CISSP

365 ВОПРОСОВ ДЛЯ ПОДГОТОВКИ

РИСКИ, АРХИТЕКТУРА, СЕТИ, ДОСТУП И БЕЗОПАСНОСТЬ

ИТОН БЛЕЙК

Итон Блейк

CISSP. 365 вопросов для подготовки. Риски, архитектура, сети, доступ и безопасность

https://litres.ru/74442659
SelfPub; 2026

Аннотация

Экзамен пугает лишь того, кто надеется на память вместо понимания. Здесь 365 вопросов превращают CISSP из тумана терминов в цепь конкретных решений: риски, архитектура, криптография, сети, IAM, аудит, инциденты и безопасная разработка. Ошибка здесь полезнее самоуверенности: она показывает слабое место до того, как его покажет экзамен. Книга для тех, кто хочет не угадывать ответ, а мыслить как специалист по безопасности.

Содержание

Итон Блейк
CISSP. 365 вопросов для подготовки. Риски, архитектура, сети, доступ и безопасность

Глава 1. Управление безопасностью, рисками и соответствием

Цели информационной безопасности: триада CIA

Какое из следующих утверждений лучше всего описывает конфиденциальность?

A. Как система защищает данные от несанкционированного доступа?

B. Уполномоченный персонал имеет доступ к системе

C. Как система предотвращает разглашение информации?

D. Процесс проверки личности пользователя

Ответ на вопрос дня: 16.02.2019

Какой из следующих аспектов наименее связан с конфиденциальностью информации?

A. Конфиденциальность

B. Целостность

C. Неотказуемость

D. Доступность

Ответ на вопрос дня: 20200526

Какой из следующих атрибутов или целей информационной безопасности НЕ определен в Федеральном законе США об управлении информационной безопасностью 2002 года (FISMA)?

A. Неотказуемость

B. Ответственность

C. Подлинность

D. Доступность

Ответ на вопрос дня: 20200101

Эмили отправила Майклу электронное письмо с юридически значимой цифровой подписью.

Какая из следующих целей безопасности в наибольшей степени соответствует намерению Эмили?

A. Конфиденциальность

B. Целостность

C. Доступность

D. Атрибуция

Ответ на вопрос дня: 20200410

Информационная безопасность — это дисциплина, которая использует средства защиты для предотвращения угроз в отношении активов с целью достижения целей конфиденциальности, целостности и доступности (CIA), поддержки бизнес-процессов, а также создания и предоставления ценности.

Какой из следующих вариантов будет препятствовать или способствовать достижению цели обеспечения безопасности «целостности»?

A. Получатель отрицает получение электронного письма

B. Недовольный сотрудник удалил конфиденциальный файл

C. Посредник отравил DNS

D. Отправитель подписывает электронное письмо с помощью цифровой подписи

Ответ на вопрос дня: 20191201

Управление информационной безопасностью

Как специалисту в области информационной безопасности (CISO), что из перечисленного вам следует освоить в первую очередь?

A. Политика информационной безопасности

B. Программа обеспечения непрерывности бизнеса

C. Стратегия информационной безопасности

D. Потенциал реагирования на инциденты

Ответ на вопрос дня: 20200417

Вы — директор по информационной безопасности (CISO) международной торговой компании. Что из перечисленного является вашей первоочередной задачей?

A. Заработная плата и льготы

B. Роль и обязанности директора по информационным технологиям (R&R)

C. Разработать и внедрить стратегии информационной безопасности

D. Соберите требования бизнеса и безопасности, разработайте планы кибербезопасности и соответствующие политики

Ответ на вопрос дня: 20190501

Вы являетесь руководителем службы информационной безопасности (CISO) многонациональной компании. После анализа миссии, видения, стратегических целей, стратегии компании, а также бизнес-требований и требований безопасности, вы начинаете разработку стратегии информационной безопасности. Что из перечисленного следует внедрить в первую очередь?

A. Определите план и этапы

B. Провести анализ пробелов

C. Учитывайте ресурсы и ограничения

D. Разработайте политику программы информационной безопасности

Ответ на вопрос дня: 22.09.2019

Вы — недавно назначенный руководитель отдела информационной безопасности (CISO), работающий в банке на Тайване, который полностью полагается на онлайн-бизнес.

Что из перечисленного следует сделать в первую очередь?

A. Встретиться и обсудить ситуацию с заинтересованными сторонами

B. Запустить программу информационной безопасности

C. Провести всестороннюю оценку рисков

D. Разработать стратегию кибербезопасности

Ответ на вопрос дня: 20200102

Какой из следующих примеров лучше всего иллюстрирует концепции согласования функций безопасности и политики?

A. Создать должность CISO специально для решения вопросов информационной безопасности

B. Напомнить генеральному директору и совету директоров об обязанности включить кибербезопасность в стратегическую повестку компании

C. Снизить риски до уровня, приемлемого для высшего руководства, для достижения целей CIA

D. Управлять информационной безопасностью с учётом бизнес-задач и создания ценности

Ответ на вопрос дня: 20190908

Вы являетесь директором по информационной безопасности (CISO) компании Northbridge Semiconductors и подчиняетесь непосредственно генеральному директору. В от-

чете говорится, что конфиденциальность клиентов и информация, касающаяся исследований и разработок, имеют для компании первостепенное значение. Следовательно, использование любого USB-устройства является нарушением Политики допустимого использования (AUP).

Менеджер по работе с клиентами сообщил, что многие крупные клиенты жалуются на неэффективность загрузки файлов на файловый сервер компании. Он предложил использовать USB-накопители для передачи данных, что упростило бы процесс совместной работы с клиентами.

Что следует сделать в первую очередь руководителю службы информационной безопасности?

A. Добавьте в AUP пункт об исключении, разрешающий использование USB-накопителей, поскольку безопасность является фактором, способствующим развитию бизнеса. Главная обязанность CISO — помогать компании создавать ценность

B. Предложение было отклонено, поскольку оно нарушало принцип AUP, а риски использования USB-флеш-накопителя были слишком высоки

C. Поддержите менеджера по работе с клиентами и представьте генеральному директору рекомендации, благоприятные для менеджера по работе с клиентами

D. Представьте генеральному директору обоснование целесообразности проекта для принятия окончательного решения

Ответ на вопрос дня: 20190423

Вы назначены на вновь созданную должность директора по информационной безопасности (CISO), ответственного за управление информационной безопасностью. Ранее эту должность неофициально занимал директор по информационным технологиям (CIO). Вы подчиняетесь непосредственно генеральному директору (аналог CIO) и отвечаете за разработку и внедрение стратегий информационной безопасности.

Что из перечисленного ниже наилучшим образом подтверждает рациональность данного соглашения?

A. Разделение обязанностей

B. Избегайте конфликта интересов

C. Стратегия и согласование с бизнесом

D. Правовые или нормативные требования

Ответ на вопрос дня: 20190916

Вы — руководитель отдела информационной безопасности многонациональной компании, участвуете в совещании высшего уровня. Повестка дня — приобретение компании в рамках стратегии роста компании. Генеральный директор

особенно обеспокоен тем, была ли проведена комплексная проверка в рамках этой сделки проведена надлежащая комплексная проверка.

