Тестовое задание для диагностического тестирования по дисциплине:

Управление корпоративной информационной безопасностью, 7-8 семестр

Код, направление подготовки	38.03.05 Бизнес-информатика
Направленность (профиль)	Экономика предприятий и управление бизнес-процессами
Форма обучения	Очная
Кафедра-разработчик	Менеджмента и бизнеса
Выпускающая кафедра	Менеджмента и бизнеса

7 семестр

№	Проверяемая компетенция	Задание	Варианты ответов	Тип сложности вопроса
1	ПК-7.1	Какие три свойства образуют основную триаду информационной безопасности (CIA)?	1) Control, Identification, Authorization 2) Confidentiality, Integrity, Availability 3) Cryptography, Infrastructure, Access 4) Compliance, Intelligence, Audit	низкий
2	ПК-7.1	Что такое СУИБ согласно российскому стандарту?	1) Служба управления информационными базами 2) Часть общей системы управления, основанной на оценке бизнес-рисков, предназначенной для создания, внедрения, эксплуатации, мониторинга и совершенствования ИБ 3) Специализированный узел управления информационной безопасностью 4) Система учёта и инвентаризации безопасности	низкий
3	ПК-7.1	Какой российский федеральный закон регулирует защиту персональных данных?	1) ФЗ № 149 «Об информации, информационных технологиях и о защите информации» 2) ФЗ № 187 «О безопасности критической информационной инфраструктуры» 3) ФЗ № 152 «О персональных данных» 4) ФЗ № 63 «Об электронной подписи»	низкий
4	ПК-7.1	Какой международный стандарт устанавливает требования к системе управления ИБ (СУИБ)?	1) ISO 9001 2) ISO 31000 3) ISO 22301 4) ISO/IEC 27001	низкий
5	ПК-7.1	Проблематика информационной безопасности в корпорации охватывает:	1) Только технические аспекты защиты сетевой инфраструктуры	низкий

			2) Только вопросы антивирусной защиты и шифрования данных 3) Как программные и технические аспекты, так и организационные особенности функционирования бизнеса 4) Исключительно правовые и нормативные требования регуляторов	
6	ПК-7.1	Модель PDCA в контексте СУИБ означает:	1) Protect → Detect → Control → Analyze 2) Plan → Do → Check → Act — непрерывный цикл планирования, внедрения, проверки и улучшения СУИБ 3) Prevent → Document → Certify → Audit 4) Policy → Deployment → Compliance → Assessment	средний
7	ПК-7.1	Gap-анализ в управлении ИБ применяется для:	1) Выявления хакерских атак на корпоративную сеть в реальном времени 2) Определения разрыва между текущим состоянием ИБ и требованиями стандарта или политики, которые необходимо достичь 3) Расчёта стоимости лицензий на средства защиты информации 4) Анализа сетевого трафика на предмет аномалий	средний
8	ПК-7.1	Что включает в себя инвентаризация активов в рамках СУИБ?	1) Только учёт серверного и сетевого оборудования 2) Выявление, оценку и ранжирование информационных активов организации с определением их ценности 3) Регистрацию программного обеспечения в реестре Минцифры 4) Составление штатного расписания ИТ-подразделения	средний
9	ПК-7.1	Модель управления доступом RBAC (Role-Based Access Control) предполагает:	1) Назначение прав доступа непосредственно каждому пользователю системы 2) Назначение прав ролям, а пользователям - ролей согласно должностным обязанностям, что упрощает администрирование 3) Ограничение доступа исключительно по IP-адресу и геолокации 4) Обязательное двухфакторное	средний

