Сертифицированный специалист по кибербезопасности – экзамен для лидеров кибербезопасности

Сертификация «Сертифицированный специалист по кибербезопасности» (ССК)- первая российская сертификация по кибербезопасности.

Примерные вопросы

Менеджмент информационной безопасности

Вопрос 1.

Петр разрабатывает план обеспечения непрерывности бизнеса и испытывает трудности с определением приоритетности ресурсов из-за сложности объединения информации о материальных и нематериальных активах. Какой подход к оценке рисков будет для него наиболее эффективным?

a) Количественная оценка рисков
b) Качественная оценка риска
c) Ни количественная, ни качественная оценка рисков
d) Комбинация количественной и качественной оценки рисков

Вопрос 2.

Что из перечисленного ниже является примером организационной меры?

a) Система обнаружения вторжений
b) Программа повышения осведомленности пользователей в сфере ИБ
c) МЭ
d) Физическая охрана

Вопрос 3.

Компания оценивает риски информационной безопасности. Что из нижеперечисленного противоречит ГОСТ Р ИСО 27001:

a) Проведение оценки вероятности и последствий каждого идентифицированного риска
b) Сравнение рисков с заранее определенным набором критериев
c) Консультации с отраслевыми экспертами для определения потенциальных рисков
d) Игнорирование рисков, которые имеют низкую вероятность возникновения

Вопрос 4.

Дарья помогает пользователю, на экране которого появилось сообщение, в котором предлагается связаться со злоумышленниками для получения ключа для расшифрования файлов. На какое свойство информации нацелена осуществившаяся угроза?

a) Доступность
b) Конфиденциальность
c) Раскрытие информации
d) Подотчетность

Вопрос 5.

Кирилл проводит оценку рисков для своей организации и пытается назначить стоимость активов для серверов в центре обработки данных. Основной его задачей является обеспечить резерв средств для восстановления центра обработки данных в случае его повреждения или

уничтожения. Какой из следующих методов оценки активов будет наиболее подходящим в данной ситуации?

a) Закупочная стоимость
b) Амортизированная стоимость
c) Стоимость замещения
d) Стоимость возможностей

Законодательство в области информационной безопасности

Вопрос 6.

Какой нормативный документ ФСТЭК России определяет требования к созданию систем безопасности значимых объектов критической информационной инфраструктуры РФ и обеспечению их функционирования?

a) 17 приказ ФСТЭК России
b) 21 приказ ФСТЭК России
c) 239 приказ ФСТЭК России
d) 235 приказ ФСТЭК России

Вопрос 7.

В каких нормативных документах закреплена обязанность передавать сведения об инцидентах информационной безопасности в ГОССОПКА?

a) 17,21 приказы ФСТЭК России
b) 187-ФЗ, 152-ФЗ
c) 235, 239 приказы ФСТЭК России
d) Указ Президента РФ от 15.01.2013 №31с

Вопрос 8.

Каким способом правового регулирования является предоставление лицу права на определенное собственное поведение, на совершение тех или иных действий?

a) Запрещение
b) Обязывание
c) Дозволение
d) Предотвращение

Вопрос 9.

Какие виды правовых документов обладают высшей юридической силой?

a) Ведомственные акты
b) Указы президента
c) Акты правительства
d) Законы

Вопрос 10.

Согласие субъекта персональных данных на обработку его персональных данных в письменном виде форме может не включать в себя:

a) фамилию, имя, отчество, адрес субъекта персональных данных, номер основного документа, удостоверяющего его личность, сведения о дате выдачи указанного документа и выдавшем его органе
b) ИНН оператора, получающего согласие субъекта персональных данных
c) цель обработки персональных данных
d) перечень персональных данных, на обработку которых дается согласие субъекта персональных данных

Безопасный доступ

Вопрос 11.

Распознавание голоса каким фактором аутентификации является?

a) То, что вы знаете
b) То, что у вас есть
c) То, кем вы являетесь
d) То, где вы находитесь

Вопрос 12.

Какой тип контроля доступа позволяет владельцу файла предоставлять доступ к нему другим пользователям, используя список управления доступом?

a) Ролевой
b) Недискреционный
c) Основанный на правилах
d) Дискреционный

Вопрос 13.

Каков наилучший способ обеспечения подотчетности использования идентификационных данных?

a) Журналирование
b) Авторизация
c) Цифровые подписи
d) Аутентификация типа 1

Вопрос 14.

В ходе тестирования на проникновение Мария обнаруживает файл, содержащий хэшированные пароли для системы, к которой она пытается получить доступ. Какой тип атаки будет скорее всего наиболее успешным в данном случае?

a) Атака методом полного перебора
b) Атака pass-the-hash
c) Атака с использование радужных таблиц
d) Восстановление salt-значения

Вопрос 15.

