Методы анализа программного обеспечения

Методы анализа

Статический анализ кода - это процесс выявления ошибок и недочетов в исходном коде программ. Статический анализ можно рассматривать как автоматизированный процесс обзора кода (code review).

Динамический анализ кода - это способ анализа программы непосредственно при ее выполнении.

[1]

Статический анализ: преимущества

- Может использоваться на ранних этапах жизненного цикла программного обеспечения, прежде чем код готов для исполнения и до начала тестирования.
- Статические анализаторы проверяют даже те фрагменты кода, которые получают управление крайне редко.
- Низкие стоимостные затраты (например, нет необходимости создавать тестовые программы); разработчики могут запускать свои собственные виды анализа.

[1, 2]

Статический анализ: недостатки

- Поскольку во время статического анализа делается попытка предсказать поведение программы, то иногда обнаруживается "ошибка", которой фактически не существует – это так называемое "ложное срабатывание" (false positive).
- Статический анализ, как правило, слаб в диагностике утечек памяти и параллельных ошибок.

[1, 2]

Динамический анализ: преимущества

- Редко возникают "ложные срабатывания" – высокая продуктивность по нахождению ошибок.
- Для отслеживания причины ошибки может быть произведена полная трассировка стека и среды исполнения.

[1, 2]

Динамический анализ: недостатки

- Полнота анализа ошибок зависит от степени покрытия кода. Кодовый путь, содержащий ошибку, должен быть обязательно пройден, а в контрольном примере должны создаваться необходимые условия для создания ошибочной ситуации.
- Происходит вмешательство в поведение системы в реальном времени. Это не всегда приводит к возникновению проблем, но об этом нужно помнить.

[1, 2]

Инструменты статического анализа

“Best 73 C static analysis tools” https://analysis-tools.dev/tag/c

3. cppcheck
9. PVS-studio

Что посмотреть еще

- gcc -c -fanalyzer имя_файла (gcc >= 10)
- clang --analyze –Xanalyzer -analyzer-output=text имя_файла

Что почитать

1. https://www.viva64.com/ru/b/ [Блог разработчиков PVS-Studio]
2. Билл Грэм, Пол Н. Леру «Использование статического и динамического анализа для повышения качества продукции и эффективности разработки»
3. Тонкости анализа исходного кода C/C++ с помощью cppcheck [хабр]
4. Александр Алексеев «Краткий обзор статических анализаторов кода на C/C++»