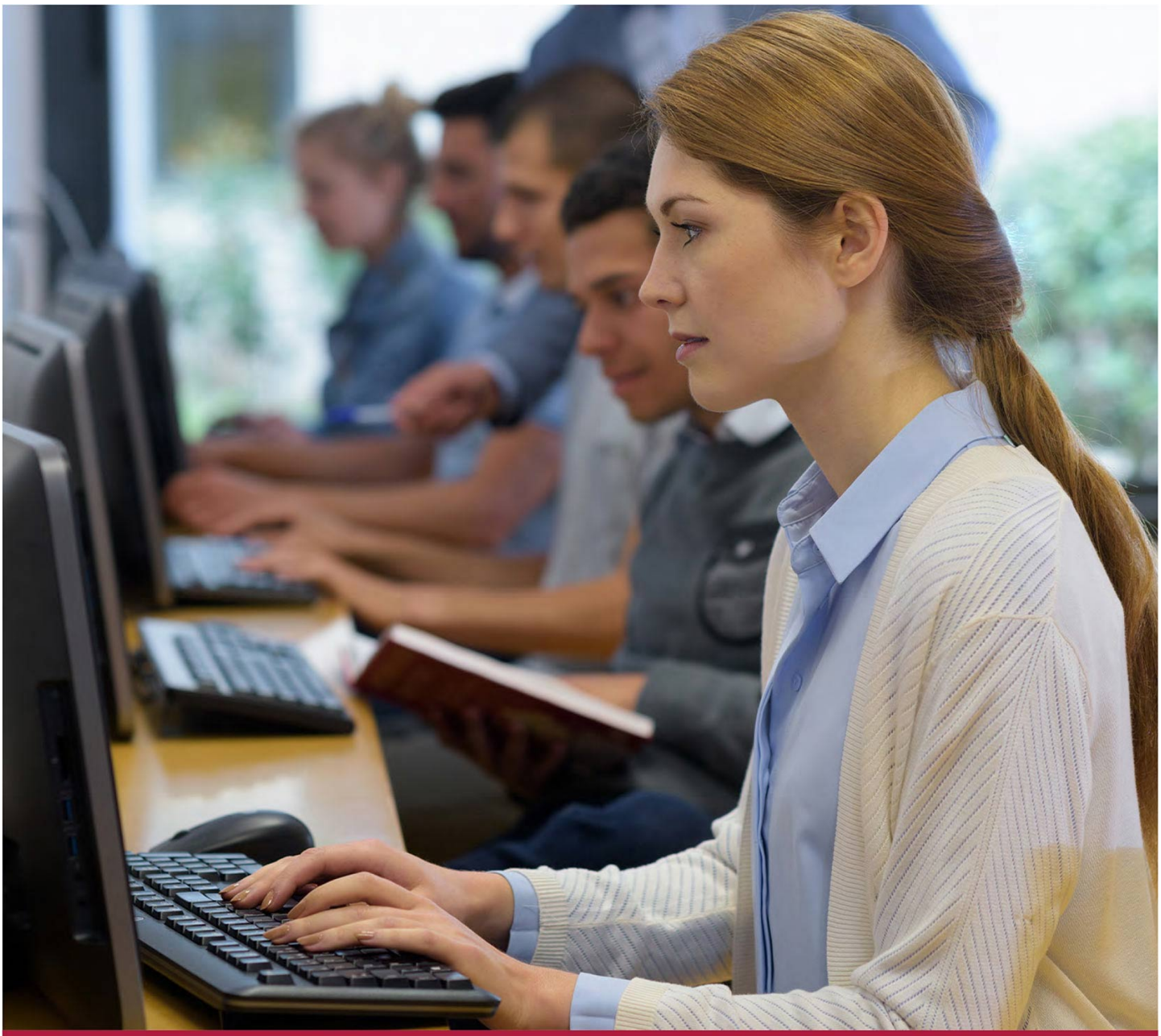
Академия АйТи
a Softline Company



Создание ИИ-агентов

Код курса: AI-AGENTS

+7 (495) 150 96 00 | academy@academyit.ru | academyit.ru

Создание ИИ-агентов

Код курса: AI-AGENTS

Длительность	32 ак. часа
Формат	
Разработчик курса	Академия АйТи
Тип	Учебный курс
Способ обучения	Под руководством тренера

О курсе

Курс посвящён практической разработке прикладных ИИ-агентов для бизнес-сценариев. Слушатели поэтапно собирают корпоративный AI-agent сервис: от базовой архитектуры и API-взаимодействия до tool calling, памяти диалога, RAG по внутренним документам, интеграции во внешний контур, guardrails и подготовки к пилотному запуску. В основе курса лежит сквозной проект - корпоративный AI-ассистент для внутренней базы знаний компании.

