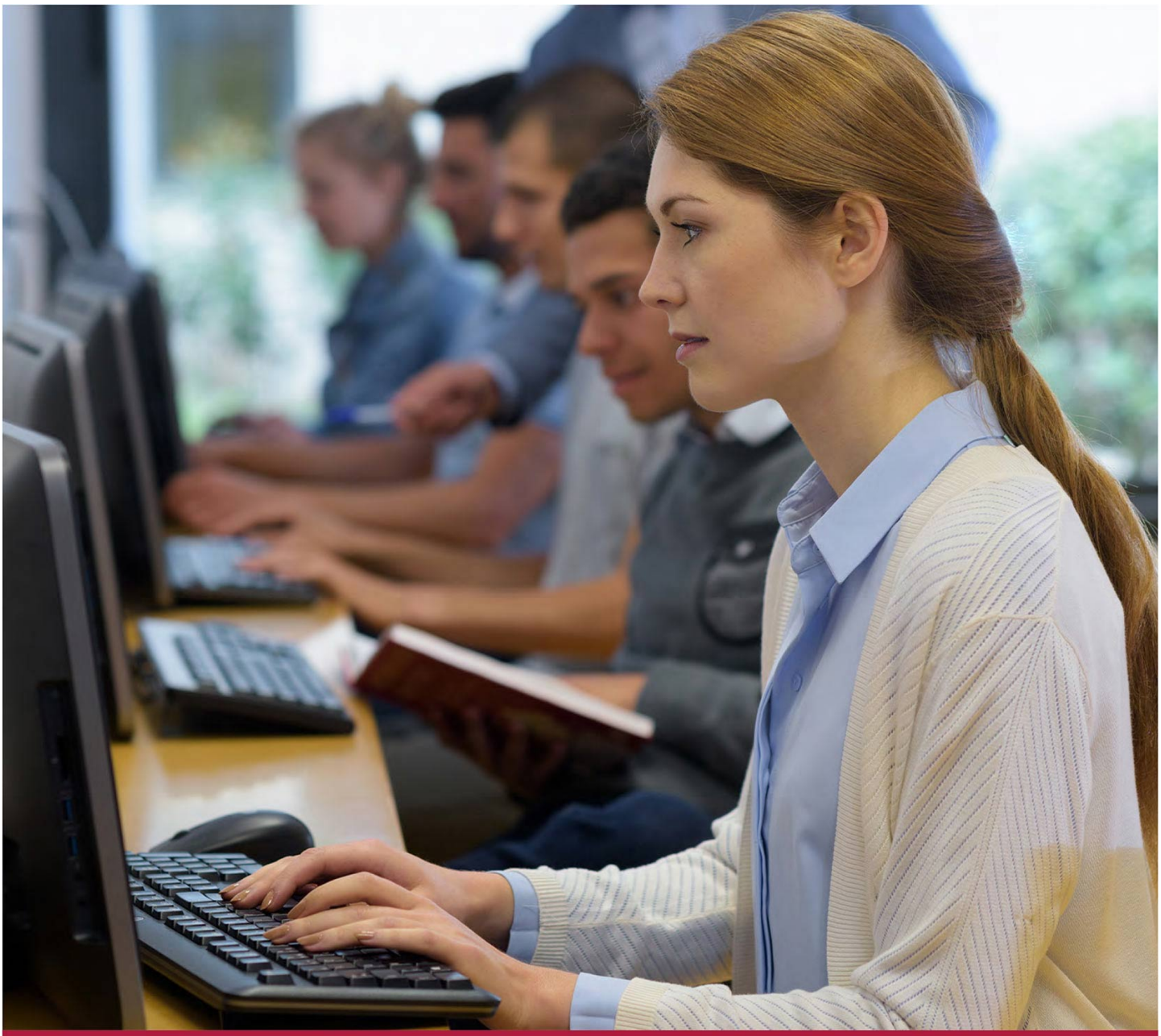
Академия АйТи
a Softline Company



Безопасная и отказоустойчивая архитектура автономных ИИ агентов и систем

Код курса: AI_A

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

Безопасная и отказоустойчивая архитектура автономных ИИ агентов и систем

Код курса: AI_A

Длительность	48 ак. часов
Формат	
Разработчик курса	Академия АйТи
Тип	Учебный курс
Способ обучения	Под руководством тренера

