Министерство науки и высшего образования Российской Федерации

ФГБОУ ВО «Дагестанский государственный технический университет»

ФОНД ОЦЕНОЧНЫХ СРЕДСТВ

по дисциплине «Интеллектуальные системы информационной безопасности в здравоохранении»
(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 «Интеллектуальные системы информационной безопасности в здравоохранении» 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 «Интеллектуальные системы информационной безопасности в здравоохранении» 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-2 Способен выполнять мониторинг и ситуационный анализ обстановки в сфере информационной безопасности;*
3) *ПК-3 Способен исследовать и разрабатывать архитектуры систем искусственного интеллекта для различных предметных областей на основе комплексов методов и инструментальных средств систем искусственного интеллекта;*
4) *ПК -5 Способен разрабатывать и модернизировать программное и аппаратное обеспечение технологий и систем искусственного интеллекта с учетом требований информационной безопасности в различных предметных областях;*
5) *ПК-7 Способен руководить проектами по созданию комплексных систем искусственного интеллекта*

Формой аттестации по дисциплине является экзамен.

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-1.1 Способен решать задачи анализа данных в целях обеспечения информационной безопасности	ПК- 1
ПК-1.3 Способен разрабатывать информационно-аналитические системы в сфере информационной безопасности	
ПК- 2.1 Способен формализовывать задачи информационно-аналитической поддержки принятия решений в сфере информационной безопасности	ПК-2
ПК –3.1 Выбирает комплексы методов и инструментальных средств искусственного интеллекта для решения задач в зависимости от особенностей предметной области	ПК-3
ПК-5.1 Разрабатывает программное и аппаратное обеспечение технологий и систем искусственного	ПК -5

интеллекта для решения профессиональных задач с учетом требований информационной безопасности в различных предметных областях	
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
Тема 1. Особенности предметной области «Здравоохранение» как объекта защиты	Письменная работа №1 Устный опрос Лабораторная работа №1 Самостоятельная работа Реферат	ПК-1: ПК-1.1; ПК-1.3; ПК-2: ПК-2.1; ПК-3: ПК-3.1	Экзаменационная работа	ПК-1: ПК-1.1; ПК-1.3; ПК-2: ПК-2.1; ПК-3: ПК-3.1
Тема 2. Нормативно-правовая база ИБ в здравоохранении	Письменная работа №2 Устный опрос Лабораторная работа №2 Самостоятельная работа Реферат	ПК-1: ПК-1.1; ПК-1.3; ПК-2: ПК-2.1; ПК-3: ПК-3.1	Экзаменационная работа	ПК-1: ПК-1.1; ПК-1.3; ПК-2: ПК-2.1; ПК-3: ПК-3.1
Тема 3. Архитектура интеллектуальных систем ИБ для медицинских организаций	Письменная работа №3 Устный опрос Лабораторная работа №3 Самостоятельная работа Реферат	ПК-1: ПК-1.1; ПК-1.3; ПК-2: ПК-2.1; ПК-3: ПК-3.1	Экзаменационная работа	ПК-1: ПК-1.1; ПК-1.3; ПК-2: ПК-2.1; ПК-3: ПК-3.1
Тема 4. Интеллектуальный анализ медицинских логов и событий безопасности	Письменная работа №4 Устный опрос Лабораторная работа №4 Самостоятельная работа Реферат	ПК-1: ПК-1.1; ПК-1.3; ПК-2: ПК-2.1; ПК-3: ПК-3.1	Экзаменационная работа	ПК-1: ПК-1.1; ПК-1.3; ПК-2: ПК-2.1; ПК-3: ПК-3.1
Тема 5. Проактивное обнаружение угроз с помощью ИИ	Письменная работа №5 Устный опрос Лабораторная работа №5 Самостоятельная работа	ПК-1: ПК-1.1; ПК-1.3; ПК-2: ПК-2.1; ПК-3: ПК-3.1	Экзаменационная работа	ПК-1: ПК-1.1; ПК-1.3; ПК-2: ПК-2.1; ПК-3: ПК-3.1

	Реферат			
Тема 6. Защита систем медицинской диагностики с использованием ИИ	Письменная работа №6 Устный опрос Лабораторная работа №6 Самостоятельная работа Реферат	ПК-1: ПК-1.1; ПК-1.3; ПК-2: ПК-2.1; ПК-3: ПК-3.1	Экзаменационная работа	ПК-1: ПК-1.1; ПК-1.3; ПК-2: ПК-2.1; ПК-3: ПК-3.1
Тема 7. **Интеллектуальные SOAR-платформы (Security Orchestration, Automation and Response) для медицины**	Письменная работа №7 Устный опрос Лабораторная работа №7 Самостоятельная работа Реферат	ПК-1: ПК-1.1; ПК-1.3; ПК-2: ПК-2.1; ПК-3: ПК-3.1	Экзаменационная работа	ПК-1: ПК-1.1; ПК-1.3; ПК-2: ПК-2.1; ПК-3: ПК-3.1
Тема 8. **Безопасность данных в геномике, биоинформатике и персонализированной медицине**	Письменная работа №8 Устный опрос Лабораторная работа №8 Самостоятельная работа Реферат	ПК-1: ПК-1.1; ПК-1.3; ПК-2: ПК-2.1; ПК-3: ПК-3.1; ПК-5: ПК-5.1 ПК-7: ПК-71.1	Экзаменационная работа	ПК-1: ПК-1.1; ПК-1.3; ПК-2: ПК-2.1; ПК-3: ПК-3.1; ПК-5: ПК-5.1 ПК-7: ПК-71.1
Тема 9. **Тренды и стратегическое управление: ИИ для прогнозирования уязвимостей и кибератак в здравоохранении**	Письменная работа №9 Устный опрос Лабораторная работа №9 Самостоятельная работа Реферат	ПК-1: ПК-1.1; ПК-1.3; ПК-2: ПК-2.1; ПК-3: ПК-3.1; ПК-5: ПК-5.1 ПК-7: ПК-71.1	Экзаменационная работа	ПК-1: ПК-1.1; ПК-1.3; ПК-2: ПК-2.1; ПК-3: ПК-3.1; ПК-5: ПК-5.1 ПК-7: ПК-71.1

3.2. Перечень заданий для текущего контроля

Формируемая компетенция: ПК-1

Перечень заданий закрытого типа

Задание № 1. Для сбалансированной оценки качества работы интеллектуальной системы обнаружения вторжений на основе машинного обучения, анализирующей сетевой трафик, чаще всего используют метрику, представляющую собой гармоническое среднее между точностью и полнотой. Эта метрика называется:
A) Доступность
B) Точность
C) F1-мера
D) Аудит

Задание № 2. Какой технологический стандарт или методика используется для формализованного описания тактик, техник и процедур злоумышленников при расследовании киберинцидентов в медицинской информационной системе?
A) ITIL
B) GDPR
C) MITRE ATT&CK
D) ISO 27001

Задание № 3. Установите соответствие между ключевым компонентом архитектуры интеллектуальной системы информационной безопасности для медицинской организации и его основной функцией.

Компонент системы	Основная функция
1. SIEM-платформа	A) Автоматическое выполнение сценариев реагирования на инциденты (например, блокировка учетной записи).
2. SOAR-платформа	B) Непрерывный сбор, нормализация и корреляция событий безопасности из различных источников (логи МИС, сетевого оборудования).
3. DLP-система	C) Мониторинг и предотвращение утечек конфиденциальных медицинских данных за пределы организации.
4. Система моделирования угроз	D) Формализованное описание активов, уязвимостей и возможных векторов атак на медицинскую сеть.

