УДК 004.052.42

Б.М. КОНОРЕВ, В.В. СЕРГИЕНКО, Ю.Г. АЛЕКСЕЕВ, Г.Н. ЧЕРТКОВ

Сертификационный центр АСУ, Украина

МОДЕЛЬ ИНВАРИАНТО-ОРИЕНТИРОВАННОЙ ОЦЕНКИ ХАРАКТЕРИСТИК КАЧЕСТВА ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ

В статье рассматривается использование формальных методов контроля неизменных свойств (инвариантов) программного обеспечения (ПО) для оценки характеристик качества ПО. Рассматривается влияние дефектов на значения инвариантов на уровне исходных кодов ПО. По результатам измерения инвариантов определяется наличие остаточных дефектов в программе. Приведена динамическая модель чувствительности набора методов к дефектам с учетом операционного спектра конкретного проекта. Предлагаемый подход позволяет формализовать проверки и автоматизировать процесс оценки основополагающих характеристик качества ПО таких, как функциональная надежность и безопасность.

Ключевые слова: *программное обеспечение, качество, тестирование, верификация, модели программного обеспечения, инвариант, профиль дефектов.*

Введение

При объективных оценках корректности критического программного обеспечения (ПО) необходимым является использование формальных методов. Такой подход обеспечивает достоверность результатов и полноту оценки, позволяет минимизировать субъективное влияние эксперта (человеку свойственно ошибаться) на результат оценки. Для оценки характеристик качества ПО в ХХП «Сертификационный центр АСУ» (г. Харьков) ведется разработка технологии независимой верификации критического ПО [1]. Технология основана на проверке корректности ПО с помощью моделей ПО, с использованием автоматизируемых формальных методов [2,3]. Модели ПО позволяют измерить определенные инварианты, - неизменные свойства ПО, представляющие собой реализацию в ПО требований нормативной и конструкторской документации. По результатам измерения сохранности инвариантов определяется наличие в ПО остаточных дефектов. Предлагаемый в статье подход обеспечивает разнообразие и независимость процесса верификации при оценке качества ПО.

Основная часть

Программному обеспечению присущи дефекты. Дефект (fault) в программе является следствием ошибок разработчика на любом из этапов разработки и может содержаться в исходных или проектных спецификациях, текстах кодов программ, эксплуатационной документация и т.п. [4]. Дефект проявляется в процессе выполнения программы и может привести ПО к отказу (неработоспособному или некорректному состоянию).

Для контроля бездефектности ПО предлагается использовать подход, основанный на контроле сохранности инвариантов. Конечный программный продукт может быть представлен как модель, реализующая все требования технического задания, алгоритмов, нормативной документации к данному продукту. При этом каждое требование реализуется в ПО в виде одного или нескольких инвариантов – неизменных свойств ПО, подтверждающих выполнение этого требования (необходимое условие). Для оценки сохранности инвариантов (и, соответственно, подтверждения реализации требований) строятся редуцированные модели, в которых отсутствуют программные конструкции, не относящиеся к данному инварианту. При этом каждая такая модель должна сохранять всю информацию, необходимую для контроля сохранности инварианта. Для измерения сохранности инвариантов в созданной модели ПО в местах, чувствительных к изменению инварианта устанавливаются «зонды». В случае фиксации нарушения значения инварианта выдается информация для дальнейшего анализа.

Изменение значения инварианта в местах установки «зондов» говорит о наличии в программе дефектов. При этом не каждый дефект способен влиять на изменение инварианта. Чтобы определить какие дефекты влияют на значение инварианта и следовательно, содержатся ли данные дефекты в ПО, разрабатывается профиль дефектов (ПД), который характерен для конкретного сочетания опе-

рандов и операций исследуемого проекта.

Использование профиля дефектов для калибровки (процедуры оценки чувствительности и степени разнообразия методов контроля сохранности инвариантов) путем многократного точечного («капельного») внесения и обнаружения тестовых дефектов из ПД позволит выбрать оптимальный набор методов для достижения заданного уровня бездефектности (степени покрытия).

Для каждого типа дефектов необходимо установить влияние на сохранность инвариантов. Для измерения должны быть отобраны инварианты, которые искажаются при наличии возможных для конкретного проекта типов дефектов. Таким образом, для оценки бездефектности ПО необходимо сформировать профиль инвариантов – перечень инвариантов, учитывающий особенности данного проекта.

Общая модель инварианто-ориентированной оценки бездефектности ПО ИУС представлена на рис.1.

