Приложение
к ППССЗ по специальности
09.02.11 Разработка и управление
программным обеспечением

ФОНД ОЦЕНОЧНЫХ СРЕДСТВ
УЧЕБНОЙ ДИСЦИПЛИНЕ
ОП.05 ОСНОВЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ
основной профессиональной образовательной программы
09.02.11 РАЗРАБОТКА И УПРАВЛЕНИЕ ПРОГРАММНЫМ ОБЕСПЕЧЕНИЕМ
Базовая подготовка среднего профессионального образования
Год начала подготовки - 2026

СОДЕРЖАНИЕ

1. Общие положения

Фонд оценочных средств (далее – ФОС) предназначен для контроля и оценки результатов освоения обучающимися учебной дисциплины «Основы информационной безопасности».

ФОС включают контрольные материалы для проведения текущего контроля успеваемости и промежуточной аттестации обучающихся, разработанные в соответствии с требованиями ФГОС СПО и содержанием рабочей программы учебной дисциплины.

2. Результаты освоения учебной дисциплины, подлежащие проверке

Код ОК, ПК	**Уметь**	**Знать**	**Владеть навыками**
ОК.01 Выбирать способы решения задач профессиональной деятельности применительно к различным контекстам	распознавать задачу и/или проблему в профессиональном и/или социальном контексте; анализировать задачу и/или проблему и выделять её составные части; определять этапы решения задачи; выявлять и эффективно искать информацию, необходимую для решения задачи и/или проблемы; составлять план действия; определять необходимые ресурсы; владеть актуальными методами работы в профессиональной и смежных сферах реализовывать составленный план; оценивать результат и последствия своих действий (самостоятельно или с помощью наставника)	актуальный профессиональный и социальный контекст, в котором приходится работать и жить; основные источники информации и ресурсы для решения задач и проблем в профессиональном и/или социальном контексте; алгоритмы выполнения работ в профессиональной и смежных областях; методы работы в профессиональной и смежных сферах; структуру плана для решения задач; порядок оценки результатов решения задач профессиональной деятельности	-
ОК.02 Использовать современные средства поиска, анализа и интерпретации информации, и информационные технологии для выполнения задач профессиональной деятельности	определять задачи для поиска информации; определять необходимые источники информации; планировать процесс поиска; структурировать получаемую информацию; выделять наиболее значимое в перечне информации; оценивать практическую значимость результатов поиска; оформлять результаты поиска, применять средства информационных	номенклатура информационных источников, применяемых в профессиональной деятельности; приемы структурирования информации; формат оформления результатов поиска информации, современные средства и устройства информатизации;	-

	технологий для решения профессиональных задач; использовать современное программное обеспечение; использовать различные цифровые средства для решения профессиональных задач	порядок их применения и программное обеспечение в профессиональной деятельности в том числе с использованием цифровых средств.	
ОК.09 Пользоваться профессиональной документацией на государственном и иностранном языках	понимать тексты на базовые профессиональные темы	лексический минимум, относящийся к описанию предметов, средств и процессов профессиональной деятельности	-
ПК 1.1 Проектировать базы данных.	-	принципы безопасности хранения данных	-
ПК 1.4 Администрировать базы данных	-	методы защиты баз данных от внешних угроз	-
ПК 1.5 Защищать информацию в базе данных с использованием технологии защиты информации.	шифровать данные и обеспечивать их конфиденциальность	принципы криптографии и методов шифрования данных стандарты и протоколы безопасности, таких как SSL/TLS, SSH, Kerberos и др. методы аутентификации и авторизации пользователей, включая использование паролей, сертификатов и биометрических данных законодательство и стандарты безопасности, такие как GDPR, HIPAA, PCI DSS и др.	-
ПК 3.1 Собирать исходные данные для разработки проектной документации на информационную систему.	-	отраслевая нормативная техническая документация источники информации, необходимой для профессиональной	-

		деятельности	
		современный отечественный и зарубежный опыт в профессиональной деятельности	-
ПК 3.2 Разрабатывать проектную документацию на разработку информационной системы в соответствии с требованиями заказчика.	-	принципы и методы обеспечения безопасности информационных систем	-
ПК 3.3 Разрабатывать подсистемы безопасности информационной системы в соответствии с техническим заданием.	анализ требований безопасности информационных систем	принципов безопасности информационных систем современных методов и технологий в области безопасности информационных систем законодательных и нормативных актов в области безопасности информационных систем	применение современных методов и технологий в области безопасности информационных систем
ПК 3.5 Интегрировать информационную систему с существующими информационными системами заказчика.	-	источники угроз информационной безопасности и меры по их предотвращению	-
ПК 3.7 Разрабатывать техническую документацию на эксплуатацию информационной системы.	разрабатывать и реализовывать меры безопасности реализовывать хэширование паролей, сессионные токены и двухфакторную аутентификацию	основные угрозы безопасности мобильных приложений принципы криптографии и шифрования данных. стандарты и протоколы безопасности, такие как HTTPS, OAuth и OpenID Connect законодательные и регуляторные требования к защите данных, включая GDPR и HIPAA основные принципы безопасности информации и методов ее защиты. стандартные	использование шифрования данных для защиты конфиденциальной информации, такой как пароли, персональные данные пользователей и другие чувствительные данные. применение механизмов хеширования для защиты паролей пользователей от несанкционированного доступа. обеспечение безопасности передачи данных между клиентскими

		криптографические алгоритмы для шифрования данных принципы обеспечения безопасности передачи данных по сети основы безопасности приложений и инфраструктуры методы анализа на уязвимости и мониторинга безопасности знание основных принципов и методов обеспечения безопасности ИТ-инфраструктуры и веб-приложений понимание различных уязвимостей и угроз безопасности, а также способов их предотвращения и обнаружения знание инструментов и технологий для обеспечения безопасности ИТ-инфраструктуры и веб-приложений, таких как брандмауэры, системы обнаружения вторжений и антивирусные программы	устройствами и серверами с использованием протоколов шифрования, таких как SSL/TLS соблюдение законодательства и регуляций в области защиты данных

