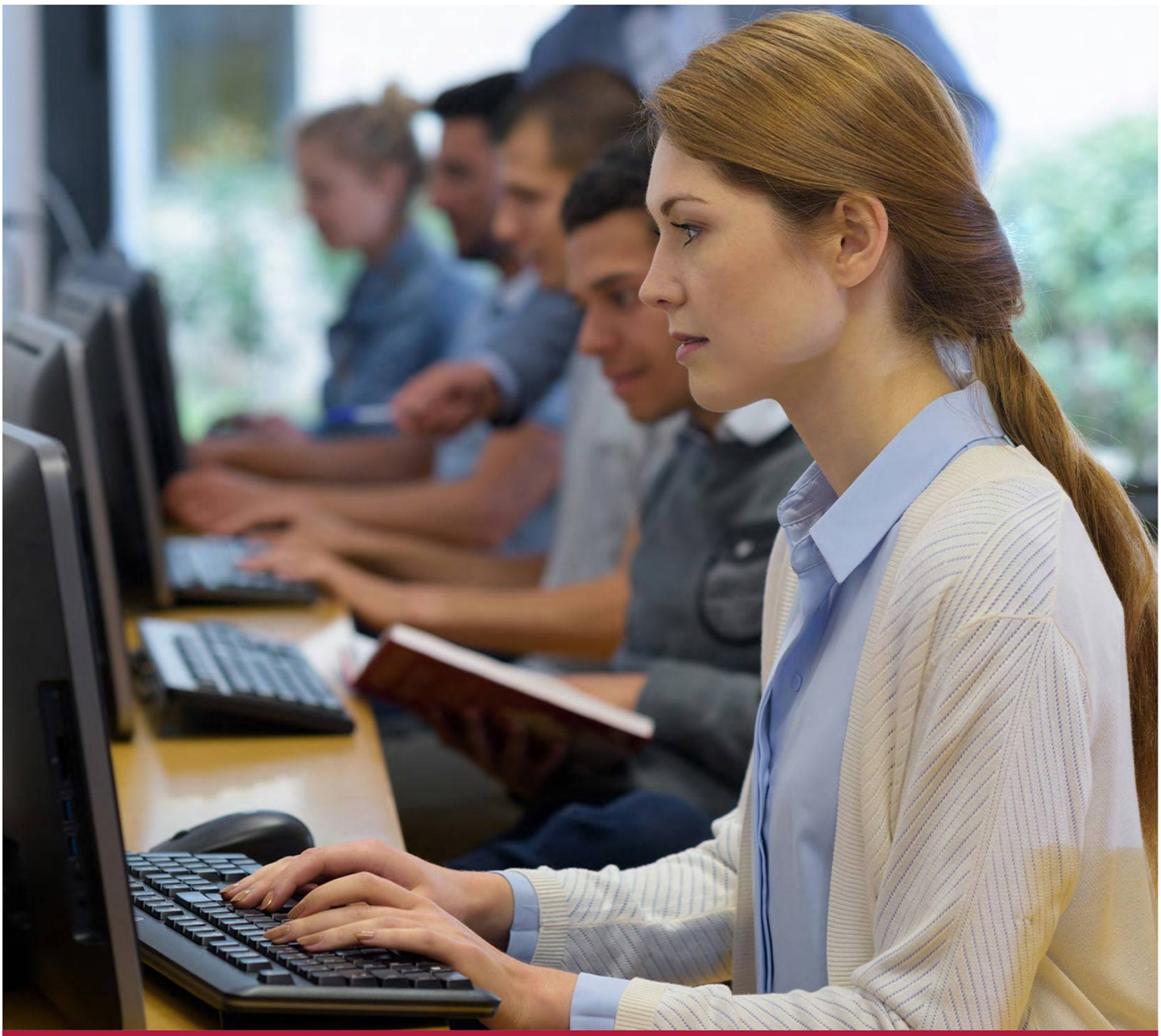
Академия АйТи
a Softline Company



Аналитик киберзащиты и безопасности ИИ-систем

Код курса: AI_CTI

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

Аналитик киберзащиты и безопасности ИИ-систем

Код курса: AI_CTI

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

О курсе

В сфере ИИ и информационной безопасности укрепляется новое направление – AI Threat Intelligence (кибербразведка для ИИ-систем). Оно находится на стыке классической кибербразведки и машинного обучения, требует комбинированных навыков как в области анализа угроз, так и понимания архитектуры нейросетей. К таким навыкам относятся: анализ специфических уязвимостей и векторов атак на модели машинного обучения, оценка тактик и техник злоумышленников и проактивное прогнозирование инцидентов. Специалисты AI Threat Intelligence защищают как сами модели искусственного интеллекта от манипуляций, так и всю инфраструктуру от атак с применением ИИ. Интерес к направлению стремительно растет, а спрос на специалистов с такими компетенциями ежегодно увеличивается многократно. Актуальность также основывается на развитии сферы искусственного интеллекта, а также внедрении регуляторных стандартов (AI Governance) и активизации злоумышленников.

Подробная информация

Профиль аудитории:
• Аналитики SOC и обнаружения киберугроз
• Специалисты информационной безопасности
• Архитекторы DevSecOps
• Руководители служб информационной безопасности
• Специалисты, использующие ИИ в своей деятельности на пользовательском уровне
Предварительные требования:
• Базовые навыки работы с нейронными сетями
• Базовые навыки обеспечения информационной безопасности в качестве пользователя (сложные пароли, антивирусная защита, блокировка экрана)
• Понимание принципов работы моделей машинного обучения
По окончании курса слушатели изучат:
