Тестовое задание для диагностического тестирования по дисциплине:

Разработка и эксплуатация защищенных информационных систем, 7 семестр

Код, направление подготовки	09.03.02 Информационные системы и технологии
Направленность (профиль)	Безопасность информационных систем и технологий
Форма обучения	Очная
Кафедра разработчик	Информатики и вычислительной техники
Выпускающая кафедра	Информатики и вычислительной техники

№	Проверяемая компетенция	Задание	Варианты ответов	Тип сложности вопроса
1.	ПК - 5.1 ПК - 5.2 ПК - 5.3 ПК -16.1 ПК -16.2 ПК -16.3 ПК -17.1 ПК -17.2 ПК -17.3	Процесс интеграции мер информационной безопасности на всех этапах жизненного цикла разработки программного обеспечения называется _____		Низкий

2.	ПК - 5.1 ПК - 5.2 ПК - 5.3 ПК -16.1 ПК -16.2 ПК -16.3 ПК -17.1 ПК -17.2 ПК -17.3	Какая модель разграничения доступа основывается на назначении ролей пользователям, а прав доступа — самим ролям?	а) DAC (дискреционная) б) MAC (мандатная) в) RBAC (ролевая) г) ABAC (атрибутивная)	Низкий
3.	ПК - 5.1 ПК - 5.2 ПК - 5.3 ПК -16.1 ПК -16.2 ПК -16.3 ПК -17.1 ПК -17.2 ПК -17.3	Архитектурный подход, предполагающий отсутствие доверия к любым субъектам внутри или снаружи сети по умолчанию, называется _____.		Низкий
4.	ПК - 5.1 ПК - 5.2 ПК - 5.3 ПК -16.1 ПК -16.2 ПК -16.3 ПК -17.1 ПК -17.2 ПК -17.3	Какой инструмент безопасности выявляет уязвимости в исходном коде до запуска приложения?	а) DAST б) SAST в) SCA г) RASP	Низкий

5.	ПК - 5.1 ПК - 5.2 ПК - 5.3 ПК -16.1 ПК -16.2 ПК -16.3 ПК -17.1 ПК -17.2 ПК -17.3	Какая технология обеспечивает шифрование данных «на отдыхе» (at rest) в реляционных СУБД?	а) TLS б) TDE в) VPN г) SSH	Низкий
6.	ПК - 5.1 ПК - 5.2 ПК - 5.3 ПК -16.1 ПК -16.2 ПК -16.3 ПК -17.1 ПК -17.2 ПК -17.3	Технология, позволяющая описывать инфраструктуру и конфигурации безопасности в виде кода для автоматизации развёртывания, называется _____.		Средний
7.	ПК - 5.1 ПК - 5.2 ПК - 5.3 ПК -16.1 ПК -16.2 ПК -16.3 ПК -17.1 ПК -17.2 ПК -17.3	Какой документ определяет правила обработки, хранения и защиты персональных данных внутри организации?	а) Регламент эксплуатации б) Политика информационной безопасности в) Техническое задание г) Акт аттестации	Средний

8.	ПК - 5.1 ПК - 5.2 ПК - 5.3 ПК -16.1 ПК -16.2 ПК -16.3 ПК -17.1 ПК -17.2 ПК -17.3	Установите соответствие между этапом жизненного цикла ПО и практикой безопасности:	Этап Практика 1. Проектирование А. Моделирование угроз 2. Разработка Б. Статический анализ кода (SAST) 3. Тестирование В. Динамический анализ (DAST) 4. Эксплуатация Г. Мониторинг событий (SIEM)	Средний

9.	ПК - 5.1 ПК - 5.2 ПК - 5.3 ПК -16.1 ПК -16.2 ПК -16.3 ПК -17.1 ПК -17.2 ПК -17.3	Какие из перечисленных мер относятся к защите контейнеризированных сред (Docker/Kubernetes)?	а) Сканирование образов на уязвимости б) Запуск контейнеров от имени root в) Использование Network Policies г) Подпись образов цифровыми сертификатами д) Отключение логирования для повышения производительности	Средний

10.	ПК - 5.1 ПК - 5.2 ПК - 5.3 ПК -16.1 ПК -16.2 ПК -16.3 ПК -17.1 ПК -17.2 ПК -17.3	Протокол, обеспечивающий безопасную передачу данных между клиентом и сервером и использующий сертификаты X.509, называется _____.		Средний
11.	ПК - 5.1 ПК - 5.2 ПК - 5.3 ПК -16.1 ПК -16.2 ПК -16.3 ПК -17.1 ПК -17.2 ПК -17.3	Какие требования предъявляются к системе управления криптографическими ключами?	а) Генерация с использованием криптографически стойких ГСЧ б) Хранение открытых ключей в незащищённом виде в) Регулярная ротация ключей согласно политике г) Уничтожение ключей после истечения срока их использования д) Передача ключей по корпоративной почте	Средний

