

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.](#)

История попыток

	Попытка	Время	Оценка
последняя	Попытка 1	52 минут(ы)	93,33 из 100

Оценка за эту попытку: **93,33** из 100
Отправлено 23 Май в 12:47
Эта попытка длилась 52 минут(ы).

Верно!

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

☐ хакеры-дилетанты

☐ «белые» хакеры

Refer to curriculum topic: 1.2.1

Хакеры определенных категорий похищают информацию с помощью вредоносного ПО.

Вопрос 2

2 / 2 балла (-ов)

Специалисту из отдела кадров предложили провести занятия с учащимися государственных школ, чтобы привлечь внимание молодых людей к сфере кибербезопасности. Назовите три темы, которым нужно уделить особое внимание на этих занятиях, чтобы мотивировать учащихся к построению карьеры в этой области? (Выберите три варианта.)

Верно!

☒ высокий доход

☐ должность, подразумевающая рутинную повседневную работу

☐ сертификация CompTIA A+ обеспечивает достаточный уровень знаний для начала карьеры

Верно!

☒ высокий спрос на специалистов

☐ необходима докторская степень (PhD)

Верно!

☒ служение обществу

Refer to curriculum topic: 1.2.2

Высокий спрос на специалистов по кибербезопасности открывает уникальные карьерные возможности.

Вопрос 3

2 / 2 балла (-ов)

К какому типу относится атака, при которой злоумышленники формируют пакеты, маскируемые под обычный сетевой трафик, и таким образом вмешиваются в работу сети?

- ☐ перехватывание пакетов
- ☐ DNS-подмена
- ☒ подделка пакетов
- ☐ неавторизованная точка доступа Wi-Fi

Верно!

Refer to curriculum topic: 1.3.1

Специалисты по кибербезопасности должны хорошо понимать механизмы различных видов атак.

Вопрос 4

0,67 / 2 балла (-ов)

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

☐ зашифрованные данные

Это правильный ответ

☒ обрабатываемые данные

Ваш ответ

☒ удаленные данные

Верно!

☒ передаваемые данные

Верно!

☒ хранимые данные

☐ расшифрованные 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 5

2 / 2 балла (-ов)

Какую технологию идентификации можно использовать в составе системы аутентификации сотрудников?

Верно!

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

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)

К специалисту по безопасности обратились за советом: нужно выбрать механизм безопасности, с помощью которого можно будет исключить доступ неавторизованных хостов в домашнюю сеть сотрудников. Какая мера наиболее эффективна в данном случае?

- ☐ Внедрение систем обнаружения вторжений.
- ☐ Применение RAID.
- ☐ Применение виртуальной локальной сети.
- ☒ Внедрение межсетевого экрана.

Верно!

Refer to curriculum topic: 2.4.1

Для защиты конфиденциальности данных необходимо понимать, какие технологии используются для защиты данных во всех их трех состояниях.

Вопрос 7

2 / 2 балла (-ов)

Какая из технологий обеспечивает конфиденциальность данных?

Верно!

- ☒ шифрование
- ☐ хэширование
- ☐ управление идентификационными данными
- ☐ RAID

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)

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

- ☐ SHS
- ☐ RAID
- ☐ сети VLAN
- ☒ VPN

Верно!

Refer to curriculum topic: 2.4.1

Для защиты конфиденциальности данных необходимо понимать, какие технологии используются для защиты данных во всех их трех состояниях.

Вопрос 9

2 / 2 балла (-ов)

К какому типу относится атака, при которой мошеннические веб-сайты размещаются на высоких позициях в списках результатов веб-поиска?

- ☐ спам
- ☒ злоупотребление поисковой оптимизацией
- ☐ атака путем подделки DNS
- ☐ угонщик браузеров

Верно!

Refer to curriculum topic: 3.1.2

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

- ☐ Внедрение межсетевых экранов.
- ☐ Внедрение сети VPN.
- ☐ Применение RAID.
- ☐ Применение надежных паролей.

Верно!

- ☒ Своевременное обновление операционной системы и остального программного обеспечения.

Верно!

- ☒ Установка и своевременное обновление антивирусного ПО.

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 11

2 / 2 балла (-ов)

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

Верно!

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

Вопрос 12

2 / 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?

Верно!

- ☐ Проверить системы на наличие вирусов.
- ☒ Проверить системы на наличие неавторизованных учетных записей.

- ☐ Проверить, нет ли учетных записей без паролей.
- ☐ Проверить в журнале событий, не было ли изменений в политике.

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 нетехнический метод, с помощью которого киберпреступники получают конфиденциальную информацию.

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

Верно!

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 14

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?

- ☒ DoS-атака

Верно!

