ПРОГРАММНОЕ ОБЕСПЕЧЕНИЕ БЕЗ ОШИБОК: ЯЗЫК ADA 2012

Статья посвящена истории развития и возможностям промышленного языка программирования Ada 2012, который используется для разработки программного обеспечения встраиваемых компьютерных систем с повышенными требованиями к надежности и безопасности.

Язык программирования Ada был разработан в начале 1980-х гг. с целью создать язык для встраиваемых систем реального времени с повышенными требованиями к надежности программного обеспечения (ПО). В 1983 г. язык Ada стал стандартом ANSI/MIL-STD-1815A, а в 1987 г. — международным стандартом ISO 8652. Первая версия языка, называемая Ada 83, также стала стандартом ГОСТ 27831-88 во времена активного внедрения этого языка в СССР при поддержке ГКНТ (Государственного комитета по науке и технике Совета министров СССР).

В дальнейшем языку Ada в России не повезло: в 1990-х гг. о нем забыли. Однако в остальном мире язык продолжал развиваться и совершенствоваться (Ada 95, Ada 2005), и сегодняшняя версия Ada 2012 является действующим международным стандартом ISO 8652:2012. Ada стал основным языком разработки ПО встраиваемых компьютерных систем, критически важных для безопасности.

Некорректная работа таких систем представляет угрозу здоровью или жизни людей (например, может привести к аварии на транспорте), может нанести существенный ущерб окружающей среде (в частности, посредством выброса на вредном производстве) или чревата значительным экономическим ущербом (таким как потерей космического аппарата). Компьютеров, критически важных для безопасности, становится все больше, и отсутствие ошибок в их встроенном ПО приобретает все бóльшую значимость. Поэтому различные отрасли ввели сертификацию ПО по специальным отраслевым стандартам безопасности, таким как DO-178 (авионика), IEC 61508 (промышленное оборудование), IEC 60880 (атомная энергетика), EN 50128 (железнодорожные системы), ISO 26262 (автоэлектроника) и IEC 62304 (медицинское оборудование).

Каждая новая редакция стандарта для Ada усиливала его позицию как языка, наиболее подходящего для разработки критически важного для безопасности ПО. Ada 2012 не стал исключением. Основным дополнением к его стандарту является «контракт» — требования к результатам работы программного модуля, описанные непосредственно в тексте программы на языке Ada. Конструкция «контракт» имеет стандартизованный синтаксис и предназначена для использования

средствами статического анализа исходного кода с целью проверить, делает ли программный модуль именно то, что написано в условиях «контракта». Идея «контрактного программирования» не нова, но Ada 2012 — единственный промышленный язык, в котором «контракт» является частью стандарта.

Среди видов проверки корректности работы ПО, или верификации, наиболее широко применяемым является его тестирование. Однако, по словам исследователя компьютерной отрасли Эдсгера Дейкстры (Edsger Wybe Dijkstra), тестирование может показать наличие ошибок, но не может доказать их отсутствие. Для доказательства отсутствия ошибок в ПО применяются формальные (математические) методы, которые анализируют требования к ПО и исходный код ПО и подтверждают, что ПО делает то, что от него требуется, и не делает того, что не требуется. Этот процесс называется «формальной верификацией» и используется для верификации сертифицируемого ПО и доказательства сертифицирующему органу, что ПО не содержит ошибок. Применение такой верификации рекомендуется сертифицирующими органами и, возможно, в будущем станет обязательным при сертификации по стандартам безопасности ПО.

Проблема состоит в том, что далеко не все возможности современных языков программирования поддаются формальной верификации. Решить ее можно путем использования ограниченного подмножества языка. Но тогда возникает другая сложность: формально верифицируемое подмножество языка получается настолько «бедным», что не находит практического применения в реальных проектах. В случае Ada 2012 удалось решить обе эти проблемы: было создано формально верифицируемое подмножество языка с достаточной для практического применения функциональностью. Это подмножество назвали SPARK (ИСКРА), и сегодня его действующей версией на базе Ada 2012 является SPARK 2014.

Компания AdaCore, основанная в 1994 г., производит компилятор и различные средства разработки для языка Ada и средства формальной верификации для языка SPARK. Поддерживаются информационные ресурсы по Ada 2012 [1] и SPARK 2014 [2], а также образовательный ресурс [3], содержащий учебные курсы по программированию на языках Ada и SPARK. Для выполнения заданий учебных курсов доступна бесплатная версия компилятора Ada и среды разработки.

В русскоязычном Интернете работает технический ресурс для разработчиков [4]. Недавно там был опубликован перевод книги Джона Барнса «Безопасное и надежное программное обеспечение на примере языка Ада 2012, SPARK 2014».

Дистрибьютор компании AdaCore в России — компания «АВД Системы», поставщик средств разработки ПО критически важных для безопасности сертифицируемых встраиваемых компьютерных систем.

ЛИТЕРАТУРА

1. www.ada2012.org
2. www.spark-2014.org
3. www.university.adacore.com
4. www.ada-ru.org