Финальный экзамен Результаты для Irina Naumenko

Оценка за эту попытку: **20** из 100
Отправлено 21 Май в 16:21
Эта попытка длилась 60 минут(ы).

Вопрос 1

2 / 2 балла (-ов)

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

- хакеры-дилетанты
- «белые» хакеры
- «черные» хакеры

Верно!

- «серые» хакеры

Refer to curriculum topic: 1.2.1
Хакеры определенных категорий похищают информацию с помощью вредоносного ПО.

Вопрос 2

2 / 2 балла (-ов)

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

- «черные» хакеры
- хактивисты
- кибермастера
- непрофессионалы
- доверенные партнеры

Верно!

Верно!

- [x] бывшие сотрудники

Refer to curriculum topic: 1.4.1
Угрозы делятся на внешние и внутренние. Специалист по кибербезопасности должен иметь ясное представление о возможных источниках угроз.

Нет ответа

Вопрос 3

0 / 2 балла (-ов)

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

то правильный ответ

- [ ] С помощью этих технологий ведется сбор конфиденциальной информации.
- [ ] Эти технологии усложняют структуру систем.
- [ ] Необходим круглосуточный мониторинг.
- [ ] Требуется больше ресурсов для обработки данных.

то правильный ответ

- [ ] В системах, созданных на основе этих технологий, хранятся персональные данные.
- [ ] Требуется больше оборудования.

Refer to curriculum topic: 1.1.1
Растущая необходимость в надежной защите продиктована характером данных, собираемых с помощью этих технологий.

Нет ответа

Вопрос 4

0 / 2 балла (-ов)

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

- расшифрованные данные
- зашифрованные данные
- удаленные данные
- обрабатываемые данные

то правильный ответ

- передаваемые данные

то правильный ответ

- хранимые данные

то правильный ответ

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.

Нет ответа

Вопрос 5

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.

- VPN
- сеть хранения данных (SAN)
- NAC

то правильный ответ

NAS

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 6

2 / 2 балла (-ов)

Какая из технологий обеспечивает конфиденциальность данных?

Верно!

- шифрование
- хэширование
- управление идентификационными данными
- RAID

Refer to curriculum topic: 2.2.1
Специалист по обеспечению кибербезопасности должен быть хорошо знаком с технологиями, реализующими конфиденциальность, целостность и доступность данных.

Нет ответа

Вопрос 7

0 / 2 балла (-ов)

Какую технологию идентификации можно использовать в составе системы аутентификации сотрудников?

то правильный ответ

- считывание смарт-карт
- виртуальный отпечаток пальца

тамбур-шлюз

Хеширование SHA-1

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)

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
- шифрование, аутентификация, идентификация
- секретность, идентификация, невозможность отказа
- технологии, политики, осведомленность

Refer to curriculum topic: 2.1.1
Конфиденциальность, целостность и доступность берутся за основу при разработке всех систем управления.

Вопрос 9

2 / 2 балла (-ов)

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

Верно!

- [x] Установка и своевременное обновление антивирусного ПО.
- [ ] Применение RAID.
- [ ] Внедрение сети VPN.
- [ ] Внедрение межсетевых экранов.
- [ ] Применение надежных паролей.

Верно!

- [x] Своевременное обновление операционной системы и остального программного обеспечения.

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 10

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.

- ( ) DoS-атака
- ( ) атака через посредника
- ( ) троян

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.

Нет ответа

Вопрос 11

0 / 2 балла (-ов)

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

- атака через посредника
- то правильный ответ социальная инженерия
- фарминг
- программа-вымогатель

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 мошеннические веб-сайты размещаются на высоких позициях в списках результатов веб-поиска?

- атака путем подделки DNS
- Верно! злоупотребление поисковой оптимизацией
- 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 13

0 / 2 балла (-ов)

Какое из описаний точнее всего соответствует DDoS-атаке?

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

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.

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.

Нет ответа

Вопрос 14

0 / 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?

- близкие отношения
- срочность
- то правильный ответ принуждение
- доверенные партнеры

Refer to curriculum topic: 3.2.1
Методы социальной инженерии включают несколько различных тактик для получения информации от жертв.

Вопрос 15

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.
- Проверить, нет ли учетных записей без паролей.
- Верно! Проверить системы на наличие неавторизованных учетных записей.
- Проверить системы на наличие вирусов.

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)

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)

Что происходит по мере увеличения длины ключа шифрования?

- ( ) Пространство ключей пропорционально увеличивается.
- ( ) Пространство ключей экспоненциально уменьшается.
- ( ) Пространство ключей пропорционально уменьшается.

Верно!

- (•) 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.

Нет ответа

Вопрос 18

0 / 2 балла (-ов)

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

- ( ) аудит входа пользователей в систему
- ( ) наблюдение за всеми сотрудниками
- ( ) устройство считывания отпечатков пальцев

то правильный ответ

- набор атрибутов, описывающих права доступа пользователя

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.

