

# 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](#)

Оценка за эту попытку: **83** из 100  
Отправлено 14 Май в 19:56  
Эта попытка длилась 18 минут(ы).

Вопрос 1	2 / 2 балла (-ов)
<p>Специалисту по кибербезопасности поручили выявить потенциальных преступников, организовавших атаку на организацию. Какая категория хакеров должна меньше всего интересовать специалиста в такой ситуации?</p>	
<div><input type="radio"/> хакеры-дилетанты</div> <div><input type="radio"/> «серые» хакеры</div> <div><input checked="" type="radio"/> «белые» хакеры</div> <div><input type="radio"/> «черные» хакеры</div>	

Верно!

Refer to curriculum topic: 1.2.1

Категории хакеров обозначены цветами, которые соответствуют целям предпринимаемых атак.

## Вопрос 2

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?

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

Верно!

Refer to curriculum topic: 1.3.1

Специалисты по кибербезопасности должны хорошо понимать механизмы различных видов атак.

Нет ответа

## Вопрос 3

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

высокий спрос на специалистов

- ☐ необходима докторская степень (PhD)

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

то правильный ответ **служение обществу**

- ☐ должность, подразумевающая рутинную повседневную работу

то правильный ответ **высокий доход**

Refer to curriculum topic: 1.2.2

Высокий спрос на специалистов по кибербезопасности открывает уникальные карьерные возможности.

Нет ответа

#### Вопрос 4

0 / 2 балла (-ов)

Назовите методы, с помощью которых можно внедрить многофакторную аутентификацию.

- ☐ сети VPN и VLAN

то правильный ответ **пароли и отпечатки пальцев**

- ☐ системы IDS и IPS

- ☐ токены и хеш-суммы

Refer to curriculum topic: 2.2.1

Специалист по обеспечению кибербезопасности должен знать, какие существуют технологии для поддержки триады «конфиденциальность, целостность, доступность».

#### Вопрос 5

2 / 2 балла (-ов)

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

☐ удаленные данные

☐ расшифрованные данные

Верно!

☒ передаваемые данные

☐ зашифрованные данные

Верно!

☒ обрабатываемые данные

Верно!

☒ хранимые 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 6

2 / 2 балла (-ов)

Специалист по кибербезопасности совместно с сотрудниками подразделения ИТ работает над планом информационной безопасности. Какой набор принципов безопасности следует взять за основу при разработке плана информационной безопасности?

Верно!

☒ конфиденциальность, целостность, доступность

☐ технологии, политики, осведомленность

☐ секретность, идентификация, невозможность отказа

☐ шифрование, аутентификация, идентификация

Refer to curriculum topic: 2.1.1

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

## Вопрос 7

2 / 2 балла (-ов)

Какая из технологий обеспечивает конфиденциальность данных?

Верно!

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

Refer to curriculum topic: 2.2.1

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

Нет ответа

## Вопрос 8

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.

то правильный ответ

- ☐ NAS
- ☐ сеть хранения данных (SAN)

☐ VPN

Refer to curriculum topic: 2.4.1

Специалист по кибербезопасности должен быть хорошо знаком с современными технологиями, позволяющими усилить политику безопасности, действующую в его организации.

## Вопрос 9

2 / 2 балла (-ов)

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

☐ атака через посредника

☐ троян

☐ DoS-атака

Верно!

☒ программа-вымогатель

Refer to curriculum topic: 3.1.1

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

## Вопрос 10

2 / 2 балла (-ов)

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

☐ внедрение SQL-кода

☐ внедрение в ОЗУ

☐ подмена ОЗУ

Верно!

☒ 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 11

0 / 2 балла (-ов)

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

☐ программа-вымогатель

☐ фарминг

☐ атака через посредника

то правильный ответ

социальная инженерия

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 12

2 / 2 балла (-ов)

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

Верно!

☒ прослушивание

☐ рассылка спама

☐ подмена

☐ фишинг

Refer to curriculum topic: 3.3.1

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

### Вопрос 13

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?

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

Верно!

☒ Проверить системы на наличие неавторизованных учетных записей.

☐ Проверить системы на наличие вирусов.

☐ Проверить, нет ли учетных записей без паролей.



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 14

2 / 2 балла (-ов)

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

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

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 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?

- ☒ интернет-червь
- ☐ фишинг

Верно!

☐ спам

☐ вирус

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

2 / 2 балла (-ов)

Какое из утверждений относится к блочным шифрам?

☐

Алгоритмы блочного шифрования обрабатывают открытый текст по одному биту и формируют из битов блоки.

Верно!

☒

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

☐

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 17

2 / 2 балла (-ов)

В какой ситуации требуются средства обнаружения?



нет возможности привлечь сторожевую собаку, поэтому требуется альтернативный вариант

Верно!



в сети организации нужно выявить запрещенную активность



необходимо восстановить нормальное состояние систем после проникновения в сеть организации



нужно ликвидировать нанесенный организации ущерб

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 18

2 / 2 балла (-ов)

Пользователь хранит большой объем конфиденциальных данных, которые необходимо защитить. Какой алгоритм лучше подходит для решения этой задачи?



RSA



ECC



алгоритм Диффи-Хеллмана

Верно!



3DES

Refer to curriculum topic: 4.1.4

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

### Вопрос 19

2 / 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?

- ☐ закрытый ключ Кэрл
- ☐ 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

0 / 2 балла (-ов)

Что происходит по мере увеличения длины ключа шифрования?

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

Ваш ответ

☐ Пространство ключей пропорционально уменьшается.

то правильный ответ

☒ Пространство ключей экспоненциально увеличивается.

Refer to curriculum topic: 4.1.4

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?

Верно!