Подробная информация

Профиль аудитории:

- Python/backend-разработчики
- AI/ML engineers
- solution architects и технические лиды
- специалисты по автоматизации и внутренним цифровым сервисам

Предварительные требования:

- уверенное владение Python
- базовое понимание REST API, JSON и HTTP
- общее понимание принципов работы LLM
- желателен опыт работы с Git, Docker и веб-сервисами

По окончании курса слушатели смогут:

- проектировать архитектуру прикладного ИИ-агента под конкретный бизнес-сценарий
- разрабатывать single-agent сервис с API-слоем, orchestrator и управлением сессиями
- подключать инструменты и внешние API через tool calling и маршрутизацию запросов
- реализовывать память диалога, ограничение истории и многопользовательский контекст
- строить RAG-пайплайн по корпоративным документам с векторным поиском
- внедрять базовые guardrails, фильтрацию опасных запросов и контроль рискованных действий
- подготавливать агентный сервис к пилоту: конфигурация, логирование, контейнеризация, readiness check

Программа курса

Модуль 1. Архитектура прикладного ИИ-агента

- Объём: 4 академических часа
- Что входит:
- Чем прикладной AI-agent отличается от обычного LLM-чата.
- Типовая схема сервиса: клиент -> API -> orchestrator -> LLM / tools / RAG / memory.
- Основные компоненты: модель, инструменты, память, retrieval, защитный слой, логирование.
- Когда достаточно одного агента, а когда нужны workflow и распределение ролей.
- Практика:
- Создание структуры проекта AI-агента на Python.
- Настройка конфигурации и переменных окружения.
- Реализация простого endpoint для общения с LLM через FastAPI.
- Результат модуля:
- Базовый сервис агента с API и понятной архитектурой.

Модуль 2. Оркестрация запросов и tool calling

- Объём: 4 академических часа
- Что входит:
- Как понять, отвечать моделью, вызывать инструмент или идти в RAG.
- Tool calling: формат аргументов, обработка результата и возврат ответа пользователю.
- Маршрутизация запросов внутри orchestrator.
- Типовые ошибки инструмента и безопасная деградация сценария.
- Практика:
- Подключение инструментов: калькулятор, погодный API, внутренняя Python-функция.
- Реализация маршрутизатора внутри orchestrator.
- Сборка единого ответа агента на основе результата инструмента.
- Результат модуля:
- Агент, который умеет вызывать внешние инструменты и корректно обрабатывать их ответы.

Модуль 3. Память и управление контекстом диалога

- Объём: 4 академических часа
- Что входит:
- Краткосрочная память и история сообщений.
- Ограничение длины истории, очистка контекста и сжатие длинного диалога.
- Session_id, user_id и client_id как основа многопользовательской архитектуры.
- Ограничения контекста и влияние истории на стоимость запросов.
- Практика:
- Реализация хранилища истории диалога.
- Ограничение числа сообщений и логика очистки.
- Поддержка нескольких пользователей и сессий.
- Результат модуля:
- Агент с управляемой памятью, пригодный для многопользовательского использования.

Модуль 4. RAG для корпоративных документов

- Объём: 4 академических часа
- Что входит:
- Когда нужен RAG, а когда достаточно prompt + tools.
- Embeddings и векторный поиск в прикладной задаче.
- Chunking документов и загрузка PDF, DOCX, HTML, CSV.
- Retrieval pipeline: ingestion -> embedding -> index -> search -> answer.
- Практика:
- Загрузка набора документов и построение векторного индекса.
- Интеграция retrieval в orchestrator.
- Сравнение ответа без RAG и с RAG.
- Результат модуля:
- Агент, который отвечает по внутренним документам компании.

Модуль 5. Интеграция агента в прикладной сервис

- Объём: 4 академических часа
- Что входит:
- API-контракт агента и внешняя точка входа.
- Подключение web-интерфейса, внутреннего портала или сервисного слоя.
- Интеграция с внешними бизнес-системами через API.
- Логирование запросов, ошибок и использования инструментов.
- Практика:
- Создание REST endpoint /chat и endpoint для сброса сессии.
- Подключение простого web UI.
- Добавление логирования обращений и технических ошибок.
- Результат модуля:
- Интегрируемый сервис агента с внешней точкой входа и логами.

Модуль 6. Безопасность и контроль работы агента

- Объём: 4 академических часа
- Что входит:
- Какие пользовательские запросы и ответы нужно блокировать или проверять.
- Prompt injection, indirect prompt injection и рискованные сценарии.
- Валидация входных данных и ответов агента.
- Guardrails и разграничение доступа к данным и инструментам.
- Практика:
- Внедрение фильтра опасных инструкций.
- Ограничение вызова отдельных инструментов.
- Тестирование атакующих сценариев.
- Результат модуля:
- Агент с базовым защитным слоем и контролем рискованных действий.

Модуль 7. Подготовка AI-agent сервиса к пилоту

- Объём: 4 академических часа
- Что входит:
- Конфигурация среды: env-переменные, модели, ключи, переключение окружений.
- Контейнеризация сервиса и базовая схема запуска.

- Health check, readiness check и минимальные критерии готовности.
- Чек-лист пилотного запуска: логирование, ограничения, fallback-сценарии, демонстрационный контур.
- Практика:
- Подготовка конфигурации dev / test / pilot.
- Сборка контейнера и базовый запуск сервиса.
- Формирование короткого readiness checklist для пилота.
- Результат модуля:
- Сервис агента, подготовленный к технической демонстрации и пилотному запуску.

Модуль 8. Итоговый проект

- Объём: 4 академических часа
- Что входит:
- Архитектура корпоративного AI-ассистента end-to-end.
- Минимум два инструмента, память диалога, RAG по внутренним документам и guardrails.
- Подготовка демонстрации и защиты решения.
- Критерии качества итогового сервиса.
- Практика:
- Демонстрация архитектуры и API.
- Показ tool calling.
- Показ RAG по документам.
- Показ обработки небезопасного сценария.
- Результат модуля:
- Корпоративный AI-ассистент end-to-end, пригодный для демонстрации заказчику и обсуждения пилота.

Посмотреть расписание курса и записаться на обучение

Обращайтесь по любым вопросам
к менеджерам Академии АйТи

+7 (495) 150 96 00 | academy@academyit.ru