УДК 681.3.069

Исследование компиляторов и статический анализ кода

Михаленя А.Н.
Белорусский национальный технический университет

Статический анализ кода – анализ программного обеспечения, производимый (в отличие от динамического анализа) без реального выполнения исследуемых программ. В большинстве случаев анализ производится над какой-либо версией исходного кода, хотя иногда анализу подвергается какой-нибудь вид объектного кода, например P-код или код на MSIL. Термин обычно применяют к анализу, производимому специальным программным обеспечением (ПО). В зависимости от используемого инструмента глубина анализа может варьироваться от определения поведения отдельных операторов до анализа, включающего весь имеющийся исходный код.

Способы использования полученной в ходе анализа информации также различны – от выявления мест, возможно содержащих ошибки, до формальных методов, позволяющих математически доказать какие-либо свойства программы (например, соответствие поведения спецификации). Некоторые люди считают программные метрики и обратное проектирование формами статического анализа. Получение метрик и статический анализ часто совмещаются, особенно при создании встраиваемых систем. В последнее время статический анализ все больше используется в верификации свойств ПО, используемого в компьютерных системах высокой надежности, особенно критичных для жизни.

Следует отметить, что анализ кода – это возможность программы прочитать код анализируемой программы в какой-либо форме, «понять» его и выдать какую-то информацию. Соответственно, практически все анализаторы кода можно представить себе как поиск в определенном представлении программы (возможно с преобразованиями) определенных паттернов и дальнейший подробный анализ найденных участков.

Большинство компиляторов (например, GNU C Compiler) выводят на экран «предупреждения» (warnings) – сообщения о том, что код, будучи синтаксически правильным, скорее всего, содержит ошибку. Например:

```
int x;
int y=x+2; // Переменная x не инициализирована.
```

Это простейший статический анализ. У компилятора есть много других немаловажных характеристик – в первую очередь скорость работы и качество машинного кода, поэтому компиляторы проверяют код лишь на очевидные ошибки. Статические анализаторы предназначены для более детального исследования кода.