

# 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=8462074)  
([https://685059869.netacad.com/courses/832407/quizzes/7516579/take?user\\_id=8462074](https://685059869.netacad.com/courses/832407/quizzes/7516579/take?user_id=8462074))

## История попыток

	Попытка	Время	Оценка
ПОСЛЕДНЯЯ	<a href="https://685059869.netacad.com/courses/832407/quizzes/7516579/history?version=1">Попытка 1</a> ( <a href="https://685059869.netacad.com/courses/832407/quizzes/7516579/history?version=1">https://685059869.netacad.com/courses/832407/quizzes/7516579/history?version=1</a> )	58 минут(ы)	92,67 из 100

Оценка за эту попытку: **92,67** из 100  
Отправлено 22 Май в 8:44  
Эта попытка длилась 58 минут(ы).

Вопрос 12 / 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

☐

неавторизованная точка доступа Wi-Fi

☐

перехватывание пакетов

☒

подделка пакетов

Верно!

Refer to curriculum topic: 1.3.1

Специалисты по кибербезопасности должны хорошо понимать механизмы различных видов атак.

## Вопрос 2

2 / 2 балла (-ов)

Назовите две группы лиц, которые относятся к категории внутренних злоумышленников. (Выберите два варианта.)

☐ кибермастера

☐ хактивисты

☐ непрофессионалы

☐ «черные» хакеры

Верно!

☒ бывшие сотрудники

Верно!

☒ доверенные партнеры

Refer to curriculum topic: 1.4.1

Угрозы делятся на внешние и внутренние. Специалист по кибербезопасности должен иметь ясное представление о возможных источниках угроз.

## Вопрос 3

2 / 2 балла (-ов)

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

☐ «серые» хакеры

☐ «белые» хакеры

☐ хакеры-дилетанты

Верно!

☒ «черные» хакеры

Refer to curriculum topic: 1.2.1

Хакеры определенных категорий похищают информацию с помощью вредоносного ПО.

#### Вопрос 4

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.

#### Вопрос 5

2 / 2 балла (-ов)

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

Верно!

- ☒ хранимые данные
- ☐ зашифрованные данные
- ☐ обрабатываемые 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 6

2 / 2 балла (-ов)

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

- ☐ удаленные данные
- ☒ хранимые данные
- ☐ расшифрованные данные
- ☐ зашифрованные данные
- ☒ передаваемые данные
- ☒ обрабатываемые данные

Верно!

Верно!

Верно!

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)

Какую технологию идентификации можно использовать в составе системы аутентификации сотрудников?

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

Верно!

Refer to curriculum topic: 2.2.1

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

### Вопрос 8

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?

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

Верно!

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 9

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 системы на наличие вирусов.
- ☒ Проверить системы на наличие неавторизованных учетных записей.
- ☐ Проверить в журнале событий, не было ли изменений в политике.
- ☐ Проверить, нет ли учетных записей без паролей.

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 10

0,67 / 2 балла (-ов)

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

- ☐ Увеличить число охранников.
- ☒ Не вводить пароли в окне чата.

Верно!

☐ Внедрить эффективные межсетевые экраны.

Ваш ответ



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

Верно!



Повысить осведомленность сотрудников относительно действующих политик.

то правильный ответ

Не переходить по ссылкам, вызывающим любопытство.

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 11

2 / 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?

☐ доверенные партнеры

Верно!

☒ принуждение

☐ срочность

☐ близкие отношения

Refer to curriculum topic: 3.2.1

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

## Вопрос 12

2 / 2 балла (-ов)

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

- ☐ атака через посредника
- ☐ программа-вымогатель
- ☐ фарминг
- ☒ 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 13

2 / 2 балла (-ов)

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

- ☐ подмена ОЗУ
- ☒ переполнение буфера
- ☐ внедрение SQL-кода
- ☐ внедрение в ОЗУ

Верно!



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.

## Вопрос 14

2 / 2 балла (-ов)

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

☐ Применение надежных паролей.

Верно!

☒ Установка и своевременное обновление антивирусного ПО.

☐ Внедрение межсетевых экранов.

Верно!

☒ Своевременное обновление операционной системы и остального программного обеспечения.

☐ Применение RAID.

☐ Внедрение сети VPN.

