

---

**УТВЕРЖДЕНА**

Решением Ученого совета  
АНО ВО «Центральный университет»  
«25» мая 2026 г.  
Протокол № 2

**Рабочая программа дисциплины (модуля)  
«Разработка интеллектуальных агентов»**

**Направление подготовки:** 02.04.01 Математика и компьютерные науки

**Направленность (профиль) подготовки:** Прикладное машинное  
обучение и интеллектуальные системы

**Квалификация (степень) выпускника:** магистр

**Форма обучения:** очная

**Срок освоения программы:** 2 года

**Год набора:** 2026

**Москва  
2026**

## 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 – магистратура по направлению 02.04.01 Математика и компьютерные науки, профиль Прикладное машинное обучение и интеллектуальные системы, утвержденный приказом Министерства науки и высшего образования Российской Федерации № 810 от 23.08.2017 года.

Изучение дисциплины (модуля) «Разработка интеллектуальных агентов» позволяет сформировать у студентов практические компетенции для проектирования, разработки и внедрения автономных интеллектуальных агентов, способных к долгосрочному взаимодействию с пользователем и внешними системами, а также обеспечивать их устойчивость, безопасность и соответствие бизнес-целям в реальных условиях эксплуатации.

### **Место дисциплины (модуля) в структуре образовательной программы**

Настоящая дисциплина (модуль) включена в учебный план по программе подготовки магистратуры по направлению 02.04.01 Математика и компьютерные науки, профиль Прикладное машинное обучение и интеллектуальные системы и входит в обязательную часть Блока 1.

Дисциплина (модуль) доступна к изучению на 2 курсе в 3 семестре.

**Цель изучения дисциплины (модуля):** подготовить специалистов к созданию современных агентных систем на основе больших языковых моделей, обладающих памятью, способностью к планированию, интеграцией с внешними сервисами и контролем поведения.

### **Задачи изучения дисциплины (модуля):**

- освоить архитектуры интеллектуальных агентов с поддержкой памяти и внешних инструментов;
- научиться разрабатывать и разворачивать MCP-серверы для подключения внешних инструментов;
- приобрести навыки тестирования агентов и выявления нецелевого или опасного поведения;
- освоить технологии сборки, деплоя и оркестрации агентных приложений;
- развить умение балансировать между автономностью агента и необходимостью контроля и безопасности.

### **В результате освоения дисциплины (модуля) обучающийся должен:**

#### **знать:**

- принципы работы больших языковых моделей, архитектуру трансформеров и подходы к их адаптации (дообучение (fine-tuning), генерация ответа пользователю с учетом дополнительно найденной релевантной информации (RAG), обучение с подкреплением на основе человеческого фидбека (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)                                                                                                                                                                      |
|-------------|----------------------------------------------------------------------------------------------------------------------------------|-----------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| ОПК-3.      | Способен находить, формулировать и решать актуальные и значимые проблемы прикладной и компьютерной математики                    | ОПК-3.1.              | 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-3.2.              | 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-3.3.              | 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-6.       | Способен разрабатывать программное обеспечение для решения прикладных задач в сфере машинного обучения и интеллектуальных систем | ПК-6.1.               | Знает основные языки программирования, методы разработки программного обеспечения, а также принципы проектирования и архитектуры программных систем, применяемых в машинном обучении и интеллектуальных системах                      |
|             |                                                                                                                                  | ПК-6.2.               | Умеет анализировать прикладные задачи, разрабатывать алгоритмы и реализовывать их в виде программного обеспечения, используя современные инструменты и технологии, а также проводить тестирование и отладку созданных решений         |

|  |  |         |                                                                                                                                                                                                                                |
|--|--|---------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|  |  | ПК-6.3. | Имеет практический опыт разработки программного обеспечения в рамках реальных проектов, включая участие в командах, где были успешно реализованы решения для конкретных прикладных задач в сфере профессиональной деятельности |
|--|--|---------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|

