ЦЕНТРАЛЬНЫЙ УНИВЕРСИТЕТ

УТВЕРЖДЕНА

Решением Ученого совета
АНО ВО «Центральный университет»
«07» марта 2024 г.
Протокол №1

Рабочая программа дисциплины (модуля)
«Разработка интеллектуальных агентов»

Направление подготовки: *02.03.01 Математика и компьютерные науки*

Направленность (профиль) подготовки: *Искусственный интеллект*

Квалификация (степень) выпускника: *бакалавр*

Форма обучения: *очная*

Срок освоения программы: *4 года*

Год набора: *2024*

Москва
2024

ДОКУМЕНТ ПОДПИСАН
ЭЛЕКТРОННОЙ ПОДПИСЬЮ

Сертификат: 0215B0C000D1B3FEB44A37EE631E0C27D4
Владелец: Ивашкевич Евгений Васильевич
Действителен: с 13.01.2026 до 13.04.2027

Электронный документ

Содержание

1. **Краткая характеристика дисциплины (модуля)** 3
2. **Перечень планируемых результатов обучения** 5
3. **Тематический план** 7
4. **Содержание дисциплины (модуля)** 7
5. **Учебно-методическое обеспечение** 8
6. **Материально-техническое обеспечение** 8
7. **Методические и оценочные материалы** 10

1. Краткая характеристика дисциплины (модуля)

Рабочая программа дисциплины (модуля) «Разработка интеллектуальных агентов» составлена в соответствии с федеральным государственным образовательным стандартом высшего образования – бакалавриат по направлению 02.03.01 «Математика и компьютерные науки», профиль «Искусственный интеллект», утвержденный приказом Министерства науки и высшего образования Российской Федерации № 807 от 23.08.2017 года.

Изучение дисциплины (модуля) «Разработка интеллектуальных агентов» формирует ключевые компетенции для создания автономных ИИ-систем, способных решать сложные задачи в реальных бизнес-средах. Полученные знания и навыки позволяют эффективно проектировать, развёртывать и контролировать агентные архитектуры, что становится критически важным в условиях роста автоматизации и ИИ-ориентированных платформ.

Место дисциплины (модуля) в структуре образовательной программы

Настоящая дисциплина (модуль) включена в учебный план по программе подготовки бакалавриата по направлению 02.03.01 «Математика и компьютерные науки», профиль «Искусственный интеллект» и входит в вариативную часть Блока 1, формируемую участниками образовательных отношений, как дисциплина по выбору.

Дисциплина (модуль) изучается на 3 курсе в 6 семестре. Доступна к изучению после успешного освоения дисциплины (модуля) «Обработка естественного языка».

Цель изучения дисциплины (модуля): сформировать системное понимание архитектуры и принципов функционирования интеллектуальных агентов на основе больших языковых моделей и развить практические навыки их разработки, тестирования и развёртывания в реальных условиях.

Задачи изучения дисциплины (модуля):

— изучить архитектуру трансформеров, принципы работы больших языковых моделей и методы их адаптации: fine-tuning, rAg, rlhf;

— освоить компоненты агентных систем: память, планирование, использование инструментов и взаимодействие с внешними сервисами;

— научиться проектировать и реализовывать интеллектуальных агентов с поддержкой mcp и api для интеграции с внешними системами;

— освоить методы оценки, тестирования и мониторинга поведения агентов, включая выявление нецелевого и рискованного поведения;

— развить навыки сборки, деплоя и обеспечения безопасности агентных приложений с использованием современных инструментов (langchain, vllm, векторные базы и др.).

В результате освоения дисциплины (модуля) обучающийся должен:

знать:

— принципы работы llm, архитектуру трансформеров и подходы к их адаптации (fine-tuning, rag, rlhf);

— архитектуру ии-агентов, включая память, планирование и взаимодействие с инструментами;

— протоколы межагентного взаимодействия и основные угрозы безопасности агентных систем;

— методы оценки, мониторинга и обеспечения надёжности агентов.

уметь:

— разрабатывать интеллектуальных агентов с памятью и интеграцией внешних сервисов (через mcp/api); разрабатывать mcp сервера;

— оценивать и тестировать поведение агентов, выявлять нецелевое поведение;

— собирать и деплоить агентные приложения для реального использования.

