Министерство науки и высшего образования Российской Федерации

ФГБОУ ВО «Дагестанский государственный технический университет»

ФОНД ОЦЕНОЧНЫХ СРЕДСТВ

по дисциплине «Интеллектуальные системы информационной безопасности в промышленных системах»
(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 промышленных системах» 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 промышленных системах» 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- 1.2 Способен интерпретировать и использовать результаты решения информационно-аналитических задач 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	ПК-3

особенностей предметной области	
ПК -5.1 Разрабатывает программное и аппаратное обеспечение технологий и систем искусственного интеллекта для решения профессиональных задач с учетом требований информационной безопасности в различных предметных областях	ПК -5
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. Основные понятия и определения интеллектуальных систем				
Тема 1.1 Введение в интеллектуальные системы информационной безопасности	Письменная работа №1 Устный опрос Лабораторная работа №1 Самостоятельная работа Реферат	ПК-1: ПК-1.2; ПК-1.3; ПК-2: ПК-2.1; ПК-3: ПК-3.1	Экзаменационная работа	ПК-1: ПК-1.2; ПК-1.3; ПК-2: ПК-2.1; ПК-3: ПК-3.1
Тема 1.2 Системы с интеллектуальной обратной связью и интеллектуальными интерфейсами	Письменная работа №2 Устный опрос Лабораторная работа №2 Самостоятельная работа Реферат	ПК-1: ПК-1.2; ПК-1.3; ПК-2: ПК-2.1; ПК-3: ПК-3.1	Экзаменационная работа	ПК-1: ПК-1.2; ПК-1.3; ПК-2: ПК-2.1; ПК-3: ПК-3.1
Тема 1.3 Автоматизированные системы распознавания образов	Письменная работа №3 Устный опрос Лабораторная работа №3 Самостоятельная работа Реферат	ПК-1: ПК-1.2; ПК-1.3; ПК-2: ПК-2.1; ПК-3: ПК-3.1	Экзаменационная работа	ПК-1: ПК-1.2; ПК-1.3; ПК-2: ПК-2.1; ПК-3: ПК-3.1
Тема 1.4 Методы поддержки принятия решений	Письменная работа №4 Устный опрос Лабораторная работа №4 Самостоятельная работа Реферат	ПК-1: ПК-1.2; ПК-1.3; ПК-2: ПК-2.1; ПК-3: ПК-3.1	Экзаменационная работа	ПК-1: ПК-1.2; ПК-1.3; ПК-2: ПК-2.1; ПК-3: ПК-3.1
Тема 1.5 Экспертные системы	Письменная работа №5 Устный опрос Лабораторная работа №5 Самостоятельная	ПК-1: ПК-1.2; ПК-1.3; ПК-2: ПК-2.1; ПК-3: ПК-3.1	Экзаменационная работа	ПК-1: ПК-1.2; ПК-1.3; ПК-2: ПК-2.1; ПК-3: ПК-3.1

	работа Реферат			
Тема 1.6 Эволюционные вычисления	Письменная работа №6 Устный опрос Лабораторная работа №6 Самостоятельная работа Реферат	ПК-1: ПК-1.2; ПК-1.3; ПК-2: ПК-2.1; ПК-3: ПК-3.1	Экзаменационная работа	ПК-1: ПК-1.2; ПК-1.3; ПК-2: ПК-2.1; ПК-3: ПК-3.1
Тема 1.7 Языки и средства разработки интеллектуальных систем	Письменная работа №7 Устный опрос Лабораторная работа №7 Самостоятельная работа Реферат	ПК-1: ПК-1.2; ПК-1.3; ПК-2: ПК-2.1; ПК-3: ПК-3.1	Экзаменационная работа	ПК-1: ПК-1.2; ПК-1.3; ПК-2: ПК-2.1; ПК-3: ПК-3.1
Тема 1.8 Методы идентификации и аутентификации пользователей	Письменная работа №8 Устный опрос Лабораторная работа №8 Самостоятельная работа Реферат	ПК-1: ПК-1.2; 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-1.2; ПК-1.3; ПК-2: ПК-2.1; ПК-3: ПК-3.1; ПК-5: ПК-5.1 ПК-7: ПК-71.1
Раздел 2. Интеллектуальные системы информационной безопасности в промышленных				
Тема 2.1 Управление жизненным циклом и проектами внедрения интеллектуальных систем ИБ в промышленности.	Письменная работа №9 Устный опрос Лабораторная работа №9 Самостоятельная работа Реферат	ПК-1: ПК-1.2; 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-1.2; 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. При проектировании информационно-аналитической системы для контроля технологического процесса нефтеперерабатывающего завода, какой из компонентов будет отвечать за централизованный сбор, нормализацию и корреляцию событий из систем АСУ ТП, сетевого оборудования и журналов безопасности?

A) Система управления базами данных.
B) SIEM-платформа.
C) Средство визуализации.
D) Сервер хранения резервных копий.

Задание № 2. Какой принцип разработки архитектуры сложной ИАС для промышленного объекта предпочтительнее для обеспечения возможности независимого обновления и

масштабирования модулей анализа сетевого трафика, детектирования аномалий в данных датчиков и генерации отчетов?

A) Использование единого универсального программного пакета.
B) Применение микросервисной архитектуры.
C) Разработка монолитного клиент-серверного приложения.
D) Заказ готового коробочного решения у вендора.

Задание № 3. Установите соответствие между ключевым компонентом архитектуры современной ИАС для промышленной безопасности и его основной функцией.

Компонент архитектуры ИАС	**Основная функция**
1. Хранилище данных (Data Warehouse)	A) Автоматическое выполнение сценариев реагирования на инциденты.
2. Аналитическая платформа (OLAP)	B) Долгосрочное структурированное хранение исторических данных для ретроспективного анализа.
3. SOAR-платформа	C) Интерактивное многомерное исследование данных аналитиком.
4. Система моделирования угроз	D) Формализованное описание активов, уязвимостей и векторов атак для оценки рисков.

Задание № 4. Установите соответствие между этапом жизненного цикла разработки ИАС и его ключевым содержанием.

Этап жизненного цикла ИАС	**Ключевое содержание**
1. Сбор и анализ требований	A) Создание диаграмм развертывания, спецификаций API и схем баз данных.
2. Проектирование архитектуры	B) Написание кода, модульное тестирование, интеграция отдельных компонентов.
3. Непосредственная разработка	C) Формализация целей системы, описание бизнес-процессов, интервью с стейкхолдерами
4. Внедрение и ввод в эксплуатацию	D) Пилотная эксплуатация на одном участке, обучение пользователей, передача документации.

Задание № 5. Установите правильную последовательность этапов работы над проектом интеллектуальной системы обнаружения аномалий в технологическом процессе на основе данных датчиков SCADA.

а) Обучить модель машинного обучения на данных, собранных в нормальном режиме работы.
б) Интерпретировать результаты работы модели, сопоставить выявленные аномалии с возможными инцидентами кибербезопасности и сформулировать рекомендации для операторов.
в) Спроектировать архитектуру системы: определить место внедрения, способы интеграции с SCADA и форматы данных.
г) Провести анализ предметной области: изучить технологический процесс, идентифицировать критические параметры и смоделировать угрозы.
д) Развернуть обученную модель в тестовом контуре, настроить пороги срабатывания и систему оповещений.

Перечень заданий открытого типа

Задание № 1. Задание № 1. Какая популярная Python-библиотека является стандартом де-факто для выполнения операций предобработки и анализа структурированных данных?