			подтверждение при каждом входе	
10	ПК-7.1	Что такое «Положение о применимости» (Statement of Applicability, SoA) в рамках ISO 27001?	1) Трудовой договор с сотрудниками службы ИБ 2) Документ, фиксирующий, какие меры защиты из Приложения А стандарта применяются в организации, а какие исключены с обоснованием 3) Технический паспорт средств защиты информации 4) Протокол аудиторской проверки внешним аудитором	средний
11	ПК-7.1	Стратегия «принятие риска» (Risk Acceptance) в управлении рисками ИБ означает:	1) Устранение угрозы путём внедрения технических средств защиты 2) Передачу финансовых последствий реализации риска страховой компании 3) Осознанное решение руководства не предпринимать дополнительных мер, так как уровень риска не превышает допустимый 4) Полный отказ от бизнес-процесса, генерирующего риск	средний
12	ПК-7.1	Что такое остаточный риск в контексте управления рисками ИБ?	1) Риски, которые были полностью устранены после внедрения СУИБ 2) Уровень риска, сохраняющийся после применения всех запланированных мер по обработке рисков 3) Риски, обнаруженные в ходе внешнего аудита ИБ 4) Совокупная стоимость всех уязвимостей информационной системы	средний
13	ПК-7.1	Многоуровневый подход к управлению ИБ предполагает:	1) Защиту только внешнего периметра сети 2) Организацию ИБ на нескольких уровнях - стратегическом (политики), тактическом (процедуры) и операционном (технические меры) с их взаимной согласованностью 3) Использование не менее трёх различных антивирусных продуктов одновременно 4) Разграничение ответственности только между CISO и CIO	средний

14	ПК-7.1	Принцип Compliance Management в управлении ИБ означает:	1) Управление техническими уязвимостями по результатам сканирования 2) Управление ИБ на основе соответствия требованиям нормативных документов, стандартов и регуляторов 3) Регулярное обновление антивирусных баз данных 4) Управление инцидентами ИБ в режиме реального времени	средний
15	ПК-7.1	Стандарт ISO/IEC 27005 посвящён:	1) Требованиям к сертификации аудиторов ИБ 2) Управлению рисками информационной безопасности: идентификации, анализу, оценке и обработке рисков 3) Техническим мерам криптографической защиты информации 4) Требованиям к облачным сервисам и их безопасности	средний
16	ПК-7.1	Организация планирует внедрить СУИБ по ISO 27001. На этапе определения границ было решено охватить только ИТ-отдел. Какой критический риск несёт такое решение и как его следует обосновать перед руководством?	1) Никакого риска нет: ИТ-отдел - главный владелец всех информационных активов 2) Риск отсутствует, если настроить межсетевой экран на границе ИТ-сегмента 3) Узкие границы СУИБ приведут к тому, что бизнес-процессы вне ИТ-отдела останутся незащищёнными; угрозы (инсайдеры, утечки через коммерческий блок, физический доступ) не будут охвачены; рекомендуется расширить границы до ключевых бизнес-процессов с обоснованием через реестр рисков 4) Достаточно добавить ещё один файрвол	высокий
17	ПК-7.1	В компании проведена количественная оценка риска: вероятность инцидента - 30% в год, ущерб - 10 млн руб. Стоимость контрмеры - 4 млн руб., она снижает вероятность до 5%. Рассчитайте ALE до и после, определите целесообразность внедрения контрмеры.	1) ALE_до = 3 млн, ALE_после = 0,5 млн; экономия 2,5 млн < стоимости 4 млн - нецелесообразно 2) ALE_до = 10 млн, ALE_после = 5 млн; экономия 5 млн > стоимости 4 млн - целесообразно 3) ALE_до = 30 млн, ALE_после = 5 млн; однозначно целесообразно 4) Расчёт ALE не применим без данных об SLE	высокий

