

ОТЗЫВ ОФИЦИАЛЬНОГО ОППОНЕНТА

на диссертацию **Белеванцева Андрея Андреевича** «Многоуровневый статический анализ исходного кода для обеспечения качества программ», представленную на соискание ученой степени доктора физико-математических наук по специальности 05.13.11 – «Математическое и программное обеспечение вычислительных машин, комплексов и компьютерных сетей»

Актуальность темы исследования.

В настоящее время сложно назвать область, в которой не применялись бы цифровые вычислительные устройства. Работа таких устройств невозможна без использования программ. Наличие ошибок в программах приводит к получению неверных результатов вычислений. Существует целый ряд областей, в которых ошибки могут привести к человеческим жертвам, значительному финансовому ущербу, экологической катастрофе. Примерами таких ошибок могут послужить ошибки в программном обеспечении ракетных систем (Ariane-5, 1996 г.), автомобилей, ошибки в программном обеспечении, обеспечивающем моделирование объектов (ошибка при моделировании нефтяной платформы Speiner A, 1991 г.).

Постоянное увеличение номенклатуры функций и их усложнение привело к невозможности качественной разработки программ без использования дополнительных инструментов для анализа и верификации. Исходные тексты современных программ состоят из миллионов строк кода, их физически невозможно проанализировать «вручную», также невозможно «вручную» в достаточной степени протестировать такие программы. В результате, в настоящее время существует целый ряд инструментов для проверки правильности программ: Isabelle/HOL, ASTREE, Cantata++, Clang Static Analyzer.

Развитие существующих языков программирования, появление новых, выпуск новых нормативных документов, регламентирующих разработку вычислительных систем и программного обеспечения, требует постоянного совершенствования методов и средств анализа и верификации. В связи с этим можно утверждать, что тематика представленной диссертационной работы является актуальной.

Содержание диссертации и автореферата.

Диссертация состоит из введения, пяти глав и заключения, изложенных на 229 страницах, списка литературы из 196 наименований, содержит 39 рисунков и 17 таблиц. Автореферат в полном объеме отражает содержание диссертации. В нем изложены основные идеи и выводы диссертации, отражен личный вклад автора в проведенное исследование, охарактеризованы степень новизны и практическая значимость полученных результатов.

Новизна и значимость результатов

В диссертации получены следующие новые результаты, которые выносятся на защиту:

- методология проведения анализа исходного кода программ для поиска ошибок, заключающаяся в проведении многоуровневого статического анализа с помощью разработанного в диссертации набора моделей программы и методов анализа с общей моделью памяти на уровнях анализа АСД, внутривычислительного анализа, межвычислительного контекстно-чувствительного анализа, чувствительного к путям выполнения анализа;

- алгоритмы поиска конкретных ошибок в программе (детекторы) на основе предложенных методов, выполняющие поиск популярных классов ошибок: ошибок кодирования, неверного использования стандартных интерфейсов, критических ошибок (разыменование нулевого указателя, переполнение буфера, ошибки управления памятью и ресурсами, использование неинициализированных переменных, ошибки многопоточных примитивов, недостижимый код и др.);

- архитектура программной системы, обеспечивающая автоматическую работу всех предложенных методов на протяжении всего процесса анализа, а также управление набором анализаторов для различных языков и единообразный показ их результатов. В частности, разработаны единое переносимое хранилище собранной для анализа информации и результатов анализа, обеспечивающее запуск анализа на любой машине; подсистема просмотра и разметки результатов анализа, которая обеспечивает перенос выполненной пользователем разметки между результатами анализа программы; инкрементальный анализ только лишь изменившейся части программы.

Разработанные в диссертации методы и алгоритмы доведены до программной реализации и составляют основу системы статического анализа программ SVACE.

Система SVACE внедрена в цикл промышленной разработки компании Samsung Electronics с 2015 года, а также используется в НИЦ «Курчатовский институт».

Достоверность и обоснованность научных положений, выводов и рекомендаций

Достоверность проведенных исследований подтверждается доказанными теоремами о вычислительной сложности и корректности разработанных алгоритмов, проведенным тестированием, а также прошедшими экспертизами работы, при получении грантов.