владеть:

— практическими навыками построения агентных систем от прототипа до работающего приложения;

— инструментами векторного поиска, оркестрации агентов и развёртывания моделей (vllm, langchain и др.);

— методами обеспечения безопасности, контроля и устойчивости агентов;

— навыками архитектурного проектирования с учётом баланса автономности и контроля.

2. Перечень планируемых результатов обучения

Компетенции, формируемые в результате освоения дисциплины (модуля) при проведении учебных занятий в форме контактной работы обучающихся с педагогическими работниками Университета и в форме самостоятельной работы обучающихся:

Компетенция	Содержание компетенции	Индикатор компетенции	Перечень планируемых результатов обучения по дисциплине (модулю)
УК-1.	Способен осуществлять поиск, критический анализ и синтез информации, применять системный подход для решения поставленных задач	УК-1.1.	Знает методы поиска и анализа информации в области искусственного интеллекта, основные принципы критической оценки источников информации и их релевантности.
		УК-1.2.	Умеет критически оценивать источники информации и синтезировать данные из различных источников для решения задач, применять системный подход к анализу и решению комплексных проблем
		УК-1.3.	Имеет практический опыт работы с современными инструментами и технологиями для обработки информации, формулировании и структурировании задач на основе полученной информации
УК-2.	Способен определять круг задач в рамках поставленной цели и выбирать оптимальные способы их решения, исходя из действующих правовых норм, имеющихся ресурсов и ограничений	УК-2.1.	Знает действующие правовые нормы, регулирующие деятельность в области решения задач, основные методы и подходы к определению круга задач
		УК-2.2.	Умеет определять круг задач в рамках поставленной цели, выбирать оптимальные способы решения задач, учитывая имеющиеся ресурсы и ограничения
		УК-2.3.	Имеет практический опыт применения знаний о правовых нормах и ресурсах в реальных ситуациях, разработки и реализации решений в соответствии с установленными ограничениями
ОПК-1.	Способен находить, формулировать и решать актуальные и значимые проблемы прикладной и компьютерной математики	ОПК-1.1.	Знает основные методы и подходы к решению задач прикладной и компьютерной математики, включая алгоритмы, математическое моделирование и теорию оптимизации, а также современные инструменты и технологии, используемые в этой области

		ОПК-1.2.	Умеет анализировать и формулировать математические задачи, применять соответствующие методы и алгоритмы для их решения, а также интерпретировать и представлять результаты в понятной и доступной форме
		ОПК-1.3.	Имеет практический опыт работы над проектами или исследованиями в области прикладной и компьютерной математики, включая участие в конкурсах, олимпиадах или научных публикациях, где были решены актуальные и значимые задачи
ПК-1.	Способен формулировать задачи с математической точностью, обосновывать утверждения строго и анализировать полученные результаты в области математики и компьютерных наук	ПК-1.1.	Знает методы и подходы к формулированию задач, а также основные принципы математического доказательства и анализа результатов.
		ПК-1.2.	Умеет корректно ставить и формулировать математические задачи, применять строгие методы доказательства и анализировать полученные результаты.
		ПК-1.3.	Имеет опыт работы с задачами в области математики и компьютерных наук, включая применение математических методов для решения практических задач
ПК-2.	Способен решать типовые задачи профессиональной деятельности в области искусственного интеллекта, опираясь на информационную и библиографическую культуру, используя информационно-коммуникационные технологии и учитывая основные требования информационной безопасности	ПК-2.1.	Знает основы информационной и библиографической культуры, а также принципы информационной безопасности и применения информационно-коммуникационных технологий в профессиональной деятельности
		ПК-2.2.	Умеет эффективно использовать информационно-коммуникационные технологии для решения стандартных задач профессиональной деятельности, учитывая требования информационной безопасности
		ПК-2.3.	Имеет опыт работы с информационными ресурсами и технологиями в области искусственного интеллекта, включая соблюдение норм информационной безопасности

