

## **ОТЗЫВ**

официального оппонента на диссертационную работу

**Ермакова Михаила Кирилловича**

«Методы повышения эффективности итеративного динамического анализа программ»,

представленной на соискание учёной степени кандидата технических наук по специальности 05.13.11 — математическое и программное обеспечение вычислительных машин, комплексов и компьютерных сетей

### **Актуальность темы**

Диссертация М.К.Ермакова посвящена вопросу увеличения производительности динамического анализа программ. Расширение сферы применения программных решений, увеличение разнообразия программного обеспечения и объемов его производства требуют повышения степени автоматизации на всех этапах его создания и сопровождения, включая этап поиска и исправления ошибок. Одним из распространенных способов обеспечения качества программного обеспечения является статический анализ, при котором программа анализируется «в целом» без выполнения. Однако известной проблемой статического анализа является потенциальная возможность «ложных срабатываний», т. е. обнаружения ситуаций, которые не являются ошибками, но классифицируются статическим анализатором как таковые. Исследование результатов статического анализа может оказаться нетривиальной и трудоемкой задачей; кроме того, существует целый класс задач, для которых до сих пор не разработаны методы статического анализа, которые можно было бы продуктивно использовать в практике разработки ПО (сюда прежде всего следует отнести межпроцедурный анализ, анализ многопоточных приложений, приложений, активно работающих с динамической памятью, использующих адресную арифметику и т.д.) Другой класс подходов — динамический анализ — исследует реальное поведение программ при их исполнении. Обнаруживаемые при динамической анализе ошибки являются истинными, воспроизводимыми при некоторых входных данных; результаты динамического анализа приближают ответ на вопрос о корректности программ «с другой стороны» (могут оставаться невыясненные ошибки). В целом можно сказать, что статический и динамический подходы к анализу программ дополняют друг друга. Подобно статическому анализу, динамический анализ является трудоемкой процедурой. Повышение производительности динамического анализа позволяет обнаруживать большее количество ошибок. Таким образом, актуальность темы диссертации не вызывает сомнений.

## Общая характеристика работы

В диссертации сформулировано два основных достигнутых результата.

Прежде всего, это применение пользовательских аннотаций при динамическом анализе программ. Автор вводит два вида аннотаций, которые позволяют специализировать динамический анализ относительно данных и относительно анализируемой программы. Использование аннотаций предполагает обладание *ad hoc*-знанием о поведении программы и особенностях её работы с входными данными, но позволяет добиться большей эффективности анализа, чем в общем случае, за счет отбрасывания рассмотрения нерелевантных сценариев исполнения. Проведенные экспериментальные исследования показали, что, действительно, использование специализированного анализа позволяет обнаруживать больше ошибок, чем в общем случае.

Затем, основным результатом диссертации является система статического инструментирования, удовлетворяющая специфическим требованиям, возникающим в силу использования в контексте динамического анализа (поддержка символьного исполнения, тонкая настройка точек инструментирования и инструментирующего кода, и т.д.) Разработка полноценного программного инструмента, предоставляющего описанные возможности, является сложной инженерно-технической задачей, которая была решена в полном объеме. Проведенное экспериментальное исследование подтвердило как применимость реализованного инструмента для целей динамического анализа, так и его большую эффективность по сравнению с использованным ранее готовым средством динамического инструментирования. За счет этого в исследуемых приложениях были обнаружены новые ошибки.

Наконец, в диссертации описана модификация инструмента динамического анализа, основанная на технике распараллеливания, которая также приводит к увеличению эффективности анализа, что подтверждается проведенными измерениями.

Помимо собственно результатов, в диссертации приведен релевантный обзор методов динамического анализа программ, а также архитектуры и принципов функционирования конкретных программных инструментов, используемых для динамического анализа.

Диссертация состоит из введения, четырех глав, заключения и списка литературы. Текст диссертации изложен на 116 страницах и содержит 31 рисунок и 5 таблиц. Список литературы содержит 77 наименований.

Результаты, изложенные в диссертации, опубликованы в четырех научных работах, из них три – статьи в журналах из перечня российских рецензируемых журналов, в которых должны быть опубликованы основные результаты диссертаций на соискание учёных степеней доктора и кандидата наук, один материал научных конференций.

Автореферат диссертации в целом адекватно отражает содержание работы.

## **Научная новизна**

Научная новизна представленных в работе результатов подтверждается анализом релевантной научной литературы и программных разработок. Описанные автором приемы повышения эффективности динамического анализа реализованы в составе инструментального средства впервые.

## **Теоретическая и практическая значимость исследования**

Результаты данной работы обладают как теоретической, так и практической значимостью.

С практической точки зрения результаты диссертации могут быть использованы как напрямую (путем применения разработанного программного инструмента), так и косвенно — для разработки аналогичных инструментов.

С теоретической точки зрения результаты диссертации, во-первых, могут быть использованы как отправная точка для дальнейших исследований, а, во-вторых, в качестве материалов для преподавания курсов по системному программному обеспечению, разработке компиляторов, анализу программ.

## **Замечания по работе**

Помимо безусловных достоинств, представленная диссертационная работа обладает определенными недостатками.

Прежде всего, необходимо отметить, что в изложении превалирует неформальный стиль. Имеющие отношения к делу алгоритмы описаны на естественном языке в виде перечня шагов (порой довольно длинного, содержащего подпункты и т.д.), предложенные модификации также обсуждаются неформально, а их свойства не доказываются. В качестве подтверждения адекватности и корректности предлагаемых решений используются результаты тестирования. Возможно, впрочем, что таковы традиции данной предметной области.

Далее, для предлагаемых автором способов описания аннотаций отсутствует какое-либо обсуждение их выразительной силы, то есть не обсуждается, какие именно свойства можно задавать с их помощью, насколько они полны с точки зрения целей, для которых они были введены, и т. д. Кроме того, отсутствует обсуждение, насколько легко или сложно пользоваться этими аннотациями.

Упомянутые недостатки, тем не менее, не могут рассматриваться как опровержение основных результатов и выводов работы.

## Общее заключение

Диссертационное исследование М.К.Ермакова «Методы повышения эффективности итеративного динамического анализа программ» является законченной научно-квалификационной работой, которая соответствует всем требованиям «Положения о порядке присуждения учёных степеней», в том числе требованиям пункта 9, абзац 2, а её автор заслуживает присуждения ему учёной степени кандидата технических наук по специальности 05.13.11 — математическое и программное обеспечение вычислительных машин, комплексов и компьютерных сетей.

Официальный оппонент,  
доцент кафедры системного программирования  
математико-механического факультета  
Санкт-Петербургского Государственного Университета,  
кандидат физико-математических наук  
Бульчев Дмитрий Юрьевич

[dboulytchev@math.spbu.ru](mailto:dboulytchev@math.spbu.ru)  
+7-911-921-08-19  
197082, Санкт-Петербург,  
Богатырский пр., 53, корп. 1, кв. 271

Д.Ю.Бульчев  
«21» *ноября* 2016 г.

Документ подготовлен  
в порядке исполнения  
трудовых обязанностей