

УДК 004.4'2

Разработка и внедрение конвейера проверки безопасности исходного кода в процессах CI/CD на платформе GitFlic
Багаутдинов А.Л. (ИТМО)

Научный руководитель – инженер-практикант Савков С.В. (ИТМО)

Введение. В современных процессах разработки программного обеспечения критически важно обеспечить безопасность исходного кода на всех этапах его жизненного цикла. Одним из эффективных решений является интеграция инструментов анализа кода в конвейеры непрерывной интеграции и развертывания (CI/CD) [1], что позволяет оперативно выявлять и устранять уязвимости. Дополнительно рекомендуется ориентироваться на ключевые модели угроз, описанные в OWASP Top 10 [2]. В рамках концепции DevOps [1, с. 45–50] особое место занимает постоянная интеграция и автоматизация, о которой подробно говорил М. Фаулер [3]. С учётом современных требований безопасности в DevSecOps-среде всё более актуальным становится включение анализа кода и мониторинга безопасности на каждом этапе разработки. Отечественная платформа Gitflic [4] предоставляет удобные средства для интеграции различных инструментов анализа кода в конвейер CI/CD, что позволяет ускорить процесс обнаружения уязвимостей и повысить надёжность программного продукта.

Основная часть. Целью исследования является автоматизация выявления уязвимостей в коде на ранних этапах разработки за счет использования инструментов статического и динамического анализа [2]. В рамках работы:

- 1) Проводится анализ существующих методов обеспечения безопасности в DevSecOps;
- 2) Выбираются оптимальные инструменты анализа кода;
- 3) Разрабатывается и тестируется конвейер безопасности, интегрированный в процессы CI/CD на платформе Gitflic [4].

Практическая часть работы включает в себя создание конвейера на основе современных инструментов анализа безопасности (например, статический анализ, проверка зависимостей, тестирование на уязвимости, а также динамический анализ на этапе развертывания), его тестирование на примерах реальных проектов и оценку эффективности выявления уязвимостей [3].

Выводы. Разработанный и внедренный конвейер безопасности позволяет автоматизировать процесс проверки исходного кода на наличие уязвимостей, снижая риски их эксплуатации [2]. Результаты работы могут быть полезны разработчикам, инженерам DevOps и инженерам по информационной безопасности для повышения уровня защищенности программного обеспечения и оптимизации процессов CI/CD [1; 4].

Список использованных источников:

1. Ким Г., Хамбл Дж., Дебуа П., Уиллис Дж. DevOps Handbook: How to Create World-Class Agility, Reliability, and Security in Technology Organizations. — Portland: IT Revolution Press, 2016. — 480 p.
2. OWASP. OWASP Top 10 — 2021: The Ten Most Critical Web Application Security Risks [Электронный ресурс]. — 2021. — Режим доступа: <https://owasp.org/Top10/> (дата обращения: 01.02.2025).
3. Фаулер М. Continuous Integration [Электронный ресурс]. — Режим доступа: <https://martinfowler.com/articles/continuousIntegration.html> (дата обращения: 01.02.2025).
4. Gitflic. Официальная документация [Электронный ресурс]. — 2025. — Режим доступа: <https://gitflic.ru/docs> (дата обращения: 01.02.2025).