Министерство науки и высшего образования Российской Федерации

ФГБОУ ВО «Дагестанский государственный технический университет»

ФОНД ОЦЕНОЧНЫХ СРЕДСТВ

по дисциплине «Системы мониторинга и управления инцидентами информационной безопасности»
(указывается индекс и наименование дисциплины)

Уровень образования — магистратура
(бакалавриат/магистратура/специалитет)

Направление подготовки — 10.04.01 Информационная безопасность
(код, наименование направления подготовки)

Направленность — Кибербразведка и противодействие угрозам с применением технологий искусственного интеллекта
(наименование)

Разработчик _____ Качаева Г.И., к.э.н.
(подпись) (ФИО, уч. степень, уч. звание)

Фонд оценочных средств обсужден на заседании кафедры ИБиПИ
«05» февраля 2026 г., протокол № 6/1

Зав. выпускающей кафедрой _____ Качаева Г.И., к.э.н.
(подпись) (ФИО, уч. степень, уч. звание)

г. Махачкала – 2026

СОДЕРЖАНИЕ

1. ПАСПОРТ ФОНДА ОЦЕНОЧНЫХ СРЕДСТВ

Фонд оценочных средств (далее - ФОС) является неотъемлемой частью рабочей программы дисциплины «Системы мониторинга и управления инцидентами информационной безопасности» и предназначен для контроля и оценки образовательных достижений обучающихся (в т.ч. самостоятельной работе обучающихся), освоивших программу данной дисциплины.

Целью разработки фонда оценочных средств является установление соответствия уровня подготовки обучающихся требованиям федерального государственного образовательного стандарта высшего образования (далее - ФГОС ВО) по направлению подготовки 10.04.01 Информационная безопасность.

Рабочей программой дисциплины «Системы мониторинга и управления инцидентами информационной безопасности» предусмотрено формирование следующих компетенций:

1) ПК-1 Способен разрабатывать и применять процедуры и интеллектуальные средства информационно-аналитических систем поддержки принятия решений по обеспечению информационной безопасности;
2) ПК-7 Способен руководить проектами по созданию комплексных систем искусственного интеллекта.

Формой аттестации по дисциплине является зачет.

2. РЕЗУЛЬТАТЫ ОСВОЕНИЯ ДИСЦИПЛИНЫ, ПОДЛЕЖАЩИЕ ПРОВЕРКЕ

В результате аттестации по дисциплине осуществляется комплексная проверка индикаторов достижения компетенций их формирования в процессе освоения ОПОП.

Таблица 1.

Результаты обучения: индикаторы достижения	**Формируемые компетенции**
ПК-1.3 Способен разрабатывать информационно-аналитические системы в сфере информационной безопасности	ПК- 1
ПК-7.1 Руководит разработкой архитектуры комплексных систем искусственного интеллекта	ПК-7

3. ОЦЕНКА ОСВОЕНИЯ ДИСЦИПЛИНЫ

3.1. Контроль и оценка освоения дисциплины по темам (разделам)

Предметом оценки служат индикаторы достижения компетенций, предусмотренные ОПОП, направленные на формирование профессиональных компетенций.

Таблица 2.

Элемент дисциплины	Формы и методы контроля			
	Текущий контроль		Промежуточная аттестация	
	Форма контроля	Проверяемые компетенции/ индикаторы достижения	Форма контроля	Проверяемые компетенции/ индикаторы достижения
Раздел 1. Технические решения мониторинга информационной безопасности				
Тема 1.1 Обзор современных технических решений мониторинга информационной безопасности	Письменная работа №1 Устный опрос Лабораторная работа №1 Самостоятельная работа Реферат	ПК-1: ПК-1.3; ПК-7: ПК-7.1	Зачетная работа	ПК-1: ПК-1.3; ПК-7: ПК-7.1
Тема 1.2 Источники сведений системы мониторинга информационной безопасности	Письменная работа №2 Устный опрос Лабораторная работа №2 Самостоятельная работа Реферат	ПК-1: ПК-1.3; ПК-7: ПК-7.1	Зачетная работа	ПК-1: ПК-1.3; ПК-7: ПК-7.1
Тема 1.3 Описание технического решения мониторинга Log Management	Письменная работа №3 Устный опрос Лабораторная работа №3 Самостоятельная работа Реферат	ПК-1: ПК-1.3; ПК-7: ПК-7.1	Зачетная работа	ПК-1: ПК-1.3; ПК-7: ПК-7.1
Тема 1.4 Централизованное хранилище журналов событий различных источников	Письменная работа №4 Устный опрос Лабораторная работа №4 Самостоятельная работа Реферат	ПК-1: ПК-1.3; ПК-7: ПК-7.1	Зачетная работа	ПК-1: ПК-1.3; ПК-7: ПК-7.1
Тема 1.5 Описание технического решения мониторинга SIEM-системы	Письменная работа №5 Устный опрос Лабораторная работа №5 Самостоятельная работа	ПК-1: ПК-1.3; ПК-7: ПК-7.1	Зачетная работа	ПК-1: ПК-1.3; ПК-7: ПК-7.1