Задание № 2. Какой фреймворк/стандарт де-факто используется для описания тактик, техник и процедур киберпротивников при моделировании угроз для промышленных систем?

Задание № 3. Назовите ключевую Python-библиотеку, предоставляющую готовые реализации множества классических алгоритмов машинного обучения и инструментов для оценки моделей.

Задание № 4. Дополните определение, вставляя пропущенное слово:
Процесс автоматической сборки, тестирования и развертывания программных компонентов при каждом изменении кода называется _____ интеграцией и доставкой.

Задание № 5. Дополните определение, вставляя пропущенное слово:
Принцип _____ требует, чтобы каждому компоненту системы, пользователю или процессу предоставлялись минимально необходимые права доступа для выполнения легитимных задач.

Формируемая компетенция: ПК-2

Перечень заданий закрытого типа

Задание № 1. Какой документ является первичным результатом формализации задачи по созданию системы мониторинга аномалий в сети промышленного предприятия и содержит детальные требования к функционалу, данным и интерфейсам?

A) Презентация для руководства.
B) Техническое задание .
C) Финансовый отчет.
D) План маркетинга.

Задание № 2. При анализе защищенности промышленной системы выявлена уязвимость в устаревшей версии ПО HMI. Какой из перечисленных форматов наименее подходит для формализации задачи по устранению этой уязвимости в виде конкретного поручения?

A) Запись в системе управления уязвимостями.
B) Статистический отчет о количестве уязвимостей за квартал.
C) Техническое задание на обновление или замену компонента.
D) Чек-лист действий для инженерной службы.

Задание № 3. Установите соответствие между этапом формализации задачи ИБ для промышленной системы и его ключевым результатом.

Этап формализации	Ключевой результат
1. Определение целей и границ анализа	A) Чек-лист или модель угроз, описывающие активы, уязвимости и потенциальные векторы атак.
2. Анализ контекста и моделирование угроз	B) Четкая формулировка: "Снизить среднее время обнаружения аномальных команд ПЛК до N минут".
3. Определение источников и методов	C) Список данных: сетевые пакеты, логи контроллеров, журналы HMI, данные датчиков.
4. Определение критериев успеха	D) Количественные метрики: процент ложных срабатываний, полнота обнаружения атак.

Задание № 4. Установите соответствие между методом обработки/интерпретации данных промышленных систем и его описанием.

Метод обработки данных	Описание
1. Декодирование промышленных протоколов	A) Анализ последовательности и временных меток событий для выявления аномальных последовательностей
2. Анализ временных последовательностей	B) Использование алгорит.мов без учителя для выявления скрытых паттернов или кластеров в данных телеметрии, не соответствующих нормальному режиму работы.
3. Обнаружение аномалий в данных датчиков	C) Преобразование сырых сетевых пакетов в читаемый формат команд и параметров для последующего анализа.
4. Корреляция событий из разнородных источников	D) Связывание событий из сетевого трафика АСУ ТП с попытками доступа из корпоративной сети для выявления сложных межсегментных атак.

Задание № 5. Установите правильную последовательность действий по формализации задачи для разработки системы мониторинга целостности программного обеспечения промышленных контроллеров.

а) Определить перечень контролируемых контроллеров и конкретные признаки несанкционированного изменения.

б) Согласовать с технологами допустимые методы и окна для проведения проверок, чтобы не нарушить технологический цикл.

в) Сформулировать итоговую постановку задачи в виде технического задания, включающего цели, источники данных и критерии успеха.

г) Проанализировать нормативные требования и типовые векторы атак на ПЛК по MITRE ATT&CK for ICS.

д) Выбрать методы и инструменты для безопасного удаленного сбора данных с ПЛК.

Перечень заданий открытого типа

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

Задание № 2. Какой класс промышленных сетевых протоколов характеризуется отсутствием встроенных механизмов аутентификации и шифрования, что должно быть учтено при формализации задач по их защите?

Задание № 3. Какой подход к обработке данных подразумевает их анализ в момент генерации и используется для формализации задач мониторинга, требующих немедленного реагирования?

Задание № 4. Дополните определение, вставляя пропущенное слово:
Подход к управлению безопасностью, при котором меры защиты выбираются и приоритезируются на основе оценки _____, называется риск-ориентированным подходом.

Задание № 5. Дополните определение, вставляя пропущенное слово:
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 классификации сетевых пакетов промышленного протокола Modbus TCP на нормальные и вредоносные в реальном времени, где критична низкая задержка и важна интерпретируемость решений, наиболее подходящим комплексом методов ИИ будет:

A) Ансамбль "легких" алгоритмов.
B) Глубокая сверточная нейронная сеть.
C) Генеративно-состязательная сеть.
D) Рекуррентная нейронная сеть с вниманием.

Задание № 2. При выборе инструментальных средств для создания прототипа системы прогнозирования кибератак в сети больницы, где команда обладает сильными навыками в Python, но ограничена во времени, ключевым решающим фактором будет:

A) Возможность развертывания на специализированных AI-ускорителях.
B) Наличие богатой экосистемы библиотек для быстрого прототипирования.
C) Поддержка распределенного обучения на сотнях GPU.
D) Наличие встроенных compliance-отчетов для стандарта HIPAA.

Задание № 3. Установите соответствие между особенностью предметной области и предпочтительным классом методов/инструментов ИИ для её решения.

Особенность предметной области / задачи ИБ	**Класс методов/инструментов ИИ**
1. Анализ последовательностей команд в журналах для выявления многоэтапных APT-атак.	A) Методы анализа временных рядов и последовательностей.
2. Обогащение событий SIEM контекстом из внешних источников угроз в реальном времени.	B) Интеграционные платформы и API для работы с Threat Intelligence Feeds.
3. Автоматическое категорирование инцидентов из тикетов SOC по стандартным тактикам.	C) Алгоритмы классификации текстов на основе предобученных моделей.
4. Визуализация сложных взаимосвязей между узлами сети и атакующими для расследования.	D) Инструменты для визуализации графов

Задание № 4. Установите соответствие между задачей в области ИБ для промышленной системы и рекомендуемым специализированным программным обеспечением или фреймворком.

Задача ИБ в АСУ ТП	**Рекомендуемое специализированное ПО / фреймворк**
1. Сбор, парсинг и нормализация данных промышленных протоколов	A) SIEM-платформа с поддержкой Industrial Add-ons.
2. Комплексная корреляция событий из IT и OT сетей, генерация алертов.	B) Специализированные средства анализа сетевого трафика АСУ ТП
3. Создание и управление плейбуками автоматического реагирования на инциденты в технологической сети.	C) Платформы класса SOAR
4. Непрерывный мониторинг активов и уязвимостей в промышленной сети.	D) Пассивные сканеры и платформы для управления активами АСУ ТП

Задание № 5. Установите правильную последовательность выбора комплекса методов и инструментов ИИ для решения задачи классификации типов атак в трафике промышленных протоколов.

а) Выбрать финальный стек технологий.
б) Сформировать список требований к решению: точность, скорость работы в реальном времени, интерпретируемость результатов, устойчивость к шуму.
в) Провести практические эксперименты с 2-3 наиболее подходящими алгоритмами на подготовленных данных.
г) Изучить особенности сетевого трафика целевых протоколов для понимания структуры данных и потенциальных аномалий.
д) Проанализировать доступные инструменты и опубликованные исследования по схожим задачам.

Перечень заданий открытого типа

Задание № 1. При работе с конфиденциальными медицинскими данными для обучения модели, какой математический метод обеспечения приватности следует выбрать, чтобы гарантировать, что модель не запомнит и не раскроет конкретные записи из обучающей выборки?

