ОТЗЫВ ОФИЦИАЛЬНОГО ОППОНЕНТА

на диссертационную работу Герасимова Александра Юрьевича

«Классификация предупреждений о программных ошибках методом динамического символьного исполнения программ»,

представленную 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»

Актуальность темы

Постоянно растущие объем и сложность программ требуют значительных усилий для поиска и устранения дефектов (ошибок, уязвимостей), которые неизбежно в них присутствуют. В последние годы наблюдается увеличение количества научных исследований и появление практических инструментов в области автоматического анализа программ на наличие ошибок, основанных *на теории компиляторов*.

Чисто статические методы и инструменты анализа исходного кода программ не всегда обладают высокой точностью обнаружения ошибок в программе из-за практических ограничений, связанных с необходимостью обеспечения удовлетворительного времени анализа программ. Поэтому в результатах анализа могут появляться ложные предупреждения об ошибках в программе, проверка которых требует трудоемкой работы квалифицированных программистов.

- Диссертационная работа А. Ю. Герасимова посвящена разработке метода классификации предупреждений о программных ошибках при помощи *динамического символьного исполнения*. Этот метод, определяющий *актуальность* работы, позволяет направить усилия разработчиков программ на анализ наиболее вероятных мест с ошибками в программах.

Структура работы

Диссертационная работа А. Ю. Герасимова состоит из четырех глав, введения и заключения. Полный объем диссертации составляет 129 страниц. Список литературы содержит 177 наименований.

Во введении обосновывается актуальность темы исследования, цель и задачи, определяется научная новизна и основные положения работы, выносимые на защиту, а именно:

- теоретическая модель обнаружения ошибок в программах методом символьного исполнения;
- алгоритмы комбинирования статического анализа и динамического символьного исполнения программ;
- метод классификации предупреждений о программных ошибках, полученных от инструмента статического анализа программ.

В первой главе описываются известные определения и классификации программных ошибок, приводится статистика регистрации программных ошибок в программном обеспечении, выпущенном на рынке, описываются причины появления программных ошибок. Наиболее сильное впечатление производит подробный обзор существующих статических и динамических методов обнаружения ошибок в программах, анализируются их преимущества и недостатки, и делается обоснованный вывод о том, что применение комбинации различных методов является наиболее перспективным направлением обнаружения ошибок в программах.

Во второй главе подробно описываются методы статического анализа и динамического символьного исполнения программ, на которых основывается подход, предложенный автором. Рассматриваются различные уровни статического анализа программ, приводится модель представления предупреждения о программной ошибке. Приводится описание метода динамического символьного исполнения программ, включающее обзор методов сбора информации о выполнении программы, методов преобразования операций программы в математическую формулу и методов выбора путей для символьного исполнения программы.

В третьей главе описывается формальная математическая модель обнаружения ошибок в программе, доказывается общая теорема о достижении состояния ошибки в программе и ещё шесть теорем, показывающих применимость предложенного подхода для обнаружения различных программных ошибок. Приводятся алгоритмы комбинирования статического анализа и динамического символьного исполнения программ, алгоритм построения путей, достигающих определенной точки в программе, и алгоритм направленного динамического символьного исполнения программы. Формулируется и обосновывается классификация предупреждений о программных ошибках.

В четвертой главе приводится описание реализации и экспериментальной проверки предложенного метода на основе интеграции инструментов статического и динамического анализа программ. Практические результаты использования предложенного в работе метода подтверждают существенное сокращение числа

предупреждений, требующих проверки программистом, а также позволяют построить входные данные, позволяющие выявить реальные ошибки.

В заключении автор формулирует основные полученные результаты исследования, описывает отличие предложенного метода от имеющихся аналогов и формулирует направления дальнейших исследований, обоснованных обнаруженными ограничениями реализации предложенного метода.

Научная новизна и достоверность работы

Диссертационная работа описывает *новый подход к классификации предупреждений о программных ошибках*, основанный на модели, алгоритмах и методе, предложенных автором. Показана применимость предложенного метода на практике. Новые результаты исследования, предложенные автором, заключаются в следующем:

- разработана теоретическая модель обнаружения ошибок в программе на основе символьного исполнения программ;
- разработан алгоритм совмещения статического анализа и динамического символьного исполнения программ;
- разработан алгоритм направленного динамического символьного исполнения программ;
- разработан метод классификации предупреждений о программных ошибках.

Обоснованность разработанных в диссертационной работе научных положений подтверждается анализом библиографических работ российских и зарубежных авторов в области теории и практики методов анализа программ. Их достоверность подтверждается корректным применением теории графов, теории множеств, методов вычислительной математики. Научные результаты диссертационной работы опубликованы в 9 научных статьях и защищены 5 свидетельствами о государственной регистрации программ для ЭВМ.

Практическая значимость полученных результатов работы состоит в том, что разработанные алгоритмы реализованы в виде программного комплекса, позволяющего снизить трудоёмкость процесса анализа предупреждений об ошибках, для которого требуется работа высококвалифицированных специалистов в области разработки программ.

В работе можно отметить следующие **недостатки**:

- экспериментальная проверка результатов исследования проводилась на наборе программ с открытым исходным кодом, для которых предложенные метод позволяет построить входные данные, необходимые для проявления ошибок; однако ничего не сказано о его применении к

анализу программ с более сложными исходными данными, например, к компиляторам;

- в автореферате недостаточно подробно описывается экспериментальная реализация предложенных методов, которая подробно изложена в тексте диссертации;
- в работе нет данных о времени работы динамического символьного исполнения программы.

Отмеченные недостатки не влияют на общую положительную оценку представленной диссертации.

Автореферат полно и правильно отражает содержание диссертационной работы.

Диссертация А. Ю. Герасимова является законченной научной работой, выполненной на высоком научно-техническом уровне. Она соответствует всем требованиям, предъявляемым к кандидатским диссертациям ВАК РФ, а её автор, Герасимов Александр Юрьевич, заслуживает присуждения учёной степени кандидата физико-математических наук по специальности 05.13.11 – «Математическое и программное обеспечение вычислительных машин, комплексов и компьютерных сетей».

Официальный оппонент
кандидат технических наук, начальник отделения «Системы программирования» Публичного акционерного общества «Институт электронных управляющих машин им. И. С. Брука», Российская федерация, 119334, Москва, ул. Вавилова, д. 24

тел. +7 (499) 135-89-49

адрес электронной почты: ineum@ineum.ru

В.Ю. Волконский

Подпись кандидата технических наук Волко
В.Ю. заверяю, зам. генерального директора
«ИНЭУМ им. И.С. Брука»

В.М. Фельдман

евраля 2019 г.