Бауманский учебный центр «Специалист»

Программа курса Разработка ИИ - агентов на Python: RAG, MCP и безопасная интеграция

Код курса: **ИИАГ**

Тема	Ак. часов
Модуль 1. Архитектура и жизненный цикл агента • Чатбот, RAG-ответ и агент; агентный цикл; tool calling / function calling; среда Python и API модели с tools; границы решений агента. **Практика:** агент с одним инструментом.	**4**
Модуль 2. MCP и инструменты • Инструмент как контракт; свои функции (HTTP, SQL, файлы); MCP: клиент и сервер; подключение к агенту; allowlist, секреты, подтверждение опасных вызовов. **Практики:** агент с 2-3 функциями; MCP-сервер и вызов из агента.	**8**
Модуль 3. RAG и PostgreSQL/pgvector • Когда нужен поиск по документам; эмбеддинги, чанкинг, сходство; корпус в pgvector; источники; поиск как tool; ответ со ссылками. **Практики:** загрузка корпуса; агент выбирает искать или ответить без поиска.	**8**
Модуль 4. Маршрутизация, память и программные ограничения • Память диалога и scratchpad; долгосрочный контекст vs поиск; маршруты искать / tool / человек / отказ; многошаговые задачи; human-in-the-loop; лимиты. **Практики:** агент с памятью; маршрут «найти > tool > подтверждение».	**8**
Модуль 5. Безопасность и оценка качества • Галлюцинации и выдуманные вызовы; неверный tool, зацикливание, обрыв контекста; набор сценариев; траектория. **Практики:** регрессионный набор; разбор провалов.	**4**
Модуль 6. Итоговый практический проект • Агент с RAG, MCP и ещё одним действием; CLI и простой API или Telegram; политика «когда не действовать»; сдача без преподавателя. **Практика:** итоговый ИИ-агент.	**8**
Аудиторная нагрузка в классе с преподавателем	**40 ак.ч. + 40 ак.ч. самостоятельно**

По окончании обучения на курсе проводится итоговая аттестация. Аттестация проводится в виде теста на последнем занятии или на основании оценок практических работ, выполняемых во время обучения на курсе.

Контакты центра

Для частных лиц
+7 (495) 232-32-16

Для организаций
+7 (495) 780-48-44

E-mail
info@specialist.ru