



## **Анализ безопасности приложения: анализ кода, состава и цепочек поставок ПО (SAST, DAST, IAST, RASP и SCA, SCS)**

Код курса: DSO\_2

# Анализ безопасности приложения: анализ кода, состава и цепочек поставок ПО (SAST, DAST, IAST, RASP и SCA, SCS)

Код курса: DSO\_2

<b>Длительность</b>	40 ак. часов
<b>Формат</b>	
<b>Разработчик курса</b>	Академия АйТи
<b>Тип</b>	Учебный курс
<b>Способ обучения</b>	Под руководством тренера

## О курсе

Курс предназначен для специалистов в области информационной безопасности, DevOps инженеров, IT-специалистов, разработчиков программного обеспечения, которые хотят освоить современные методы обеспечения безопасности на всех этапах разработки и развертывания ПО. Программа охватывает ключевые подходы к обеспечению безопасности приложения на базе CI/CD и контейнеризации. Участники курса углубят свои знания в области анализа цепочки поставок, внедрения процессов SSDLC, работы с инструментами анализа безопасности. Получат представление о современных фреймворках защиты от supply chain. Особое внимание уделяется практическим навыкам: вы научитесь настраивать, мониторить и улучшать безопасность контейнеров, защищать цепочку поставок ПО, проводить триаж уязвимостей и адаптировать защитные меры под реальные проекты.

## Подробная информация

### Профиль аудитории:

- DevOps-инженеры: обладающие базовыми навыками автоматизации, bash, docker
- системные администраторы
- разработчики ПО: стремящиеся улучшить понимание специфики разработки безопасного ПО безопасного и окружения
- инженеры ИБ: с базовым представлением о жизненном цикле разработки ПО, желающие получить навыки укрепления DevOps-инфраструктуры
- начинающие DevSecOps-специалисты: которые хотят освоить ключевые практики безопасности
- технические руководители и тимлиды: желающие лучше разбираться в том, как строится и защищается безопасное окружение разработки и эксплуатации ПО

### Предварительные требования:

- базовые знания в области программирования и разработки программного обеспечения
- понимание основ работы с контейнерами (docker) и системами управления версиями (например, Git)

- основы информационной безопасности и знакомство с такими концепциями, как уязвимости и методы атаки

### **По окончании курса слушатели смогут:**

- понимать и интегрировать инструменты безопасности в существующий SSDLC
- применять инструменты анализа зависимостей программного обеспечения и среды окружения – контейнеры, ОС
- обеспечивать защиту цепочки поставок ПО, используя современные фреймворки
- разрабатывать и внедрять практики безопасности и интегрировать их в существующие процессы
- работать с объединёнными решениями для управления уязвимостями и интегрировать сканеры в такие системы, на примере DefectDojo
- проводить триаж уязвимостей

## Программа курса

### Модуль 1. Инструментарий SSDLC

- Цикл безопасной разработки на примере SSDLC
- Инструменты для каждого из этапов
- Выбор инструментов для своих проектов

### Модуль 2. Анализ уязвимостей с помощью SCA/OSA

- Введение в SCA, принципы работы и популярные инструменты
- Типы уязвимостей открытого ПО
- Инструменты SCA для поиска зависимостей ОС
- Инструменты SCA для поиска зависимостей в контейнерах
- Применение SCA для поиска зависимостей в бинарных файлах
- Что такое OSA, сравнение с SCA

### Модуль 3. Безопасность цепочки поставок (supply chain)

- Ключевые понятия supply chain
- Основные векторы атак
- Стандарты и фреймворки
- SBOM и подпись артефактов
- Пример процесса реализации защита цепочки поставок

### Модуль 4. Безопасность контейнеров (Container Sec)

- Основы контейнерной безопасности
- Принципы безопасности в контейнеризации
- Харденинг образов
- Работа с trivy image, dockle, hadolint, kics
- Runtime защита
- Интеграция процессов безопасности контейнеров в CI/CD (используя GitLab)

## Модуль 5. Объединённые решения для управления уязвимостями (ASOC ASPM)

- Основные понятия
- Ключевые функции ASOC и ASPM
- Приоритизация уязвимостей
- Развертывание и интеграция сканеров в систему DefectDojo

## Модуль 6. Тriage уязвимостей

- Что такое триаж, зачем он нужен
- Критерии оценки уязвимостей
- Методологии и стратегии проведения
- Верификация обнаруженных фэйдингов

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

**Обращайтесь по любым вопросам**

к менеджерам Академии АйТи

**+7 (495) 150 96 00** | [academy@academyit.ru](mailto:academy@academyit.ru)