УДК 004.056.3

ПОДХОД К ОБЕСПЕЧЕНИЮ БЕЗОПАСНОСТИ ЦЕПОЧКИ ПОСТАВОК ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ В ОБЪЕКТАХ КИИ

Секретарева Е. Н.[1]
Научный руководитель – канд. экон. наук, доцент Нехорошков Е. В.[1]
[1]Научно-технологический университет «Сириус»
liza.sek.000@mail.ru

Введение

DevSecOps рассматривается как один из ключевых подходов интеграции механизмов информационной безопасности в процессы непрерывной интеграции и доставки (CI/CD), обеспечивая включение проверок безопасности на ранних этапах жизненного цикла программного обеспечения. По данным отраслевого исследования, 68% респондентов полностью внедрили методы DevSecOps, а 22% находятся в процессе их внедрения, что отражает рост распространённости данного подхода и его практическую значимость [1].

В отечественной научной литературе также рассматриваются модели, ориентированные на повышение безопасности процесса поставки программного обеспечения. При этом подчёркивается, что при проектировании приложений для объектов критической информационной инфраструктуры одним из основных критериев является безопасность разработки и внедрения программного обеспечения, а также необходимость соблюдения требований Федерального закона №187-ФЗ [2].

Одновременно с этим в российской практике отмечается дефицит отечественных корпоративных DevSecOps-решений, сопоставимых по функциональности с зарубежными аналогами [3]. Указанное противоречие между востребованностью DevSecOps-подхода и ограничениями, связанными с нормативными требованиями КИИ и наличием инструментов, определяет актуальность исследования и обосновывает необходимость разработки концептуальной модели, применимой в условиях объектов КИИ.

Основная часть

В рамках исследования предлагается подход к обеспечению безопасности цепочки поставок программного обеспечения в объектах критической информационной инфраструктуры, основанный на формировании концептуальной модели DevSecOps-процесса, адаптированного к условиям строгого нормативного регулирования. Предлагаемый подход ориентирован на управление изменениями состава программного обеспечения, возникающими при обновлении библиотек и программных компонентов, контроль их внедрения в эксплуатируемую инфраструктуру.

Суть предлагаемого решения заключается в формировании концептуальной модели контроля обновлений программных компонентов, при котором каждое изменение программного компонента рассматривается как потенциальный риск для безопасности объекта КИИ и подлежит обязательной проверке на этапах разработки, сборки и развертывания. В рамках концептуальной модели выделяются ключевые стадии жизненного цикла программного обеспечения, выполняется статический анализ исходного кода и зависимостей, а также динамический анализ развернутых сервисов. Результаты проверок используются для принятия решения о внедрении изменений.

В отличие от типовых DevSecOps-реализаций, ориентированных на облачные и коммерческие среды, предлагаемая модель не предполагает использования внешних сервисов и программного обеспечения, не соответствующего законодательным и регуляторным требованиям для значимых объектов КИИ. Оригинальность подхода

заключается в интеграции требований нормативно-правовой базы в методологию DevSecOps. Предлагаемый подход предназначен для использования на ранних этапах проектирования и может служить основой для последующей реализации.

Выводы

Проведен анализ применения DevSecOps-подхода в объектах критической информационной инфраструктуры и предложена концептуальная модель обеспечения безопасности цепочки поставок программного обеспечения. Предложенное решение может быть использовано при построении регламентированных CI/CD-процессов с контролем цепочки поставок программных компонентов.

Литература

1. Cheenepalli J., Hastings J. D., Ahmed K. M., Fenner C. Advancing DevSecOps in SMEs: Challenges and Best Practices for Secure CI/CD Pipelines [Электронный ресурс]. – Режим доступа: https://arxiv.org/abs/2503.22612 (Дата обращения 03.02.2026).
2. Пилькевич П. В., Спеваков А. Г., Калуцкий И. В. Модель системы принятия решений на основании мониторинга инцидентов // Труды МАИ. 2025. № 143. – Режим доступа: https://cyberleninka.ru/article/n/model-sistemy-prinyatiya-resheniy-na-osnovanii-monitoringa-intsidentov (Дата обращения 03.02.2026).
3. Житнюк П. П. Не было бы счастья // Россия в глобальной политике. 2024. № 1. – Режим доступа: https://cyberleninka.ru/article/n/ne-bylo-by-schastya-1 (Дата обращения 04.02.2026).