РАЗРАБОТКА ТРЕБОВАНИИ К ФУНКЦИОНАЛЬНОМУ ПРОГРАММНОМУ ОБЕСПЕЧЕНИЮ КРИТИЧНЫХ ПО БЕЗОПАСНОСТИ СИСТЕМ С ИСПОЛЬЗОВАНИЕМ ФОРМАЛЬНЫХ СПЕЦИФИКАЦИЙ

О.О. Бойкова, Г.И. Герасимов, И.А. Мезенцев, А.С. Никулин, М.И. Орехов
ОАО "Раменское приборостроительное конструкторское бюро"

Надежность функционирования системы находится в зависимости от функциональных требований к программному обеспечению системы. Проблема, рассматриваемая в работе, - представление требований в таком виде, который бы позволил анализировать их для исключения неоднозначности и противоречий.

DEVELOPMENT OF FUNCTIONAL SOFTWARE REQUIREMENTS FOR SAFETY CRITICAL SYSTEMS WITH USE OF FORMAL SPECIFICATION

O.O. Boykova, **G.I.** Gerasimov, LA. Mezentsev. A.S. **Nikulin, M.I. Orehov**

The safety of system under development depends on quality of functional software requirements for this system. Problem disclosed in the research covers representation of requirements with use of formal specification and justification ofunambiguity and consistency of requirements.

Проблема определения и анализа функциональных требований к программному обеспечению актуальна при разработке критичных по безопасности систем. Учитывая, что требования современных российских [1] и международных стандартов на разработку и документирование программного обеспечения встроенных систем, а также квалификационные требования международных сертифицирующих организаций [2] выделяют процесс определения требований в важный первоначальный этап разработки, встает задача формирования методик описания и анализа функциональных требований для исключения неоднозначности, противоречивости и неопределенности условий. Спецификация, как результат процесса определения требований, является исходным документом для процессов проектирования и квалификационного тестирования программного обеспечения. Таким образом, форма представления требований должна способствовать общему однозначному их пониманию среди всех участников проекта.

В настоящее время изложение функциональных требований к программному обеспечению, как правило, осуществляется в повествовательной форме. Требования технического задания на разработку программного обеспечения комплексов пилотажно-навигационного оборудования носят декларативный характер и могут рассматриваться как перечень решаемых задач, логика реализации которых должна быть изложена в дополнительных документах. Логики функционирования комплексов пилотажно-навигационного оборудования в различных режимах работы содержат конкретизацию требований технического задания, но требования, изложенные в этих документах, как правило, рассматривают как тесно связанные те компоненты программного обеспечения, разработка и квалификационное тестирование которых должны проводиться отдельно. Такая форма представления значительно затрудняет анализ іребований.

Программное обеспечение комплексов пилотажно-навигационного оборудования относится к классу критических по безопасности систем. Функциональные требования к подобным системам должны быть однозначны и непротиворечивы. Форма представления требований должна обеспечивать возможность их анализа, в том числе автоматического с использованием ЭВМ. В связи с этим в процессе определения требований предлагается использовать формальные спецификации. Формальные спецификации обеспечивают более строгое представление, основанное на использовании математического аппарата, и, таким образом, могут быть использованы для математического обоснования полноты спецификаций и правильности их исполнения. Формальные спецификации используют математическую нотацию для точного описания свойств, которыми должна обладать информационная система, без чрезмерного ограничения метода их реализации. Формальные спецификации описывают, что система должна делать, без указания того, как она должна это делать. Такая абстракция делает формальные спецификации полезными в процессе разработки компьютерных систем, так как позволяет уверенно отвечать

