

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 интеграции методов статического и динамического анализа, а также анализа состава программного обеспечения. В частности, акцент будет сделан на использовании инструментов SCA (Software Composition Analysis), SAST (Static Application Security Testing) и DAST (Dynamic Application Security Testing).

В рамках исследования будет изучено применение open-сурсных библиотек, доступных для скачивания в России, что обеспечит доступность и возможность практической реализации предложенных решений. Особое внимание будет уделено поиску и оценке русских аналогов анализируемых инструментов, если таковые найдутся.

В результате работы будет представлена практическая реализация интеграции инструментов SCA и SAST в процесс разработки микросервисов, что позволит продемонстрировать их взаимодополняемость и вклад в повышение уровня безопасности приложений. Кроме того, будет рассмотрено применение DAST в рамках тестирования и эксплуатации, что подчеркнет важность комплексного подхода к обеспечению безопасности. Таким образом, работа направлена не только на решение конкретных прикладных задач, но и на развитие понимания актуальных методов обеспечения безопасности в контексте современного программного обеспечения.

2.2. Требования к результатам работы

1. Параметры анализа.

Установление критериев анализа для SAST и SCA. Определение параметров конфигурации для DAST (методы тестирования, целевые URL и т.д.).

2. Интеграция инструментов SCA, SAST и DAST.

Автоматическая интеграция SCA и SAST в CI/CD для анализа кода на этапе разработки. Настройка DAST для проверки развернутых микросервисов на уязвимости с автоматизацией сканирования после релиза.

### 3. Документация конфигурации.

Подготовка документации по настройке инструментов, включая версии ПО и пошаговые инструкции. Описание процесса настройки CI/CD с примерами конфигурационных файлов.

### 3. Отчетность и мониторинг.

Реализация механизма формирования отчетов о результатах анализа. Настройка уведомлений о критических уязвимостях для команды разработки.

### 4. Повышение уровня безопасности

Проведение минимум двух полных циклов тестирования с анализом результатов.

Формирование рекомендаций по улучшению процессов разработки и тестирования.

### 5. Тестирование на реальном окружении.

Проведение комплексной проверки всех инструментов в тестовой или песочнице с целью подтверждения успешного внедрения и соответствия установленным требованиям безопасности.

### 2.3. Требования к документации

Текст ВКР должен быть оформлен в соответствии с ГОСТ.

### 3. Содержание работы

3.1. Обзор научно-технической литературы по теме работы

3.2. Обзор инструментов SCA, SAST и DAST

3.3. Настройка инструментов

3.4. Интеграция инструментов

3.5. Настройка отчетности и мониторинга

3.6. Проведение циклов тестирования и анализ результатов

3.7. Тестирование на реальном окружении

3.8. Документация конфигурации

3.9. Подготовка пояснительной записки к ВКР

3.10. Заключение

### 4. Сроки выполнения этапов работы

Проект ВКР представляется студентом в срок до	«16» февраля 2025 г.
Первый вариант ВКР представляется студентом в срок до	«31» марта 2025 г.
Итоговый вариант ВКР представляется студентом руководителю до загрузки работы в систему «Антиплагиат» в срок до	«30» апреля 2025 г.

Задание выдано

«20» декабря 2024 г.

  
подпись руководителя

В.О. Минченков

Задание принято к  
исполнению

«20» декабря 2024 г.

  
подпись студента

М.Н. Будяк