

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	39 минут(ы)	64,33 из 100

Оценка за эту попытку: **64,33** из 100

Отправлено 6 Май в 16:56

Эта попытка длилась 39 минут(ы).

Вопрос 1

0 / 2 балла (-ов)

Такие технологии, как IoT и GIS, способствуют накоплению огромных объемов данных. Назовите две причины, в силу которых эти технологии увеличивают спрос на специалистов по кибербезопасности. (Выберите два варианта.)

☐ Требуется больше ресурсов для обработки данных.

то правильный ответ

В системах, созданных на основе этих технологий, хранятся персональные данные.

Ваш ответ

☒ Необходим круглосуточный мониторинг.

Ваш ответ

☒ Эти технологии усложняют структуру систем.☐ Требуется больше оборудования.

то правильный ответ

С помощью этих технологий ведется сбор конфиденциальной информации.

Refer to curriculum topic: 1.1.1

Растущая необходимость в надежной защите продиктована характером данных, собираемых с помощью этих технологий.

Вопрос 2

0,67 / 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☐ необходима докторская степень (PhD)

Верно!

☒ высокий спрос на специалистов

Ваш ответ

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

то правильный ответ лужение обществу

Refer to curriculum topic: 1.2.2

Высокий спрос на специалистов по кибербезопасности открывает уникальные карьерные возможности.

Вопрос 3

2 / 2 балла (-ов)

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

- ☐ Программа ISO/IEC 27000
- ☒ Проект Honeynet
- ☐ Infragard
- ☐ База данных общих уязвимостей и рисков (CVE)

Верно!

Refer to curriculum topic: 1.2.2

Системы раннего оповещения **помогают** распознать атаки и могут быть эффективным защитным инструментом в руках специалистов по кибербезопасности.

Вопрос 4

2 / 2 балла (-ов)

Какая из технологий обеспечивает конфиденциальность данных?

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

Верно!

Refer to curriculum topic: 2.2.1

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

Вопрос 5

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?

☐ сети переноса данных вручную

☒ беспроводные сети

☐ проводные сети

☐ виртуальные 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 6

2 / 2 балла (-ов)

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

☒ хранимые данные

☐ обрабатываемые данные

☐ зашифрованные данные

Верно!

☐ 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 7

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?

☐ сети VLAN

☒ VPN

☐ SHS

☐ RAID

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 8

0 / 2 балла (-ов)

Назовите методы, с помощью которых можно внедрить многофакторную аутентификацию.

☒ токены и хеш-суммы

Ваш ответ

☐ системы IDS и IPS

то правильный ответ

ароли и отпечатки пальцев

☐ сети VPN и VLAN

Refer to curriculum topic: 2.2.1

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

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?

Верно!

☒ злоупотребление поисковой оптимизацией

☐ атака путем подделки DNS

☐ угонщик браузеров

☐ спам

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

0 / 2 балла (-ов)

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

Ваш ответ

☒ атака через посредника☐ рассылка спама

то правильный ответ одмена

☐ 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 11

0 / 2 балла (-ов)

Какое из описаний точнее всего соответствует DDoS-атаке?

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

Ваш ответ

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

то правильный ответ злоумышленник формирует ботнет из компьютеров-зомби.

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

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)

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

Верно!

☒ прослушивание

☐ подмена

☐ рассылка спама

☐ 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

0,67 / 2 балла (-ов)

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

☐ Внедрить эффективные межсетевые экраны.

☐ Увеличить число охранников.

Ваш ответ

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

то правильный ответ

Повысить осведомленность сотрудников относительно действующих политик.

Верно!

Не переходить по ссылкам, вызывающим любопытство.

Верно!

Не вводить пароли в окне чата.

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 14

2 / 2 балла (-ов)

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



подмена ОЗУ



внедрение в ОЗУ



переполнение буфера



внедрение SQL-кода

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 15

2 / 2 балла (-ов)

Киберпреступник отправляет ряд специально подготовленных некорректных пакетов на сервер базы данных. Сервер безуспешно пытается обработать пакеты, что приводит к его сбою. Какую атаку реализует киберпреступник?

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

Верно!

Refer to curriculum topic: 3.3.1

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

Вопрос 16

2 / 2 балла (-ов)

В какой ситуации требуются средства обнаружения?

- ☒ в сети организации нужно выявить запрещенную активность
- ☐ необходимо восстановить нормальное состояние систем после проникновения в сеть организации

Верно!