Иван начинает работать на новом месте и обнаруживает, что у него административный доступ к ряду систем. С какой проблемой он столкнулся?

a) Ущемление привилегий пользователей
b) Коллизия прав

c) Нарушение принципа «наименьшей привилегии»
d) Нарушение принципа «нужно знать»

Сетевая безопасность

Вопрос 16.

Петр настраивает СОВ для отслеживания незашифрованного FTP-трафика. Какие порты следует Петру использовать при конфигурации сигнатур?

a) TCP 20 и 21
b) Только TCP 21
c) UDP-порт 69
d) TCP-порт 21 и UDP-порт 21

Вопрос 17.

Если VPN предоставляет удаленным пользователям такой же доступ к сетевым и системным ресурсам, как и локальным рабочим станциям, какую проблему безопасности необходимо рассмотреть?

a) Пользователи VPN не смогут получить доступ к веб-серверу.
b) Дополнительных проблем с безопасностью нет; логическое сетевое расположение VPN-концентратора совпадает с логическим сетевым расположением рабочих станций.
c) Трафик веб-сервера не подвергается контролю.
d) Пользователи VPN должны подключаться только с контролируемых ПК.

Вопрос 18.

Во время устранения неполадок Полина использует команду nslookup, чтобы проверить IP-адрес узла по имени узла, к которому она пытается подключиться, но IP-адрес, который она видит в ответе, не является тем IP-адресом, который должен быть на самом деле. Какой тип атаки, скорее всего, был проведен?

a) Подмена DNS
b) ARP-poisoning
c) ARP-спуфинг
d) Снифинг

Вопрос 19.

На каком уровне модели OSI работают ARP и RARP протоколы?

a) Уровень 1
b) Уровень 2
c) Уровень 3
d) Уровень 4

Вопрос 20.

SMTP, HTTP и SNMP находятся на каком уровне модели OSI?

a) Уровень 4
b) Уровень 5
c) Уровень 6

d) Уровень 7

Вопрос 21.

Максим развернул 1-гигабитную сеть 1000BaseT и должен проложить кабель в другое здание. Если Максим прокладывает кабель напрямую от коммутатора к другому коммутатору, то какой может быть максимальная длина кабеля в соответствии со спецификацией 1000BaseT?

a) 2 километра
b) 500 метров
c) 185 метров
d) 100 метров

Криптография

Вопрос 22.

Маша и Петр хотели бы начать общаться с помощью симметричной криптосистемы, но у них нет заранее оговоренного пароля и они не могут встретиться лично, чтобы обменяться ключами. Какой алгоритм они могут использовать для безопасного обмена секретным ключом?

a) IDEA
b) Диффи-Хеллмана
c) RSA
d) MD5

Вопрос 23.

Какой криптографический принцип лежит в основе идеи о том, что криптографические алгоритмы должны быть открыты для изучения?

a) Безопасность через неясность
b) Принцип Керкхоффа
c) Эшелонированная защита
d) Принцип Гейзенбурга

Вопрос 24.

Какая длина ключа предусмотрена алгоритмом «Кузнечик»?

a) 128 бит
b) 256 бит
c) 512 бит
d) 1024 бит

Вопрос 25.

Какое высказывание относительно алгоритма «Магма» является неверным?

a) Это вариант алгоритма ГОСТ 28147-89
b) Это алгоритм ассиметричного шифрования
c) Длина ключа – 256 бит
d) Является частью стандартов ГОСТ Р 34.12-2015 и ГОСТ 34.12-2018

Вопрос 26.

Какой атакой является ситуация, описываемая следующим образом: для осуществления такого типа атаки криптоаналитику необходимо иметь не только какое-то количество открытых

текстов и полученных на их основе шифротекстов, но и обладать возможностью подобрать несколько открытых текстов и получить результат их шифрования?

a) Атака на основе шифротекста
b) Атака на основе открытых текстов и соответствующих шифротекстов
c) Атака на основе подобранного открытого текста
d) Атака на основе подобранного шифротекста

Обеспечение непрерывности бизнеса и восстановления

Вопрос 27.

Вы завершаете работу по планированию непрерывности бизнеса и решили, что хотите принять один из рисков. Что вы должны сделать далее?

a) Внедрить новые меры безопасности, чтобы снизить уровень риска.
b) Разработать план аварийного восстановления.
c) Повторить оценку воздействия на бизнес.
d) Задокументировать процесс принятия решения.

Вопрос 28.

Екатерина разрабатывает отказоустойчивую систему и хочет внедрить RAID уровня 5 для своей системы. Какое минимальное количество физических жестких дисков она может использовать для создания этой системы?

a) Один
b) Два
c) Три
d) Пять

Вопрос 29.

