УДК 004.056

ВОПРОСЫ ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ ВНЕДРЕНИЯ ИТ ПРОЕКТОВ С ИСПОЛЬЗОВАНИЕМ СОВРЕМЕННЫХ СТАНДАРТОВ

Андрущенко А. М. (Российский государственный гидрометеорологический университет)

Научный руководитель — профессор кафедры информационных технологий и систем безопасности Завгородний В.Н. (Российский государственный гидрометеорологический университет)

Введение. В современном мире, где программное обеспечение становится основой практически всех аспектов жизни — от критически важных инфраструктур до повседневных приложений — обеспечение его безопасности и надёжности превращается в одну из ключевых задач разработки. Однако, несмотря на повсеместное внедрение современных инструментов, таких как системы контроля версий Git [1], многие компании, особенно небольшие, сталкиваются с серьёзными вызовами при создании безопасной и эффективной сборочной линии. Уязвимости, внесённые на этапе сборки, могут стать причиной катастрофических последствий: от утечек конфиденциальных данных до полного выхода из строя критически важных систем [2].

Согласно исследованиям, более 60% уязвимостей в программном обеспечении возникают из-за ошибок в процессе разработки и сборки [3]. При этом объём и сложность программного обеспечения продолжают расти, что делает ручные методы контроля и обеспечения безопасности всё менее эффективными [4]. В таких условиях даже одна небольшая ошибка в сборочной среде может привести к масштабным убыткам, репутационным потерям и юридическим последствиям [5].

Осознавая эту проблему, ведущие компании в области информационной безопасности, а также государственные структуры разработали ГОСТ Р 56939-2024 [6]. Этот стандарт устанавливает чёткие требования к созданию безопасной сборочной среды, что особенно актуально в условиях ужесточения регуляторных норм и роста киберугроз [7]. Внедрение таких стандартов не только помогает минимизировать риски, но и способствует повышению качества продукта, что напрямую влияет на конкурентоспособность компании на рынке [8].

Основная часть. Цель исследования: Проектирование безопасной сборочной линии программного обеспечения в соответствии с ГОСТ Р 56939-2024

В ходе тщательного изучения технической документации и анализа промышленного опыта работы с системой контроля версий, были определены следующие ключевые шаги для обеспечения безопасной сборочной среды:

1. Формирование и поддержание в актуальном состоянии правил кодирования: общие правила оформления исходного кода позволяют значительно сократить время на выявление ошибок и проведение экспертизы отдельных участков программы;
2. Экспертиза исходного кода: ручная проверка каждого фрагмента исходного кода;
3. Статический анализ исходного кода: предотвращение внесения потенциально опасных конструкций и ошибок в код продукта с использованием специализированного программного обеспечения;
4. Динамический анализ кода программы: обнаружение недостатков и уязвимостей в коде продукта непосредственно в процессе его выполнения;
5. Обеспечение безопасности используемых секретов: проверка фрагментов кода на наличие секретов и обеспечение их безопасного использования;
6. Проверка кода на предмет внедрения вредоносного кода через цепочки поставок: формирование списка заимствованных компонентов и последующая проверка этих компонентов на наличие уязвимостей и вредоносного кода.

Создание безопасной сборочной среды требует комплексного подхода, который включает разработку чётких регламентов, фиксацию информации о системе сборки, обеспечение повторяемости процессов и защиту конфиденциальных данных. Все перечисленные меры направлены на минимизацию рисков внесения ошибок и уязвимостей на всех этапах сборки программного обеспечения.

Вывод. В результате исследования были определены ключевые шаги для создания безопасной сборочной среды программного обеспечения. Эти меры легли в основу методики, направленной на минимизацию рисков внесения ошибок и уязвимостей на всех этапах сборки. Разработанный подход позволяет повысить надёжность и безопасность программного обеспечения, что особенно важно в условиях растущей сложности и объёмов разработки.

Список использованных источников:

1. Chacon S., Straub B. "Pro Git" – Apress, 2014.
2. Verizon "Data Breach Investigations Report (DBIR)" – Verizon, 2023.
3. Synopsys "Cybersecurity Research Report" – Synopsys, 2022.
4. Gartner "Market Guide for Application Security Testing" – Gartner, 2023.
5. Ponemon Institute "Cost of a Data Breach Report" – Ponemon Institute, 2022.
6. ГОСТ Р 56939-2024 "Разработка безопасного программного обеспечения. Требования к процессам жизненного цикла" – М.: Стандартинформ, 2024.
7. OWASP "OWASP Top Ten Web Application Security Risks" – OWASP Foundation, 2021.
8. Krebs B. "The SolarWinds Hack: What Happened and What’s Next?" – Krebs on Security, 2021.