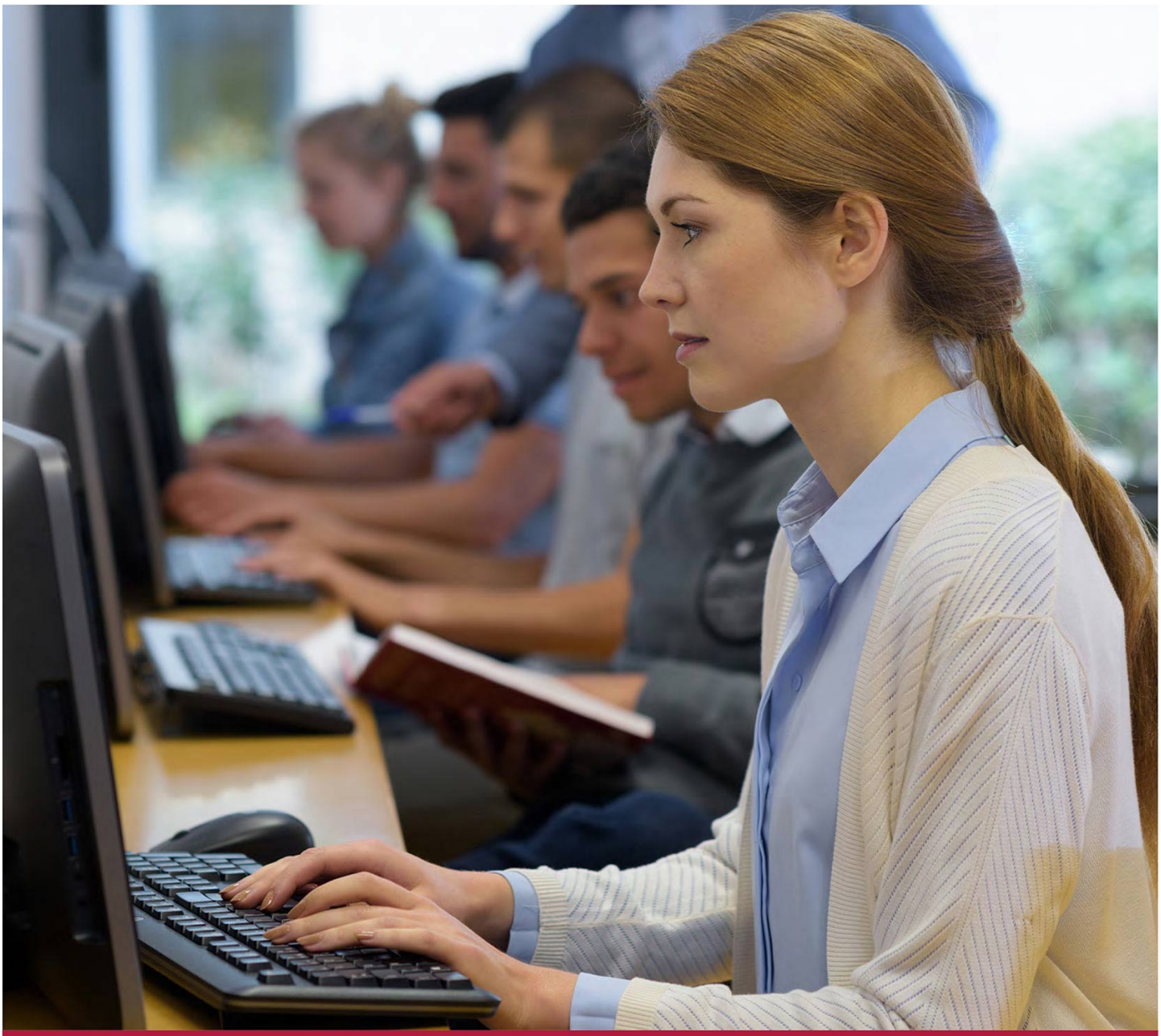
Академия АйТи
a Softline Company



Специалист DevSecOps

Код курса: devsecops_mid

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

© Академия АйТи, 2026

Специалист DevSecOps

Код курса: devsecops_mid

Длительность	180 ак. часов
Формат	-
Разработчик курса	Академия АйТи
Тип	Учебный курс
Способ обучения	Под руководством тренера

О курсе

Программа "Специалист DevSecOps" разработана для подготовки профессионалов, способных интегрировать передовые практики безопасности в процессы разработки и эксплуатации систем. Методология DevSecOps, объединяющая традиционные DevOps-принципы с акцентом на кибербезопасность, становится неотъемлемой частью успешного управления IT-инфраструктурами. В рамках программы слушатели получат комплексные знания о принципах DevSecOps-культуры, научатся автоматизировать процессы безопасности, выявлять уязвимости на ранних стадиях разработки и развивать гибридные системы, сочетающие скорость и надежность. Практическая направленность курса позволяет участникам нарабатывать прикладные навыки на актуальных инструментах и методиках, востребованных в сложных корпоративных средах.

