Глава 1. Контрольная работа

Какие из нижеуказанных мер эффективны в борьбе с киберпреступниками? (Выберите два варианта.)

Обмен результатами анализа киберугроз Внедрение систем раннего оповещения

Какие три типа данных киберпреступники чаще всего пытаются похитить у организаций? (Выберите три варианта.)

здравоохранение образование трудоустройство

К какой категории, согласно классификации NICE Workforce Framework, относится специализированная оценка поступающей информации о кибербезопасности с целью определения ее пригодности для аналитики?

Анализ

При какой атаке цель выводится из строя путем отправки ей огромного количества запросов от множества других систем?

DDoS-атака

При какой атаке компьютер выводится из строя за счет переполнения памяти или перегрузки центрального процессора?

алгоритмическая атака

Как называют хакера, занимающегося взломами ради продвижения некой идеи?

хактивист

Как называют хакеров-дилетантов?

«скрипт-кидди»

Что означает аббревиатура BYOD?

bring your own device (принеси свое устройство)

Что из перечисленного является примером домена данных в Интернете?

LinkedIn

Что означает термин «уязвимость»?

уязвимость, из-за которого целевая система подвержена тем или иным атакам

Что означает аббревиатура IoE?

Internet of Everything (Всеобъемлющий Интернет)

Глава 2. Контрольная работа

Что из перечисленного относится к первой грани куба кибербезопасности?

цели

Как называется защищенная виртуальная сеть, существующая внутри общедоступной сети?

VPN

Назовите три принципа проектирования, благодаря которым достигается высокая доступность. (Выберите три варианта.)**обеспечение надежного механизма переключения на резервные ресурсы выявление отказов по мере их возникновения исключение единых точек отказа**

Как называют устройство хранения данных, подключенное к сети?

NAS

Назовите два метода обеспечения доступности систем. (Выберите два варианта.) **своевременное обновление операционных систем обслуживание оборудования**

Назовите три метода идентификации, применяемые в процессе аутентификации. (Выберите три варианта.) **фактор знанияфактор свойства фактор владения**

Назовите три средства контроля доступа. (Выберите три варианта.) **учет авторизация аутентификация**

Назовите две наиболее распространенные хеш-функции. (Выберите два варианта.) **SHA MD5**

Какой механизм определяет перечень доступных пользователю ресурсов и операций? учет **авторизация**

Назовите два метода проверки целостности данных. (Выберите два варианта.) **хэширование проверка согласованности данных**

Назовите два метода обеспечения конфиденциальности. (Выберите два варианта.) невозможность отказа **шифрованиеаутентификация**

К какой категории относятся законы в сфере кибербезопасности, регулирующие раскрытие организациями конфиденциальной информации о вас? **конфиденциальность персональных данных**

Какой из принципов подразумевает исключение доступа неавторизованных лиц, ресурсов и процессов к информации?**конфиденциальность**

Как называется механизм передачи информации с одного устройства на другое с помощью съемного носителя? **перенос данных вручную**

Как называется действие, в результате которого первоначальные данные изменяются (путем изменения пользователями вручную, обработки и изменения этих данных приложениями или их изменения в результате отказа оборудования)?**модификация**

Назовите три задачи, которые должна решать комплексная политика безопасности. (Выберите три варианта.) **установление правил ожидаемого поведения определение правовых последствий нарушений создание инструментов управления для специалистов по информационной безопасности**

Какой механизм можно применить в организации в качестве средства защиты от непреднамеренного изменения информации авторизованными пользователями? **управление версиями**

Каковы три основных принципа кибербезопасности? (Выберите три варианта.) **конфиденциальность доступностьцелостность**

Назовите три состояния данных. (Выберите три варианта.) **неактивные передаваемые обрабатываемые**

Назовите три вида конфиденциальной информации. (Выберите три варианта.)
публичная **персональные данныегосударственная тайна коммерческая информация**

Глава 3. Контрольная работа

Злоумышленник применяет специальное ПО, чтобы получить информацию о компьютере пользователя. К какой категории относится такое ПО?
шпионское ПО

Назовите две тактики социальной инженерии, применяемые для получения персональных данных от ничего не подозревающей жертвы? (Выберите два варианта.)
принуждение срочность

Назовите два способа защиты компьютера от вредоносного ПО. (Выберите два варианта.)
Своевременное обновление ПО. Установка антивирусного ПО.

Как называют сценарий, при котором злоумышленник отправляет мошенническое электронное сообщение, выдавая его за сообщение из надежного источника?
фишинг

По каким двум причинам протокол WEP считается ненадежным? (Выберите два варианта.) У всех устройств в сети разные ключи.
Ключ передается в виде отрытого текста. Ключ является статическим и неизбежно повторяется в сетях с большим количеством устройств.

Злоумышленник находится около магазина и с помощью беспроводной связи копирует адреса электронной почты и списки контактов с устройств ничего не подозревающих прохожих. К какому типу относится такая атака?
блюснарфинг

Как называют атаку, при которой электронное сообщение адресуется конкретному сотруднику финансового учреждения?
направленный фишинг

Что означает термин «логическая бомба»?

программа, выполняющая вредоносный код при определенных условиях

Как называют программу или код для обхода стандартного механизма аутентификации?

бэкдор

Что именно модифицируют руткиты?

операционную систему

Что происходит на компьютере, если объем данных превышает пределы буфера?

переполнение буфера

Пользователь видит на экране сообщение о том, что доступ к данным закрыт и будет восстановлен только после уплаты некоторой денежной суммы. К какой категории относится вредоносное ПО, выводящее такие сообщения?

программа-вымогатель

К какому типу относятся атаки, при которых для доступа к базе данных SQL используется поле, в которое пользователь обычно вводит информацию?

Внедрение SQL-кода

Как называется ПО, которое демонстрирует всплывающие окна с рекламой, тем самым принося доход его авторам?

рекламное ПО

Чем вирусы отличаются от интернет-червей?

Интернет-черви могут распространять копии самих себя без участия пользователя.

Вирусы не имеют такой способности.

Как называется уязвимость, посредством которой злоумышленники внедряют сценарии в веб-страницы, просматриваемые пользователями?

Межсайтовый скриптинг

Назовите два основных признака спам-письма. (Выберите два варианта.)

Не указана тема письма.

Орфографические и/или пунктуационные ошибки.

Как называют атаку, при которой злоумышленник отправляет короткое SMS-сообщение, обманом вынуждающее жертву посетить веб-сайт?
смишинг

Глава 4. Контрольная работа

Как называется метод шифрования, при котором криптограмму получают путем перестановки букв? **перестановка**

Как называется технология замены конфиденциальной информации на неконфиденциальную версию этой информации?**маскирование**

Сопоставьте описания с соответствующими терминами. (Не все утверждения применимы.)

стеганография: **сокрытие данных внутри аудиофайла**
стегоанализ: **обнаружение скрытой информации внутри графического файла**
социальная стеганография: **создание сообщения, которое содержит скрытый смысл, понятный лишь конкретной целевой аудитории**
обфускация: **создание запутанного сообщения, которое трудно понять**

Как называется вид шифрования, при котором каждый бит или байт открытого текста обрабатывается отдельно? **поточное**

При каждом входе в систему пользователь видит предупреждающее сообщение с перечнем негативных последствий нарушения правил, предусмотренных политиками компании. К какому типу относится данное средство контроля доступа?**сдерживающие**

Какой из асимметричных алгоритмов определяет схему электронной передачи общего секретного ключа? **алгоритм Диффи-Хеллмана**

Назовите три протокола, в которых применяются асимметричные алгоритмы шифрования. (Выберите три варианта.)**Протокол Secure Shell (SSH) Протокол SSL Pretty Good Privacy (PGP)**

При каком шифровании данные шифруются одним ключом, а расшифровываются — другим? **асимметричное**

Назовите три процесса, которые относятся к категории логических средств контроля доступа? (Выберите три варианта.)**мониторинг трафика с помощью межсетевых экранов выявление подозрительной активности в сети с помощью системы обнаружения вторжений Cisco IDS проверка физических характеристик с помощью систем биометрической идентификации**

При каком алгоритме шифрования применяется один и тот же общий PSK-ключ, чтобы зашифровать и расшифровать данные? **симметричное**

Как называется технология защиты программного обеспечения от несанкционированного доступа или модификации?**цифровой водяной знак**

Назовите три вида устройств, которые относятся к категории физических средств контроля доступа. (Выберите три варианта.)**карты с магнитной полосой видеокамеры замки**

Какой криптографический алгоритм применяется в АНБ и подразумевает использование эллиптических кривых для формирования цифровых подписей и обмена ключами? **ECC**

Как называется наука о создании и взломе шифров? **криптология**

Как называется способ сокрытия данных путем их внедрения в некоторый файл (например, графический, звуковой или текстовый)? **Стеганография**

Расположите типы многофакторной аутентификации напротив соответствующих описаний.

