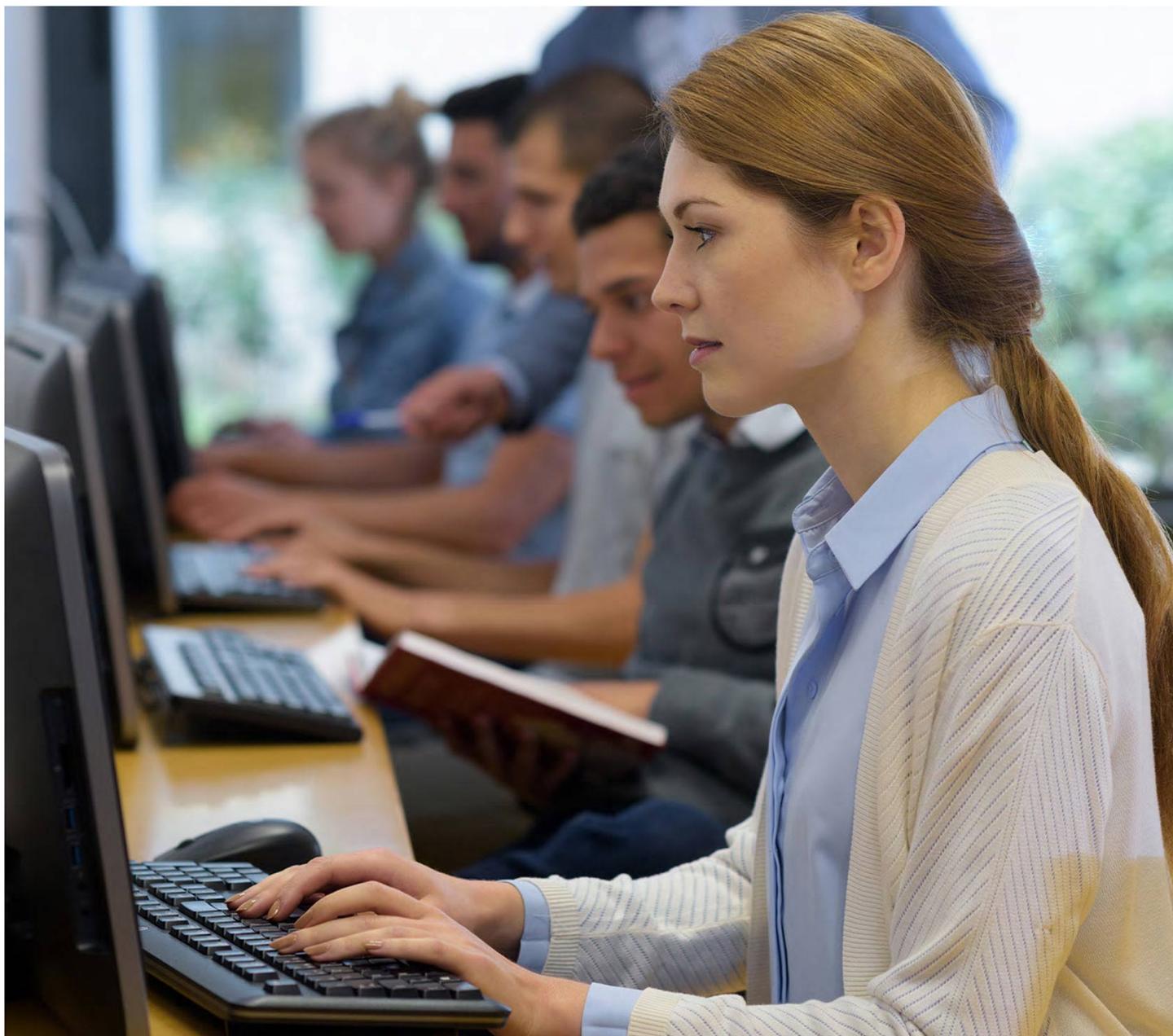




Академия АйТи
a Softline Company



Технологии в информационной безопасности: тренды, методологии, фреймворки

Код курса: `tech_sec`

Технологии в информационной безопасности: тренды, методологии, фреймворки

Код курса: tech_sec

Длительность	92 ак. часа
Формат	
Разработчик курса	Академия АйТи
Тип	Учебный курс
Способ обучения	Под руководством тренера

О курсе

Информационные технологии развиваются ежедневно, тем самым формируя необходимость интеграции новых, более эффективных ресурсов в существующие процессы. Однако, помимо этого, появление новых инструментов, систем, сервисов и средств провоцирует появление новых возможностей для совершения кибератак и проникновения в информационный периметр организации. Данный курс позволит не только ознакомиться с новейшими технологиями, доказывающими свой бизнес-результат, но и рассмотреть их внедрение с точки зрения обеспечения информационной безопасности. Secure by Design, внедрение процессов безопасной разработки и работа с форматами по типу Киберучений – это и много другое будет подробно рассмотрено в данной программе повышения квалификации.

Подробная информация

Профиль аудитории:

- Сотрудники и специалисты службы информационной безопасности.
- Руководители организаций, моделирующих архитектуру системы информационной безопасности.
- Сотрудники ИТ-направления, сталкивающиеся с задачами информационной безопасности в своей деятельности.
- Продуктовые и проектные менеджеры, которые сталкиваются с полным циклом бизнес-процессов.

Предварительные требования:

- Знания о фреймворках оценки эффективности внедрения ПО и технологических решений.
- Знания о существующих и развивающихся сквозных технологиях на рынке для бизнеса.

По окончании курса слушатели изучат:

- Процесс разработки моделей угроз безопасности и нарушителя.
- Методики оценивания ущерба от кибератак.

- Сквозные технологии (ИИ, RPA, блокчейн и пр.).
- Управление экономической эффективностью обеспечения ИБ.

Программа курса

Технологии в информационной безопасности

- Разработка моделей угроз безопасности и нарушителя (Методика ФСТЭК РФ, MITRE ATT&CK®)
- Методики оценивания ущерба от кибератак
- Продуктовая культура. DevOps
- Основы MLSecOps. Основы DevSecOps - AppSec, безопасная web-разработка, роль руководителя
- Пентестинг и этичный хакинг в компании - основные принципы и задачи
- Сквозные технологии безопасности Цифровой экономики (AI + Big Data + ETL). Иммунная защита Индустрии 4.0
- Эталонные архитектуры безопасных цифровых платформ.
- Информационная безопасность на этапе разработки ПО.
- Разработка и реализация корпоративной программы повышения киберосведомленности сотрудников компании
- Организация взаимодействия с национальными и региональными центрами реагирования на инциденты ИБ
- Управление экономической эффективностью обеспечения ИБ
- Возврат инвестиций на развитие информационной безопасности

[Посмотреть расписание курса и записаться на обучение](#)

Обращайтесь по любым вопросам

к менеджерам Академии АйТи

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