☐ нужно ликвидировать нанесенный организации ущерб

☐ нет возможности привлечь сторожевую собаку, поэтому требуется альтернативный вариант

Refer to curriculum topic: 4.2.7

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

Вопрос 17

0 / 2 балла (-ов)

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

☐ алгоритм Диффи-Хеллмана

☐ RSA

Ваш ответ

☒ ECC

то правильный ответ DES

Refer to curriculum topic: 4.1.4

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

Вопрос 18

0 / 2 балла (-ов)

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

☐ Обязательное разграничение доступа

то правильный ответ избирательный контроль доступа

☐ ACL

Ваш ответ

☒ Контроль доступа на основе ролей

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 19

0 / 2 балла (-ов)

Подразделению ИТ поручили внедрить систему, которая будет контролировать полномочия пользователей в корпоративной сети. Какое решение следует применить в этом случае?

Ваш ответ

☒ аудит входа пользователей в систему

то правильный ответ набор атрибутов, описывающих права доступа пользователя

☐ наблюдение за всеми сотрудниками

☐ устройство считывания отпечатков пальцев

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 20

0 / 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?



общий PSK-ключ, которым шифруются сообщения, адресованные Алисе

Ваш ответ



закрытый ключ Кэрол



открытый ключ Боба

то правильный ответ овый общий PSK-ключ

Refer to curriculum topic: 4.1.2

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

Вопрос 21

2 / 2 балла (-ов)

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



средства обнаружения

Верно!

- ☐ компенсационные средства контроля
- ☒ средства восстановления
- ☐ 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 22**2 / 2 балла (-ов)**

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

- ☐ обфускация данных
- ☐ изменение старшего бита
- ☐ маскирование 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.

Вопрос 23**2 / 2 балла (-ов)**

Что происходит по мере увеличения длины ключа шифрования?

Верно!

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

Refer to curriculum topic: 4.1.4

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

Вопрос 24**0 / 2 балла (-ов)**

Какая технология хеширования подразумевает обмен ключами?

- ☐ добавление соли
- ☐ AES

Ваш ответ

- ☒ MD5

то правильный ответ HMAC

Refer to curriculum topic: 5.1.3

Механизм HMAC отличается от обычного хеширования наличием ключей.

Вопрос 25**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?

Верно!

- ☐ AES
- ☒ SHA-256
- ☐ SHA-1
- ☐ MD5

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 26

1 / 2 балла (-ов)

Технические специалисты проверяют безопасность системы аутентификации, где применяются пароли. Проверив 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.

то правильный ответ } системах применяются различные алгоритмы хеширования.

Верно!

- ☒ В одной системе применяется только хеширование, тогда как в другой системе, помимо хеширования, применяется механизм добавления соли.
- ☐ В одной системе применяется симметричное хеширование, в другой — асимметричное.
- ☐ В обеих системах применяется алгоритм MD5.

Refer to curriculum topic: 5.1.2

Хеширование позволяет обеспечить целостность данных в различных ситуациях.

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?

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

Верно!

Refer to curriculum topic: 5.3.1

Цифровые сертификаты предназначены для защиты участников защищенного информационного обмена.

Вопрос 28

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.)

- ☒ таблицы поиска

Верно!

Верно!☒ реверсивные таблицы поиска☐ таблицы алгоритмов**Верно!**☒ радужные таблицы☐ хеш-суммы паролей☐ неавторизованные точки доступа

Refer to curriculum topic: 5.1.2

Пароли взламываются с помощью таблиц с возможными вариантами паролей.

Вопрос 29**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☐ добавление соли**Верно!**☒ цифровой сертификат

Refer to curriculum topic: 5.2.2

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

Вопрос 30**2 / 2 балла (-ов)**

Какой алгоритм хеширования следует использовать для защиты конфиденциальной несекретной информации?

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

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 31

2 / 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?

- ☐ имя пользователя и пароль Алисы
- ☐ закрытый ключ Боба
- ☐ открытый ключ Боба
- ☒ закрытый ключ Алисы

Верно!

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

2 / 2 балла (-ов)

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

- ☐ принятие риска
- ☐ снижение риска
- ☒ передача 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 33

0 / 2 балла (-ов)

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

☒ количественная величина убытков

☐ ценность ресурса

Ваш ответ

☐ мера уязвимости ресурса к угрозе☐ коэффициент частоты**Верно!**☒ ожидаемый ущерб в результате реализации единичной угрозы

то правильный ответ

оличество реализаций угрозы в год

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 34

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☐ разнообразие☐ ограничение**Верно!**☒ многоуровневый подход

Refer to curriculum topic: 6.2.2

Многоуровневая защита подразумевает несколько уровней безопасности.

