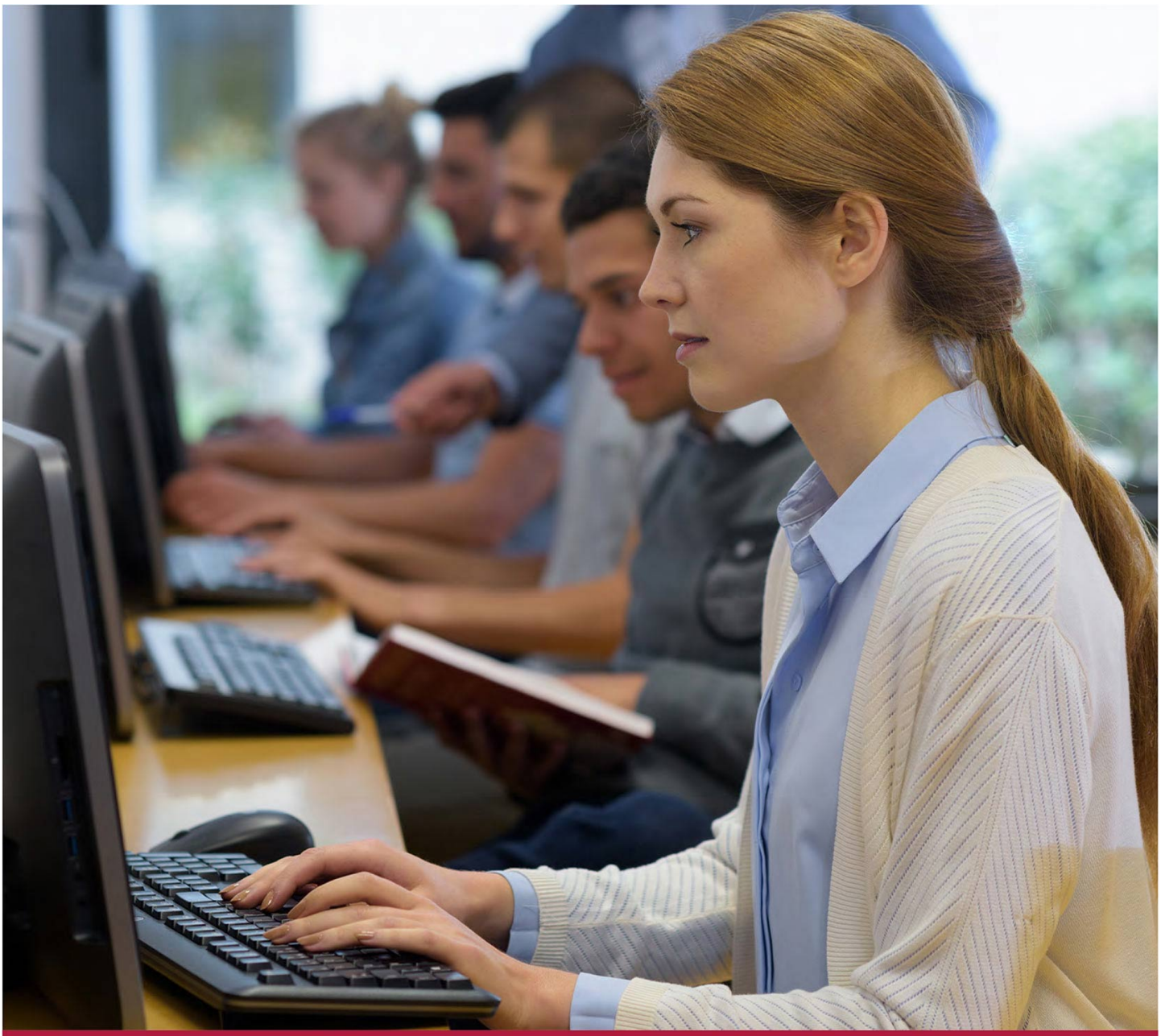
Академия АйТи
a Softline Company



AI Governance в критических отраслях: от рисков и угроз к этике и доверию

Код курса: AI_G

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

AI Governance в критических отраслях: от рисков и угроз к этике и доверию

Код курса: AI_G

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

О курсе

Вопрос построения системы и обеспечения AI Governance (управления искусственным интеллектом) в критических отраслях и его безопасности является чрезвычайно важным и востребованным по нескольким ключевым причинам, обусловленным как технологическими, так и социальными, экономическими и правовыми аспектами. Многие современные ИИ-модели, особенно глубокие нейросети, работают как «чёрные ящики» — их решения трудно интерпретировать. В критических отраслях это неприемлемо: участники процессов должны четко понимать, почему ИИ принял то или иное решение, и отсутствие объяснимости затрудняет аудит, ответственность и доверие. Программа ориентирована на техническую, прикладную часть и делает сильный акцент на информационную безопасность при работе с ИИ-системами. Программа ориентирована на оценку рисков, этику, юридическую и отраслевую специфику применения искусственного интеллекта, поэтому будет обладать высокой устойчивостью к изменениям рынка и соответствовать глобальному тренду «secure, trustworthy, compliant AI».

Подробная информация

Профиль аудитории:

- сотрудники и профильные специалисты организаций в критических отраслях
- аналитики и data-steward’ы
- руководители организаций, выстраивающие стратегию управления AI-технологий

Предварительные требования:

- Навыки работы на компьютере на уровне опытного пользователя
- Базовые навыки работы с нейронными сетями
- Базовое понимание принципов Data-Governance

По окончании курса слушатели изучат:

- Основные принципы стабильного и устойчивого функционирования парадигмы AI-Governance
- Тенденции и тренды в регулировании применении ИИ в критических отраслях (российский и международный опыт)

- Процесс подготовки предложений в плановые, нормативные и другие документы по обеспечению безопасности искусственного интеллекта в организации
- Процесс оптимизации процессов управления данными и ИИ-технологиями: улучшать существующие процессы для повышения эффективности и снижения затрат

Программа курса

Модуль 1. Введение в AI Governance: вызовы и стандарты в критических отраслях

Модуль 2. Риски и угрозы ИИ-систем: от Data Poisoning до адверсариальных атак

Модуль 3. Этические основы и принципы ответственного ИИ (Responsible AI)

Модуль 4. Регуляторные требования и нормативное регулирование ИИ и России и других странах (EU AI Act, NIST AI RMF, ГОСТы и др.)

Модуль 5. Управление данными для ИИ: Data Governance как основа AI Governance

Модуль 6. Безопасность жизненного цикла ИИ: от разработки до эксплуатации и вывода из эксплуатации

Модуль 7. MLSecOps в критической инфраструктуре: лучшие практики защиты ИИ-систем

Модуль 8. Управление доверием к ИИ: прозрачность, объяснимость (XAI) и аудит моделей

Модуль 9. Идентификация и оценка воздействия (ущерба) рисков на права пользователей, безопасность и отказоустойчивость ИИ-систем

Модуль 10. Внедрение AI Governance в организацию: ролевые модели, процессы и KPI

Модуль 11. Инструменты и фреймворки для реализации AI Governance (включая open-source решения)

Модуль 12. Кейсы и стратегии критических отраслей: лучшие практики AI Governance в финансах, обороне, здравоохранении и госсекторе

Посмотреть расписание курса и записаться на обучение

Обращайтесь по любым вопросам
к менеджерам Академии АйТи

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