Какую важную функцию обычно выполняют топ-менеджеры в группе планирования непрерывности бизнеса?

a) Урегулирование споров о критичности
b) Оценка правовых аспектов
c) Обучение персонала
d) Разработка мер обеспечения непрерывности бизнеса

Вопрос 30.

Кто должен пройти первоначальное обучение плану обеспечения непрерывности бизнеса в организации?

a) Топ-менеджеры
b) Лица, выполняющие конкретные функции по обеспечению непрерывности бизнеса
c) Все сотрудники организации
d) Генеральный директор

Вопрос 31.

Кто является идеальным лицом для утверждения плана обеспечения непрерывности бизнеса организации?

a) ИТ-директор
b) Генеральный директор

c) Руководитель службы информационной безопасности
d) Исполнительный директор

Вопрос 32.

Какой подход к оценке воздействия на бизнес является наиболее подходящим при попытке оценить влияние прерывания бизнеса на доверие клиентов?

a) Количественный
b) Качественный
c) Ожидаемый годовой размер потерь
d) Структурирование

Контроль защищенности и мониторинг информационной безопасности

Вопрос 33.

Во время сканирования портов с помощью nmap Глеб обнаруживает, что в системе открыты два порта, которые вызывают у него беспокойство:

21/open

23/open

Какие службы, вероятно, работают на этих портах?

a) SSH и FTP
b) FTP и Telnet
c) SMTP и Telnet
d) POP3 и SMTP

Вопрос 34.

Какой идентификатор присваивается уязвимости, когда она регистрируется в базе ФСТЭК России?

a) CVE
b) CVSS
c) BDU
d) CWE

Вопрос 35.

Петр решил проверить возможно ли проэксплуатировать обнаруженную уязвимость. Какой инструмент будет наиболее полезным?

a) Сетевой сканер уязвимостей
b) Metasploit Framework
c) Nikto
d) Netcat

Вопрос 36.

Nmap является примером какого типа инструмента?

a) Сканер уязвимостей
b) Фаззер веб-приложений
c) Инструмент для проектирования сети

d) Сканер портов

Вопрос 37.

Какой тип уязвимостей не может быть обнаружен сканером уязвимостей?

a) Локальные уязвимости
b) Уязвимости в сетевых сервисах
c) Уязвимости нулевого дня
d) Уязвимости, для обнаружения, которых требуется пройти аутентификацию

Вопрос 38.

База данных CVE компании MITRE предоставляет информацию какого типа?

a) Текущие версии программного обеспечения
b) Информация об исправлениях для приложений
c) Информация об уязвимостях
d) Список затрат и усилий, необходимых для выполнения процесса управления уязвимостями

Разработка безопасного программного обеспечения

Вопрос 39.

Что из перечисленного ниже не является целью формальной программы управления изменениями?

a) Осуществлять изменения упорядоченным образом.
b) Тестировать изменения перед внедрением.
c) Формировать планы отката изменений.
d) Информировать заинтересованные стороны об изменениях после их внесения.

Вопрос 40.

Изольда, работающая разработчиком ИТ-компании, должна предоставлять свой код для тестирования и проверки. После того как код пройдет этот процесс и будет одобрен, другой специалист переносит код в производственную среду. Данный процесс представляет собой:

a) Регрессионное тестирование
b) Ревью кода
c) Управление изменениями
d) Фаззинг-тестирование

Вопрос 41.

Во время оценки потенциального инцидента безопасности Дарья натыкается на запись в журнале запросов веб-сервера, показывающую, что пользователь ввел в поле формы следующее: CARROT'&1=1;--. Какой тип атаки был предпринят?

a) Переполнение буфера
b) Межсайтовый скриптинг
c) SQL-инъекция
d) Подделка межсайтовых запросов

Вопрос 42.

Станислав просматривает сообщения на форуме на сайте своей компании и в ходе просмотра диалоговом окне на его экране появляется надпись "Alert". Он просматривает исходный код сообщения и находит следующий фрагмент:

<script>alert('Alert');</script>.

Какая уязвимость определенно существует на данном форуме?

a) Межсайтовый скриптинг
b) Подделка межсайтовых запросов
c) SQL-инъекция
d) Неправильная аутентификация

Вопрос 43.

Иван работает с базой данных DynamoDB. Эта база данных не структурирована как реляционная база данных, но позволяет Ивану хранить данные с помощью хранилища пар ключ-значение. К какому типу баз данных относится DynamoDB?

a) Реляционная база данных
b) Графовая база данных
c) Иерархическая база данных
d) База данных NoSQL