Как CISO, каким способом вы можете наиболее эффективно поддержать это приобретение?

A. Проанализировать соглашение о приобретении и выявить потенциальные договорные риски

B. Провести тестирование безопасности для выявления потенциальных уязвимостей и угроз

C. Обучить сотрудников службы безопасности приобретаемой компании политике безопасности вашей компании

D. Провести комплексную оценку безопасности и выявить пробелы в политике безопасности приобретаемой компании

Ответ на вопрос дня: 15.09.2019

Ваша компания планирует создать новую должность специалиста по информационной безопасности (CISO) для разработки и внедрения стратегий информационной безопасности.

Совет директоров проводит заседание для внесения изменений в устав компании и близок к принятию решения о том, что CISO должна отчитаться перед аудиторским комитетом.

Какой из следующих вариантов обратной связи был бы наиболее подходящим для генерального директора, присут-

ствующего на встрече?

A. Принятие этой резолюции — хорошее решение

B. Рекомендуется, чтобы главный аудитор (CISO) обладал навыками внутреннего аудита

C. Предложите пункты, разделяющие обязанности директора по информационной безопасности и директора по информационным технологиям во избежание конфликтов интересов

D. Это говорит о том, что независимость аудита будет ограничена

Ответ на вопрос дня: 17.09.2019

Ваша компания, зарегистрированная на Тайване, решила начать продажу игрушек и предоставлять услуги доставки по всему миру. Для выхода на рынок США ваша компания... В Соединенных Штатах был открыт филиал.

Модель управления централизована; местным филиалам могут быть делегированы только решения, которые должны соответствовать местным нормативным актам. Политика хранения данных в филиале США отличается от местных нормативных актов.

Какой из следующих вариантов действий будет наилучшим для специалиста по безопасности в филиале?

A. Ознакомиться с местной политикой хранения данных

B. Рекомендовать местному филиалу соблюдать политику головного офиса

C. Потребовать корректирующих мер для соблюдения местных законов и правил

D. Пересмотреть местную политику в соответствии с местным законодательством

Ответ на вопрос дня: 17.10.2019

Ваша компания решила начать продавать игрушки онлайн и отправлять их по всему миру — это стратегический шаг. Вас назначили руководителем программы по развитию электронной коммерции, спонсируемой операционным директором, и вы возглавите внутреннюю команду по разработке системы электронной коммерции для поддержки нового бизнеса.

Что из перечисленного наиболее важно для вашего успеха?

A. Самая компетентная команда

B. Политика, полностью доведённая до участников

C. Осуществимая стратегия

D. Документированный план программы

Ответ на вопрос дня: 20191224

Вы являетесь директором по информационной безопасности (CISO) банка на Тайване, который полностью полагается на онлайн-бизнес. Разработка политики информационной безопасности ведется с целью создания рамочной основы для дальнейшего развития соответствующих вспомогательных политик, а также для рассмотрения целей, масштабов, ролей и обязанностей таких политик.

Что из перечисленного наиболее подходит для включения в сферу действия политики?

A. Уровни конфиденциальности данных

B. Высшее руководство

C. Заинтересованные стороны, на которых распространяется политика

D. Конфиденциальность, целостность и доступность

Ответ на вопрос дня: 20200112

Совет директоров недоволен эффективностью и результативностью инвестиций организации в ИТ. Как специалист по безопасности, вы участвуете в разработке плана по улучшению, направленного на удовлетворение бизнес-требований и требований безопасности, предъявляемых к инвестициям в ИТ.

Какая из следующих управленческих практик является

наиболее эффективной?

A. Провести анализ затрат и выгод

B. Создать корпоративную архитектуру

C. Разработать комплексную политику информационной безопасности

D. Оценить надёжность ИКТ-услуг, продуктов и поставщиков

Ответ на вопрос дня: 20200205

В качестве руководителя отдела информационной безопасности вы подчиняетесь непосредственно генеральному директору и периодически получаете приглашения консультировать совет директоров.

Что из перечисленного ниже наилучшим образом убедило бы генерального директора, совет директоров и других заинтересованных лиц в том, что управление информационной безопасностью является надежным и надлежащим?

A. Политика информационной безопасности

B. Аудит безопасности

C. Оценка рисков

D. Стратегия информационной безопасности

Ответ на вопрос дня: 18.05.2020

Вы являетесь директором по информационной безопасности (CISO) банка на Тайване, который полностью полагается на онлайн-бизнес. Команда разработчиков программного обеспечения создает систему управления взаимоотношениями с клиентами (CRM). Вы разрабатываете политику конфиденциальности данных клиентов.

Какое из следующих действий системы вызывает у вас наибольшее беспокойство?

A. Система отображает политику конфиденциальности и заранее отмечает пункт «Согласен»

B. Система предоставляет ссылку для отказа от маркетинговых рассылок

C. Система запрещает клиентам обновлять личные профили, ссылаясь на принцип ограничения использования

D. Система позволяет клиентам обновлять личные данные онлайн

Ответ на вопрос дня: 20200118

Управление рисками

Согласно стандарту ISO 31000, риск — это «влияние неопределенности на объективную цель». Что из перечисленного является риском?

A. Природное явление

B. Разрушительное событие

C. Ущерб в размере 500 000 долларов

D. Ни один из перечисленных вариантов

Ответ на вопрос дня: 20200527

Что должна определить организация перед проведением анализа рисков?

A. Источники угроз и события, представляющие угрозу

B. Уязвимости / недостатки, которыми можно воспользоваться

C. Любые сомнения, а также влияние или последствия ключевых активов

D. Любой из вышеперечисленных пунктов может быть отдан в приоритетном порядке

Ответ на вопрос дня: 15.10.2019

Будучи руководителем службы информационной безопасности (CISO), вы решаете создать систему управления информационной безопасностью и получить сертификат ISO 27001; одним из требований является принятие мер по устранению рисков и использованию возможностей.

Вы понимаете, что эта потребность связана с управлением рисками, и начинаете оценивать систему управления рисками для удовлетворения этой потребности.

Какой из следующих вариантов наименее вероятно соответствует требованию внедрения плана управления рисками?

A. Стандарт NIST RMF (Структура, Оценка, Реагирование и Мониторинг)

B. ISO 27002

C. ISO 27005

D. ISO 31000

Ответ на вопрос дня: 18.10.2019

Ваша компания решила начать продажу и доставку игрушек по всему миру. Система электронной коммерции, поддерживающая этот новый бизнес, будет разработана собственными силами.

В ходе совещания по моделированию угроз проектная

группа анализирует и расставляет приоритеты рисков.

Какой из следующих методов лучше всего использовать специалисту по безопасности для определения приоритетности рисков?

A. Годовая частота возникновения (ARO)

B. Коэффициент воздействия

C. Анализ влияния на бизнес (BIA)

D. Оценочные финансовые потери

Ответ на вопрос дня: 21.10.2019

Ваша компания решила начать продажу и доставку игрушек по всему миру. Система электронной коммерции, поддерживающая этот новый бизнес, будет разработана собственными силами.