Задание № 2. Какой открытый фреймворк от MITRE предоставляет таксономию атак на системы ИИ и должен быть использован для выбора методов тестирования и защиты разрабатываемой интеллектуальной системы?

Задание № 3. Какой класс архитектур нейронных сетей является доминирующим выбором для задач обработки естественного языка в системах анализа инцидентов и должен быть предпочтен простым методам "мешка слов" для сложных задач?

Задание № 4. Дополните определение, вставляя пропущенное слово:
Принцип _____ в разработке безопасных систем ИИ требует внедрения контроля безопасности на всех этапах жизненного цикла — от проектирования до эксплуатации.

Задание № 5. Дополните определение, вставляя пропущенное слово:
_____ вычислительная парадигма позволяет обрабатывать данные непосредственно на edge-устройствах, что снижает задержки и риски утечки при передаче в центр обработки.

Формируемая компетенция: ПК-5

Перечень заданий закрытого типа

Задание № 1. Для проектирования аппаратно-программного комплекса ИИ, который будет непрерывно обрабатывать потоки видео с камер наблюдения в режиме реального времени на промышленном объекте, ключевым аппаратным решением, позволяющим эффективно выполнять нейросетевой инференс с низкой задержкой, является:
A) Центральный процессор высокой частоты.
B) Графический процессор или специализированный ускоритель.
C) Большой объем оперативной памяти.
D) Быстрый твердотельный накопитель.

Задание № 2. При разработке программного обеспечения для интеллектуальной системы прогнозирования отказов медицинского оборудования, где точность напрямую влияет на безопасность пациентов, критически важным принципом разработки является:
A) Максимизация быстродействия алгоритмов в ущерб точности.
B) Обеспечение надежности, отказоустойчивости и валидации результатов модели.
C) Использование исключительно open-source библиотек.
D) Минимизация количества строк кода.

Задание № 3. Установите соответствие между этапом руководства разработкой архитектуры комплексной системы ИИ и ключевым решением или действием руководителя проекта.

Этап руководства разработкой архитектуры	Ключевое решение/действие руководителя проекта
1. Анализ предметной области и требований	A) Выбор парадигмы взаимодействия компонентов и протоколов обмена данными с учетом требований ИБ.
2. Определение высокоуровневой архитектуры	B) Утверждение решений по резервированию, мониторингу работоспособности и аварийному восстановлению компонентов ИИ.
3. Проектирование интеграции и безопасности	C) Определение ключевых нефункциональных требований: латентность, пропускная способность, доступность, безопасность данных
4. Планирование эксплуатационных характеристик	D) Внедрение практик DevSecOps, выбор инструментов статического/динамического анализа кода, планирование аудитов безопасности.

Задание № 4. Установите соответствие между классом интеллектуальных систем для предметной области «Киберфизические системы» и особенностью учета требований ИБ при их разработке/модернизации.

Класс интеллектуальных систем	Особенность учета требований ИБ при разработке
1. Беспилотный транспорт	A) Обеспечение безопасности жизни, защита от дистанционного захвата управления, целостность данных сенсоров.
2. Промышленные АСУ ТП	B) Защита критических технологических процессов от саботажа, устойчивость к целевым APT-атакам, работа в изолированных сетях.
3. Медицинские системы жизнеобеспечения	C) Гарантированная доступность и безотказность, защита конфиденциальных данных пациентов, валидация решений ИИ.
4. Умные энергетические сети	D) Защита от атак, способных вызвать каскадные отказы и масштабные отключения, контроль целостности данных телеметрии.

Задание № 5. Установите правильную последовательность этапов разработки программного обеспечения lightweight-агента для анализа событий безопасности на edge-устройстве в промышленной сети.

а) Разработать и протестировать прототип агента, проверив корректность сбора данных и работу алгоритмов в изолированной среде.

б) Определить технические требования к агенту: поддержка ОС устройства, ограничения по памяти/CPU, защищенный канал связи с сервером.

в) Внедрить в код агента механизмы обеспечения целостности и аутентичности.

г) Провести приемо-сдаточные испытания агента на реальном целевом оборудовании в промышленной сети.

д) Выбрать язык программирования и библиотеки, соответствующие требованиям производительности и безопасности.

Перечень заданий открытого типа

Задание № 1. При построении интеллектуальной системы для обработки персональных медицинских данных какой математический метод следует применить на этапе обучения модели, чтобы гарантировать конфиденциальность данных и соответствие требованиям регуляторов?

Задание № 2. Назовите ключевой международный стандарт, который необходимо учитывать при модернизации программно-аппаратного обеспечения систем ИИ для промышленных систем управления в части требований кибербезопасности.

Задание № 3. Какой архитектурный стиль является предпочтительным при разработке комплексной, масштабируемой и легко обновляемой системы ИИ, объединяющей модули сбора данных, ML-пайплайны и сервисы инференса?

Задание № 4. Дополните определение, вставляя пропущенное слово:
_____ обучение — это децентрализованный подход к машинному обучению, позволяющий обучать модель на данных, которые остаются на устройствах-источниках, что повышает безопасность и конфиденциальность данных.

Задание № 5. Дополните определение, вставляя пропущенное слово:
Процесс проверки и подтверждения того, что данные, используемые для обучения и работы модели ИИ, не были намеренно искажены для манипуляции её результатами, называется защитой от _____ данных.

Формируемая компетенция: ПК- 7

Перечень заданий закрытого типа

Задание № 1. Какой этап разработки архитектуры комплексной системы ИИ является первым и ключевым для последующего успеха проекта?

A) Написание кода отдельных модулей.
B) Выбор фреймворка для машинного обучения.
C) Анализ предметной области и определение требований заинтересованных сторон.
D) Закупка серверного оборудования.

Задание № 2. Какой из перечисленных инструментов является стандартом де-факто для описания и документирования архитектуры программных систем, включая комплексные системы ИИ?

A) Microsoft Visio.
B) Язык UML.
C) Trello.
D) Блок-схемы в PowerPoint.

Задание № 3. Установите соответствие между ключевым решением при проектировании архитектуры комплексной системы ИИ и его основной целью.

Ключевое архитектурное решение	**Основная цель**
1. Использование микросервисной архитектуры	A) Обеспечение возможности независимого масштабирования и обновления компонентов
2. Внедрение шины данных	B) Гарантированная и отказоустойчивая передача событий и данных между компонентами
3. Создание отдельного хранилища для моделей	C) Управление жизненным циклом, версионирование и контроль развертывания ML-моделей
4. Применение контейнеризации	D) Обеспечение идентичности среды выполнения на всех этапах — от разработки до промышленной эксплуатации

Задание № 4. Установите соответствие между архитектурным решением при проектировании комплексной системы ИИ для промышленной безопасности и его основной целью.

Архитектурное решение	Цель
1. Выделение микросервиса для управления моделями в отдельный контейнер.	A) Обеспечение целостности и конфиденциальности данных и кода на периферии сети.
2. Использование шины сообщений между модулем сбора данных и аналитическим движком.	B) Возможность независимого масштабирования и обновления компонента, отвечающего за исполнение ML-моделей.
3. Внедрение модуля аппаратного обеспечения с поддержкой TPM на edge-устройствах.	C) Гарантированная доставка событий и асинхронное взаимодействие в условиях высокой нагрузки.
4. Разделение слоя данных на «озеро» сырых данных и витрины для конкретных задач	D) Эффективное хранение больших объемов разнородных данных и их подготовка для задач анализа.

Задание № 5. Установите правильную последовательность основных этапов руководства разработкой архитектуры комплексной системы искусственного интеллекта для промышленной безопасности.