Нет ответа

Вопрос 19

0 / 2 балла (-ов)

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

RSA

алгоритм Диффи-Хеллмана

ECC

то правильный ответ 3DES

Refer to curriculum topic: 4.1.4
Шифрование — важная технология, предназначенная для защиты конфиденциальности данных. Важно понимать особенности различных методов шифрования.

Нет ответа

Вопрос 20

0 / 2 балла (-ов)

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

авторизация

идентификация

то правильный ответ аутентификация

доступ

Refer to curriculum topic: 4.2.4
Для усиления систем контроля доступа применяются различные методы аутентификации. Нужно понимать особенности каждого из этих методов.

Нет ответа

Вопрос 21

0 / 2 балла (-ов)

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

- технологические
- то правильный ответ логические
- физические
- 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.

Нет ответа

Вопрос 22

0 / 2 балла (-ов)

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

- компенсирующие
- распознавательные
- превентивные
- то правильный ответ 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.

Нет ответа

Вопрос 23

0 / 2 балла (-ов)

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

то правильный ответ

- AES
- 3DES
- DES
- RSA

Refer to curriculum topic: 4.1.4
Шифрование — важная технология, предназначенная для защиты конфиденциальности данных. Важно понимать особенности различных методов шифрования.

Нет ответа

Вопрос 24

0 / 2 балла (-ов)

Какой алгоритм хеширования следует использовать для защиты конфиденциальной несекретной информации?

- AES-256
- MD5

3DES

то правильный ответ SHA-256

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.

Нет ответа

Вопрос 25

0 / 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.)

неавторизованные точки доступа

таблицы алгоритмов

то правильный ответ реверсивные таблицы поиска

то правильный ответ таблицы поиска

хеш-суммы паролей

то правильный ответ радужные таблицы

Refer to curriculum topic: 5.1.2
Пароли взламываются с помощью таблиц с возможными вариантами паролей.

Нет ответа

Вопрос 26

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?

- MD5
- то правильный ответ HMAC
- AES
- радужные таблицы

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.

Нет ответа

Вопрос 27

0 / 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.

- добавление соли
- CRC
- пароль
- то правильный ответ HMAC

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.

Нет ответа

Вопрос 28

0 / 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?

то правильный ответ

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

Refer to curriculum topic: 5.3.1
Цифровые сертификаты предназначены для защиты участников защищенного информационного обмена.

Нет ответа

Вопрос 29

0 / 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?

- цифровая подпись

добавление соли

то правильный ответ цифровой сертификат

асимметричное шифрование

Refer to curriculum topic: 5.2.2
Шифрование — важная технология, предназначенная для защиты конфиденциальности данных. Важно понимать особенности различных методов шифрования.

Нет ответа

Вопрос 30

0 / 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.)

то правильный ответ В системах применяются различные алгоритмы хеширования.

Обе системы шифруют пароли перед хешированием.

В одной системе применяется симметричное хеширование, в другой — асимметричное.

то правильный ответ

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

В обеих системах применяется алгоритм MD5.

Refer to curriculum topic: 5.1.2
Хеширование позволяет обеспечить целостность данных в различных ситуациях.

Нет ответа

Вопрос 31

0 / 2 балла (-ов)

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

- ссылочная целостность
- доменная целостность
- Определяемая пользователем целостность

то правильный ответ сущностная целостность

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.

Нет ответа

Вопрос 32

0 / 2 балла (-ов)

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

- ограничение

то правильный ответ многоуровневый подход

разнообразие

сокрытие информации

Refer to curriculum topic: 6.2.2
Многоуровневая защита подразумевает несколько уровней безопасности.

Нет ответа

Вопрос 33

0 / 2 балла (-ов)

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

то правильный ответ обнаружение и анализ

анализ рисков и высокая доступность

устранение угроз и принятие

предотвращение и изоляция

то правильный ответ изоляция и восстановление

конфиденциальность и ликвидация

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.

Нет ответа

Вопрос 34

0 / 2 балла (-ов)

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

упрощение

многоуровневый подход

сокрытие информации

то правильный ответ ограничение

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.

Нет ответа

Вопрос 35

0 / 2 балла (-ов)

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

мера уязвимости ресурса к угрозе

то правильный ответ количество реализаций угрозы в год

коэффициент частоты

то правильный ответ ожидаемый ущерб в результате реализации единичной угрозы

ценность ресурса

количественная величина убытков

Refer to curriculum topic: 6.2.1
При количественном анализе рисков используются следующие величины: ожидаемый ущерб в результате реализации единичной угрозы; количество реализаций угрозы в годовом исчислении; ожидаемый объем убытков в годовом исчислении.

Нет ответа

Вопрос 36

0 / 2 балла (-ов)

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

- бесперебойное обслуживание
- единая точка отказа

то правильный ответ

- отказоустойчивость системы
- 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.

