МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ
РОССИЙСКОЙ ФЕДЕРАЦИИ
Федеральное государственное автономное образовательное учреждение
высшего образования
«СЕВЕРО-КАВКАЗСКИЙ ФЕДЕРАЛЬНЫЙ УНИВЕРСИТЕТ»

УТВЕРЖДАЮ
И.о. директора института
перспективной инженерии канд.
техн. наук, доцент Порохня А.А.

ФОНД ОЦЕНОЧНЫХ СРЕДСТВ ПО ДИСЦИПЛИНЕ
Управление облачными и гибридными платформами

Направление подготовки	09.04.04 Программная инженерия
Направленность (профиль)	Разработка, мониторинг и управление жизненным циклом инженерных систем
Год начала обучения	2026
Форма обучения	очная
Реализуется в семестре	2

Введение

Назначение: ФОС предназначен для объективной оценки уровня сформированности компетенций.

ФОС является приложением к программе дисциплины «Управление облачными и гибридными платформами».

Разработчик Е.Н. Новикова, к.ф.-м.н., доцент, заведующий межинститутский базовой кафедрой департамента цифровых, робототехнических систем и электроники.

Проведена экспертиза ФОС.

Председатель Новикова Е.Н., межинститутской базовой кафедры департамента цифровых, робототехнических систем и электроники института перспективной инженерии

Члены комиссии:

Азаров И.В., и.о. директора департамента цифровых, робототехнических систем и электроники института перспективной инженерии

Николаев Е. И., доцент департамента цифровых, робототехнических систем и электроники института перспективной инженерии

Представитель организации-работодателя:

Руководитель группы разработки А.А. Шипулин, ООО «Стилсофт».

Экспертное заключение: ФОС по дисциплине позволяет оценить уровень сформированности компетенций. Приступить к апробации.

Срок действия ФОС определяется сроком реализации образовательной программы.

1. **Описание критериев оценивания компетенции на различных этапах их формирования, описание шкал оценивания**

Уровни сформированности компетенций, индикаторов	Дескрипторы			
	Минимальный уровень не до- стигнут (Неудовлетворительно) 2 балла	Минимальный уровень (удовлетворительно) 3 балла	Средний уро- вень (хорошо) 4 балла	Высокий уро- вень (отлично) 5 баллов
ПК-8- Способен интегрировать практики безопасности на всех этапах ЖЦ, включая статический и динамический анализ кода, анализ уязвимостей зависимостей, безопасность контейнеров и облачной инфраструктуры, обеспечивая непрерывное соответствие требованиям безопасности				
ИД-5$_{ПК-8}$. Сканирует конфигурации инфраструктуры как кода (IaC) на соответствие политикам безопасности и лучшим практикам до их применения 1.	Не умеет использовать инструменты статического анализа IaC (Checkov, tfsec). Не понимает принципов Shift Left. Не может интерпретировать отчёты о нарушениях.	Устанавливает и запускает Checkov/tfsec на готовой конфигурации. Идентифицирует основные нарушения, но не всегда корректно их классифицирует.	Самостоятельно интегрирует статический анализ IaC в pre-commit хуки и CI/CD-пайплайн. Устраняет все HIGH и CRITICAL нарушения. Документирует ложные срабатывания.	Разрабатывает кастомные политики для Checkov/tfsec. Настраивает Quality Gate с блокировкой пайплайна. Автоматизирует генерацию отчётов и отправку уведомлений
ИД-6$_{ПК-8}$ Интегрирует инструменты безопасности в CI/CD-пайплайны, настраивая автоматические шлюзы качества (quality gates), блокирующие поставку при обнаружении критических уязвимостей	Не может настроить CI/CD-пайплайн для запуска инструментов безопасности. Не понимает механизмов OIDC-федерации. Оставляет статические ключи в переменных окружения.	Настраивает базовый пайплайн с этапами сканирования (Trivy, Checkov). Использует статические ключи доступа. Quality Gate настроен, но не всегда блокирует пайплайн.	Настраивает OIDC-федерацию между CI/CD-системой и облачным провайдером. Реализует Quality Gate с блокировкой при CRITICAL уязвимостях. Автоматизирует публикацию артефактов.	Внедряет zero-trust пайплайн с разделением ролей и изолированными раннерами. Интегрирует подпись образов (Cosign) и проверку подписи на этапе деплоя. Настраивает автоматический откат при провале Quality Gate.
ИД-7$_{ПК-8}$ Мониторит состояние безопасности контейнеров и инфраструктуры в рантайме, выявляя инциденты и аномальное поведение	Не знаком с инструментами рантайм-мониторинга (Falco, Istio, PSA). Не может отличить нормальное поведение системы от аномального. Не настраивает алерты.	Устанавливает и запускает базовый мониторинг (Prometheus + Grafana). Может визуализировать метрики, но не настраивает детектирование аномалий.	Настраивает Pod Security Admission (PSA) в режиме enforce. Внедряет Service Mesh (Istio) с mTLS в режиме STRICT. Создаёт алерты на критические события безопасности	Разворачивает Falco/Tetragon для детектирования рантайм-аномалий. Настраивает корреляцию событий из разных источников. Интегрирует SIEM (ELK) и строит дашборды безопасности с ML-детекцией.