	Реферат			
Тема 1.6 Выявление инцидентов с помощью MaxPatrol SIEM	Письменная работа №6 Устный опрос Лабораторная работа №6 Самостоятельная работа Реферат	ПК-1: ПК-1.3; ПК-7: ПК-7.1	Зачетная работа	ПК-1: ПК-1.3; ПК-7: ПК-7.1
Тема 1.7 Описание технического решения Threat Intelligence	Письменная работа №7 Устный опрос Лабораторная работа №7 Самостоятельная работа Реферат	ПК-1: ПК-1.3; ПК-7: ПК-7.1	Зачетная работа	ПК-1: ПК-1.3; ПК-7: ПК-7.1
Тема 1.8 Автоматизация процессов киберразведки на основе решений класса Threat Intelligence Platform	Письменная работа №8 Устный опрос Лабораторная работа №8 Самостоятельная работа Реферат	ПК-1: ПК-1.3; ПК-7: ПК-7.1	Зачетная работа	ПК-1: ПК-1.3; ПК-7: ПК-7.1
Раздел 2. Применение искусственного интеллекта при управлении информационной				
Тема 2.1 Организация системы безопасностью мониторинга информационной безопасности	Письменная работа №9 Устный опрос Лабораторная работа №9 Самостоятельная работа Реферат	ПК-1: ПК-1.3; ПК-7: ПК-7.1	Зачетная работа	ПК-1: ПК-1.3; ПК-7: ПК-7.1
Тема 2.2 Особенности организации системы мониторинга информационной безопасности от APT-атак	Письменная работа №10 Устный опрос Лабораторная работа №10 Самостоятельная работа Реферат	ПК-1: ПК-1.3; ПК-7: ПК-7.1	Зачетная работа	ПК-1: ПК-1.3; ПК-7: ПК-7.1
Тема 2.3 Интеллектуальный анализ событий информационной безопасности домена	Письменная работа №11 Устный опрос Лабораторная работа №11 Самостоятельная работа Реферат	ПК-1: ПК-1.3; ПК-7: ПК-7.1	Зачетная работа	ПК-1: ПК-1.3; ПК-7: ПК-7.1
Тема 2.4 Интеллектуальный	Письменная работа №12	ПК-1: ПК-1.3; ПК-7: ПК-7.1	Зачетная работа	ПК-1: ПК-1.3; ПК-7: ПК-7.1

анализ событий информационной безопасности Linux-серверов	Устный опрос Лабораторная работа №12 Самостоятельная работа Реферат			
Тема 2.5 Основы разработки информационно-аналитической системы в сфере ИБ	Письменная работа №13 Устный опрос Лабораторная работа №13 Самостоятельная работа Реферат	ПК-1: ПК-1.3; ПК-7: ПК-7.1	Зачетная работа	ПК-1: ПК-1.3; ПК-7: ПК-7.1
Тема 2.6 Этапы разработки информационно-аналитической системы в сфере ИБ	Письменная работа №14 Устный опрос Лабораторная работа №14 Самостоятельная работа Реферат	ПК-1: ПК-1.3; ПК-7: ПК-7.1	Зачетная работа	ПК-1: ПК-1.3; ПК-7: ПК-7.1
Тема 2.7 Применение моделей машинного обучения для анализа трафика	Письменная работа №15 Устный опрос Лабораторная работа №15 Самостоятельная работа Реферат	ПК-1: ПК-1.3; ПК-7: ПК-7.1	Зачетная работа	ПК-1: ПК-1.3; ПК-7: ПК-7.1
Тема 2.8 Применение методов машинного обучения для анализа трафика	Письменная работа №16 Устный опрос Лабораторная работа №16 Самостоятельная работа Реферат	ПК-1: ПК-1.3; ПК-7: ПК-7.1	Зачетная работа	ПК-1: ПК-1.3; ПК-7: ПК-7.1
Тема 2.9 Тренды и будущее SOC: автономные SOC, AI-driven security, конфиденциальные вычисления для анализа.	Письменная работа №17 Устный опрос Лабораторная работа №17 Самостоятельная работа Реферат	ПК-1: ПК-1.3; ПК-7: ПК-7.1	Зачетная работа	ПК-1: ПК-1.3; ПК-7: ПК-7.1