Задание № 4. Установите соответствие между технологией защиты данных в здравоохранении и решаемой с её помощью задачей.

Технология	Решаемая задача
1. Дифференциальная приватность	A) Обеспечение возможности проведения вычислений (например, диагностики) непосредственно на зашифрованных медицинских изображениях.
2. Гомоморфное шифрование	B) Гарантия того, что добавление или удаление одной записи пациента из обучающей выборки не окажет значимого влияния на результат статистического анализа.
3. Многопартийные вычисления	C) Совместный анализ геномных данных из нескольких медицинских центров без передачи самих исходных данных в единый

	центр.
4. Анонимизация	D) Удаление прямых идентификаторов (ФИО, паспорт) из набора медицинских данных для использования в научных исследованиях.

Задания № 5. Установите правильную последовательность этапов разработки прототипа интеллектуального модуля обнаружения аномалий в работе медицинского IoT-оборудования:
а) Выбор и обучение модели машинного обучения на данных, собранных в нормальном режиме работы.
б) Сбор и предобработка телеметрических данных с датчиков и эмуляторов.
в) Анализ предметной области: изучение протоколов, типов датчиков и моделирование угроз.
г) Интерпретация результатов работы модели, формирование отчета с рекомендациями.
д) Развертывание модели в тестовом контуре и настройка порогов срабатывания.

Перечень заданий открытого типа

Задание № 1. Назовите ключевую Python-библиотеку, предоставляющую структуры данных DataFrame и Series и инструменты для эффективного анализа и предобработки табличных данных, например, логов безопасности.

Задание № 2. Как называется класс атак на системы машинного обучения, при котором злоумышленник вносит малозаметные искажения во входные данные (например, рентгеновский снимок), чтобы вызвать ошибочное предсказание модели?

Задание № 3. Какой принцип информационной безопасности гарантирует, что медицинские данные, хранящиеся в PACS (архиве изображений), не были изменены несанкционированно?

Задание № 4. Непрерывный процесс автоматической интеграции изменений кода от разных разработчиков в общую основную ветку с последующим автоматическим тестированием и развертыванием называется _____ интеграцией и доставкой.

Задание № 5. Формализованное описание этапов кибератаки от первоначальной разведки до достижения цели и сокрытия следов в виде тактик и техник называется _____ кибератаки.

Формируемая компетенция: ПК-2

Перечень заданий закрытого типа

Задания № 1. Какой документ является основным результатом формализации задачи по разработке системы ситуационной осведомлённости (Security Operations Center) для сети крупной больницы и содержит детальные требования к источникам данных, аналитическим функциям и интерфейсам?
A) Презентация для инвесторов.
B) Техническое задание.
C) Годовой финансовый план.
D) Рекламный буклет.

Задание № 2. После анализа защищенности телемедицинской платформы выявлен риск утечки видеоконсультаций из-за отсутствия шифрования трафика. Какой из перечисленных форматов наименее подходит для формализации задачи по устранению этого риска в виде конкретного поручения?
A) Запись в реестре рисков с указанием ответственного и срока.
B) Отчет о количестве проведенных консультаций за месяц.
C) Техническое задание на настройку VPN или TLS.

D) Чек-лист действий для администратора сети.

Задания № 3. Установите соответствие между этапом формализации задачи мониторинга ИБ для медицинской организации и его ключевым результатом.

Этап формализации	Ключевой результат
1. Определение целей	A) Модель угроз для МИС, PACS и медицинского IoT, описывающая активы и векторы атак.
2. Анализ контекста и активов	B) Четкая формулировка: "Снизить среднее время обнаружения аномального доступа к ЭМК до X минут".
3. Определение источников данных	C) Перечень: журналы доступа МИС, NetFlow, алерты SIEM, логи межсетевых экранов.
4. Определение метрик эффективности	D) Количественные показатели: процент ложных срабатываний, полнота обнаружения инцидентов.

Задание № 4. Установите соответствие между методом обработки данных для ситуационного анализа в здравоохранении и его описанием.

Метод обработки данных	Описание
1. Корреляция событий	A) Анализ последовательности действий пользователя в МИС для выявления аномальных поведенческих паттернов, характерных для инсайдера.
2. Поведенческий анализ (UEBA)	B) Связывание события блокировки учетной записи в Active Directory с попыткой доступа к серверу БД пациентов из той же сети для выявления цепочки атаки.
3. Анализ временных рядов данных датчиков IoT	C) Выявление отклонений в периодичности передачи показаний кардиомонитора, что может указывать на сбой устройства или манипуляцию данными.
4. Сбор индикаторов компрометации (IoC)	D) Использование актуальных списков вредоносных IP-адресов и хэшей для поиска уже известных угроз в сети.

Задания № 5. Установите правильную последовательность действий по формализации задачи для создания системы мониторинга целостности конфигураций медицинского сетевого оборудования.

а) Согласовать с сетевыми администраторами допустимые методы и окна для проведения сканирований.

б) Сформулировать итоговую постановку задачи в виде ТЗ, включающего цели, источники данных и критерии.

в) Определить перечень критического оборудования (маршрутизаторы, коммутаторы) и эталонные конфигурации.

г) Проанализировать требования стандартов и типовые угрозы целостности сетевой инфраструктуры.

д) Выбрать методы и инструменты для безопасного автоматизированного сбора и сравнения конфигураций.

Перечень заданий открытого типа

Задание № 1. Как называется основной открытый фреймворк, используемый для формализации и описания тактик, техник и процедур (TTPs) киберпротивников?

Задания № 2. Какой класс сетевых протоколов, часто используемых в медицинском оборудовании (например, для мониторов), исторически характеризуется отсутствием встроенных механизмов безопасности, что критично для формализации задач по их защите?

Задания № 3. Какой подход к обработке данных в мониторинге подразумевает их анализ в реальном времени по мере поступления и используется для задач, требующих немедленного реагирования?

Задания № 4. Подход к управлению безопасностью, при котором меры защиты выбираются и приоритезируются на основе оценки _____, называется риск-ориентированным подходом.

Задания № 5. Анализ _____, проводимый после инцидента, направлен на выявление глубинных организационных и технических причин, а не просто констатацию факта сбоя.

Формируемая компетенция: ПК-3

Перечень заданий закрытого типа

Задание № 1. Для задачи автоматической классификации сетевых пакетов в системе мониторинга больницы на «нормальные» и «вредоносные» на основе их заголовков и временных меток, какой класс алгоритмов машинного обучения является наиболее подходящим для начального прототипа?
A) Кластеризация (без учителя).
B) Классификация (с учителем).
C) Понижение размерности.
D) Рекомендательные системы.

Задания № 2. Для выявления ранее неизвестных аномальных паттернов в поведении пользователей медицинской информационной системы, когда размеченных данных об атаках недостаточно, какой подход машинного обучения является приоритетным?
A) Обучение с подкреплением.
B) Обучение с учителем.
C) Обучение без учителя.
D) Трансферное обучение.

Задания № 3. Установите соответствие между задачей информационной безопасности в медицинской организации и наиболее подходящим для её решения комплексом методов искусственного интеллекта.