3. Распределение оценивания результатов обучения по видам контроля

<table>
<tr><td rowspan="2">Наименование элемента практического опыта, умений или знаний</td><td colspan="2">Наименование оценочного средства текущего контроля и промежуточной аттестации</td></tr>
<tr><td>Текущий контроль</td><td>Промежуточная аттестация</td></tr>
<tr><td>ПО.1. способен применять теоретические знания на практике при работе с различными операционными системами
ПО.2. умеет анализировать и решать задачи системного администрирования;
ПО.3 готов к освоению новых технологий в области операционных систем и сред</td><td rowspan="4">Компьютерное тестирование на знание терминологии по теме.
Контрольные задания, решение задач по теме.</td><td rowspan="4">Вопросы к зачету</td></tr>
<tr><td>У1. определять задачи для поиска информации; определять необходимые источники информации; планировать процесс поиска; структурировать получаемую информацию;
У2. выделять наиболее значимое в перечне информации; оценивать практическую значимость результатов поиска;
У3. оформлять результаты поиска, применять средства информационных технологий для решения профессиональных задач</td></tr>
<tr><td>З1.номенклатура информационных источников, применяемых в профессиональной деятельности; приемы структурирования информации;
З2. формат оформления результатов поиска информации, современные средства и устройства информатизации;
З3. порядок их применения и программное обеспечение в профессиональной деятельности в том числе с использованием цифровых средств.</td></tr>
</table>

4. Контрольные задания для оценки результатов освоения учебной дисциплины

4.1. Контрольные задания для текущего контроля Раздел

1. Управление безопасностью информации Тестовые задания

1. (OB) Базовая триада информационной безопасности (CIA Triad) включает:
a) Конфиденциальность, целостность, доступность
b) Криптография, идентификация, аутентификация
c) Защита, контроль, аудит
d) Риски, угрозы, уязвимости

2. (MB) Какие из следующих элементов являются компонентами системы управления информационной безопасностью (СМИБ)?
a) Политики и процедуры безопасности
b) Технические средства защиты (брандмауэры, антивирусы)
c) Осведомленность и обучение персонала
d) Процессы управления инцидентами и непрерывностью бизнеса

3. (CO) Процесс выявления, анализа и оценки потенциальных негативных событий, которые могут повлиять на активы организации, называется _____рисков. *Ответ:* _____

4. (OB) Законодательный акт Российской Федерации, который является основным регулятором в области обработки персональных данных, — это:
a) ФЗ-152 «О персональных данных»
b) ФЗ-149 «Об информации, информационных технологиях и о защите информации»
c) ФЗ-187 «О безопасности критической информационной инфраструктуры»
d) УК РФ, глава 28

5. (MB) Какие из перечисленных угроз можно отнести к социальной инженерии?
a) Фишинг (поддельные письма)
b) Вирус-шифровальщик (ransomware)
c) Претекстинг (создание ложного предлога для получения информации)
d) DDoS-атака

6. (OB) Слабость в системе, процедуре или контроле, которой может воспользоваться угроза, называется:
a) Риском
b) Уязвимостью
c) Инцидентом
d) Контрмерой

7. (CO) Тип вредоносного программного обеспечения, которое маскируется под легитимную программу, но выполняет вредоносные действия, называется _____.
Ответ: _____

8. (OB) Атака, при которой злоумышленник перехватывает и, возможно, изменяет связь между двумя сторонами, которые считают, что общаются напрямую, — это:
a) Отказ в обслуживании (DoS)
b) Человек посередине (Man-in-the-Middle, MitM)
c) SQL-инъекция
d) Подбор пароля (Brute-force)

9. (OB) Какой из перечисленных методов является наиболее надежным для

аутентификации?

a) Простой пароль
b) Парольная фраза
c) Двухфакторная аутентификация (2FA)
d) Секретный вопрос

10. (МВ) Какие из перечисленных мер относятся к организационным мерам защиты информации?

a) Разработка и внедрение политики парольной безопасности
b) Установка межсетевого экрана
c) Проведение регулярных тренингов по ИБ для сотрудников

11. Внедрение системы обнаружения вторжений (IDS)(СО) Принцип безопасности, согласно которому пользователь должен получать только те права доступа, которые минимально необходимы для выполнения его рабочих задач, называется принципом ____.

Ответ: _____

12. (ОВ) Криптографический метод, который гарантирует, что полученное сообщение не было изменено в процессе передачи, — это:

a) Шифрование
b) Цифровая подпись
c) Стеганография
d) Хэширование

13. (МВ) Какие из следующих этапов входят в жизненный цикл управления инцидентами информационной безопасности?

a) Подготовка и предотвращение
b) Обнаружение и анализ
c) Сдерживание, ликвидация и восстановление
d) Извлечение уроков и улучшение (постинцидентный анализ)

14. (ОВ) Международный стандарт, который описывает требования к системе управления информационной безопасностью (СМИБ), — это:

a) ISO 9001 (Управление качеством)
b) ISO/IEC 27001
c) ISO 14001 (Экологический менеджмент)
d) PCI DSS (стандарт безопасности данных индустрии платёжных карт)

15. (СО) Процесс регулярной оценки защищенности информационных систем путем моделирования атак с разрешения владельца — это _____тестирование.

Ответ: _____

16. (ОВ) Какой документ определяет порядок действий персонала при возникновении инцидента информационной безопасности?

a) Политика информационной безопасности
b) План непрерывности бизнеса (BCP)
c) Регламент реагирования на инциденты (IRP)
d) Положение об обработке ПДн

17. (МВ) Какие из следующих действий являются обязательными для оператора при обработке персональных данных по ФЗ-152?

a) Получить согласие субъекта ПДн (за исключением установленных случаев)
b) Обеспечить конфиденциальность ПДн
c) Уведомлять Роскомнадзор о начале обработки (если не подпадает под исключения)
d) Назначить ответственного за организацию обработки ПДн

18. (СО) Сокр. GDPR расшифровывается как _____. Это регламент ЕС о защите персональных данных.

Ответ (на русском или английском): _____

19. (ОВ) К какому типу информации, согласно ФЗ-149, относится информация, доступ к которой ограничен федеральными законами (например, персональные данные, коммерческая тайна)?

a) Общедоступная информация
b) Информация ограниченного доступа
c) Государственная тайна
d) Массовая информация

20. (СО) Процесс приведения уровня защищенности информации в соответствие с установленными требованиями регулятора называется _____.

