# ОТЗЫВ

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

В диссертационной работе Кошелева В.К. описывается разработка методов статического анализа, предназначенного для поиска ошибок в исходном коде программ на языке C#. Применение статического анализа в жизненном цикле разработке программного позволяет осуществлять поиск ошибок на путях, плохо покрытых при динамическом анализе и тестировании. Ключевая сложность при разработке статического анализа заключается в поиске компромисса между числом ложных срабатываний, поддерживаемыми классами ошибок и временем работы. В работе В.К. Кошелева рассматриваются методы, позволяющие построить анализатор, имеющий высокий процент истинных срабатываний (более 50%), поддерживающий поиск межпроцедурных ошибок с учетом условий переходов, и позволяющий за несколько часов или менее осуществлять анализ проектов, состоящих из более чем миллиона строк кода.

Структура диссертации включает в себя введение, шесть глав и заключение. Диссертация состоит из 104 страниц, двух таблиц и одного рисунка.

**Во введении** формулируются цель работы, обосновывается её актуальность, приводятся выносимые на защиту основные положения диссертационной работы.

**В первой** главе рассматриваются научные работы, описывающие методы статического анализа для поиска ошибок в исходном коде программ. Приводится классификация данных методов исходя из их применимости. Для решения задачи поиска ошибок на практике используются методы, сочетающие чувствительность к путям с использованием резюме. В главе обсуждаются особенности и различия ряда открытых и коммерческих статических анализаторов для языков C# и C/C++.

**Во второй** главе обсуждаются особенности организации статического анализа для Sпрограмм на языке C#. Описывается использующееся в работе внутреннее представление с учётом специфики языка C#.

**Третья** глава описывает внутрипроцедурный анализ, чувствительный к потоку, контексту и путям. Приведённый анализ использует метод символьного выполнения, адаптированный к задаче статического поиска ошибок в исходном коде. Отличительными особенностями приведённого внутрипроцедурного анализа являются: сохраняющее чувствительность к путям объединение состояний; использование свойств доминирования

и постдоминирования для вычисления предикатов пути и условий в точках слияния. Для алгоритмов построения объединённого символьного состояния, а также для операций, проводимых с объединённым символьным состоянием, доказана корректность. Показана корректность алгоритмов построения предикатов пути и условий в точках слияния. В последней части главы обсуждается метод обработки циклов с фиксированным числом итераций.

**В четвертой** главе описываются алгоритмы построения и применения резюме. Использующиеся алгоритмы сохраняют информацию о состоянии памяти вызванного метода. В резюме также сохраняется информация о возможных исключениях и условиях, при которых они происходят. Рассматривается вариант организации межпроцедурного анализа помеченных данных, основанный на сведении к IFDS-задаче. Также рассматриваются вопросы организации анализа чистых методов на основании построенных резюме.

**В пятой** главе вводится определение ошибочной ситуации для рассматриваемого ранее символьного выполнения. Рассматривается класс возможных определений ошибочной ситуации, проводится сравнение этих классов. Приводятся примеры, иллюстрирующие различия между ними. Для одного из определений ошибки предлагаются алгоритмы поиска ошибок доступа к нулевому указателю и утечки ресурсов. В завершении главы рассматриваются причины, по которым приведённые алгоритмы поиска ошибок являются нестрогими.

**Шестая** глава посвящена инструменту статического анализа SharpChecker. В данном инструменте реализованы предложные ранее алгоритмы поиска ошибок. В главе обсуждаются технические детали реализации, такие, как построение графов вызовов и потоков управления, порядок обхода методов. Тестирования анализатора на соответствие заявленным требованиям проводилось на наборе проектов с открытым исходным кодом. Для проектов, содержащих 1.2-1.5 миллионов строк кода, время анализа не превысило получаса. Среди ошибок доступа к нулевому указателю истинными являются не менее 60%, а среди утечек ресурсов – не менее 70%. Таким образом, показано соответствие предложенных методов анализа заявленным требованиям.

Заключение содержит список результатов, достигнутых в ходе данной работы.

По диссертации могут быть сделаны следующие замечания:

1. Для демонстрации соответствия предложенных методов заявленным требованиям предлагается провести тестирование инструмента, реализующего методы, на наборе проектов с открытым исходным кодом. Однако в диссертации отсутствует обоснование выбора проектов для тестирования.

2. В четвертой главе предлагается использовать основанный на алгоритме IFDS анализ помеченных данных. Для данного анализа отсутствуют детальное описание и результаты практического применения.
3. Тестирование разработанного инструмента проводилось только для двух групп дефектов («доступ к нулевому указателю» и «утечка ресурсов»), в работе отсутствует оценка зависимости времени анализа от количества включенных детекторов.
4. Разработанный алгоритм не учитывает возможности вызова из программы на языке C# неуправляемого кода на языке C++ при помощи маршаллинга (создание моста между управляемым и неуправляемым кодом). Следует отметить, что аналогичные коммерческие и открытые статические анализаторы для языка C# также не имеют данной функциональности.

Отмеченные замечания не снижают общей научной и практической ценности диссертационной работы и не влияют на её положительную оценку. Автореферат кратко и правильно отражает содержание диссертационной работы. Диссертация В.К. Кошелева является законченной научно-исследовательской работой. Она отвечает всем требованиям ВАК РФ, предъявляемым к диссертациям на соискание ученой степени кандидата физико-математических наук, а Кошелев Владимир Константинович заслуживает присуждения ему ученой степени кандидата физико-математических наук по специальности 05.13.11 – математическое и программное обеспечение вычислительных машин, комплексов и компьютерных сетей.

Старший инженер-программист
ООО «Исследовательский центр Самсунг»
Кандидат технических наук
по специальности
05.13.11 - математическое и программное
обеспечение вычислительных машин,
комплексов и компьютерных сетей Павлов Евгений Геннадьевич

Дата: 24.04.17