Задача ИБ в здравоохранении	**Комплекс методов ИИ**
1. Анализ рентгеновских снимков на предмет признаков их алгоритмической модификации (adversarial attacks).	A) Методы обработки естественного языка (NLP) для классификации текста.
2. Прогнозирование периодов повышенного риска DDoS-атак на портал телемедицины на основе исторических данных.	B) Глубокое обучение на основе сверточных нейронных сетей (CNN).
3. Автоматическая категоризация инцидентов, описанных в текстовых отчетах аналитиков, по тактикам MITRE ATT&CK.	C) Методы анализа временных рядов и регрессионного прогнозирования.
4. Обнаружение аномалий в сетевом трафике медицинских IoT-устройств (например, инфузионных насосов) без заранее известных шаблонов атак.	D) Методы обучения без учителя, такие как Isolation Forest или Autoencoders.

Задания № 4. Установите соответствие между инструментальным средством/платформой ИИ и ключевой областью его применения в контексте разработки систем безопасности.

Инструментальное средство / Платформа	Ключевая область применения в разработке систем ИБ
1. TensorFlow / PyTorch	A) Создание и обучение пользовательских моделей глубокого обучения (нейронных сетей).
2. Scikit-learn	B) Быстрое прототипирование и построение конвейеров данных для машинного обучения.
3. spaCy / NLTK	C) Работа с классическими алгоритмами ML (классификация, регрессия, кластеризация) и предобработка данных.
4. Jupyter Notebook / Google Colab	D) Обработка и анализ текстовых данных (логи, отчеты) с помощью NLP.

Задания № 5. Установите правильную последовательность основных этапов выбора и применения методов ИИ для решения задачи классификации вредоносного трафика в сети больницы:
а) Выбор и обучение конкретной модели (например, градиентного бустинга или нейронной сети) на подготовленных данных.
б) Формулировка бизнес-задачи и определение критериев успеха (точность, полнота).
в) Предобработка и разметка собранных сетевых данных (нормализация, создание признаков).
г) Сбор и анализ данных о сетевом трафике.
д) Оценка модели на тестовой выборке и интерпретация результатов.

Перечень заданий открытого типа

Задание № 1. Какая популярная открытая библиотека для Python является де-факто стандартом для реализации и обучения глубоких нейронных сетей с использованием динамических вычислительных графов?

Задания № 2. Как называется тип обучения модели машинного обучения, при котором используется заранее размеченный набор данных, где каждому примеру присвоен правильный ответ?

Задания № 3. Какая область искусственного интеллекта, основанная на работе с большими объемами текстовых данных, используется для анализа инцидентов безопасности, описанных в естественном языке?

Задания № 4. Процесс, при котором модель машинного обучения настраивает свои внутренние параметры на обучающих данных для минимизации ошибки, называется _____ модели.

Задания № 5. Тип данных, для эффективной обработки которых сверточные нейронные сети (CNN) стали основным инструментом в ИИ, — это _____.

Формируемая компетенция: ПК-5

Перечень заданий закрытого типа

Задание № 1. При разработке модуля системы ИИ, обрабатывающего конфиденциальные данные пациентов, для обеспечения принципа конфиденциальности на уровне приложения необходимо в первую очередь реализовать:
A) Резервное копирование данных.
B) Шифрование данных при хранении и передаче.
C) Мониторинг температуры сервера.
D) Логирование всех действий.

Задания № 2. Какой подход к проектированию архитектуры системы машинного обучения для диагностики по снимкам минимизирует риски утечки исходных медицинских изображений при использовании облачных сервисов?
A) Загрузка всех данных в публичное облако для обучения.
B) Использование гомоморфного шифрования для обработки данных без их расшифровки.
C) Передача изображений по незащищенному протоколу HTTP.
D) Хранение приватных ключей шифрования вместе с данными.

Задания № 3. Установите соответствие между этапом жизненного цикла системы ИИ в здравоохранении и ключевой мерой информационной безопасности, которую необходимо реализовать на данном этапе.

Этап жизненного цикла системы ИИ	**Ключевая мера информационной безопасности**
1. Сбор и подготовка данных	A) Контроль целостности и аутентичности обновлений модели, проверка цифровых подписей.
2. Обучение модели	B) Аудит доступа к данным, маскирование или псевдонимизация персональных данных пациентов.
3. Развертывание и эксплуатация	C) Изоляция тренировочного кластера от производственной сети, защита от утечек через метаданные.
4. Обновление и вывод из эксплуатации	D) Шифрование конфиденциальных данных модели на устройстве, обеспечение безопасного удаления данных.

Задания № 4. Установите соответствие между типом аппаратного обеспечения, используемого в системах ИИ для медицинской безопасности, и связанным с ним ключевым требованием или риском ИБ.

Аппаратное обеспечение	**Ключевое требование или риск ИБ**
1. Сервер с GPU для тренировки моделей	A) Риск несанкционированного физического доступа или изъятия носителя с данными.
2. Edge-устройство (камера, датчик) с ИИ на периметре больницы	B) Необходимость обеспечения высокой отказоустойчивости и минимальных задержек для критичных систем.
3. Медицинский IoT-прибор со встроенной моделью ИИ (например, умный ингалятор)	C) Риск перехвата беспроводного трафика или взлома прошивки для подмены данных.
4. Высокопроизводительный кластер для обработки геномных данных	D) Высокое энергопотребление и тепловыделение, требующие защиты от сбоев электропитания и перегрева.

Задания № 5. Установите правильную последовательность основных этапов безопасного развертывания обновленной модели ИИ в рабочую медицинскую информационную систему:

а) Развертывание модели на изолированном тестовом стенде, максимально приближенном к продуктивной среде.
б) Проведение приемочного тестирования с участием врачей-пользователей и специалистов по безопасности.
в) Подписание обновления цифровой подписью и подготовка пакета для установки.
г) Валидация результатов работы модели на независимой тестовой выборке, проверка на смещения (bias).
д) Поэтапный «канареечный» rollout обновления на часть продуктивных серверов с мониторингом метрик.

Перечень заданий открытого типа

Задание № 1. Какой принцип информационной безопасности обеспечивает, что пациент или система, запрашивающая диагноз у модели ИИ, являются теми, за кого себя выдают?

Задания № 2. Какая аппаратная технология, специализированная для ускорения матричных вычислений в глубоком обучении, часто используется вместо GPU в крупных дата-центрах?

Задания № 3. Как называется процесс проверки того, что обновление программного обеспечения или модели ИИ не нарушило существующую функциональность и требования безопасности?

Задания № 4. Процесс сокрытия исходного кода или логики программы (например, модели ИИ) для защиты от анализа и понимания злоумышленником называется _____.

Задания № 5. Подход к безопасности, при котором защитные меры встроены в архитектуру и дизайн системы с самого начала, а не добавлены позже, называется Security by _____.

Формируемая компетенция: ПК- 7

Перечень заданий закрытого типа

Задание № 1. Какой документ, разрабатываемый под руководством архитектора проекта, является ключевым для формализации высокоуровневого видения, бизнес-целей, ограничений и принципов будущей комплексной системы ИИ?
A) Ежедневный отчет о ходе работ.
B) Техническое задание.
C) Видение архитектуры (Architecture Vision).
D) Рекламная брошюра.

Задания № 2. Руководитель проекта по созданию системы ИБ на основе ИИ для сети клиник решает использовать итеративный подход к разработке архитектуры. Какой из фреймворков наиболее подходит для этого?
A) Водопадная модель (Waterfall).
B) Архитектурный фреймворк TOGAF и его метод ADM.
C) Жесткое следование первоначальному плану.
D) Отсутствие формальной методологии.

Задания № 3. Установите соответствие между ролью в проекте по созданию комплексной системы ИИ и ее ключевой ответственностью в процессе разработки архитектуры.