ключ-брелок безопасности: **фактор владения**
сканирование отпечатка пальца: **фактор свойства**
пароль: **фактор знания**

Какой алгоритм блочного шифрования с длиной блока в 128 бит применяется в государственных органах США для защиты секретной информации? **AES**

Выберите три примера административных средств контроля доступа. (Выберите три варианта.) **практики найма сотрудников проверка биографии политики и процедуры**

Какие два термина применяются для описания ключей шифрования? (Выберите два варианта.) **длина ключа пространство ключей**

При каком шифровании блок открытого текста фиксированной длины может быть в любой момент времени преобразован в 128-битный блок криптограммы? **Блочное**

Глава 5. Контрольная работа

Назовите три проверочных критерия, которые применяются в правилах проверки ввода данных. (Выберите три варианта.)
диапазон
размер
формат

Причиной недавней утечки данных в компании стала уязвимость, из-за которой хакер смог получить доступ к корпоративной базе данных через веб-сайт компании, вводя некорректные данные в форму для входа в систему. Какая проблема присутствует на веб-сайте компании?
неэффективный механизм проверки ввода

Пользователь получает от руководителя указание: необходимо найти эффективный метод для защиты паролей в процессе их передачи. Пользователь изучил несколько вариантов и остановился на механизме HMAC. Назовите ключевые элементы, необходимые для внедрения механизма HMAC.
секретный ключ и хеш-сумма

Назовите три ситуации, в которых можно применить хеш-функцию. (Выберите три варианта.)

CHAP

IPsec

PKI

Следователь обнаружил на месте преступления USB-накопитель и намерен представить его в суде в качестве вещественного доказательства. Следователь создает образ этого USB-накопителя для криминалистического анализа и рассчитывает хеш-сумму для созданного образа и самого устройства USB. Какой факт следователь пытается доказать применительно к USB-накопителю, который будет представлен в суде?

Данные, содержащиеся в образе, являются точной копией данных с накопителя и не были изменены в процессе снятия копии.

В какой последовательности следует выполнять действия при создании цифровой подписи?

Создать хеш-сумму; зашифровать хеш-сумму закрытым ключом отправителя; объединить сообщение, зашифрованную хеш-сумму и открытый ключ и таким образом сформировать подпись для документа.

В электронном письме, которое было разослано внутри компании, говорится о том, что в ближайшее время будут внесены изменения в политику безопасности. Сотрудник службы безопасности, с адреса которого якобы отправлено это письмо, сообщает, что служба безопасности компании не рассылала таких писем и что в сети компании, по-видимому, имела место рассылка с подменой адреса отправителя. Что можно было добавить в сообщение, чтобы впоследствии иметь возможность точно определить, было ли это письмо отправлено сотрудником службы безопасности?

цифровая подпись

Пользователь создал программу и желает передать ее всем сотрудникам компании. При этом необходимо гарантировать, что программа не будет изменена в процессе ее загрузки. Каким образом можно обеспечить уверенность в том, что программа не была изменена в ходе ее загрузки?

Вычислить хеш-сумму файла программы, которая может быть использована для проверки целостности файла после его загрузки.

Назовите наиболее важное свойство хеш-функции.
Хеш-функция необратима.

У Алисы и Боба одинаковые пароли для входа в корпоративную сеть. Соответственно, хеш-суммы паролей также одинаковы. Каким образом можно создать различные хеш-суммы для одинаковых паролей?
добавление соли

Пользователь устанавливает соединение с сервером интернет-магазина, чтобы закупить нужные виджеты для компании. Установив соединение с веб-сайтом, пользователь обращает внимание на то, что в строке состояния безопасности браузера отсутствует значок замка. Веб-сайт запрашивает имя пользователя и пароль. Пользователь вводит их, успешно входит на сайт и намерен выполнить транзакцию. Какая возникает опасность?
На веб-сайте отсутствует цифровой сертификат для защиты транзакции, поэтому данные передаются в незашифрованном виде.

Назовите три вида атак, которые можно предотвратить за счет добавления соли? (Выберите три варианта.)
радужные таблицы
таблицы поиска
реверсивные таблицы поиска

Какой метод подразумевает поиск пароля путем перебора всех возможных комбинаций?
атака методом грубой силы

Пользователь оценивает инфраструктуру безопасности компании и обращает внимание на то, что в некоторых системах аутентификации применяются не самые лучшие методы хранения паролей. Пользователь может легко взломать пароли и получить доступ к конфиденциальным данным. Пользователь намерен представить рекомендацию руководству компании по реализации метода добавления соли, который поможет предотвратить взлом паролей. Назовите три лучшие практики добавления случайных данных в виде соли. (Выберите три варианта.)

Соль должна быть уникальной.

Не использовать одну и ту же соль многократно.

Добавлять уникальную соль к каждому паролю.

Пользователь выполняет обязанности администратора баз данных. Этому пользователю поручили внедрить правило обеспечения целостности, согласно которому каждая таблица должна иметь первичный ключ, при этом столбец или столбцы, играющие роль первичного ключа, должны содержать уникальные ненулевые значения. Какое требование к целостности реализует этот пользователь?

сущностная целостность

Назовите три алгоритма создания цифровой подписи, одобренные институтом NIST. (Выберите три варианта.)

RSA

DSA

ECDSA

Пользователь загружает с веб-сайта новую версию драйвера для видеокарты. На экране появляется сообщение о том, что драйвер из непроверенного источника. Что отсутствует в загруженном драйвере?

цифровая подпись

Как называется стандарт инфраструктуры открытых ключей для работы с цифровыми сертификатами?

x.509

Пользователю поручили внедрить набор протоколов IPsec для входящих внешних соединений. В качестве одного из компонентов пользователь планирует применить алгоритм SHA-1. При этом необходимо гарантировать целостность и подлинность соединения. Какое средство обеспечения безопасности следует выбрать?

HMAC

Для чего применяется криптографически стойкий генератор псевдослучайных чисел?

генерирование соли

Глава 6. Контрольная работа

Пользователю поручили оценить сетевую инфраструктуру компании. Пользователь обнаружил, что для многих систем и устройств предусмотрено резервирование, но при этом отсутствует общая оценка сети. В своем отчете пользователь описывает целостную систему методов и конфигураций, которую необходимо применить, чтобы добиться полной отказоустойчивости сети. О какой конструкции сети идет речь в отчете пользователя?

отказоустойчивая

Пользователь приобретает новый сервер для центра обработки данных. Пользователь намерен применить массив из трех дисков с чередованием данных и контролем четности. Какой уровень RAID следует выбрать?

5

Пользователь реорганизует сеть небольшой компании и намерен обеспечить безопасность, не выходя за рамки небольшого бюджета. Между сетью компании и сетью интернет-провайдера пользователь помещает новый межсетевой экран, который снабжен системой обнаружения вторжений и функционирует с учетом особенностей используемого программного обеспечения. Кроме того, пользователь отделяет сеть компании от общедоступной сети с помощью второго межсетевого экрана. При этом во внутренней сети компании пользователь развертывает систему предотвращения вторжений IPS. Какой подход применяется в данном случае?