Проектная группа выявила следующие риски:

R001 — Репутация компании может быть подорвана. R002 — Транспортные операции могут быть нарушены. R003 — Злоумышленник может осуществить распределенную атаку типа «отказ в обслуживании» (DDoS).

Как эксперту по безопасности, какой из следующих рисков следует устранить в первую очередь?

A. R001

B. R002

C. R003

D. Ни один из вышеперечисленных вариантов

Ответ на вопрос дня: 20191028

Вы являетесь специалистом по информационной безопасности (CISO) и работаете в банке прямого обслуживания на Тайване, где банковские услуги предоставляются только онлайн.

Синтаксис SQL для обхода аутентификации, введя его в форму входа.

Что из перечисленного лучше всего описывает ваши опасения?

A. Риск воздействия

B. Угроза событию

C. Угроза ситуации (сценарий)

D. Профиль риска

Ответ на вопрос дня: 20200103

Вы являетесь специалистом по информационной безопасности (CISO) и работаете в банке прямого обслуживания на Тайване, где банковские услуги предоставляются только онлайн.

Вы проводите оценку системы мер безопасности для сни-

жения рисков и повышения уровня защиты.

Что из перечисленного наименее вероятно будет включено в систему мер безопасности?

A. Остаточный риск после внедрения мер контроля

B. Аудиторские процедуры или методы оценки

C. Процесс исключения групп мер контроля из базового набора

D. Рекомендации по внедрению мер контроля

Ответ на вопрос дня: 20200113

Вы являетесь специалистом по информационной безопасности (CISO) и работаете в банке прямого обслуживания на Тайване, где банковские услуги предоставляются только онлайн.

Ваш банк рассматривает возможность передачи своей системы управления взаимоотношениями с клиентами (CRM) на аутсорсинг зарубежному разработчику программного обеспечения.

Какие действия должен предпринять ваш банк в первую очередь?

A. Провести анализ сценариев угроз

B. Опишите источники угроз, имеющих отношение к организации

C. Разработайте и выберите события, представляющие угрозу, для анализа

D. Определите применимые меры контроля

Ответ на вопрос дня: 20200120

Ваша организация использует структуру управления рисками NIST RMF для определения, оценки, реагирования и мониторинга рисков, исходящих из различных источников или на разных уровнях (например, информационных систем, бизнес-процессов или самой организации).

Как специалист по информационной безопасности, вы рассматриваете структуры управления с организационной точки зрения для управления рисками.

Что из перечисленного НЕ является для вас основной проблемой?

A. Стратегия разработки информационных продуктов собственными силами или с привлечением поставщиков

B. Стратегия управления рисками

C. Стратегия замены устаревших информационных систем

D. Корпоративная архитектура

Ответ на вопрос дня: 20200127

Вы являетесь менеджером, уполномоченным принимать решение о принятии риска. После устранения риска вы рассматриваете ситуацию, когда затраты на устранение остаточного риска значительно превышают критерии принятия риска.

Хотя количественные экономические выгоды не могут оправдать его целесообразность, вы твердо убеждены, что, хотя вероятность возникновения риска низка и не является неотложной, его влияние на организацию значительно, и поэтому его следует рассмотреть.

Какое из следующих решений лучше всего соответствует принципу принятия риска?

A. Не предпринимать дальнейших действий, поскольку риск не соответствует критерию приемлемости

B. Не предпринимать дальнейших действий, поскольку субъективная оценка ненадёжна

C. По возможности пересмотреть критерии приемлемости риска, чтобы учесть этот риск

D. Внедрить меры управления риском вне обычного плана работ и документировать основания решения

Ответ на вопрос дня: 20200129

Ваша компания решила в следующем году инвестировать в решения для поддержки своих сотрудников отдела продаж,

часто находящихся вне офиса, и для увеличения объёма продаж. В число выбранных решений входят ноутбуки, мобильные телефоны, VPN, беспроводные сети и системы управления взаимоотношениями с клиентами (CRM).

С точки зрения специалиста по информационной безопасности (CISO), вызывает наименьшее беспокойство при разработке стратегии управления рисками?

A. Иностранная собственность, контроль или влияние на поставщиков (FOCI)

B. Инвестиционная стратегия

C. Влияние решения на бизнес-процессы

D. Законы и правила

Ответ на вопрос дня: 20200201

Ваша компания рассматривает решения для увеличения продаж. Менеджер по продажам рекомендует внедрить CRM-систему, обеспечить сотрудников отдела продаж мобильными устройствами и VPN-подключением.

ИТ-менеджер указывает на то, что это решение может привести к утечке персональных данных и значительным финансовым потерям. Как специалист по безопасности, вы оцениваете этот риск.

Какой из следующих методов является наиболее эффективным?

A. Используйте качественный анализ для определения вероятности и последствий риска

B. Проведите количественный анализ для определения вероятности риска и финансовых потерь

C. Определите степень подверженности риску и выявите допустимый уровень риска

D. Проведите анализ влияния на бизнес (Business Impact Analysis, BIA), чтобы определить общее воздействие на организацию

Ответ на вопрос дня: 20200203

Ваша компания рассматривает возможность приобретения новых планшетов для поддержки сотрудников отдела продаж и увеличения объёма продаж.

В качестве старшего менеджера по закупкам вы формируете контекст рисков для управления рисками в цепочке поставок информационно — коммуникационных технологий (ИКТ SCRM).

Что из перечисленного следует рассмотреть в первую очередь?

A. Функции миссии

B. Тип поставщика (COTS, внешний поставщик услуг, индивидуальный поставщик и т. д)

C. Стратегические отношения с поставщиками

D. Технологии, используемые организацией

Ответ на вопрос дня: 20200204

Организации сталкиваются с различными видами рисков, которые препятствуют достижению их целей.

Как эксперт по безопасности, вы являетесь участником программы управления рисками.

При создании рискованной ситуации, что из перечисленного наименее вероятно будет сделано?

A. Определите допустимый уровень риска

B. Предоставьте эталонную модель риска

C. Создание корпоративной архитектуры

D. Назначьте специалиста по управлению рисками

Ответ на вопрос дня: 20200207

Вы изучили следующие формулы из учебного пособия CISSP и использовали их в своем плане управления рисками.

Общий риск = Угроза X Слабость X Стоимость активов.

Вы обнаружили, что хакеры и начинающие программисты могут использовать SQLMap для осуществления SQL-инъекционных атак, направленных на системы баз данных через

веб-серверы.

Клиентские файлы были засекречены как конфиденциальные, их стоимость оценивалась в 500 миллионов долларов. Обработка клиентских данных осуществлялась веб-системой CRM, однако эта система была крайне уязвима из-за плохого дизайна и задержек с обновлением.

Вы проводите оценку рисков. Какой из следующих способов выражения совокупного риска является наименее распространенным и наиболее дорогостоящим?

A. 7 438 399,5 доллара США

B. Низкий

C. Оценка риска: 2 из 5

D. Очень высокий

Ответ на вопрос дня: 20200217

Из-за риска нарушения целостности и доступности данных некоторые глобальные поставщики облачных услуг отказались от создания центров обработки данных в регионах с нестабильным электроснабжением.

