ОТЗЫВ ОФИЦИАЛЬНОГО ОППОНЕНТА
доктора технических наук, член-корр. РАН
Шабанова Бориса Михайловича
на диссертационную работу Чан Ти Тхиена
по теме «**Разработка нового метода автоматизированного тестирования программных библиотек**»,
представленную к защите на соискание ученой степени кандидата технических наук по специальности 2.3.5 – «Математическое и программное обеспечение вычислительных систем, комплексов и компьютерных сетей»

Актуальность темы

Широкое применение библиотек в разработке программного обеспечения, рост их размера и сложности делает актуальной задачу автоматического тестирования программных библиотек. Одним из эффективных методов поиска ошибок в программном обеспечении (ПО) является метод фаззинга, который является частью процесса безопасной разработки ПО. При применении тестирования методом фаззинга для библиотек тестировщики тратят много усилий на изучение исходного кода библиотек и написание для каждой функции библиотеки тестового окружения (фаззинг-обертки), необходимых для передачи мутационных данных из фаззера на вход тестируемым программам.

Диссертационная работа Чан Ти Тхиена посвящена разработке метода автоматизированного тестирования библиотек, который позволяет сократить трудоемкость тестирования за счет автоматической генерации фаззинг-оберток. Предложенный метод представляет интерес как в научном плане, так и в практике промышленного тестирования.

Автор подготовил достаточно полный обзор существующих подходов и инструментов, из которого следует, что полученные результаты являются новыми и значимыми на фоне известных результатов в данной области. По результатам работы опубликовано 5 печатных работ, в том числе 3 публикации, удовлетворяющие требованиям п.11 Положения о присуждении ученых степеней.

Научная новизна представленных результатов состоит в том, что

- Предложен метод генерации фаззинг-оберток для функций библиотеки, который позволяет генерировать нацеленные тесты в условиях отсутствия информации о контексте использования библиотеки.
- Предложен метод генерации фаззинг-оберток для функций библиотеки с учетом контекста использования библиотеки в пользовательской программе, который позволяет нацелить генератор только на используемые интерфейсы библиотеки.

Достоверность и апробация результатов исследования

В основу работы были положены новейшие результаты в области средств анализа программного кода, опубликованные в российских и зарубежных изданиях. Положения диссертации логично следуют их этих результатов, развивая и дополняя их. Кроме этого, достоверность результатов подтверждается в диссертации многочисленными примерами работы предложенных методов и программного средства Futag, публичным размещением программного средства Futag в виде открытых исходных кодов, наличием акта о внедрении результатов исследования в практику. Результаты диссертационной работы докладывались на международных и российских научных конференциях.

Практическая значимость

Разработанные соискателем методы реализованы им в виде инструментального программного средства Futag и внедрены в практическую деятельность НТЦ «Фобос-НТ» и были применены в сертификационных испытаниях в системе сертификации ФСТЭК России.

Основные результаты и положительные стороны исследования

Предложенные соискателем методы генерации фаззинг-оберток для функций библиотеки способны работать как с учетом контекста

использования, так и в условиях отсутствия информации о контексте использования. Анализ диссертации позволяет сделать вывод о высоком профессиональном уровне соискателя как программиста-разработчика. Предложенные в диссертации решения в достаточной степени обоснованы и логически следуют из поставленных в работе цели, задач и анализа предметной области. Автореферат соответствует тексту диссертации, адекватно и полно отражая ее основное содержание.

Замечания.

По работе могут быть сделаны следующие замечания.

1. Приведенное в п. 5.4.3 диссертации сравнение предложенных соискателем решений с известными инструментами FuzzGen и OzzFuzz носит преимущественно качественный характер, количественные экспериментальные оценки отсутствуют.

2. Не представлены результаты тестирования разработанного соискателем инструмента Futag на проектах с исходным кодом на языке C++, а также не проведено обоснование полученных результатов времени работы и их разницы между проектами: так, в библиотеке openssl на создание 255 оберток потрачено 2172 секунды, а в libjson – на 612 оберток потрачено всего 180 секунд.

3. При оформлении диссертации проявлены небрежности, затрудняющие ее чтение.

– по тексту диссертации в разных местах применяются разные разделители групп разрядов в числах (например, в таблице 1 – точка, а таблицах 2 и 3 – пробел);

– отсутствуют параграфы выводов по главам 2-5;

– заголовок таблицы 3 приведен после таблицы.

Несмотря на сделанные замечания, считаю, что диссертационная работа соискателя представляет собой законченное исследование, обладающее внутренним единством и имеющее несомненную научную и практическую ценность. Представленная работа удовлетворяет

требованиям ВАК, предъявляемым к кандидатским диссертациям, а ее автор Чан Ти Тхиен заслуживает присуждения ученой степени кандидата технических наук по специальности 2.3.5 – «Математическое и программное обеспечение вычислительных систем, комплексов и компьютерных сетей».

Официальный оппонент,
член-корр. РАН, д.т.н., доцент,
директор Межведомственного суперкомпьютерного
центра РАН (МСЦ РАН),
заместитель директора по научной работе
Федерального государственного учреждения
«Федеральный научный центр
Научно-исследовательский институт
системных исследований
Российской академии наук» Б.М. Шабанов

Подпись Шабанова Б.М. удостоверяю
Начальник отдела кадров МСЦ РАН В.В. Шишкина
«26» октября 2023 г.