- ☐ подмена пакетов
- ☐ атака через посредника
- ☐ 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 15

2 / 2 балла (-ов)

Сотрудники компании получают электронные письма, в которых говорится, что срок действия пароля учетной записи истекает в ближайшее время и поэтому нужно сменить пароль в течение 5 минут. Какое из описаний подходит для такого электронного сообщения?

- ☐ Атака, при которой злоумышленник выдает себя за авторизованную сторону.
- ☐ DDoS-атака.
- ☐ Атака, при которой злоумышленник проникает в систему, пользуясь действующим подключением авторизованного пользователя.
- ☒ Обман.

Верно!

Refer to curriculum topic: 3.2.2

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

Вопрос 16

2 / 2 балла (-ов)

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

Верно!

- ☒ открытый ключ Боба
- ☐ открытый ключ Алисы
- ☐ закрытый ключ Боба
- ☐ закрытый ключ Алисы

Refer to curriculum topic: 4.1.3

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

Вопрос 17

2 / 2 балла (-ов)

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

Верно!

- ☐ компенсационные средства контроля
- ☒ средства восстановления
- ☐ сдерживающие средства контроля
- ☐ средства обнаружения

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)

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 19

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
- ☐ стеганография
- ☒ замена данных путем маскирования

Верно!

Refer to curriculum topic: 4.3.1

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

Вопрос 20

2 / 2 балла (-ов)

Какое из утверждений относится к блочным шифрам?

Верно!



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.



Алгоритмы блочного шифрования быстрее алгоритмов поточного шифрования.



Блочное шифрование сжимают шифруемую информацию.

Refer to curriculum topic: 4.1.2

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

Верно!

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

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)

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

- ☐ доступ
- ☐ авторизация
- ☐ идентификация
- ☒ аутентификация

Верно!

Refer to curriculum topic: 4.2.4

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

Вопрос 23

2 / 2 балла (-ов)

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

- ☐ технологические
- ☐ административные
- ☐ физические
- ☒ логические

Верно!

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 24

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?

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

Верно!

Refer to curriculum topic: 5.3.1

Цифровые сертификаты предназначены для защиты участников защищенного информационного обмена.

Вопрос 25

2 / 2 балла (-ов)

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

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

Вопрос 26

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
- ☐ SHA-1
- ☒ SHA-256
- ☐ AES

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 27

2 / 2 балла (-ов)

К какой технологии обеспечения безопасности относится стандарт X.509?

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

Верно!

Refer to curriculum topic: 5.3.2

С помощью цифровых сертификатов обеспечивается безопасность сторон защищенного соединения.

Вопрос 28

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?

- ☒ цифровые сертификаты
- ☐ сети VPN и сервисы шифрования
- ☐ правила проверки данных
- ☐ операции хеширования

Верно!

Refer to curriculum topic: 5.3.2

Цифровые сертификаты предназначены для защиты участников защищенного информационного обмена.

Вопрос 29**2 / 2 балла (-ов)**

Какой алгоритм хеширования следует использовать для защиты конфиденциальной несекретной информации?

- ☐ MD5
- ☒ SHA-256
- ☐ 3DES
- ☐ AES-256

Верно!

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 30**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?

- ☐ MD5
- ☐ AES
- ☐ радужные таблицы
- ☒ HMAC

Верно!

Refer to curriculum topic: 5.1.3

В НМАС 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 31

0 / 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?

☐ открытый ключ Боба

Это правильный ответ

☒ закрытый ключ Алисы

Ваш ответ

☒ 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 32

0 / 2 балла (-ов)

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

Ваш ответ

☒ многоуровневый подход

Что правильный ответ

ограничение

☐ сокрытие информации

☐ упрощение

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 33

2 / 2 балла (-ов)

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

Верно!

☒ обнаружение и анализ

☐ устранение угроз и принятие

☐ конфиденциальность и ликвидация

☐ предотвращение и изоляция

☐ анализ рисков и высокая доступность

Верно!

☒ изоляция и восстановление

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 34

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?

Верно!

- ☐ Министерство образования США
- ☒ Нью-Йоркская фондовая биржа
- ☐ магазины в местном торговом центре
- ☐ офис спортивной команды высшей лиги

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 35

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.

Верно!

- ☐ Модель ISO/IEC 27000
- ☒ Национальная база данных общих уязвимостей и рисков (CVE)
- ☐ Архитектура NIST/NICE
- ☐ Infragard

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 36

2 / 2 балла (-ов)

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

- ☐ снижение риска
- ☒ передача риска
- ☐ принятие риска
- ☐ уклонение от риска

Верно!

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 37

2 / 2 балла (-ов)

В организации недавно внедрили программу по обеспечению доступности на уровне «пять девяток», которая охватывает два критически важных сервера баз данных. Какие меры потребуются для реализации этой программы?