Ответ: _____

Ключ для проверки Раздел 1:

1. **a)** Конфиденциальность, целостность, доступность
2. **a, b, c, d** (Все перечисленное является частью комплексной СМИБ)
3. **оценка** (или **анализ**)
4. **a)** ФЗ-152 «О персональных данных»

Раздел 2:

5. **a, c** (b — вредоносное ПО, d — сетевая атака, социальная инженерия — манипулирование людьми)
6. **b)** Уязвимостью
7. **троян** (троянская программа, trojan)
8. **b)** Человек посередине (Man-in-the-Middle, MitM)

Раздел 3:

9. **c)** Двухфакторная аутентификация (2FA)
10. **a, c** (b и d — технические меры)
11. **наименьших привилегий** (least privilege)
12. **d)** Хэширование (с использованием криптографических хэш-функций для контроля целостности)

Раздел 4:

13. **a, b, c, d** (Все этапы входят в полный жизненный цикл)
14. **b)** ISO/IEC 27001
15. **пентест** (пентестинг, penetration testing) или **тестирование на проникновение**
16. **c)** Регламент реагирования на инциденты (IRP)

Раздел 5:

17. **a, b, c, d** (Все перечисленные действия являются ключевыми обязанностями оператора по ФЗ-152)
18. **General Data Protection Regulation (Общий регламент по защите данных)**
19. **b)** Информация ограниченного доступа
20. **аттестация** (или **сертификация**)

Контрольные задания

Блок 1: Анализ рисков и построение политик

Задание 1. «Проведение оценки рисков для стартапа FinTech»
Стартап разрабатывает мобильное приложение для микрозаймов. Система включает: мобильное приложение (iOS/Android), серверную часть на AWS, базу данных с персональными данными (ПДн) и финансовой информацией клиентов.

Требуется:

1. **Идентификация активов:** Составьте список из 5 ключевых информационных активов компании (например, база данных клиентов, исходный код, приватные ключи API).
2. **Анализ угроз и уязвимостей:** Для актива «База данных клиентов» проведите мозговой штурм и определите:
   - 2 наиболее вероятные угрозы (например, SQL-инъекция через уязвимое API, утечка данных администратором).
   - 2 соответствующие уязвимости (например, отсутствие параметризованных запросов, избыточные права у администраторов БД).
3. **Оценка риска:** Используя упрощенную матрицу (Вероятность: Низкая-1, Средняя-2, Высокая-3; Ущерб: Низкий-1, Средний-2, Критический-3), оцените риск для каждой пары «угроза-уязвимость».
4. **Разработка плана обработки:** Для риска с наивысшим рейтингом предложите конкретные меры по его снижению (контроль), с указанием ответственного и сроков. Например, для риска SQL-инъекции: «Внедрить статический анализ кода (SAST) в CI/CD, ответственен — тимлид бэкенда, срок — 2 недели».

Задание 2. «Разработка политики информационной безопасности»
Вы — новый CISO (Chief Information Security Officer) в компании «БыстрыйДоставка» (200 сотрудников, есть курьеры с мобильными устройствами, клиентская база, внутренний портал).

Требуется: Разработать разделы корпоративной **Политики информационной безопасности**. Напишите содержание и ключевые тезисы для трех следующих разделов:

1. **Политика использования электронной почты и интернета.**
   - *Пример тезиса:* «Запрещается использование корпоративной почты для регистрации на личных сайтах. Весь интернет-трафик журналируется».
2. **Политика работы с персональными данными клиентов и сотрудников.**
   - *Пример тезиса:* «Доступ к базе ПДн предоставляется по принципу наименьших привилегий. Передача ПДн третьим лицам возможна только после подписания NDA и согласия субъекта».
3. **Политика удаленной работы и использования мобильных устройств (BYOD — Bring Your Own Device).**
   - *Пример тезиса:* «Для доступа к корпоративным ресурсам с личного устройства необходимо установить одобренный MDM-клиент. Данные на устройстве должны быть зашифрованы».

Блок 2: Моделирование инцидентов и реагирование

Задание 3. «Кейс: Инцидент с фишингом и утечкой данных»
Сценарий: В понедельник утром несколько сотрудников отдела бухгалтерии получили письмо якобы от гендиректора с темой «СРОЧНО: Выплата премии». В письме была ссылка на поддельную страницу входа в корпоративный портал. Один сотрудник ввел свои учетные данные. Через 2 часа в DarkWeb появилась выборка внутренних финансовых отчетов компании.

Требуется: Вы — руководитель группы реагирования на инциденты (CSIRT). Ваши действия:

1. **Составьте чек-лист первоочередных действий** (первые 60 минут) по фазам:
   - **Подготовка:** Кого оповестить? (юрист, PR, руководство).
   - **Обнаружение и анализ:** Как подтвердить факт утечки? Как найти скомпрометированный аккаунт и точку утечки? (анализ логов почтового сервера, прокси, DLP).
   - **Сдерживание:** Какие технические меры принять немедленно? (сброс пароля учетной записи, блокировка сессий, изоляция сегмента сети).
2. **Напишите шаблон внутреннего уведомления** для сотрудников компании об инциденте (без паники, с указанием фактов и рекомендаций по осторожности).
3. **Спланируйте пост-инцидентный анализ:** Какие 3 вопроса необходимо задать, чтобы предотвратить подобное в будущем? (Пример: «Почему система антифишинга не сработала?»)

Задание 4. «Настольная игра-симулятор: Киберкризис в банке»
Цель: В группе из 3-4 человек промоделировать управление серьезным инцидентом.
Роли:

- **Технический директор:** Отвечает за техническое восстановление.
- **Руководитель CSIRT:** Координирует расследование.
- **PR-директор:** Работает с репутацией, готовит заявления.
- **Юрист:** Оценивает правовые последствия, взаимодействие с регуляторами.

Сценарий: В банке атака ransomware. Зашифрованы данные в ЦОД, недоступны онлайн- банк и процессинг. Злоумышленники требуют выкуп в биткоинах. Угрожают обнародовать данные VIP-клиентов.

Задание для группы:

1. Проведите 20-минутное совещание в кризисном режиме. Каждый участник выступает со своей ролью.
2. **Итоговый артефакт:** Создайте **протокол принятых решений** со столбцами: «Время», «Решение», «Обоснование», «Ответственный». Например: «10:15 — Отключить зараженный ЦОД от сети. Обоснование: Остановить распространение шифровальщика. Ответственный: Техдир.»
3. **Анализ:** После игры обсудите, какой была самая сложная дилемма (например, платить выкуп или нет) и какие нормативные документы (ФЗ-187 о КИИ, указания ЦБ) влияли на решения.

Блок 3: Техническая защита и комплаенс

Задание 5. «Проектирование сегментированной сети для гостиницы»
Сеть гостиницы включает: административную зону (бухгалтерия, управление), зону для

гостей (Wi-Fi), систему управления номерами (умные замки, кондиционеры), платежный киоск в лобби.