3.2. Перечень заданий для текущего контроля

Формируемая компетенция: ПК- 1

Перечень заданий закрытого типа

Задание № 1. Какой компонент современной SIEM-системы отвечает за автоматическое выполнение заранее заданных сценариев реагирования на инциденты?

A) ETL-процессор.
B) SOAR-движок.
C) Корреляционный движок.
D) База данных инцидентов.

Задание № 2. Какой из этапов разработки ИАС является первым и определяет её функциональные требования и архитектурный облик?

A) Написание пользовательской документации.
B) Разработка концепции и технического задания.
C) Выбор аппаратного обеспечения.
D) Тестирование производительности.

Задание № 3. Установите соответствие между компонентом архитектуры SOC (Security Operations Center) и его основной функцией.

Компонент архитектуры SOC	Основная функция
1. SIEM (Security Information and Event Management)	A) Автоматизация рутинных задач аналитика, исполнение плейбуков реагирования.
2. SOAR (Security Orchestration, Automation and Response)	B) Централизованный сбор, нормализация, корреляция событий безопасности и генерация алертов.
3. TIP (Threat Intelligence Platform)	C) Визуализация показателей, трендов и статуса безопасности на дашбордах.
4. База знаний и дашборды KPI	D) Агрегация, нормализация и управление индикаторами компрометации (IoC) из внешних источников.

Задание № 4. Установите соответствие между этапом жизненного цикла инцидента ИБ и типовой функцией ИАС, которая для него применяется.

Этап жизненного цикла инцидента	Функция ИАС
1. Обнаружение (Detection)	A) Формирование отчета, обновление правил корреляции и баз знаний на основе урока.
2. Анализ и эскалация (Analysis & Escalation)	B) Сбор дополнительных артефактов, изоляция зараженных систем, блокировка IoC.
3. Реагирование (Containment & Eradication)	C) Обогащение исходного алерта контекстом, оценка критичности, создание тикета.
4. Восстановление и извлечение уроков (Recovery & Lessons Learned)	D) Корреляция событий по заданным правилам, генерация алерта.

Задание № 5. Установите правильную последовательность основных этапов разработки информационно-аналитической системы поддержки принятия решений в сфере ИБ.

а) Спроектировать архитектуру системы и интерфейсы взаимодействия компонентов.
б) Согласовать и утвердить техническое задание на разработку.
в) Провести интеграционное тестирование системы в тестовом контуре.
г) Выполнить сбор и анализ требований от стейкхолдеров.
д) Развернуть систему в промышленную эксплуатацию и передать заказчику.
е) Разработать и согласовать техническое задание.
ж) Реализовать и протестировать отдельные модули системы.

Перечень заданий открытого типа

Задание № 1.Назовите ключевой компонент ИАС, который выполняет автоматическое сопоставление событий по заданным логическим правилам и временным окнам для выявления сложных атак.

Задание № 2. Какой класс алгоритмов машинного обучения наиболее часто применяется в системах UEBA для выявления отклонений от нормального поведения пользователя?

Задание № 3. Как называется документ, который является формальным результатом фазы проектирования ИАС и содержит детальные схемы взаимодействия компонентов, спецификации интерфейсов и требования к инфраструктуре?

Задание № 4. Дополните определение, вставляя пропущенное слово:

Формализованная последовательность действий для автоматического реагирования на конкретный тип инцидента безопасности в SOAR-системе называется _____.

Задание № 5. Дополните определение, вставляя пропущенное слово:

Компонент SIEM, отвечающий за сбор данных с конечных устройств через легковесных агентов, часто называется _____.

Формируемая компетенция: ПК-7

Перечень заданий закрытого типа

Задание № 1. На каком из этапов управления проектом по созданию комплексной системы ИИ для ИБ происходит формальное утверждение объёма работ, бюджета, ключевых ролей и графика высокого уровня?

