

ЗАКЛЮЧЕНИЕ ДИССЕРТАЦИОННОГО СОВЕТА Д 002.087.01
на базе Федерального государственного бюджетного учреждения науки
Институт системного программирования Российской академии наук
Федерального агентства научных организаций РФ
по диссертации на соискание ученой степени кандидата наук

аттестационное дело № _____

Решение диссертационного совета от 15 декабря 2016 года № 2016/17

О присуждении Ермакову Михаилу Кирилловичу, гражданину РФ, ученой степени кандидата технических наук.

Диссертация «Методы повышения эффективности итеративного динамического анализа программ» по специальности 05.13.11 – «математическое и программное обеспечение вычислительных машин, комплексов и компьютерных сетей» принята к защите 14 октября 2016 года, протокол № 2016/15 диссертационным советом Д 002.087.01 на базе Федерального государственного бюджетного учреждения науки Институт системного программирования Российской академии наук (ведомственная принадлежность – Федеральное агентство научных организаций, адрес: 109004, г. Москва, ул. А. Солженицына, дом 25), создан Приказом Минобрнауки России о советах по защите докторских и кандидатских диссертаций от 2 ноября 2012 г. № 714/нк.

Соискатель Ермаков Михаил Кириллович, 1990 года рождения, работает младшим научным сотрудником в Федеральном государственном бюджетном учреждении науки Институт системного программирования Российской академии наук (ведомственная принадлежность – Федеральное агентство научных организаций).

В 2012 году соискатель окончил Федеральное государственное бюджетное образовательное учреждение высшего образования «Московский государственный университет имени М.В.Ломоносова». В 2015 году соискатель окончил аспирантуру Федерального государственного

бюджетного образовательного учреждения высшего образования «Московский государственный университет имени М.В.Ломоносова».

Диссертация выполнена на кафедре системного программирования Федерального государственного бюджетного образовательного учреждения высшего образования «Московский государственный университет имени М.В.Ломоносова» (ведомственная принадлежность — Московский государственный университет имени М.В.Ломоносова) и в отделе системного программирования Федерального государственного бюджетного учреждения науки Институт системного программирования Российской академии наук (ведомственная принадлежность — Федеральное агентство научных организаций).

Научный руководитель — доктор физико-математических наук, академик Российской академии наук, профессор Иванников Виктор Петрович.

Официальные оппоненты:

1. Горбунов-Посадов Михаил Михайлович, доктор физико-математических наук, Федеральное государственное учреждение "Федеральный исследовательский центр Институт прикладной математики им. М.В. Келдыша Российской академии наук", отдел информационных технологий, руководитель отдела
 2. Булычев Дмитрий Юрьевич, кандидат физико-математических наук, Федеральное государственное бюджетное образовательное учреждение высшего образования "Санкт-Петербургский государственный университет", математико-механический факультет, доцент кафедры
- дали положительные отзывы на диссертацию.

Ведущая организация Вычислительный центр им. А.А. Дородницына Российской академии наук Федерального исследовательского центра «Информатика и управление» Российской академии наук, Москва в своем положительном заключении, подписанном Серебряковым Владимиром Алексеевичем, доктором физико-математических наук, профессором, заведующим отделом систем математического обеспечения, указала, что диссертация Ермакова М.К. является законченной научно-исследовательской

работой и удовлетворяет всем требованиям ВАК, предъявляемым к диссертациям на соискание ученой степени кандидата технических наук по специальности 05.13.11 – математическое и программное обеспечение вычислительных машин, комплексов и компьютерных сетей, а Ермаков Михаил Кириллович заслуживает присуждения ученой степени кандидата технических наук по специальности 05.13.11.

Выбор официальных оппонентов и ведущей организации обосновывается их компетентностью и достижениями в данной отрасли науки и способностью определить научную и практическую ценность диссертации.

Соискатель имеет 9 опубликованных работ, в том числе по теме диссертации 4 работы, в том числе 3 работы опубликованы в рецензируемых научных изданиях.

Публикации посвящены методам динамического анализа программ, основывающимся на применении символьного исполнения и решателей булевых ограничений и позволяющим автоматически обнаруживать критические дефекты в исполняемом коде. В публикациях представлены методы, направленные на ускорение динамического анализа программ, практические реализации данных методов и вспомогательных программных систем обработки исполняемого кода. В работах, выполненных в соавторстве, где соискатель значится первым автором, личным вкладом соискателя является проведение основных исследовательских работ, создание программных реализаций и подготовка публикаций.