- ☒ повышение надежности и эксплуатационной готовности серверов
- ☐ повышение надежности шифрования

Верно!

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

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 38

2 / 2 балла (-ов)

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

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

Верно!

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 39

2 / 2 балла (-ов)

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

☐ административные

☐ распознавательные

Верно!

☒ превентивные

☐ корректирующие

Refer to curriculum topic: 6.4.1

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

Вопрос 40

2 / 2 балла (-ов)

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

Верно!

☒ количество реализаций угрозы в год

☐ мера уязвимости ресурса к угрозе

☐ ценность ресурса

☐ коэффициент частоты

Верно!

☒ ожидаемый ущерб в результате реализации единичной угрозы

☐ количественная величина убытков

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.

Вопрос 41

2 / 2 балла (-ов)

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

☐ RIP

☐ IP

☐ WPA2

☐ ICMP

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)

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

Верно!

☒ WPA2

☐ TKIP

☐ 802.11q

Верно!

☒ WPA

Верно!

☒ 802.11i

☐ WEP

Refer to curriculum topic: 7.3.1

Защищенную систему связи можно организовать с помощью различных протоколов. Алгоритм AES является наиболее стойким алгоритмом шифрования.

Вопрос 43

2 / 2 балла (-ов)

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

- ☐ WPA
- ☐ WEP2
- ☒ WPA2
- ☐ 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 44

2 / 2 балла (-ов)

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

- ☐ ARP
- ☐ SSH
- ☐ сильная аутентификация

Верно!

- ☒ шифрование голосового трафика

Refer to curriculum topic: 7.3.2

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

Вопрос 45

2 / 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»
- ☐ Управление компьютером
- ☐ Журнал безопасности в средстве просмотра событий

Верно!

- ☒ 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».

Вопрос 46

2 / 2 балла (-ов)

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

- ☐ SCP

☐ Telnet

☐ WPA

Верно!

☒ SSH

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 47

2 / 2 балла (-ов)

Какие атаки можно предотвратить с помощью взаимной аутентификации?

☐ анализ беспроводного трафика

Верно!

☒ атака через посредника

☐ подмена IP-адреса отправителя в беспроводных сетях

☐ беспроводной спам

Refer to curriculum topic: 7.1.2

Специалист по обеспечению кибербезопасности должен знать, какие существуют технологии и средства, которые используются в качестве контрмер для защиты организации от угроз и нейтрализации уязвимостей.

Вопрос 48

2 / 2 балла (-ов)

Несанкционированные посетители вошли в офис компании и ходят по зданию. Какие две меры могут предотвратить доступ несанкционированных посетителей в здание? (Выберите два варианта.)

Верно!

☒ Определение правил и процедур для гостей, посещающих здание

☐ Запрет на выход из здания в рабочее время

Верно!

☒ Регулярное проведение обучения по вопросам безопасности

☐ Замки на шкафах

Refer to curriculum topic: 8.1.6

Любое несанкционированное лицо, входящее на объект, может представлять потенциальную угрозу. Общие меры для повышения физической безопасности включают:

- управление доступом и установку средств видеонаблюдения у каждого входа;
- определение правил и процедур для гостей, посещающих объект;
- проверку безопасности здания с помощью физических средств, используемых для тайного получения доступа;
- шифрование пропусков для доступа;
- регулярное проведение обучения по вопросам безопасности;
- внедрение системы маркировки ресурсов.

Вопрос 49

0,67 / 2 балла (-ов)

Каковы три основные категории должностей по информационной безопасности? (Выберите три варианта.)

Ваш ответ

☒ Исполняющие

Что правильный ответ

Создающие

Верно!

☒ Определяющие

☐ Ищущие

Верно!

☒ Наблюдающие

☐ Творящие

Refer to curriculum topic: 8.3.1

Должности по информационной безопасности можно отнести к следующим трем категориям:

- определяющие;
- создающие;
- наблюдающие.

Вопрос 50

2 / 2 балла (-ов)

Компания пытается снизить затраты на развертывание коммерческого программного обеспечения и рассматривает возможность использования облачных служб. Какая облачная служба будет наилучшей для размещения программного обеспечения?

- ☐ Восстановление как услуга (RaaS)
- ☒ ПО как услуга (SaaS)
- ☐ Инфраструктура как услуга (IaaS)
- ☐ Платформа как услуга (PaaS)

Верно!

Refer to curriculum topic: 8.1.5

Программное обеспечение как услуга (SaaS) обеспечивает пользователям доступ к централизованно размещенному в облаке программному обеспечению через веб-обозреватель.

Оценка контрольной работы: **93,33** из 100