ИД-8$_{ПК-8}$ Обеспечивает непрерывное соответствие (continuous compliance) систем требованиям стандартов безопасности и регуляторным нормам через автоматизированный сбор доказательств и генерацию отчетов	Не знает стандартов (CIS, PCI DSS). Не понимает концепции Compliance as Code. Не может сгенерировать отчёт о соответствии.	Запускает аудит (Prowler/ScoutSuite) и получает HTML-отчёт. Идентифицирует основные нарушения, но не ранжирует их по критичности.	Настраивает периодический автоматический аудит. Разрабатывает OPA/Rego-политики для предотвращения нарушений. Генерирует отчёты для внешнего аудитора.	Внедряет полный цикл Continuous Compliance: политики → тесты → CI/CD Quality Gate → рантайм-аудит (Custodian) → дашборд Compliance Score. Интегрирует аудит с системой управления уязвимостями (DefectDojo) и SOAR.

ОЦЕНОЧНЫЕ СРЕДСТВА ДЛЯ ПРОВЕРКИ УРОВНЯ СФОРМИРОВАННОСТИ КОМПЕТЕНЦИЙ

Номер задания	Правильный ответ	Содержание вопроса	Компетенция
1	**B**	Какая модель ответственности (Shared Responsibility) применяется для IaaS-облака? A) Провайдер отвечает за всё B) Провайдер отвечает за «безопасность облака», клиент — за «безопасность в облаке» C) Клиент отвечает за всё D) Ответственность разделена поровну 50/50	ПК-8
2	**B**	Какой инструмент используется для статического анализа безопасности Terraform-конфигураций? A) Trivy B) Checkov C) Falco D) Prometheus	ПК-8
3	**D**	Что означает режим mTLS «STRICT» в Istio? A) Разрешён только plain-text трафик B) Разрешён и plain-text, и mTLS C) Запрещён любой трафик D) Разрешён ТОЛЬКО mTLS-трафик	ПК-8
4	**C**	Какой механизм в HashiCorp Vault позволяет генерировать временные учётные данные для доступа к базе данных? A) KV Secrets Engine	ПК-8

Номер задания	Правильный ответ	Содержание вопроса	Компетенция
		B) Transit Secrets Engine C) Database Secrets Engine D) PKI Secrets Engine	
5	**B**	Какой протокол позволяет CI/CD-пайплайну получать временные IAM-роли без хранения статических ключей? A) SAML B) OIDC (OpenID Connect) C) LDAP D) Kerberos	ПК-8
6	**A**	Какая утилита используется для сканирования Docker-образов на наличие уязвимостей CVE? A) Trivy B) Terraform C) Kubectl D) Helm	ПК-8
7	**D**	Что такое Quality Gate в контексте CI/CD? A) Шифрованный канал связи B) Механизм автоматического масштабирования C) Инструмент для сбора логов D) Автоматическое условие, блокирующее пайплайн при нарушении	ПК-8