### 3. Тематический план

| №<br>п/п                               | Наименование<br>раздела дисциплины<br>(модуля)        | Трудоемкость, академические часы |                                           |          |                               | ТКУ<br>(текущий<br>контроль<br>успеваемости) |
|----------------------------------------|-------------------------------------------------------|----------------------------------|-------------------------------------------|----------|-------------------------------|----------------------------------------------|
|                                        |                                                       | Очная форма                      |                                           |          |                               |                                              |
|                                        |                                                       | Аудиторная работа                |                                           | Контроль | Самостояте<br>льная<br>работа |                                              |
|                                        |                                                       | Лекции                           | Семинары<br>(практичес<br>кие<br>занятия) |          |                               |                                              |
| 1                                      | Основные принципы LLM приложений                      | 10                               | 10                                        |          | 42                            | Домашние задания                             |
| 2                                      | Основные принципы построения интеллектуальных агентов | 10                               | 10                                        |          | 42                            | Домашние задания                             |
| 3                                      | Архитектура и проектирование агентских приложений     | 10                               | 10                                        |          | 42                            | Домашние задания                             |
|                                        | Зачет 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                      | Адаптация больших языковых моделей под целевые задачи<br>Обучение с подкреплением на основе человеческого фидбека<br>Подготовка модели к эксплуатации<br>Генерация ответа пользователю с учетом дополнительно найденной релевантной информации (Retrieval Augmented Generation, RAG) |
| 2    | Основные принципы построения интеллектуальных агентов | Агенты<br>Мультиагентные системы<br>Мультимодальные агентные системы<br>Самоадаптирующиеся и саморазвивающиеся агентные системы<br>Оценка качества агентных систем                                                                                                                   |
| 3    | Архитектура и проектирование агентских приложений     | Агентные системы без программирования и с минимальным программированием<br>Безопасность агентных систем<br>Надежность и управляемость агентных систем<br>Проектирование и деплой агентных систем<br>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<br>(издания, курса, документа)                            | Ссылка                                                                          |
|----|--------------------------------------------------------------------------------|---------------------------------------------------------------------------------|
| 1. | Научная электронная библиотека elibrary.ru библиотека                          | <a href="https://elibrary.ru/defaultx.asp">https://elibrary.ru/defaultx.asp</a> |
| 2. | База данных для IT-специалистов                                                | <a href="https://habr.com">https://habr.com</a>                                 |
| 3. | База данных ScienceDirect                                                      | <a href="https://www.sciencedirect.com">https://www.sciencedirect.com</a>       |
| 4. | Официальный сайт Министерства науки и высшего образования Российской Федерации | <a href="https://minobrnauki.gov.ru/">https://minobrnauki.gov.ru/</a>           |
| 5. | Федеральный портал «Российское образование»                                    | <a href="https://www.edu.ru/">https://www.edu.ru/</a>                           |
| 6. | Информационная система «Единое окно доступа к образовательным ресурсам»        | <a href="http://window.edu.ru/">http://window.edu.ru/</a>                       |
| 7. | Единая коллекция цифровых образовательных ресурсов                             | <a href="http://school-collection.edu.ru/">http://school-collection.edu.ru/</a> |
| 8. | Федеральный центр информационно - образовательных ресурсов                     | <a href="http://fcior.edu.ru/">http://fcior.edu.ru/</a>                         |

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 |
|------------------------------------------------------------------|---------------|------------------------------------------|
| <b>Операционные системы:</b>                                     |               |                                          |
| Microsoft Imagine (Windows Client, Server)                       | зарубежное    | лицензионное                             |
| <b>Браузеры:</b>                                                 |               |                                          |
| Яндекс.Браузер                                                   | отечественное | свободно распространяемое                |
| Google Chrome                                                    | зарубежное    | свободно распространяемое                |
| <b>Офисные приложения:</b>                                       |               |                                          |
| Microsoft Imagine (Visio, OneNote)                               | зарубежное    | лицензионное                             |
| TeXstudio                                                        | зарубежное    | свободно распространяемое                |
| Adobe Acrobat Reader                                             | зарубежное    | свободно распространяемое                |
| <b>Программное обеспечение для планирования и учета времени:</b> |               |                                          |
| Toggle app                                                       | зарубежное    | свободно распространяемое                |
| <b>Системы управления проектами:</b>                             |               |                                          |