многоуровневый

Пользователь принят на работу в службу безопасности компании. Ему поручают первый проект — нужно инвентаризировать аппаратные ресурсы компании и создать всеобъемлющую базу данных. Назовите три категории информации, которые следует включить в базу данных аппаратных ресурсов. (Выберите три варианта.)

аппаратные сетевые устройства

рабочие станции

операционные системы

Компания нанимает специалиста по обеспечению высокой доступности сетевой инфраструктуры. Он намерен внедрить в сеть механизмы резервирования на случай

отказа коммутаторов, но при этом желает исключить петли на уровне 2. Что нужно применить в такой ситуации?

протокол STP

Пользователь проводит плановый аудит аппаратного обеспечения серверов в центре обработки данных. На нескольких серверах применяется следующая конфигурация: операционная система находится на отдельном накопителе, тогда как данные хранятся в подключенных системах хранения различных типов. Пользователь намерен предложить более эффективное решение, которое позволит избежать отказа в случае выхода из строя накопителя. Какое решение будет наилучшим?

RAID

Группе специалистов поручили разработать план реагирования на события безопасности. На каком этапе разработки плана группа должна согласовать план с руководством организации?

подготовка

Пользователю поручили добавить резервирование маршрутизаторов в сети компании. Назовите три варианта решения этой задачи. (Выберите три варианта.)

VRRP

GLBP

HSRP

В крупной корпорации произошло нарушение безопасности. Соответствующая группа специалистов предприняла необходимые действия согласно плану реагирования на инциденты. На каком этапе следует применить опыт, полученный при реагировании на этот инцидент?

мероприятия после инцидента

В сети компании обнаружен подозрительный трафик. В компании опасаются, что источником этого трафика является вредоносное ПО, которое не было заблокировано или удалено антивирусом. Какая технология поможет обнаружить в сети трафик, генерируемый вредоносным ПО?

IDS

Пользователю поручили оценить производительность центра обработки данных, чтобы повысить уровень доступности услуг для заказчиков. Пользователь отмечает следующие особенности: имеется лишь одно подключение к интернет-провайдеру; в парке оборудования присутствуют устройства с истекшим гарантийным сроком; запасные компоненты отсутствуют; никто не следит за ИБП, который дважды отключался в течение месяца. Таким образом, пользователь обнаружил три недочета, которые негативно влияют на доступность услуг. Назовите их. (Выберите три варианта.)

присутствуют единые точки отказа

не налажена система выявления ошибок по мере их возникновения

при проектировании не учтены требования к надежности

Пользователю поручили разработать для организации план аварийного восстановления. Для решения этой задачи пользователь должен получить от руководителей организации ответы на некоторые вопросы. Назовите три вопроса, которые пользователь должен задать руководству организации, чтобы правильно составить план. (Выберите три варианта.)

Кто несет ответственность за процесс?

Опишите процесс.

Где именно ответственное лицо реализует этот процесс?

Консультанту предстоит подготовить доклад для Правительства о том, в каких сферах необходимо гарантировать доступность систем на уровне «пять девяток». Назовите три отрасли, которые нужно включить в этот отчет. (Выберите три варианта.)

общественная безопасность

финансовый сектор

здравоохранение

Генеральный директор компании обеспокоен правовыми последствиям утечки данных. Если это произойдет, заказчики могут начать судебное разбирательство из-за разглашения конфиденциальной информации. В связи с этим генеральный директор принимает решение о приобретении соответствующего страхового полиса. К какому типу относится такая мера по снижению рисков?

передача риска

Пользователь выполнил шестимесячный проект: нужно было определить местоположение всех данных и составить список выявленных хранилищ. Следующий этап — классификация данных и формирование критериев их конфиденциальности. Назовите два шага, которые следует выполнить при классификации данных. (Выберите два варианта.)

Определить владельца данных.

Определить степень конфиденциальности данных.

Пользователю поручили провести анализ рисков внутри компании. Пользователь запрашивает базу данных аппаратных ресурсов с полным перечнем оборудования компании и пользуется этой информацией в ходе анализа рисков. Какой вид анализа рисков можно применить в данном случае?

количественный

Пользователю поручили оценить степень защищенности компании. Пользователь анализирует предпринятые ранее попытки проникновения в корпоративную сеть, выявляя угрозы и риски, чтобы составить отчет. Какой вид анализа рисков можно применить в данном случае?

качественный

Глава 7. Контрольная работа

Пользователь обращается в службу поддержки с жалобой на то, что приложение, которое было установлено на компьютер, не может подключиться к Интернету. Антивирусное ПО не выдает никаких предупреждений, при этом пользователь свободно открывает интернет-страницы в браузере. Укажите наиболее вероятную причину проблемы.

межсетевой экран

Пользователь предлагает приобрести для организации систему управления обновлениями. Это предложение нужно подкрепить аргументами. Какие преимущества обеспечивает система управления обновлениями? (Выберите три варианта.)

От установки обновлений невозможно отказаться.

Администраторы получают возможность одобрять или отклонять исправления. Можно незамедлительно запустить обновление систем.

По какой причине алгоритм WEP не рекомендуется к использованию в современных беспроводных сетях?
алгоритм легко взламывается

В чем разница между системой обнаружения вторжений на базе хостов (HIDS) и межсетевым экраном? Это правильный ответ
HIDS отслеживают состояние операционных систем на компьютерах и анализируют операции файловой системы. Межсетевые экраны пропускают или отбрасывают входящий и исходящий трафик между оконечным устройством и другими системами.

Перед руководителем службы поддержки настольных систем стоит следующая задача: нужно сократить время простоя рабочих станций, на которых происходят сбои и возникают другие проблемы программного характера. Назовите три преимущества клонирования дисков. (Выберите три варианта.)
возможно создать полную резервную копию системы
возможно создание «чистой» системы из образа
упрощается развертывание новых компьютеров в организации

В чем преимущество протокола WPA2 перед WPA?
обязательное использование алгоритмов AES

В компании довольно много сотрудников, работающих удаленно. Необходимо обеспечить защищенный канал связи для удаленного доступа этих пользователей к сети компании. Какое решение лучше всего подойдет в такой ситуации?
VPN

Назовите три опасные неполадки электропитания с точки зрения технического специалиста. (Выберите три варианта.)
кратковременное исчезновение напряжения
импульсный бросок напряжения
обесточивание

Назовите три вида вредоносного ПО. (Выберите три варианта.)

вирус

троян

кейлоггер

Пользователь обращается в службу поддержки с жалобой на то, что пароль доступа к беспроводной сети изменен без предварительного уведомления. Пользователю разрешают сменить пароль, однако приблизительно через час повторяется то же самое. Что может являться причиной этого?

неавторизованная точка доступа

Пользователь предлагает внедрить в организации службу управления обновлениями. Нужно обосновать это предложение. Назовите три аргумента, которые пользователь мог бы привести в качестве обоснования. (Выберите три варианта.)

получение отчетов о состоянии систем

пользователи не смогут отказаться от установки обновлений

возможность контролировать время установки обновлений

Пользователю поручили проанализировать текущее состояние операционной системы компьютера. Что является эталоном при проверке операционной системы на наличие потенциальных уязвимостей?

снимок базового состояния

Администратору небольшого центра обработки данных требуется функциональное и безопасное средство, чтобы устанавливать удаленные соединения с серверами. Какой протокол лучше всего подойдет в такой ситуации?

Протокол Secure Shell

Стажер начинает работу в отделе поддержки. Одна из его обязанностей — определение локальной политики паролей для рабочих станций. Какое средство лучше всего подходит для решения этой задачи?

secpol.msc

Какой сервис преобразует веб-адрес в IP-адрес целевого веб-сервера?

DNS

Многие компании имеют несколько оперативных центров, занимающихся различными аспектами ИТ. Какой оперативный центр решает проблемы в сетевой инфраструктуре?

NOC

Руководитель подразделения подозревает, что в нерабочее время кто-то пытается получить доступ к компьютерам. Вам поручили разобраться в ситуации. Назовите журнал, ведение которого нужно включить в такой ситуации.