а) Формализация нефункциональных требований: отказоустойчивость, масштабируемость, безопасность, латентность.

б) Выбор и обоснование конкретных технологий, инструментов и протоколов для реализации каждого компонента.

в) Согласование архитектурного видения и ключевых решений с заказчиком и ключевыми стейкхолдерами.

г) Анализ предметной области, выявление бизнес-требований и ограничений.

д) Декомпозиция системы на ключевые компоненты и определение взаимодействий между ними.

Перечень заданий открытого типа

Задание № 1. Как называется лицо, которое утверждает бюджет, ключевые продукты и обладает высшей властью в проекте?

Задание № 2. Как называется процесс выявления, анализа и реагирования на риски проекта?

Задание № 3. Как называется график, визуализирующий зависимость задач проекта от времени и ресурсов?

Задание № 4. Дополните определение, вставляя пропущенное слово:
Модель проекта, при которой разработка ведется короткими циклами (итерациями), поставляющими инкремент рабочего продукта, называется _____ разработкой.

Задание № 5. Дополните предложение, вставляя пропущенное слово:
Дополните принцип проектирования: Принцип _____ в архитектуре означает, что компонент должен быть открыт для расширения, но закрыт для модификации.

4. ПЕРЕЧЕНЬ ЗАДАНИЙ ДЛЯ ОЦЕНКИ СФОРМИРОВАННОСТИ КОМПЕТЕНЦИЙ

Формируемая компетенция: ПК-1

Перечень заданий закрытого типа

Задание № 1. При проектировании информационно-аналитической системы для контроля технологического процесса нефтеперерабатывающего завода, какой из компонентов будет отвечать за централизованный сбор, нормализацию и корреляцию событий из систем АСУ ТП, сетевого оборудования и журналов безопасности?

A) Система управления базами данных.
B) SIEM-платформа.
C) Средство визуализации.
D) Сервер хранения резервных копий.

Задание № 2. Какой принцип разработки архитектуры сложной ИАС для промышленного объекта предпочтительнее для обеспечения возможности независимого обновления и масштабирования модулей анализа сетевого трафика, детектирования аномалий в данных датчиков и генерации отчетов?

A) Использование единого универсального программного пакета.
B) Применение микросервисной архитектуры.
C) Разработка монолитного клиент-серверного приложения.
D) Заказ готового коробочного решения у вендора.

Задание № 3. При разработке модуля машинного обучения для ИАС, предназначенного для прогнозирования сбоев оборудования на основе данных вибрационных датчиков, какой Python-библиотекой нецелесообразно пользоваться для первичной обработки и очистки временных рядов?

A) Scapy.
B) Pandas.
C) NumPy.
D) scikit-learn.

Задание № 4. Какой из перечисленных этапов является логическим началом процесса разработки новой ИАС для мониторинга безопасности промышленной сети?

A) Покупка серверного оборудования.
B) Написание кода для пользовательского интерфейса.
C) Определение целей, требований и модели угроз.
D) Настройка правил межсетевого экрана.

Задание № 5. Для реализации в ИАС функции автоматического реагирования на инциденты путем исполнения заранее описанных сценариев используется компонент класса:

A) ETL-система.
B) SOAR.
C) VPN-шлюз.
D) Система резервного копирования.

Задание № 6. Какой подход к интеграции практик безопасности в жизненный цикл разработки программных компонентов для ИАС позволяет выявлять уязвимости на ранних этапах и является частью культуры DevSecOps?

A) Выделенный этап пентеста после сдачи проекта.
B) «Сдвиг влево» безопасности.
C) Годовой аудит безопасности силами третьей стороны.
D) Установка антивируса на рабочие станции разработчиков.

Задание № 7. Установите соответствие между ключевым компонентом архитектуры современной ИАС для промышленной безопасности и его основной функцией.

Компонент архитектуры ИАС	**Основная функция**
1. Хранилище данных (Data Warehouse)	A) Автоматическое выполнение сценариев реагирования на инциденты.
2. Аналитическая платформа (OLAP)	B) Долгосрочное структурированное хранение исторических данных для ретроспективного анализа.
3. SOAR-платформа	C) Интерактивное многомерное исследование данных аналитиком.
4. Система моделирования угроз	D) Формализованное описание активов, уязвимостей и векторов атак для оценки рисков.

Задание № 8. Установите соответствие между этапом жизненного цикла разработки ИАС и его ключевым содержанием.

Этап жизненного цикла ИАС	**Ключевое содержание**
1. Сбор и анализ требований	A) Создание диаграмм развертывания, спецификаций API и схем баз данных.
2. Проектирование архитектуры	B) Написание кода, модульное тестирование, интеграция отдельных компонентов.
3. Непосредственная разработка	C) Формализация целей системы, описание бизнес-процессов, интервью с стейкхолдерами
4. Внедрение и ввод в эксплуатацию	D) Пилотная эксплуатация на одном участке, обучение пользователей, передача документации.

Задание № 9. Установите правильную последовательность этапов работы над проектом интеллектуальной системы обнаружения аномалий в технологическом процессе на основе данных датчиков SCADA.

а) Обучить модель машинного обучения на данных, собранных в нормальном режиме работы.

б) Интерпретировать результаты работы модели, сопоставить выявленные аномалии с возможными инцидентами кибербезопасности и сформулировать рекомендации для операторов.

в) Спроектировать архитектуру системы: определить место внедрения, способы интеграции с SCADA и форматы данных.

г) Провести анализ предметной области: изучить технологический процесс, идентифицировать критические параметры и смоделировать угрозы.

д) Развернуть обученную модель в тестовом контуре, настроить пороги срабатывания и систему оповещений.

Задание 10. Установите правильную последовательность разработки алгоритма интеллектуального анализа журналов событий безопасности для выявления аномалий в действиях операторов промышленной системы.

а) Собрать и предобработать исторические журналы событий, выделив признаки, связанные с действиями пользователей.

б) Применить алгоритм кластеризации или обнаружения аномалий для выявления отклоняющихся сессий работы.

в) Сформулировать задачу: автоматическое выявление сессий работы оператора, отклоняющихся от его типичного поведения или корпоративных политик.

г) Интерпретировать результаты: проанализировать выявленные аномальные сессии, определить их потенциальную опасность и сформировать отчет для службы безопасности.

д) Разработать и обучить модель нормального поведения для каждого оператора на основе его исторических данных.

Перечень заданий открытого типа

Задание № 1. Задание № 1. Какая популярная Python-библиотека является стандартом де-факто для выполнения операций предобработки и анализа структурированных данных?

Задание № 2. Какой фреймворк/стандарт де-факто используется для описания тактик, техник и процедур киберпротивников при моделировании угроз для промышленных систем?

Задание № 3. Назовите ключевую Python-библиотеку, предоставляющую готовые реализации множества классических алгоритмов машинного обучения и инструментов для оценки моделей.

Задание № 4. Какой основной международный стандарт серии МЭК 62443 регулирует вопросы кибербезопасности систем АСУ ТП и промышленных сетей?

Задание № 5. Дополните определение, вставляя пропущенное слово:
Процесс автоматической сборки, тестирования и развертывания программных компонентов при каждом изменении кода называется _____ интеграцией и доставкой.

Задание № 6. Дополните определение, вставляя пропущенное слово:
Принцип _____ требует, чтобы каждому компоненту системы, пользователю или процессу предоставлялись минимально необходимые права доступа для выполнения легитимных задач.

