

Финальный экзамен Результаты для Irina Naumenko

Оценка за эту попытку: **90** из 100

Отправлено 21 Май в 21:01

Эта попытка длилась 46 минут(ы).

Вопрос 1

2 / 2 балла (-ов)

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

Верно!

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

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 2

2 / 2 балла (-ов)

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

- ☐ хакеры-дилетанты
- ☐ «серые» хакеры
- ☒ «черные» хакеры
- ☐ «белые» хакеры

Верно!

Refer to curriculum topic: 1.2.1

Хакеры определенных категорий похищают информацию с помощью вредоносного ПО.

Вопрос 3

2 / 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 оборудования.

☐ Необходим круглосуточный мониторинг.

Верно!



С помощью этих технологий ведется сбор конфиденциальной информации.

Верно!



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

☐ Требуется больше ресурсов для обработки данных.

☐ Эти технологии усложняют структуру систем.

Refer to curriculum topic: 1.1.1

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

Вопрос 4

2 / 2 балла (-ов)

К какому типу относятся сети, требующие все больше и больше усилий со стороны специалистов по кибербезопасности из-за распространения концепции BYOD?

- ☐ проводные сети
- ☐ виртуальные сети
- ☐ сети переноса данных вручную
- ☒ беспроводные 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 5

2 / 2 балла (-ов)

Какая из технологий обеспечивает конфиденциальность данных?

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

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 6

2 / 2 балла (-ов)

Назовите методы, с помощью которых можно внедрить многофакторную аутентификацию.

- ☐ системы IDS и IPS
- ☒ пароли и отпечатки пальцев
- ☐ токены и хеш-суммы
- ☐ сети VPN и VLAN

Верно!

Refer to curriculum topic: 2.2.1

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

Вопрос 7

2 / 2 балла (-ов)

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

- ☒ ISO/IEC 27000
- ☐ Триада «КЦД»
- ☐ Модель ISO/OSI
- ☐ Архитектура NIST/NICE

Верно!

Refer to curriculum topic: 2.5.1

Специалист по кибербезопасности должен быть знаком с различными стандартами, архитектурами и моделями управления информационной безопасностью.

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?

Верно!

☒ VPN

☐ SHS

☐ сети VLAN

☐ RAID

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 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 10

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

Верно!

☒ DoS-атака

☐ внедрение SQL-кода

☐ атака через посредника

Refer to curriculum topic: 3.3.1

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

Вопрос 11

2 / 2 балла (-ов)

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

Верно!

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

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)

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?

- ☐ вирус
- ☐ фишинг
- ☒ интернет-червь
- ☐ спам

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 13

2 / 2 балла (-ов)

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

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

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.

- ☐ троян
- ☐ DoS-атака
- ☒ программа-вымогатель
- ☐ атака через посредника

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 15

0 / 2 балла (-ов)

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

то правильный ответ подмена

☐ рассылка спама

Ваш ответ

☒ 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 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

☐ закрытый ключ Боба

☐ открытый ключ Алисы

☐ 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)

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

Верно!

☒ AES

☐ RSA

☐ 3DES

☐ DES

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)

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?

☐ обфускация программного обеспечения

☐ стеганография

Верно!

☒ замена данных путем маскирования

☐ стегоанализ

Refer to curriculum topic: 4.3.1

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

Вопрос 19

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 20

2 / 2 балла (-ов)

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

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

Верно!

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 21

2 / 2 балла (-ов)

В какой ситуации требуются средства обнаружения?

- ☐ нужно ликвидировать нанесенный организации ущерб
- ☐ необходимо восстановить нормальное состояние систем после проникновения в сеть организации
- ☒ в сети организации нужно выявить запрещенную активность
- ☐ нет возможности привлечь сторожевую собаку, поэтому требуется альтернативный вариант

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 22

2 / 2 балла (-ов)

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

☐ алгоритм Диффи-Хеллмана

☐ RSA

☐ ECC

Верно!

☒ 3DES

Refer to curriculum topic: 4.1.4

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

Вопрос 23

2 / 2 балла (-ов)

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

☐ превентивные

Верно!

☒ корректирующие

☐ распознавательные

☐ компенсирующие

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 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

☐ симметричное шифрование

☐ асимметричное шифрование

Refer to curriculum topic: 5.3.1

Цифровые сертификаты предназначены для защиты участников защищенного информационного обмена.

Вопрос 25

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?

Верно!

- ☒ цифровой сертификат
- ☐ цифровая подпись
- ☐ асимметричное шифрование
- ☐ добавление соли

Refer to curriculum topic: 5.2.2

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

Вопрос 26

2 / 2 балла (-ов)

Какая технология хеширования подразумевает обмен ключами?

Верно!

- ☐ AES
- ☒ HMAC
- ☐ добавление соли
- ☐ MD5

Refer to curriculum topic: 5.1.3

Механизм HMAC отличается от обычного хеширования наличием ключей.

Вопрос 27

0 / 2 балла (-ов)

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



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



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

то правильный ответ

правило проверки ввода, гарантирующее полноту, точность и непротиворечивость данных

Ваш ответ



средства контроля ввода, допускающие лишь просмотр текущих данных

Refer to curriculum topic: 5.4.2

Целостность данных обеспечивается путем их проверки.

Вопрос 28

0 / 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?

то правильный ответ

цифровые сертификаты



операции хеширования

☐ правила проверки данных

Ваш ответ

☒ сети VPN и сервисы шифрования

Refer to curriculum topic: 5.3.2

Цифровые сертификаты предназначены для защиты участников защищенного информационного обмена.