☒ набор атрибутов, описывающих права доступа пользователя

☐ аудит входа пользователей в систему

☐ устройство считывания отпечатков пальцев

☐ 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)

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

Верно!

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

Refer to curriculum topic: 4.3.2

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

### Вопрос 23

2 / 2 балла (-ов)

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

Верно!

- ☒ Избирательный контроль доступа
- ☐ Контроль доступа на основе ролей
- ☐ Обязательное разграничение доступа
- ☐ ACL

Refer to curriculum topic: 4.2.2

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

### Вопрос 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?

☐ хеширование данных

Верно!

☒ цифровые сертификаты

☐ асимметричное шифрование

☐ симметричное шифрование

Refer to curriculum topic: 5.3.1

Цифровые сертификаты предназначены для защиты участников защищенного информационного обмена.

## Вопрос 25

2 / 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.)

Верно!

☒ таблицы поиска

☐ хеш-суммы паролей

Верно!

☒ реверсивные таблицы поиска

☐ неавторизованные точки доступа

☐ таблицы алгоритмов

Верно!

☒ радужные таблицы

Refer to curriculum topic: 5.1.2

Пароли взламываются с помощью таблиц с возможными вариантами паролей.

## Вопрос 26

2 / 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?



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



правило проверки ввода, гарантирующее полноту, точность и непротиворечивость данных



средства контроля ввода, допускающие лишь просмотр текущих данных



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

Верно!

Refer to curriculum topic: 5.4.2

Целостность данных обеспечивается путем их проверки.

## Вопрос 27

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

☐ MD5

☐ AES

Верно!

☒ SHA-256

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 28

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.

### Вопрос 29

2 / 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
- ☒ HMAC

Верно!

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

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?

- ☐ AES
- ☐ радужные таблицы

то правильный ответ HMAC

Ваш ответ

- ☒ MD5

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 31

1 / 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.)

☐ Обе системы шифруют пароли перед хешированием.



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

то правильный ответ

В системах применяются различные алгоритмы хеширования.

☐ 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 32

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

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.

### Вопрос 33

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?

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

Верно!

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 34

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?

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

Верно!

Refer to curriculum topic: 6.2.1

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

### Вопрос 35

2 / 2 балла (-ов)

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

☐ конфиденциальность и ликвидация

☐ устранение угроз и принятие

☐ предотвращение и изоляция

Верно!

☒ изоляция и восстановление

Верно!

☒ 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.

### Вопрос 36

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 37

2 / 2 балла (-ов)

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

Верно!

- ☒ ограничение
- ☐ сокрытие информации
- ☐ упрощение
- ☐ 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 38

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.

то правильный ответ

Национальная база данных общих уязвимостей и рисков (CVE)

☐ Infragard

Ваш ответ

☒ Модель ISO/IEC 27000

☐ 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.

### Вопрос 39

2 / 2 балла (-ов)

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

☐ ценность ресурса

☐ количественная величина убытков

Верно!

☒ ожидаемый ущерб в результате реализации единичной угрозы

☐ коэффициент частоты

Верно!

☒ количество реализаций угрозы в год

☐ мера уязвимости ресурса к угрозе



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 40

2 / 2 балла (-ов)

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

☐ сокрытие информации

☐ ограничение

Верно!

☒ многоуровневый подход

☐ разнообразие

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?

☐ сильная аутентификация

☐ SSH

☐ ARP

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 42

2 / 2 балла (-ов)

Какая из утилит использует протокол ICMP?

☐ NTP

Верно!

☒ ping

☐ RIP

☐ DNS

Refer to curriculum topic: 7.3.1

С помощью протокола ICMP сетевые устройства передают сообщения об ошибках.

## Вопрос 43

2 / 2 балла (-ов)

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

☐ SANS Baselining System (SBS)

☐ CVE Baseline Analyzer

☐ MS Baseliner

Верно!

☒ Microsoft Security Baseline Analyzer

Refer to curriculum topic: 7.1.1

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

#### 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?

Ваш ответ

☒ 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».

#### Вопрос 45

2 / 2 балла (-ов)

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

☐ WEP2

☐ WEP

☐ WPA

Верно!

☒ 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.

#### Вопрос 46

2 / 2 балла (-ов)

Какие атаки можно предотвратить с помощью взаимной аутентификации?

Верно!

☒ атака через посредника

☐ подмена IP-адреса отправителя в беспроводных сетях

☐ анализ беспроводного трафика

☐ 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 47

2 / 2 балла (-ов)

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

☐ IP

Верно!

☒ STP

☐ ICMP

Верно!

☒ ARP

☐ WPA2

☐ RIP

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)

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

Верно!

☒ Закон о компьютерном мошенничестве (CFAA)

☐ Закон о тайне обмена электронной информацией (ECPA)

☐ Закон Сарбейнса — Оксли (SOX)

☐ Закон Грэмма — Лича — Блайли (GLBA)

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.

### Вопрос 49

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)

Верно!

☒ ПО как услуга (SaaS)

☐ Инфраструктура как услуга (IaaS)

☐ Платформа как услуга (PaaS)

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.

### Вопрос 50

2 / 2 балла (-ов)

Аудитору предлагают оценить потенциальные угрозы для локальной сети компании. Какие три потенциальные угрозы может отметить аудитор? (Выберите три варианта.)

☐ Политика допустимого использования

Верно!

Верно!

Верно!

☐ Сложные пароли

☒ Неправильно настроенный межсетевой экран

☒ Открытый доступ к сетевому оборудованию

☒ Несанкционированное сканирование портов и зондирования сети

☐ Закрытый доступ к системам

Refer to curriculum topic: 8.1.3

К локальной сети может быть подключено множество оконечных устройств. Анализ сетевых и подключенных оконечных устройств важен для определения угроз.

Оценка контрольной работы: **83** из 100