3. Тематический план

№п/п	Наименование раздела дисциплины (модуля)	Трудоемкость, академические часы				ТКУ (текущий контроль успеваемости)
		Очная форма				
		Аудиторная работа		Контроль	Самостоятельная работа	
		Лекции	Семинары			
1	Основные принципы LLM приложений	10	10		42	Домашнее задание
2	Основные принципы построения интеллектуальных агентов	10	10		42	Домашнее задание
3	Архитектура и проектирование агентских приложений	10	10		42	Домашнее задание
	Зачёт с оценкой			4		Проект
	Итого:	***30***	***30***	***4***	***126***	
Объем дисциплины (модуля) (в ак. ч.)		***190***				
Объем дисциплины (модуля) (в зач. ед.)		***5***				

4. Содержание дисциплины (модуля)

№п/п	Наименование раздела дисциплины (модуля)	Содержание дисциплины (модуля) по темам
1	Основные принципы LLM приложений	Введение Адаптация больших языковых моделей под целевые задачи Обучение с подкреплением на основе человеческого фидбека Подготовка модели к эксплуатации Генерация ответа пользователю с учетом дополнительно найденной релевантной информации (Retrieval Augmented Generation, RAG)
2	Основные принципы построения интеллектуальных агентов	Агенты Мультиагентные системы Мультимодальные агентные системы Самоадаптирующиеся и саморазвивающиеся агентные систем Оценка качества агентных систем
3	Архитектура и проектирование агентских приложений	Агентные системы без программирования и с минимальным программированием Безопасность агентных систем Надежность и управляемость агентных систем Проектирование и деплой агентных систем Примеры агентных систем

5. Учебно-методическое обеспечение

Университет располагает полным набором лицензионного и свободно распространяемого программного обеспечения, включая продукты отечественного производства.

Каждый студент в течение всего периода обучения получает индивидуальный неограниченный доступ к электронно-библиотечной системе и электронной информационно-образовательной среде университета. Эти системы предоставляют возможность доступа к ресурсам из любой точки, где есть подключение к сети Интернет, как на территории университета, так и за его пределами.

Студентам обеспечен удаленный доступ к современным профессиональным базам данных и информационным справочным системам.

Основная литература:

1. Мэрфи, К. П. Вероятностное машинное обучение. Дополнительные темы: основания, вывод : монография / К. П. Мэрфи ; пер. с англ. А. А. Слинкина. – Москва : ДМК Пресс, 2024. - 772 с. – ISBN 978-5-93700-120-7. - Текст : электронный. - URL: https://znanium.ru/catalog/product/2204219.

2. Лакшманан, В. Машинное обучение. Паттерны проектирования : практическое пособие / В. Лакшманан, С. Робинсон, М. Мунн. - Санкт-Петербург : БХВ-Петербург, 2022. - 448 с. - ISBN 978-5-9775-6797-8. - Текст : электронный. - URL: https://znanium.ru/catalog/product/2140204.

Дополнительная литература:

1. Коэльо, Л. Построение систем машинного обучения на языке Python : практическое руководство / Л. Коэльо, В. Ричарт ; пер. с англ. А. А. Слинкина. - 3-е изд. - Москва : ДМК Пресс, 2023. - 304 с. - ISBN 978-5-89818-331-8. - Текст : электронный. - URL: https://znanium.ru/catalog/product/2102618.

6. Материально-техническое обеспечение

Университет располагает материально-технической базой, соответствующей действующим противопожарным правилам и нормам и обеспечивающей проведение всех видов дисциплинарной и междисциплинарной подготовки, практической и научно-исследовательской работ обучающихся, предусмотренных учебным планом.

Помещения, которые представляют собой учебные аудитории для проведения занятий лекционного типа, занятий семинарского (практического) типа, групповых и индивидуальных консультаций, текущего контроля и промежуточной аттестации, а также помещения для самостоятельной работы и помещения для хранения и профилактического обслуживания учебного оборудования. Помещения укомплектованы специализированной мебелью и техническими средствами обучения, служащими для представления учебной информации большой аудитории.

Изучение дисциплины (модуля) обеспечивается в учебных аудиториях, оснащенных:

- столами и стульями;
- компьютерной техникой;
- механическими калькуляторами;
- специализированным оборудованием, включая демонстрационное оборудование.