18	ПК-7.1	CISO компании обнаружил, что корпоративная политика ИБ была утверждена 5 лет назад, не пересматривалась, не доведена до 60% сотрудников и не охватывает облачные сервисы, активно используемые последние 2 года. Оцените ситуацию с позиций ISO 27001 и предложите план корректирующих действий.	1) Ситуация некритична: достаточно опубликовать политику на корпоративном портале 2) Это значительное несоответствие сразу по нескольким пунктам ISO 27001 (п. 5.2, 7.3, 6.1.1); план: провести актуализацию политики с учётом облачных рисков, организовать обязательное ознакомление сотрудников с подтверждением, ввести регулярный (не реже 1 раза в год) цикл пересмотра политики 3) Необходимо только добавить раздел об облачных сервисах 4) Провести внеплановый аудит ИТ-инфраструктуры	высокий
19	ПК-7.1	В ходе оценки рисков выявлено: уязвимость в веб-приложении позволяет несанкционированно экспортировать базу персональных данных (152-ФЗ). Вероятность - высокая (известна группировка, атакующая отрасль). Ущерб - критический (штрафы Роскомнадзора + репутационные потери). Какой метод обработки риска и порядок действий наиболее корректен?	1) Принять риск, так как исправление уязвимости требует длительной разработки 2) Передать риск страховщику 3) Немедленно применить компенсирующие меры (WAF, ограничение экспорта данных, усиленный мониторинг), параллельно запланировать устранение уязвимости в ближайшем релизе, уведомить DPO об актуальной угрозе 4) Заблокировать доступ к веб-приложению до полного устранения уязвимости	высокий
20	ПК-7.1	Топ-менеджмент компании ставит задачу: «Пройти сертификацию ISO 27001 за 3 месяца». CISO знает, что ни документация, ни процессы, ни осведомлённость персонала не готовы. Как должен действовать CISO?	1) Согласиться и ускорить все процессы любой ценой 2) Отказаться от сертификации как нереалистичной 3) Подготовить для руководства обоснованный roadmap с реальными сроками (обычно 9-18 месяцев), указать конкретные gap'ы, оценить ресурсы (бюджет, команда, консультанты), объяснить, что формальная сертификация без реального внедрения СУИБ несёт правовые и репутационные риски 4) Привлечь внешних консультантов для быстрого оформления документов	высокий

№	Проверяемая компетенция	Задание	Варианты ответов	Тип сложности вопроса
1	ПК-7.1	Что такое DLP-система в корпоративной ИБ?	1) Distributed Logging Platform - платформа распределённого журналирования 2) Data Loss Prevention - система предотвращения утечек конфиденциальных данных 3) Dynamic Link Protocol - протокол маршрутизации 4) Digital License Processing - управление лицензиями ПО	низкий
2	ПК-7.1	Какой стандарт регулирует управление инцидентами информационной безопасности?	1) ISO 22301 2) ISO/IEC 27001 3) ISO/IEC 27035 4) NIST SP 800-53	низкий
3	ПК-7.1	Что означает аббревиатура SOC в контексте корпоративной ИБ?	1) System of Controls - система технического контроля 2) Security Operations Center - центр мониторинга и реагирования на инциденты ИБ 3) Software Object Controller - контроллер программных объектов 4) Secure Online Channel - защищённый онлайн-канал	низкий
4	ПК-7.1	Что такое Pentest (тестирование на проникновение)?	1) Плановое резервное копирование данных 2) Авторизованная имитация атаки на информационную систему с целью выявления уязвимостей до того, как ими воспользуются злоумышленники 3) Установка обновлений безопасности на серверы 4) Мониторинг сетевого трафика с помощью IDS	низкий
5	ПК-7.1	APT (Advanced Persistent Threat) - это:	1) Автоматизированная программа для проверки паролей 2) Целенаправленная длительная кибератака высококвалифицированных злоумышленников, нацеленная на скрытое закрепление в инфраструктуре жертвы 3) Обычный вирус типа «червь», распространяющийся по сети 4) Инструмент автоматической патч-менеджмент системы	низкий
6	ПК-7.1	SIEM-система выполняет следующие ключевые функции:	1) Только хранение и архивирование журналов событий 2) Сбор, нормализацию, корреляцию событий безопасности из разнородных источников и выявление инцидентов в режиме реального времени 3) Разработку политики ИБ и обучение персонала 4) Физическую защиту серверных помещений	средний
7	ПК-7.1	Показатель RPO (Recovery Point	1) Максимальное допустимое время	средний