Роль в проекте	**Ключевая ответственность в разработке архитектуры**
1. Руководитель проекта /	A) Обеспечение соответствия архитектуры

Роль в проекте	Ключевая ответственность в разработке архитектуры
Архитектор	действующим правовым нормам (ФЗ-152, ФЗ-323) и отраслевым стандартам.
2. Системный архитектор	B) Донесение бизнес-требований и ограничений, утверждение ключевых архитектурных решений.
3. Бизнес-аналитик / Владелец продукта	C) Определение и поддержание целостного видения архитектуры, управление компромиссами, координация команды.
4. Специалист по безопасности и соответствию	D) Детальная проработка технических аспектов: выбор компонентов, паттернов, спецификация интерфейсов.

Задания № 4. Установите соответствие между ключевым принципом архитектуры комплексных систем ИИ и его практическим проявлением при проектировании.

Принцип архитектуры	Практическое проявление при проектировании
1. Модульность и слабая связанность	A) Возможность увеличивать объем обрабатываемых медицинских данных за счет добавления новых серверов обработки.
2. Масштабируемость	B) Разделение системы на независимые сервисы (например, сервис предобработки изображений, сервис инференса модели, сервис управления доступом).
3. Устойчивость к отказам (Resilience)	C) Использование шины данных (Data Bus) для унифицированного обмена событиями между компонентами.
4. Единый канал данных	D) Наличие автоматических механизмов переключения на резервный вычислительный кластер при сбое основного.

Задания № 5. Установите правильную последовательность фаз типичного цикла разработки архитектуры (согласно TOGAF ADM) для проекта комплексной системы ИИ:
а) Архитектура возможностей (Architecture Capability): настройка процесса архитектурной работы.
б) Архитектура решений (Solutions Architecture): планирование и управление реализацией.
в) Архитектура требований (Requirements Architecture): анализ и уточнение требований.
г) Архитектура видения (Architecture Vision): определение цели, заинтересованных лиц.
д) Архитектура бизнеса, данных, приложений, технологий (Business, Data, Application, Technology): детальное проектирование доменов.

Перечень заданий открытого типа

Задание № 1. Какой широко признанный открытый стандарт (фреймворк) для разработки архитектуры предприятия часто используется в качестве методологической основы для управления архитектурой комплексных ИС и систем ИИ?

Задания № 2. Какой гибкий фреймворк управления проектами, основанный на итеративных спринтах и ролях Product Owner/Scrum Master, часто используется при разработке сложного ПО?

Задания № 3. Какой ключевой документ в проекте описывает, КАК система будет построена с технической точки зрения, детализируя компоненты, их взаимодействие и технологии?

Задания № 4. Процесс формального анализа предлагаемого значительного изменения архитектуры на предмет его последствий, затрат и пользы называется _____ архитектурного изменения.

Задания № 5. Повторяющийся процесс пересмотра и улучшения архитектуры системы по мере поступления новой информации называется архитектурным _____.

4. ПЕРЕЧЕНЬ ЗАДАНИЙ ДЛЯ ОЦЕНКИ СФОРМИРОВАННОСТИ КОМПЕТЕНЦИЙ

Формируемая компетенция: ПК-1

Перечень заданий закрытого типа

Задание № 1. Для сбалансированной оценки качества работы интеллектуальной системы обнаружения вторжений на основе машинного обучения, анализирующей сетевой трафик, чаще всего используют метрику, представляющую собой гармоническое среднее между точностью и полнотой. Эта метрика называется:
A) Доступность
B) Точность
C) F1-мера
D) Аудит

Задание № 2. Какой технологический стандарт или методика используется для формализованного описания тактик, техник и процедур злоумышленников при расследовании киберинцидентов в медицинской информационной системе?
A) ITIL
B) GDPR
C) MITRE ATT&CK
D) ISO 27001

Задание № 3. При создании прототипа системы анализа логов для выявления аномалий в доступе к электронным медицинским картам разработчик решает использовать язык программирования Python и готовые реализации алгоритмов машинного обучения. Какую библиотеку ему следует выбрать в первую очередь?
A) TensorFlow
B) PyTorch
C) Scikit-learn
D) Pandas

Задание № 4. Какой ключевой российский нормативно-правовой акт регулирует вопросы защиты персональных данных пациентов, обрабатываемых в медицинских информационных системах?
A) ФЗ-187
B) ФЗ-152
C) ФЗ-149
D) ФЗ-323

Задание № 5. Какая из перечисленных технологий искусственного интеллекта позволяет обрабатывать зашифрованные медицинские данные для обучения моделей, не раскрывая их содержимое исследователям?
A) Блокчейн
B) Гомоморфное шифрование
C) Дифференциальная приватность
D) Квантовые вычисления

Задание № 6. Результатом какого этапа проектирования информационно-аналитической системы является документ, определяющий цели, функции, ограничения и общую архитектуру будущей системы?
A) Тестирование
B) Формирование технического задания
C) Внедрение
D) Сбор требований

Задание № 7. Установите соответствие между ключевым компонентом архитектуры интеллектуальной системы информационной безопасности для медицинской организации и его основной функцией.

Компонент системы	Основная функция
1. SIEM-платформа	A) Автоматическое выполнение сценариев реагирования на инциденты (например, блокировка учетной записи).
2. SOAR-платформа	B) Непрерывный сбор, нормализация и корреляция событий безопасности из различных источников (логи МИС, сетевого оборудования).
3. DLP-система	C) Мониторинг и предотвращение утечек конфиденциальных медицинских данных за пределы организации.
4. Система моделирования угроз	D) Формализованное описание активов, уязвимостей и возможных векторов атак на медицинскую сеть.

Задание № 8. Установите соответствие между технологией защиты данных в здравоохранении и решаемой с её помощью задачей.

Технология	Решаемая задача
1. Дифференциальная приватность	A) Обеспечение возможности проведения вычислений (например, диагностики) непосредственно на зашифрованных медицинских изображениях.
2. Гомоморфное шифрование	B) Гарантия того, что добавление или удаление одной записи пациента из обучающей выборки не окажет значимого влияния на результат статистического анализа.
3. Многопартийные вычисления	C) Совместный анализ геномных данных из нескольких медицинских центров без передачи самих исходных данных в единый центр.
4. Анонимизация	D) Удаление прямых идентификаторов (ФИО, паспорт) из набора медицинских данных для использования в научных исследованиях.

Задания № 9. Установите правильную последовательность этапов разработки прототипа интеллектуального модуля обнаружения аномалий в работе медицинского IoT-оборудования:
а) Выбор и обучение модели машинного обучения на данных, собранных в нормальном режиме работы.
б) Сбор и предобработка телеметрических данных с датчиков и эмуляторов.
в) Анализ предметной области: изучение протоколов, типов датчиков и моделирование угроз.
г) Интерпретация результатов работы модели, формирование отчета с рекомендациями.
д) Развертывание модели в тестовом контуре и настройка порогов срабатывания.

Задание № 10. Установите правильную последовательность этапов реагирования на инцидент с использованием SOAR-платформы в медицинской организации:
а) Автоматическое выполнение плейбука: изоляция зараженного хоста, сбор артефактов.
б) Корреляция событий и автоматическое создание тикета-инцидента в системе.
в) Триггер: SIEM-система обнаруживает серию неудачных попыток входа в МИС с последующей успешной аутентификацией.

г) Ручной анализ и закрытие инцидента специалистом после устранения угрозы.
д) Обогащение данных инцидента: проверка IP-адреса по Threat Intelligence-базам.

Перечень заданий открытого типа

Задание № 1. Назовите ключевую Python-библиотеку, предоставляющую структуры данных DataFrame и Series и инструменты для эффективного анализа и предобработки табличных данных, например, логов безопасности.