Формируемая компетенция: ПК-2

Перечень заданий закрытого типа

Задание № 1. Какой документ является первичным результатом формализации задачи по созданию системы мониторинга аномалий в сети промышленного предприятия и содержит детальные требования к функционалу, данным и интерфейсам?

A) Презентация для руководства.
B) Техническое задание .
C) Финансовый отчет.
D) План маркетинга.

Задание № 2. При анализе защищенности промышленной системы выявлена уязвимость в устаревшей версии ПО HMI. Какой из перечисленных форматов наименее подходит для формализации задачи по устранению этой уязвимости в виде конкретного поручения?

A) Запись в системе управления уязвимостями.
B) Статистический отчет о количестве уязвимостей за квартал.
C) Техническое задание на обновление или замену компонента.
D) Чек-лист действий для инженерной службы.

Задание № 3. Какой международный стандарт является ключевым для формализации требований к безопасности при проектировании и аудите систем АСУ ТП и промышленных сетей?

A) ISO 9001.
B) МЭК 62443 .
C) PCI DSS.
D) GDPR

Задание № 4. Для формализации гипотезы о возможности атаки на контроллер методом подмены данных по протоколу Modbus TCP необходимо в первую очередь определить:

A) Стоимость нового контроллера.
B) Конкретные наблюдаемые индикаторы в сетевом трафике.
C) График отпусков обслуживающего персонала.
D) Бренд используемого межсетевого экрана.

Задание № 5. Какой метод анализа данных наиболее применим для формализации задачи по прогнозированию периодов повышенного риска сбоев в работе промышленной сети на основе исторических логов событий?

A) Кластеризация).
B) Анализ временных рядов.
C) Классификация по известным сигнатурам.
D) Ручной выборочный аудит.

Задание № 6. При формализации рекомендаций по результатам анализа инцидента с заражением рабочей станции инженера неправильным будет предложение:

A) Внедрить сегментацию сети, изолировав инженерный сегмент от корпоративного.
B) Обновить антивирусные базы на всех узлах.
C) Увеличить частоту создания резервных копий технологических данных без изменения политик доступа.
D) Внедрить двухфакторную аутентификацию для доступа к системам АСУ ТП.

Задание № 7. Установите соответствие между этапом формализации задачи ИБ для промышленной системы и его ключевым результатом.

Этап формализации	**Ключевой результат**
1. Определение целей и границ анализа	A) Чек-лист или модель угроз, описывающие активы, уязвимости и потенциальные векторы атак.
2. Анализ контекста и моделирование угроз	B) Четкая формулировка: "Снизить среднее время обнаружения аномальных команд ПЛК до N минут".
3. Определение источников и методов	C) Список данных: сетевые пакеты, логи контроллеров, журналы HMI, данные датчиков.
4. Определение критериев успеха	D) Количественные метрики: процент ложных срабатываний, полнота обнаружения атак.

Задание № 8. Установите соответствие между методом обработки/интерпретации данных промышленных систем и его описанием.

Метод обработки данных	**Описание**
1. Декодирование промышленных протоколов	A) Анализ последовательности и временных меток событий для выявления аномальных последовательностей
2. Анализ временных последовательностей	B) Использование алгорит.мов без учителя для выявления скрытых паттернов или кластеров в данных телеметрии, не соответствующих нормальному режиму работы.
3. Обнаружение аномалий в данных датчиков	C) Преобразование сырых сетевых пакетов в читаемый формат команд и параметров для последующего анализа.
4. Корреляция событий из разнородных источников	D) Связывание событий из сетевого трафика АСУ ТП с попытками доступа из

	корпоративной сети для выявления сложных межсегментных атак.

Задание № 9. Установите правильную последовательность действий по формализации задачи для разработки системы мониторинга целостности программного обеспечения промышленных контроллеров.

а) Определить перечень контролируемых контроллеров и конкретные признаки несанкционированного изменения.

б) Согласовать с технологами допустимые методы и окна для проведения проверок, чтобы не нарушить технологический цикл.

в) Сформулировать итоговую постановку задачи в виде технического задания, включающего цели, источники данных и критерии успеха.

г) Проанализировать нормативные требования и типовые векторы атак на ПЛК по MITRE ATT&CK for ICS.

д) Выбрать методы и инструменты для безопасного удаленного сбора данных с ПЛК.

Задание 10. Установите правильную последовательность формализации задачи по созданию системы мониторинга сетевого трафика промышленных протоколов на предмет признаков целевой атаки.

а) Определить конкретные индикаторы компрометации в сетевом трафике: нестандартные коды функций, аномальные интервалы запросов, передача данных на внешние адреса.

б) Согласовать итоговую постановку задачи, включающую модель угроз, план сбора данных и ожидаемые результаты.

в) Изучить спецификации целевых промышленных протоколов и их типовое использование в системе.

г) Сформулировать гипотезу угрозы на основе тактики MITRE ATT&CK for ICS, например, «Манипулирование управляющими командами».

д) Выбрать методы обнаружения: сигнатурный анализ, статистические методы анализа временных рядов трафика.

Перечень заданий открытого типа

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

Задание № 2. Какой класс промышленных сетевых протоколов характеризуется отсутствием встроенных механизмов аутентификации и шифрования, что должно быть учтено при формализации задач по их защите?

Задание № 3. Какой подход к обработке данных подразумевает их анализ в момент генерации и используется для формализации задач мониторинга, требующих немедленного реагирования?

Задание № 4. Какая одна из ключевых составных частей технического задания на систему мониторинга ИБ определяет, как система должна масштабироваться, отказывать и восстанавливаться?

Задание № 5. Дополните определение, вставляя пропущенное слово:
Подход к управлению безопасностью, при котором меры защиты выбираются и приоритезируются на основе оценки _____, называется риск-ориентированным подходом.

Задание № 6. Дополните определение, вставляя пропущенное слово:
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 классификации сетевых пакетов промышленного протокола Modbus TCP на нормальные и вредоносные в реальном времени, где критична низкая задержка и важна интерпретируемость решений, наиболее подходящим комплексом методов ИИ будет:

A) Ансамбль "легких" алгоритмов.
B) Глубокая сверточная нейронная сеть.
C) Генеративно-состязательная сеть.
D) Рекуррентная нейронная сеть с вниманием.

Задание № 2. При выборе инструментальных средств для создания прототипа системы прогнозирования кибератак в сети больницы, где команда обладает сильными навыками в Python, но ограничена во времени, ключевым решающим фактором будет:

A) Возможность развертывания на специализированных AI-ускорителях.
B) Наличие богатой экосистемы библиотек для быстрого прототипирования.
C) Поддержка распределенного обучения на сотнях GPU.
D) Наличие встроенных compliance-отчетов для стандарта HIPAA.

Задание № 3. Какой Python-фреймворк является специализированным инструментальным средством для исследования, генерации и защиты от состязательных атак на модели машинного обучения и должен быть выбран для соответствующих задач в ИБ?

A) Apache Spark.
B) IBM Adversarial Robustness Toolbox.
C) TensorFlow Extended.
D) MLflow.

Задание № 4. Для задачи анализа тональности текстовых сообщений в корпоративном чате на предмет внутренних угроз, где важна высокая точность понимания контекста и сленга, оптимальным выбором будет использование:

A) Метода "мешок слов" с классификатором SVM.
B) Предобученной языковой модели на архитектуре Transformer
C) Скрытой марковской модели.
D) Ручного написания правил.

Задание № 5. При выборе архитектуры системы ИИ для мониторинга видео с камер наблюдения в защищенном помещении на предмет несанкционированного доступа, ключевым нефункциональным требованием, влияющим на выбор, является:

A) Необходимость обработки потока видео в реальном времени с низкой латенцией.
B) Требование к хранению всех видеозаписей в сыром виде в течение 10 лет.
C) Наличие интерфейса на русском языке.
D) Стоимость лицензии на операционную систему для сервера.