Помещения для самостоятельной работы обучающихся, в том числе приспособленные для использования инвалидами и лицами с ограниченными возможностями здоровья, оснащены компьютерной техникой с возможностью подключения к сети «Интернет» и обеспечением доступа в электронную информационно-образовательную среду Университета.

Обучающимся предоставляется доступ (в том числе удаленный) к ресурсам информационно-телекоммуникационной сети «Интернет», электронным ресурсам (в том числе электронным библиотечным системам, современным профессиональным базам данных и информационным справочным системам):

№	Наименование портала (издания, курса, документа)	Ссылка
1.	Научная электронная библиотека elibrary.ru библиотека	https://elibrary.ru/defaultx.asp
2.	База данных для IT-специалистов	https://habr.com
3.	База данных ScienceDirect	https://www.sciencedirect.com
4.	Официальный сайт Министерства науки и высшего образования Российской Федерации	https://minobrnauki.gov.ru/
5.	Федеральный портал «Российское образование"	https://www.edu.ru/
6.	Информационная система "Единое окно доступа к образовательным ресурсам"	http://window.edu.ru/
7.	Единая коллекция цифровых образовательных ресурсов	http://school-collection.edu.ru/
8.	Федеральный центр информационно - образовательных ресурсов	http://fcior.edu.ru/

Перечень информационных технологий, используемых при осуществлении образовательного процесса по дисциплине (модулю), в том числе комплект лицензионного программного обеспечения, современные профессиональные базы данных и информационные справочные системы:

Наименование ПО	Производство	Лицензионное / свободно распространяемое
Операционные системы:		
Microsoft Imagine (Windows Client, Server)	зарубежное	лицензионное
Браузеры:		
Яндекс.Браузер	отечественное	свободно распространяемое
Google Chrome	зарубежное	свободно распространяемое
Офисные приложения:		
Microsoft Imagine (Visio, OneNote)	зарубежное	лицензионное
TeXstudio	зарубежное	свободно распространяемое
Adobe Acrobat Reader	зарубежное	свободно распространяемое
Программное обеспечение для планирования и учета времени:		
Toggle app	зарубежное	свободно распространяемое
Системы управления проектами:		
Microsoft Imagine (Project)	зарубежное	лицензионное
Системы управления базами данных:		
Microsoft Imagine (SQL Server)	зарубежное	лицензионное
Системы резервного копирования (backup):		
Acronis Backup Advanced for HyperV	зарубежное	лицензионное
Справочно-правовые системы:		
КонсультантПлюс: справочно-правовая система	отечественное	лицензионное
Средства антивирусной защиты:		
Kaspersky Endpoint Security для бизнеса Стандартный Russian Edition	отечественное	лицензионное
Среды разработки:		
Visual Studio Code	зарубежное	свободно распространяемое
Bash (Unix shell)	зарубежное	свободно распространяемое

Anaconda	зарубежное	свободно распространяемое
Robotic Operating System	зарубежное	свободно распространяемое
CopelliaSim	зарубежное	свободно распространяемое
Google Colaboratory	зарубежное	свободно распространяемое
Пакеты программных средств и библиотек:		
AutoPsy	зарубежное	свободно распространяемое
Interactive Disassembler (IDA)	зарубежное	свободно распространяемое
Системы управления библиографической информацией:		
Zotero	зарубежное	свободно распространяемое
Сервисы и службы:		
Bind	зарубежное	свободно распространяемое
Docker	зарубежное	свободно распространяемое

7. Методические и оценочные материалы

Методические указания для обучающихся по освоению дисциплины (модуля)

В процессе изучения дисциплины (модуля) «Разработка интеллектуальных агентов» в рамках текущего контроля успеваемости используются такие виды учебной работы, как лекции, семинары, домашние задания, проект, а также различные виды самостоятельной работы обучающихся по заданию преподавателя, направленные на развитие навыков профессиональной лексики, закрепление практических профессиональных компетенций, поощрение инициатив.

Лекция – систематическое, последовательное, монологическое изложение преподавателем учебного материала, как правило, теоретического характера.