A) На этапе мониторинга и контроля исполнения.
B) На этапе тестирования и ввода в эксплуатацию.
C) На этапе инициации проекта.
D) На этапе сбора требований.

Задание № 2. Какой архитектурный стиль наиболее предпочтителен для построения комплексной, масштабируемой и легко обновляемой системы ИИ, объединяющей модули сбора данных, ML-пайплайны и сервисы инференса?

A) Монолитная архитектура.
B) Архитектура на основе готовых коробочных решений.
C) Микросервисная архитектура.
D) Архитектура "большой файл скриптов".

Задание № 3. Установите соответствие между этапом разработки архитектуры комплексной системы ИИ и его ключевым результатом.

Этап разработки архитектуры	Ключевой результат
1. Анализ бизнес-требований и ограничений	A) Выбор конкретных технологий, фреймворков, протоколов и их версий.
2. Определение архитектурных паттернов и стилей	B) Утверждённый перечень нефункциональных требований: масштабируемость, отказоустойчивость, безопасность.
3. Выбор технологического стека	C) Концептуальная модель системы, диаграммы компонентов и взаимодействий.
4. Детальное проектирование	D) Чёткое понимание целей системы, KPI успеха, бюджетных и нормативных рамок.

Задание № 4. Установите соответствие между ключевым компонентом архитектуры безопасной системы ИИ для SOC и его основной функцией.

Компонент системы	Основная функция
1. Feature Store (Хранилище признаков)	A) Централизованное управление жизненным циклом моделей: версионирование, развертывание, мониторинг.
2. ML Metadata Store (Хранилище метаданных)	B) Обеспечение воспроизводимости экспериментов и аудита всех запусков обучения и оценки.

3. Model Registry (Реестр моделей)	C) Согласованное вычисление, хранение и обслуживание актуальных признаков для обучения и инференса.
4. Adversarial Robustness Module	D) Регулярная проверка моделей на устойчивость к состязательным атакам и генерация тестовых данных.

Задание № 5. Установите правильную последовательность ключевых этапов руководства проектом по созданию комплексной системы искусственного интеллекта для центра мониторинга безопасности.

а) Утвердить итоговый архитектурный проект системы и план его реализации.

б) Организовать работу проектной команды: распределить роли, зоны ответственности и утвердить график работ.

в) Согласовать с заказчиком концепцию, цели, ключевые требования и бюджет проекта.

г) Провести аудит и приемку готовой системы, передать документацию и обучить персонал заказчика.

д) Контролировать выполнение работ, проводить регулярные совещания и корректировать план при возникновении рисков.

е) Сформировать техническое задание на основании согласованной концепции.

ж) Согласовать с техническими специалистами выбор технологического стека и ключевых архитектурных решений.

Перечень заданий открытого типа

Задание № 1. Назовите ключевой компонент ИАС, который выполняет автоматическое сопоставление событий по заданным логическим правилам и временным окнам для выявления сложных атак.

Задание № 2. Какой класс алгоритмов машинного обучения наиболее часто применяется в системах UEBA для выявления отклонений от нормального поведения пользователя?

Задание № 3. Как называется документ, который является формальным результатом фазы проектирования ИАС и содержит детальные схемы взаимодействия компонентов, спецификации интерфейсов и требования к инфраструктуре?

Задание № 4. Дополните определение, вставляя пропущенное слово:

Технология _____, использующая такие инструменты как Docker и Kubernetes, является стандартом для упаковки и развертывания микросервисов системы ИИ, обеспечивая их изоляцию и переносимость.

Задание № 5. Дополните определение, вставляя пропущенное слово:

Ключевой показатель эффективности (KPI), измеряющий соотношение полезного результата проекта к понесённым затратам, называется _____ от инвестиций.

4. ПЕРЕЧЕНЬ ЗАДАНИЙ ДЛЯ ОЦЕНКИ СФОРМИРОВАННОСТИ КОМПЕТЕНЦИЙ

Формируемая компетенция: ПК-1

Перечень заданий закрытого типа

Задание № 1. Какой компонент современной SIEM-системы отвечает за автоматическое выполнение заранее заданных сценариев реагирования на инциденты?

A) ETL-процессор.
B) SOAR-движок.
C) Корреляционный движок.
D) База данных инцидентов.