Требуется:

1. Нарисуйте **схему сегментированной сети** (можно от руки), выделив как минимум 4 VLAN/подсети. Укажите устройства (маршрутизатор, коммутаторы L3, межсетевой экран).
2. **Сформулируйте 5 правил для межсетевого экрана (NGFW):**
   - *Пример:* «Разрешить только исходящие HTTP/HTTPS запросы из гостевой сети VLAN_GUEST во внешнюю сеть. Запретить любой трафик из VLAN_GUEST в административную VLAN_ADMIN.»
3. **Опишите архитектуру защиты платежного киоска** в соответствии со стандартом PCI DSS. Какие конкретно требования стандарта (например, шифрование трафика, отсутствие хранения данных CVV) и как их реализовать технически?

Задание 6. «Оценка соответствия требованиям GDPR для SaaS-сервиса»
Ваша компания разрабатывает облачный сервис для управления проектами (SaaS). Клиенты — компании из ЕС. В системе хранятся имена, email, задачи сотрудников клиентов.

Требуется:

1. Определите **роли** согласно GDPR: Кто является контроллером данных (data controller), процессором (data processor), субъектом данных (data subject) в данном сценарии?
2. **Составьте таблицу соответствия:** В левой колонке — 5 ключевых требований GDPR (например, «Право на доступ», «Право на удаление — Right to be forgotten», «Уведомление об утечках», «Защита данных Privacy by Design», «Назначение DPO»). В правой колонке — как ваш SaaS-сервис будет их выполнять (технически и организационно).
3. **Напишите фрагмент Пользовательского соглашения (Privacy Policy)** на английском языке, описывающий, как вы собираете, обрабатываете и храните данные, и как пользователь может воспользоваться своими правами.
4. **Спроектируйте техническую функцию** в личном кабинете пользователя «Экспорт/Удаление всех моих данных» (с учетом связанности данных в БД).

Блок 4: Аудит и обучение персонала

Задание 7. «Проведение внутреннего аудита ИБ»
Вы — внутренний аудитор. Вам поручено проверить безопасность DevOps-процессов.

Требуется: Разработать **чек-лист аудита** из 10 пунктов, разделенных на 3 области:

1. **Контроль доступа к репозиториям (Git):**
   - *Пример пункта:* «Включена ли обязательная 2FA для всех пользователей GitHub/GitLab? Проверить настройки организации.»
   - *Пример пункта:* «Используется ли модель защищенных веток (protected branches) с обязательным код-ревью перед мержем в main?»
2. **Безопасность CI/CD пайплайна:**
   - *Пример пункта:* «Как хранятся и используются секреты (API-ключи, пароли) в пайплайне? Проверить, не хардкодятся ли они в файлы конфигурации.»

- *Пример пункта:* «Запускаются ли статические анализаторы безопасности кода (SAST), например, SonarQube или GitLab SAST, на этапе CI?»

3. **Конфигурация и харденинг контейнеров (Docker):**

- *Пример пункта:* «Сканируются ли образы Docker на наличие известных уязвимостей (CVE) перед деплоем? (Инструмент: Trivy, Clair)»
- *Пример пункта:* «Запускаются ли контейнеры от непривилегированного пользователя (USER nobody)? Проверить Dockerfile.»

Итог: Представьте гипотетический **отчет об аудите** с выводами (соответствует/не соответствует), рисками и рекомендациями по 2 найденным несоответствиям.

Задание 8. «Создание программы обучения киберграмотности»
Цель: Снизить риск инцидентов, вызванных человеческим фактором.

Требуется: Разработать план **годовой программы обучения** для сотрудников офиса (не технических специалистов):

1. **Формат и темы:** Распределите 4 учебных модуля по кварталам. Например:

- **Q1:** «Основы ИБ: Фишинг и пароли» (формат: 30-минутный вебинар + рассылка с инфографикой).
- **Q2:** «Безопасная удаленная работа» (формат: интерактивный тест-симулятор выбора безопасного действия).
- **Q3:** «Защита персональных и корпоративных данных» (формат: живой воркшоп с разбором кейсов).
- **Q4:** «Итоговое тестирование и симуляция фишинговой атаки» (формат: контролируемая рассылка тестовых фишинговых писем, сбор статистики).

2. **Измеримые метрики успеха (KPI):** Предложите 3 KPI для оценки эффективности программы (например, процент сотрудников, прошедших итоговый тест >90%; снижение числа кликов по тестовым фишинговым письмам на 40% за год).
3. **Разработайте материал:** Создайте **инфографику на одну страницу А4** для первого модуля «Как распознать фишинг». Включите 5 простых правил с иконками (пример:
«Проверяйте отправителя», «Не спешите кликать», «Обращайте внимание на URL»).

Критерии оценки:

- **Блок 1 (Анализ и политики):** Оценивается системность подхода к анализу рисков, практическая применимость и полнота разработанных политик.
- **Блок 2 (Инциденты):** Оценивается реалистичность и оперативность плана реагирования, глубина пост-инцидентного анализа, навыки командной работы и принятия решений в кризисе.
- **Блок 3 (Техническая защита и комплаенс):** Оценивается корректность технических решений, глубокое понимание требований стандартов (GDPR, PCI DSS) и умение
перевести их в практические меры.
- **Блок 4 (Аудит и обучение):** Оценивается структурированность чек-листа аудита, качество рекомендаций, креативность и измеримость программы обучения.
- **Общее:** Умение работать с нормативной базой (ФЗ-152, ФЗ-187, GDPR), четкость и структурированность представления результатов (схемы, таблицы, протоколы), профессиональный язык.

Раздел 2. Безопасность облачных технологий Тестовые задания

1. (ОВ) Модель облачных услуг, при которой провайдер управляет инфраструктурой, операционной системой и средой выполнения, а клиент развертывает и управляет своим приложением и данными, — это:

a) IaaS (Infrastructure as a Service)
b) PaaS (Platform as a Service)
c) SaaS (Software as a Service)
d) FaaS (Function as a Service)

2. (МВ) Согласно модели разделенной ответственности в облаке, за какие из перечисленных аспектов обычно отвечает клиент при использовании IaaS?

a) Физическая безопасность дата-центров
b) Конфигурация и защита операционной системы на виртуальной машине
c) Обновление сетевого оборудования
d) Управление сетевыми группами безопасности (Security Groups) и правилами брандмауэра

3. (СО) Модель, описывающая распределение обязанностей по безопасности между облачным провайдером и клиентом, называется моделью _____ответственности. *Ответ:* _____

4. (ОВ) В какой модели облачных услуг клиент несет НАИМЕНЬШУЮ ответственность за безопасность?

a) IaaS
b) PaaS
c) SaaS
d) On-premise (локальное развертывание)

5. (МВ) Какие из перечисленных угроз являются специфичными или особенно актуальными для облачных сред?

a) Неправильная конфигурация облачных сервисов (например, публично открытое S3-ведро)
b) Уязвимости в гипервизоре (виртуализации)
c) Угроза внутреннего нарушителя со стороны облачного провайдера
d) Атаки на цепочку поставок ПО (Supply Chain Attacks)

6. (ОВ) Практика, при которой злоумышленник создает множество бесплатных пробных аккаунтов в облачном сервисе для злонамеренной деятельности (рассылка спама, майнинг криптовалюты), называется:

a) Account Hijacking
b) Cloud Cryptojacking
c) Cloud Hoarding
d) Cloud Sprawl

7. (СО) Утечка конфиденциальных данных из-за неправильно настроенных прав доступа к публичному облачному хранилищу (например, AWS S3, Yandex Object Storage) часто называется утечкой из-за конфигурации.