Задание № 2. Как называется класс атак на системы машинного обучения, при котором злоумышленник вносит малозаметные искажения во входные данные (например, рентгеновский снимок), чтобы вызвать ошибочное предсказание модели?

Задание № 3. Какой принцип информационной безопасности гарантирует, что медицинские данные, хранящиеся в PACS (архиве изображений), не были изменены несанкционированно?

Задание № 4. Какой международный стандарт описывает лучшие практики для систем менеджмента информационной безопасности и может использоваться для сертификации медицинских организаций?

Задание № 5. Непрерывный процесс автоматической интеграции изменений кода от разных разработчиков в общую основную ветку с последующим автоматическим тестированием и развертыванием называется _____ интеграцией и доставкой.

Задание № 6. Формализованное описание этапов кибератаки от первоначальной разведки до достижения цели и сокрытия следов в виде тактик и техник называется _____ кибератаки.

Формируемая компетенция: ПК-2

Перечень заданий закрытого типа

Задания № 1. Какой документ является основным результатом формализации задачи по разработке системы ситуационной осведомлённости (Security Operations Center) для сети крупной больницы и содержит детальные требования к источникам данных, аналитическим функциям и интерфейсам?
A) Презентация для инвесторов.
B) Техническое задание.
C) Годовой финансовый план.
D) Рекламный буклет.

Задание № 2. После анализа защищенности телемедицинской платформы выявлен риск утечки видеоконсультаций из-за отсутствия шифрования трафика. Какой из перечисленных форматов наименее подходит для формализации задачи по устранению этого риска в виде конкретного поручения?
A) Запись в реестре рисков с указанием ответственного и срока.
B) Отчет о количестве проведенных консультаций за месяц.
C) Техническое задание на настройку VPN или TLS.
D) Чек-лист действий для администратора сети.

Задание № 3. Какой международный стандарт является ключевым для формализации требований к безопасности информации в системах здравоохранения?
A) ISO 9001.
B) ISO/IEC 27001.
C) PCI DSS.
D) GOST R 7.0.97.

Задание № 4. Для формализации гипотезы о возможности несанкционированного доступа к архивным рентгеновским снимкам в PACS необходимо в первую очередь определить:
A) Стоимость системы хранения.
B) Конкретные наблюдаемые индикаторы в журналах доступа.
C) График работы рентгенологов.
D) Марку медицинских мониторов.

Задание № 5. Какой метод анализа данных наиболее применим для формализации задачи по прогнозированию пиковой нагрузки на систему мониторинга безопасности на основе исторических данных о кибератаках в отрасли здравоохранения?
A) Кластеризация.
B) Анализ временных рядов.
C) Классификация по известным сигнатурам.
D) Случайная выборка.

Задание № 6. При формализации рекомендаций по итогам анализа инцидента с кражей базы данных пациентов неправильным будет предложение:
A) Внедрить классификацию данных и DLP-систему.
B) Обязать всех сотрудников сменить пароли.
C) Увеличить частоту резервного копирования, не изменяя политики контроля доступа к бэкапам.
D) Внедрить многофакторную аутентификацию для доступа к МИС.

Задания № 7. Установите соответствие между этапом формализации задачи мониторинга ИБ для медицинской организации и его ключевым результатом.

Этап формализации	**Ключевой результат**
1. Определение целей	A) Модель угроз для МИС, PACS и медицинского IoT, описывающая активы и векторы атак.
2. Анализ контекста и активов	B) Четкая формулировка: "Снизить среднее время обнаружения аномального доступа к ЭМК до X минут".
3. Определение источников данных	C) Перечень: журналы доступа МИС, NetFlow, алерты SIEM, логи межсетевых экранов.
4. Определение метрик эффективности	D) Количественные показатели: процент ложных срабатываний, полнота обнаружения инцидентов.

Задание № 8. Установите соответствие между методом обработки данных для ситуационного анализа в здравоохранении и его описанием.

Метод обработки данных	**Описание**
1. Корреляция событий	A) Анализ последовательности действий пользователя в МИС для выявления аномальных поведенческих паттернов, характерных для инсайдера.
2. Поведенческий анализ (UEBA)	B) Связывание события блокировки учетной записи в Active Directory с попыткой доступа к серверу БД пациентов из той же сети для выявления цепочки атаки.
3. Анализ временных рядов данных датчиков IoT	C) Выявление отклонений в периодичности передачи показаний кардиомонитора, что может указывать на сбой устройства или манипуляцию данными.
4. Сбор индикаторов компрометации (IoC)	D) Использование актуальных списков

	вредоносных IP-адресов и хэшей для поиска уже известных угроз в сети.

Задания № 9. Установите правильную последовательность действий по формализации задачи для создания системы мониторинга целостности конфигураций медицинского сетевого оборудования.
а) Согласовать с сетевыми администраторами допустимые методы и окна для проведения сканирований.
б) Сформулировать итоговую постановку задачи в виде ТЗ, включающего цели, источники данных и критерии.
в) Определить перечень критического оборудования (маршрутизаторы, коммутаторы) и эталонные конфигурации.
г) Проанализировать требования стандартов и типовые угрозы целостности сетевой инфраструктуры.
д) Выбрать методы и инструменты для безопасного автоматизированного сбора и сравнения конфигураций.

Задания № 10. Установите правильную последовательность формализации задачи по расследованию гипотетического инцидента утечки данных из медицинской лаборатории.
а) Определить возможные точки и методы эксфильтрации данных: внешние накопители, облачные сервисы, электронная почта.
б) Согласовать план расследования, включая круг лиц, источники данных (логи DLP, proxy, МИС) и ожидаемые артефакты.
в) Изучить типовые бизнес-процессы работы лаборатории и потоки данных.
г) Сформулировать гипотезу инцидента на основе первичного сигнала (например, срабатывание DLP).
д) Выбрать методы анализа: поиск по ключевым словам, анализ сетевых соединений, проверка действий учетных записей.

Перечень заданий открытого типа

Задание № 1. Как называется основной открытый фреймворк, используемый для формализации и описания тактик, техник и процедур (TTPs) киберпротивников?

Задания № 2. Какой класс сетевых протоколов, часто используемых в медицинском оборудовании (например, для мониторов), исторически характеризуется отсутствием встроенных механизмов безопасности, что критично для формализации задач по их защите?

Задания № 3. Какой подход к обработке данных в мониторинге подразумевает их анализ в реальном времени по мере поступления и используется для задач, требующих немедленного реагирования?

Задания № 4. Какая одна из ключевых нефункциональных требований в ТЗ на систему мониторинга определяет её способность выдерживать рост объема обрабатываемых данных и числа источников?

Задания № 5. Подход к управлению безопасностью, при котором меры защиты выбираются и приоритезируются на основе оценки _____, называется риск-ориентированным подходом.

Задания № 6. Анализ _____, проводимый после инцидента, направлен на выявление глубинных организационных и технических причин, а не просто констатацию факта сбоя.

Формируемая компетенция: ПК-3

Перечень заданий закрытого типа

Задание № 1. Для задачи автоматической классификации сетевых пакетов в системе мониторинга больницы на «нормальные» и «вредоносные» на основе их заголовков и временных меток, какой класс алгоритмов машинного обучения является наиболее подходящим для начального прототипа?
A) Кластеризация (без учителя).
B) Классификация (с учителем).
C) Понижение размерности.
D) Рекомендательные системы.