Какой из следующих вариантов управления рисками или стратегий реагирования на риски лучше всего описывает это решение?

A. Устранение риска

B. Передача риска

C. Снижение риска

D. Избежание риска

Ответ на вопрос дня: 20200306

Информационная система получила разрешение на ввод в эксплуатацию (АТО). (уполномочено на эксплуатацию е). При мониторинге рисков на уровне информационной системы следует учитывать следующее. Какой из них вызывает наименьшее беспокойство?

A. Соответствие

B. Остаточный риск

C. Возникающие изменения

D. Действующая авторизация

Ответ на вопрос дня: 20200419

Ваша компания — известный поставщик облачных услуг. Из отчетов по анализу угроз вы узнали о наличии уязвимостей на аппаратном уровне в уязвимостях Meltdown и Spectre, затрагивающих практически все марки процессоров.

Атаки Meltdown позволяют вредоносным программам использовать состояния гонки для чтения всего пространства

памяти, что приводит к несанкционированному доступу.

Атака Spectr — это атака на основе временных рядов, использующая спекулятивное выполнение, позволяющая даже вредоносным скриптам считывать всё пространство памяти программы.

Несмотря на неоднократные попытки снизить риски, последнее обновление программного обеспечения продолжает серьезно ухудшать производительность системы. Рассмотрев все возможные варианты снижения рисков, высшее руководство решило принять этот риск.

Какой из следующих вариантов наименее вероятно отражает это управленческое решение?

A. Отслеживайте риски и реагируйте на них до момента их возникновения

B. Уровень подверженности присущему риску ниже стандарта приемлемости риска

C. Уровень остаточного риска ниже допустимого уровня риска

D. Регистрируйте риски в реестре рисков и постоянно отслеживайте их

Ответ на вопрос дня: 20200501

Соответствие требованиям

Вы сдаёте экзамен CISSP. На экране отображается соглашение, обязывающее вас (кандидата) не делиться материалами экзамена с другими.

После ознакомления нажмите кнопку «Я согласен», а затем начните экзамен.

Какое из следующих утверждений лучше всего описывает ваше поведение?

A. Ответственность

B. Цифровая подпись

C. Должная осмотрительность

D. Юридическая экспертиза

Ответ на вопрос дня: 20191220

Вы готовитесь к экзамену CISSP. Некоторые поставщики рекламируют свои услуги, предлагая подлинные экзаменационные вопросы прошлых лет или возможность получения сертификата без сдачи экзамена.

Как кандидат на сертификацию CISSP вы решили сообщить о подобных недобросовестных методах продаж. Какое из следующих этических правил $(ISC)^2$ было нарушено?

A. Действовать честно, справедливо, ответственно и в со-

ответствии с законом

B. Обеспечивать добросовестное и компетентное обслуживание работодателя

C. Содействовать развитию и защите профессии

D. Ни один из перечисленных вариантов

Ответ на вопрос дня: 20200108

Ваша компания решила начать продавать игрушки онлайн и отправлять их по всему миру. Недавно принятый на работу разработчик Дэниел был выбран благодаря своей дипломной работе. Был опубликован ключевой алгоритм.

Он присоединился к внутренней команде разработчиков и переработал компонент анализа корзины покупок, воспроизведя идеи бывшей компании. Та утверждала, что владеет патентом на алгоритм, разработанный её бывшим сотрудником.

На что из перечисленного ниже следует обратить наибольшее внимание специалисту по безопасности?

A. Товарный знак

B. Коммерческая тайна

C. Патент

D. Авторское право

Ответ на вопрос дня: 20191222

Ваша компания — это онлайн-банк, полностью зависящий от интернета, а также публичная акционерная компания.

Вы проводите комплексную проверку на соответствие действующему законодательству и нормативным актам компании.

Что из перечисленного оказывает существенное влияние на корпоративное управление и возлагает на директоров и высших руководителей личную ответственность за точность финансовой отчетности?

A. GDPR

B. GLBA

C. SOX

D. HITECH

Ответ на вопрос дня: 20200222

Вы являетесь специалистом по информационной безопасности (CISO) и работаете в банке прямого обслуживания на Тайване, где банковские услуги предоставляются только онлайн.

Вы изучаете применимые нормативные акты для соблюдения требований соответствия.

Что из перечисленного вызывает у вас наибольшую обеспокоенность?

A. В договоре, заключённом отделом закупок, не указаны минимальные требования безопасности

B. Команда разработчиков использовала компонент с открытым исходным кодом из неизвестного источника

C. В ответ на новые законы или нормативные акты компания публикует соответствующую политику

D. Субъект персональных данных может обновлять свои личные данные

Ответ на вопрос дня: 20200117

Персональные данные и конфиденциальность

Ваша компания продает игрушки онлайн и по всему миру. Для исследования потребительских предпочтений отдел маркетинга разработал анонимную анкету и разместил её на официальном сайте для заполнения посетителями. Однако менеджер по маркетингу попросил, чтобы анкета собирала данные из городов, которые посещали посетители, для регионального анализа.

Учитывая вопросы конфиденциальности, какой из следующих принципов защиты персональных данных следует соблюдать?

A. Разумные ожидания неприкосновенности частной жизни

B. Многоуровневая защита

C. Соответствие требованиям и выбор

D. Ни один из вышеперечисленных

Ответ на вопрос дня: 26.09.2019

Ваша компания решила продавать игрушки онлайн по всему миру. Внутренняя команда и внешняя команда сотрудничают над разработкой веб-сайта для онлайн-покупок.

Внешняя команда запрашивает данные клиента для тестирования программного обеспечения.

Данные клиентов были зашифрованы и затем помечены звездочкой (*), чтобы предотвратить разглашение информации о них и защитить конфиденциальность.

Какое из следующих утверждений лучше всего описывает метод деидентификации?

A. Анонимизация

B. Перетасовка

C. Удалить обработку конфиденциальной информации

D. Псевдонимизация

Ответ на вопрос дня: 20200317

Распространение сотрудником фотографий, сделанных в офисе или в повседневной жизни, может привести к утечке данных.

Какой из следующих методов обеспечения безопасности является наиболее эффективным и должен быть внедрен в первую очередь для гарантирования безопасности?

A. Решение для предотвращения утечек данных (DLP)

B. Политика использования личных устройств (BYOD)

C. Политика допустимого использования (AUP)

D. Обучение и повышение осведомлённости по вопросам безопасности

Ответ на вопрос дня: 20200416

Ваша компания разрабатывает информационную систему для поддержки своего нового бизнеса по онлайн-продаже игрушек в Соединенных Штатах.

Отдел маркетинга рекомендует системе получать информацию о клиентах из социальных сетей при регистрации, чтобы упростить и ускорить процесс регистрации.

Они решили принимать только внутренние заказы и отклонять заказы от граждан ЕС, чтобы избежать юридических и нормативных рисков.

Как специалист по информационной безопасности, вы понимаете, что вопросы конфиденциальности необходимо решать. Что из перечисленного вызывает у вас наибольшее беспокойство?