Вопрос 29

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?

то правильный ответ

закрытый ключ Алисы

Ваш ответ

☒ закрытый ключ Боба

☐ имя пользователя и пароль Алисы

☐ открытый ключ Боба

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 30

0 / 2 балла (-ов)

Назовите главную особенность криптографической хеш-функции.



По выходному значению хеш-функции можно вычислить входное значение.

то правильный ответ

Хеш-функция необратима.

Ваш ответ



Выходные значения имеют различную длину.



Для хеширования необходимы открытый и закрытый ключи.

Refer to curriculum topic: 5.1.1

Целостность данных является одним из трех руководящих принципов обеспечения информационной безопасности.

Специалист по обеспечению кибербезопасности должен быть знаком со средствами и технологиями, предназначенными для обеспечения целостности данных.

Вопрос 31

2 / 2 балла (-ов)

Вам поручили разъяснить суть механизма проверки данных сотрудникам отдела дебиторской задолженности, выполняющим ввод данных. Выберите наилучший пример для иллюстрации типов данных «строка», «целое число», «десятичная дробь».

Верно!



женщина, 9866, 125,50 \$



мужчина, 25,25 \$, ветеран



800-900-4560, 4040-2020-8978-0090, 21.01.2013



да/нет 345-60-8745, TRF562

Refer to curriculum topic: 5.4.2

Строка — это набор букв, цифр и специальных символов. Целое число — это число без дробной части. Десятичная дробь — это дробное число в десятичной форме.

Вопрос 32

2 / 2 балла (-ов)

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

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

Верно!

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)

В организации намерены ввести систему маркировки, которая будет отражать ценность, конфиденциальность и важность информации. Какой компонент управления рисками рекомендуется в данном случае?

- ☐ доступность ресурсов
- ☒ классификация ресурсов

Верно!

☐ идентификация ресурсов

☐ стандартизация ресурсов

Refer to curriculum topic: 6.2.1

Одна из важнейших составляющих управления рисками — классификация ресурсов.

Вопрос 34

2 / 2 балла (-ов)

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

☐ устранение угроз и принятие

☒ изоляция и восстановление

☒ обнаружение и анализ

☐ конфиденциальность и ликвидация

☐ предотвращение и изоляция

☐ анализ рисков и высокая доступность

Верно!

Верно!

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 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!

- ☒ Национальная база данных общих уязвимостей и рисков (CVE)
- ☐ Модель ISO/IEC 27000
- ☐ Infragard
- ☐ 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 36

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
- ☐ анализ потерь
- ☐ качественный анализ

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 37

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?

- ☐ доступность ресурсов
- ☐ классификация ресурсов
- ☐ идентификация ресурсов
- ☒ стандартизация 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 38

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?

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

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 39

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 40

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

☐ количественная величина убытков

☐ ценность ресурса

☐ 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 41

2 / 2 балла (-ов)

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

Верно!

☐ SCP

☒ SSH

☐ Telnet

☐ WPA

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 42

2 / 2 балла (-ов)

Какая из утилит использует протокол ICMP?

Верно!

☒ ping

☐ DNS

☐ RIP

☐ NTP

Refer to curriculum topic: 7.3.1

С помощью протокола ICMP сетевые устройства передают сообщения об ошибках.

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
- ☐ Инструмент «Безопасность Active Directory»
- ☐ 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 44

2 / 2 балла (-ов)

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

- ☐ ICMP
- ☐ WPA2
- ☐ IP
- ☒ ARP
- ☐ RIP
- ☒ STP

Верно!

Верно!

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 45

2 / 2 балла (-ов)

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

☐ SSH

☐ ARP

Верно!

☒ шифрование голосового трафика

☐ сильная аутентификация

Refer to curriculum topic: 7.3.2

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

Вопрос 46

2 / 2 балла (-ов)

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

☐ WEP

Верно!

☒ WPA

Верно!

☒ WPA2

☐ TKIP

Верно!

☒ 802.11i

☐ 802.11q

Refer to curriculum topic: 7.3.1

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

Вопрос 47

2 / 2 балла (-ов)

Какие атаки можно предотвратить с помощью взаимной аутентификации?

☐ беспроводной спам

☐ анализ беспроводного трафика

Верно!

☒ атака через посредника

☐ подмена IP-адреса отправителя в беспроводных сетях

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)

В рамках кадровой политики компании физическое лицо может отказаться предоставлять информацию любой третьей стороне, кроме работодателя. Какой закон защищает конфиденциальность предоставленной личной информации?

Верно!

☒ Закон Грэmma — Лича — Блайли (GLBA)

☐

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

☐

Стандарт безопасности данных индустрии платежных карт (PCI)

☐

Закон Сарбейнса — Оксли (SOX)

Refer to curriculum topic: 8.2.2

Закон Грэmma — Лича — Блайли (GLBA) включает положения о конфиденциальности для отдельных лиц и способы ограничения предоставления информации сторонним организациям.

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?

☐

Платформа как услуга (PaaS)

☐

Восстановление как услуга (RaaS)

☐

Инфраструктура как услуга (IaaS)

Верно!

☒ ПО как услуга (SaaS)

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)

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

☐ социальная инженерия

Верно!

☒ потеря данных

☐ Перебои питания

Верно!

☒ несанкционированный доступ

Refer to curriculum topic: 8.1.7

Угрозы для приложений могут включать:

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

Оценка контрольной работы: **90** из 100