ОТЗЫВ
ОФИЦИАЛЬНОГО ОППОНЕНТА
на диссертационную работу Герасимова Александра Юрьевича «Классификация предупреждений о программных ошибках методом динамического символьного исполнения программ», представленной к защите на соискание учёной степени кандидата физико-математических наук по специальности 05.13.11 – «Математическое и программное обеспечение вычислительных машин, комплексов и компьютерных сетей»

Диссертационная работа А.Ю. Герасимова посвящена разработке нового метода классификации предупреждений о программных ошибках, найденных методом статического анализа программ. Актуальность темы исследования продиктована ограничениями методов статического анализа программ, связанными с теоретически обоснованной неразрешимостью проблемы определения свойств вычислимых функций, а также с временными ограничениями современных инструментов статического анализа программ. Проблема, на решение которой направлено исследование А.Ю. Герасимова, связана с возможностью получения ложных предупреждений об ошибках в программах от инструментов статического анализа программ. На анализ каждого из таких предупреждений, как правило, требуются значительные усилия высококвалифицированного специалиста. Классификация предупреждений на истинные и ложные в конечном итоге позволит эффективно распределить усилия программистов при работе с результатами статического анализатора кода программ. В диссертационной работе рассматривается подход, совмещающий статический анализ исходного кода программ, статический анализ машинного кода программ и динамическое символьное исполнение программ. Несмотря на ограничения каждого из перечисленных методов анализа программ, примененного отдельно, в диссертации показывается возможность преодоления этих ограничений при использовании комбинированного подхода. Именно в комплексном характере предлагаемого подхода имеется высокая степень научной новизны диссертационной работы А.Ю. Герасимова. Проблема взрывного роста количества путей для анализа в процессе динамического символьного исполнения программ, препятствующая реализации исчерпывающего анализа кода программы, в диссертации решается путём использования результатов статического анализа программ. Статический анализатор указывает в каких местах программы наиболее вероятно появление ошибки, а динамическое символьное исполнение программы производится по путям исполнения, содержащим указанные места потенциальных ошибок. Большой интерес представляют такие результаты как формальная модель обнаружения ошибок в программах методами символьного исполнения, а также алгоритмы комбинирования статического и динамического анализа программ и метод классификации предупреждений о программных ошибках, основанный на разработанных алгоритмах и модели. Научная новизна полученных результатов заключается также в формализации понятия программной ошибки, в разработке формальной модели обнаружения программных ошибок.

Стоит отметить, что предложенная формальная теоретическая модель обнаружения ошибок в программе методами символьного исполнения может быть применена для обнаружения широкого класса программных ошибок. Практическая значимость выносимых на защиту результатов основывается на том, что разработанные алгоритмы

были реализованы в рамках промышленных инструментов анализа программ Svace и Anxiety, разрабатываемых в Институте системного программирования им. В.П. Иванникова РАН. Научная обоснованность полученных результатов определяется строгостью определений и теорем, являющихся основой разработанной модели обнаружения ошибок, строгостью их доказательств, а также верификацией реализации предложенных алгоритмов в инструменте Anxiety.

Диссертационная работа А. Ю. Герасимова состоит из 129 страниц и включает Введение, четыре Главы, Заключение и список литературы (177 источников). В тексте диссертации имеется 4 рисунка и 8 таблиц.

Во Введении обосновывается актуальность работы, формулируются цель и задачи исследования, показывается научная новизна полученных результатов и перечисляются выносимые на защиту положения.

В Первой главе проводится обзор методов и инструментов обнаружения программных ошибок, описываются характеристики инструментов, позволяющие их классифицировать. Приводятся различные определения и классификации программных ошибок. Описываются причины их появления.

Во Второй главе приводится описание различных уровней статического анализа программ, а также обобщается представление результата анализа программ в виде трассы предупреждения о программной ошибке. Также подробно рассматривается метод динамического символьного исполнения программ.

В Третьей главе описываются алгоритмы комбинирования статического и динамического анализа программ, вводится формальная математическая модель обнаружения ошибок в программе, состоящая из 7 теорем и 14 определений, и обосновывается классификация предупреждений о программных ошибках.

В Четвертой главе описывается экспериментальная реализация предложенных алгоритмов на основе инструментов статического и динамического анализа программ, разрабатываемых в Институте системного программирования им. В.П. Иванникова РАН. Приводятся результаты экспериментальной проверки реализованных алгоритмов на наборе программ с открытым исходным кодом и проводится их анализ.

В Заключении формулируются полученные результаты исследования, указываются отличия предложенного метода от существующих аналогов и формулируются направления дальнейших исследований в данной области.

Результаты, выносимые на защиту опубликованы в 9 работах. Из них 6 опубликованы в реферируемых журналах из перечня ВАК РФ, и 5 из них опубликованы научных журналах, в индексируемых международной базой цитирования Scopus. Результаты исследования докладывались на 1-й всероссийской и 2-х международных конференциях по научному профилю диссертации. Зарегистрированы 5 свидетельств о государственной регистрации программы для ЭВМ.

Диссертация А. Ю. Герасимова выполнена на высоком научном уровне. Тем не менее стоит отметить следующее замечание. В Первой главе присутствует упоминание методов рандомизированного тестирования программ, но в диссертации нигде нет упоминания о применении этих методов. Подчеркнем, однако, что указанный недостаток не снижает положительную оценку полученных в диссертации результатов и выносимых на защиту положений, и не влияет на общую высокую оценку представленной диссертации.

В заключении отметим, что диссертация А. Ю. Герасимова представляет собой завершенное научное исследование, проведенное на высоком научно-техническом уровне, и указывает новые направления для исследования в области автоматического анализа программ на наличие ошибок. Автореферат правильно и полно отражает содержание работы.

Диссертационная работа Герасимова Александра Юрьевича по теме «Классификация предупреждений о программных ошибках методом динамического символьного исполнения программ», представленная на соискание учёной степени кандидата физико-математических наук по специальности 05.13.11 – «Математическое и программное обеспечение вычислительных машин, комплексов и компьютерных сетей», соответствует положению ВАК РФ о присуждении учёных степеней, утвержденного Постановлением Правительства РФ №842 от 24.09.2013 года, а её автор, Герасимов Александр Юрьевич, заслуживает присуждения учёной степени кандидата физико-математических наук по специальности 05.13.11.

Официальный оппонент
доктор физико-математических наук,
старший научный сотрудник,
начальник отдела Курчатовского
комплекса НБИКС-природоподобных
технологий Национального
исследовательского центра «Курчатовский
институт»
Почтовый адрес: 123182, РФ, Москва, пл.
Академика Курчатова, д. 1
Телефон: +7 (499) 196–95–39
Электронная почта: nrcki@nrcki.ru

Ильин Вячеслав Анатольевич

25.02.2019

Подпись сотрудника НИЦ «Курчатовский институт» В.А. Ильина заверяю
Главный ученый секретарь
НИЦ «Курчатовский институт»
доктор физико-математических н

П.А. Форш