Задание № 6. Какой метод машинного обучения является наиболее подходящим для задачи обнаружения новых, ранее неизвестных типов аномалий в поведении пользователей медицинской информационной системы, когда размеченных данных об атаках практически нет?

A) Логистическая регрессия.
B) Обучение без учителя, например, изолирующий лес (Isolation Forest) или автокодировщик.
C) Метод опорных векторов с учителем.
D) Глубокое обучение с подкреплением.

Задание № 7. Установите соответствие между особенностью предметной области и предпочтительным классом методов/инструментов ИИ для её решения.

Особенность предметной области / задачи ИБ	Класс методов/инструментов ИИ
1. Анализ последовательностей команд в журналах для выявления многоэтапных APT-атак.	A) Методы анализа временных рядов и последовательностей.
2. Обогащение событий SIEM контекстом из внешних источников угроз в реальном времени.	B) Интеграционные платформы и API для работы с Threat Intelligence Feeds.
3. Автоматическое категорирование инцидентов из тикетов SOC по стандартным тактикам.	C) Алгоритмы классификации текстов на основе предобученных моделей.
4. Визуализация сложных взаимосвязей между узлами сети и атакующими для расследования.	D) Инструменты для визуализации графов

Задание № 8. Установите соответствие между задачей в области ИБ для промышленной системы и рекомендуемым специализированным программным обеспечением или фреймворком.

Задача ИБ в АСУ ТП	Рекомендуемое специализированное ПО / фреймворк
1. Сбор, парсинг и нормализация данных промышленных протоколов	A) SIEM-платформа с поддержкой Industrial Add-ons.
2. Комплексная корреляция событий из IT и OT сетей, генерация алертов.	B) Специализированные средства анализа сетевого трафика АСУ ТП
3. Создание и управление плейбуками автоматического реагирования на инциденты в технологической сети.	C) Платформы класса SOAR
4. Непрерывный мониторинг активов и уязвимостей в промышленной сети.	D) Пассивные сканеры и платформы для управления активами АСУ ТП

Задание № 9. Установите правильную последовательность выбора комплекса методов и инструментов ИИ для решения задачи классификации типов атак в трафике промышленных протоколов.

а) Выбрать финальный стек технологий.

б) Сформировать список требований к решению: точность, скорость работы в реальном времени, интерпретируемость результатов, устойчивость к шуму.

в) Провести практические эксперименты с 2-3 наиболее подходящими алгоритмами на подготовленных данных.

г) Изучить особенности сетевого трафика целевых протоколов для понимания структуры данных и потенциальных аномалий.

д) Проанализировать доступные инструменты и опубликованные исследования по схожим задачам.

Задание 10. Установите правильную последовательность выбора методов и инструментов для задачи прогнозирования отказов оборудования на основе данных вибрационных датчиков и телеметрии.

а) Провести сравнительное тестирование выбранных алгоритмов на исторических данных с известными отказами.

б) Сформулировать задачу как проблему прогнозирования временного ряда с целью заблаговременного обнаружения признаков поломки.

в) Определить критерии выбора: точность прогноза, раннее предупреждение, возможность работы в режиме реального времени, интерпретируемость.

г) Изучить предметную область: типы отказов, физику процессов, доступные датчики и характерные признаки в данных.

д) Выбрать инструментарий: библиотеки для обработки временных рядов, фреймворки машинного обучения.

Перечень заданий открытого типа

Задание № 1. При работе с конфиденциальными медицинскими данными для обучения модели, какой математический метод обеспечения приватности следует выбрать, чтобы гарантировать, что модель не запомнит и не раскроет конкретные записи из обучающей выборки?

Задание № 2. Какой открытый фреймворк от MITRE предоставляет таксономию атак на системы ИИ и должен быть использован для выбора методов тестирования и защиты разрабатываемой интеллектуальной системы?

Задание № 3. Какой класс архитектур нейронных сетей является доминирующим выбором для задач обработки естественного языка в системах анализа инцидентов и должен быть предпочтен простым методам "мешка слов" для сложных задач?

Задание № 4. Для интеграции самописной ML-модели детектирования аномалий в существующую корпоративную SIEM-систему, какой стандартный подход или формат данных следует использовать для отправки результатов?

Задание № 5. Дополните определение, вставляя пропущенное слово:
Принцип _____ в разработке безопасных систем ИИ требует внедрения контроля безопасности на всех этапах жизненного цикла — от проектирования до эксплуатации.

Задание № 6. Дополните определение, вставляя пропущенное слово:
_____ вычислительная парадигма позволяет обрабатывать данные непосредственно на edge-устройствах, что снижает задержки и риски утечки при передаче в центр обработки.

Формируемая компетенция: ПК-5

Перечень заданий закрытого типа

Задание № 1. Для проектирования аппаратно-программного комплекса ИИ, который будет непрерывно обрабатывать потоки видео с камер наблюдения в режиме реального времени на промышленном объекте, ключевым аппаратным решением, позволяющим эффективно выполнять нейросетевой инференс с низкой задержкой, является:

A) Центральный процессор высокой частоты.
B) Графический процессор или специализированный ускоритель.
C) Большой объем оперативной памяти.
D) Быстрый твердотельный накопитель.

Задание № 2. При разработке программного обеспечения для интеллектуальной системы прогнозирования отказов медицинского оборудования, где точность напрямую влияет на безопасность пациентов, критически важным принципом разработки является:

A) Максимизация быстродействия алгоритмов в ущерб точности.
B) Обеспечение надежности, отказоустойчивости и валидации результатов модели.
C) Использование исключительно open-source библиотек.
D) Минимизация количества строк кода.

Задание № 3. Какой подход является ключевым при модернизации существующей системы контроля доступа с внедрением модуля распознавания лиц для обеспечения его информационной безопасности на этапе разработки?

A) Принцип «Security by Design».
B) Тестирование безопасности после завершения всех работ.
C) Надежда на встроенные механизмы безопасности операционной системы.

D) Использование только аппаратных средств защиты.

Задание № 4. При выборе программного фреймворка для разработки компонента машинного обучения, который будет интегрирован в распределенную систему безопасности умного города, наименее значимым критерием в контексте ПК-5.1 будет:

A) Наличие встроенных средств для обеспечения конфиденциальности данных.
B) Поддержка развертывания в изолированных сетях.
C) Популярность фреймворка в академической среде для исследовательских задач.
D) Соответствие требованиям отраслевых стандартов безопасности.

Задание № 5. Какой аспект аппаратного обеспечения становится критически важным при разработке edge-устройства ИИ для автономного анализа данных датчиков на удаленной нефтяной вышке?

A) Поддержка последней версии графического интерфейса.
B) Устойчивость к экстремальным условиям, энергоэффективность и надежность.
C) Максимальная тактовая частота процессора.
D) Наличие подсветки корпуса.

Задание № 6. При модернизации SCADA-системы завода путем добавления интеллектуального модуля для детектирования аномалий в технологическом процессе, первоочередным требованием информационной безопасности к новому программному компоненту является:

A) Наличие сложной анимации в интерфейсе оператора.
B) Невозможность его несанкционированного воздействия на исполнительные механизмы (ПЛК) и гарантированная целостность данных.
C) Максимальная скорость обучения модели на исторических данных.
D) Использование облачных сервисов для хранения всех данных.