аудит

В ходе аудита безопасности выяснилось, что в системе присутствует несколько учетных записей с привилегированным доступом к системам и устройствам. Какие три лучшие практики для защиты привилегированных учетных записей следует упомянуть в отчете о результатах аудита? (Выберите три варианта.)

Необходимо применять принцип минимальных прав.

Количество учетных записей с привилегированным доступом должно быть минимальным.

Необходимо обеспечить надежное хранение паролей.

ИТ-директор компании поручает специалистам внедрить шифрование данных на корпоративных ноутбуках. Специалисты приходят к выводу, что лучше всего подойдет шифрование всех жестких дисков с помощью Windows BitLocker. Назовите два элемента, которые необходимы для внедрения такого решения. (Выберите два варианта.)

как минимум два тома

TPM

Новый компьютер распаковали, запустили и подключили к Интернету. Все исправления загружены и установлены. Антивирусное ПО обновлено. Что еще можно сделать для укрепления безопасности операционной системы?

Удалить ненужные программы и службы.

В компании хотят внедрить систему биометрического контроля доступа в центр обработки данных. Однако есть опасения возможных сбоев в работе системы, из-за которых посторонние лица будут ошибочно идентифицированы как сотрудники, имеющие право доступа в центр. К какому типу ошибок относится ошибочное признание?

ошибка второго рода

Глава 8. Контрольная работа

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

Закон Грэмма — Лича — Блайли (GLBA)

Какие два вида информации можно найти на веб-сайте Internet Storm Center? (Выберите два варианта.)

Вакансии InfoSec

Отчеты InfoSec

Администратор учебного заведения обеспокоен раскрытием информации о студентах в результате взлома системы. Какой закон защищает данные студентов?

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

В компании произошло несколько инцидентов, когда пользователи загружали несанкционированное ПО, использовали запрещенные веб-сайты и личные USB-накопители. ИТ-директор хочет внедрить схему управления угрозами, исходящими от пользователей. Какие три меры могли бы использоваться для управления угрозами? (Выберите три варианта.)

Фильтрация содержимого

Отключение доступа к CD и USB

Проведение обучения по вопросам безопасности

Компания пытается снизить затраты на развертывание коммерческого программного обеспечения и рассматривает возможность использования облачных служб. Какая облачная служба будет наилучшей для размещения программного обеспечения?

ПО как услуга (SaaS)

Организация внедрила инфраструктуру частного облака. Администратору системы безопасности поручают защитить инфраструктуру от потенциальных угроз. Какие три тактики можно использовать для защиты частного облака? (Выберите три варианта.)

Отключение ping-запросов, зондирования и сканирования портов

Установка на устройства последних исправлений и обновлений для системы

безопасности

Проверка входящего и исходящего трафика

В компании, которая обрабатывает информацию о кредитных картах, происходит нарушение безопасности. Какой отраслевой закон регулирует защиту данных кредитной карты?

Стандарт безопасности данных индустрии платежных карт (PCI DSS)

Специалисту по безопасности предлагают выполнить анализ текущего состояния сети компании. Какой инструмент будет использовать специалист по безопасности для сканирования сети исключительно в целях выявления угроз безопасности?

Сканер уязвимостей

Аудитору предлагают оценить потенциальные угрозы для локальной сети компании. Какие три потенциальные угрозы может отметить аудитор? (Выберите три варианта.)

Несанкционированное сканирование портов и зондирования сети

Неправильно настроенный межсетевой экран

Открытый доступ к сетевому оборудованию

Почему для тестирования безопасности сети организации часто выбирают дистрибутив Kali Linux?

Это дистрибутив Linux с открытым исходным кодом, включающий в себя более 300 инструментов для защиты.

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

Разработка инструментов, продуктов и методик для анализа уязвимостей

Разработка инструментов, продуктов и методик технической экспертизы

Устранения уязвимостей программного обеспечения

Для сбора рекомендаций по защите устройств от угроз компания наняла консультанта. Какие три общие рекомендации можно выявить? (Выберите три варианта.)

Включение блокировки экрана

Отмена административных прав для пользователей

Включение автоматического антивирусного сканирования

Если лицо сознательно получает доступ к компьютеру, который связан с правительством, без разрешения, какие федеральные законы на него распространяются?

Закон о компьютерном мошенничестве (CFAA)

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

Национальная база данных об уязвимостях (NVD)

Специалист по безопасности может иметь доступ к конфиденциальным данным и ресурсам. Что из следующего должен понимать специалист по безопасности для принятия обоснованных, этических решений (выбрать один пункт)?

Законы, регулирующие обработку данных

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

Создающие

Наблюдающие

Определяющие

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

несанкционированный доступ

потеря данных

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

Документация правоохранительных органов, попадающая под перечисленные исключения

Конфиденциальная коммерческая информация

Информация, касающаяся национальной безопасности и внешней политики

Несанкционированные посетители вошли в офис компании и ходят по зданию. Какие две меры могут предотвратить доступ несанкционированных посетителей в здание? (Выберите два варианта.)

Регулярное проведение обучения по вопросам безопасности

Определение правил и процедур для гостей, посещающих здание

Финальный экзамен

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

доверенные партнеры

бывшие сотрудники

К какому типу относится атака, при которой злоумышленники формируют пакеты, маскируемые под обычный сетевой трафик, и таким образом вмешиваются в работу сети?

подделка пакетов

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

«черные» хакеры

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

ISO/IEC 27000

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

беспроводные сети

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?

конфиденциальность, целостность, доступность

Два дня в неделю сотрудники организации имеют право работать удаленно, находясь дома. Необходимо обеспечить конфиденциальность передаваемых данных. Какую технологию следует применить в данном случае?

VPN

Какая из технологий обеспечивает конфиденциальность данных?

шифрование

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?

DoS-атака

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 системы на наличие неавторизованных учетных записей.

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

прослушивание

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

Своевременное обновление операционной системы и остального программного обеспечения.

Установка и своевременное обновление антивирусного ПО.

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?

интернет-червь

К какому типу относится атака, при которой мошеннические веб-сайты размещаются на высоких позициях в списках результатов веб-поиска?

злоупотребление поисковой оптимизацией

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.

программа-вымогатель

Предположим, некие данные необходимо передать третьей стороне для проведения анализа. Какой метод может быть использован вне среды компании для защиты конфиденциальной информации в передаваемых данных путем ее замены?

замена данных путем маскирования

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

изменение младшего бита

Что происходит по мере увеличения длины ключа шифрования?

Пространство ключей экспоненциально увеличивается.

Назовите компонент, представляющий наибольшую сложность при разработке криптосистемы.

управление ключами

В организации планируют провести тренинг по обучению всех сотрудников действующим политикам безопасности. Какой тип контроля доступа стараются применить в организации?

административный

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

средства восстановления

Алиса и Боб обмениваются сообщениями, применяя шифрование с открытым ключом. Каким ключом Алиса должна зашифровать сообщение, адресованное Бобу?

открытый ключ Боба

В какой ситуации требуются средства обнаружения?

в сети организации нужно выявить запрещенную активность

Какую технологию следует внедрить, чтобы пользователь, поставивший подпись под документом, не смог в дальнейшем заявить о том, что не подписывал этот документ?
цифровая подпись

Какой алгоритм хеширования следует использовать для защиты конфиденциальной несекретной информации?
SHA-256

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.)
В одной системе применяется только хеширование, тогда как в другой системе, помимо хеширования, применяется механизм добавления соли. В обеих системах применяется алгоритм MD5.

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».
женщина, 9866, 125,50 $

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

Выяснилось, что один из сотрудников организации взламывает пароли административных учетных записей, чтобы получить доступ к конфиденциальной информации о заработной плате. Что следует искать в операционной системе этого сотрудника? (Выберите три варианта.)
таблицы поиска
радужные таблицы
реверсивные таблицы поиска

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?

цифровые сертификаты

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-256

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

многоуровневый подход

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

изоляция и восстановление

обнаружение и анализ

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

ожидаемый ущерб в результате реализации единичной угрозы

количество реализаций угрозы в год

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?