В процессе лекций рекомендуется вести конспект лекций: кратко и схематично фиксировать основные идеи, выводы и обобщения лекции; выделять важные мысли, ключевые слова и термины. Необходимо отметить вопросы или материалы, которые вызывают затруднения, и попытаться найти ответы в рекомендованной литературе. Если разобраться в материале не удается, следует сформулировать вопрос и задать его преподавателю на консультации или во время семинарского (практического) занятия.

Семинар – это форма учебной деятельности, проводимая в учебном заведении под руководством преподавателя, где студенты активно участвуют в обсуждениях, практических заданиях и других формах взаимодействия.

Для успешной подготовки к семинару рекомендуется заранее ознакомиться с темой занятия и основными материалами, чтобы иметь возможность активно участвовать в обсуждении. Также полезно подготовить вопросы и идеи для обсуждения, что поможет глубже понять материал и продемонстрировать заинтересованность.

Домашнее задание – набор задач по темам недели.

При работе над домашними заданиями важно внимательно ознакомиться с требованиями и сроками выполнения. Рекомендуется разбивать задания на этапы, чтобы избежать перегрузки и лучше усвоить материал. Использовать различные источники информации, включая учебники и онлайн-ресурсы, для более глубокого понимания темы.

Проект – исследовательская работа по дисциплине (модулю) и презентация результатов.

Для успешной подготовки к проекту рекомендуется: четко определить цели и задачи проекта; составить план работы, разбив проект на этапы с указанием сроков выполнения каждого из них; использовать разнообразные источники информации и инструменты для исследования темы; регулярно проверять прогресс и вносить коррективы в план, если это необходимо.

Самостоятельная работа – работа студентов, направленная на углубленное изучение отдельных тем и вопросов учебной дисциплины (модуля).

В процессе самостоятельной работы студенты взаимодействуют с рекомендованными материалами при минимальном участии преподавателя. Задачи студента включают работу с конспектами лекций (обработка текста), повторное изучение учебных материалов планов и тезисов ответов, изучение дополнительных тем, выполнение учебно-исследовательских заданий и другое.

Система оценивания результатов обучения по дисциплине (модулю)

Критерии получения уровня и оценивания сформированности компетенций по дисциплине (модулю) «Разработка интеллектуальных агентов»

Оценивание уровня учебных достижений, обучающихся по дисциплине (модулю), осуществляется в виде текущего контроля успеваемости и промежуточной аттестации.

Промежуточная аттестация по дисциплине (модулю) осуществляется в форме ***зачёта с оценкой***, при этом проводится оценка компетенций, сформированных по дисциплине.

Для оценивания текущего контроля успеваемости и промежуточной аттестации используется десятибалльная шкала оценивания, которая соотносится с традиционной пятибалльной шкалой следующим образом, если иное не указано в силлабусе дисциплины:

Десятибалльная оценка	**Пятибалльная оценка**	**Общая характеристика результата обучения по дисциплине (модулю)**
10	Отлично	Студент полностью владеет знаниями, изложенными в рабочей программе, и глубоко осмысляет дисциплину. Он самостоятельно и логически последовательно отвечает на все вопросы, акцентируя внимание на наиболее важном. Умеет анализировать, сравнивать, классифицировать, обобщать, конкретизировать и систематизировать изученный материал, выделяя ключевые моменты и устанавливая причинно-следственные связи. Четко формулирует ответы, уверенно интерпретирует результаты анализов и других исследований, а также решает сложные задачи. Студент хорошо знаком с методами исследования, необходимыми для практической деятельности, и умеет связывать теоретические аспекты дисциплины (модуля) с практическими задачами.
9	Отлично	
8	Отлично	
7	Хорошо	Студент обладает знаниями предмета почти в полном объеме рабочей программы и самостоятельно, логически последовательно и всесторонне отвечает на все вопросы, акцентируя внимание на наиболее значимых моментах. Он умеет анализировать, сравнивать, классифицировать, обобщать, конкретизировать и систематизировать изученный материал, выделяя его ключевые аспекты и устанавливая причинно-следственные связи. Формулирует свои ответы, уверенно интерпретирует результаты анализов и других исследований, а также решает сложные ситуационные задачи. Студент хорошо знаком с методами исследования, необходимыми для практической
6	Хорошо	