• Принципы инженерии мониторинга и обнаружения угроз
• Принципы инженерии данных и специфика аналитики в области информационной безопасности
• Особенности работы с угрозами и атаками ИИ-систем
• Процесс оценивания и анализа рисков киберугроз
• Процесс выявления трендов и появление новых критических угроз и угроз уровня «zero-day»

• Координация действий команды при активных атаках
• Создание регламентов, инструкций и стандартов по информационной безопасности сотрудников

Программа курса

Модуль 1 «Фундамент киберзащиты и архитектура безопасности ИИ-систем»

- Эволюция угроз и новая парадигма безопасности: от CIA-триады к защите данных и моделей ИИ.
- Архитектура современных ИТ- и AI-инфраструктур. Уязвимости в гибридных системах.
- Правовой ландшафт и суверенитет данных. ФЗ-152, ФЗ-187, ГОСТы, ПНСТы и роль отечественных фреймворков.
- Аналитик киберзащиты ИИ-систем как ключевое звено выживания организации и профессия будущего. Проблемы, тенденции и перспективы.

Модуль 2 «Инженерия мониторинга, сетевая аналитика и обнаружение угроз»

- Архитектура и инженерия SIEM-систем. Эволюция SIEM, сбор логов, нормализация, корреляция, дашборды.
- Сетевой мониторинг и глубокий анализ трафика: протоколы, перехват, C2, эксфильтрация, шифрованный трафик.
- Системы обнаружения и предотвращения вторжений (IDS/IPS), сигнатурный и аномальный анализ.
- Применение ML и ИИ в мониторинге.

Модуль 3 «Инженерия данных и продвинутая аналитика для ИБ и AI-инфраструктур»

- Архитектура данных и телеметрия в ИБ и AI-системах. Форматы логов, специфика телеметрии ML-моделей.
- Инструментарий аналитика от SQL до Python. BI-инструменты. Очистка данных.
- Поведенческая аналитика и статистические методы. Базовые линии, графовая аналитика, детектирование отклонений.
- Применение машинного обучения в детектировании угроз. Алгоритмы кластеризации, изолирующие леса, NLP для анализа логов.