Основные результаты работы докладывались и обсуждались на международных (4) и всероссийских (5) научных конференциях и семинарах: Sixth International Conference on Computer Science and Information Technologies (CSIT' 2007), 24-28 September, Yerevan, Armenia; 9th International Conference on Computer Science and Information Technologies (CSIT 2013), 23 - 27 September, 2013, Yerevan, Armenia; Открытая конференция по компиляторным технологиям 2015, Москва, Россия; Открытая конференция ИСП РАН 2016, Москва, Россия; Tizen Developers' Conference 2017, San Francisco, USA; международная Ершовская конференция по информатике PSI-2017 27-29 июня 2017 года, Москва, Россия; Ломоносовские чтения 2017; конференция OS DAY 2017; X Всероссийская межведомственная конференция «Актуальные направления развития систем охраны, специальной связи и информации для нужд государственной власти Российской Федерации», Академия ФСО России, г. Орел 2017 г.

Основные научные результаты диссертации опубликованы в рецензируемых научных изданиях: 10 работ в журналах из перечня ВАК РФ; 4 – в изданиях, индексируемых Scopus и Web of Science; 9 свидетельств о государственной регистрации программ для ЭВМ. Диссертация не содержит заимствованных материалов или отдельных результатов без ссылок на авторов и источники заимствования.

Диссертация соответствует паспорту научной специальности 05.13.11 «Математическое и программное обеспечение вычислительных машин, комплексов и компьютерных сетей» (пункт 1).

Рекомендации по использованию результатов

Разработанные в диссертации алгоритмы и программный инструментарий могут найти применение в организациях, ведущих разработку программного обеспечения: ФГУП «НИИ «Квант» (г. Москва), НИИ МВС ЮФУ (г. Таганрог), ФГУП «ГосНИИАС» (г. Москва), АО «Концерн «Вега» и др.

Полученные результаты также могут найти применение в учебном процессе, в частности, в курсах по технологии разработки программного обеспечения для систем ответственного применения.

Замечания

1. Недостаточно проработаны вопросы представления и компоновки материала, что затрудняет его понимание:

- недостаточное количество иллюстраций в автореферате и диссертации;
- из-за ограниченного объема чрезмерная детализация материала в автореферате привела к недостаточной наглядности его (материала) представления;
- в главах диссертации отсутствуют разделы с выводами.

2. Не указан источник данных о среднем значении метрики вложенности управляющих операторов в ОС Tizen (стр. 66 диссертации), кроме того, не уточняется, на основании анализа каких программ сделан вывод о небольшой глубине циклов.

3. В алгоритме 2.4 (стр. 69 диссертации) нет объяснения, почему в циклах анализируется только 2 итерации.

4. В разделе 4 для языков C/C++ не рассмотрен вопрос обнаружения потенциальных взаимных блокировок, что важно при разработке систем реального времени.

5. Гипотеза о существовании контекстов (стр. 175 диссертации) рассмотрена недостаточно подробно, не приведено ее сравнение с методами формализации понятия ошибки, рассмотренными в разделе 1.4.

6. Описка на стр.85 диссертации и стр.20 автореферата (предложение перед теоремой 2.6).

Заключение

Диссертация Белеванцева Андрея Андреевича «Многоуровневый статический анализ исходного кода для обеспечения качества программ» является

самостоятельной, законченной научно-квалификационной работой, в которой на основании выполненных исследований и разработок получено решение важной научной проблемы разработки методологии проведения статического анализа исходного кода программ для поиска ошибок в программах, обеспечивающей высокий процент истинных срабатываний анализатора. Диссертация отвечает требованиям Положения ВАК РФ о порядке присуждения ученых степеней, а ее автор, Белеванцев Андрей Андреевич, заслуживает присуждения ему ученой степени доктора физико-математических наук по специальности 05.13.11 - «Математическое и программное обеспечение вычислительных машин, комплексов и компьютерных сетей»

Мельник Эдуард Всеволодович _____

25.12.17г.

д.т.н., и.о. зав. отделом информационных технологий и процессов управления,
г.н.с.

Федеральное государственное бюджетное учреждение науки Южный научный
центр Российской академии наук
344006, Россия, г. Ростов-на-Дону, пр. Чехова, 41
Тел.: +7 (918) 556 69 84
E-mail: evm17@mail.ru

Подпись Мельника Эдуарда Всеь

Ученый секретарь ЮНЦ РАН, к.б.н.

Н. И. Булышева

М.П.