Ответ: _____

8. (OB) Атака, направленная на исчерпание ресурсов облачного приложения (вычислительных мощностей, памяти) с целью вызвать отказ в обслуживании и привести к значительным финансовым потерям клиента из-за модели оплаты по факту использования, — это:

a) Фишинг
b) Economic Denial of Sustainability (EDoS)
c) SQL-инъекция
d) Атака на стороне канала (Side-channel attack)

9. (OB) Основной сервис управления идентификацией и доступом (IAM) в облаке AWS называется:

a) Azure Active Directory
b) Google Cloud IAM
c) AWS Identity and Access Management (IAM)
d) CloudHSM

10. (MB) Какие из перечисленных мер повышают безопасность облачных рабочих нагрузок?

a) Шифрование данных не только при передаче (TLS), но и при хранении (encryption at rest)
b) Использование многофакторной аутентификации (MFA) для всех привилегированных учетных записей
c) Регулярное проведение аудита конфигураций с помощью инструментов типа AWS Config, Azure Security Center
d) Хранение секретов (паролей, ключей API) непосредственно в коде приложения

11. (CO) Технология, которая позволяет изолировать и безопасно запускать приложения, упаковывая их со всеми зависимостями в легковесные контейнеры, называется _____.

Ответ: _____

12. (OB) Специализированное аппаратное устройство в облаке, предназначенное для безопасного генерации и хранения криптографических ключей, — это:

a) KMS (Key Management Service)
b) HSM (Hardware Security Module)
c) VPN Gateway
d) WAF (Web Application Firewall)

13. (MB) Какие из перечисленных стандартов и сертификатов актуальны для оценки безопасности облачных провайдеров?

a) ISO/IEC 27001
b) PCI DSS (для обработки платежных карт)
c) СЗИ КИИ (Соответствие требованиям ФЗ-187 в РФ)
d) GDPR (для работы с данными граждан ЕС)

14. (OB) Облачный сервис, который непрерывно отслеживает конфигурации ресурсов на предмет отклонений от заданных политик безопасности, называется:

a) CloudTrail (журналирование событий)
b) CloudWatch (мониторинг метрик)
c) AWS Config / Azure Policy (управление конфигурацией и соответствием)
d) GuardDuty (интеллектуальное обнаружение угроз)

15. (CO) Практика, при которой для каждой рабочей нагрузки (приложения, микросервиса) создается отдельная, изолированная учетная запись или проект в облаке, чтобы ограничить радиус взрыва при компрометации, называется _____.
Ответ: _____

16. (OB) Какой принцип безопасности предполагает, что доступ к ресурсам по умолчанию запрещен, и разрешения предоставляются явно только по необходимости?
a) Принцип наименьших привилегий
b) Принцип нулевого доверия (Zero Trust)
c) Принцип разделения обязанностей (SoD)
d) Принцип явного отказа (Explicit Deny)

17. (MB) Какие архитектурные подходы способствуют безопасности в облаке?
a) Использование микросервисной архитектуры для изоляции компонентов
b) Единая большая виртуальная машина, выполняющая все функции
c) Внедрение сервисной сетки (Service Mesh) для управления безопасным взаимодействием микросервисов
d) Шифрование всех данных «от корки до корки» (End-to-End Encryption)

18. (CO) Модель безопасности, которая предполагает, что угроза может исходить как извне, так и изнутри сети, и поэтому требует строгой проверки подлинности и авторизации для каждого запроса к ресурсу, независимо от его источника, называется _____.
Ответ: _____

19. (OB) Технология, которая позволяет выполнять код в ответ на события без необходимости создания и управления серверами, называется:
a) Виртуальная машина (VM)
b) Бессерверные вычисления (Serverless, FaaS)
c) Контейнеризация (Docker)
d) Управляемый Kubernetes-сервис (EKS, GKE)

20. (CO) Процесс регулярной проверки безопасности облачной инфраструктуры путем моделирования атак с разрешения владельца с фокусом на облачные сервисы и конфигурации называется _____тестирование.
Ответ: _____

Ключ для проверки Раздел 1:

1. **b)** PaaS (Platform as a Service)
2. **b, d** (a, c — ответственность провайдера)
3. **разделенной** (shared responsibility model)
4. **c)** SaaS

Раздел 2:
5. **a, b, c** (d — актуально, но не специфично только для облака)
6. **b)** Cloud Cryptojacking (или **Cloud Account Fraud**)
7. **небезопасной / ошибочной** (misconfiguration)
8. **b)** Economic Denial of Sustainability (EDoS)

Раздел 3:

9. **c)** AWS Identity and Access Management (IAM)
10. **a, b, c** (d — грубая ошибка безопасности)
11. **контейнеризация** (Docker, containerization)
12. **b)** HSM (Hardware Security Module) **/ Облачный HSM**

Раздел 4:

13. **a, b, c, d** (Все актуальны в различных контекстах)
14. **c)** AWS Config / Azure Policy (управление конфигурацией и соответствием)
15. **изоляция на уровне аккаунта** (account isolation) **/ multi-account strategy**
16. **d)** Принцип явного отказа (Explicit Deny) (Является реализацией Zero Trust и наименьших привилегий на уровне правил)

Раздел 5:

17. **a, c, d** (b — монолитная архитектура усложняет изоляцию и повышает риски)
18. **Zero Trust** (Нулевое доверие, Zero Trust Architecture - ZTA)
19. **b)** Бессерверные вычисления (Serverless, FaaS)
20. **облачный пентест** (cloud penetration testing) **/ аудит безопасности облачной среды**

Контрольные задания

Блок 1: Модель разделенной ответственности и оценка рисков

Задание 1. «Карта ответственности для стартапа на разных облачных моделях»
Стартап разрабатывает мобильное приложение для доставки еды. Рассматривает три варианта инфраструктуры в Yandex Cloud:

1. **Вариант IaaS:** Виртуальные машины (Yandex Compute Cloud) для бэкенда и БД.
2. **Вариант PaaS:** Контейнеры в Yandex Managed Service for Kubernetes (Yandex Managed Kubernetes) + Managed Service for PostgreSQL.
3. **Вариант SaaS:** Готовый мобильный бэкенд как сервис (MBaaS) от стороннего вендора.