|                                                                     |               |                           |
|---------------------------------------------------------------------|---------------|---------------------------|
| Microsoft Imagine (Project)                                         | зарубежное    | лицензионное              |
| <b>Системы управления базами данных:</b>                            |               |                           |
| Microsoft Imagine (SQL Server)                                      | зарубежное    | лицензионное              |
| <b>Системы резервного копирования (backup):</b>                     |               |                           |
| Acronis Backup Advanced for HyperV                                  | зарубежное    | лицензионное              |
| <b>Справочно-правовые системы:</b>                                  |               |                           |
| КонсультантПлюс: справочно-правовая система                         | отечественное | лицензионное              |
| <b>Средства антивирусной защиты:</b>                                |               |                           |
| Kaspersky Endpoint Security для бизнеса Стандартный Russian Edition | отечественное | лицензионное              |
| <b>Среды разработки:</b>                                            |               |                           |
| 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 |
| <b>Пакеты программных средств и библиотек:</b>                      |               |                           |
| AutoPsy                                                             | зарубежное    | свободно распространяемое |
| Interactive Disassembler (IDA)                                      | зарубежное    | свободно распространяемое |
| <b>Системы управления библиографической информацией:</b>            |               |                           |
| Zotero                                                              | зарубежное    | свободно распространяемое |
| <b>Сервисы и службы:</b>                                            |               |                           |
| 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 удастся, 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 *зачета 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. |
| 9                     | Отлично             |                                                                                                                                                                                                                     |
| 8                     | Отлично             |                                                                                                                                                                                                                     |

| Десятибалльная оценка | Пятибалльная оценка | Общая характеристика результата обучения по дисциплине (модулю)                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
|-----------------------|---------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|                       |                     | 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.                                                                                                                                                                                                                          |
| 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 деятельности, и умеет связывать теоретические аспекты предмета с практическими задачами. |
| 6                     | Хорошо              |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
| 5                     | Удовлетворительно   | Студент обладает базовыми знаниями по дисциплине, 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.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |

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

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

**Формула расчёта итоговой оценки по дисциплине (модулю) «Разработка интеллектуальных агентов»:**  $0,7 \times \text{Среднее за домашние задания} + 0,3 \times \text{Зачет с оценкой}$ .

Электронный документ

## Текущий контроль успеваемости обучающихся по дисциплине (модулю)

### Примерные домашние задания

#### Домашнее задание 1. Настройка RAG-системы для агента поддержки

1. Разработайте RAG-систему для агента технической поддержки.
2. Подготовьте векторное хранилище (например, с помощью FAISS или Chroma) на основе документации (предоставленный набор .pdf или .txt).
3. Настройте модель (например, Llama 3 или Mistral через Ollama) для генерации ответов с подтягиванием релевантной информации.
4. Реализуйте цепочку:  
Поиск по запросу пользователя → Извлечение релевантных фрагментов → Генерация ответа с контекстом
5. Протестируйте на 5 тестовых вопросах.

##### Требования:

- код на Python (с использованием LangChain или LlamaIndex);
- описание архитектуры;
- примеры запросов и ответов.

#### Домашнее задание 2. Разработка агента с памятью и инструментами (MCP)

1. Создайте агента, который может:
  - вести диалог с памятью (краткосрочной и долгосрочной);
  - выполнять действия через внешние инструменты (например, поиск в интернете, отправка email, запрос погоды).
2. Реализуйте MCP-сервер (Model Context Protocol) для подключения одного из инструментов.
3. Интегрируйте агента с LLM (например, через OpenAI API или локальную модель).
4. Продемонстрируйте сценарий: пользователь просит "напомнить завтра о встрече в 15:00 и отправить приглашение коллеге".

##### Требования:

- MCP-сервер на FastAPI/Flask;
- работающий агент с демонстрацией сценария;
- описание схемы взаимодействия.

#### Домашнее задание 3. Оценка и тестирование поведения агента

1. Возьмите готового агента (своего или предложенного преподавателем).
2. Разработайте набор тестовых сценариев:
  - корректное поведение;
  - попытка обхода безопасности;
  - работа с противоречивыми инструкциями.
3. Выявите случаи нецелевого поведения (hallucinations, игнорирование ограничений, избыточная автономность).
4. Предложите меры по улучшению:
  - промпт-инжиниринг;
  - добавление контрольных узлов;
  - ограничение доступа к инструментам.

5. Оформите отчёт с рекомендациями.

**Требования:**

- тест-кейсы и результаты;
- анализ уязвимостей;
- предложения по улучшению безопасности и управляемости.

**Примерное описание задания и критерии оценивания к проекту**

**Описание задания:**

Разработать и развернуть мультиагентную систему, решающую конкретную бизнес-задачу (например: подбор кандидатов, планирование мероприятий, обработка запросов клиентов). Система должна включать нескольких взаимодействующих агентов, использовать внешние инструменты, обладать памятью и механизмами контроля.