Нью-Йоркская фондовая биржа

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

отказоустойчивость системы

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

передача риска

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?

повышение надежности и эксплуатационной готовности серверов

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

RAID

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

классификация ресурсов

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

STP

ARP

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

шифрование голосового трафика

Какая из утилит использует протокол ICMP?

ping

Какие атаки можно предотвратить с помощью взаимной аутентификации?

атака через посредника

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

802.11i

WPA

WPA2

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

количество ложноотрицательных результатов и количество ложноположительных результатов

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

WPA2

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

Национальная база данных об уязвимостях (NVD)

Специалисту по безопасности предлагают выполнить анализ текущего состояния сети компании. Какой инструмент будет использовать специалист по безопасности для сканирования сети исключительно в целях выявления угроз безопасности? Верно!

Сканер уязвимостей

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

потеря данных

несанкционированный доступ

Возможные вопросы:

Какие из нижеуказанных мер эффективны в борьбе с киберпреступниками? (Выберите два варианта.)

Обмен результатами анализа киберугроз

Внедрение систем раннего оповещения

Какие три типа данных киберпреступники чаще всего пытаются похитить у организаций? (Выберите три варианта.)

здравоохранение

образование

трудоустройство

К какой категории, согласно классификации NICE Workforce Framework, относится специализированная оценка поступающей информации о кибербезопасности с целью определения ее пригодности для аналитики?

Анализ

При какой атаке цель выводится из строя путем отправки ей огромного количества запросов от множества других систем?

DDoS-атака

При какой атаке компьютер выводится из строя за счет переполнения памяти или перегрузки центрального процессора?

алгоритмическая атака

Как называют хакера, занимающегося взломами ради продвижения некой идеи?

хактивист

Как называют хакеров-дилетантов?

«скрипт-кидди»

Что означает аббревиатура BYOD?

bring your own device (принеси свое устройство)

Что из перечисленного является примером домена данных в Интернете?

LinkedIn

Что означает термин «уязвимость»?

уязвимость, из-за которого целевая система подвержена тем или иным атакам

Что означает аббревиатура IoE?

Internet of Everything (Всеобъемлющий Интернет)

Что из перечисленного относится к первой грани куба кибербезопасности?

цели

Как называется защищенная виртуальная сеть, существующая внутри общедоступной сети?

VPN

Назовите три принципа проектирования, благодаря которым достигается высокая доступность. (Выберите три варианта.)

обеспечение надежного механизма переключения на резервные ресурсы

выявление отказов по мере их возникновения

исключение единых точек отказа

Как называют устройство хранения данных, подключенное к сети?

NAS

Назовите два метода обеспечения доступности систем. (Выберите два варианта.)

своевременное обновление операционных систем

обслуживание оборудования

Назовите три метода идентификации, применяемые в процессе аутентификации. (Выберите три варианта.)

фактор знания

фактор свойства

фактор владения

Назовите три средства контроля доступа. (Выберите три варианта.)

учет

авторизация

аутентификация

Назовите две наиболее распространенные хеш-функции. (Выберите два варианта.)

SHA

MD5

Какой механизм определяет перечень доступных пользователю ресурсов и операций?

учет

авторизация

Назовите два метода проверки целостности данных. (Выберите два варианта.)

хэширование

проверка согласованности данных

Назовите два метода обеспечения конфиденциальности. (Выберите два варианта.)

невозможность отказа

шифрование

аутентификация

К какой категории относятся законы в сфере кибербезопасности, регулирующие раскрытие организациями конфиденциальной информации о вас?

конфиденциальность персональных данных

Какой из принципов подразумевает исключение доступа неавторизованных лиц, ресурсов и процессов к информации?

конфиденциальность

Как называется механизм передачи информации с одного устройства на другое с помощью съемного носителя?

перенос данных вручную

Как называется действие, в результате которого первоначальные данные изменяются (путем изменения пользователями вручную, обработки и изменения этих данных приложениями или их изменения в результате отказа оборудования)?

модификация

Назовите три задачи, которые должна решать комплексная политика безопасности. (Выберите три варианта.)

установление правил ожидаемого поведения

определение правовых последствий нарушений

создание инструментов управления для специалистов по информационной безопасности

Какой механизм можно применить в организации в качестве средства защиты от непреднамеренного изменения информации авторизованными пользователями?

управление версиями

Каковы три основных принципа кибербезопасности? (Выберите три варианта.)

конфиденциальность

доступность

целостность

Назовите три состояния данных. (Выберите три варианта.)

неактивные

передаваемые

обрабатываемые

Назовите три вида конфиденциальной информации. (Выберите три варианта.) публичная

персональные данные

государственная тайна

коммерческая информация

Что из перечисленного относится к первой грани куба кибербезопасности?

цели

Как называется защищенная виртуальная сеть, существующая внутри общедоступной сети?

VPN

Назовите три принципа проектирования, благодаря которым достигается высокая доступность. (Выберите три варианта.)

обеспечение надежного механизма переключения на резервные ресурсы

выявление отказов по мере их возникновения

исключение единых точек отказа

Как называют устройство хранения данных, подключенное к сети?

NAS

Назовите два метода обеспечения доступности систем. (Выберите два варианта.)

своевременное обновление операционных систем

обслуживание оборудования

Назовите три метода идентификации, применяемые в процессе аутентификации. (Выберите три варианта.)

фактор знания

фактор свойства

фактор владения

Назовите три средства контроля доступа. (Выберите три варианта.)

учет

авторизация

аутентификация

Назовите две наиболее распространенные хеш-функции. (Выберите два варианта.)

SHA

MD5

Какой механизм определяет перечень доступных пользователю ресурсов и операций?

учет

авторизация

Назовите два метода проверки целостности данных. (Выберите два варианта.)

хэширование

проверка согласованности данных

Назовите два метода обеспечения конфиденциальности. (Выберите два варианта.)

невозможность отказа

шифрование

аутентификация

К какой категории относятся законы в сфере кибербезопасности, регулирующие раскрытие организациями конфиденциальной информации о вас?

конфиденциальность персональных данных

Какой из принципов подразумевает исключение доступа неавторизованных лиц, ресурсов и процессов к информации?

конфиденциальность

Как называется механизм передачи информации с одного устройства на другое с помощью съемного носителя?

перенос данных вручную

Как называется действие, в результате которого первоначальные данные изменяются (путем изменения пользователями вручную, обработки и изменения этих данных приложениями или их изменения в результате отказа оборудования)?

модификация

Назовите три задачи, которые должна решать комплексная политика безопасности. (Выберите три варианта.)

установление правил ожидаемого поведения

определение правовых последствий нарушений

создание инструментов управления для специалистов по информационной безопасности

Какой механизм можно применить в организации в качестве средства защиты от непреднамеренного изменения информации авторизованными пользователями?

управление версиями

Каковы три основных принципа кибербезопасности? (Выберите три варианта.)

конфиденциальность

доступность

целостность

Назовите три состояния данных. (Выберите три варианта.)

неактивные

передаваемые

обрабатываемые

Назовите три вида конфиденциальной информации. (Выберите три варианта.) публичная

персональные данные

государственная тайна

коммерческая информация

Злоумышленник применяет специальное ПО, чтобы получить информацию о компьютере пользователя. К какой категории относится такое ПО?

шпионское ПО

Назовите две тактики социальной инженерии, применяемые для получения персональных данных от ничего не подозревающей жертвы? (Выберите два варианта.)

принуждение

срочность

Назовите два способа защиты компьютера от вредоносного ПО. (Выберите два варианта.)

Своевременное обновление ПО.

Установка антивирусного ПО.

Как называют сценарий, при котором злоумышленник отправляет мошенническое электронное сообщение, выдавая его за сообщение из надежного источника?

фишинг

По каким двум причинам протокол WEP считается ненадежным? (Выберите два варианта.) У всех устройств в сети разные ключи.

Ключ передается в виде отрытого текста.

Ключ является статическим и неизбежно повторяется в сетях с большим количеством устройств.

Злоумышленник находится около магазина и с помощью беспроводной связи копирует адреса электронной почты и списки контактов с устройств ничего не подозревающих

прохожих. К какому типу относится такая атака?