О курсе

Стабильная архитектура ИИ-агентов и систем является одним из фундаментальных вопросов использования этих технологий, потому что такие системы всё чаще принимают решения без прямого участия человека в условиях высокой неопределённости и динамически меняющейся среды. В критически важных областях — от медицины и энергетики до транспорта и обороны — любая ошибка, сбой или непредвиденное поведение ИИ может привести к тяжёлым последствиям, включая угрозу жизни и масштабный экономический ущерб. Отказоустойчивость обеспечивает продолжение корректной работы даже при частичном выходе из строя компонентов, а встроенные механизмы безопасности предотвращают опасные или непредсказуемые действия агента. Это особенно актуально в свете роста сложности ИИ-систем и их интеграции в реальный мир, где невозможно предусмотреть все сценарии заранее. Доверие к автономным системам напрямую зависит от уверенности в их надёжности и предсказуемости, что делает безопасную архитектуру не просто технической деталью, а фундаментальным требованием. Программа охватывает все этапы: от проектирования и разработки до эксплуатации, мониторинга и аудита автономных ИИ-систем, что обеспечивает системное понимание безопасности и отказоустойчивости. Программа специализируется на наиболее сложном и перспективном классе систем — автономных агентах, где риски и требования к надёжности максимальны. Это системы вроде дронов или элементов IIoT, количество и сложность которых стремительно растут.

Подробная информация

Профиль аудитории:

- сотрудники и профильные специалисты организаций в критических отраслях
- аналитики и data-steward’ы
- ИБ-специалисты, обеспечивающие отказоустойчивость инфраструктуры организации

Предварительные требования:

- Навыки работы на компьютере на уровне опытного пользователя
- Понимание принципов отказоустойчивости и безопасного жизненного цикла решений
- Базовые навыки работы с нейронными сетями
- Понимание архитектуры ИИ-агентов и систем

- Базовое понимание принципов Data-Governance

По окончании курса слушатели изучат:

- Жизненный цикл автономных ИИ-агентов и систем
- Метрики контроля и мониторинга безопасности и доверия к ИИ-системам
- Процесс вывода решений в реализацию и обеспечение отказоустойчивости в активной фазе развития и использования
- Передовые технологии и инструменты по разработке безопасных ИИ-систем
- Аудит и контроль состояния и защищенности ИИ-агентов и систем

Программа курса

Модуль 1. Современные вызовы и тренды в области автономных ИИ-систем: от концепции агента до реальных применений

Модуль 2. Стратегия и архитектурные принципы проектирования безопасных ИИ-агентов

Модуль 3. Планирование автономных ИИ-систем: цели, ограничения, этические и регуляторные рамки

Модуль 4. Безопасное моделирование поведения и принятия решений автономными ИИ-агентами

Модуль 5. Управление данными и метаданными в контексте автономных ИИ-систем

Модуль 6. Жизненный цикл автономной ИИ-системы: от разработки до вывода из эксплуатации

Модуль 7. Обеспечение безопасности ИИ: защита от атак, манипуляций и непреднамеренных последствий

Модуль 8. Взаимодействие автономных ИИ-агентов с людьми и бизнес-процессами: интерфейсы, доверие, контроль

Модуль 9. MLSecOps для автономных систем: интеграция безопасности в CI/CD и MLOps-конвейеры

Модуль 10. Обеспечение отказоустойчивости, надёжности и устойчивости автономных ИИ-систем в production

Модуль 11. Инструменты, технологии и стандарты для разработки и мониторинга безопасных ИИ-агентов

Модуль 12. Аудит, сертификация и непрерывное управление безопасностью автономных ИИ-систем

Посмотреть расписание курса и записаться на обучение

Обращайтесь по любым вопросам
к менеджерам Академии АйТи

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