ОТЗЫВ

официального оппонента на диссертацию
Кривчикова Максима Александровича
«Формальные модели и верификация свойств программ с использованием промежуточного представления»
представленную на соискание учёной степени
кандидата физико-математических наук по специальности
05.13.17 – «Теоретические основы информатики»

В диссертации М.А.Кривчикова рассматривается область знаний формальной верификации программного обеспечения, в рамках которой решается задача получения математических моделей программ с целью дальнейшего получения математических доказательств выполнения для программ требуемых функциональных свойств. Соискатель исследует вопросы получения таких моделей с помощью методов на основе лямбда-исчисления с зависимыми типами для программ, разрабатываемых с использованием нескольких различных языков программирования. В целом, историю развития таких методов можно отследить до интуиционистской теории типов П. Мартин-Лёфа (первая половина 1970-х годов), программные реализации которой первоначально применялись в системах компьютерной математики (один из наиболее известных представителей — NuPRL, 1984 год), а в начале 1990-х годов, с появлением Исчисления Конструкций Т. Кокана (1988 год), начали использоваться и в задачах формальной верификации аппаратного и программного обеспечения.

На настоящее время исследования в области формальной верификации с использованием программирования с зависимыми типами активно ведутся. За 2014 год вышло более 100 публикаций по этой тематике в зарубежных и российских научных изданиях, тезисах докладов и материалах международных конференций. Результаты в этой области имеют высокую практическую значимость, так как могут быть использованы для получения строгих гарантий корректности программ.

Диссертация М.А. Кривчикова «Формальные модели и верификация свойств программ с использованием промежуточного представления» состоит из введения, пяти глав, разделённых на 19 параграфов, заключения, списка рисунков, списка таблиц, списка листинга, списка литературы и шести приложений. Список литературы содержит 191

наименование. Во введении и автореферате приведены 11 работ автора по теме диссертации, в том числе 5 статьи в изданиях Перечня ВАК РФ. Объем диссертации составляет 214 страниц.

Обзор диссертационной работы и отдельные замечания.

Во введении приводится достаточно подробный обзор исследований по теме диссертации, описываются цели и задачи работы, обосновывается ее актуальность и практическая значимость.

В первой главе исследуются исторические и современные публикации, содержащие результаты исследований в области описания формальных моделей программ. В результате анализа таких публикаций, соискатель делает следующие выводы: на настоящее время наличие формальной семантики языков программирования не входит в состав требований профильных комитетов по стандартизации, что обусловлено высокой наукоемкостью и значительными трудозатратами существующих методов; методы дедуктивной верификации на основе лямбда-исчисления с зависимыми типами могут применяться на практике для решения задач формальной верификации; для проведения дедуктивной верификации необходимо получить формальную модель программы. На основе этих выводов автор приводит постановку задач исследования.

Вторая глава посвящена теоретическим положениям лямбда-исчисления с зависимыми типами. Первый раздел главы имеет вводный характер, а во втором решается задача расширения исчисления новыми правилами редукции. Полученная путем такого расширения разновидность соответствует основным положениям современной разновидности конструктивной теории типов — гомотопической теории типов. Автор исследует свойства дополнительных правил редукции и получает строгие доказательства того факта, что эти свойства соответствуют ожидаемым. А именно, термы удаления элементов типов идентичности могут быть редуцированы, если известна структура шаблона подстановки, и такая редукция выполняется с сохранением типов относительно заданного при определении исчисления отношения совместимости.

В третьей главе приведены результаты реализации макета программного средства на основе полученной разновидности исчисления. В первом разделе набор термов исчисления дополняется термами, которые затем используются для описания типов данных. В число таких конструкций входят типы с конечным числом различимых элементов, натуральные числа, индуктивные и коиндуктивные типы, а также специфичные для гомотопической теории типов высшие индуктивные типы. Во втором разделе представлено решение

практических задач, связанных с реализацией макета программного средства. Автор приводит описание синтаксиса, набор основных конструкций языка формальной спецификации и соответствие таких конструкций термам исчисления. Ключевая для программного средства стадия проверки типов построена на основе известной схемы, используемой в ряде научно-исследовательских проектов.

Основное содержание **четвертой главы** связано с вопросами описания формальной семантики существующих языков программирования с использованием разработанного автором макета программного средства. Главным результатом главы является описание статической формальной семантики промежуточного кода, который используется виртуальной машиной Common Langugage Infrastructure. В дополнение к статической автор описывает динамическую формальную семантику для подмножества инструкций. Такого подмножества достаточно для описания семантики фрагмента кода из существующего программного комплекса.