на возможные вопросы о функциональности системы, без необходимости углубления в детали программного кода или размышлений о значении фраз, содержащихся в словесном описании [3]. Формальная спецификация может служить общей надежной базой для аналитиков (тех, кто исследует потребности заказчика), программистов (тех, кто реализует программы, чтобы удовлетворить потребности заказчика), тестировщиков (тех, кто проверяет результаты) и технических писателей (тех, кто пишет инструкции по использованию системы). Независимость от исходного кода позволяет формальной спецификации быть завершенной на ранних этапах разработки. Хотя, возможно, она будет нуждаться в корректировке по мере того, как развиваются потребности заказчика, и углубляется понимание задачи командой разработчиков. Формальная спецификация может быть ценным средством, способствующим общему пониманию среди всех заинтересованных сторон проекта. Применение формальных методов дает возможность строгой проверки, позволяющей избавиться от ошибок, которые могут быть допущены при текстовом описании требований. Однако, применение формальных методов не означает отказ от словесного описания, но каждое требование, описанное словами, соответствует формальному, т.е. максимально точному и выразительному, представлению.

В РПКБ для составления формальных спецификаций была реализована методика, которая использует Z - нотацию [4]. Эта нотация, т.е. формальное описание требований, основана на логике предикатов и теории множеств. Один из способов использования математической нотации для достижения обозначенных целей - моделирование системы с помощью математических объектов (множеств, отображений, кортежей, последовательностей, декартовых произведений и т.д.).

Нотация позволяет определять функции и операции для обработки данных этих типов. Такие объекты не ориентированы на машинное представление, но они подчиняются многообразным математическим законам, которые позволяют эффективно рассуждать о поведении указанной системы. Логика предикатов используется для абстрактного описания результатов каждого действия в нашей системе. Другая важная составная часть в Z- методе - декомпозиция спецификации на небольшие части, называемые схемами. Разделяя спецификацию на схемы, можно представлять ее последовательно, часть за частью. Каждая часть может быть связана с комментарием, который в свободном стиле поясняет смысл формальной математики. Схемы используются для описания как статических (возможные состояния и постоянные соотношения, которые поддерживаются системой при переходе от состояния к состоянию), так и динамических (возможные операции, отношения между входными и выходными данными, возможные изменения состояния) аспектов системы. Язык схем позволяет описать различные части системы раздельно, а затем связать и объединить их. Спецификации Z - метода представляют собой набор схем, которые являются описаниями сущностей и связей между ними. Схемы, таким образом, обеспечивают среду для разработки спецификаций системы и их постепенного развития и уточнения. Использование схем для описания преобразований от общего представления системы к более детальному позволяет обосновать корректность спецификации, содержащей больше деталей конкретного проекта, которая реализует абстрактную спецификацию. Создавая последовательность спецификаций, каждая из которых содержит больше деталей, чем предыдущая, в конечном счете можно получить настолько детальную спецификацию, полностью удовлетворяющую начальной абстрактной спецификации, что она будет являться программой [3].

Разработанная Спецификация требований к функциональному программному обеспечению комплекса пилотажно-навигационного оборудования в части решения задач навигации с использованием формальных математических спецификаций, записанных в Z-нотации, является первым опытом разработки в РПКБ спецификации требований к функциональному программному обеспечению. Практическая значимость заключается в том, что форма представления требований, разработанных по представляемой методике, обеспечивает возможность повторного использования и анализа их, в том числе автоматического с использованием ЭВМ. Полученные формальные спецификации могут быть использованы для частичной автоматизации процессов проектирования и квалификационного тестирования функционального программного обеспечения.

Использование формальных спецификаций и точных математических методов связано с увеличением трудоемкости. Однако, стоимость применения этих методов оправдана при разработке программного обеспечения критических систем, там, где потенциальные человеческие и финансовые потери могут быть значительными - атомная энергетика, транспорт, военная техника.

СПИСОК ЛИТЕРАТУРЫ

1. ***ГОСТ*** Р 51904-2002 Программное обеспечение встроенных систем. Общие требования к разработке и документированию.
2. *RTCA/DO-178* Software Considerations in Airborne Systems and Equipment Certification.
3. *J.M. Spivey,* The Z Notation: A Reference Manual, Oriel College, Oxford, 0X1 4EW, England, 1998.
4. ***ISO/IEC*** 13568 Information technology - Z formal specification notation - Syntax, type system and semantics.