Номер задания	Правильный ответ	Содержание вопроса	Компетенция
8	**C**	Какой тип ресурса Kubernetes запрещает запуск привилегированных контейнеров? A) NetworkPolicy B) ResourceQuota C) Pod Security Admission (PSA) в режиме restricted D) Ingress	ПК-8
9	**B**	Какой инструмент реализует политики безопасности как код через язык Rego? A) Terraform B) Open Policy Agent (OPA) C) Ansible D) Docker	ПК-8
10	**A**	Что означает аббревиатура CIS в контексте облачной безопасности? A) Center for Internet Security B) Cloud Infrastructure Standard C) Continuous Integration System D) Container Isolation Service	ПК-8
11	**D**	Какой инструмент аудита безопасности облачной инфраструктуры генерирует интерактивные HTML-отчёты и строит граф ресурсов? A) Checkov B) tfsec C) Trivy D) ScoutSuite	ПК-8

Номер задания	Правильный ответ	Содержание вопроса	Компетенция
12	**B**	Какой механизм Cloud Custodian позволяет пометить ресурс на удаление через 7 дней? A) filter: age B) mark-for-op и marked-for-op C) action: stop D) mode: periodic	ПК-8
13	**C**	Какой из перечисленных протоколов VPN считается более современным, быстрым и имеет меньшую кодовую базу? A) OpenVPN B) IPSec C) WireGuard D) PPTP	ПК-8
14	**A**	Что такое Envelope Encryption? A) Шифрование данных ключом DEK, затем шифрование DEK мастер-ключом KEK B) Шифрование только заголовков сообщений C) Шифрование без аутентификации D) Хранение ключей в открытом виде	ПК-8
15	**B**	Какая метрика FinOps показывает долю неиспользуемых или простаивающих ресурсов? A) Total Cloud Spend B) Waste C) Utilization Rate D) Cost per Unit	ПК-8

Номер задания	Правильный ответ	Содержание вопроса	Компетенция
16	**D**	Какой режим OPA Gatekeeper позволяет только логировать нарушения, но не блокировать ресурс? A) enforce B) protect C) audit D) dryrun или warn	ПК-8
17	**C**	Какой паттерн защищает от эффекта «Thundering Herd» при инвалидации кэша? A) Circuit Breaker B) Bulkhead C) Request Coalescing D) Retry with Jitter	ПК-8
18	**B**	Какое действие в Cloud Custodian выполняет остановку инстанса? A) action: terminate B) action: stop C) action: delete D) action: tag	ПК-8
19	**A**	Что такое Thundering Herd? A) Резкий скачок нагрузки на БД при одновременной инвалидации популярного кэша B) Атака переполнением буфера C) Утечка памяти в контейнере D) Проблема с сертификатами mTLS	ПК-8

Номер задания	Правильный ответ	Содержание вопроса	Компетенция
20	**C**	Какой ресурс Istio определяет политику аутентификации (PERMISSIVE / STRICT)? A) AuthorizationPolicy B) VirtualService C) PeerAuthentication D) DestinationRule	ПК-8
21	**D**	Какой инструмент позволяет оценить стоимость Terraform-плана до его применения? A) Checkov B) Prowler C) OPA D) Infracost	ПК-8
22	**B**	Что такое OIDC-федерация в контексте CI/CD? A) Хранение статических ключей в переменных GitLab B) Обмен JWT-токенами между CI/CD-системой и облачным провайдером для получения временных прав C) Шифрование артефактов пайплайна D) Балансировка нагрузки между раннерами	ПК-8
23	**C**	Какой инструмент используется для runtime-безопасности контейнеров и обнаружения аномального поведения (например, запуск chroot внутри контейнера)? A) Checkov B) tfsec C) Falco	ПК-8

Номер задания	Правильный ответ	Содержание вопроса	Компетенция
		D) Infracost	
24	**A**	Какая политика Pod Security Admission в Kubernetes является наиболее строгой? A) restricted B) baseline C) privileged D) isolated	ПК-8
25	**B**	Что такое Service Mesh? A) Балансировщик нагрузки для микросервисов B) Инфраструктурный слой для управления коммуникациями между сервисами с mTLS, наблюдаемостью и политиками C) База данных для хранения конфигураций D) CI/CD-инструмент	ПК-8
26	**D**	Какой инструмент является SIEM-системой с открытым исходным кодом? A) Prometheus B) Grafana C) Trivy D) Wazuh	ПК-8
27	**A**	Что такое RACI-матрица в модели BYOC? A) Модель разграничения ответственности между командами B) Алгоритм шифрования	ПК-8