Задания № 2. Для выявления ранее неизвестных аномальных паттернов в поведении пользователей медицинской информационной системы, когда размеченных данных об атаках недостаточно, какой подход машинного обучения является приоритетным?
A) Обучение с подкреплением.
B) Обучение с учителем.
C) Обучение без учителя.
D) Трансферное обучение.

Задания № 3. При разработке системы, которая должна обнаруживать подозрительные изменения в последовательности действий врача в электронной медицинской карте в реальном времени, какой тип нейронных сетей наиболее эффективен для анализа временных рядов?
A) Сверточные нейронные сети (CNN).
B) Рекуррентные нейронные сети (RNN).
C) Генеративно-состязательные сети (GAN).
D) Полносвязные нейронные сети.

Задания № 4. Для обработки и анализа текстовых полей в логах доступа к МИС (например, для поиска шаблонов вручную введенных SQL-запросов) в рамках системы обнаружения угроз, какой инструментарий ИИ является наиболее специализированным?
A) Библиотеки компьютерного зрения.
B) Инструменты обработки естественного языка (NLP).
C) Платформы для рекомендательных систем.
D) Инструменты анализа временных рядов.

Задания № 5. При разработке прототипа системы, которая должна генерировать реалистичные, но синтетические журналы атак для обучения моделей обнаружения вторжений без использования реальных конфиденциальных данных, какой метод ИИ следует рассмотреть?
A) Дерево решений.
B) Метод опорных векторов (SVM).
C) Генеративно-состязательные сети (GAN).
D) Линейная регрессия.

Задания № 6. Если требуется разработать интеллектуальный агент, который будет обучаться оптимальной стратегии распределения вычислительных ресурсов системы безопасности в ответ на изменяющуюся киберугрозу, какой парадигмальный подход ИИ лежит в основе?
A) Символьный искусственный интеллект.
B) Обучение с подкреплением.
C) Экспертные системы.
D) Эволюционные алгоритмы.

Задания № 7. Установите соответствие между задачей информационной безопасности в медицинской организации и наиболее подходящим для её решения комплексом методов искусственного интеллекта.

Задача ИБ в здравоохранении	Комплекс методов ИИ
1. Анализ рентгеновских снимков на предмет признаков их алгоритмической модификации (adversarial attacks).	A) Методы обработки естественного языка (NLP) для классификации текста.
2. Прогнозирование периодов повышенного риска DDoS-атак на портал телемедицины на основе исторических данных.	B) Глубокое обучение на основе сверточных нейронных сетей (CNN).
3. Автоматическая категоризация инцидентов, описанных в текстовых отчетах аналитиков, по тактикам MITRE ATT&CK.	C) Методы анализа временных рядов и регрессионного прогнозирования.
4. Обнаружение аномалий в сетевом трафике медицинских IoT-устройств (например, инфузионных насосов) без заранее известных шаблонов атак.	D) Методы обучения без учителя, такие как Isolation Forest или Autoencoders.

Задания № 8. Установите соответствие между инструментальным средством/платформой ИИ и ключевой областью его применения в контексте разработки систем безопасности.

Инструментальное средство / Платформа	Ключевая область применения в разработке систем ИБ
1. TensorFlow / PyTorch	A) Создание и обучение пользовательских моделей глубокого обучения (нейронных сетей).
2. Scikit-learn	B) Быстрое прототипирование и построение конвейеров данных для машинного обучения.
3. spaCy / NLTK	C) Работа с классическими алгоритмами ML (классификация, регрессия, кластеризация) и предобработка данных.
4. Jupyter Notebook / Google Colab	D) Обработка и анализ текстовых данных (логи, отчеты) с помощью NLP.

Задания № 9. Установите правильную последовательность основных этапов выбора и применения методов ИИ для решения задачи классификации вредоносного трафика в сети больницы:

а) Выбор и обучение конкретной модели (например, градиентного бустинга или нейронной сети) на подготовленных данных.

б) Формулировка бизнес-задачи и определение критериев успеха (точность, полнота).

в) Предобработка и разметка собранных сетевых данных (нормализация, создание признаков).

г) Сбор и анализ данных о сетевом трафике.

д) Оценка модели на тестовой выборке и интерпретация результатов.

Задания № 10. Установите правильную последовательность шагов при исследовании архитектуры системы ИИ для обнаружения аномалий доступа к медицинским изображениям в PACS:

а) Исследование и выбор подходящих архитектур нейронных сетей (например, автоэнкодеры для реконструкции ошибок).

б) Определение источников данных: журналы доступа к PACS, метаданные исследований, сетевые логи.

в) Проектирование компонента сбора и предобработки данных в реальном времени.

г) Формализация технической задачи: обнаружение аномальных последовательностей запросов к изображениям.

д) Проектирование модуля интеграции с SIEM для отправки алертов.

Часть 2. Задания открытого типа

Перечень заданий открытого типа

Задание № 1. Какая популярная открытая библиотека для Python является де-факто стандартом для реализации и обучения глубоких нейронных сетей с использованием динамических вычислительных графов?

Задания № 2. Как называется тип обучения модели машинного обучения, при котором используется заранее размеченный набор данных, где каждому примеру присвоен правильный ответ?

Задания № 3. Какая область искусственного интеллекта, основанная на работе с большими объемами текстовых данных, используется для анализа инцидентов безопасности, описанных в естественном языке?

Задания № 4. Какое ключевое нефункциональное требование к инструментарию ИИ часто становится критичным при выборе платформы для развертывания модели анализа сетевого трафика в реальном времени?

Задания № 5. Процесс, при котором модель машинного обучения настраивает свои внутренние параметры на обучающих данных для минимизации ошибки, называется _____ модели.

Задания № 6. Тип данных, для эффективной обработки которых сверточные нейронные сети (CNN) стали основным инструментом в ИИ, — это _____.

Формируемая компетенция: ПК-5

Перечень заданий закрытого типа

Задание № 1. При разработке модуля системы ИИ, обрабатывающего конфиденциальные данные пациентов, для обеспечения принципа конфиденциальности на уровне приложения необходимо в первую очередь реализовать:
A) Резервное копирование данных.
B) Шифрование данных при хранении и передаче.
C) Мониторинг температуры сервера.
D) Логирование всех действий.

Задания № 2. Какой подход к проектированию архитектуры системы машинного обучения для диагностики по снимкам минимизирует риски утечки исходных медицинских изображений при использовании облачных сервисов?
A) Загрузка всех данных в публичное облако для обучения.
B) Использование гомоморфного шифрования для обработки данных без их расшифровки.
C) Передача изображений по незащищенному протоколу HTTP.
D) Хранение приватных ключей шифрования вместе с данными.

Задания № 3. Для ускорения вычислений в нейронной сети, анализирующей поток видео с медицинских камер в реальном времени, разработчик планирует модернизировать аппаратное обеспечение. Какой компонент наиболее критичен для этой задачи?
A) Оперативная память большого объема (RAM).
B) Графический процессор (GPU) или тензорный процессор (TPU).
C) Звуковая карта высокой четкости.
D) Блок питания повышенной мощности.

Задания № 4. При разработке системы ИИ, интегрированной с медицинским оборудованием (например, ИВЛ), какое нефункциональное требование по безопасности является наивысшим приоритетом?
A) Удобный пользовательский интерфейс.
B) Гарантированная доступность и отказоустойчивость.

C) Низкая стоимость разработки.
D) Высокая скорость обучения моделей.

Задания № 5. Для защиты обученной модели ИИ, используемой для прогнозирования заболеваний, от обратной разработки (reverse engineering) и кражи интеллектуальной собственности при развертывании на edge-устройствах в поликлиниках, следует применить:
A) Обфускацию исполняемого кода модели.
B) Увеличение размера обучающей выборки.
C) Публикацию исходного кода модели в открытом доступе.
D) Использование только устаревших алгоритмов.