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 15

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
- ☐ атака через посредника
- ☒ подмена
- ☐ прослушивание

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 16

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
- ☒ замена данных путем маскирования
- ☐ стеганография

Верно!

Refer to curriculum topic: 4.3.1

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

## Вопрос 17

2 / 2 балла (-ов)

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

☐ RSA

☐ DES

Верно!

☒ AES

☐ 3DES

Refer to curriculum topic: 4.1.4

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

## Вопрос 18

2 / 2 балла (-ов)

Назовите компонент, представляющий наибольшую сложность при разработке криптосистемы.

☐ длина ключа

☐ алгоритм шифрования

Верно!

☒ управление ключами

☐ обратная разработка

Refer to curriculum topic: 4.1.1

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

## Вопрос 19

0 / 2 балла (-ов)

Какое из утверждений относится к блочным шифрам?

Ваш ответ



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

то правильный ответ

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



Блочное шифрование сжимают шифруемую информацию.



Алгоритмы блочного шифрования быстрее алгоритмов поточного шифрования.

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)

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



Обязательное разграничение доступа

Верно!



Избирательный контроль доступа



Контроль доступа на основе ролей



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 21

2 / 2 балла (-ов)

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

☐ распознавательные

☐ компенсирующие

☐ превентивные

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 22

2 / 2 балла (-ов)

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

☐ компенсационные средства контроля

Верно!

☒ 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 23

2 / 2 балла (-ов)

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

☐ технологические

☐ физические

Верно!

☒ логические

☐ административные

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)

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

☐ SHA-256

☐ CRC

Верно!

☒ добавление соли

☐ HMAC

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 25

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

☐ правила проверки данных

☐ операции хеширования

Верно!

☒ цифровые сертификаты

Refer to curriculum topic: 5.3.2

Цифровые сертификаты предназначены для защиты участников защищенного информационного обмена.

## Вопрос 26

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
- ☐ Определяемая пользователем целостность
- ☒ сущностная 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 27

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?

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

Верно!



Refer to curriculum topic: 5.3.1

Цифровые сертификаты предназначены для защиты участников защищенного информационного обмена.

## Вопрос 28

2 / 2 балла (-ов)

К какой технологии обеспечения безопасности относится стандарт X.509?

☐ технология биометрической идентификации

Верно!

☒ цифровые сертификаты

☐ надежные пароли

☐ токены безопасности

Refer to curriculum topic: 5.3.2

С помощью цифровых сертификатов обеспечивается безопасность сторон защищенного соединения.

## Вопрос 29

2 / 2 балла (-ов)

Назовите главную особенность криптографической хеш-функции.

☐ По выходному значению хеш-функции можно вычислить входное значение.

☐ Для хеширования необходимы открытый и закрытый ключи.

☐ Выходные значения имеют различную длину.

Верно!

☒ Хеш-функция необратима.

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)

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-256

☐ AES

☐ SHA-1

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 31

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!

☒ радужные таблицы

Верно!

☒ реверсивные таблицы поиска

☐ неавторизованные точки доступа

☐ таблицы алгоритмов

☐ хеш-суммы паролей

Верно!

☒ таблицы поиска

Refer to curriculum topic: 5.1.2

Пароли взламываются с помощью таблиц с возможными вариантами паролей.

## Вопрос 32

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?

☐ анализ потерь

☐ количественный анализ

☐ анализ степени уязвимости к угрозам

Верно!

☒ 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 33

2 / 2 балла (-ов)

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

Верно!

- ☒ многоуровневый подход
- ☐ ограничение
- ☐ сокрытие информации
- ☐ разнообразие

Refer to curriculum topic: 6.2.2

Многоуровневая защита подразумевает несколько уровней безопасности.

### Вопрос 34

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?

- ☐ доступность ресурсов

то правильный ответ

стандартизация ресурсов

☐ классификация ресурсов

Ваш ответ

☒ идентификация 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)

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

Верно!

☒ ожидаемый ущерб в результате реализации единичной угрозы

Верно!