Задание № 2. Какой из этапов разработки ИАС является первым и определяет её функциональные требования и архитектурный облик?

A) Написание пользовательской документации.
B) Разработка концепции и технического задания.
C) Выбор аппаратного обеспечения.
D) Тестирование производительности.

Задание № 3. Для чего в ИАС мониторинга ИБ применяется контекстное обогащение событий безопасности?

A) Для уменьшения объёма хранимых логов.
B) Для добавления к событию информации об активе, пользователе или индикаторах угроз, что повышает качество анализа.
C) Для шифрования передаваемых данных.
D) Для создания резервных копий данных.

Задание № 4. Какой open-source стек технологий является стандартом для построения систем централизованного логирования и часто служит основой для SIEM?

A) LAMP (Linux, Apache, MySQL, PHP).
B) Elastic Stack (Elasticsearch, Logstash, Kibana, Beats).
C) MEAN (MongoDB, Express.js, Angular, Node.js).
D) Kubernetes, Docker, Helm.

Задание № 5. Какой тип архитектурного стиля наиболее характерен для современных комплексных систем ИИ в сфере ИБ, обеспечивая гибкость, масштабируемость и независимое развертывание компонентов?

A) Монолитная архитектура.
B) Архитектура «клиент-сервер».
C) Микросервисная архитектура.
D) Peer-to-peer архитектура.

Задание № 6. Что является основной целью внедрения системы класса UEBA в составе ИАС?

A) Автоматическая установка патчей на конечные устройства.
B) Сканирование сети на наличие открытых портов.
C) Выявление аномалий в поведении пользователей и систем, указывающих на внутренние угрозы или скомпрометированные учетные записи.
D) Управление паролями и политиками доступа.

Задание № 7. Установите соответствие между компонентом архитектуры SOC (Security Operations Center) и его основной функцией.

Компонент архитектуры SOC	Основная функция
1. SIEM (Security Information and Event Management)	A) Автоматизация рутинных задач аналитика, исполнение плейбуков реагирования.
2. SOAR (Security Orchestration, Automation and Response)	B) Централизованный сбор, нормализация, корреляция событий безопасности и генерация

	алертов.
3. TIP (Threat Intelligence Platform)	C) Визуализация показателей, трендов и статуса безопасности на дашбордах.
4. База знаний и дашборды KPI	D) Агрегация, нормализация и управление индикаторами компрометации (IoC) из внешних источников.

Задание № 8. Установите соответствие между этапом жизненного цикла инцидента ИБ и типовой функцией ИАС, которая для него применяется.

Этап жизненного цикла инцидента	**Функция ИАС**
1. Обнаружение (Detection)	A) Формирование отчета, обновление правил корреляции и баз знаний на основе урока.
2. Анализ и эскалация (Analysis & Escalation)	B) Сбор дополнительных артефактов, изоляция зараженных систем, блокировка IoC.
3. Реагирование (Containment & Eradication)	C) Обогащение исходного алерта контекстом, оценка критичности, создание тикета.
4. Восстановление и извлечение уроков (Recovery & Lessons Learned)	D) Корреляция событий по заданным правилам, генерация алерта.

Задание № 9. Установите правильную последовательность основных этапов разработки информационно-аналитической системы поддержки принятия решений в сфере ИБ.

а) Спроектировать архитектуру системы и интерфейсы взаимодействия компонентов.
б) Согласовать и утвердить техническое задание на разработку.
в) Провести интеграционное тестирование системы в тестовом контуре.
г) Выполнить сбор и анализ требований от стейкхолдеров.
д) Развернуть систему в промышленную эксплуатацию и передать заказчику.
е) Разработать и согласовать техническое задание.
ж) Реализовать и протестировать отдельные модули системы.

Задание № 10. Установите правильную последовательность действий при проектировании архитектуры нового модуля корреляции событий для интеграции в существующую SIEM-платформу.

а) Определить форматы и протоколы для приема данных от внешних источников угроз.
б) Прототипировать и испытать ядро нового модуля на исторических данных.
в) Проанализировать ограничения и возможности API существующей SIEM-платформы.
г) Составить технический проект модуля, специфицировать его интерфейсы.
д) Выбрать методы и алгоритмы корреляции событий на основе тактик MITRE ATT&CK.
е) Сформулировать цели и требования к новому модулю на основе анализа пробелов текущей системы.
ж) Утвердить проект и план внедрения модуля.

