ЗАКЛЮЧЕНИЕ ДИССЕРТАЦИОННОГО СОВЕТА Д 002.087.01
на базе Федерального государственного бюджетного учреждения науки
Институт системного программирования им. В.П. Иванникова
Российской академии наук
Федерального агентства научных организаций РФ
по диссертации на соискание ученой степени доктора наук

аттестационное дело № _____

решение диссертационного совета от 15 февраля 2018 года № 2018/03

О присуждении Белеванцеву Андрею Андреевичу, гражданину РФ ученой степени доктора физико-математических наук.

Диссертация «Многоуровневый статический анализ исходного кода для обеспечения качества программ» по специальности 05.13.11 – «математическое и программное обеспечение вычислительных машин, комплексов и компьютерных сетей» принята к защите 14 ноября 2017 г., протокол № 2017/24 диссертационным советом Д 002.087.01 на базе Федерального государственного бюджетного учреждения науки Институт системного программирования им. В.П. Иванникова 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 Белеванцев Андрей Андреевич, 1981 года рождения, работает ведущим научным сотрудником в Федеральном государственном бюджетном учреждении науки «Институт системного программирования им. В.П. Иванникова Российской академии наук», ФАНО.

Диссертацию на соискание ученой степени кандидата физико-математических наук защитил в 2008 году в Диссертационном совете, созданном при Институте системного программирования Российской академии наук.

Диссертация выполнена в отделе компиляторных технологий Федерального государственного бюджетного учреждения науки «Институт системного программирования им. В.П. Иванникова Российской академии наук», ФАНО.

Научный консультант – доктор физико-математических наук, член-корреспондент РАН Аветисян Арутюн Ишханович, Федеральное государственное бюджетное учреждение науки «Институт системного программирования им. В.П. Иванникова Российской академии наук», ФАНО, директор.

Официальные оппоненты:

1. Галатенко Владимир Антонович, доктор физико-математических наук, заведующий сектором Федерального государственного учреждения «Федеральный научный центр Научно-исследовательский институт системных исследований Российской академии наук»,
2. Мельник Эдуард Всеволодович, доктор технических наук, заведующий отделом Федерального государственного бюджетного учреждения науки «Южный научный центр Российской академии наук»,
3. Терехов Андрей Николаевич, доктор физико-математических наук, профессор, заведующий кафедрой системного программирования Федерального государственного бюджетного образовательного учреждения высшего профессионального образования «Санкт-Петербургский государственный университет»

дали положительные отзывы на диссертацию.

Ведущая организация Федеральный исследовательский центр «Информатика и управление» Российской академии наук, г. Москва в своем положительном заключении, подписанном Синициным И.Н., доктором технических наук, профессором, главным научным сотрудником ФИЦ ИУ РАН, указала, что диссертационная работа содержит математически обоснованные положения и практические результаты, которые могут быть в целом квалифицированы как решение крупной научной проблемы, направленной на повышение качества разрабатываемого программного обеспечения.

Выбор официальных оппонентов и ведущей организации обосновывается их компетентностью и достижениями в данной отрасли науки, наличием

публикаций в сфере исследований, соответствующей теме диссертации, и способностью определить научную и практическую ценность диссертации.

Соискатель имеет 42 опубликованных работы, в том числе по теме диссертации 12 работ, из них 10 работ [1-10] опубликованы в рецензируемых научных изданиях, в том числе 4 работы в журнале, индексируемом в WoS и Scopus. По теме диссертации получено 9 свидетельств о государственной регистрации программ для ЭВМ, наиболее важные из которых представлены ниже [13-15].

В работе [9] содержится разработанная автором методология многоуровневого статического анализа программ. В работах [1-4,7] представлены разработанная архитектура анализатора, в котором реализованы предложенные методы анализа. В работах [5, 8] автором представлены методы анализа для языков Java и C#. В работе [6] представлен разработанный под руководством автора метод межпроцедурного анализа для поиска ошибок переполнения буфера.

1. Бородин А. Е., Белеванцев А. А. Статический анализатор Svace как коллекция анализаторов разных уровней сложности // Труды ИСП РАН. 2015. Т. 27, № 6. С. 111–134.
2. V. P. Ivannikov, A. A. Belevantsev, A. E. Borodin, V. N. Ignatiev, D. M. Zhurikhin, A. I. Avetisyan. Static analyzer Svace for finding defects in a source program code. Programming and Computer Software, 2014, vol. 40, issue 5, pp. 265-275.
3. В.П. Иванников, А.А. Белеванцев, А.Е. Бородин, В.Н. Игнатьев, Д.М. Журихин, А.И. Аветисян, М.И. Леонов. Статический анализатор Svace для поиска дефектов в исходном коде программ // Труды ИСП РАН. 2014. Т. 26, выпуск 1. Стр. 231-250.
4. А.Аветисян, А.Белеванцев, Алексей Бородин, В.Несов. Использование статического анализа для поиска уязвимостей и критических ошибок в исходном коде программ // Труды ИСП РАН, т.21, 2011. Стр. 23-38.
5. V. K. Koshelev, V. N. Ignat'ev, A. I. Borzilov, and A. A. Belevantsev. SharpChecker Static Analysis Tool for C# Programs. Programming and Computer Software, 2017, Vol. 43, No. 4, pp. 268–276.