A. Соответствие требованиям соответствующего лица

B. Ограничения на использование, хранение и раскрытие информации

C. Согласно правилам, требуется

D. Подотчётность

Ответ на вопрос дня: 20190911

Безопасность персонала

В вашей компании введены обязательные отпуска и ротация кадров для выявления и предотвращения коррупции. Как специалист по безопасности, какую из следующих рекомендаций вы бы поставили в приоритет?

A. Регулярно проверять права доступа пользователей

B. Во время обязательного отпуска ограничивать сотрудникам доступ к корпоративным системам

C. Во время ротации проводить обучение и сертификацию для эффективного выполнения новых обязанностей

D. При переводе на новую должность требовать немедленной смены пароля

Ответ на вопрос дня: 20191124

Вы работаете в компании, занимающейся проектированием интегральных схем. Конфиденциальность данных клиентов и данные, используемые в исследованиях и разработках, являются для компании первостепенными задачами.

Дэниел К. — недовольный администратор по безопасности, который только что устроился на новую работу в другую компанию и неделю назад уведомил отдел кадров о своем увольнении.

Сотрудники отдела кадров сочли ситуацию потенциально конфликтной.

Как специалист по безопасности, какое из следующих предложений вы бы, скорее всего, не стали давать?

A. Немедленно прекратить доступ к системе

B. Попросить подготовить документы для передачи дел

C. На период уведомления об увольнении перевести сотрудника в зону с ограниченным доступом

D. Попросить сотрудника оставаться дома и не приходить в офис

Ответ на вопрос дня: 20191130

Вы являетесь специалистом по информационной безопасности (CISO) и работаете в банке прямого обслуживания на Тайване, где банковские услуги предоставляются только онлайн.

Вы сотрудничаете с отделом кадров (HR) для повышения уровня безопасности персонала.

Какой из следующих вариантов вы бы порекомендовали изучить в первую очередь?

A. Механизм контроля доступа на основе ролей

B. Процедура проверки биографических данных

C. Внедрить разделение обязанностей

D. Достоверность и правильность описания должностных обязанностей

Ответ на вопрос дня: 20200122

Вы являетесь инструктором по обучению основам информационной безопасности в вашей компании. Вы хотели бы привести несколько примеров атак с использованием методов социальной инженерии.

Какое из следующих действий пользователя позволяет источнику угроз собирать информацию о конфигурации системы с наименьшими затратами?

A. Размещение вакансий на сайтах поиска работы

B. Публикация фотографий в социальных сетях

C. Подключение неизвестного USB-устройства к компьютеру

D. Пересылка электронного письма коллегам

Ответ на вопрос дня: 20200609

Глава 2. Защита информационных активов

Роли и обязанности

Вы планируете программу повышения осведомленности о технике безопасности, обучения и повышения квалификации.

Какая из перечисленных групп НЕ относится к основным группам людей, которым необходимы дополнительные знания и навыки для более эффективного выполнения своей работы?

A. Все сотрудники

B. Конечные пользователи

C. Администраторы безопасности

D. Инженер в области информационных технологий (ИТ)

Ответ на вопрос дня: 20200628

По продажам вы назначены владельцем данных основной базы данных клиента.

Вы изучаете роль и обязанности владельца данных. Что из

перечисленного наименее актуально для владельца данных?

A. Классифицировать данные по их коммерческой ценности

B. Делегировать системному администратору предоставление полномочий пользователям

C. Нести ответственность за утечку данных

D. Определить схему классификации

Ответ на вопрос дня: 23.09.2019

Ваша компания завершила инвентаризацию активов. Менеджер по продажам Меган назначена ответственной за основные данные о клиентах. Директор по информационным технологиям Лорен является ответственной за систему ERP. Система ERP поддерживает процесс продаж. Кроме того, они также отвечают за обработку данных из различных отделов.

На заседании Руководящего комитета по информационной безопасности Меган рекомендовала внедрить многофакторную аутентификацию в ERP-системы для обеспечения достаточного уровня безопасности и защиты основных данных клиентов.

Как председателю, как вам следует отреагировать на это предложение?

A. Внедрить многофакторную аутентификацию, поскольк-

ку Меган является владельцем основных данных клиента

B. Попросить Меган предложить решение по многофакторной аутентификации

C. Поручить Лорен подготовить предложение

D. Для принятия предложения требовалось провести голосование на месте

Ответ на вопрос дня: 24.09.2019

Ваша компания готовится списать 50 настольных компьютеров и 50 ноутбуков. Амортизация этих ноутбуков начислялась в течение пяти лет, и их остаточная стоимость на балансе очень невелика.

Поэтому компания предоставляет сотрудникам приоритетное право на приобретение этих устаревших устройств для личного или семейного использования. Оставшиеся устройства, не приобретенные сотрудниками, будут проданы на открытом рынке.

Во всех ноутбуках для обеспечения безопасности включено полное шифрование диска.

Какой из следующих вариантов является наилучшим решением?

A. Полностью отформатировать все диски штатной утилитой операционной системы

B. Выполнить сброс компьютеров и ноутбуков к заводским настройкам

C. Удалить все данные с помощью специализированных утилит и команд производителя

D. Выполнить криптографическое стирание дисков ноутбуков и размагнитить диски настольных компьютеров

Ответ на вопрос дня: 25.09.2019

Ваша компания продает игрушки онлайн и по всему миру. Для ведения этого бизнеса используется собственная система электронной коммерции, развернутая в публичном облаке с применением модели «Платформа как услуга» (PaaS).

Вашей компании необходимо собирать данные о клиентах для выставления счетов и осуществления доставки. Как специалист по безопасности, вы должны определить роль вашей компании в обеспечении конфиденциальности и соответствующие нормативные акты.

Какой из следующих вариантов лучше всего описывает роль вашей компании?

A. Владелец данных

B. Ответственный за данные

C. Контроллер данных

D. Директор

Ответ на вопрос дня: 27.09.2019

Информация — это актив организации. Что из перечисленного относится к бережному и ответственному управлению информацией, которой владеет организация, независимо от её источника, организации, которая её создала или собрала, или её происхождения?

A. Хранение информации

B. Информационная безопасность

C. Ответственное управление информацией

D. Право собственности на информацию

Ответ на вопрос дня: 20200208

Ваша организация разрабатывает систему управления транспортом (TMS), которая обрабатывает два типа данных: данные о воздушном и наземном транспорте.

При классификации систем для определения критериев безопасности, какая из следующих ролей наименее вовлечена в процесс категоризации систем?

A. Старший руководитель

B. Ответственный за данные

C. Владелец информации

D. Владелец системы

Ответ на вопрос дня: 20200212

Вопросы владения активами являются одними из главных в информационной безопасности. После проведения инвентаризации информационных активов ваша организация проверит вопрос владения ими.

Какой из следующих споров о праве собственности наименее вероятен?

A. Готовое коммерческое программное обеспечение (COTS)

B. Производственные параметры или формула

C. Основной файл клиента или его профиль

D. Изобретения, созданные в результате исследований

Ответ на вопрос дня: 20200214

Ваша компания продает игрушки онлайн по всему миру. Система веб-сайта электронной коммерции, поддерживающая этот бизнес, была разработана внутри компании. Ответственность за эту систему несет IT- менеджер, который также отвечает за обработку различных данных, хранящихся у руководителей отделов.

