Е. О. Деревенец, Е. Н. Трошина, А. В. Чернов

Восстановление управляющих конструкций обработки исключений языка Си++

Авторами рассматриваются некоторые методы декомпиляции программ на языке Си++ — методы восстановления структурных конструкций обработки исключений языка Си++ try-catch и оператора генерации исключений throw.

Введение

Обратная инженерия ставит своей задачей наиболее полное восстановление информации о том, как работает система. Для этого в системе требуется выделить компоненты, определить взаимосвязи между ними и законы, по которым происходит функционирование компонент. При обратной инженерии программных систем необходимо по доступному исполняемому коду построить их высокоуровневое представление, включающее описание алгоритмов, реализованных в их компонентах, одним из способов которого может служить представление в виде программы на языке высокого уровня. Для его получения используют *декомпилятор* — программный инструмент для проведения декомпиляции.

Декомпиляция — восстановление программы на языке высокого уровня из программы на языке низкого уровня, из объектного кода, исполняемых файлов или трасс выполнения; включает решение следующих подзадач:

1) выделение функций во входной программе;

2) восстановление управляющих конструкций языка высокого уровня;

3) анализ потоков данных, восстановление локальных переменных и аргументов функций;

4) восстановление базовых и производных типов данных;

5) генерация кода на языке высокого уровня.

Данная работа посвящена проблеме восстановления высокоуровневых управляющих структурных конструкций.

На сегодняшний день наиболее распространенные языки программирования, транслируемые в машинный код, — языки Си и Си++. Поэтому декомпиляция программ, написанных на этих языках, представляет наибольшую практическую ценность.

Настоящая статья является продолжением работы [1], посвященной восстановлению структурных конструкций языка Си **if-then**, **if-then-else**, **while**, **do-while**, **for**, **switch**. С точки зрения структурного анализа язык Си++ — это расширение языка Си. В языке Си++ появились встроенные средства, предназначенные для обработки ошибок — аппарат исключений. В данной работе проводится анализ особенностей восстановления конструкций языка Си++, предназначенных для обработки исключительных ситуаций: блоков **try-catch** и оператора генерации исключений **throw**. В качестве программы на языке низкого уровня рассматриваются программы на языке ассемблера.

Статья имеет следующую структуру. Первый раздел содержит обзор работ по теме восстановления структурных конструкций языка Си++ и обратной инженерии различных способов реализации механизма исключений в языке Си++. Во втором разделе представлены описания наиболее популярных способов реализации исключений компиляторами на платформах Windows и GNU/Linux и методы восстановления плат-