Нет ответа

Вопрос 37

0 / 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

то правильный ответ

- количественный анализ
- качественный анализ
- анализ потерь

Refer to curriculum topic: 6.2.1
Качественный или количественный анализ рисков используется для определения угроз организации и распределения их по приоритетам.

Нет ответа

Вопрос 38

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?

то правильный ответ

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

Refer to curriculum topic: 6.2.1
Качественный или количественный анализ рисков используется для определения угроз организации и распределения их по приоритетам.

Нет ответа

Вопрос 39

0 / 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?

то правильный ответ

- классификация ресурсов

доступность ресурсов

стандартизация ресурсов

идентификация ресурсов

Refer to curriculum topic: 6.2.1
Одна из важнейших составляющих управления рисками — классификация ресурсов.

Нет ответа

Вопрос 40

0 / 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?

офис спортивной команды высшей лиги

то правильный ответ Нью-Йоркская фондовая биржа

Министерство образования США

магазины в местном торговом центре

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.

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»
- то правильный ответ Оснастка «Локальная политика безопасности»
- Управление компьютером
- Журнал безопасности в средстве просмотра событий

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)

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

- то правильный ответ 802.11i
- 802.11q
- TKIP
- то правильный ответ WPA2
- то правильный ответ WPA
- WEP

Refer to curriculum topic: 7.3.1
Защищенную систему связи можно организовать с помощью различных протоколов. Алгоритм AES является наиболее стойким алгоритмом шифрования.

Нет ответа

Вопрос 43

0 / 2 балла (-ов)

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

- WPA
- Telnet
- SCP

то правильный ответ SSH

Refer to curriculum topic: 7.2.1
Для организации обмена данными между системами используются различные протоколы уровня приложений. Защищенный протокол позволяет установить защищенное соединение в незащищенной сети.

Нет ответа

Вопрос 44

0 / 2 балла (-ов)

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

то правильный ответ шифрование голосового трафика

- SSH

сильная аутентификация

ARP

Refer to curriculum topic: 7.3.2
Многие передовые технологии, включая VoIP, передачу потокового видео и конференц-связь, требуют соответствующих мер безопасности.

Нет ответа

Вопрос 45

0 / 2 балла (-ов)

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

то правильный ответ

количество ложноотрицательных результатов и количество ложноположительных результатов

степень неприемлемости и количество ложноотрицательных срабатываний

степень приемлемости и количество ложноотрицательных срабатываний

количество ложноположительных срабатываний и степень приемлемости

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.

Нет ответа

Вопрос 46

0 / 2 балла (-ов)

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

- [ ] RIP
- [x] ARP
- [ ] ICMP
- [ ] WPA2
- [x] STP
- [ ] IP

то правильный ответ

то правильный ответ

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.

Нет ответа

Вопрос 47

0 / 2 балла (-ов)

Какая из утилит использует протокол ICMP?

- [ ] DNS
- [x] ping
- [ ] RIP
- [ ] NTP

то правильный ответ

Refer to curriculum topic: 7.3.1
С помощью протокола ICMP сетевые устройства передают сообщения об ошибках.

Нет ответа

Вопрос 48

0 / 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 защите личных сведений детей в Интернете (COPPA)

то правильный ответ

- Закон о правах семьи на образование и неприкосновенность частной жизни (FERPA)
- Закон о преемственности страхования и отчетности в области здравоохранения (HIPPA)

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.

Нет ответа

Вопрос 49

0 / 2 балла (-ов)

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

- Исполняющие

то правильный ответ Наблюдающие

Творящие

то правильный ответ Определяющие

Ищущие

то правильный ответ Создающие

Refer to curriculum topic: 8.3.1
Должности по информационной безопасности можно отнести к следующим трем категориям:

- определяющие;
- создающие;
- наблюдающие.

Нет ответа

Вопрос 50

0 / 2 балла (-ов)

Какие три услуги предоставляют CERT? (Выберите три варианта.)

то правильный ответ Устранения уязвимостей программного обеспечения

Разработка инструментов атаки

Соблюдение стандартов программного обеспечения

то правильный ответ

Разработка инструментов, продуктов и методик для анализа уязвимостей

Создание инструментов для разработки вредоносного ПО

то правильный ответ

Разработка инструментов, продуктов и методик технической экспертизы

Refer to curriculum topic: 8.2.3
Услуги CERT включают:

- помощь в устранении уязвимостей ПО;
- разработку инструментов, продуктов и методик для технической экспертизы;
- разработку инструментов, продуктов и методик для анализа уязвимостей;
- разработку инструментов, продуктов и методик для мониторинга крупных сетей;
- помощь организациям в оценке эффективности методов, используемых ими для обеспечения безопасности.

Оценка контрольной работы: **20** из 100