Какой из следующих вариантов является наилучшим для

определения мер безопасности данной системы с точки зрения консультанта по корпоративной безопасности (CIS)?

A. Ты,

B. Владелец данных

C. Владелец системы

D. Д. Менеджеры информационных технологий и владельцы данных

Ответ на вопрос дня: 20200613

В день своего ухода увольняющийся торговый представитель скачал с файлового сервера на USB-устройство данные о клиентах, принадлежащие руководителю отдела продаж, и продал их онлайн.

Утечка данных произошла из-за плохой коммуникации между отделами кадров и ИТ. Отдел кадров не уведомил ИТ-отдел о необходимости немедленно заблокировать учётные записи пользователей и отозвать привилегии у недовольных сотрудников.

Кто несёт ответственность за утечку данных клиентов?

A. Владелец системы файлового сервера из-за недостаточных мер безопасности

B. Вице-президент по кадрам из-за небрежности

C. Директор по информационным технологиям из-за недостатков процесса предоставления и отзыва прав доступа

D. Вице-президент по продажам как владелец данных, отвечающий за их классификацию и защиту

Ответ на вопрос дня: 07.07.2020

Классификация активов

Вы только что были официально признаны специалистом CISSP и повышены до уровня CISO. Для соответствия нормативным требованиям вы разработали политику, которая будет регулировать и поддерживать программу управления данными.

Что из перечисленного следует сделать в первую очередь?

A. Классифицировать данные

B. Определить область применения и адаптировать меры безопасности

C. Провести инвентаризацию данных

D. Разработать стратегию информационной безопасности

Ответ на вопрос дня: 20200705

Ваша компания решила начать продавать игрушки онлайн и отправлять их по всему миру. Внутренняя команда отвечает за разработку системы электронной коммерции для поддержки этого нового бизнеса.

Команда разработчиков проводит моделирование угроз для выявления потенциальных угроз для базы данных.

Какие из следующих данных, касающихся контроля безопасности и отдыха, наименее актуальны?

A. Классификация данных

B. Авторизация

C. Избыточность хранения

D. Маркировка данных

Ответ на вопрос дня: 20191117

Вы работаете в должности CISO в банке, осуществляющем прямые операции, на Тайване. С этой целью банковские операции могут проводиться только в режиме онлайн.

Вы разрабатываете политику в отношении данных и рассматриваете схему классификации данных. Вы предпочитаете широкую систему классификации.

Какой из следующих критериев классификации лучше всего соответствует вашим требованиям?

A. Чувствительность

B. Критичность

C. Деловая ценность

D. Стоимость восстановления

Ответ на вопрос дня: 20200107

Было найдено потерянное USB-устройство инженера, но на нем не было физической маркировки, указывающей на

конфиденциальность информации. Однако, согласно политике компании в отношении данных, все носители информации должны быть маркированы.

Какое из следующих действий следует предпринять в первую очередь?

A. Обозначьте USB-устройство как устройство с наивысшим уровнем чувствительности

B. Классифицируйте и обозначьте USB-устройство как устройство с самым низким начальным уровнем

C. Проверьте USB-устройство на рабочем месте службы безопасности и по результатам проверки пометьте его символом

D. Уведомите владельца USB-устройства и попросите его наклеить этикетку

Ответ на вопрос дня: 20200210

Жизненный цикл данных

Ваша компания решила начать продавать игрушки онлайн и отправлять их по всему миру. Система электронной коммерции, поддерживающая этот новый бизнес, будет разработана внутри компании.

Архитекторы решений выбрали систему хранения данных RAID, состоящую из высокопроизводительных и высокоскоростных твердотельных накопителей (SSD). В настоящее время команда разработчиков разрабатывает план обеспечения безопасности системы.

Проблем сохранения данных при утилизации дисков или систем хранения?

A. Размагничивание

B. Низкоуровневое форматирование

C. Перезапись

D. Криптографическое удаление

Ответ на вопрос дня: 20191101

Настольные ПК с жесткими дисками ATA, используемые инженерами в отделе исследований и разработок, будут постепенно выведены из эксплуатации. В соответствии с политикой маркировки носителей информации, жесткие диски,

содержащие конфиденциальные данные, должны быть стерты без возможности восстановления.

Какая из следующих процедур дезинфекции не соответствует этому требованию?

A. Использовать команду блочного стирания

B. Записать нули в каждый байт логической области

C. Перезаписать внутренний носитель фиксированным значением

D. Изменить внутренний ключ шифрования пользовательских данных

Ответ на вопрос дня: 20200209

Организации должны хранить только необходимую информацию. Чтобы уменьшить объем хранимых данных и гарантировать сохранение только релевантной информации, что из перечисленного вызывает наименьшее беспокойство?

A. Место хранения данных

B. Тип данных

C. Стойкость алгоритма шифрования

D. Срок хранения

Ответ на вопрос дня: 20200211

В соответствии с требованиями законодательства, ваша организация должна хранить бухгалтерские записи не менее десяти лет.

5 % транзакций, хранящихся в базе данных более года, с высокой вероятностью будут использованы или запрошены повторно.

Что из перечисленного вызывает наименьшее беспокойство в отношении соблюдения нормативных требований?

A. Иерархическое управление хранением данных

B. Политика хранения данных

C. Проверка резервных копий

D. Внеофисное хранение магнитных лент

Ответ на вопрос дня: 20200220

Ваша компания продает игрушки онлайн и по всему миру. В течение примерно четырех лет бизнес поддерживается трёхуровневой системой веб-сайта.

Сервер базы данных оснащен системой хранения данных RAID 5 для повышения эффективности транзакций. Устройство хранения данных состоит из трех твердотельных накопителей SSD емкостью 1 ТБ каждый и поставляется с трехлетней гарантией MTBF (средним временем безотказной работы (MTBF) и сервисным обслуживанием.

Новый системный администратор планирует заменить

старую систему на новую, более вместительную систему хранения данных на твердотельных накопителях (SSD). Данные клиентов в базе данных классифицируются как конфиденциальные.

Какой из следующих способов является наилучшим для решения этой проблемы?

A. Проконсультироваться с владельцем информационной системы

B. Уничтожить носители, чтобы предотвратить утечку информации

C. Связаться с поставщиком обслуживания и обменять старые SSD по гарантии или со скидкой

D. Обновить систему хранения до RAID на пяти SSD по 2 ТБ с пятилетним показателем MTBF

Ответ на вопрос дня: 20191001

Категории мер безопасности

Правило A Закона HIPAA о безопасности определяет определенные меры защиты как «защиту электронной конфиденциальной медицинской информации (ePHI) и контроль технологий, политик и процедур доступа к такой информации».

Какое из следующих утверждений лучше всего описывает категорию или тип вышеупомянутых защитных мер?

A. Директива

B. Управление

C. Технический

D. Логика

Ответ на вопрос дня: 20191221

Глава 3. Архитектура и инженерия безопасности

Инженерия безопасности

Ваша компания решила начать продавать игрушки онлайн и отправлять их по всему миру. Внутренняя команда отвечает за разработку системы электронной коммерции для поддержки этого нового бизнеса.