		Objective) в планировании непрерывности бизнеса означает:	восстановления системы после сбоя 2) Стоимость восстановления инфраструктуры после инцидента 3) Максимально допустимый объём потерянных данных (временной период), который организация готова принять при инциденте 4) Количество резервных копий, хранящихся в архиве	
8	ПК-7.1	Pentest типа «White Box» отличается тем, что:	1) Тестирование проводится без каких-либо предварительных данных об объекте 2) Тестировщик получает полную информацию об архитектуре, исходном коде, учётных данных - имитация атаки инсайдера или привилегированного злоумышленника 3) Тестирование ограничено только внешним периметром сети 4) Проверяются исключительно физические средства защиты	средний
9	ПК-7.1	Что такое Playbook в контексте управления инцидентами ИБ?	1) Список контактов поставщиков средств защиты информации 2) Детализированный сценарий реагирования на конкретный тип инцидента: пошаговые действия, ответственные, инструменты, критерии эскалации 3) Технический журнал событий безопасности за отчётный период 4) Регламент проведения ежегодного аудита ИБ	средний
10	ПК-7.1	Стандарт ISO 22301 регулирует:	1) Требования к криптографической защите информации 2) Управление непрерывностью бизнеса: процессы, планирование, тестирование BCP/DRP 3) Оценку рисков ИБ и построение СУИБ 4) Управление инцидентами и компьютерную криминалистику	средний
11	ПК-7.1	Атака типа Supply Chain Attack (атака на цепочку поставок) заключается в:	1) Физическом проникновении в серверное помещение через зону погрузки 2) Компрометации поставщика ПО или подрядчика с целью использования доверия к нему для атаки на конечного клиента 3) Перехвате данных в процессе их передачи по каналам связи (MITM) 4) DDoS-атаке на логистическую инфраструктуру предприятия	средний
12	ПК-7.1	EDR-решения (Endpoint Detection and Response) в отличие от традиционных антивирусов:	1) Защищают только почтовый трафик и веб-браузеры 2) Обеспечивают поведенческий мониторинг конечных точек, обнаружение угроз нулевого дня и автоматизированное реагирование на инциденты на уровне хоста	средний

			3) Работают исключительно на уровне сетевого периметра 4) Осуществляют только сигнатурный анализ вредоносного ПО	
13	ПК-7.1	Уровни SOC (L1/L2/L3) различаются по:	1) Стоимости лицензий на используемые SIEM-решения 2) Глубине анализа инцидентов: L1 - первичная сортировка, L2 - углублённый анализ, L3 -расследование сложных инцидентов и Threat Hunting 3) Географическому расположению операторов мониторинга 4) Типу используемого оборудования (физическое / виртуальное)	средний
14	ПК-7.1	Что такое «Chain of Custody» (цепочка хранения улик) в цифровой криминалистике?	1) Алгоритм шифрования цифровых доказательств 2) Документированный процесс фиксации, хранения и передачи цифровых доказательств, гарантирующий их целостность и допустимость в судебном разбирательстве 3) Протокол безопасной передачи данных между узлами сети 4) Реестр уязвимостей, выявленных в ходе пентеста	средний
15	ПК-7.1	В рамках импортозамещения в сфере ИБ реестр ФСТЭК России содержит:	1) Перечень запрещённых иностранных программных продуктов 2) Список сертифицированных отечественных средств защиты информации, допущенных к применению в государственных и критических информационных системах 3) Реестр уязвимостей в зарубежном программном обеспечении 4) Базу данных инцидентов кибербезопасности в России	средний
16	ПК-7.1	Производственное предприятие подверглось атаке ransomware. Зашифровано 80% файловых серверов. RTO = 4 ч, RPO = 1 ч. Резервные копии создавались раз в 24 ч и хранились в той же сети (оказались зашифрованы). Оцените нарушения и разработайте план немедленных и долгосрочных действий.	1) Нарушений нет: нужно просто обратиться в службу поддержки антивируса 2) RPO нарушен (24 ч >> 1 ч), бэкапы скомпрометированы из-за отсутствия изоляции; немедленно: активировать план реагирования, изолировать заражённые сегменты, оценить возможность восстановления из изолированных (если есть) копий; долгосрочно: внедрить изолированное (air-gap) хранилище бэкапов, сократить RPO до 1 ч (инкрементальные бэкапы), провести учения по DRP 3) Достаточно заплатить выкуп и восстановить данные 4) Проблема только в отсутствии антивируса на файловых серверах	высокий
17	ПК-7.1	SOC-аналитик L1 получает алерт от SIEM о 500 неудачных попытках входа за 5 минут на	1) Закрыть алерт как ложное срабатывание - возможно, пользователь в командировке	высокий