Перечень заданий открытого типа

Задание № 1.Назовите ключевой компонент ИАС, который выполняет автоматическое сопоставление событий по заданным логическим правилам и временным окнам для выявления сложных атак.

Задание № 2. Какой класс алгоритмов машинного обучения наиболее часто применяется в системах UEBA для выявления отклонений от нормального поведения пользователя?

Задание № 3. Как называется документ, который является формальным результатом фазы проектирования ИАС и содержит детальные схемы взаимодействия компонентов, спецификации интерфейсов и требования к инфраструктуре?

Задание № 4. Какой принцип проектирования безопасных систем предполагает, что каждому компоненту предоставляются минимально необходимые права доступа для выполнения его функций?

Задание № 5. Дополните определение, вставляя пропущенное слово:
Формализованная последовательность действий для автоматического реагирования на конкретный тип инцидента безопасности в SOAR-системе называется _____.

Задание № 6. Дополните определение, вставляя пропущенное слово:
Компонент SIEM, отвечающий за сбор данных с конечных устройств через легковесных агентов, часто называется _____.

Формируемая компетенция: ПК-7

Перечень заданий закрытого типа

Задание № 1. На каком из этапов управления проектом по созданию комплексной системы ИИ для ИБ происходит формальное утверждение объёма работ, бюджета, ключевых ролей и графика высокого уровня?
A) На этапе мониторинга и контроля исполнения.
B) На этапе тестирования и ввода в эксплуатацию.
C) На этапе инициации проекта.
D) На этапе сбора требований.

Задание № 2. Какой архитектурный стиль наиболее предпочтителен для построения комплексной, масштабируемой и легко обновляемой системы ИИ, объединяющей модули сбора данных, ML-пайплайны и сервисы инференса?
A) Монолитная архитектура.
B) Архитектура на основе готовых коробочных решений.
C) Микросервисная архитектура.
D) Архитектура "большой файл скриптов".

Задание № 3. Какой из перечисленных компонентов НЕ является типичным для архитектуры комплексной системы ИИ в сфере ИБ, построенной по принципам MLOps?
A) Хранилище признаков .
B) Реестр моделей и система версионирования.
C) Единая реляционная база данных для хранения всех логов, сырых данных и метаданных моделей.
D) Конвейер CI/CD для моделей машинного обучения.

Задание № 4. Какой ключевой документ, создаваемый архитектором на ранней стадии, визуализирует высокоуровневую структуру системы, ключевые технологические решения и потоки данных между основными компонентами?
A) Пользовательская история .
B) Диаграмма архитектуры решения.
C) Отчет о тестировании.
D) План коммуникаций с заказчиком.

Задание № 5. Руководитель проекта вносит в план рисков вероятность того, что выбранная открытая ML-библиотека может содержать уязвимость, приводящую к компрометации модели. Какой тип риска это представляет?
A) Операционный риск.
B) Риск безопасности цепочки поставок (Supply Chain Risk).
C) Финансовый риск перерасхода бюджета.
D) Риск несоответствия требованиям законодательства.

Задание № 6. Какой критерий является наименее значимым при выборе между облачной и on-premise инфраструктурой для развертывания системы ИИ, обрабатывающей конфиденциальные данные разведки?
A) Требования к задержке при обработке данных в реальном времени.
B) Стоимость месячной подписки на облачные сервисы.
C) Нормативные требования к локализации и суверенитету данных.
D) Наличие у команды экспертизы по администрированию выбранной платформы.

Задание № 7. Установите соответствие между этапом разработки архитектуры комплексной системы ИИ и его ключевым результатом.

Этап разработки архитектуры	Ключевой результат
1. Анализ бизнес-требований и ограничений	A) Выбор конкретных технологий, фреймворков, протоколов и их версий.
2. Определение архитектурных паттернов и стилей	B) Утверждённый перечень нефункциональных требований: масштабируемость, отказоустойчивость, безопасность.
3. Выбор технологического стека	C) Концептуальная модель системы, диаграммы компонентов и взаимодействий.
4. Детальное проектирование	D) Чёткое понимание целей системы, KPI успеха, бюджетных и нормативных рамок.

Задание № 8. Установите соответствие между ключевым компонентом архитектуры безопасной системы ИИ для SOC и его основной функцией.

