

## **Отзыв официального оппонента**

на диссертацию Кривчикова Максима Александровича «Формальные модели и верификация свойств программ с использованием промежуточного представления», представленную на соискание ученой степени к.ф.-м.н. по специальности 05.13.17 — теоретические основы информатики (физико-математические науки)

### **Актуальность темы диссертации**

Диссертация М.А. Кривчикова «Формальные модели и верификация свойств программ с использованием промежуточного представления» рассматривает задачу описания формальных моделей программ, которая входит в область формальной верификации программного обеспечения. Результаты, полученные в этой области, направлены на повышение качества программ в части обеспечения их соответствия поставленным требованиям. Исследования в области методов формальной верификации ведутся в течение последних нескольких десятилетий. На настоящее время выделяют теоретико-модельные (model checking) и теоретико-доказательные (дедуктивные) методы формальной верификации. Диссертационное исследование посвящено развитию теоретико-доказательных методов на направлении программирования с зависимыми типами, начало развития которого можно отнести к концу 1980-х годов.

В диссертации автор рассматривает применение методов верификации с зависимыми типами в отношении сложных программных комплексов, написанных с использованием нескольких языков программирования. Целью диссертационного исследования является получение промежуточного представления, предназначенного для формальной верификации таких программ. Тема исследования является актуальной согласно следующим обстоятельствам. Во-первых, на практике существует потребность в снижении количества ошибок в программном обеспечении информационных систем критически важных объектов, однако уровень развития таких методов на настоящее время не позволяет удовлетворить эту потребность. Во-вторых, при разработке сложных программных комплексов достаточно часто используются несколько языков программирования, что не учитывается в традиционно используемых методах верификации.

### **Общая оценка работы**

Диссертация состоит из введения, пяти глав, заключения и списка литературы.

В введении обоснована актуальность и практическая значимость темы исследования, отмечена цель исследования и перечислены поставленные автором задачи. Кроме того, введение содержит описание методов и характеристику полученных автором результатов, включая их научную новизну, теоретическую и практическую значимость.

В первой главе приведен обзор исторических и современных публикаций по теме диссертации. Отмечена предыстория исследований и вопросы, актуальные для задач описания формальных моделей программ. Автор анализирует и обобщает существующие результаты и делает выводы о возможных дальнейших направлениях развития используемых методов. В заключении главы представлена постановка задач исследования, для которых отмечены предпосылки к их возникновению и потенциальные направления приложения результатов.

Вторая глава диссертации содержит описание новой, предложенной автором разновидности лямбда-исчисления с зависимыми типами, поддерживающего нетривиальные типы идентичности с помощью дополнительных правил редукции. В первом разделе рас-

смотрена известная разновидность исчисления — расширенное исчисление конструкций. На основе расширенного исчисления конструкций во втором разделе автор вводит дополнительные термы и правила их редукции. Для предложенных правил приведено доказательство их основных свойств, а для общей совокупности правил доказано две теоремы, которые обеспечивают редукцию отдельных термов.

В третьей главе описываются результаты реализации программного средства, предназначенного для проверки типов (спецификаций) предложенной автором разновидности лямбда-исчисления с зависимыми типами, и промежуточного представления на основе этой разновидности. В первом разделе представлены расширения исчисления, необходимые для его использования в качестве промежуточного представления. Второй раздел содержит детали реализации, а также выводы по итогам реализации программного средства.

Четвёртая глава посвящена описанию статической формальной семантики существующего промежуточного представления, соответствующего стандарту ECMA-335. Статическая семантика дополняется динамической для некоторого подмножества стандарта. Это позволяет автору исследовать применимость полученных методов и средств в приложении к описанию формальной семантики фрагмента существующего комплекса математического моделирования физических процессов.

В пятой главе представлена модель отдельного аспекта динамической семантики современных программ — модель динамического параллельного исполнения. С учетом ограничений, наложенных на рассматриваемые программы, модель обладает свойствами, обеспечивающими корректность параллельного исполнения. Сформулированные и доказанные свойства используют дополнительные термы, представленные во второй и третьей главах. В завершающем разделе представлены результаты применения модели к примеру из четвертой главы.

Автор использует в диссертации методы теории категорий, теории доменов, математической логики и теории доказательств, теории графов, функционального программирования и программной инженерии.

К диссертации прилагается автореферат на 24 страницах, в полной мере отражающий содержание диссертации и ее основные положения. Основные результаты диссертации опубликованы в открытой печати в 11 работах, в том числе, в 5 статьях в центральных изданиях из Перечня ВАК.