блюснарфинг

Как называют атаку, при которой электронное сообщение адресуется конкретному сотруднику финансового учреждения?

направленный фишинг

Что означает термин «логическая бомба»?

программа, выполняющая вредоносный код при определенных условиях

Как называют программу или код для обхода стандартного механизма аутентификации?

бэкдор

Что именно модифицируют руткиты?

операционную систему

Что происходит на компьютере, если объем данных превышает пределы буфера?

переполнение буфера

Пользователь видит на экране сообщение о том, что доступ к данным закрыт и будет восстановлен только после уплаты некоторой денежной суммы. К какой категории относится вредоносное ПО, выводящее такие сообщения?

программа-вымогатель

К какому типу относятся атаки, при которых для доступа к базе данных SQL используется поле, в которое пользователь обычно вводит информацию?

Внедрение SQL-кода

Как называется ПО, которое демонстрирует всплывающие окна с рекламой, тем самым принося доход его авторам?

рекламное ПО

Чем вирусы отличаются от интернет-червей?

Интернет-черви могут распространять копии самих себя без участия пользователя. Вирусы не имеют такой способности.

Как называется уязвимость, посредством которой злоумышленники внедряют сценарии в веб-страницы, просматриваемые пользователями?

Межсайтовый скриптинг

Назовите два основных признака спам-письма. (Выберите два варианта.)

Не указана тема письма.

Орфографические и/или пунктуационные ошибки.

Как называют атаку, при которой злоумышленник отправляет короткое SMS-сообщение, обманом вынуждающее жертву посетить веб-сайт?

смишинг

Как называется метод шифрования, при котором криптограмму получают путем перестановки букв?

перестановка

Как называется технология замены конфиденциальной информации на неконфиденциальную версию этой информации?

маскирование

Сопоставьте описания с соответствующими терминами. (Не все утверждения применимы.)

стеганография:

сокрытие данных внутри аудиофайла

стегоанализ:

обнаружение скрытой информации внутри графического файла

социальная стеганография:

создание сообщения, которое содержит скрытый смысл, понятный лишь конкретной целевой аудитории

обфускация:

создание запутанного сообщения, которое трудно понять

Как называется вид шифрования, при котором каждый бит или байт открытого текста обрабатывается отдельно?

поточное

При каждом входе в систему пользователь видит предупреждающее сообщение с перечнем негативных последствий нарушения правил, предусмотренных политиками компании. К какому типу относится данное средство контроля доступа?

сдерживающие

Какой из асимметричных алгоритмов определяет схему электронной передачи общего секретного ключа?

алгоритм Диффи-Хеллмана

Назовите три протокола, в которых применяются асимметричные алгоритмы шифрования. (Выберите три варианта.)

Протокол Secure Shell (SSH)

Протокол SSL

Pretty Good Privacy (PGP)

При каком шифровании данные шифруются одним ключом, а расшифровываются — другим?

асимметричное

Назовите три процесса, которые относятся к категории логических средств контроля доступа? (Выберите три варианта.)

мониторинг трафика с помощью межсетевых экранов

выявление подозрительной активности в сети с помощью системы обнаружения вторжений Cisco IDS

проверка физических характеристик с помощью систем биометрической идентификации

При каком алгоритме шифрования применяется один и тот же общий PSK-ключ, чтобы зашифровать и расшифровать данные?

симметричное

Как называется технология защиты программного обеспечения от несанкционированного доступа или модификации?

цифровой водяной знак

Назовите три вида устройств, которые относятся к категории физических средств контроля доступа. (Выберите три варианта.)

карты с магнитной полосой

видеокамеры

замки

Какой криптографический алгоритм применяется в АНБ и подразумевает использование эллиптических кривых для формирования цифровых подписей и обмена ключами?

ECC

Как называется наука о создании и взломе шифров?

криптология

Как называется способ сокрытия данных путем их внедрения в некоторый файл (например, графический, звуковой или текстовый)?

стеганография

Расположите типы многофакторной аутентификации напротив соответствующих описаний.

ключ-брелок безопасности:

фактор владения

сканирование отпечатка пальца:

фактор свойства

пароль:

фактор знания

Какой алгоритм блочного шифрования с длиной блока в 128 бит применяется в государственных органах США для защиты секретной информации?

AES

Выберите три примера административных средств контроля доступа. (Выберите три варианта.)

практики найма сотрудников

проверка биографии

политики и процедуры

Какие два термина применяются для описания ключей шифрования? (Выберите два варианта.)

длина ключа

пространство ключей

При каком шифровании блок открытого текста фиксированной длины может быть в любой момент времени преобразован в 128-битный блок криптограммы?

блочное

Назовите три проверочных критерия, которые применяются в правилах проверки ввода данных. (Выберите три варианта.)

диапазон

размер

формат

Причиной недавней утечки данных в компании стала уязвимость, из-за которой хакер смог получить доступ к корпоративной базе данных через веб-сайт компании, вводя некорректные данные в форму для входа в систему. Какая проблема присутствует на веб-сайте компании?

неэффективный механизм проверки ввода

Пользователь получает от руководителя указание: необходимо найти эффективный метод для защиты паролей в процессе их передачи. Пользователь изучил несколько вариантов и остановился на механизме HMAC. Назовите ключевые элементы, необходимые для внедрения механизма HMAC.

секретный ключ и хеш-сумма

Назовите три ситуации, в которых можно применить хеш-функцию. (Выберите три варианта.)

CHAP

IPsec

PKI

Следователь обнаружил на месте преступления USB-накопитель и намерен представить его в суде в качестве вещественного доказательства. Следователь создает образ этого USB-накопителя для криминалистического анализа и рассчитывает хеш-сумму для созданного образа и самого устройства USB. Какой факт следователь пытается доказать применительно к USB-накопителю, который будет представлен в суде?
Данные, содержащиеся в образе, являются точной копией данных с накопителя и не были изменены в процессе снятия копии.

В какой последовательности следует выполнять действия при создании цифровой подписи?
Создать хеш-сумму; зашифровать хеш-сумму закрытым ключом отправителя; объединить сообщение, зашифрованную хеш-сумму и открытый ключ и таким образом сформировать подпись для документа.

В электронном письме, которое было разослано внутри компании, говорится о том, что в ближайшее время будут внесены изменения в политику безопасности. Сотрудник службы безопасности, с адреса которого якобы отправлено это письмо, сообщает, что служба безопасности компании не рассылала таких писем и что в сети компании, по-видимому, имела место рассылка с подменой адреса отправителя. Что можно было добавить в сообщение, чтобы впоследствии иметь возможность точно определить, было ли это письмо отправлено сотрудником службы безопасности?
цифровая подпись

Пользователь создал программу и желает передать ее всем сотрудникам компании. При этом необходимо гарантировать, что программа не будет изменена в процессе ее загрузки. Каким образом можно обеспечить уверенность в том, что программа не была изменена в ходе ее загрузки?
Вычислить хеш-сумму файла программы, которая может быть использована для проверки целостности файла после его загрузки.

Назовите наиболее важное свойство хеш-функции.
Хеш-функция необратима.

У Алисы и Боба одинаковые пароли для входа в корпоративную сеть. Соответственно, хеш-суммы паролей также одинаковы. Каким образом можно создать различные хеш-суммы для одинаковых паролей?

добавление соли

Пользователь устанавливает соединение с сервером интернет-магазина, чтобы закупить нужные виджеты для компании. Установив соединение с веб-сайтом, пользователь обращает внимание на то, что в строке состояния безопасности браузера отсутствует значок замка. Веб-сайт запрашивает имя пользователя и пароль. Пользователь вводит их, успешно входит на сайт и намерен выполнить транзакцию. Какая возникает опасность?

На веб-сайте отсутствует цифровой сертификат для защиты транзакции, поэтому данные передаются в незашифрованном виде.

Назовите три вида атак, которые можно предотвратить за счет добавления соли? (Выберите три варианта.)