Наиболее значимые научные работы по теме диссертации:

1. Ермаков М.К., Герасимов А.Ю. Avalanche: применение параллельного и распределенного динамического анализа программ для ускорения поиска дефектов и уязвимостей // Труды Института системного программирования РАН. — 2013. — т. 25. — с. 29-38.
2. Ермаков М.К., Варганов С.П. Применение статической бинарной инструментации с целью проведения динамического анализа программ для платформы ARM // Труды Института системного программирования РАН. — 2015. — т. 27 (1). — с. 5-24.

3. Ермаков М.К. Проведение динамического анализа исполняемого кода формата ARM ELF на основе статического бинарного инструментирования // Научно-технические ведомости СПбГПУ. Информатика. Телекоммуникации. Управление — 2016 — Выпуск 1(236). — с. 108-117.

Диссертационный совет отмечает, что соискателем получены новые научные результаты:

- разработан метод частичного динамического анализа программ на основе пользовательских спецификаций, ограничивающих обход путей выполнения программ по входным данным и структуре программ, и метод применения статической инструментации исполняемого кода для получения трасс выполнения программ во время проведения итеративного динамического анализа;
- разработан подход к использованию знаний о структуре программы и формате входных данных, обрабатываемых данной программой, с целью настройки итеративного динамического анализа, осуществляющего обход путей выполнения программы;
- доказана перспективность практического применения предложенных методов и их программных реализаций при проведении динамического анализа программ.

Теоретическая значимость исследования состоит в том, что:

- применительно к проблематике диссертации результативно использованы методы экспериментального и теоретического исследования, методы обработки и модификации исполняемого кода, методы символьного исполнения программ;
- изложены элементы теории динамического анализа программ, использующего символьное исполнение, и решатели булевых ограничений для автоматического построения тестового покрытия, факторы, обуславливающие практическую сложность достижения полноты проводимого анализа;

- раскрыты ограничения существующих методов итеративного динамического анализа, связанные с вычислительной сложностью различных этапов данного анализа и возможностью развития данных методов с целью создания средств поиска дефектов и контроля качества программного обеспечения;
- исследованы особенности кода программ, приводящие к росту числа возможных путей выполнения, преимущества и недостатки существующих подходов к проведению итеративного динамического анализа программ, основные направления повышения эффективности методов итеративного динамического анализа программ, развивающиеся в настоящее время.

Значение полученных соискателем результатов исследования для практики состоит в том, что:

- разработаны и внедрены в открытом инструменте динамического анализа программ *Avalanche*, разрабатываемом в Институте системного программирования РАН, модификации модуля построения трасс булевых ограничений с целью проведения частичного динамического анализа и система статической инструментации исполняемого кода, позволяющая понизить накладные расходы на проведение анализа программ;
- определены перспективы применения разработанных методов на практике, основанные на экспериментальных результатах проведения динамического анализа проектов с открытым исходным кодом;
- создана архитектура системы статической инструментации исполняемого кода платформы ARM, позволяющая создавать инструменты динамического анализа программ.

Достоверность результатов исследования состоит в том, что:

- теория, изложенная в диссертации, основывается на достижениях научных дисциплин в области анализа кода и согласуется с опубликованными экспериментальными данными по теме диссертации;
- разработанные в диссертации методы базируются на анализе практики, обобщении опыта зарубежных и отечественных ученых в области

динамического анализа программ, символьного исполнения и инструментации кода;

- использовано сравнение авторских данных и данных, полученных ранее по рассматриваемой тематике;

Личный вклад соискателя состоит в определяющем участии соискателя в получении новых научных результатов, разработке модификаций системы динамического анализа программ и системы статической инструментации исполняемого кода, обработке и оценке полученных экспериментальных данных, подготовке основных публикаций по выполненной работе (двух публикаций — в соавторстве с сотрудниками Института системного программирования Российской академии наук).

На заседании 15 декабря 2016 года диссертационный совет принял решение присудить Ермакову Михаилу Кирилловичу ученую степень кандидата технических наук.

При проведении тайного голосования члены диссертационного совета в количестве 15 человек, из них 7 докторов наук по специальности рассматриваемой диссертации, участвовавших в заседании, из 21 человек, входящих в состав совета, проголосовали: за – 15, против – 0, недействительных бюллетеней – 0.

Заместитель председателя диссертационного совета,
доктор физико-математических наук

Томилин А. Н.

Исполняющий обязанности ученого секретаря
диссертационного совета,
доктор технических наук

Карпов Л.Е.

15 декабря 2016 года