

Оценка степени безопасности программ в специализированных языках программирования

Розов Андрей Сергеевич

Институт автоматизации и электрометрии СО РАН (Новосибирск), Россия
e-mail: deadproger@gmail.com

Несмотря на то что большая часть программного обеспечения в настоящее время разрабатывается с использованием языков программирования общего назначения, таких как Java и C++, в областях, требующих высокой надежности и сопровождаемости программных систем, широко распространено использование специализированных языков программирования. Преимущества специализированных языков – повышенная надежность программ, читаемость кода, простота сопровождения и модификации. Эффективное использование языка в значительной мере зависит от стиля программирования. При этом синтаксис языка не может гарантировать качество текста программ и их безопасность. Это обуславливает интерес к методикам получения численных оценок безопасности кода.

Проблема оценки безопасности рассматривается на примере разработки языка iC [1], выполненного как расширение языка C. Язык iC реализует концепцию процесс-ориентированного программирования, и предназначен для решения задач автоматизации на микроконтроллерных платформах. Анализ безопасности программ на iC предлагается разделить на три уровня: уровень гиперпроцесса, уровень процесса, и уровень состояния. На уровнях гиперпроцесса и процесса оценка безопасности программы может быть получена путем вычисления цикломатической сложности (McCabe). Оценку безопасности кода на уровне состояния предлагается выполнять следующим образом. Каждой синтаксической конструкции языка присваивается коэффициент S_i , соответствующий базовой безопасности этой конструкции, и коэффициент S_{ci} , зависящий от контекста (значения коэффициентов лежат в области от 0 до 1). Наличие коэффициента S_{ci} обусловлено зависимостью уровня безопасности конструкции от контекста ее использования. Общая безопасность участка кода вычисляется как произведение безопасностей всех входящих в него конструкций.

Полученные таким образом оценки безопасности могут быть использованы для выявления проблемных участков кода и последующего указания на них программисту, например, путем цветового выделения небезопасного синтаксиса. В продолжение работы предполагается разработка критериев задания коэффициентов S_i и S_{ci} , разработка методик анализа контекста использования синтаксических конструкций, и исследование эффективности применения полученных оценок для увеличения общего качества кода.

Список литературы

1. Розов А.С. "Опыт использования процесс-ориентированного подхода при автоматизации на платформе Arduino" // XIII Всероссийская конференция молодых ученых по математическому моделированию и информационным технологиям, Новосибирск, 15-17 октября 2012, С. 60-61