Задание № 7. Установите соответствие между этапом руководства разработкой архитектуры комплексной системы ИИ и ключевым решением или действием руководителя проекта.

Этап руководства разработкой архитектуры	**Ключевое решение/действие руководителя проекта**
1. Анализ предметной области и требований	A) Выбор парадигмы взаимодействия компонентов и протоколов обмена данными с учетом требований ИБ.
2. Определение высокоуровневой архитектуры	B) Утверждение решений по резервированию, мониторингу работоспособности и аварийному восстановлению компонентов ИИ.
3. Проектирование интеграции и безопасности	C) Определение ключевых нефункциональных требований: латентность, пропускная способность, доступность, безопасность данных
4. Планирование эксплуатационных характеристик	D) Внедрение практик DevSecOps, выбор инструментов статического/динамического анализа кода, планирование аудитов безопасности.

Задание № 8. Установите соответствие между классом интеллектуальных систем для предметной области «Киберфизические системы» и особенностью учета требований ИБ при их разработке/модернизации.

Класс интеллектуальных систем	**Особенность учета требований ИБ при разработке**
1. Беспилотный транспорт	A) Обеспечение безопасности жизни, защита от дистанционного захвата управления, целостность данных сенсоров.

2. Промышленные АСУ ТП	B) Защита критических технологических процессов от саботажа, устойчивость к целевым APT-атакам, работа в изолированных сетях.
3. Медицинские системы жизнеобеспечения	C) Гарантированная доступность и безотказность, защита конфиденциальных данных пациентов, валидация решений ИИ.
4. Умные энергетические сети	D) Защита от атак, способных вызвать каскадные отказы и масштабные отключения, контроль целостности данных телеметрии.

Задание № 9. Установите правильную последовательность этапов разработки программного обеспечения lightweight-агента для анализа событий безопасности на edge-устройстве в промышленной сети.

а) Разработать и протестировать прототип агента, проверив корректность сбора данных и работу алгоритмов в изолированной среде.

б) Определить технические требования к агенту: поддержка ОС устройства, ограничения по памяти/CPU, защищенный канал связи с сервером.

в) Внедрить в код агента механизмы обеспечения целостности и аутентичности.

г) Провести приемо-сдаточные испытания агента на реальном целевом оборудовании в промышленной сети.

д) Выбрать язык программирования и библиотеки, соответствующие требованиям производительности и безопасности.

Задание 10. Установите правильную последовательность разработки защищенного шлюза для безопасной передачи телеметрии с промышленных датчиков в облачную систему аналитики.

а) Реализовать и протестировать функции шлюза: сбор данных, предварительная обработка, шифрование, передача по защищенному каналу.

б) Определить требования: поддержка интерфейсов датчиков, пропускная способность, алгоритмы шифрования, стойкость к средам.

в) Внедрить механизмы контроля целостности программного обеспечения шлюза и аутентификации при загрузке.

г) Провести пентест шлюза на предмет уязвимостей и испытания в условиях, близких к эксплуатационным.

д) Выбрать аппаратную платформу и компоненты, соответствующие требованиям надежности и безопасности.

Перечень заданий открытого типа

Задание № 1. При построении интеллектуальной системы для обработки персональных медицинских данных какой математический метод следует применить на этапе обучения модели, чтобы гарантировать конфиденциальность данных и соответствие требованиям регуляторов?

Задание № 2. Назовите ключевой международный стандарт, который необходимо учитывать при модернизации программно-аппаратного обеспечения систем ИИ для промышленных систем управления в части требований кибербезопасности.

Задание № 3. Какой архитектурный стиль является предпочтительным при разработке комплексной, масштабируемой и легко обновляемой системы ИИ, объединяющей модули сбора данных, ML-пайплайны и сервисы инференса?

Задание № 4. Какая практика управления инфраструктурой позволяет единообразно и безопасно разворачивать как программные компоненты ИИ, так и их среду выполнения на различных аппаратных платформах?

Задание № 5. Дополните определение, вставляя пропущенное слово:
_____ обучение — это децентрализованный подход к машинному обучению, позволяющий обучать модель на данных, которые остаются на устройствах-источниках, что повышает безопасность и конфиденциальность данных.

Задание № 6. Дополните определение, вставляя пропущенное слово:
Процесс проверки и подтверждения того, что данные, используемые для обучения и работы модели ИИ, не были намеренно искажены для манипуляции её результатами, называется защитой от _____ данных.

Формируемая компетенция: ПК- 7

Перечень заданий закрытого типа

Задание № 1. Какой этап разработки архитектуры комплексной системы ИИ является первым и ключевым для последующего успеха проекта?
A) Написание кода отдельных модулей.
B) Выбор фреймворка для машинного обучения.
C) Анализ предметной области и определение требований заинтересованных сторон.
D) Закупка серверного оборудования.

Задание № 2. Какой из перечисленных инструментов является стандартом де-факто для описания и документирования архитектуры программных систем, включая комплексные системы ИИ?
A) Microsoft Visio.
B) Язык UML.
C) Trello.
D) Блок-схемы в PowerPoint.

Задание № 3. Руководитель проекта по созданию интеллектуальной системы ИБ для АСУ ТП решает, где будет выполняться обработка данных ML-моделью: на периферийных устройствах или в центральном облаке. Какой нефункциональный аспект архитектуры является для него самым критичным при данном выборе?
A) Стоимость лицензий на ПО.
B) Задержка при принятии решений.
C) Цвет интерфейса администратора.
D) Количество строк кода.

Задание № 4. Какой международный стандарт следует использовать в качестве основы для проектирования архитектуры кибербезопасности в промышленных системах при создании комплексной системы ИИ?
A) ISO 9001.
B) МЭК 62443.
C) ITIL.
D) COBIT.

Задание № 5. Какой из перечисленных документов является основным формальным документом, утверждающим объем, сроки, бюджет и ключевых участников проекта по созданию комплексной системы ИИ?
A) Техническое задание.
B) Презентация для инвесторов.
C) Устав проекта.
D) План коммуникаций.

Задание № 6. Какая из перечисленных диаграмм в рамках UML является наиболее важной для визуализации высокоуровневого взаимодействия основных компонентов системы и внешних сущностей?

A) Диаграмма классов (Class Diagram).
B) Диаграмма развертывания (Deployment Diagram).
C) Диаграмма компонентов (Component Diagram).
D) Диаграмма вариантов использования

Задание № 7. Установите соответствие между ключевым решением при проектировании архитектуры комплексной системы ИИ и его основной целью.

Ключевое архитектурное решение	**Основная цель**
5. Использование микросервисной архитектуры	A) Обеспечение возможности независимого масштабирования и обновления компонентов
6. Внедрение шины данных	B) Гарантированная и отказоустойчивая передача событий и данных между компонентами
7. Создание отдельного хранилища для моделей	C) Управление жизненным циклом, версионирование и контроль развертывания ML-моделей
8. Применение контейнеризации	D) Обеспечение идентичности среды выполнения на всех этапах — от разработки до промышленной эксплуатации

Задание № 8. Установите соответствие между архитектурным решением при проектировании комплексной системы ИИ для промышленной безопасности и его основной целью.

Архитектурное решение	**Цель**
5. Выделение микросервиса для управления моделями в отдельный контейнер.	A) Обеспечение целостности и конфиденциальности данных и кода на периферии сети.
6. Использование шины сообщений между модулем сбора данных и аналитическим движком.	B) Возможность независимого масштабирования и обновления компонента, отвечающего за исполнение ML-моделей.
7. Внедрение модуля аппаратного обеспечения с поддержкой TPM на edge-устройствах.	C) Гарантированная доставка событий и асинхронное взаимодействие в условиях высокой нагрузки.
8. Разделение слоя данных на «озеро» сырых данных и витрины для конкретных задач	D) Эффективное хранение больших объемов разнородных данных и их подготовка для задач анализа.