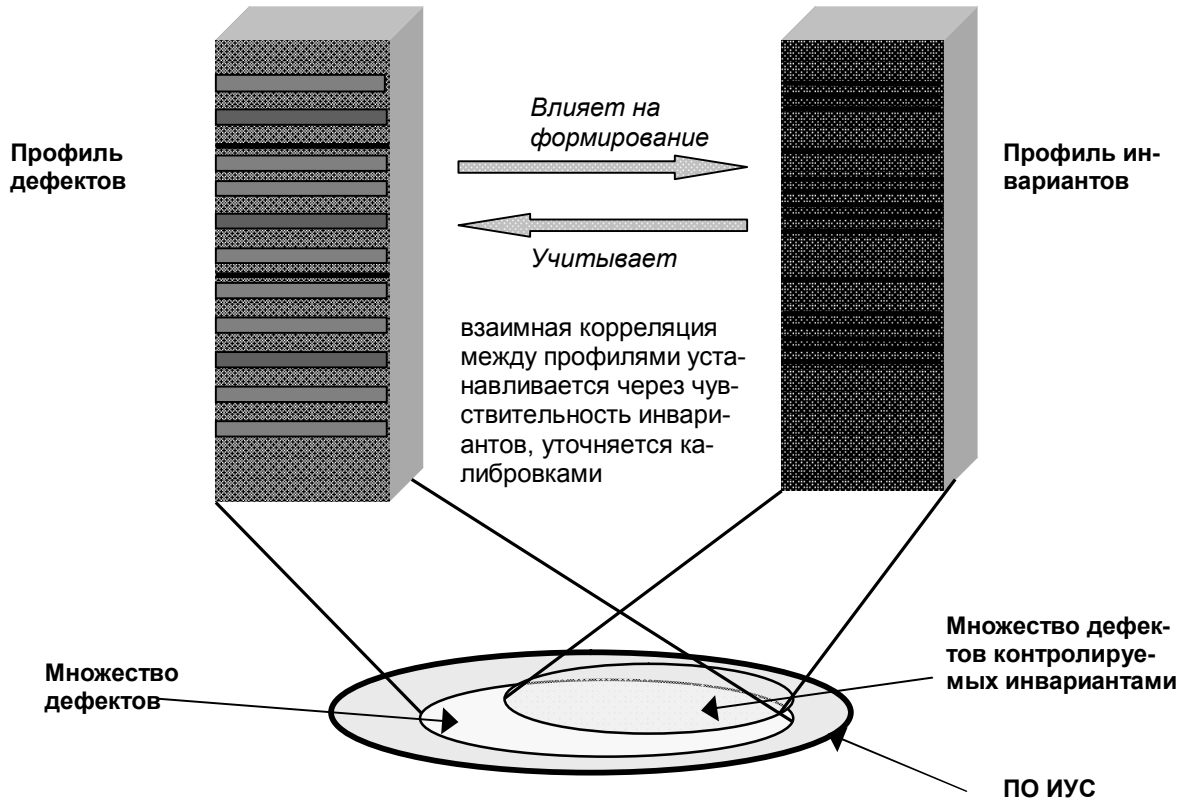

Рис. 1. Модель инварианто-ориентированной оценки бездефектности ПО ИУС

Модель позволяет определить интегральную проверяющую способность композиции диверсных технологий верификации, основанных на измерении числовых, семантических, логических и др. инвариантов. Модель инварианто-ориентированной оценки позволяет формализовать проверки и автоматизировать процесс оценки основополагающих характеристик качества ПО таких, как функциональная надежность и безопасность и, таким образом, убрать фактор субъективного влияния эксперта (оценщика) на результат.

Возможное взаимное расположение множеств дефектов в виде диаграмм Эйлера-Венна с математическим описанием было ранее рассмотрено в [5].

Необходимо отметить, что в случае обнаружения нарушения сохранности инварианта реализация требования уточняется. Вносятся необходимые изменения, и процедура контроля повторяется.

Если какие-либо инварианты не установлены или измерение их сохранности не реализовано, тогда необходимо использовать альтернативные методы проверки: динамическое тестирование, проверка кода вручную («за столом») и т.д. Упрощенно алгоритм оценки характеристик качества критического ПО с использованием инвариантов представлен на рис.2.

В терминах исходного кода модели для измерения инвариантов представляются набором операций и операндов. Таким образом, при выборе моделей и методов для контроля сохранности инвариантов необходимо учитывать операционный спектр конкретного проекта. Более пристальное внимание

необходимо уделить контролю конструкций (операндам и операциям), которые встречаются чаще в конкретном проекте и для которых возможно большее количество видов искажений. Для доказательства этого рассмотрим появление дефекта в коде ПО как некоторое случайное событие.

