

ПРАВИТЕЛЬСТВО РОССИЙСКОЙ ФЕДЕРАЦИИ

ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ АВТОНОМНОЕ
ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ
«НАЦИОНАЛЬНЫЙ ИССЛЕДОВАТЕЛЬСКИЙ УНИВЕРСИТЕТ
«ВЫСШАЯ ШКОЛА ЭКОНОМИКИ»

Московский институт электроники и математики им. А.Н. Тихонова

ЗАДАНИЕ
на выполнение выпускной квалификационной работы

студенту группы МКБ231 Будяк Марии Николаевны

1. Тема работы

Интеграция практик безопасности в CI/CD для приложений Spring Boot.

2. Требования к работе

2.1. Цель работы

Цель данной работы заключается в повышении эффективности разработки и обеспечения безопасности микросервисов, построенных на платформе Java Spring Boot, путем оценки и выбора наиболее эффективных open-source инструментов статического и динамического анализа, а также анализа состава программного обеспечения. В частности, акцент будет сделан на инструментах SCA (Software Composition Analysis), SAST (Static Application Security Testing) и DAST (Dynamic Application Security Testing).

В рамках исследования будет проведен анализ доступных open-source библиотек для практической реализации предложенных решений. Оценка инструментов будет осуществляться на основе бенчмарков и методик, что позволит выявить их эффективность и соответствие современным требованиям безопасности.

В данной работе тестируются различные инструменты SCA, SAST и DAST на основе бенчмарков. Это поможет оценить их эффективность и выявить достоинства и недостатки каждого из них в контексте разработки микросервисов. Особое внимание будет уделено анализу взаимодополняемости этих инструментов и их роли в повышении уровня безопасности приложений. Таким образом, работа фокусируется как на решении прикладных задач, так и на углублении понимания современных

методов обеспечения безопасности в разработке программного обеспечения.

2.2. Требования к результатам работы

1. Исследование инструментов SCA, SAST и DAST

- 1) Провести исследование и описать доступные open-source инструменты для статического анализа кода (SAST), анализа зависимости (SCA) и динамического анализа приложений (DAST), применимых для сервисов на Java.
- 2) Указать, как интегрировать эти инструменты в CI/CD процессы, с возможностью использования в GitHub и GitLab.

2. Определение бенчмарков

- 1) Найти и описать релевантные бенчмарки, которые можно использовать для оценки предложенных инструментов анализа.
- 2) Оценить показатели и критерии, по которым будут производиться сравнительные анализы.

3. Методики оценки

- 1) Разработать или адаптировать методики оценки эффективности инструментов для SAST, SCA и DAST.
- 2) Описать, какие параметры и метрики будут использоваться для оценки (например, точность обнаружения уязвимостей, скорость анализа, легкость интеграции и т.д.).

4. Проведение оценки и анализа результатов

- 1) Провести оценку каждого инструмента по установленным бенчмаркам и методикам.
- 2) Провести углубленный анализ полученных результатов, выявить сильные и слабые стороны каждого инструмента.
- 3) Обсудить влияние полученных данных на выбор инструмента для конкретных задач.