**Научная новизна.** В диссертации предложен новый подход к построению формальных моделей программ, написанных на нескольких языках программирования, использующий промежуточное представление. Такое промежуточное представление основано на разновидности лямбда-исчисления с зависимыми типами, использующей новые предложенные автором правила редукции. С использованием промежуточного представления автором получены следующие результаты в области описания формальных моделей программ: новая модель статической семантики управляемого кода стандарта ECMA-335 и модель динамического параллельного исполнения программ, составленных из функций, не имеющих побочных эффектов. Полученные результаты применения промежуточного представления, в том числе — к фрагментам исходного кода существующих, используемых на практике программных комплексов, позволяют утверждать, что предложенный подход по сравнению с существующими обладает преимуществами в задачах описания формальных моделей программ, разрабатываемых с использованием нескольких языков программирования.

**Значимость представленных результатов** определяется тем обстоятельством, что предложенное промежуточное представление может быть использовано для описания программ, написанных с использованием нескольких языков программирования. Теоретические результаты, в частности — разновидность лямбда-исчисления с зависимыми типами совместно с полученным автором доказательством отдельных свойств исчисления, — могут найти применение в других областях математики, в том числе и в математической логике. Представленные результаты были реализованы автором в форме макета программного средства для ЭВМ, которое использовалось для проверки полученных результатов.

**Достоверность и обоснованность** полученных автором результатов обеспечивается строгими математическими формулировками и доказательствами ряда лемм и теорем, отражающих положения, выносимые на защиту.

**Результаты исследования могут представлять интерес** для сотрудников научных организаций, работающих в области формальных методов программной инженерии, а также для предприятий, выполняющих разработку программного обеспечения с высокими требованиями по их верификации. Основные результаты прошли апробацию на ряде научных и научно-практических конференций, а также научных семинаров на механико-математическом факультете и факультете вычислительной математики и кибернетики МГУ им. М.В. Ломоносова, в ИСП РАН, ИМ СО РАН, ИСИ СО РАН. В диссертации представлены результаты тестов на фрагменте программного комплекса моделирования теплогидравлических процессов в реакторах АЭС, которые были проведены в рамках совместной научно-исследовательской работы Института механики МГУ и ОАО «ВНИИА-ЭС».

#### **Замечания и пожелания по диссертации**

Следует отметить, что в работе не проведено полного теоретического исследования свойств предложенной разновидности лямбда-исчисления (например, свойство нормализации).

В разделах 3.1.4 и 3.1.5 используются разные методы валидации схемы описания индуктивных и коиндуктивных типов: непосредственное доказательство ожидаемых свойств и определение объекта с использованием схемы в среде Соq, соответственно. В то же время автор отмечает, что для задания коиндуктивных типов используется схема, аналогичная случаю индуктивных типов. Поэтому целесообразным было бы использование обоих методов валидации для каждой схемы.

Автором не получены оценки сложности разработанных алгоритмов, в частности, реализующих схему проверки типов.

В диссертации содержится также незначительное количество опечаток и грамматических ошибок, что не удивительно с учетом ее значительного объема. Например, во Введении (как и в автореферате) указано, что диссертация состоит из 4-х глав, в то время как фактически их 5.

Перечисленные недостатки не являются существенными для диссертационной работы в целом и не снижают ценности полученных в ней результатов.

## **Заключение**

Диссертация является завершенной научно-квалификационной работой, в которой содержится решение задачи описания формальных моделей программ, написанных с использованием нескольких языков программирования, с целью выполнения формальной верификации. Предложенное автором решение этой задачи вносит весомый вклад в развитие теоретической информатики и может найти применение на практике в задачах контроля качества программного обеспечения критически важных объектов.

Основные результаты, представленные в диссертации, в достаточной степени отражены в публикациях в центральных изданиях, в том числе в журналах, входящих в Перечень ВАК. Результаты были апробированы на ряде международных конференций и научных семинаров в ведущих научных организациях.

Диссертация соответствует п.п. 9–14 Положения о присуждении ученых степеней, а автор, М.А. Кривчиков, заслуживает присуждения ему ученой степени кандидата физико-математических наук по специальности 05.13.17 — теоретические основы информатики (физико-математические науки).

## **Официальный оппонент**

заведующий кафедрой математического обеспечения ЭВМ ФГБОУ ВПО «Воронежский государственный университет»,

доктор физико-математических наук, доцент Махортов Сергей Дмитриевич  
e-mail: sd@expert.vrn.ru

394006 г. Воронеж, Университетская пл., 1

Факультет ПММ, кафедра МО ЭВМ

тел. +7 (473) 220-86-98

САТ МОСКОВСКАЯ ПРОВИНЦИЯ

ОГЛАВЛЕНИЕ