ПРОГРАММНОЕ ОБЕСПЕЧЕНИЕ БЕЗ ОШИБОК? ЯЗЫК ADA 2012

Язык программирования Ada был разработан в начале 80-х годов. Целью разработки было создание языка для встраиваемых систем реального времени с повышенными требованиями к надежности ПО. В 1983 году язык становится стандартом ANSI/MIL-STD-1815A, а в 1987 году - международным стандартом ISO 8652. Эта первая версия языка, называемая Ada 83, стала стандартом ГОСТ 27831-88 во времена бурного внедрения языка Ada в СССР при поддержке ГКНТ (Государственного Комитета по Науке и Технике Совета Министров СССР).

В дальнейшем языку Ada в России не повезло – в 90-х годах нам всем стало не до языков программирования. А в остальном мире язык продолжал развиваться и совершенствоваться (Ada 95, Ada 2005) и сегодняшняя версия Ada 2012 является действующим международным стандартом ISO 8652:2012. Во всем мире Ada является основным языком разработки ПО встраиваемых компьютерных систем, критически важных для безопасности.

Критически важной для безопасности является компьютерная система, некорректная работа которой несет угрозу здоровью или жизни людей (например, авария на транспорте), или может нанести существенный ущерб окружающей среде (например, выброс на вредном производстве) или чревата значительным экономическим ущербом (например, потерей космического аппарата). Компьютеров, критически важных для безопасности, становится вокруг нас все больше, наша жизнь все больше зависит от их корректной работы, и отсутствие ошибок в их встроенном программном обеспечении становится все важнее. Поэтому различные отрасли ввели сертификацию программного обеспечения по специальным отраслевым стандартам безопасности ПО, таким как DO-178 (авионика), IEC 61508 (промышленное оборудование), EN 50128 (железнодорожные системы), ISO 26262 (автоэлектроника) и IEC 62304 (медицинское оборудование).

Каждая новая редакция стандарта языка Ada усиливала его позицию как языка, наиболее подходящего языка для разработки критически важного для безопасности ПО. Вот и Ada 2012 продолжил эту традицию. Основным дополнением к стандарту стал «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 для проверки того, что программный модуль делает именно то, что написано в условиях «контракта». Идея «контрактного программирования» не нова, но Ada 2012 – единственный промышленный язык, в котором «контракт» является частью стандарта языка.

Проверка корректности работы ПО называется верификацией. Наиболее широко применяемым видом верификации ПО является его тестирование. Но как сказал исследователь компьютерной отрасли Эдсгер Дейкстра, 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 применяется для верификации сертифицируемого ПО и доказательства сертифицирующему органу, что ПО не содержит ошибок. Применение формальной 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 эту проблему можно путем использования ограниченного подмножества языка. Но тут возникает другая проблема: формально верифицируемое подмножество языка получается настолько «бедным», что не находит практического применения в реальных проектах. В случае Ada 2012 удалось решить обе эти проблемы: создано формально верифицируемое подмножество языка с достаточной для практического применения функциональностью. Это подмножество назвали SPARK (ИСКРА), и его действующая на сегодняшний день версия на базе Ada 2012 называется SPARK 2014.

Компания AdaCore (www.adacore.com), основанная в 1994 году, производит компилятор и различные средства разработки для языка Ada и средства формальной верификации для языка SPARK. Поддерживаются информационные ресурсы по Ada 2012 (www.ada2012.org) и SPARK 2014 (www.spark-2014.org), а также образовательный ресурс http://university.adacore.com, 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 www.ada-ru.org. Недавно там был опубликован перевод книги Джона Барнса «Безопасное и надежное программное обеспечение на примере языка Ада 2012, SPARK 2014».

На странице www.adacore.com/tech-do-178c можно загрузить руководство по применению средств разработки компании AdaCore - «AdaCore Technologies for DO-178C/ED-12C». В руководстве рассматриваются четыре сценария применения продуктов AdaCore при разработке и верификации ПО по авиационным требованиям DO-178C/ED-12C:

1. Разработка на языке Ada 2012 без применения объектно-ориентированных технологий (ООТ) согласно основному стандарту DO-178C/ED-12C;

2. Разработка на языке Ada 2012 с применением объектно-ориентированных технологий (ООТ) согласно дополнительному стандарту DO-332/ED-217 «Object-Oriented Technologies and Related Technologies»;

3. Модельно-ориентированная разработка с применением квалифицированного кодогенератора QGen согласно дополнительному стандарту DO-331/ED-218 «Model-Based Development and Verification»;

4. Использование языка SPARK и формальной верификации согласно дополнительному стандарту DO-333/ED-216 «Formal Methods».

Дистрибьютор компании AdaCore в России – компания АВД Системы (www.avdsys.ru), поставщик средств разработки программного обеспечения критически важных для безопасности сертифицируемых встраиваемых компьютерных систем.