6. И.А. Дудина, А.А. Белеванцев. Применение статического символьного выполнения для поиска ошибок доступа к буферу. Программирование, 2017, № 5, стр. 3-17.
7. А.А. Белеванцев, А.О. Избышев, Д.М. Журихин. Организация контролируемой сборки в статическом анализаторе Svace. Системный администратор, выпуск 6-7 (176-177), 2017, стр. 135-139.
8. А.П. Меркулов, С.А. Поляков, А.А. Белеванцев. Анализ программ на языке Java в инструменте Svace. Труды ИСП РАН, том 29, вып. 3, 2017 г., стр. 57-74. DOI: 10.15514/ISPRAS-2017-29(3)-5
9. А. А. Белеванцев. Многоуровневый статический анализ исходного кода программ для обеспечения качества программ. Программирование, 2017, Том 43, №6, стр. 3-26.
10. Беляев М.В., Шимчик Н.В., Игнатьев В.Н., Белеванцев А.А. Сравнительный анализ двух подходов к статическому анализу помеченных данных. Труды ИСП РАН, том 29, вып. 3, 2017 г., стр. 99-116. DOI: 10.15514/ISPRAS-2017-29(3)-7
11. Аветисян А.И., Белеванцев А.А., Чукляев И.И. Технологии статического и динамического анализа уязвимостей программного обеспечения. Вопросы кибербезопасности. №3 (4) июль-сентябрь 2014 г., стр. 20-28.
12. А. А. Белеванцев, И.А. Дудина. К вопросу о преодолении ограничений статического анализа при поиске дефектов переполнения буфера. Ломоносовские чтения, 2017.
13. Белеванцев А.А. «Инструмент преобразования Java-библиотек ОС Android формата Jack в формат JAR «Llij». Свидетельство о государственной регистрации программы для ЭВМ № 2017660048 от 13.09.2017.
14. Игнатьев В.Н., Кошелев В.К., Борзилов А.И., Белеванцев А.А., Велесевич Е.А. «Инфраструктура чувствительного к контексту вызова, потоку и путям исполнения анализа инструмента «SharpChecker». Свидетельство о государственной регистрации программы для ЭВМ № 2017610526 от 12.01.2017.
15. Игнатьев В.Н., Чукляев И.И., Белеванцев А.А. «Инструмент статического анализа «RuleChecker» для языков C и C++».

Свидетельство о государственной регистрации программы для ЭВМ № 2016611555 от 04.02.2016.

Диссертационный совет отмечает, что соискателем получены следующие новые научные результаты.

- Разработана методология статического анализа программ для поиска ошибок в программах, заключающаяся в проведении многоуровневого статического анализа – анализа абстрактного синтаксического дерева, внутрипроцедурного анализа, межпроцедурного контекстно-чувствительного и чувствительного к путям выполнения анализа.
- Разработаны методы статического анализа программ на основе общей для всех уровней анализа модели памяти программы и набора моделей программы, включающего в себя объединение одинаковых значений программы в классы эквивалентности и отслеживание изменения этих классов, отслеживание условий, при которых указанные классы будут принимать конкретные значения, символьное выполнение с объединением состояний над ячейками памяти из модели памяти программы.
- Разработаны алгоритмы поиска ошибок в программе на основе описанных методов анализа, покрывающие часто встречающиеся классы критических ошибок и ошибок кодирования, в том числе алгоритмы поиска ошибок работы с указателями, ошибок переполнения буфера, ошибок управления ресурсами.
- Разработана архитектура программной системы, обеспечивающая автоматическую работу предложенных методов на протяжении всего процесса анализа, а также единообразное управление набором анализаторов для различных языков программирования и показ результатов работы этих анализаторов.

Теоретическая значимость исследования состоит в том, что:

- разработанные методы анализа математически обоснованы, доказаны теоремы о корректности реализующих эти методы алгоритмов и об их сложности;
- с получением обладающих научной новизной результатов применительно к проблематике диссертации использованы методы анализа потока данных и потока управления, методы абстрактной интерпретации, методы

символьного выполнения, методы организации межпроцедурного статического анализа. В частности, указанные методы использованы для построения моделей программы и ее памяти, а также для построения алгоритмов поиска критических ошибок, позволяющих находить ошибки в исходном коде программы и анализировать большие программные системы в миллионы строк кода, получая в среднем 60% истинных предупреждений об ошибках.

Значение полученных соискателем результатов исследования для практики состоит в том, что на основе предложенных автором методов анализа исходного кода программ и архитектуры программной системы анализа разработано и реализовано семейство статических анализаторов Svace, внедренное в жизненный цикл разработки программного обеспечения компании «Самсунг». Инструмент Svace используется также в НИЦ «Курчатовский институт» и для проверки публично создаваемых изменений в исходном коде операционной системы Tizen.

Достоверность результатов исследования состоит в том, что:

- экспериментальные результаты работы получены при анализе больших программных систем на языках Си, Си++, Java, C# размером в миллионы строк исходного кода и показывают в среднем 60% истинных предупреждений об ошибках как результат работы предложенных методов;
- полученные результаты применения разработанных методов анализа находятся на мировом уровне, будучи сопоставимыми с опубликованными в открытых источниках результатами использования других статических анализаторов.

Личный вклад соискателя состоит в личном участии на всех этапах процесса разработки и реализации предложенных методов анализа. В опубликованных совместных работах постановка и исследование задач осуществлялись совместными усилиями соавторов при непосредственном участии соискателя. Выносимые на защиту результаты получены соискателем лично.

На заседании 15 февраля 2018 г. диссертационный совет принял решение присудить Белеванцеву А.А. ученую степень доктора физико-математических наук.

При проведении тайного голосования диссертационный совет в количестве 16 человек, из них 7 докторов наук по специальности рассматриваемой диссертации, участвовавших в заседании, из 20 человек, входящих в состав совета, проголосовали: за – 16, против – 0, недействительных бюллетеней – 0.

Заместитель председателя диссертационного совета,
доктор физико-математических наук Томилин А. Н.

Ученый секретарь диссертационного совета,
кандидат физико-математических наук Зеленов С. В.

15 февраля 2018 года