УДК 004.056

ОСОБЕННОСТИ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ В ВИРТУАЛЬНЫХ ЛОКАЛЬНЫХ ВЫЧИСЛИТЕЛЬНЫХ СЕТЯХ С CI/CD И IAC

Воронцов Е.Н. (ИТМО)
Научный руководитель – инженер Савков С.В. (ИТМО)

Введение. В условиях стремительного развития информационных технологий и роста зависимости предприятий от виртуальных систем, обеспечение информационной безопасности становится критически важным. Инструменты автоматизации, такие как GitLab, играют ключевую роль в ускорении процессов continuous integration и continuous delivery (CI/CD) и предлагают значительные преимущества в автоматизации развертывания и управления виртуальными локальными вычислительными сетями (ЛВС) через использования подхода Infrastructure as Code (IaC). Однако использование этих инструментов накладывают дополнительные требования к информационной безопасности системы, что может порождать потенциальные векторы атак и создавать новые угрозы.

Основная часть. Разработка и развертывание виртуальных ЛВС при помощи GitLab CI/CD требует решения ряда дополнительных задач обеспечения информационной безопасности сети:

1) Задачи авторизации и контроля доступа. Для корректной работы конвейеров CI/CD необходим доступ к конфиденциальным данным. При предоставлении избыточных полномочий существует риск несанкционированного доступа к конфиденциальной информации, что может привести к изменению кода или утечке данных. Мерой защиты от угроз, эксплуатирующих избыточные привилегии, является внедрение ролевой модели доступа и использование принципа «наименьших привилегий».
2) Задачи организации управления безопасностью и хранения конфиденциальной информации. Конвейерам часто требуется доступ к такой информации, как пароли, ключи и сертификаты. Если они хранятся небезопасно или обрабатываются в открытом виде внутри конвейера, то злоумышленники могут перехватить их, что в свою очередь может привести к несанкционированному доступу к компонентам ЛВС. Так, подходом к защите от угроз, эксплуатирующих уязвимость хранения паролей в открытом виде, является использование защищенных переменных окружения или использование специальных хранилищ секретов, как, например, StarVault. [2]
3) Использование актуальных рекомендаций и современных подходов к работе с кодом. Одна из основных функций конвейера CI/CD - выявление уязвимостей кода перед развертыванием. Без последовательных проверок безопасности уязвимый код может остаться незамеченным, подвергая приложения потенциальному воздействию внешних угроз. Мерой защиты от угроз, эксплуатирующих уязвимый код, является внедрение static application security testing (SAST), которое определяет ошибки и уязвимости в исходном коде. [1]

Выводы. Проведен анализ основных векторов угроз информационной безопасности при автоматизации развертывания виртуальных ЛВС с использованием процессов CI/CD, разработан модель угроз и предложены методы защиты в соответствии с этой моделью.

Список использованных источников:

1. Secure GitLab [Электронный ресурс] — режим доступа: https://docs.gitlab.com/ee/security/ (дата обращения: 11.02.2025).
2. Tony Hsu. Hands-On Security in DevOps Ensure continuous security, deployment, and delivery with DevSecOps // Packt Publishing, 2018.