Подробная информация

Профиль аудитории:

- DevOps-инженеры.
- Архитеторы ПО
- Программисты
- Специалисты по ИБ

Предварительные требования:

- Знание основ программирования

По окончании курса слушатели смогут:

- Отлаживать программный код;
- Использовать вспомогательные инструментальные программные средства для обработки исходного текста программного кода;
- Выявлять ошибки в программном коде;
- Контролировать компоненты с открытым исходным кодом при попадании в периметр разработки (Open Source Analysis, OSA);
- Проводить статический анализ кода (Static Application Security Testing, SAST);

© Академия АйТи, 2026

- Контролировать состав компонент ПО (Software Composition Analysis, SCA);
- Проводить динамический анализ кода (Dynamic Application Security Testing, DAST/Interactive Application Security Testing, IAST/Behavioral Application Security Testing, BAST);
- Проводить анализ бинарного кода и контроль состава контейнеров (Bytecode and Container Analysis, BCA);
- Применять известные технические меры безопасности для разработки безопасного ПО;

После успешного окончания курса, слушатель будет знать:

- Основные методы и практики DevSecOps
- Методы и приемы алгоритмизации поставленных задач безопасной разработки ПО
- Алгоритмы решения типовых задач, области и способы их применения
- Технологии безопасного программирования
- Особенности выбранной среды программирования
- Методы и приемы отладки программного кода
- Типы и форматы сообщений об ошибках и уязвимостях ПО

Программа курса

Модуль 1 «Основные концепции DevSecOps».

Тренды разработки современного ПО (внедрение практик DevOps, снижение общих сроков разработки ПО (time to market), повышение гибкости в разработке ПО, переход от монолитных к микросервисным приложениям, динамическое выделение ИТ-ресурсов, повышение внимания к вопросам разработки безопасного ПО).

Основные понятия и определения DevOps и DevSecOps.

Ключевые компоненты DevSecOps (анализ кода, управление изменениями, мониторинг соотвествия, иследование угроз безопасности, оценка уязвимости кода, обучение и повышение осведомленности).

Основные этапы DevSecOps (разработка приложения и работа с репозиторием программ, непрерывная интеграция (CI) и тестирование приложения, непрерывное развертывание (CD) приложения в рабочей среде, контроль новой версии приложения в рабочей среде).

Возможные сценарии интеграции DevSecOps в процессы и инфраструктуру компании.

Адаптации функции кибербезопасности и интеграции DevSecOps.

Проведение оценки безопасности процесса разработки, а также идентификация ключевых рисков и риск-факторов, связанных с недостатками процесса.

Ключевые точки процесса разработки, где необходимо включение мер безопасности

Информирование сотрудников о критических рисках и мерах для их снижения.

Модуль 2. «Основные практики DevSecOps».

Контроль компонент с открытым исходным кодом (Open Source Analysis, OSA)

 © Академия АйТи, 2026

Статический анализ кода (Static Application Security Testing, SAST).

Контроль состава компонент ПО (Software Composition Analysis, SCA).

Динамический анализ кода (Dynamic Application Security Testing, DAST/Interactive Application Security Testing, IAST/Behavioral Application Security Testing, BAST).

Фаззинг - как метод исследования уязвимостей.

Фаззинг-тестирование (fuzzing).

Практика по использованию сканеров уязвимостей (выполняется под непосредственным руководством преподавателя). Решения для выявления и нейтрализации уязвимостей программного кода.

Модуль 3. «Трансформация DevOps в DevSecOp».

Трансформация DevOps в DevSecOps. Использование безопасных по умолчанию библиотек, фреймворков и компонент ПО в процессе разработки (Secure-by-Default).

Интеграция технологических практик ИБ в начало конвейера CI/CD (Shift-Left подход).

Автоматизация процессов в концепции Everything-as-a-Code.

Формирование сообщества security-чемпионов в производственных командах для повышения инженерной security-культуры.

Применение модели зрелости DevSecOps для оценки существующего процесса и для постоянного совершенствования.

Обеспечение прозрачности security активностей для участников инженерного производственного процесса.

DevSecOps-оркестрация (Application Security Testing Orchestration, ASTO) для непрерывного улучшения процесса разработки безопасного ПО.

Модуль 4. «Национальные требования (ГОСТ Р 56939-2016 и ГОСТ Р ИСО/МЭК 12207) в части разработки безопасного ПО».

Требования в части идентификации и аутентификации.

Требования по защите от несанкционированного доступа к информации.

Требования в части регистрации событий безопасности.

Требования контроля точности, полноты и правильности входных и выходных данных.

Требования по обработке программных ошибок и исключительных ситуаций.

Требования класса ASE ""Оценка задания по безопасности"" (ГОСТ Р ИСО/МЭК 15408-3).

Меры по разработке безопасного программного обеспечения, реализуемые при выполнении

 © Академия АйТи, 2026

инсталляции программы и поддержки приемки программного обеспечения.

Меры по разработке безопасного программного обеспечения, реализуемые при решении проблем в программном обеспечении в процессе эксплуатации.

Меры по разработке безопасного программного обеспечения, реализуемые в процессе менеджмента инфраструктурой среды разработки программного обеспечения.

Модуль 5. «Роли и кадровое обеспечение DevSecOps».

Принятие методологии разработки безопасного ПО, DevSecOps (оценка текущих мер безопасности и распределение ролей в команде разработки ПО, внедрение мер безопасности на стадии проектирования программных систем, внедрение инструментов и авто-тестов безопасности в пайплайн, тестирование безопасности разработанных решений, анализ выявленных уязвимостей и подготовка рекомендаций по их устранению, обучение лучшим практикам разработки безопасного ПО, Best Practices).

Распределение ролей в процессе DevSecOps (продакт менеджер, архитектор, команда разработки, QA, AppSec специалист, DevOps инженер).

Воспитание чемпионов безопасности Security Champions (масштабирование безопасности с помощью нескольких команд разработки, привлечение сотрудников, не связанных с безопасностью, но связанных с DevOps, создание и развитие культуры безопасности).

Повышение осведомленности по вопросам разработки безопасного ПО.

Развитие корпоративной культуры DevSecOps и безопасности в целом.

Посмотреть расписание курса и записаться на обучение

Обращайтесь по любым вопросам
к менеджерам Академии АйТи

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

© Академия АйТи, 2026