Требуется:

1. Создайте **три таблицы / диаграммы**, визуализирующие модель разделенной ответственности для каждого варианта.
2. Для каждого уровня (физическая инфраструктура, гипервизор, ОС, среда выполнения, приложение, данные) четко укажите, кто отвечает: провайдер (P), клиент (C) или оба (P+C).
3. Проведите **сравнительный анализ рисков**: для каждого варианта определите 2 ключевых риска безопасности, которые ложатся на плечи стартапа. Объясните, почему при выборе SaaS эти риски смещаются, но не исчезают.

Задание 2. «Оценка рисков миграции в облако для банковского подразделения»
Нефункциональное подразделение банка (например, отдел обучения) планирует перенести в облако (Yandex Cloud или AWS) свою систему дистанционного обучения (LMS), которая содержит только учебные материалы, но не персональные данные клиентов.

Требуется:

1. **Идентификация активов:** Перечислите 5 ключевых активов, подлежащих защите в облаке (например, база данных пользователей LMS, учебный контент, SSL-сертификаты).
2. **SWOT-анализ миграции:** Заполните таблицу 2x2 (Сильные стороны, Слабые стороны, Возможности, Угрозы) для перехода в облако с точки зрения безопасности.
3. **Матрица решений:** Для угрозы «Несанкционированный доступ к управляющей консоли облака» предложите:

- **Меры снижения риска** (технические: MFA, выделенные аккаунты для админов; организационные: процедура выдачи временных прав).
- **Ответственного** за реализацию.
- **Критерий эффективности** меры (например, 100% охват привилегированных пользователей MFA).

Блок 2: Конфигурация, IAM и защита данных

Задание 3. «Аудит безопасности аккаунта Yandex Cloud / AWS»
Вам предоставлен доступ только для чтения к тестовому облачному проекту. Ваша задача — провести ручной аудит.

Данные для проверки (предположим, что вы видите эти настройки):

- **Объектное хранилище (Yandex Object Storage / S3):** Есть бакет company-backups. Политика доступа разрешает GetObject действию * (всем пользователям).
- **IAM / Cloud IAM:** Существует группа developers. Этой группе присвоена роль editor на весь каталог/проект.
- **Виртуальная машина:** На ВМ в Yandex Compute Cloud / EC2 в группе безопасности разрешен входящий трафик по порту 22 (SSH) с источника 0.0.0.0/0.
- **База данных (Managed PostgreSQL):** Пароль администратора БД не менялся с момента создания 2 года назад.

Требуется:

1. Для каждой из 4-х находок:

- **Сформулируйте проблему** (например, «Публичный доступ к бакету с бэкапами»).
- **Оцените критичность** (Низкая, Средняя, Высокая).
- **Дайте конкретную рекомендацию** по исправлению.

2. Составьте **чек-лист из 10 пунктов** для регулярного самостоятельного аудита небольшого облачного проекта.
3. **Автоматизация:** Предложите, какой нативный инструмент облачного провайдера (например, Yandex Security Command Center, AWS Security Hub) или стороннее решение можно использовать для автоматического мониторинга подобных нарушений.

Задание 4. «Проектирование безопасной облачной сети (VPC) для интернет-магазина»
Спроектируйте сетевую архитектуру в Yandex Cloud для двухзвенного веб-приложения (frontend + backend + БД).

Требуется:

1. Нарисуйте **схему облачной сети (VPC)**. Включите:

- Публичную и приватную подсети.
- Группы безопасности (Security Groups) или ACL.

- NAT-шлюз для исходящего трафика из приватной подсети.
- Бастион-хост (jump server) для администрирования.
- Application Load Balancer (Yandex Application Load Balancer) во внешней подсети.

2. **Сформулируйте правила групп безопасности** в табличном виде:

- Для **фронтенд-серверов:** (Разрешить HTTP/80, HTTPS/443 от LB; Запретить всё остальное).
- Для **бэкенд-серверов:** (Разрешить HTTP/8080 только от фронтенда; SSH/22 только от бастион-хоста).
- Для **БД:** (Разрешить порт БД только от бэкенд-серверов).

3. **Шифрование данных:** Опишите, как будете шифровать:

- **Данные в транзите** между клиентом и приложением, между компонентами.
- **Данные в покое** на дисках ВМ и в managed БД.

Укажите, какие сервисы (KMS, управляемые диски с шифрованием) будете использовать.

Блок 3: Комплаенс, мониторинг и реагирование на инциденты

Задание 5. «Обеспечение соответствия требованиям 152-ФЗ и GDPR в облаке» Компания-резидент РФ, оказывающая услуги клиентам из ЕС, хранит персональные данные в Yandex Cloud.

Требуется:

1. **Сравнительная таблица требований:** Создайте таблицу, где в строках — ключевые требования (Уведомление регулятора, Согласие на обработку, Право на забвение, Защита при трансграничной передаче), а в столбцах — особенности реализации в облаке для ФЗ- 152 и GDPR.
2. **Выбор региона:** Объясните, почему для хранения данных граждан ЕС нельзя использовать регион ru-central1 (Москва), а нужно выбрать, например, eu-central-1 в AWS или fi-1 в Yandex Cloud. Какие правовые последствия могут быть?
3. **План действий при утечке:** Разработайте регламент первых 4 часов после обнаружения утечки ПДн из облачной БД. Включите шаги: изоляция ресурса, оповещение облачного провайдера (запросить логи), внутреннее оповещение (юрист, DPO), подготовка уведомления для регулятора (Роскомнадзор).

Задание 6. «Построение SOC (Security Operations Center) в облаке»
Необходимо настроить сбор и анализ логов безопасности для небольшого проекта.

Требуется:

1. **Архитектура сбора логов:** Нарисуйте схему, как логи с ВМ, лог групп безопасности, аудит Cloud Logging (Yandex) / CloudTrail (AWS) будут централизованно собираться в отдельный **логовый аккаунт/проект** (для изоляции).
2. **Детектирование угроз:** Сформулируйте 3 **правила корреляции** для SIEM-системы (можно на основе Open Source — Wazuh, Elastic SIEM), которые позволят обнаружить:

- Попытку подбора пароля к ВМ (много неудачных попыток SSH за короткий период).
- Изменение политики безопасности бакета, делающее его публичным.
- Запуск криптомайнера на инстансе (аномально высокое использование CPU).