радужные таблицы

таблицы поиска

реверсивные таблицы поиска

Какой метод подразумевает поиск пароля путем перебора всех возможных комбинаций?

атака методом грубой силы

Пользователь оценивает инфраструктуру безопасности компании и обращает внимание на то, что в некоторых системах аутентификации применяются не самые лучшие методы хранения паролей. Пользователь может легко взломать пароли и получить доступ к конфиденциальным данным. Пользователь намерен представить рекомендацию руководству компании по реализации метода добавления соли, который поможет предотвратить взлом паролей. Назовите три лучшие практики добавления случайных данных в виде соли. (Выберите три варианта.)

Соль должна быть уникальной.

Не использовать одну и ту же соль многократно.

Добавлять уникальную соль к каждому паролю.

Пользователь выполняет обязанности администратора баз данных. Этому пользователю поручили внедрить правило обеспечения целостности, согласно которому каждая

таблица должна иметь первичный ключ, при этом столбец или столбцы, играющие роль первичного ключа, должны содержать уникальные ненулевые значения. Какое требование к целостности реализует этот пользователь?

сущностная целостность

Назовите три алгоритма создания цифровой подписи, одобренные институтом NIST. (Выберите три варианта.)

RSA

DSA

ECDSA

Пользователь загружает с веб-сайта новую версию драйвера для видеокарты. На экране появляется сообщение о том, что драйвер из непроверенного источника. Что отсутствует в загруженном драйвере?

цифровая подпись

Как называется стандарт инфраструктуры открытых ключей для работы с цифровыми сертификатами?

x.509

Пользователю поручили внедрить набор протоколов IPsec для входящих внешних соединений. В качестве одного из компонентов пользователь планирует применить алгоритм SHA-1. При этом необходимо гарантировать целостность и подлинность соединения. Какое средство обеспечения безопасности следует выбрать?

HMAC

Для чего применяется криптографически стойкий генератор псевдослучайных чисел?

генерирование соли

Пользователю поручили оценить сетевую инфраструктуру компании. Пользователь обнаружил, что для многих систем и устройств предусмотрено резервирование, но при этом отсутствует общая оценка сети. В своем отчете пользователь описывает целостную систему методов и конфигураций, которую необходимо применить, чтобы добиться полной отказоустойчивости сети. О какой конструкции сети идет речь в отчете пользователя?

отказоустойчивая

Пользователь приобретает новый сервер для центра обработки данных. Пользователь намерен применить массив из трех дисков с чередованием данных и контролем четности. Какой уровень RAID следует выбрать?

5

Пользователь реорганизует сеть небольшой компании и намерен обеспечить безопасность, не выходя за рамки небольшого бюджета. Между сетью компании и сетью интернет-провайдера пользователь помещает новый межсетевой экран, который снабжен системой обнаружения вторжений и функционирует с учетом особенностей используемого программного обеспечения. Кроме того, пользователь отделяет сеть компании от общедоступной сети с помощью второго межсетевого экрана. При этом во внутренней сети компании пользователь развертывает систему предотвращения вторжений IPS. Какой подход применяется в данном случае?

многоуровневый

Пользователь принят на работу в службу безопасности компании. Ему поручают первый проект — нужно инвентаризировать аппаратные ресурсы компании и создать всеобъемлющую базу данных. Назовите три категории информации, которые следует включить в базу данных аппаратных ресурсов. (Выберите три варианта.)

аппаратные сетевые устройства

рабочие станции

операционные системы

Компания нанимает специалиста по обеспечению высокой доступности сетевой инфраструктуры. Он намерен внедрить в сеть механизмы резервирования на случай отказа коммутаторов, но при этом желает исключить петли на уровне 2. Что нужно применить в такой ситуации?

протокол STP

Пользователь проводит плановый аудит аппаратного обеспечения серверов в центре обработки данных. На нескольких серверах применяется следующая конфигурация: операционная система находится на отдельном накопителе, тогда как данные хранятся в подключенных системах хранения различных типов. Пользователь намерен предложить более эффективное решение, которое позволит избежать отказа в случае выхода из строя

накопителя. Какое решение будет наилучшим?

RAID

Группе специалистов поручили разработать план реагирования на события безопасности. На каком этапе разработки плана группа должна согласовать план с руководством организации?

подготовка

Пользователю поручили добавить резервирование маршрутизаторов в сети компании. Назовите три варианта решения этой задачи. (Выберите три варианта.)

VRRP

GLBP

HSRP

В крупной корпорации произошло нарушение безопасности. Соответствующая группа специалистов предприняла необходимые действия согласно плану реагирования на инциденты. На каком этапе следует применить опыт, полученный при реагировании на этот инцидент?

мероприятия после инцидента

В сети компании обнаружен подозрительный трафик. В компании опасаются, что источником этого трафика является вредоносное ПО, которое не было заблокировано или удалено антивирусом. Какая технология поможет обнаружить в сети трафик, генерируемый вредоносным ПО?

IDS

Пользователю поручили оценить производительность центра обработки данных, чтобы повысить уровень доступности услуг для заказчиков. Пользователь отмечает следующие особенности: имеется лишь одно подключение к интернет-провайдеру; в парке оборудования присутствуют устройства с истекшим гарантийным сроком; запасные компоненты отсутствуют; никто не следит за ИБП, который дважды отключался в течение месяца. Таким образом, пользователь обнаружил три недочета, которые негативно влияют на доступность услуг. Назовите их. (Выберите три варианта.)

присутствуют единые точки отказа

не налажена система выявления ошибок по мере их возникновения

при проектировании не учтены требования к надежности

Пользователю поручили разработать для организации план аварийного восстановления. Для решения этой задачи пользователь должен получить от руководителей организации ответы на некоторые вопросы. Назовите три вопроса, которые пользователь должен задать руководству организации, чтобы правильно составить план. (Выберите три варианта.)

Кто несет ответственность за процесс?

Опишите процесс.

Где именно ответственное лицо реализует этот процесс?

Консультанту предстоит подготовить доклад для Правительства о том, в каких сферах необходимо гарантировать доступность систем на уровне «пять девяток». Назовите три отрасли, которые нужно включить в этот отчет. (Выберите три варианта.)

общественная безопасность

финансовый сектор

здравоохранение

Генеральный директор компании обеспокоен правовыми последствиям утечки данных. Если это произойдет, заказчики могут начать судебное разбирательство из-за разглашения конфиденциальной информации. В связи с этим генеральный директор принимает решение о приобретении соответствующего страхового полиса. К какому типу относится такая мера по снижению рисков?

передача риска

Пользователь выполнил шестимесячный проект: нужно было определить местоположение всех данных и составить список выявленных хранилищ. Следующий этап — классификация данных и формирование критериев их конфиденциальности. Назовите два шага, которые следует выполнить при классификации данных. (Выберите два варианта.)

Определить владельца данных.

Определить степень конфиденциальности данных.

Пользователю поручили провести анализ рисков внутри компании. Пользователь запрашивает базу данных аппаратных ресурсов с полным перечнем оборудования компании и пользуется этой информацией в ходе анализа рисков. Какой вид анализа рисков можно применить в данном случае?

количественный

Пользователю поручили оценить степень защищенности компании. Пользователь анализирует предпринятые ранее попытки проникновения в корпоративную сеть, выявляя угрозы и риски, чтобы составить отчет. Какой вид анализа рисков можно применить в данном случае?

качественный

Пользователь обращается в службу поддержки с жалобой на то, что приложение, которое было установлено на компьютер, не может подключиться к Интернету. Антивирусное ПО не выдает никаких предупреждений, при этом пользователь свободно открывает интернет-страницы в браузере. Укажите наиболее вероятную причину проблемы.

межсетевой экран

Пользователь предлагает приобрести для организации систему управления обновлениями. Это предложение нужно подкрепить аргументами. Какие преимущества обеспечивает система управления обновлениями? (Выберите три варианта.)

От установки обновлений невозможно отказаться.

Администраторы получают возможность одобрять или отклонять исправления.

Можно незамедлительно запустить обновление систем.

По какой причине алгоритм WEP не рекомендуется к использованию в современных беспроводных сетях?