Десятибалльная оценка	Пятибалльная оценка	Общая характеристика результата обучения по дисциплине (модулю)
		деятельности, и умеет связывать теоретические аспекты предмета с практическими задачами.
5	Удовлетворительно	Студент обладает базовыми знаниями по дисциплине (модулю), но испытывает трудности при самостоятельных ответах и использует неточные формулировки. В ходе ответов он допускает ошибки, касающиеся сути вопросов. Студент способен решать только самые простые задачи и владеет лишь минимальным набором методов исследования.
4	Удовлетворительно	
3	Не сдан	Студент не овладел обязательным минимумом знаний по предмету и не может ответить на вопросы, даже если преподаватель задает дополнительные наводящие вопросы.
2	Не сдан	
1	Не сдан	

Дисциплина (модуль) «Разработка интеллектуальных агентов» оценивается следующим образом:

Активность	Вес	Количество	Описание
Домашние задания	70%	4	Набор задач по темам недели
Зачёт с оценкой	30%	1	Проект - Исследовательская работа по дисциплине (модулю) и презентация результатов

Формула расчёта итоговой оценки по дисциплине (модулю) «Разработка интеллектуальных агентов»: «0,7 × среднее за домашние задания + 0,3 × зачёт с оценкой».

Текущий контроль успеваемости обучающихся по дисциплине (модулю)

Примерные домашние задания

Домашнее задание 1.

1. Объясните, в чём заключается разница между прямым использованием LLM и её адаптацией под конкретную задачу с помощью RAG;
2. Опишите, как работает механизм RAG и какие компоненты в него входят: векторное хранилище, генеративная модель;
3. Объясните, зачем используется обучение с подкреплением на основе человеческого фидбека (RLHF) и как оно влияет на поведение модели;
4. Опишите ключевые этапы подготовки LLM к эксплуатации: квантизация, оптимизация инференса, развертывание;
5. Реализуйте простой RAG-пайплайн: загрузите документ, создайте эмбеддинги, сохраните в векторное хранилище и реализуйте поиск по запросу.

Домашнее задание 2.

1. Объясните, из каких основных компонентов состоит архитектура интеллектуального агента: планирование, память, инструменты, исполнение;
2. Опишите, как мультиагентные системы взаимодействуют между собой: обмен сообщениями, координация, делегирование задач;
3. Проанализируйте, как мультимодальные агенты обрабатывают разные типы данных (текст, изображение, аудио) и принимают решения на их основе;
4. Объясните концепцию самоадаптирующихся агентов: как они учатся на ошибках и улучшают свои стратегии со временем;

5. Оцените качество работы агента по таким критериям, как точность выполнения задач, устойчивость к ошибкам и интерпретируемость действий.

Домашнее задание 3.

1. Объясните, как можно создать агентную систему с минимальным программированием с помощью платформ;
2. Опишите основные угрозы безопасности агентных систем: инъекции, нецелевое поведение, утечка данных и способы их предотвращения;
3. Объясните, как обеспечивается надёжность и управляемость агентов: контроль за действиями, логирование, ограничение доступа к инструментам;
4. Разработайте схему архитектуры агентного приложения: определите компоненты, поток данных, точки интеграции и механизм деплоя;
5. Приведите пример реальной агентной системы (например, ассистент поддержки, автоматический аналитик, бот для бронирования) и опишите её структуру и сценарии использования.

Примерное описание задания и критерии оценивания к проекту

Цель проекта: разработать функционального интеллектуального агента или мультиагентную систему, демонстрирующую применение современных подходов к адаптации больших языковых моделей, управлению памятью, взаимодействию с инструментами и обеспечению безопасности в реальных сценариях.

