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	33 минут(ы)	90,67 из 100

Оценка за эту попытку: **90,67** из 100
Отправлено 22 Май в 18:08
Эта попытка длилась 33 минут(ы).

Вопрос 1 **0 / 2 балла (-ов)**

Специалисту по кибербезопасности поручили выявить потенциальных преступников, организовавших атаку на организацию. Какая категория хакеров должна меньше всего интересовать специалиста в такой ситуации?

то правильный ответ «белые» хакеры

«черные» хакеры

Ваш ответ хакеры-дилетанты

«серые» хакеры

Refer to curriculum topic: 1.2.1
Категории хакеров обозначены цветами, которые соответствуют целям предпринимаемых атак.

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.)

Ваш ответ

- [x] сертификация CompTIA A+ обеспечивает достаточный уровень знаний для начала карьеры
- [ ] необходима докторская степень (PhD)

Верно!

- [x] высокий доход

Верно!

- [x] высокий спрос на специалистов

то правильный ответ

- [ ] служение обществу
- [ ] должность, подразумевающая рутинную повседневную работу

Refer to curriculum topic: 1.2.2
Высокий спрос на специалистов по кибербезопасности открывает уникальные карьерные возможности.

Вопрос 3

2 / 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.)

- [ ] Необходим круглосуточный мониторинг.

Верно!

- [x] В системах, созданных на основе этих технологий, хранятся персональные данные.

Верно!

- [x] С помощью этих технологий ведется сбор конфиденциальной информации.

- [ ] Эти технологии усложняют структуру систем.
- [ ] Требуется больше ресурсов для обработки данных.
- [ ] Требуется больше оборудования.

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)

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
- ( ) сети VLAN
- ( ) SHS

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 5

2 / 2 балла (-ов)

Какую технологию идентификации можно использовать в составе системы аутентификации сотрудников?

тамбур-шлюз

Верно!

считывание смарт-карт

виртуальный отпечаток пальца

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 6

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

сети переноса данных вручную

виртуальные сети

Верно!

беспроводные сети

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 7

2 / 2 балла (-ов)

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

обрабатываемые данные

передаваемые данные

Верно!

хранимые данные

зашифрованные 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 8

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.

Вопрос 9

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

Верно!

- (•) интернет-червь
- ( ) спам

Refer to curriculum topic: 3.1.1
Специалист по обеспечению кибербезопасности должен быть знаком с особенностями разных видов вредоносного ПО и атак, которые угрожают организации.

Вопрос 10

2 / 2 балла (-ов)

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

- рассылка спама
- подмена
- фишинг
- 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 11

2 / 2 балла (-ов)

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

- прослушивание
- атака через посредника
- подмена
- рассылка спама

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 12

0 / 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, нет ли учетных записей без паролей.
- Проверить системы на наличие вирусов. — Ваш ответ
- Проверить системы на наличие неавторизованных учетных записей. — то правильный ответ
- Проверить в журнале событий, не было ли изменений в политике.

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)

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

- социальная инженерия — Верно!
- 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 14

2 / 2 балла (-ов)

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

Верно!

- (•) переполнение буфера
- ( ) внедрение в ОЗУ
- ( ) подмена ОЗУ
- ( ) внедрение SQL-кода

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
- ( ) атака через посредника

Верно!

- DoS-атака
- внедрение SQL-кода

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)

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

- компенсирующие

Верно!

- корректирующие
- распознавательные
- превентивные

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

2 / 2 балла (-ов)

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

авторизация

доступ

идентификация

Верно!

аутентификация

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

Вопрос 18

2 / 2 балла (-ов)

Назовите компонент, представляющий наибольшую сложность при разработке криптосистемы.

Верно!

управление ключами

алгоритм шифрования

обратная разработка

длина ключа

Refer to curriculum topic: 4.1.1
Шифрование — важная технология, предназначенная для защиты конфиденциальности данных. Важно понимать особенности различных методов шифрования.

Вопрос 19

2 / 2 балла (-ов)

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

Верно!

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

Refer to curriculum topic: 4.2.5
Контроль доступа препятствует получению доступа неавторизованным пользователем к конфиденциальным данным и сетевым системам. Существует несколько технологий, с помощью которых реализуются эффективные стратегии контроля доступа.

Вопрос 20

2 / 2 балла (-ов)

Что происходит по мере увеличения длины ключа шифрования?

- ( ) Пространство ключей пропорционально уменьшается.

Верно!

- (•) Пространство ключей экспоненциально увеличивается.
- ( ) Пространство ключей пропорционально увеличивается.
- ( ) 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 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
- нет возможности привлечь сторожевую собаку, поэтому требуется альтернативный вариант

Верно!

- в сети организации нужно выявить запрещенную активность

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)

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

- административные
- физические
- технологические

Верно!

- логические

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 23

2 / 2 балла (-ов)

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

- ECC
- RSA
- алгоритм Диффи-Хеллмана
- 3DES

Верно!

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

Вопрос 24

2 / 2 балла (-ов)

Вам поручили внедрить систему обеспечения целостности данных для защиты файлов, загружаемых сотрудниками отдела продаж. Вы намерены применить самый стойкий из всех алгоритмов хеширования, имеющихся в системах вашей организации. Какой алгоритм хеширования вы выберете?

SHA-1

MD5

Верно!

SHA-256

AES

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 25

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

симметричное шифрование

асимметричное шифрование

Верно!

цифровые сертификаты

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

Вопрос 26

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 алгоритмов
- [ ] неавторизованные точки доступа
- [ ] хеш-суммы паролей
- [x] радужные таблицы — Верно!
- [x] таблицы поиска — Верно!
- [x] реверсивные таблицы поиска — Верно!