Проектная группа оценивает процесс разработки системы информационной безопасности, которому следует следовать.

Что из перечисленного наименее применимо к системной инженерии данного проекта?

A. SSE-CMM (Модель зрелости возможностей проектирования системной безопасности)

B. Руководство по системной инженерии INCOSE

C. NIST SP 800-160 (Проектирование системной безопасности)

D. ISO 15288 (Системная и программная инженерия —

Процессы жизненного цикла системы)

Ответ на вопрос дня: 20191120

Ваша компания разрабатывает информационную систему для поддержки своего нового бизнеса по онлайн-продаже игрушек.

Как специалист по безопасности, вы рекомендуете следовать стандарту ISO/IEC/IEEE 1528 8 (Системная и программная инженерия — Процессы жизненного цикла системы) для обеспечения использования безопасных процессов разработки информационных систем и подчеркиваете, что «управление информацией» является одним из наиболее важных процессов.

К какой из следующих серий процессов относится «Управление информацией»?

A. Процесс заключения соглашения

B. Проект — Вспомогательный процесс

C. Процесс управления технологиями

D. Технический процесс

Ответ на вопрос дня: 20190830

Для решения проблем безопасности необходимо привести жизненный цикл разработки программного обеспечения в соответствие со стандартом ISO 15288. Выравнивание.

Стандарт ISO 1528 8 включает четыре группы процессов

жизненного цикла системы: процессы согласования, процессы обеспечения реализации проектов, процессы управления технологиями и технологические процессы.

Какой из следующих вариантов относится к группе технологических процессов?

A. Управление конфигурацией

B. Управление моделью жизненного цикла

C. Обеспечение качества

D. Анализ бизнеса или миссии

Ответ на вопрос дня: 20200128

Ваша компания получила контракт на разработку специализированного межсетевого экрана для известной компании, занимающейся вопросами безопасности.

Как специалист по безопасности, вы являетесь членом интегрированной продуктовой команды. После проведения семинаров, сбора и получения требований к защите от клиентов и заинтересованных сторон, вы завершаете разработку спецификаций требований к функциям и гарантиям безопасности.

Какое из следующих действий, выполняемых группой обеспечения качества, гарантирует соответствие продукции техническим характеристикам?

A. Сертификация

B. Аккредитация

C. Проверка

D. Д. Валидация

Ответ на вопрос дня: 20200623

Ваши клиенты продают игрушки онлайн по всему миру. Этот бизнес работает на основе собственной системы электронной коммерции. Платежный шлюз для этой системы планируется передать вашей компании на аутсорсинг в рамках программного проекта.

Ваша компания получила этот контракт. Какой из следующих подходов, методологий или концептуальных основ лучше всего подходит для определения конкретных этапов, процессов, ролей и обязанностей, которые будут определять разработку программного обеспечения?

A. Интеграция модели зрелости процессов (CMMI)

B. Жизненный цикл безопасной разработки (SDL)

C. Структура управления рисками NIST (RMF)

D. Единый процесс разработки программного обеспечения

Ответ на вопрос дня: 20200611

Жизненный цикл систем и RMF

Ваша компания разрабатывает информационную систему для поддержки своего нового бизнеса по онлайн-продаже игрушек.

, согласно жизненному циклу разработки информационных систем (SDLC) Национального института стандартов и технологий (NIST), специалисту по информационной безопасности следует определить, следует ли использовать безопасный процесс разработки информационных систем для данного проекта?

A. Инициация

B. Разработка или приобретение

C. Внедрение и оценка

D. Эксплуатация и сопровождение

Ответ на вопрос дня: 20190901

Ваша компания решила начать продавать игрушки онлайн и отправлять их по всему миру. Внутренняя команда отвечает за разработку системы электронной коммерции для поддержки этого нового бизнеса.

В качестве специалиста по безопасности вы проводите оценку воздействия на конфиденциальность в соответствии

со стандартом ISO 29134 (Руководство по оценке воздействия на конфиденциальность), в то время как другие члены команды отвечают за другую работу по проекту.

Что из перечисленного наименее вероятно произойдет на данном этапе?

A. Меры безопасности при работе на полигоне и резке

B. Классифицируйте системы электронной коммерции как

C. Оцените влияние на бизнес

D. Обеспечьте использование безопасных процессов SDLC

Ответ на вопрос дня: 20191110

Ваша компания решила начать продавать игрушки онлайн и отправлять их по всему миру. Внутренняя команда отвечает за разработку системы электронной коммерции для поддержки этого нового бизнеса.

Проектная группа завершила анализ влияния на бизнес и конфиденциальность. Какие из следующих мероприятий по обеспечению безопасности следует выполнить далее?

A. Провести оценку безопасности системы

B. Разработать подробный план сертификации и аккредитации (C&A)

C. Провести оценку рисков системы

D. Проверить операционную готовность

Ответ на вопрос дня: 20191126

Ваша компания решила начать продавать игрушки онлайн и отправлять их по всему миру. Система электронной коммерции, поддерживающая этот новый бизнес, будет разработана внутри компании.

Проект по разработке программного обеспечения запущен всего несколько дней назад, и вы готовитесь к завтрашнему совещанию по проекту.

Что из перечисленного следует рассмотреть в первую очередь специалисту по безопасности?

A. Риски, с которыми сталкивается система

B. Последствия нарушения конфиденциальности

C. Архитектура безопасности системы

D. Потребности и требования заинтересованных сторон в области безопасности

Ответ на вопрос дня: 20191011

Ваша компания приняла решение внедрить стандарт ISO 27001 и получить сертификацию. После проведения оценки рисков вы определяете меры контроля для снижения этих

рисков.

Для соответствия требованиям настоящего стандарта вы подготовили описание применимости, которое включает все меры контроля, рекомендованные в Приложении А настоящего стандарта, содержит перечень указанных мер контроля и обосновывает включение или исключение каждой меры контроля из описания.

Какое из следующих утверждений лучше всего описывает этот процесс?

A. Категоризация и классификация

B. Верификация и валидация

C. Сертификация и аккредитация

D. Определение масштаба и адаптация

Ответ на вопрос дня: 20190914

Согласно стандарту NIST SDLC, какое из следующих мероприятий по обеспечению безопасности следует выполнить в первую очередь перед вводом в эксплуатацию авторизованной информационной системы?

A. Оценить риски системы

B. Оценить влияние предоставляемых услуг

C. Оценить состояние безопасности системы

D. Проверить операционную готовность

Ответ на вопрос дня: 20200411

Вы являетесь владельцем недавно внедренной в вашей организации системы управления транспортом. Вы подготовили документ для подачи заявки на получение разрешения на эксплуатацию (ATO).

Что из перечисленного наименее вероятно будет включено в документы заявки на авторизацию?