Задачи, которые необходимо выполнить:

— выбрать и обосновать предметную область применения агента (например: техническая поддержка, автоматизация анализа данных, персональный помощник, резервирование ресурсов);

— реализовать агента с использованием одной из современных платформ (langchain, llama index, semantic kernel и др.) и интегрировать механизм rag для доступа к внешним знаниям;

— добавить компоненты агентной архитектуры: память (краткосрочную и долгосрочную), планирование, использование инструментов (api, mcp-серверы), логику принятия решений;

— обеспечить безопасность и контролируемость: реализовать проверку действий, фильтрацию запросов, защиту от инъекций и нецелевого поведения;

— подготовить систему к деплою: оформить в виде веб-интерфейса (streamlit, gradio), задокументировать архитектуру и сценарии использования, при необходимости — развернуть в облаке.

Проект может быть представлен в виде:

— репозитория на github с кодом, документацией и инструкцией по запуску,

— ноутбука с пошаговым описанием,

— демонстрационного видео и презентации,

— работающего веб-приложения.

Критерии оценивания проекта:

— соответствие проекта изученным темам: использование компонентов агентной архитектуры (память, планирование, инструменты), применение rag и адаптации llm;

— глубина реализации: наличие функциональных модулей, работа с внешними сервисами, поддержка диалога и контекста;

— учёт безопасности и надёжности: реализованы меры по контролю действий, фильтрации ввода и предотвращению рискованного поведения;

— качество архитектуры и документации: система спроектирована с учётом масштабируемости, код структурирован, архитектура описана понятно;

— работоспособность и воспроизводимость: приложение запускается, сценарии проверены, инструкции полные и понятные.

Задания для промежуточной аттестации по дисциплине (модулю)

№ п/п	Задание	Ответ	Компетенция
1	Назовите ключевую технологию, лежащую в основе современных интеллектуальных агентов.	Большая языковая модель / LLM	УК-1
2	Укажите подход, при котором модель дополняется внешними знаниями для генерации ответа.	Retrieval Augmented Generation / RAG	УК-1
3	Как называется процесс адаптации модели с учётом предпочтений человека?	Обучение с подкреплением на основе человеческого фидбека / RLHF	УК-1
4	Назовите принцип, при котором система рассматривается как совокупность автономных взаимодействующих компонентов.	Агентный подход / Мультиагентная система	УК-1
5	Как называется документ, описывающий цели, роли и правила взаимодействия агентов в системе?	Агентный контракт / Спецификация поведения	УК-2
6	Назовите метод, позволяющий контролировать действия агента и предотвращать нежелательное поведение.	Механизм сдержек и противовесов / Проверка действий	УК-2
7	Укажите способ обеспечения надёжности агентной системы при сбоях или ошибках.	Восстановление состояния / Fault tolerance	УК-2
8	Как называется процесс оценки корректности и полезности действий агента?	Оценка качества агентной системы / Agent evaluation	УК-2
9	Назовите архитектурный компонент, отвечающий за хранение контекста диалога.	Память агента / Memory	ОПК-1
10	Укажите механизм, позволяющий агенту планировать последовательность действий.	Планирование / Planning	ОПК-1
11	Как называется модуль, с помощью которого агент взаимодействует с внешними сервисами?	Инструмент / Tool / MCP	ОПК-1
12	Назовите формат представления знаний, используемый в RAG-системах.	Векторное хранилище / Embeddings	ОПК-1
13	Назовите платформу для создания агентов с минимальным программированием.	LangChain / LlamaIndex / SmythOS	ПК-1
14	Как называется компонент агента, отвечающий за выбор следующего действия?	Политика / Policy / Reasoning module	ПК-1
15	Назовите технологию, позволяющую агенту использовать внешние API.	MCP / Tool calling / Function calling	ПК-1
16	Как называется подход, при котором агент учится на собственных ошибках?	Самоадаптация / Self-improvement	ПК-1
17	Назовите принцип защиты агентной системы от prompt-инъекций.	Валидация ввода / Input sanitization	ПК-2
18	Как называется механизм, ограничивающий доступ агента к чувствительным операциям?	Контроль привилегий / Role-	ПК-2

		based access	
19	Назовите технологию, обеспечивающую безопасную передачу данных между агентами.	Шифрование / TLS / Secure messaging	ПК-2
20	Назовите систему, централизованно управляющую жизненным циклом агентов.	Платформа оркестрации агентов / Agent orchestration platform	ПК-2