3. **Runbook для инцидента:** Напишите пошаговую инструкцию (runbook) для аналитика SOC на случай срабатывания правила «Обнаружена публикация приватного SSH-ключа в публичном Git-репозитории компании». Какие действия предпринять? (Пример:

Немедленная ротация ключа, оповещение разработчика, сканирование логов на предмет использования скомпрометированного ключа).

Блок 4: Продвинутые сценарии и DevSecOps

Задание 7. «Внедрение безопасности в CI/CD пайплайн (DevSecOps)»
Команда использует GitLab CI/CD для развертывания контейнеризованного приложения в Yandex Managed Kubernetes.

Требуется:

1. Модифицируйте предоставленный **.gitlab-ci.yml**, добавив этапы

безопасности: yaml

```
stages:
- build
- test
- security_scan  # <-- Добавленный этап
- deploy

security_scan:
stage: security_scan
image: docker:stable
services:
- docker:dind script:
# Задание: Напишите скрипт, который:
# 1. Сканирует Docker-образ на уязвимости (CVE) с помощью Trivy.
# 2. Проверяет манифесты Kubernetes (k8s/*.yaml) на соответствие лучшим практика м безопасности с помощью kube-score или kubeaudit.
# 3. Если найдены критические уязвимости (> CRITICAL) — завершает пайплайн с оши бкой.
```

2. **Secure Secrets Management:** Где и как безопасно хранить и подавать в пайплайн секреты для доступа к облаку (Service Account Key) и БД? Опишите подход (например, использование Variables в GitLab с флагом protected, или HashiCorp Vault).
3. **Инфраструктура как код (IaC) с безопасностью:** Примените к Terraform-конфигурации, создающей ВМ, принцип «безопасность по умолчанию». Напишите фрагмент кода, который гарантированно создает ВМ без публичного IP и с минимально необходимыми правилами в SG.

Задание 8. «Кейс-чемпионат: Анализ реального инцидента (на основе публичных отчетов)»
Изучите публичный отчет об инциденте безопасности у крупного облачного провайдера или их клиента (например, инцидент с Capital One 2019, утечки из открытых S3-бакетов).

Требуется (письменный отчет на 2-3 страницы):

1. **Хронология:** Восстановите последовательность событий атаки.

2. **Анализ коренных причин (Root Cause Analysis):** Определите технические и организационные провалы, которые позволили инциденту произойти (например, чрезмерные права IAM-роли, отсутствие сегментации, неактивный мониторинг).
3. **Оценка по модели STRIDE:** К каким типам угроз (Spoofing, Tampering, Repudiation, Information Disclosure, Denial of Service, Elevation of Privilege) можно отнести действия злоумышленника?
4. **Рекомендации:** Предложите 5 конкретных мер, которые должны были быть внедрены для предотвращения подобного инцидента. Разделите их на технические (например, внедрение сканирования конфигураций) и процессные (например, обязательное обучение для разработчиков по облачной безопасности).

Критерии оценки:

- **Блок 1 (Ответственность и риски):** Оценивается четкость визуализации модели разделенной ответственности, глубина сравнительного анализа рисков для разных сервисных моделей.
- **Блок 2 (Конфигурация и IAM):** Оценивается точность выявления уязвимостей в конфигурации, практичность рекомендаций, качество проектирования безопасной сетевой архитектуры.
- **Блок 3 (Комплаенс и SOC):** Оценивается понимание правовых нюансов, структурированность планов реагирования, реалистичность правил детектирования угроз для SIEM.
- **Блок 4 (DevSecOps и анализ):** Оценивается работоспособность предложенных скриптов для CI/CD, зрелость подхода к управлению секретами, глубина и системность анализа
реального инцидента.
- **Общее:** Умение применять теоретические знания к конкретным облачным сервисам (Yandex Cloud, AWS, etc.), использование профессиональной терминологии, структурированность и ясность представления решений.

4.2 Контрольные задания для промежуточной аттестации

Вопросы для зачета

1. Дайте определение облачным вычислениям по версии NIST. Перечислите и кратко охарактеризуйте пять их основных характеристик.
2. Опишите сервисные модели облачных вычислений (IaaS, PaaS, SaaS). Приведите по два практических примера сервисов для каждой модели и объясните, как меняется зона ответственности клиента.
3. Что такое модель разделенной ответственности (Shared Responsibility Model)? Проиллюстрируйте её на примере развертывания веб-приложения на виртуальной машине (IaaS) и в бессерверной среде (FaaS).
4. Объясните разницу между публичным, частным, гибридным и мультиоблачным (multi- cloud) развертыванием. Какие уникальные риски безопасности присущи гибридной и мультиоблачной архитектурам?
5. Каковы основные мотивационные факторы и сопутствующие риски при миграции бизнеса в облако? Объясните на примере перехода от локального ЦОД к публичному IaaS.
6. Что такое доверенная вычислительная среда (Trusted Computing Base, TCB) в контексте облака? Как концепция "доверенного гипервизора" влияет на безопасность мультитенантных сред?

7. Опишите жизненный цикл безопасности данных в облаке (Data Lifecycle Security). Какие механизмы защиты необходимо применять на каждом этапе (создание, хранение, использование, передача, уничтожение)?
8. Как модель "pay-as-you-go" (оплата по факту использования) влияет на профиль рисков, связанных с атаками типа "отказ в обслуживании" (DoS/DDoS) в облаке?

Раздел 2: Угрозы, уязвимости и управление идентификацией (10 вопросов)

9. Перечислите и охарактеризуйте не менее пяти ключевых угроз безопасности, описанных в отчете Cloud Security Alliance (CSA) "Treacherous 12" или "Top Threats". Приведите примеры для каждой.
10. Что такое "небезопасные интерфейсы и API" (Insecure Interfaces and APIs) в облаке? Какие атаки возможны через уязвимые API управления облаком (Cloud Management APIs)?
11. Объясните угрозу "утечки данных из-за ошибочной конфигурации" (Misconfiguration). Какие инструменты и практики позволяют эффективно выявлять и предотвращать такие утечки?
12. В чем заключается специфика атак на цепочку поставок ПО (Supply Chain Attacks) в облачных экосистемах? Приведите пример атаки через публичные контейнерные образы или библиотеки зависимостей.
13. Дайте определение и приведите примеры атак типа "экономический отказ в устойчивости" (Economic Denial of Sustainability, EDoS). Как защитить облачную среду от подобных
атак?
14. Что такое управление идентификацией и доступом (IAM) в облаке? Опишите ключевые концепции: принцип наименьших привилегий, разделение обязанностей, временный
доступ (JIT).
15. Объясните разницу между федерацией идентификации (Identity Federation) и единым входом (Single Sign-On, SSO) в контексте гибридных облачных сред. Какую роль играют протоколы SAML и OIDC?
16. Для чего предназначены сервисы управления секретами (Secrets Management) в облаке? Сравните подходы к хранению секретов в переменных среды, специализированных сервисах (AWS Secrets Manager, HashiCorp Vault) и аппаратных модулях безопасности (HSM).
17. Что такое атаки на стороне канала (Side-Channel Attacks) в мультитенантных облаках? Какие меры принимают облачные провайдеры для изоляции вычислительных сред клиентов на физическом уровне?
18. Опишите угрозу "захвата учетных записей" (Account Hijacking) в облаке. Какие многофакторные методы аутентификации (MFA) наиболее эффективны для защиты привилегированных аккаунтов?