Компонент системы	Основная функция
1. Feature Store (Хранилище признаков)	A) Централизованное управление жизненным циклом моделей: версионирование, развертывание, мониторинг.
2. ML Metadata Store (Хранилище метаданных)	B) Обеспечение воспроизводимости экспериментов и аудита всех запусков обучения и оценки.
3. Model Registry (Реестр моделей)	C) Согласованное вычисление, хранение и обслуживание актуальных признаков для обучения и инференса.
4. Adversarial Robustness Module	D) Регулярная проверка моделей на устойчивость к состязательным атакам и генерация тестовых данных.

Задание № 9. Установите правильную последовательность ключевых этапов руководства проектом по созданию комплексной системы искусственного интеллекта для центра мониторинга безопасности.

а) Утвердить итоговый архитектурный проект системы и план его реализации.

б) Организовать работу проектной команды: распределить роли, зоны ответственности и утвердить график работ.

в) Согласовать с заказчиком концепцию, цели, ключевые требования и бюджет проекта.

г) Провести аудит и приемку готовой системы, передать документацию и обучить персонал заказчика.

д) Контролировать выполнение работ, проводить регулярные совещания и корректировать план при возникновении рисков.

е) Сформировать техническое задание на основании согласованной концепции.

ж) Согласовать с техническими специалистами выбор технологического стека и ключевых архитектурных решений.

Задание № 10. Установите правильную последовательность ключевых этапов руководства проектом по созданию комплексной системы искусственного интеллекта для центра мониторинга безопасности.

а) Утвердить итоговый архитектурный проект системы и план его реализации.

б) Организовать работу проектной команды: распределить роли, зоны ответственности и утвердить график работ.

в) Согласовать с заказчиком концепцию, цели, ключевые требования и бюджет проекта.

г) Провести аудит и приемку готовой системы, передать документацию и обучить персонал заказчика.

д) Контролировать выполнение работ, проводить регулярные совещания и корректировать план при возникновении рисков.

е) Сформировать техническое задание на основании согласованной концепции.

ж) Согласовать с техническими специалистами выбор технологического стека и ключевых архитектурных решений.

Перечень заданий открытого типа

Задание № 1. Назовите ключевой документ, фиксирующий договорённости между заказчиком и исполнителем по целям, содержанию, срокам, стоимости и критериям приёмки проекта.

Задание № 2. Как называется организационная структура проекта, в которой участники подчиняются как руководителю проекта, так и своему функциональному руководителю?

Задание № 3. Какой класс диаграмм в нотации UML наиболее часто используется на этапе проектирования архитектуры для отображения статической структуры системы в виде компонентов, классов и их взаимосвязей?

Задание № 4. Какая методология управления проектами, основанная на коротких итеративных циклах разработки , наиболее распространена при создании гибких комплексных систем ИИ?

Задание № 5. Дополните определение, вставляя пропущенное слово:

Технология _____, использующая такие инструменты как Docker и Kubernetes, является стандартом для упаковки и развертывания микросервисов системы ИИ, обеспечивая их изоляцию и переносимость.

Задание № 6. Дополните определение, вставляя пропущенное слово:

Ключевой показатель эффективности, измеряющий соотношение полезного результата проекта к понесённым затратам, называется _____ от инвестиций.

5. КРИТЕРИИ ОЦЕНКИ

5.1. Критерии оценки текущего контроля и промежуточной аттестации

В ФГБОУ ВО «ДГТУ» внедрена модульно-рейтинговая система оценки учебной деятельности обучающихся. В соответствии с этой системой применяются пятибальная, двадцатибальная и стобальная шкалы знаний, умений, навыков.

Таблица 3.