A. Стратегия управления рисками

B. План обеспечения безопасности и конфиденциальности

C. Отчёт об оценке безопасности и конфиденциальности

D. Краткое резюме для руководства

Ответ на вопрос дня: 20200206

В рамках системы управления рисками NIST (RMF) авторизация относится к процессу, в ходе которого высшее руководство или уполномоченные должностные лица проверяют текущее состояние безопасности и конфиденциальности информационных систем или общих средств контроля. Общие средства контроля наследуются или используются несколькими системами.

Какой из следующих вариантов НЕ является вариантом

принятия решения в процессе авторизации?

A. Разрешение на эксплуатацию

B. Действующее разрешение

C. Отказ в разрешении

D. Общее разрешение на контроль

Ответ на вопрос дня: 20200418

Ваша компания решила подписаться на SaaS-сервисы от известного поставщика облачных услуг. Как специалист по безопасности, вы получили задание разработать план обеспечения безопасности.

Что из перечисленного следует сделать в первую очередь?

A. Определить тип данных, обрабатываемых облачным сервисом SaaS

B. Категорировать систему по уровню воздействия

C. Определить область применения и адаптировать меры безопасности

D. Определить заинтересованные стороны

Ответ на вопрос дня: 30.06.2020

Ваша компания разрабатывает информационную систему для поддержки своего нового бизнеса по онлайн-продаже иг-

рушек.

Как специалист по безопасности, вы являетесь членом проектной группы инженеров и отвечаете за обеспечение надлежащего удовлетворения потребностей в области безопасности и за соответствие информационных систем политике безопасности компании.

Проект был запущен всего неделю назад. Какое из следующих решений следует принять в первую очередь?

A. Категорировать систему по уровню воздействия

B. Выбрать базовый набор мер безопасности

C. Определить область применения и адаптировать меры безопасности к потребностям бизнеса

D. Оценить ценность обрабатываемых данных и последствия их утечки

Ответ на вопрос дня: 27.08.2019

Вы являетесь специалистом по информационной безопасности (CISO) и работаете в банке прямого обслуживания на Тайване, где банковские услуги предоставляются только онлайн.

Вы ссылаетесь на структуру управления рисками NIST (NIST Risk Management Framework, RMF) для определения мер безопасности, необходимых для основных систем банка.

Какой из следующих вариантов лучше всего описыва-

ет критерии, необходимые для выбора средств обеспечения безопасности?

A. Уровень воздействия системы

B. Типы информации, обрабатываемые системой

C. Чувствительность информации, обрабатываемой системой

D. Ценность информации, обрабатываемой системой

Ответ на вопрос дня: 20200105

Ваша компания внедряет систему планирования ресурсов предприятия (ERP). Как специалист по безопасности, вы выбираете меры безопасности из известных систем контроля безопасности в качестве базового варианта и корректируете их в соответствии со специфическими требованиями и ограничениями вашей компании.

В процессе определения и сужения вышеупомянутой сферы действия, какой из следующих вопросов вызывает наименьшее беспокойство?

A. Компенсирующие меры контроля

B. Общие меры контроля

C. Категория воздействия системы ERP

D. Сертификация и аккредитация
Ответ на вопрос дня: 20200620

Архитектурные решения

Ваша компания решила начать продавать игрушки онлайн и отправлять их по всему миру. Внутренняя команда отвечает за разработку системы электронной коммерции для поддержки этого нового бизнеса.

Зашифровала строку подключения к базе данных (содержащую пароли и другие данные), используемую каждым сервером в кластере приложений, с помощью алгоритма AES и сохранила зашифрованный текст в конфигурационном файле.

Для защиты ключа AES команда разработчиков должна использовать модуль доверенной платформы (TPM) на сервере приложений, не прибегая к измерениям платформы.

Какое из следующих решений является наилучшим?

A. Подписание ключа

B. Связывание ключа

C. Запечатывание ключа

D. Кластеризация ключей

Ответ на вопрос дня: 20191116

Ваша компания решила начать продавать игрушки онлайн и отправлять их по всему миру. Система электронной ком-

мерции, поддерживающая этот новый бизнес, будет разработана внутри компании.

Среду выполнения клиентского программного обеспечения, уделяя первостепенное внимание безопасности.

Учитывая такие факторы, как ограничение свободы и установление границ, какая из следующих сред является наиболее безопасной или наиболее ограничительной?

A. Среда выполнения приложений (например, JVM или.NET)

B. Современные веб-браузеры

C. Гипервизор «без привязки к аппаратному обеспечению«(тип I)

D. Размещенный гипервизор (тип II)

Ответ на вопрос дня: 20191002

Переполнение буфера — одна из самых распространенных атак. Что означает «буфер»?

A. Небольшая память внутри процессора или рядом с ним, например кэш или временное хранилище

B. Область основной памяти, например стек или куча

C. Встроенная память жёсткого диска

D. Память, зарезервированная для DNS-записей

Ответ на вопрос дня: 20200329

Программе необходимо загрузить значение 0x30 (хранящееся по адресу памяти #100) в регистр процессора с именем AX для обработки данных. Ассемблерный код выглядит следующим образом:

LD AX, #100

Какие режимы адресации памяти использует эта объединенная программа?

A. Немедленное обращение

B. Адресация регистров

C. Прямая адресация

D. Косвенная адресация

Ответ на вопрос дня: 20200413

Политики безопасности и модели

В вашей организации используется обязательный контроль доступа (MAC) на основе модели Белла — ЛаПадулы, которая не поддерживает свойства «звезды» (*), являющиеся альтернативой свойствам «звезды».

В вашей организации есть принтер, засекреченный как «совершенно секретный».

Майкл — офицер среднего звена с допуском к секретной информации. Его учётная запись настроена с использованием двух атрибутов безопасности, определенных в модели Белла — ЛаПадулы: Simple и Star (*).

Может ли Майкл распечатать свой отчёт на принтере, засекреченном как «совершенно секретно»?

A. Да. Модель Белла — ЛаПадулы не запрещает такой информационный поток

B. Да. Модель Белла — ЛаПадулы позволяет читать данные более высокого уровня секретности

C. Нет. Модель Белла — ЛаПадулы запрещает чтение данных более высокого уровня секретности

D. Нет. Модель Белла — ЛаПадулы запрещает запись данных на более низкий уровень секретности

Ответ на вопрос дня: 28.08.2019

В вашей организации внедрена многоуровневая система обязательного контроля доступа (MAC), основанная на модели Белла — ЛаПадулы.

Сотрудник, имеющий доступ к секретной информации, пожаловался на невозможность записи в документы, засекреченные как «совершенно секретные».

Какая из следующих причин наиболее вероятна?

A. Сотруднику назначено звёздочное свойство (*)

B. Сотруднику не назначено простое свойство безопасности

C. Сотрудник и документы относятся к разным решёткам доступа

D. Файл сотрудника заблокирован другим пользователем

Ответ на вопрос дня: 20191014

Допуск к секретной информации для каждого сотрудника вашей организации будет предоставлен только после тщательной проверки биографических данных; активы будут помечены после их классификации.

Если ваш уровень безопасности выше уровня безопасности ресурса, то ваш доступ к конфиденциальному ресурсу будет разрешен. Однако вы не можете записывать данные на ресурсы с более низким уровнем безопасности.

Конец ознакомительного фрагмента.