Раздел 3: Архитектура безопасности и защита данных (10 вопросов)

19. Что такое нулевое доверие (Zero Trust) и как эта архитектурная модель применяется в облачных средах? Объясните принцип "никогда не доверяй, всегда проверяй".
20. Опишите модель безопасности микросервисной архитектуры в облаке. Какую роль играют API-шлюзы, сервисная сетка (Service Mesh) и взаимная аутентификация TLS (mTLS)?
21. Как обеспечить безопасность контейнеров (Docker) в облаке? Опишите практики: сканирование образов на уязвимости, запуск от непривилегированного пользователя, использование подписанных образов.

22. Каковы ключевые аспекты безопасной конфигурации облачных сетей (VPC/VNet)? Объясните назначение и разницу между сетевыми ACL, группами безопасности и виртуальными брандмауэрами следующего поколения.
23. Для чего предназначен облачный мониторинг безопасности и система управления информацией и событиями безопасности (SIEM)? Приведите примеры ключевых источников логов в облаке (CloudTrail, Flow Logs, GuardDuty).
24. Опишите методы шифрования данных в облаке: шифрование в покое (at rest), при передаче (in transit) и в использовании (in use). Какие технологии (TLS, KMS, TPM, конфиденциальные вычисления) используются для каждого случая?
25. Что такое управляемые услуги безопасности (MSSP) в облаке? Приведите примеры встроенных сервисов безопасности от провайдеров (AWS Security Hub, Microsoft Defender for Cloud) и их преимущества.
26. Объясните принцип "безопасность по умолчанию" (Security by Default) и "безопасность как код" (Security as Code) при развертывании облачной инфраструктуры. Какую роль играют инструменты IaC (Terraform, CloudFormation)?
27. Какие существуют стратегии резервного копирования и аварийного восстановления (DR) в облаке? Сравните подходы "резервное копирование в облако" и "резервное копирование между облаками".
28. Как обеспечить безопасность бессерверных архитектур (Serverless/FaaS)? Какие уникальные риски (например, инъекция событий, неправильная конфигурация прав функций) им присущи?

Раздел 4: Комплаенс, аудит и юридические аспекты (8 вопросов)

29. Какие международные стандарты и framework наиболее актуальны для оценки безопасности облачных сред? Опишите назначение ISO/IEC 27017, ISO/IEC 27018 и CIS Benchmarks для облачных технологий.
30. Как требования регуляторов (GDPR, ФЗ-152, HIPAA) влияют на архитектуру и эксплуатацию облачных систем? Объясните на примере хранения персональных данных граждан ЕС в облаке.
31. Что такое аттестация и сертификация облачных провайдеров в России? Опишите требования ФЗ-187 "О безопасности КИИ" к облачным сервисам, отнесенным к критической информационной инфраструктуре.
32. Каковы правовые аспекты проведения пентестов (тестирования на проникновение) в облачных средах? Почему необходимо предварительное письменное согласие облачного провайдера?
33. Опишите процесс облачного аудита безопасности. Какие инструменты (Cloud Security Posture Management - CSPM) используются для непрерывного контроля соответствия политикам безопасности?
34. Что такое соглашение об уровне обслуживания (SLA) в облаке и как в нем отражаются аспекты безопасности? На что следует обращать внимание в разделе SLA, касающемся инцидентов безопасности и уведомлений?
35. Каковы особенности судебной компьютерной экспертизы (digital forensics) в облачных средах? Какие сложности возникают при сборе и сохранении доказательств в условиях мультитенантности и динамической инфраструктуры?
36. Как регламентируется трансграничная передача данных при использовании облачных сервисов? Объясните значение "шлюмминг-клаузулы" (Schrems II) для европейских компаний, использующих американские облака.

Раздел 5: Стратегия и будущие тренды (4 вопроса)

37. Опишите этапы разработки стратегии безопасности для гибридного облака (Cloud Security Strategy). Какие три ключевых документа должны быть разработаны в первую очередь?
38. Что такое DevSecOps и как эта практика интегрируется в жизненный цикл разработки облачных приложений? Приведите пример автоматизированной проверки безопасности на этапах CI/CD.
39. Каковы основные тренды и вызовы в облачной безопасности на ближайшие 3-5 лет? Обсудите влияние искусственного интеллекта, квантовых вычислений и расширения периметра до "края" (edge computing).
40. Как оценить общую стоимость владения (TCO) системой безопасности облачной инфраструктуры? Какие скрытые затраты (например, на обучение персонала, интеграцию инструментов) часто не учитываются при планировании?

Критерии оценки

Оценка «5» - (отлично)

При ответе материал изложен грамотным языком в определенной логической последовательности, точно использована терминология, полно раскрыто содержание материала в объеме, предусмотренном программой, продемонстрировано усвоение ранее изученных сопутствующих вопросов. Возможны одна - две неточности при освещении второстепенных вопросов.

Оценка «4» - (хорошо)

Ответ удовлетворяет в основном требованиям на оценку «5», но при этом имеет один из недостатков: в изложении допущены небольшие пробелы; допущены один – два недочета при освещении основного содержания ответа, исправленные по замечанию преподавателя; допущены ошибка или более двух недочетов при освещении второстепенных вопросов, легко исправленные по замечанию преподавателя.

Оценка «3» - (удовлетворительно)

При ответе неполно или непоследовательно раскрыто содержание материала, но показано общее понимание, имелись затруднения или допущены ошибки в определении понятий.

Оценка «2» - (неудовлетворительно)

При ответе не раскрыто основное содержание учебного материала; обнаружено незнание или непонимание обучающимся большей или наиболее важной части учебного материала; допущены ошибки в определении понятий, допущены существенные ошибки, показавшие, что обучающийся не владеет обязательными умениями по данной теме в полной мере.