алгоритм легко взламывается

В чем разница между системой обнаружения вторжений на базе хостов (HIDS) и межсетевым экраном? Это правильный ответ

HIDS отслеживают состояние операционных систем на компьютерах и анализируют операции файловой системы. Межсетевые экраны пропускают или отбрасывают входящий и исходящий трафик между оконечным устройством и другими системами.

Перед руководителем службы поддержки настольных систем стоит следующая задача: нужно сократить время простоя рабочих станций, на которых происходят сбои и возникают другие проблемы программного характера. Назовите три преимущества клонирования дисков. (Выберите три варианта.)

возможно создать полную резервную копию системы

возможно создание «чистой» системы из образа

упрощается развертывание новых компьютеров в организации

В чем преимущество протокола WPA2 перед WPA?

обязательное использование алгоритмов AES

В компании довольно много сотрудников, работающих удаленно. Необходимо обеспечить защищенный канал связи для удаленного доступа этих пользователей к сети компании. Какое решение лучше всего подойдет в такой ситуации?

VPN

Назовите три опасные неполадки электропитания с точки зрения технического специалиста. (Выберите три варианта.)

кратковременное исчезновение напряжения

импульсный бросок напряжения

обесточивание

Назовите три вида вредоносного ПО. (Выберите три варианта.)

вирус

троян

кейлоггер

Пользователь обращается в службу поддержки с жалобой на то, что пароль доступа к беспроводной сети изменен без предварительного уведомления. Пользователю разрешают сменить пароль, однако приблизительно через час повторяется то же самое. Что может являться причиной этого?

неавторизованная точка доступа

Пользователь предлагает внедрить в организации службу управления обновлениями. Нужно обосновать это предложение. Назовите три аргумента, которые пользователь мог

бы привести в качестве обоснования. (Выберите три варианта.)

получение отчетов о состоянии систем

пользователи не смогут отказаться от установки обновлений

возможность контролировать время установки обновлений

Пользователю поручили проанализировать текущее состояние операционной системы компьютера. Что является эталоном при проверке операционной системы на наличие потенциальных уязвимостей?

снимок базового состояния

Администратору небольшого центра обработки данных требуется функциональное и безопасное средство, чтобы устанавливать удаленные соединения с серверами. Какой протокол лучше всего подойдет в такой ситуации?

Протокол Secure Shell

Стажер начинает работу в отделе поддержки. Одна из его обязанностей — определение локальной политики паролей для рабочих станций. Какое средство лучше всего подходит для решения этой задачи?

secpol.msc

Какой сервис преобразует веб-адрес в IP-адрес целевого веб-сервера?

DNS

Многие компании имеют несколько оперативных центров, занимающихся различными аспектами ИТ. Какой оперативный центр решает проблемы в сетевой инфраструктуре?

NOC

Руководитель подразделения подозревает, что в нерабочее время кто-то пытается получить доступ к компьютерам. Вам поручили разобраться в ситуации. Назовите журнал, ведение которого нужно включить в такой ситуации.

аудит

В ходе аудита безопасности выяснилось, что в системе присутствует несколько учетных записей с привилегированным доступом к системам и устройствам. Какие три лучшие практики для защиты привилегированных учетных записей следует упомянуть в отчете о результатах аудита? (Выберите три варианта.)

Необходимо применять принцип минимальных прав.

Количество учетных записей с привилегированным доступом должно быть минимальным.

Необходимо обеспечить надежное хранение паролей.

ИТ-директор компании поручает специалистам внедрить шифрование данных на корпоративных ноутбуках. Специалисты приходят к выводу, что лучше всего подойдет шифрование всех жестких дисков с помощью Windows BitLocker. Назовите два элемента, которые необходимы для внедрения такого решения. (Выберите два варианта.)

как минимум два тома

TPM

Новый компьютер распаковали, запустили и подключили к Интернету. Все исправления загружены и установлены. Антивирусное ПО обновлено. Что еще можно сделать для укрепления безопасности операционной системы?

Удалить ненужные программы и службы.

В компании хотят внедрить систему биометрического контроля доступа в центр обработки данных. Однако есть опасения возможных сбоев в работе системы, из-за которых посторонние лица будут ошибочно идентифицированы как сотрудники, имеющие право доступа в центр. К какому типу ошибок относится ошибочное признание?

ошибка второго рода

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

Закон Грэмма — Лича — Блайли (GLBA)

Какие два вида информации можно найти на веб-сайте Internet Storm Center? (Выберите два варианта.)

Вакансии InfoSec

Отчеты InfoSec

Администратор учебного заведения обеспокоен раскрытием информации о студентах в результате взлома системы. Какой закон защищает данные студентов?

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

В компании произошло несколько инцидентов, когда пользователи загружали несанкционированное ПО, использовали запрещенные веб-сайты и личные USB-накопители. ИТ-директор хочет внедрить схему управления угрозами, исходящими от пользователей. Какие три меры могли бы использоваться для управления угрозами? (Выберите три варианта.)

Фильтрация содержимого

Отключение доступа к CD и USB

Проведение обучения по вопросам безопасности

Компания пытается снизить затраты на развертывание коммерческого программного обеспечения и рассматривает возможность использования облачных служб. Какая облачная служба будет наилучшей для размещения программного обеспечения?

ПО как услуга (SaaS)

Организация внедрила инфраструктуру частного облака. Администратору системы безопасности поручают защитить инфраструктуру от потенциальных угроз. Какие три тактики можно использовать для защиты частного облака? (Выберите три варианта.)

Отключение ping-запросов, зондирования и сканирования портов

Установка на устройства последних исправлений и обновлений для системы безопасности

Проверка входящего и исходящего трафика

В компании, которая обрабатывает информацию о кредитных картах, происходит нарушение безопасности. Какой отраслевой закон регулирует защиту данных кредитной карты?

Стандарт безопасности данных индустрии платежных карт (PCI DSS)

Специалисту по безопасности предлагают выполнить анализ текущего состояния сети компании. Какой инструмент будет использовать специалист по безопасности для сканирования сети исключительно в целях выявления угроз безопасности?

Сканер уязвимостей

Аудитору предлагают оценить потенциальные угрозы для локальной сети компании. Какие три потенциальные угрозы может отметить аудитор? (Выберите три варианта.)

Несанкционированное сканирование портов и зондирования сети

Неправильно настроенный межсетевой экран

Открытый доступ к сетевому оборудованию

Почему для тестирования безопасности сети организации часто выбирают дистрибутив Kali Linux?

Это дистрибутив Linux с открытым исходным кодом, включающий в себя более 300 инструментов для защиты.

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

Разработка инструментов, продуктов и методик для анализа уязвимостей

Разработка инструментов, продуктов и методик технической экспертизы

Устранения уязвимостей программного обеспечения

Для сбора рекомендаций по защите устройств от угроз компания наняла консультанта. Какие три общие рекомендации можно выявить? (Выберите три варианта.)

Включение блокировки экрана

Отмена административных прав для пользователей

Включение автоматического антивирусного сканирования

Если лицо сознательно получает доступ к компьютеру, который связан с правительством, без разрешения, какие федеральные законы на него распространяются?

Закон о компьютерном мошенничестве (CFAA)

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

Национальная база данных об уязвимостях (NVD)

Специалист по безопасности может иметь доступ к конфиденциальным данным и ресурсам. Что из следующего должен понимать специалист по безопасности для принятия обоснованных, этических решений (выбрать один пункт)?

Законы, регулирующие обработку данных

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

Создающие

Наблюдающие

Определяющие

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

несанкционированный доступ

потеря данных

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

Документация правоохранительных органов, попадающая под перечисленные исключения

Конфиденциальная коммерческая информация

Информация, касающаяся национальной безопасности и внешней политики

Несанкционированные посетители вошли в офис компании и ходят по зданию. Какие две меры могут предотвратить доступ несанкционированных посетителей в здание? (Выберите два варианта.)

Регулярное проведение обучения по вопросам безопасности

Определение правил и процедур для гостей, посещающих здание