ОТЗЫВ НАУЧНОГО РУКОВОДИТЕЛЯ

на диссертацию Кошелева Владимира Константиновича
«Межпроцедурный статический анализ для поиска ошибок в исходном коде программ на языке C#», представленную на соискание ученой степени кандидата физико-математических наук по специальности 05.13.11 – математическое и программное обеспечение вычислительных машин, комплексов и компьютерных сетей

Применение методов статического анализа для поиска дефектов и критических ошибок в программах теперь является общепринятым. Для успешного промышленного внедрения при разработке таких методов необходимо достичь компромисса между качеством выдаваемых предупреждений (не менее 60-70% истинных) и количеством пропускаемых ошибок, сохраняя при этом масштабируемость до миллионов строк исходного кода. Задача В.К. Кошелева заключалась в том, чтобы предложить межпроцедурные методы статического анализа для языка C#, который в настоящее время является основным языком разработки в экосистеме Windows, а также набирает популярность в области мобильных приложений (ОС Tizen).

Заданную выше планку анализа для критических ошибок поддерживает единственный инструмент – Coverity Prevent, исходный код которого недоступен. Открытые инструменты сосредоточены на более простых ошибках, для поиска которых достаточно применения анализа на уровне абстрактного синтаксического дерева. Собственный инструмент ИСП РАН Svace статического анализа программ не поддерживает программы на языке C#. Тем самым выбранная тема работы актуальна.

При выборе методов решения исходной задачи Кошелев В.К. сконцентрировался на подходе символьного выполнения, обеспечивающего чувствительность к путям выполнения за счет поддержки формул для выражения текущего пути выполнения и условия искомой ошибки, которые далее проверяются на совместность с помощью SMT-решателей. Так как непосредственное применение символьного выполнения не доставляет необходимой масштабируемости, диссертант использовал технику объединения символьных состояний, позволившую уменьшить их количество, не теряя при этом в точности. Получающиеся логические формулы упрощаются (по результатам тестирования примерно на 30%) за счет знаний об их структуре, полученных из свойств графа потока управления анализируемой процедуры. С помощью вычисления резюме процедуры результаты разработанного внутрипроцедурного алгоритма анализа могут использоваться для межпроцедурного анализа, при этом ограничивается максимальный размер резюме. Диссертантом рассмотрены важные частные случаи анализа процедур без побочных эффектов и межпроцедурного анализа помеченных данных. Корректность всех упомянутых алгоритмов математически доказана.

В ходе рассмотрения вопроса о построении детекторов ошибок доступа по нулевому указателю и утечек ресурсов Кошелев В.К. уделил особое внимание формализации критерия выдачи предупреждения об ошибках. В большинстве известных работ эта тема не затрагивается вообще либо предлагаются некоторые эвристические критерии. Диссертант предложил метод определения ошибочного состояния на основе выбора множества абстрактных состояний, на которых проявляется ошибка, и показал, что различный выбор множества состояний по сути означает разные априорные предположения о контрактах процедур, сделанные анализатором, и, как следствие, определяет набор находимых ошибочных ситуаций. Этот результат был использован при построении алгоритмов упомянутых выше детекторов.

Кошелевым В.К. была выполнена реализация предложенных методов анализа в инструменте SharpChecker, который может использоваться как отдельно, так и в составе пакета инструментов Svace. При тестировании инструмента SharpChecker оказалось, что время анализа пакетов из 1,5 млн. строк кода не превышает получаса, а процент истинных срабатываний для рассмотренных детекторов обнаружения доступа к нулевому указателю и утечки ресурсов не ниже 60%, что показывает полную состоятельность разработанных алгоритмов. Инструмент SharpChecker наряду с инструментом Svace используется в промышленном цикле разработки крупной зарубежной компании.

Считаю, что диссертационная работа соответствует всем требованиям, предъявляемым ВАК к работам на соискание ученой степени кандидата физико-математических наук по специальности 05.13.11 – математическое и программное обеспечение вычислительных машин, комплексов и компьютерных сетей, а ее автор, Кошелев Владимир Константинович, заслуживает присуждения ему ученой степени кандидата физико-математических наук.

Научный руководитель:
в.н.с. ИСП РАН, к.ф.-м.н. А. А. Белеванцев
20 марта 2017 года

Подпись Белеванцева А.А. удостоверяю

Директор ИСП РАН,
д.ф.-м.н. А.И. Аветисян