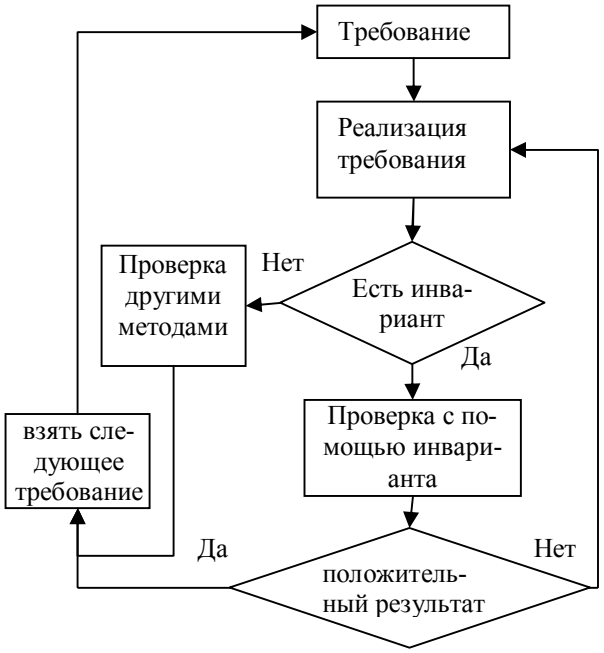

Рис. 2 Процедура оценки качества критического ПО с помощью инвариантов

Появление дефекта в последовательности переходов между операциями и операндами обладает следующими свойствами: ординарностью, т.к. дефекты появляются поодиночке; отсутствием последействия, т.к. для любых неперекрывающихся участков кода количество дефектов является независимой случайной величиной, т.е. вероятность попадания любого количества дефектов не зависит от того, сколько их попало на другие; стационарностью, т.к. вероятностные характеристики не меняются в адресном пространстве ПО, и вероятность попадания определенного количества дефектов на участок кода зависит только от длины участка и не зависит от расположения.

Вследствие того, что поток дефектов обладает свойствами ординарности, стационарности и отсутствия последействия, он является простейшим, или стационарным пуассоновским потоком, что позволяет для исследования свойств ПО использовать методы теорий случайных функций и случайных процессов.

Модель, описывающая способность набора методов контролировать корректное состояние ПО в виде переходов состояний представлена на рис. 3.

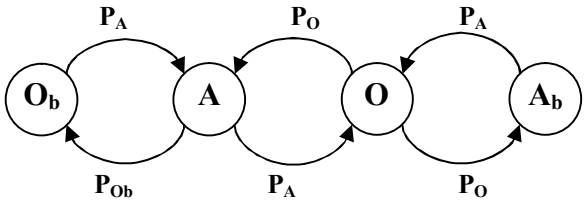

Рис. 3. Граф переходов

A, A_b – корректный/некорректный операнд (вершина графа),

O, O_b – корректная/некорректная операция (ветка графа),

P_i – вероятности переходов из одного состояния в другое.

Модель позволяет записать систему линейных алгебраических уравнений (СЛАУ), описывающих потоки вероятностей для каждого из статических состояний узлов:

$$\begin{cases} C_{Ob} * P_A = C_A * P_{Ob} \\ C_A * (P_O + P_{Ob}) = C_{Ob} * P_A + C_O * P_A \\ C_O * (P_A + P_{Ab}) = C_A * P_O + C_{Ab} * P_O \\ C_{Ab} * P_O = C_O * P_{Ab} \end{cases}$$

Вероятность скрытых дефектов (не обнаруженных при испытаниях):

$P_{lat} = 1 - P(O/A) = P(A_b) + P(O_b)$.

В результате решения СЛАУ находим:

$P(A_b) = C_{Ab} / (C_O + C_{Ab} + C_{Ob} + C_A)$;

$P(O_b) = C_{Ob} / (C_O + C_{Ab} + C_{Ob} + C_A)$.

Таким образом:

$Plat = (C_{Ab} + C_{Ob}) / (C_O + C_{Ab} + C_{Ob} + C_A)$.

Учитывая большой объем анализируемого программного кода, можно рассматривать процесс статического анализа как непрерывный процесс и перейти от вероятностных характеристик к интенсивностям. И тогда из последней формулы можно заметить, что возможность появления скрытого дефекта пропорционально зависит от количества возможных искажений состояния (операндов и операций) данного типа, что и требовалось доказать.