Модуль 4 «Расследование инцидентов и Incident Response»

- Методология расследования киберинцидентов. Фреймворки расследований (NIST SP 800-61, SANS PICERL). Сохранение цифровых доказательств (chain of custody). Форензика и ее инструменты.
- Управление инцидентами, создание, ведение и обновление IRP. Роли и ответственность в команде реагирования. Эскалация и коммуникация при инцидентах. Минимизация ущерба при инцидентах.
- Анализ вредоносного ПО. Статический и динамический анализ. Песочницы для безопасного исполнения. Индикаторы компрометации и тактики злоумышленников.

Модуль 5 «Особенности аналитики ИИ-систем»

- Этапы создания ИИ-системы.

- Аналитика обучающих данных и аналитика на всех этапах создания ИИ-системы.
- Детектирование отравления данных, защита от отравления.
- Мониторинг дрейфа данных, телеметрия инференса ML.

Модуль 6 «MLSecOps. Обеспечение безопасности ИИ-систем»

- Специфические угрозы для ML-моделей (adversarial attacks, data poisoning)
- Базовый аудит AI-пайплайнов и MLOps-инфраструктуры
- Инциденты MLSecOps и способы защиты.
- MLSecOps-практики, инструменты и фреймворки

Модуль 7 «Разработка политик и соответствие требованиям»

- Разработка политик безопасности. Структура политик ИБ: от стратегических до операционных. Разработка регламентов доступа, парольной политики, инцидент-менеджмента
- Стандарты безопасной разработки DevSecOps. Документирование процедур и инструкций
- Compliance и регуляторные требования. Российское законодательство: ФЗ-152, ФЗ-187, приказы ФСТЭК. Международные стандарты: ISO 27001, NIST CSF, GDPR. Отраслевые требования. Взаимодействие с регуляторами и отчетность

Модуль 8 «Оценка рисков, выгод и ущербов в аналитике кибербезопасности»

- Оценка рисков в аналитике кибербезопасности и машинного обучения
- Оценка потенциального и мультипликативного ущерба
- Оценка потенциальных и мультипликативных выгод
- Навыки презентации рисков бизнесу и обоснование целесообразности предлагаемых мер

Модуль 9 «Обучение персонала и культура безопасности»

- Программы ускоренного и адаптивного обучения. Разработка учебных материалов по кибергигиене.
- Геймификация обучения безопасности. Симуляции фишинговых атак. Тестирование, измерение ROI программ обучения и оценка эффективности.
- Коммуникация и изменение поведения. Психология восприятия рисков пользователями. Техники эффективного донесения информации. Педагогический дизайн. Работа с сопротивлением изменениям.
- Построение культуры безопасности в организации

Модуль 10 «Аналитика, отчетность и тренды»

- Подготовка отчетов для стейкхолдеров. Типовые аналитические отчеты.
- Анализ трендов. Превентивный мониторинг угроз. Анализ критических угроз и zero-day уязвимостей.
- Прогнозирование векторов атак на основе трендов. Сценарное моделирование будущих угроз
- Лучшие практики и бенчмаркинг. Изучение крупных инцидентов.

Модуль 11 «Обеспечение надежности и отказоустойчивости информационных систем»

- Обеспечение высокой доступности информационных систем. Методы предотвращения

простоев в работе. Техники SRE
- Резервирование и резервное копирование данных. Защита от потери данных и сбоев системы
- Мониторинг инфраструктуры. Отслеживание состояния серверов и другого оборудования
- Планирование аварийного восстановления. Процедуры для быстрого восстановления работоспособности

Модуль 12 «Лучшие практики и итоговая аттестация»

- Полный цикл аналитики: от оценки уязвимостей до разработки политик
- Лучшие практики аналитики кибербезопасности и машинного обучения
- Карьерное развитие в аналитике. Составление портфолио проектов. Подготовка резюме. Нетворкинг в индустрии кибербезопасности. План непрерывного профессионального развития

Посмотреть расписание курса и записаться на обучение

Обращайтесь по любым вопросам
к менеджерам Академии АйТи

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