В пятой главе представлены результаты приложения макета программного средства к задачам описания семантики параллельных программ. Автор предлагает на основе лямбда-исчисления с зависимыми типами модель динамического параллельного исполнения программ, которые составлены из функций, не имеющих побочных эффектов. Модель поддерживает два способа взаимодействия параллельно исполняемых потоков, а именно: порождение нового потока и ожидание завершения ранее запущенного потока с получением значения, с которым завершилось вычисление потока. Для такого набора ограничений автор доказывает свойства, гарантирующие корректность параллельного исполнения.

В заключении сформулированы основные результаты диссертации, обоснована их новизна.

В приложении А приводится краткий обзор современных исследований в области программной инженерии.

В приложении В приводится исходный код системы Coq – средства автоматизации математических доказательств.

В Приложении С представлен текст статьи С.В. Антонова, М.А. Кривчикова «Формальная модель вычислений с плавающей точкой на основе лямбда-исчисления с зависимыми типами».

В Приложении D представлен фрагмент статической формальной семантики стандарта ECMA-335, описанный в главе 4, в терминах базового языка.

В Приложении Е представлен фрагмент кода CMS, применяемый в программном обеспечении тренажёров по обучению управлением и отработке действий при чрезвычайных ситуациях персонала атомных электростанций.

В Приложении F представлено два варианта реализации модели динамического параллельного исполнения программ.

В диссертации получены следующие основные результаты:

- разновидность лямбда-исчисления с зависимыми типами, лежащая в основе гомотопической теории типов, расширена новым набором правил редукции, которые обеспечивают редукцию нетривиальных элементов типов идентичности;
- реализован макет программного средства, использующий лямбда-исчисление с зависимыми типами для описания формальных моделей программ, написанных с использованием нескольких языков программирования;
- получено новое описание статической формальной семантики управляемого кода, соответствующего стандарту ECMA-335 (Common Language Infrastructure), а для подмножества инструкций управляемого кода получена также динамическая семантика;
- предложена новая модель динамического параллельного исполнения программ, которая задана в форме модификатора семантики программ на исходном языке программирования.

Как отмечено автором в заключении, основные результаты работы могут применяться на практике в задачах верификации программ, которые могут быть представлены в виде управляемого кода стандарта ECMA-335.

В работе используются методы теории категорий и теории доменов, программной инженерии, математической логики и теории доказательств, теории графов, функционального программирования.

В качестве замечаний необходимо отметить следующее:

Стр. 17. В описании структуры диссертации указано, что «работа состоит из введения, четырех глав …». На самом же деле, диссертация включает в себя пять глав. Эта же опечатка повторена в автопеферате (стр. 7).

Стр. 21. Описывается «проблема разрешения». Более употребляемый термин для этой проблемы – «проблема разрешимости».

Стр. 155. Список листингов не полный. Не все листинги, встречающиеся в Приложениях, отражены в этом списке.

Стр. 183-192. В Приложение С приводится текст статьи принятой к печати, но еще не опубликованной. Автор отмечает, что результаты этой стать включены в главы 2 и 3. Считаю,

что было излишним выносить текст статьи в отдельное Приложение. А так же на стр. 191 список литературы «приклеился» к тексту Заключения.

Указанные замечания не снижают общей положительной оценки диссертации М.А. Кривчикова и не влияют на корректность полученных автором выводов.

Автореферат соответствует содержанию диссертации. Основные результаты, полученные в диссертации, опубликованы в открытой печати в 11 работах, из числа которых 5 статей опубликованы в центральных изданиях, входящих в список ВАК. Результаты диссертации могут найти применение как в теоретических исследованиях, так и на практике.

Диссертационная работа Кривчикова Максима Александровича является законченной научно-квалификационной работой, в которой содержится решение задач получения формальных моделей программ, имеющих значение для развития теоретической информатики. Диссертация соответствует требованиям п.п.9–12 Положения «О порядке присуждения ученых степеней». Автор заслуживает присуждения ему ученой степени кандидата физико-математических наук по специальности 05.13.17 — теоретические основы информатики (физико-математические науки).

Официальный оппонент
д.ф.-м.н., доцент,
ведущий научный сотрудник
Лаборатории вычислимости и прикладной логики
ФГБУН «Институт математики
им. С. Л. Соболева СО РАН» Д.Е.Пальчунов