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 № 2016/18

О присуждении Мандрыкину Михаилу Усамовичу, гражданину РФ, ученой степени кандидата физико-математических наук.

Диссертация «Моделирование памяти Си-программ для инструментов статической верификации на основе SMT-решателей» по специальности 05.13.11 – «математическое и программное обеспечение вычислительных машин, комплексов и компьютерных сетей» принята к защите 14 октября 2016 года, протокол № 2016/16 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 Мандрыкин Михаил Усамович, 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 технологий программирования Федерального государственного бюджетного учреждения науки Институт системного программирования Российской академии наук (ведомственная принадлежность – Федеральное агентство научных организаций).

Научный руководитель – доктор физико-математических наук, профессор Петренко Александр Константинович, заведующий отделом технологий программирования Федерального государственного бюджетного учреждения науки Институт системного программирования Российской академии наук.

Официальные оппоненты:

1. Галатенко Владимир Антонович, доктор физико-математических наук, заведующий сектором автоматизации программирования Федерального государственного учреждения «Федеральный научный центр Научно-исследовательский институт системных исследований Российской академии наук»,
2. Климов Юрий Андреевич, кандидат физико-математических наук, старший научный сотрудник в отделе инструментального и прикладного программного обеспечения Федерального государственного учреждения «Федеральный исследовательский центр Институт прикладной математики им. М.В. Келдыша Российской академии наук»

дали положительные отзывы на диссертацию.

Ведущая организация Федеральное государственное бюджетное образовательное учреждение высшего образования «Санкт-Петербургский

государственный университет», город Санкт-Петербург в своем положительном заключении, подписанном Тереховым Андреем Николаевичем, профессором, доктором физико-математических наук, профессором с возложенными обязанностями заведующего кафедрой системного программирования, Дмитрием Владимировичем Козновым, доцентом, доктором технических наук, доцентом кафедры системного программирования и Дмитрием Юрьевичем Булычевым, кандидатом физико-математических наук, доцентом кафедры системного программирования, указала, что проведенное в рамках диссертационной работы теоретическое исследование и разработанные программы являются полезным вкладом в область верификации программного обеспечения, диссертационная работа Мандрыкина М. У. удовлетворяет требованиям ВАК Минобрнауки РФ, предъявляемым к кандидатским диссертациям, и соответствует требованиям пункта 9 «Положения о присуждении учёных степеней», утверждённого постановлением Правительства РФ от 24 сентября 2013 г. №842, а ее автор, Мандрыкин Михаил Усамович, заслуживает присуждения учёной степени кандидата физико-математических наук по специальности 05.13.11 – математическое и программное обеспечение вычислительных машин, комплексов и компьютерных сетей.

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 14 опубликованных работ, в том числе по теме диссертации 10 работ, в том числе 9 из них опубликованных в рецензируемых научных изданиях.

Публикации посвящены методам статической верификации Си-программ, основывающимся на применении решателей логических формул (SMT-решателей) и позволяющим доказывать соответствие программ заданным формальным спецификациям и находить ошибки в исходном коде программ, а именно, в публикациях рассматриваются методы дедуктивной верификации и методы автоматической статической верификации на основе предикатной

абстракции. Предлагаются методы повышения точности автоматической статической верификации Си-программ, а также методы расширения области применимости инструментов дедуктивной верификации Си-программ, в частности, для кода ядер операционных систем. Представлены результаты применения предложенных методов при верификации модулей ядра операционной системы Linux.

Наиболее значимые научные работы по теме диссертации:

1. Mandrykin, M. U. Region analysis for deductive verification of C programs M. U. Mandrykin, A. V. Khoroshilov // Programming and Computer Software. — 2016. — Vol. 42. — no. 5. — P. 257–278.
2. Mandrykin, M. U. High-level memory model with low-level pointer cast support for Jessie intermediate language / M. U. Mandrykin, A. V. Khoroshilov // Programming and Computer Software. — 2015. — Vol. 41. — no. 4. — P. 197–207.
3. Мандрыкин, М. У. Моделирование памяти с использованием неинтерпретируемых функций в предикатных абстракциях / М. У. Мандрыкин, В. С. Мутилин // Труды Института системного программирования РАН. — 2015. — том 27. — стр. 117–142.

Диссертационный совет отмечает, что соискателем получены новые научные результаты:

- разработан метод моделирования памяти Си-программ с помощью логических формул, поддерживающий автоматическое разбиение памяти на непересекающиеся области, для инструмента дедуктивной верификации Си-программ, содержащих вложенные структуры и массивы, объединения, а также произвольные приведения типов указателей; метод позволил расширить область применимости инструмента дедуктивной верификации, поддерживающего разбиение памяти на непересекающиеся области;
- разработан метод моделирования памяти Си-программ с помощью логических формул в теориях для инструмента автоматической статической верификации, использующего итеративное уточнение предикатной

абстракции по контрпримерам; разработанный метод позволил повысить точность верификации модулей ядра ОС Linux с помощью применения указанного инструмента;

- предложена формализация низкоуровневой семантики практически значимого фрагмента языка Си, включающего вложенные структуры и массивы, объединения, а также произвольные приведения типов указателей.

Теоретическая значимость исследования состоит в том, что:

- доказаны теоремы о корректности и полноте разработанного метода моделирования памяти для инструмента дедуктивной верификации относительно предложенной формализации низкоуровневой семантики фрагмента языка Си;
- раскрыты ограничения существующих методов моделирования памяти Си-программ в инструментах статической верификации, использующих решатели логических формул в теориях, связанные с некорректным и неполным моделированием низкоуровневой семантики языка Си;
- проведена модификация существующего метода моделирования памяти Си-программ с разделением памяти на непересекающиеся регионы, позволившая расширить область применимости метода для дедуктивной верификации модулей ядер операционных систем.

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

- разработана и внедрена в открытый инструмент статической верификации программ CPAchecker новая реализация механизма построения формул пути, которая позволила снизить число некорректных вердиктов при верификации модулей ядра операционной системы Linux;
- новая реализация механизма моделирования памяти с использованием автоматизированного разбиения памяти на непересекающиеся области внедрена в открытый набор инструментов дедуктивной верификации Frama-

C/Jessie/Why3, что позволило применить данный набор инструментов при верификации модуля безопасности ядра операционной системы Linux.

Достоверность результатов исследования состоит в том, что:

- теория, изложенная в диссертации, построена на известных и проверяемых данных и фактах, и согласуется с опубликованными экспериментальными данными по теме диссертации;
- положения диссертации базируются на анализе практики и обобщении результатов исследований в области автоматической статической и дедуктивной верификации;
- использованы методики получения и сравнительного анализа результатов измерений характеристик работы инструментов автоматической статической верификации на представительной совокупности верификационных заданий.

Личный вклад соискателя состоит в определяющем участии соискателя в получении новых научных результатов, разработке модификаций инструментов автоматической статической и дедуктивной верификации, получении и оценке экспериментальных данных, подготовке основных публикаций по теме диссертации (в соавторстве с сотрудниками Федерального государственного бюджетного учреждения науки Институт системного программирования Российской академии наук).

На заседании 15.декабря 2016 года диссертационный совет принял решение присудить Мандрыкину М. У. ученую степень кандидата физико-математических наук.

При проведении тайного голосования диссертационный совет в количестве 15 человек, из них 8 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