Шкалы оценивания			**Критерии оценивания**
пятибальная	двадцатибальная	стобальная	
«Отлично» - 5 баллов	«Отлично» - 18-20 баллов	«Отлично» - 85 – 100 баллов	Показывает высокий уровень сформированности компетенций, т.е.: – продемонстрирует глубокое и прочное усвоение материала; – исчерпывающе, четко, последовательно, грамотно и логически стройно излагает теоретический материал; – правильно формирует определения; – демонстрирует умения самостоятельной работы с нормативно-правовой литературой; – умеет делать выводы по излагаемому материалу.
«Хорошо» - 4 баллов	«Хорошо» - 15 - 17 баллов	«Хорошо» - 70 - 84 баллов	Показывает достаточный уровень сформированности компетенций, т.е.: – демонстрирует достаточно полное знание материала, основных теоретических положений; – достаточно последовательно, грамотно логически стройно излагает материал; – демонстрирует умения ориентироваться в нормальной литературе; – умеет делать достаточно обоснованные выводы по излагаемому материалу.
«Удовлетворительно» - 3 баллов	«Удовлетворительно» - 12 - 14 баллов	«Удовлетворительно» - 56 – 69 баллов	Показывает пороговый уровень сформированности компетенций, т.е.: – демонстрирует общее знание изучаемого материала; – испытывает серьезные затруднения при ответах на дополнительные вопросы; – знает основную рекомендуемую литературу; – умеет строить ответ в соответствии со структурой излагаемого материала.
«Неудовлетворительно» - 2 баллов	«Неудовлетворительно» - 1-11 баллов	«Неудовлетворительно» - 1-55 баллов	Ставится в случае: – незнания значительной части программного материала; – не владения понятийным аппаратом дисциплины; – допущения существенных ошибок при изложении учебного материала; – неумение строить ответ в соответствии со структурой излагаемого вопроса; – неумение делать выводы по излагаемому материалу.

Критерии оценки тестовых заданий

Таблица 4.

Процент выполненных тестовых заданий	**Оценка**
до 50%	неудовлетворительно
50-69%	удовлетворительно
70-84%	хорошо
85-100%	отлично

Критерии оценки тестовых заданий, заданий на дополнение, с развернутым ответом и на установление правильной последовательности

Верный ответ - 2 балла.
Неверный ответ или его отсутствие - 0 баллов.

Критерии оценки заданий на сопоставление

Верный ответ - 2 балла
1 ошибка - 1 балл
более 1-й ошибки или ответ отсутствует - 0 баллов.

КЛЮЧИ К ЗАДАНИЯМ ДЛЯ ТЕКУЩЕГО КОНТРОЛЯ

Таблица 5.

Формируемые компетенции	№ задания	Ответ
ПК-1	**Задания закрытого типа**	
	№ 1	B)
	№ 2	B)
	№ 3	1 — B, 2 — A, 3 — D, 4 — C
	№ 4	1 — D, 2 — C, 3 — B, 4 — A
	№ 5	гебажвд
	Задания открытого типа	
	№ 1	Корреляционный движок
	№ 2	Алгоритмы обнаружения аномалий
	№ 3	Технический проект
	№ 4	плейбук
	№ 5	Forwarder
ПК-7	**Задания закрытого типа**	
	№ 1	C)
	№ 2	C)
	№ 3	1 — D, 2 — B, 3 — A, 4 — C
	№ 4	1 — C, 2 — B, 3 — A, 4 — D
	№ 5	вебжадг
	Задания открытого типа	
	№ 1	Устав проекта
	№ 2	Матричная структура
	№ 3	Диаграмма компонентов
	№ 4	контейнеризация
	№ 5	возврат

КЛЮЧИ К ЗАДАНИЯМ ДЛЯ ОЦЕНКИ СФОРМИРОВАННОСТИ КОМПЕТЕНЦИЙ

Таблица 6.

Формируемые компетенции	№ задания	Ответ
ПК-1	**Задания закрытого типа**	
	№ 1	B)
	№ 2	B)
	№ 3	B)
	№ 4	B)
	№ 5	C)
	№ 6	C)
	№ 7	1 — B, 2 — A, 3 — D, 4 — C
	№ 8	1 — D, 2 — C, 3 — B, 4 — A
	№ 9	гебажвд
	№ 10	евдагбж
	Задания открытого типа	
	№ 1	Корреляционный движок
	№ 2	Алгоритмы обнаружения аномалий
	№ 3	Технический проект
	№ 4	Принцип наименьших привилегий
	№ 5	плейбук
	№ 6	Forwarder
ПК-7	**Задания закрытого типа**	
	№ 1	C)
	№ 2	C)
	№ 3	C)
	№ 4	B)
	№ 5	B)
	№ 6	B)
	№ 7	1 — D, 2 — B, 3 — A, 4 — C
	№ 8	1 — C, 2 — B, 3 — A, 4 — D
	№ 9	вебжадг
	№ 10	гвдаеб
	Задания открытого типа	
	№ 1	Устав проекта
	№ 2	Матричная структура
	№ 3	Диаграмма компонентов
	№ 4	Гибкая методология
	№ 5	контейнеризация
	№ 6	возврат