Номер задания	Правильный ответ	Содержание вопроса	Компетенция
		C) Протокол аутентификации D) Формат отчёта о безопасности	
28	**C**	Какой компонент HashiCorp Vault используется для шифрования данных приложением без их хранения в Vault? A) Database Secrets Engine B) KV Secrets Engine C) Transit Secrets Engine D) PKI Secrets Engine	ПК-8
29	**B**	Какой механизм защиты резервных копий предотвращает их удаление даже администратором (WORM)? A) Versioning B) Object Lock в режиме Compliance C) MFA Delete D) Lifecycle rule	ПК-8
30	**D**	Что такое Model of Shared Responsibility? A) Модель экономии затрат в облаке B) Модель масштабирования приложений C) Модель развёртывания контейнеров D) Модель разделения ответственности за безопасность между провайдером и клиентом	ПК-8
31	**A**	Какой ресурс Cloud Custodian выполняет действие только после того, как ресурс был	ПК-8

Номер задания	Правильный ответ	Содержание вопроса	Компетенция
		помечен mark-for-op и прошло указанное время? A) marked-for-op B) filter: and C) mode: pull D) action: notify	
32	**B**	Какой алгоритм шифрования рекомендуется для client-side encryption с аутентификацией (AEAD)? A) AES-256-CBC B) AES-256-GCM C) DES D) MD5	ПК-8
33	**C**	Что такое Compliance Score? A) Стоимость услуг облачного провайдера B) Количество сотрудников в отделе безопасности C) Процент ресурсов, соответствующих политикам безопасности D) Скорость развёртывания инфраструктуры	ПК-8
34	**A**	Какой инструмент специализируется на аудите AWS по стандартам CIS? A) Prowler B) ScoutSuite C) Checkov D) OPA	ПК-8

Номер задания	Правильный ответ	Содержание вопроса	Компетенция
35	**B**	Что такое BYOC (Bring Your Own Cloud)? A) Передача всех облачных ресурсов провайдеру B) Модель, при которой команды самостоятельно выбирают и управляют облачными ресурсами в рамках корпоративных политик C) Отказ от использования облака D) Миграция из одного облака в другое	ПК-8
36	**C**	Какая команда Terraform сохраняет план в бинарный файл для последующего применения? A) terraform validate B) terraform apply C) terraform plan -out=tfplan D) terraform state list	ПК-8
37	**D**	Какое расширение Kubernetes Gatekeeper позволяет писать политики на Rego? A) ValidatingWebhookConfiguration B) MutatingWebhookConfiguration C) NetworkPolicy D) ConstraintTemplate	ПК-8
38	**A**	Какой паттерн предотвращает каскадные отказы при многократных ошибках вызова внешнего сервиса? A) Circuit Breaker B) Request Coalescing	ПК-8

Номер задания	Правильный ответ	Содержание вопроса	Компетенция
		C) Exponential Backoff D) Bulkhead	
39	**B**	Какой флаг в Checkov позволяет игнорировать конкретную проверку для ресурса? A) --skip-resource B) # checkov:skip= в комментарии к коду C) --ignore-policy D) --quiet	ПК-8
40	**C**	Что такое MFA Delete в S3 / Object Storage? A) Автоматическое удаление старых версий B) Шифрование при удалении C) Требование подтверждения через MFA-токен для удаления объектов D) Логирование всех операций удаления	ПК-8
41	**A**	Какой режим Cloud Custodian запускается в ответ на событие CloudTrail / Audit Trails? A) mode: cloudtrail B) mode: pull C) mode: periodic D) mode: push	ПК-8
42	**D**	Какой инструмент используется для анализа CloudTrail-логов и выявления нарушений политик? A) Trivy	ПК-8