Задание № 9. Установите правильную последовательность основных этапов руководства разработкой архитектуры комплексной системы искусственного интеллекта для промышленной безопасности.

а) Формализация нефункциональных требований: отказоустойчивость, масштабируемость, безопасность, латентность.
б) Выбор и обоснование конкретных технологий, инструментов и протоколов для реализации каждого компонента.
в) Согласование архитектурного видения и ключевых решений с заказчиком и ключевыми стейкхолдерами.
г) Анализ предметной области, выявление бизнес-требований и ограничений.
д) Декомпозиция системы на ключевые компоненты и определение взаимодействий между ними.

Задание № 10. Установите правильную последовательность ключевых этапов руководства разработкой архитектуры комплексной системы искусственного интеллекта для промышленного объекта.

а) Детализация архитектурных решений: выбор конкретных технологий, протоколов, инструментов и проектирование взаимодействий между компонентами (низкоуровневое проектирование).

б) Сбор и анализ функциональных и нефункциональных требований от заказчика, технологов и специалистов по безопасности.

в) Утверждение итоговой архитектурной документации у спонсора проекта и ключевых заинтересованных сторон.

г) Идентификация критически важных активов, моделирование угроз и определение ограничений (регуляторных, технических, бюджетных).

д) Создание и согласование концептуальной архитектуры (высокоуровневой модели), определяющей основные компоненты системы и их назначение.

е) Проведение архитектурного обзора (review) и оценка решений на соответствие требованиям, включая пилотное тестирование критических компонентов.

Перечень заданий открытого типа

Задание № 1. Как называется лицо, которое утверждает бюджет, ключевые продукты и обладает высшей властью в проекте?

Задание № 2. Как называется процесс выявления, анализа и реагирования на риски проекта?

Задание № 3. Как называется график, визуализирующий зависимость задач проекта от времени и ресурсов?

Задание № 4. Как называется документ, описывающий подход, методы и инструменты управления содержанием проекта?

Задание № 5. Дополните определение, вставляя пропущенное слово:
Модель проекта, при которой разработка ведется короткими циклами, поставляющими инкремент рабочего продукта, называется _____ разработкой.

Задание № 6. Дополните предложение, вставляя пропущенное слово:
Дополните принцип проектирования: Принцип _____ в архитектуре означает, что компонент должен быть открыт для расширения, но закрыт для модификации.

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	В
	№ 2	В
	№ 3	1-B, 2-C, 3-A, 4-D.
	№ 4	1-C, 2-A, 3-B, 4-D
	№ 5	г в а д б
	Задания открытого типа	
	№ 1	Pandas.
	№ 2	MITRE ATT&CK
	№ 3	scikit-learn
	№ 4	непрерывной
	№ 5	наименьших привилегий
ПК-2	**Задания закрытого типа**	
	№ 1	В
	№ 2	В
	№ 3	1-B, 2-A, 3-C, 4-D
	№ 4	1-C, 2-A, 3-B, 4-D
	№ 5	г а б д в
	Задания открытого типа	
	№ 1	MITRE ATT&CK
	№ 2	Унаследованные
	№ 3	Stream Processing
	№ 4	рисков
	№ 5	первопричин
ПК-3	**Задания закрытого типа**	
	№ 1	А
	№ 2	В
	№ 3	1-A, 2-B, 3-C, 4-D
	№ 4	1-B, 2-A, 3-C, 4-D
	№ 5	г б д в а
	Задания открытого типа	
	№ 1	Дифференциальная приватность
	№ 2	MITRE ATLAS
	№ 3	Трансформеры
	№ 4	Безопасность по умолчанию
	№ 5	Граничные
ПК-5	**Задания закрытого типа**	
	№ 1	В
	№ 2	В
	№ 3	1-C, 2-A, 3-D, 4-B
	№ 4	1-A, 2-B, 3-C, 4-D
	№ 5	б д а в г
	Задания открытого типа	
	№ 1	Дифференциальная приватность

	№ 2	МЭК 62443
	№ 3	Микросервисная архитектура
	№ 4	Федеративное
	№ 5	отравления
ПК-7	**Задания закрытого типа**	
	№ 1	C
	№ 2	B
	№ 3	1-A, 2-B, 3-C, 4-D
	№ 4	1-B, 2-C, 3-A, 4-D
	№ 5	г а д б в
	Задания открытого типа	
	№ 1	Спонсор
	№ 2	Управление
	№ 3	Диаграмма
	№ 4	итерационной
	№ 5	открытости

КЛЮЧИ К ЗАДАНИЯМ ДЛЯ ОЦЕНКИ СФОРМИРОВАННОСТИ КОМПЕТЕНЦИЙ

Таблица 6.

Формируемые компетенции	№ задания	Ответ
ПК-1	**Задания закрытого типа**	
	№ 1	B
	№ 2	B
	№ 3	A
	№ 4	A
	№ 5	C
	№ 6	B
	№ 7	1-B, 2-C, 3-A, 4-D.
	№ 8	1-C, 2-A, 3-B, 4-D
	№ 9	г в а д б
	№ 10	в а д б г
	Задания открытого типа	
	№ 1	Pandas.
	№ 2	MITRE ATT&CK
	№ 3	scikit-learn
	№ 4	МЭК 62443
	№ 5	непрерывной
	№ 6	наименьших привилегий
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-C, 2-A, 3-B, 4-D
	№ 9	г а б д в
	№ 10	г в а д б
	Задания открытого типа	
	№ 1	MITRE ATT&CK
	№ 2	Унаследованные
	№ 3	Stream Processing
	№ 4	Нефункциональные требования
	№ 5	рисков
	№ 6	первопричин
ПК-3	**Задания закрытого типа**	
	№ 1	A
	№ 2	B
	№ 3	B
	№ 4	B
	№ 5	A
	№ 6	B
	№ 7	1-A, 2-B, 3-C, 4-D

	№ 8	1-B, 2-A, 3-C, 4-D
	№ 9	г б д в а
	№ 10	г б в д а
	Задания открытого типа	
	№ 1	Дифференциальная приватность
	№ 2	MITRE ATLAS
	№ 3	Трансформеры
	№ 4	API SIEM
	№ 5	Безопасность по умолчанию
	№ 6	Граничные
ПК-5	**Задания закрытого типа**	
	№ 1	B
	№ 2	B
	№ 3	A
	№ 4	C
	№ 5	B
	№ 6	B
	№ 7	1-C, 2-A, 3-D, 4-B
	№ 8	1-A, 2-B, 3-C, 4-D
	№ 9	б д а в г
	№ 10	б д а в г
	Задания открытого типа	
	№ 1	Дифференциальная приватность
	№ 2	МЭК 62443
	№ 3	Микросервисная архитектура
	№ 4	Контейнеризация
	№ 5	Федеративное
	№ 6	отравления
ПК-7	**Задания закрытого типа**	
	№ 1	C
	№ 2	B
	№ 3	B
	№ 4	B
	№ 5	C
	№ 6	D
	№ 7	1-A, 2-B, 3-C, 4-D
	№ 8	1-B, 2-C, 3-A, 4-D
	№ 9	г а д б в
	№ 10	г д а б в
	Задания открытого типа	
	№ 1	Спонсор
	№ 2	Управление
	№ 3	Диаграмма
	№ 4	План
	№ 5	итерационной
	№ 6	открытости