		один аккаунт, после чего - одна успешная авторизация с нетипичного IP (страна - нероссийская геолокация). Опишите правильную цепочку реагирования.	2) Немедленно заблокировать учётную запись без уведомления пользователя 3) L1 эскалирует на L2: подтвердить признаки Brute Force + Account Takeover, временно заблокировать сессию, уведомить владельца аккаунта и службу ИБ, собрать IOC (IP, user-agent, timestamp), инициировать смену пароля и проверку MFA, проверить действия в системе после успешного входа на предмет lateral movement 4) Дождаться повторного инцидента для подтверждения угрозы	
18	ПК-7.1	Компания завершила внешний Pentest (Black Box). Отчёт выявил: критическую уязвимость SQL Injection в публичном API, возможность получения прав администратора. CVSS Score = 9.8. Как должна быть выстроена приоритизация устранения и коммуникация с руководством?	1) Включить в плановый релиз через 3 месяца 2) Уведомить разработчиков и ждать их решения 3) Немедленная эскалация до топ-менеджмента; ввести компенсирующие меры (WAF-правила, ограничение доступа к API); установить SLA на устранение – 48-72 часа; провести повторное тестирование после патча; проверить смежные API на аналогичные уязвимости; зафиксировать инцидент в реестре рисков 4) Опубликовать уязвимость в Bug Bounty и ждать предложений от исследователей	высокий
19	ПК-7.1	Организация переходит с зарубежного SIEM-решения (Splunk) на отечественный аналог в рамках импортозамещения. Команда ИБ выявила: (1) часть правил корреляции несовместима с новой системой; (2) интеграции с 3 источниками данных требуют доработки; (3) аналитики не обучены новому интерфейсу. Предложите план миграции с минимизацией окна риска.	1) Немедленно отключить Splunk и перейти на новое решение 2) Провести параллельную эксплуатацию обеих систем на период миграции; поэтапно переносить правила корреляции с тестированием; настроить приоритетные интеграции в первую очередь; организовать обучение аналитиков до переключения; определить критерии готовности к финальному переходу и дату плановой остановки Splunk 3) Отложить миграцию до лучших времён 4) Заменить SIEM более простым решением - журналированием в файлы	высокий
20	ПК-7.1	Компания внедряет Zero Trust Architecture. Сотрудник с действующими корпоративными учётными данными запрашивает доступ к критичной БД с нового устройства из нетипичной геолокации в нерабочее время. Как отреагирует система ZTA и почему именно так?	1) Предоставит доступ - учётные данные корректны, значит пользователь легитимен 2) Навсегда заблокирует аккаунт как подозрительный 3) Запросит повторную аутентификацию (MFA), проверит Device Compliance (регистрация, патчи, антивирус), оценит поведенческий контекст (время, геолокация, аномалии), при несоответствии политике предоставит минимальные привилегии или откажет в доступе - принцип «Never Trust, Always Verify» не допускает неявного доверия даже к	высокий

			авторизованным пользователям 4) Направит запрос вручную системному администратору	