Номер задания	Правильный ответ	Содержание вопроса	Компетенция
		B) Istio C) Terraform D) Cloud Custodian	
43	**B**	Что такое Stale Cache Serving? A) Немедленная инвалидация кэша при истечении TTL B) Отдача устаревших данных из кэша во время фонового обновления C) Шифрование кэша D) Репликация кэша между регионами	ПК-8
44	**C**	Какой протокол используется в Istio для взаимной аутентификации (mTLS)? A) WireGuard B) OpenVPN C) SPIFFE (X.509 сертификаты) D) JWT	ПК-8
45	**D**	Что такое Policy as Code? A) Хранение политик в PDF-файлах B) Устное согласование политик C) Ручная проверка конфигураций D) Описание политик безопасности в декларативных или программных артефактах, управляемых через Git	ПК-8
46	**B**	Какой механизм в OPA Gatekeeper позволяет проверить существующие ресурсы на	ПК-8

Номер задания	Правильный ответ	Содержание вопроса	Компетенция
		соответствие политикам (без блокировки создания)? A) ConstraintTemplate B) Audit C) Enforcement D) Dry-run	
47	**C**	Что такое зашифрование данных на стороне клиента (client-side encryption)? A) Данные шифруются на стороне облачного провайдера B) Данные передаются без шифрования C) Данные шифруются до отправки в облако, ключ не покидает клиента D) Данные шифруются после загрузки в облако	ПК-8
48	**A**	Какой стандарт безопасности описывает «Best practices for cloud configuration»? A) CIS Benchmarks B) ISO 27001 C) PCI DSS D) GDPR	ПК-8
49	**C**	Какой паттерн ограничивает количество одновременных вызовов к ресурсу для предотвращения его перегрузки? A) Circuit Breaker B) Retry C) Bulkhead D) Timeout	ПК-8

Номер задания	Правильный ответ	Содержание вопроса	Компетенция
50	**B**	Какой инструмент автоматически генерирует SBOM (Software Bill of Materials) для Docker-образа? A) Checkov B) Trivy (с флагом --format cyclonedx) C) Terraform D) Prowler	ПК-8

Описание шкалы оценивания
В рамках рейтинговой системы успеваемость студентов по каждой дисциплине оценивается в ходе текущего контроля и промежуточной аттестации. Рейтинговая система оценки знаний студентов основана на использовании совокупности контрольных мероприятий по проверке пройденного материала, оптимально расположенных на всем временном интервале изучения дисциплины. Принципы рейтинговой системы оценки знаний студентов основываются на требованиях, описанных в Положении об организации образовательного процесса на основе рейтинговой системы оценки знаний студентов в ФГАОУ ВО «СКФУ».

Критерии оценивания компетенций

Оценка «отлично» (5 баллов) - высокий уровень сформированности
Оценка «отлично» выставляется студенту, если он:
По индикатору ИД-5пк-8 (сканирование IaC, безопасность контейнеров, статический анализ)

1. Самостоятельно разрабатывает и внедряет кастомные политики для Checkov/tfsec/Trivy, адаптированные под корпоративные требования безопасности.
2. Настраивает полностью автоматизированный Quality Gate в CI/CD-пайплайне, блокирующий деплой при обнаружении любых CRITICAL или HIGH уязвимостей.
3. Интегрирует статический анализ IaC в pre-commit хуки и CI/CD-пайплайн, обеспечивая «сдвиг влево» (Shift Left) для всех изменений инфраструктуры.
4. Документирует ложные срабатывания и умеет обоснованно отключать проверки с комментариями (# checkov:skip=...).
5. Генерирует **SBOM (Software Bill of Materials)** для образов и анализирует цепочку поставок (supply chain security).

По индикатору ИД-6пк-8 (безопасность CI/CD, OIDC, Quality Gates)

1. Настраивает OIDC-федерацию между CI/CD-системой (GitLab CI / GitHub Actions) и облачным провайдером без использования статических ключей доступа.
2. Реализует zero-trust пайплайн с разделением ролей, изолированными раннерами и минимальными правами для каждого этапа.
3. Внедряет подпись артефактов (Cosign/Sigstore) и проверку подписи на этапе деплоя.
4. Настраивает автоматический откат (rollback) при провале Quality Gate или сбое health-проверок после деплоя.
5. Интегрирует безопасность CI/CD с системой управления уязвимостями (DefectDojo, Jira X-Ray) и **SIEM**.