Заключение

Разработанная модель инвариантно-ориентированной оценки позволяет определить интегральную проверяющую способность композиции диверсных технологий верификации, основанных на измерении числовых, семантических, логических и др. Инвариантов. Модельный подход позволяет формализовать проверки и автоматизировать процесс оценки основополагающих характеристик качества ПО

таких, как функциональная надежность и безопасность и, таким образом, убрать фактор субъективного влияния эксперта (оценщика) на результат.

Литература

1. Конорев Б.М. Целевая технология рентабельной оценки надежности и функциональной безопасности критического программного обеспечения / Б.М. Конорев, Ю.Г. Алексеев, В.В. Сергиенко, В.С. Харченко, Г.Н. Чертков // Радіоелектронні і комп'ютерні системи. – 2007. – №6 (25). – С. 162-170.

2. Конорев Б.М. Инвариантно-ориентированная оценка качества программного обеспечения космических систем / Под ред. Конорева Б.М., Харченко В.С. – Х: ГП Госцентркачества, Национальный аэрокосмический университет им. Н.Е. Жуковского «ХАИ», 2009. – 224 с.

3. Кларк Э.М. Верификация моделей программ: Model Checking / Э.М. Кларк, О. Грамберг, Д. Пелед. Пер. с англ. Под ред. Р. Смелянского. – М.: МЦНМО, 2002. – 416 с.

4. IEEE Std. 610.12-1990, IEEE Standard Glossary of Software Engineering Terminology. Approved September 28,1990 by IEEE Standards Board.

5. Конорев Б.М. Доказательная независимая верификация и оценка скрытых дефектов критического программного обеспечения на основе диверсифицированного измерения инвариантов / Б.М. Конорев, В.В. Сергиенко, Г.Н. Чертков, Ю.Г. Алексеев // Радіоелектронні і комп'ютерні системи. – 2009. – №7(41). – С. 192-199.

Поступила в редакцию 26.02.2010

Рецензент: д-р техн. наук, проф. А.Л. Ляхов, Полтавский национальный технический университет им. Ю. Кондратюка, Полтава, Украина.

МОДЕЛЬ ІНВАРІАНТО-ОРІЄНТОВАНОЇ ОЦІНКИ ХАРАКТЕРИСТИК ЯКОСТІ ПРОГРАМНОГО ЗАБЕЗПЕЧЕННЯ

Б.М. Конорев, В.В. Сергієнко, Ю.Г. Алексеєв, Г.М. Чертков

У статті розглядається використання формальних методів контролю незмінних властивостей (інваріантів) програмного забезпечення (ПЗ) для оцінки характеристик якості ПЗ. Розглядається вплив дефектів на значення інваріантів на рівні вихідних кодів ПЗ. За результатами виміру інваріантів визначається наявність залишкових дефектів у програмі. Наведено динамічну модель чутливості набору методів до дефектів з урахуванням операційного спектра конкретного проекту. Запропонований підхід дозволяє формалізувати перевірки й автоматизувати процес оцінки основних характеристик якості ПЗ таких, як функціональна надійність і безпека.

Ключові слова: програмне забезпечення, якість, тестування, верифікація, моделі програмного забезпечення, інваріант, профіль дефектів.

INVARIANT-ORIENTED MODEL FOR SOFTWARE QUALITY CHARACTERISTICS ASSESSMENT

B.M. Konorev, V.V. Sergiyenko, U.G. Alexeev, G.N. Chertkov

The present article is concerned with formal methods of software invariable properties (invariants) check for software quality characteristics assessment. The effect of faults on invariant values at the level of source codes is considered. By results of invariants measurement the presence of residual faults in software is defined. The dynamic model of sensitivity of methods to software faults taking into account an operational spectrum of the specific project is presented. The offered approach allows to formalize checking process and automate process of estimation of basic software quality characteristics such as functional reliability and safety.

Keywords: software, quality, testing, verification, software models, invariant, profile of faults.

Конорев Борис Михайлович – д-р техн. наук, проф.., проф. кафедры программного обеспечения компьютерных систем, Национальный аэрокосмический университет им. Н.Е. Жуковского «ХАИ», Харьков, Украина, e-mail: admin@scasu.com.

Сергиенко Владимир Владимирович – руководитель испытательной лаборатории, Сертификационный центр АСУ ГП Госцентркачества, Харьков, Украина, e-mail: admin@scasu.com.

Чертков Георгий Николаевич – директор, Сертификационный центр АСУ ГП Госцентркачества, Харьков, Украина, e-mail: scasu@scasu.com.

Алексеев Юрий Гаврилович – нач. отд. экспертизы ПО и ПТК, Сертификационный центр АСУ ГП Госцентркачества, Харьков, Украина, e-mail: ugalex@scasu.com.