12.	ПК - 5.1 ПК - 5.2 ПК - 5.3 ПК -16.1 ПК -16.2 ПК -16.3 ПК -17.1 ПК -17.2 ПК -17.3	Установите соответствие между типом тестирования безопасности и его описанием:	Тип Описание 1. SAST А. Анализ исходного кода без выполнения приложения 2. DAST Б. Тестирование работающего приложения извне (через интерфейсы) 3. SCA В. Проверка сторонних библиотек и зависимостей на известные уязвимости 4. IAST Г. Инструментирование приложения во время выполнения для анализа трафика и кода	Средний
13.	ПК - 5.1 ПК - 5.2 ПК - 5.3 ПК -16.1 ПК -16.2 ПК -16.3 ПК -17.1 ПК -17.2 ПК -17.3	Какие компоненты входят в инфраструктуру открытых ключей (PKI)?	а) Центр сертификации (CA) б) Реестр отозванных сертификатов (CRL/OCSP) в) Сервер DHCP г) Регистрационный центр (RA) д) Каталог LDAP/Active Directory	Средний

14.	ПК - 5.1 ПК - 5.2 ПК - 5.3 ПК -16.1 ПК -16.2 ПК -16.3 ПК -17.1 ПК -17.2 ПК -17.3	Установите правильный порядок этапов жизненного цикла управления инцидентами ИБ по NIST SP 800-61:	А. Возврат к нормальной эксплуатации Б. Подготовка (создание политик, инструментов, обучение) В. Обнаружение и анализ инцидента Г. Локализация, устранение и восстановление Д. Постинцидентный анализ (извлечение уроков)	Средний
15.	ПК - 5.1 ПК - 5.2 ПК - 5.3 ПК -16.1 ПК -16.2 ПК -16.3 ПК -17.1 ПК -17.2 ПК -17.3	Какие утверждения о DevSecOps являются верными?	а) Безопасность проверяется только перед релизом б) Автоматизация проверок в CI/CD снижает среднее время обнаружения уязвимостей в) Разработчики не несут ответственности за безопасность кода г) Shift Left подразумевает перенос проверок безопасности на ранние этапы разработки д) Инфраструктура как код (IaC) исключает необходимость аудита конфигураций	Средний

16.	ПК - 5.1 ПК - 5.2 ПК - 5.3 ПК -16.1 ПК -16.2 ПК -16.3 ПК -17.1 ПК -17.2 ПК -17.3	Установите логический порядок интеграции криптографической защиты в веб-приложение:	А. Выбор алгоритмов шифрования и хеширования согласно требованиям регулятора/стандартам Б. Реализация механизма управления ключами (KMS/HSM) В. Настройка TLS для защиты канала связи Г. Внедрение шифрования данных в базе данных (TDE/прикладное шифрование) Д. Тестирование производительности и корректности криптографических операций	Высокий

17.	ПК - 5.1 ПК - 5.2 ПК - 5.3 ПК -16.1 ПК -16.2 ПК -16.3 ПК -17.1 ПК -17.2 ПК -17.3	Какие принципы лежат в основе модели Zero Trust?	а) Никогда не доверяй, всегда проверяй б) Сегментация на основе микросервисов и идентификации в) Доверие по умолчанию внутри сетевого периметра г) Непрерывная оценка рисков и адаптивный доступ д) Централизованное управление политиками доступа (PDP/PEP)	Высокий
18.	ПК - 5.1 ПК - 5.2 ПК - 5.3 ПК -16.1 ПК -16.2 ПК -16.3 ПК -17.1 ПК -17.2 ПК -17.3	Что означает принцип «Shift Left» в методологии DevSecOps?	а) Перенос проверки безопасности на этап эксплуатации б) Перенос проверок безопасности на ранние этапы жизненного цикла разработки в) Передача ответственности за безопасность только отделу ИБ г) Отказ от автоматизированных тестов в пользу ручного аудита	Высокий

19.	ПК - 5.1 ПК - 5.2 ПК - 5.3 ПК -16.1 ПК -16.2 ПК -16.3 ПК -17.1 ПК -17.2 ПК -17.3	Какой федеральный закон регулирует обработку и защиту персональных данных в Российской Федерации?	а) 187-ФЗ б) 63-ФЗ в) 152-ФЗ г) 149-ФЗ	Высокий
20.	ПК - 5.1 ПК - 5.2 ПК - 5.3 ПК -16.1 ПК -16.2 ПК -16.3 ПК -17.1 ПК -17.2 ПК -17.3	Практика логического или физического разделения сети на изолированные сегменты для ограничения горизонтального перемещения злоумышленника называется сетевой _____.		Высокий