Задания № 6. Какой принцип безопасной разработки ПО (Secure SDLC) требует проверки кода модуля машинного обучения на наличие уязвимостей (например, инъекций через входные данные) перед его слиянием в основную ветку?
A) Статический анализ кода.
B) Нагрузочное тестирование.
C) Юзабилити-тестирование.
D) Тестирование совместимости.

Задания № 7. Установите соответствие между этапом жизненного цикла системы ИИ в здравоохранении и ключевой мерой информационной безопасности, которую необходимо реализовать на данном этапе.

Этап жизненного цикла системы ИИ	**Ключевая мера информационной безопасности**
1. Сбор и подготовка данных	A) Контроль целостности и аутентичности обновлений модели, проверка цифровых подписей.
2. Обучение модели	B) Аудит доступа к данным, маскирование или псевдонимизация персональных данных пациентов.
3. Развертывание и эксплуатация	C) Изоляция тренировочного кластера от производственной сети, защита от утечек через метаданные.
4. Обновление и вывод из эксплуатации	D) Шифрование конфиденциальных данных модели на устройстве, обеспечение безопасного удаления данных.

Задания № 8. Установите соответствие между типом аппаратного обеспечения, используемого в системах ИИ для медицинской безопасности, и связанным с ним ключевым требованием или риском ИБ.

Аппаратное обеспечение	**Ключевое требование или риск ИБ**
1. Сервер с GPU для тренировки моделей	A) Риск несанкционированного физического доступа или изъятия носителя с данными.
2. Edge-устройство (камера, датчик) с ИИ на периметре больницы	B) Необходимость обеспечения высокой отказоустойчивости и минимальных задержек для критичных систем.

Аппаратное обеспечение	Ключевое требование или риск ИБ
3. Медицинский IoT-прибор со встроенной моделью ИИ (например, умный ингалятор)	C) Риск перехвата беспроводного трафика или взлома прошивки для подмены данных.
4. Высокопроизводительный кластер для обработки геномных данных	D) Высокое энергопотребление и тепловыделение, требующие защиты от сбоев электропитания и перегрева.

Задания № 9. Установите правильную последовательность основных этапов безопасного развертывания обновленной модели ИИ в рабочую медицинскую информационную систему:
а) Развертывание модели на изолированном тестовом стенде, максимально приближенном к продуктивной среде.
б) Проведение приемочного тестирования с участием врачей-пользователей и специалистов по безопасности.
в) Подписание обновления цифровой подписью и подготовка пакета для установки.
г) Валидация результатов работы модели на независимой тестовой выборке, проверка на смещения (bias).
д) Поэтапный «канареечный» rollout обновления на часть продуктивных серверов с мониторингом метрик.

Задания № 10. Установите правильную последовательность действий при модернизации аппаратного обеспечения для локального запуска модели ИИ, анализирующей медицинские изображения, в условиях районной поликлиники:
а) Анализ требований модели к вычислительным ресурсам (оперативная память, производительность GPU).
б) Установка и настройка нового оборудования в защищенном помещении с контролем доступа.
в) Тестирование производительности и точности модели на новом оборудовании.
г) Выбор и закупка сервера или рабочей станции с необходимыми характеристиками.
д) Обеспечение бесперебойного электропитания и системы охлаждения для нового оборудования.

Перечень заданий открытого типа

Задание № 1. Какой принцип информационной безопасности обеспечивает, что пациент или система, запрашивающая диагноз у модели ИИ, являются теми, за кого себя выдают?

Задания № 2. Какая аппаратная технология, специализированная для ускорения матричных вычислений в глубоком обучении, часто используется вместо GPU в крупных дата-центрах?

Задания № 3. Как называется процесс проверки того, что обновление программного обеспечения или модели ИИ не нарушило существующую функциональность и требования безопасности?

Задания № 4. Какой тип программного обеспечения используется для автоматизации сборки, тестирования и развертывания (CI/CD) контейнеризованных приложений ИИ?

Задания № 5. Процесс сокрытия исходного кода или логики программы (например, модели ИИ) для защиты от анализа и понимания злоумышленником называется _____.

Задания № 6. Подход к безопасности, при котором защитные меры встроены в архитектуру и дизайн системы с самого начала, а не добавлены позже, называется Security by _____.

Формируемая компетенция: ПК- 7

Перечень заданий закрытого типа

Задание № 1. Какой документ, разрабатываемый под руководством архитектора проекта, является ключевым для формализации высокоуровневого видения, бизнес-целей, ограничений и принципов будущей комплексной системы ИИ?
A) Ежедневный отчет о ходе работ.
B) Техническое задание.
C) Видение архитектуры (Architecture Vision).
D) Рекламная брошюра.

Задания № 2. Руководитель проекта по созданию системы ИБ на основе ИИ для сети клиник решает использовать итеративный подход к разработке архитектуры. Какой из фреймворков наиболее подходит для этого?
A) Водопадная модель (Waterfall).
B) Архитектурный фреймворк TOGAF и его метод ADM.
C) Жесткое следование первоначальному плану.
D) Отсутствие формальной методологии.

Задания № 3. При принятии ключевого решения о выборе между облачной и гибридной архитектурой для системы анализа медицинских изображений, руководитель проекта должен в первую очередь провести:
A) Анализ заинтересованных сторон и их требований.
B) Розыгрыш лотереи.
C) Выбор самой дорогой технологи.
D) Копирование архитектуры конкурента.

Задания № 4. Какой ключевой артефакт, создаваемый при разработке архитектуры, наглядно отображает основные компоненты системы ИИ, их взаимосвязи и внешние зависимости?
A) Диаграмма компонентов (Component Diagram).
B) Штатное расписание.
C) Финансовый бюджет.
D) График отпусков команды.

Задания № 5. При управлении разработкой архитектуры, какую нефункциональную характеристику системы (атрибут качества) сложнее всего обеспечить постфактум, если она не была заложена в архитектурные решения изначально?
A) Масштабируемость.
B) Производительность.
C) Надежность.
D) Безопасность.

Задания № 6. Для документирования и управления решениями по архитектуре, такими как выбор стека технологий или паттернов интеграции, руководитель проекта использует:
A) Журнал архитектурных решений (Architecture Decision Log).
B) Случайные заметки в блокноте.
C) Устные договоренности.
D) Корпоративную почту.

Задания № 7. Установите соответствие между ролью в проекте по созданию комплексной системы ИИ и ее ключевой ответственностью в процессе разработки архитектуры.

Роль в проекте	**Ключевая ответственность в разработке архитектуры**

Роль в проекте	Ключевая ответственность в разработке архитектуры
1. Руководитель проекта / Архитектор	A) Обеспечение соответствия архитектуры действующим правовым нормам (ФЗ-152, ФЗ-323) и отраслевым стандартам.
2. Системный архитектор	B) Донесение бизнес-требований и ограничений, утверждение ключевых архитектурных решений.
3. Бизнес-аналитик / Владелец продукта	C) Определение и поддержание целостного видения архитектуры, управление компромиссами, координация команды.
4. Специалист по безопасности и соответствию	D) Детальная проработка технических аспектов: выбор компонентов, паттернов, спецификация интерфейсов.

Задания № 8. Установите соответствие между ключевым принципом архитектуры комплексных систем ИИ и его практическим проявлением при проектировании.