Вопрос 35

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!

- ☐ магазины в местном торговом центре
- ☒ Нью-Йоркская фондовая биржа
- ☐ Министерство образования США
- ☐ 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 36

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
- ☐ Архитектура NIST/NICE
- ☒ Национальная база данных общих уязвимостей и рисков (CVE)
- ☐ 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.

Нет ответа

Вопрос 37

0 / 2 балла (-ов)

Риск-менеджер вашей организации представил схему, где уровни угрозы для ключевых ресурсов систем информационной безопасности обозначены тремя цветами. Красный, желтый и зеленый цвета обозначают соответственно высокий, средний и низкий уровень угрозы. Какому виду анализа рисков соответствует такая схема?

☐ количественный анализ

то правильный ответ

качественный 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 38

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 шифрования
- ☐ обеспечение удаленного доступа для тысяч внешних пользователей
- ☒ повышение надежности и эксплуатационной готовности серверов
- ☐ 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.

Вопрос 39**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.

Нет ответа

Вопрос 40**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?

- ☐ идентификация ресурсов
- ☐ доступность ресурсов
- ☐ классификация ресурсов

то правильный ответ тандартизация 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.

Нет ответа

Вопрос 41**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?

- ☐ 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».

Нет ответа

Вопрос 42

0 / 2 балла (-ов)

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

- ☐ CVE Baseline Analyzer
- ☐ MS Baseliner
- ☐ SANS Baselining System (SBS)

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 43

2 / 2 балла (-ов)

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

Верно!

☐ RIP☐ WPA2☒ STP☐ IP☐ ICMP

Верно!

☒ ARP

Refer to curriculum topic: 7.3.1

Ядро современной сетевой инфраструктуры передачи данных составляют сетевые коммутаторы. Сетевые коммутаторы подвержены таким угрозам, как кража, взлом, удаленный доступ и атаки с использованием сетевых протоколов.

Вопрос 44**2 / 2 балла (-ов)**

Какие атаки можно предотвратить с помощью взаимной аутентификации?

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

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 45**2 / 2 балла (-ов)**

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

☐ 802.11q☒ 802.11i☒ WPA☒ WPA2☐ WEP☐ TKIP

Refer to curriculum topic: 7.3.1

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

Верно!**Верно!****Верно!****Нет ответа****Вопрос 46****0 / 2 балла (-ов)**

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

☐ SCP**то правильный ответ** ;SSH☐ WPA☐ 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 47

2 / 2 балла (-ов)

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



количество ложноположительных срабатываний и степень приемлемости



количество ложноотрицательных результатов и количество ложноположительных результатов



степень неприемлемости и количество ложноотрицательных срабатываний



степень приемлемости и количество ложноотрицательных срабатываний

Верно!

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 48

2 / 2 балла (-ов)

Администратор учебного заведения обеспокоен раскрытием информации о студентах в результате взлома системы. Какой закон

защищает данные студентов?



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



Закон о защите детей в Интернете (CIPA)



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 49

2 / 2 балла (-ов)

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



Информация, не защищенная специальными законами



Негеологическая информация о скважинах



Документация правоохранительных органов, попадающая под перечисленные исключения



Общедоступная информация финансовых учреждений

Верно!



Информация, касающаяся национальной безопасности и внешней политики

Верно!

Верно!☒ Конфиденциальная коммерческая информация

Refer to curriculum topic: 8.2.2

Закон о свободе информации (FOIA) предусматривает следующие исключения:

1. Информация, касающаяся национальной безопасности и внешней политики
2. Внутренние правила и практики для сотрудников государственных органов
3. Информация, защищенная специальными законами
4. Конфиденциальная коммерческая информация
5. Сведения, передаваемые внутри органов или между ними и попадающие под адвокатскую тайну (в связи с совещательными процессами, судебными разбирательствами и т. д.)
6. Информация, которая в случае раскрытия может расцениваться как явное незаконное вторжение в личную жизнь
7. Документация правоохранительных органов, попадающая под перечисленные исключения
8. Данные государственных органов, полученные от финансовых учреждений
9. Геологическая и геофизическая информация о скважинах

Вопрос 50**0 / 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?

☐ Инфраструктура как услуга (IaaS)**то правильный ответ** IO как услуга (SaaS)**Ваш ответ**☒ Платформа как услуга (PaaS)☐ Восстановление как услуга (RaaS)

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: **64,33** из 100