По индикатору ИД-7пк-8 (рантайм-мониторинг, сеть, mTLS, контейнеры)

1. Разворачивает Service Mesh (Istio/Linkerd) с mTLS в режиме STRICT, настраивает AuthorizationPolicy для микросегментации (Zero Trust).
2. Внедряет Pod Security Admission (PSA) в режиме enforce с кастомными исключениями для легитимных рабочих нагрузок.
3. Настраивает Falco/Tetragon для детектирования рантайм-аномалий (привилегированные операции, запуск шелла, монтирование sensitive path).
4. Организует централизованный SIEM (ELK / Wazuh / Grafana Loki) с корреляцией событий из облачных трейлов, логов приложений и Kubernetes audit.
5. Строит дашборды безопасности с ML-детекцией аномалий и историческими трендами.

По индикатору ИД-8пк-8 (Continuous Compliance, аудит, политики, BYOC, FinOps)

1. Проводит комплексный аудит облачной инфраструктуры с использованием минимум 3 инструментов (Prowler, ScoutSuite, Cloud Custodian, Checkov).
2. Разрабатывает библиотеку из 10+ кастомных OPA/Rego-политик с полным покрытием unit-тестами (opa test).
3. Внедряет полный цикл Continuous Compliance: политики → тесты → CI/CD Quality Gate → рантайм-аудит → дашборд Compliance Score.
4. Настраивает Cloud Custodian в режиме реального времени (event-driven) с автоматической коррекцией (auto-remediation) минимум для 3 типов нарушений.
5. Рассчитывает Compliance Score ≥ 95% и предоставляет детальный отчёт «Как было → Как стало» с измеримыми метриками (MTTR, количество нарушений, экономия).
6. Демонстрирует эксплуатацию найденных уязвимостей (Red Team) с последующим исправлением и повторным аудитом.

Общие требования для оценки «отлично»

- Все лабораторные работы (ЛР №1–-) выполнены **на повышенном уровне сложности**.
- Комплексный проект (ЛР №18) защищён с презентацией, демонстрацией и ответами на вопросы.
- Отчёт по проекту содержит сравнительный анализ ДО и ПОСЛЕ внедрения мер безопасности с графиками и метриками.
- Студент уверенно ориентируется в инструментах (Terraform, Vault, OPA, Istio, Prowler, Custodian, ELK) и может обосновать выбор архитектурных решений.

Оценка «хорошо» (4 балла) - средний уровень сформированности

Оценка «хорошо» выставляется студенту, если он:

1. Выполнил все лабораторные работы **на среднем уровне сложности**.
2. Настроил статический анализ IaC (Checkov/tfsec) в CI/CD, устранил все **CRITICAL и HIGH** нарушения, но кастомные политики не разрабатывал.
3. Настроил OIDC-федерацию для CI/CD, но Quality Gate может быть настроен с использованием статических ключей (или OIDC настроен не для всех этапов).
4. Внедрил mTLS в Istio и базовые AuthorizationPolicy, но не реализовал Falco/Tetragon или ML-детекцию.
5. Провёл аудит с использованием 1-2 инструментов, разработал **5–9 OPA-политик** с тестами.
6. Внедрил Cloud Custodian в режиме pull/periodic, автоматическая коррекция (auto-remediation) реализована частично или для 1 типа нарушений.
7. Compliance Score достиг **85–94%**.
8. Комплексный проект выполнен, отчёт содержит основные разделы, но может отсутствовать сравнительный анализ ДО/ПОСЛЕ или детальный Threat Modeling.