Принцип архитектуры	Практическое проявление при проектировании
1. Модульность и слабая связанность	A) Возможность увеличивать объем обрабатываемых медицинских данных за счет добавления новых серверов обработки.
2. Масштабируемость	B) Разделение системы на независимые сервисы (например, сервис предобработки изображений, сервис инференса модели, сервис управления доступом).
3. Устойчивость к отказам (Resilience)	C) Использование шины данных (Data Bus) для унифицированного обмена событиями между компонентами.
4. Единый канал данных	D) Наличие автоматических механизмов переключения на резервный вычислительный кластер при сбое основного.

Задания № 9. Установите правильную последовательность фаз типичного цикла разработки архитектуры (согласно TOGAF ADM) для проекта комплексной системы ИИ:
а) Архитектура возможностей (Architecture Capability): настройка процесса архитектурной работы.
б) Архитектура решений (Solutions Architecture): планирование и управление реализацией.
в) Архитектура требований (Requirements Architecture): анализ и уточнение требований.
г) Архитектура видения (Architecture Vision): определение цели, заинтересованных лиц.
д) Архитектура бизнеса, данных, приложений, технологий (Business, Data, Application, Technology): детальное проектирование доменов.

Задания № 10. Установите правильную последовательность действий руководителя проекта при выявлении критического архитектурного риска (например, неготовность выбранной СУБД к пиковой нагрузке):
а) Разработка плана по смягчению риска (например, тестирование под нагрузкой, выбор альтернативы).
б) Идентификация и документирование риска в реестре.
в) Реализация плана, мониторинг результата.
г) Качественная и количественная оценка вероятности и последствий риска.
д) Приоритизация риска относительно других.

Перечень заданий открытого типа

Задание № 1. Какой широко признанный открытый стандарт (фреймворк) для разработки архитектуры предприятия часто используется в качестве методологической основы для управления архитектурой комплексных ИС и систем ИИ?

Задания № 2. Какой гибкий фреймворк управления проектами, основанный на итеративных спринтах и ролях Product Owner/Scrum Master, часто используется при разработке сложного ПО?

Задания № 3. Какой ключевой документ в проекте описывает, КАК система будет построена с технической точки зрения, детализируя компоненты, их взаимодействие и технологии?

Задания № 4. Какой процесс направлен на обеспечение того, что реализованная система соответствует утвержденным архитектурным решениям и стандартам?

Задания № 5. Процесс формального анализа предлагаемого значительного изменения архитектуры на предмет его последствий, затрат и пользы называется _____ архитектурного изменения.

Задания № 6. Повторяющийся процесс пересмотра и улучшения архитектуры системы по мере поступления новой информации называется архитектурным _____.

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	C
	№ 2	C
	№ 3	1-B, 2-A, 3-C, 4-D
	№ 4	1-B, 2-A, 3-C, 4-D
	№ 5	в б а д г
	Задания открытого типа	
	№ 1	Pandas.
	№ 2	Adversarial
	№ 3	Целостность
	№ 4	непрерывной
	№ 5	Моделью
ПК-2	**Задания закрытого типа**	
	№ 1	B
	№ 2	B
	№ 3	1-B, 2-A, 3-C, 4-D
	№ 4	1-B, 2-A, 3-C, 4-D
	№ 5	г в а д б
	Задания открытого типа	
	№ 1	MITRE
	№ 2	Проприетарные
	№ 3	Потоковый
	№ 4	рисков
	№ 5	причин
ПК-3	**Задания закрытого типа**	
	№ 1	B
	№ 2	C
	№ 3	1-B, 2-C, 3-A, 4-D
	№ 4	1-A, 2-C, 3-D, 4-B
	№ 5	б г в а д
	Задания открытого типа	
	№ 1	PyTorch
	№ 2	Супервизированное
	№ 3	NLP
	№ 4	Обучение
	№ 5	Изображения
ПК-5	**Задания закрытого типа**	
	№ 1	B
	№ 2	B
	№ 3	1-B, 2-C, 3-D, 4-A
	№ 4	1-D, 2-A, 3-C, 4-B
	№ 5	г а б в д
	Задания открытого типа	
	№ 1	Аутентичность

	№ 2	TPU
	№ 3	Регрессионное
	№ 4	Обфускация
	№ 5	Design
ПК-7	**Задания закрытого типа**	
	№ 1	C
	№ 2	B
	№ 3	1-C, 2-D, 3-B, 4-A
	№ 4	1-B, 2-A, 3-D, 4-C
	№ 5	г в д б а
	Задания открытого типа	
	№ 1	TOGAF
	№ 2	Scrum
	№ 3	Дизайн
	№ 4	Оценка
	№ 5	Рефакторинг

КЛЮЧИ К ЗАДАНИЯМ ДЛЯ ОЦЕНКИ СФОРМИРОВАННОСТИ КОМПЕТЕНЦИЙ

Таблица 6.

Формируемые компетенции	№ задания	Ответ
ПК-1	**Задания закрытого типа**	
	№ 1	C
	№ 2	C
	№ 3	C
	№ 4	B
	№ 5	B
	№ 6	B
	№ 7	1-B, 2-A, 3-C, 4-D
	№ 8	1-B, 2-A, 3-C, 4-D
	№ 9	в б а д г
	№ 10	в б д а г
	Задания открытого типа	
	№ 1	Pandas.
	№ 2	Adversarial
	№ 3	Целостность
	№ 4	ISO27001
	№ 5	непрерывной
	№ 6	Моделью
ПК-2	**Задания закрытого типа**	
	№ 1	B
	№ 2	B
	№ 3	B
	№ 4	B
	№ 5	B
	№ 6	C
	№ 7	1-B, 2-A, 3-C, 4-D
	№ 8	1-B, 2-A, 3-C, 4-D
	№ 9	г в а д б
	№ 10	г в а д б
	Задания открытого типа	
	№ 1	MITRE
	№ 2	Проприетарные
	№ 3	Потоковый
	№ 4	Масштабируемость
	№ 5	рисков
	№ 6	причин
ПК-3	**Задания закрытого типа**	
	№ 1	B
	№ 2	C
	№ 3	B
	№ 4	B
	№ 5	C
	№ 6	B
	№ 7	1-B, 2-C, 3-A, 4-D
	№ 8	1-A, 2-C, 3-D, 4-B
	№ 9	б г в а д

	№ 10	г б а в д
	Задания открытого типа	
	№ 1	PyTorch
	№ 2	Супервизированное
	№ 3	NLP
	№ 4	Производительность
	№ 5	Обучение
	№ 6	Изображения
ПК-5	**Задания закрытого типа**	
	№ 1	B
	№ 2	B
	№ 3	B
	№ 4	B
	№ 5	A
	№ 6	A
	№ 7	1-B, 2-C, 3-D, 4-A
	№ 8	1-D, 2-A, 3-C, 4-B
	№ 9	г а б в д
	№ 10	а г д б в
	Задания открытого типа	
	№ 1	Аутентичность
	№ 2	TPU
	№ 3	Регрессионное
	№ 4	Kubernetes
	№ 5	Обфускация
	№ 6	Design
ПК-7	**Задания закрытого типа**	
	№ 1	C
	№ 2	B
	№ 3	A
	№ 4	A
	№ 5	D
	№ 6	A
	№ 7	1-C, 2-D, 3-B, 4-A
	№ 8	1-B, 2-A, 3-D, 4-C
	№ 9	г в д б а
	№ 10	б г д а в
	Задания открытого типа	
	№ 1	TOGAF
	№ 2	Scrum
	№ 3	Дизайн
	№ 4	Валидация
	№ 5	Оценка
	№ 6	Рефакторинг