☒ количество реализаций угрозы в год

☐ мера уязвимости ресурса к угрозе

☐ ценность ресурса

☐ количественная величина убытков

☐ коэффициент частоты

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 36

2 / 2 балла (-ов)

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

☐ бесперебойное обслуживание

☒ отказоустойчивость системы

☐ единая точка отказа

☐ отказоустойчивость

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 37

2 / 2 балла (-ов)

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

☐ многоуровневый подход

Верно!

☒ ограничение

☐ упрощение

☐ сокрытие информации

Refer to curriculum topic: 6.2.2

Обеспечение доступности систем и данных составляет особо важную обязанность специалиста по кибербезопасности. Важно понимать технологии, процессы и средства контроля, с помощью которых обеспечивается высокая доступность.

### Вопрос 38

2 / 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

☐ качественный анализ

☐ анализ потерь

Верно!

☒ 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 39

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!

- ☒ повышение надежности и эксплуатационной готовности серверов
- ☐ повышение надежности шифрования
- ☐ 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 40

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!

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



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 41

2 / 2 балла (-ов)

Какие атаки можно предотвратить с помощью взаимной аутентификации?

- ☐ анализ беспроводного трафика
- ☐ беспроводной спам
- ☐ 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 42

2 / 2 балла (-ов)

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

- ☐ WPA
- ☒ SSH

Верно!

☐ 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)

Какой инструмент Windows следует использовать для настройки политики паролей и политики блокировки учетных записей в системе, которая не входит в домен?

☐ Управление компьютером

☐ Журнал безопасности в средстве просмотра событий

☐ Инструмент «Безопасность Active Directory»

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 44

0 / 2 балла (-ов)

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

Ваш ответ

☒ MS Baseliner

☐ SANS Baselining System (SBS)

☐ CVE Baseline Analyzer

то правильный ответ

Microsoft Security Baseline Analyzer

Refer to curriculum topic: 7.1.1

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

## Вопрос 45

2 / 2 балла (-ов)

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

Верно!

☒ STP

☐ WPA2

☐ RIP

☐ ICMP

Верно!

☒ ARP

☐ IP

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 46

2 / 2 балла (-ов)

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

Верно!

☒ WPA2

☐ WEP

☐ WEP2

☐ WPA

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)

Какая из утилит использует протокол ICMP?

☐ DNS

Верно!

☒ ping

☐ NTP

☐ RIP

Refer to curriculum topic: 7.3.1

С помощью протокола ICMP сетевые устройства передают сообщения об ошибках.

## Вопрос 48

2 / 2 балла (-ов)

В компании произошло несколько инцидентов, когда пользователи загружали несанкционированное ПО, использовали запрещенные веб-сайты и личные USB-накопители. ИТ-директор хочет внедрить схему управления угрозами, исходящими от пользователей. Какие три меры могли бы использоваться для управления угрозами? (Выберите три варианта.)

Верно!

☒ Проведение обучения по вопросам безопасности

Верно!

☒ Отключение доступа к CD и USB

☐ Дисциплинарное взыскание

☐ Отслеживание всех действий пользователей

☐ Переход на тонкие клиенты

Верно!

☒ Фильтрация содержимого

Refer to curriculum topic: 8.1.1

Пользователи могут не знать о последствиях своих действий, если им не рассказать о возможных проблемах. Внедрение ряда технических и организационных практик может уменьшить угрозы.

## Вопрос 49

2 / 2 балла (-ов)

Администратор учебного заведения обеспокоен раскрытием информации о студентах в результате взлома системы. Какой закон защищает данные студентов?

☐ Закон о защите детей в Интернете (CIPA)

☐ Закон о преемственности страхования и отчетности в области здравоохранения (HIPPA)

☐ Закон о защите личных сведений детей в Интернете (COPPA)

Верно!

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

Refer to curriculum topic: 8.2.2

Закон о правах семьи на образование и неприкосновенность частной жизни (FERPA) запрещает неправомерное разглашение личных данных об образовании.

## Вопрос 50

2 / 2 балла (-ов)

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

☐ Исполняющие

Верно!

☒ Наблюдающие

Верно!

☒ Создающие

☐ Ищущие

Верно!

☒ Определяющие

☐ Творящие

Refer to curriculum topic: 8.3.1

Должности по информационной безопасности можно отнести к следующим трем категориям:

- определяющие;
- создающие;
- наблюдающие.

Оценка контрольной работы: **92,67** из 100