Оценка «удовлетворительно» (3 балла) - минимальный уровень сформированности

Оценка «удовлетворительно» выставляется студенту, если он:

1. Выполнил лабораторные работы на базовом уровне сложности (минимум 70% от общего объёма).
2. Установил и запустил Checkov/tfsec, может интерпретировать отчёт, но не интегрировал инструмент в CI/CD и не устранил все HIGH-нарушения.
3. Настроил базовый CI/CD-пайплайн, но использует **статические ключи доступа** (OIDC не настроен или настроен с ошибками).
4. Включил Pod Security Admission в режиме warn или audit (не enforce), mTLS в Istio не настроен или работает в режиме PERMISSIVE.
5. Провёл аудит одним инструментом (Prowler/ScoutSuite), получил HTML-отчёт, но **не** реализовал OPA-политики или реализовал 1–4 политики без тестов.
6. Cloud Custodian не внедрял или запустил в dry-run без автоматической коррекции.
7. Compliance Score составляет **70–84%**.
8. Комплексный проект выполнен частично, отчёт содержит базовые разделы, но отсутствуют развёрнутые рекомендации или план коррекции.
9. Студент отвечает на контрольные вопросы с помощью преподавателя (наводящие вопросы).

Оценка «неудовлетворительно» (2 балла) - минимальный уровень не достигнут

Оценка «неудовлетворительно» выставляется студенту, если он:

1. Не выполнил более 50% лабораторных работ или не предоставил отчёты по ним.
2. Не может установить и запустить базовые инструменты безопасности (Checkov, Trivy, Prowler).
3. Не понимает модели разделения ответственности, OIDC-федерации, mTLS, Compliance as Code.
4. Использует **хардкод секретов** в репозиториях или переменных CI/CD без шифрования/Vault.
5. Не провёл аудит облачной инфраструктуры или не предоставил отчёт.
6. OPA-политики не разработаны или содержат синтаксические ошибки, не проходят opa test.
7. Комплексный проект не выполнен или выполнен формально (копирование чужих конфигураций без понимания).
8. На контрольные вопросы **не отвечает** или демонстрирует полное отсутствие знаний по дисциплине.

Сводная таблица критериев оценивания

Критерий	**Отлично (5)**	**Хорошо (4)**	**Удовлетворительно (3)**	**Неудовлетворительно (2)**
Выполнение лабораторных работ (ЛР №1-17)	Повышенный уровень (100%)	Средний уровень (≥85%)	Базовый уровень (≥70%)	<50%
Статический анализ IaC	Кастомные политики +	Интеграция в	Базовый запуск,	Не выполнен

Критерий	Отлично (5)	Хорошо (4)	Удовлетворительно (3)	Неудовлетворительно (2)
(Checkov/tfsec)	pre-commit + Quality Gate	CI/CD, устранены CRITICAL	отчёт получен	
OIDC-федерация CI/CD	Полная OIDC + Cosign + auto-rollback	OIDC настроен	Статические ключи	Не настроен
mTLS и Service Mesh	STRICT + AuthorizationPolicy + Falco	STRICT + базовая политика	PERMISSIVE или не настроен	Отсутствует
OPA/Rego-политики	≥10 политик + unit-тесты	5–9 политик + тесты	1–4 политики без тестов	0 политик
Continuous Compliance (Custodian)	Event-driven + auto-remediation (3+ типов)	Periodic + частичная remediation	Dry-run только	Не настроен
Аудит (Prowler/ScoutSuite)	3+ инструмента + Threat Modeling	2 инструмента	1 инструмент	Не проведён
Compliance Score	≥95%	85–94%	70–84%	<70%
Комплексный проект (ЛР №18)	Полный отчёт + сравнительный анализ +	Полный отчёт	Базовый отчёт	Не выполнен

Критерий	Отлично (5)	Хорошо (4)	Удовлетворительно (3)	Неудовлетворительно (2)
	демо			
Ответы на контрольные вопросы	Уверенные, развёрнутые	С небольшими ошибками	С наводящими вопросами	Нет ответов

Шкала перевода баллов в итоговую оценку (зачёт с оценкой)

Набранные баллы (процент от максимума)	Оценка
90–100%	Отлично (5)
75–89%	Хорошо (4)
60–74%	Удовлетворительно (3)
менее 60%	Неудовлетворительно (2)

Для допуска к зачёту с оценкой студент должен:

- выполнить и защитить не менее 70% лабораторных работ (базовый уровень);
- выполнить и защитить комплексный проект (ЛР №18);
- предоставить отчёты в электронном виде в установленный срок.