология биометрической идентификации
- ☐ токены безопасности

Refer to curriculum topic: 5.3.2

С помощью цифровых сертификатов обеспечивается безопасность сторон защищенного соединения.

Нет ответа

Вопрос 29

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.

- ☐ добавление соли

то правильный ответ

HMAC

- ☐ CRC
- ☐ пароль

Refer to curriculum topic: 5.1.3

Алгоритм HMAC предназначен для аутентификации. Отправитель и получатель пользуются секретным ключом, который совместно с данными применяется для аутентификации источника сообщения и проверки подлинности данных.

Вопрос 30

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 31

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

Верно!

☒ SHA-256

☐ MD5

☐ 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.

Вопрос 32

2 / 2 балла (-ов)

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

Верно!

- ☒ отказоустойчивость системы
- ☐ бесперебойное обслуживание
- ☐ единая точка отказа
- ☐ 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.

Вопрос 33

2 / 2 балла (-ов)

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

Верно!

- ☒ передача риска
- ☐ уклонение от риска

☐ снижение риска

☐ принятие риска

Refer to curriculum topic: 6.2.1

Меры по снижению рисков уменьшают степень уязвимости организации к угрозам, что достигается за счет передачи, принятия или снижения риска, а также уклонения от него.

Вопрос 34

2 / 2 балла (-ов)

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

☐ классификация ресурсов

Верно!

☒ стандартизация ресурсов

☐ доступность 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 35**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?

Верно!

- ☐ обеспечение удаленного доступа для тысяч внешних пользователей
- ☒ повышение надежности и эксплуатационной готовности серверов
- ☐ 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 36****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 потерь

то правильный ответ

- ☒ количественный анализ
- ☐ анализ защищенности

☐ 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 37

2 / 2 балла (-ов)

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

Верно!

☒ обнаружение и анализ

☐ предотвращение и изоляция

☐ анализ рисков и высокая доступность

☐ устранение угроз и принятие

Верно!

☒ изоляция и восстановление

☐ 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 38

2 / 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?

Верно!

- ☒ качественный анализ
- ☐ количественный анализ
- ☐ анализ степени уязвимости к угрозам
- ☐ анализ потерь

Refer to curriculum topic: 6.2.1

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

Вопрос 39

2 / 2 балла (-ов)

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

Верно!

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.

Нет ответа

Вопрос 40

0 / 2 балла (-ов)

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

☐ распознавательные

то правильный ответ

превентивные

☐ административные

☐ корректирующие

Refer to curriculum topic: 6.4.1

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

Нет ответа

Вопрос 41

0 / 2 балла (-ов)

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

☐ Забор сможет противостоять нарушителю, намеренно проникающему на территорию.

☐ Забор ненадолго задержит нарушителя, намеренно проникающего на территорию.

☐ Забор ограждает территорию от случайных прохожих благодаря своей высоте.

то правильный ответ

Забор сдерживает только случайных прохожих.

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 42

2 / 2 балла (-ов)

Какие атаки можно предотвратить с помощью взаимной аутентификации?

- ☐ беспроводной спам
- ☐ анализ беспроводного трафика
- ☐ подмена IP-адреса отправителя в беспроводных сетях
- ☒ атака через посредника

Верно!

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 43

2 / 2 балла (-ов)

Какая из утилит использует протокол ICMP?

- ☒ ping
- ☐ NTP

Верно!

☐ RIP

☐ DNS

Refer to curriculum topic: 7.3.1

С помощью протокола ICMP сетевые устройства передают сообщения об ошибках.

Вопрос 44

2 / 2 балла (-ов)

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

☐

количество ложноположительных срабатываний и степень приемлемости

☐

степень приемлемости и количество ложноотрицательных срабатываний

☐

степень неприемлемости и количество ложноотрицательных срабатываний

Верно!

☒

количество ложноотрицательных результатов и количество ложноположительных результатов

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)

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

☐ SSH

Верно!

☒ шифрование голосового трафика

☐ сильная аутентификация

☐ ARP

Refer to curriculum topic: 7.3.2

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

Вопрос 46

2 / 2 балла (-ов)

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

☐ WPA

☐ WEP

Верно!

☒ WPA2

☐ WEP2

Refer to curriculum topic: 7.1.2

Безопасность беспроводных сетей определяется соответствующими стандартами, которые постепенно становятся все более и более надежными. На смену WEP пришел стандарт WPA, который уступил место WPA2.

Вопрос 47

2 / 2 балла (-ов)

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

Верно!

☒ STP

Верно!

☒ ARP

☐ IP

☐ RIP

☐ WPA2

☐ 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 48

2 / 2 балла (-ов)

Что можно использовать для балльной оценки серьезности угроз в целях определения важных уязвимостей?

☐ Центр реагирования на компьютерные инциденты (CERT)

Верно!

☒ Национальная база данных об уязвимостях (NVD)

☐ ACSC

☐ ISC

Refer to curriculum topic: 8.2.3

Национальная база данных об уязвимостях (NVD) используется для оценки серьезности уязвимостей и используется организациями для балльной оценки критичности уязвимостей, обнаруженных в сети.

Вопрос 49

2 / 2 балла (-ов)

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



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



Он может использоваться для перехвата и регистрации сетевого трафика.

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.

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)

Каковы две потенциальные угрозы для приложений? (Выберите два варианта.)

☐ Перебои питания

Верно!

☒ потеря данных

Верно!

☒ несанкционированный доступ

☐ социальная инженерия

Refer to curriculum topic: 8.1.7

Угрозы для приложений могут включать:

- несанкционированный доступ к центрам обработки данных, машинным залам и коммутационным шкафам;
- остановку сервера для технического обслуживания;
- уязвимость ПО сетевой операционной системы;
- несанкционированный доступ к системам;
- потерю данных;
- продолжительный простой информационных систем;
- уязвимости, возникающие при разработке клиентских, серверных и веб-приложений.

Оценка контрольной работы: **74** из 100