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

Вопрос 27

2 / 2 балла (-ов)

Назовите главную особенность криптографической хеш-функции.

- (•) Хеш-функция необратима. — Верно!
- ( ) Выходные значения имеют различную длину.
- ( ) По выходному значению хеш-функции можно вычислить входное значение.
- ( ) 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 28

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?

Верно!

- (•) цифровые сертификаты
- ( ) сети VPN и сервисы шифрования
- ( ) операции хеширования
- ( ) правила проверки данных

Refer to curriculum topic: 5.3.2
Цифровые сертификаты предназначены для защиты участников защищенного информационного обмена.

Вопрос 29

2 / 2 балла (-ов)

К какой технологии обеспечения безопасности относится стандарт X.509?

- ( ) надежные пароли
- ( ) токены безопасности

Верно!

- (•) цифровые сертификаты
- ( ) технология биометрической идентификации

Refer to curriculum topic: 5.3.2
С помощью цифровых сертификатов обеспечивается безопасность сторон защищенного соединения.

Вопрос 30

2 / 2 балла (-ов)

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

- ( ) шифрование данных, благодаря которому доступ к конфиденциальным данным имеют только авторизованные пользователи
- ( ) средства контроля ввода, допускающие лишь просмотр текущих данных
- ( ) ограничение, согласно которому ввод конфиденциальных данных могут выполнять только авторизованные сотрудники

Верно!

- (•) правило проверки ввода, гарантирующее полноту, точность и непротиворечивость данных

Refer to curriculum topic: 5.4.2
Целостность данных обеспечивается путем их проверки.

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».

- да/нет 345-60-8745, TRF562
- мужчина, 25,25 $, ветеран
- Верно! женщина, 9866, 125,50 $
- 800-900-4560, 4040-2020-8978-0090, 21.01.2013

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

0 / 2 балла (-ов)

К какой категории методов аварийного восстановления относится размещение резервных копий на удаленной площадке?

- корректирующие
- Ваш ответ административные
- распознавательные
- то правильный ответ превентивные

Refer to curriculum topic: 6.4.1
План аварийного восстановления помогает подготовить организацию к потенциальным аварийным ситуациям и минимизировать время простоя.

Вопрос 33

2 / 2 балла (-ов)

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

Верно!

- (•) отказоустойчивость системы
- ( ) отказоустойчивость
- ( ) бесперебойное обслуживание
- ( ) единая точка отказа

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 34

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.

- ( ) Infragard

Верно!

- (•) Национальная база данных общих уязвимостей и рисков (CVE)
- ( ) Архитектура NIST/NICE
- ( ) 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 35

2 / 2 балла (-ов)

Какую технологию следует внедрить, чтобы обеспечить высокую доступность систем хранения данных?

- ( ) N+1
- ( ) обновление ПО
- ( ) горячий резерв

Верно!

- (•) RAID

Refer to curriculum topic: 6.2.3
Обеспечение доступности систем и данных составляет особо важную обязанность специалиста по кибербезопасности. Необходимо иметь ясное представление о технологиях, процессах и средствах контроля, обеспечивающих резервирование.

Вопрос 36

0 / 2 балла (-ов)

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

- сокрытие информации
- то правильный ответ ограничение
- Ваш ответ многоуровневый подход
- упрощение

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 37

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
- обеспечение удаленного доступа для тысяч внешних пользователей
- 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 38

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?

Верно!

- (•) стандартизация ресурсов
- ( ) классификация ресурсов
- ( ) доступность ресурсов
- ( ) 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 39

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
- анализ степени уязвимости к угрозам
- количественный анализ

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 40

2 / 2 балла (-ов)

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

Верно!

- передача риска
- уклонение от риска
- снижение риска
- принятие риска

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 41

2 / 2 балла (-ов)

Какая из утилит использует протокол ICMP?

- NTP
- DNS
- Верно! ping
- RIP

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

Вопрос 42

2 / 2 балла (-ов)

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

- SCP
- Верно! 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 43

2 / 2 балла (-ов)

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

- [ ] ICMP
- [x] ARP — Верно!
- [ ] WPA2
- [ ] RIP
- [ ] IP
- [x] STP — 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 44

2 / 2 балла (-ов)

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

SSH

сильная аутентификация

Верно!

шифрование голосового трафика

ARP

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

Вопрос 45

2 / 2 балла (-ов)

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

Верно!

WPA2

WEP

WPA

WEP2

Refer to curriculum topic: 7.1.2
Безопасность беспроводных сетей определяется соответствующими стандартами, которые постепенно становятся все более и более надежными. На смену WEP пришел стандарт WPA, который уступил место WPA2.

Вопрос 46

2 / 2 балла (-ов)

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

- количество ложноположительных срабатываний и степень приемлемости
- степень неприемлемости и количество ложноотрицательных срабатываний
- степень приемлемости и количество ложноотрицательных срабатываний

Верно!

- количество ложноотрицательных результатов и количество ложноположительных результатов

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 47

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 48

2 / 2 балла (-ов)

Что можно использовать для балльной оценки серьезности угроз в целях определения важных уязвимостей?

- ACSC
- Центр реагирования на компьютерные инциденты (CERT)
- ISC
- Национальная база данных об уязвимостях (NVD)

Верно!

Refer to curriculum topic: 8.2.3
Национальная база данных об уязвимостях (NVD) используется для оценки серьезности уязвимостей и используется организациями для балльной оценки критичности уязвимостей, обнаруженных в сети.

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)

Верно!

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

Закон о защите личных сведений детей в Интернете (COPPA)

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.

Вопрос 50

2 / 2 балла (-ов)

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

Перебои питания

социальная инженерия

Верно!

потеря данных

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: **90,67** из 100