**Этапы выполнения:**

**1. Формулировка задачи и проектирование архитектуры.**

- определить сценарий использования;
- спроектировать роли агентов (менеджер, исполнитель, контролёр и др.);
- описать взаимодействие между агентами и внешними сервисами.

**2. Реализация агентов.**

- настроить память (векторная БД + краткосрочная память);
- подключить инструменты через MCP или API;
- реализовать логику принятия решений.

**3. Интеграция и оркестрация.**

- настроить взаимодействие между агентами;
- реализовать механизм координации (например, через LangGraph или собственный оркестратор).

**4. Тестирование и оценка.**

- проверить корректность работы на сценариях;
- оценить качество, безопасность, устойчивость;
- выявить и устранить нецелевое поведение.

**5. Деплой и документация.**

- собрать приложение (Docker, FastAPI, веб-интерфейс);
- подготовить инструкцию по запуску и использованию;
- презентовать результат.

**Критерии оценивания:**

1. Архитектурное решение — логичность, масштабируемость, баланс автономности и контроля.

2. Реализация функциональности — работоспособность агентов, память, интеграция с инструментами.

3. Качество взаимодействия — корректность ответов, отсутствие hallucinations, эффективность оркестрации.

4. Безопасность и надёжность — наличие контроля, защита от нецелевого поведения.

5. Деплой и документация — готовность к использованию, ясность инструкций, качество презентации.

### Задания для промежуточной аттестации по дисциплине (модулю)

| № п/п | Задание                                                        | Ответ                                         | Компетенция |
|-------|----------------------------------------------------------------|-----------------------------------------------|-------------|
| 1.    | Какова основная цель RLHF в обучении моделей?                  | Выравнивание модели с предпочтениями человека | ОПК-3       |
| 2.    | Как записывается функция потерь для ранжирования предпочтений? | $L = \log \text{sigmoid}(r_w - r_l)$          | ОПК-3       |
| 3.    | Какой компонент архитектуры RAG отвечает за поиск?             | Векторная база данных                         | ПК-6        |
| 4.    | Какая метрика оценивает качество retrieval в RAG?              | Recall@K или MRR                              | ПК-6        |
| 5.    | Что определяет интеллектуального агента в системе?             | Способность восприятия и действия             | ОПК-3       |
| 6.    | Какой протокол часто используется для общения агентов?         | JSON-RPC или gRPC                             | ПК-6        |
| 7.    | Какой риск безопасности критичен для агентных систем?          | Выполнение вредоносного кода                  | ПК-6        |
| 8.    | Что такое галлюцинация в контексте LLM?                        | Генерация фактологически неверного текста     | ОПК-3       |
| 9.    | Какой метод снижает вероятность галлюцинаций?                  | Grounding через внешние данные                | ПК-6        |
| 10.   | В чем суть паттерна Chain of Thought?                          | Пошаговое рассуждение перед ответом           | ОПК-3       |
| 11.   | Как записывается формула механизма Attention?                  | $\text{Softmax}(\frac{QK^T}{\sqrt{d}})V$      | ОПК-3       |
| 12.   | Что контролирует параметр Temperature при генерации?           | Случайность выбора токенов                    | ПК-6        |
| 13.   | Какая метрика измеряет успешность выполнения задачи агентом?   | Task Success Rate                             | ОПК-3       |
| 14.   | Какой фреймворк используется для оркестрации агентов?          | LangGraph или AutoGen                         | ПК-6        |
| 15.   | Что означает аббревиатура паттерна ReAct?                      | Reasoning and Acting                          | ОПК-3       |
| 16.   | Как защитить API агента от злоупотреблений?                    | Rate Limiting и авторизация                   | ПК-6        |
| 17.   | Что ограничивает контекстное окно модели?                      | Максимальное количество токенов               | ОПК-3       |
| 18.   | Какая стратегия работает с текстом длиннее контекста?          | RAG или Map-Reduce                            | ПК-6        |
| 19.   | В чем разница между Fine-tuning и Prompting?                   | Изменение весов против контекста              | ОПК-3       |
| 20.   | Как оптимизировать затраты на inference модели?                | Квантование или дистилляция                   | ПК-6        |

