ОТЗЫВ ОФИЦИАЛЬНОГО ОППОНЕНТА

Тормасова Александра Геннадьевича

на диссертационную работу Захарова Ильи Сергеевича «Методы декомпозиции систем и моделирования окружения программных модулей для верификации Си-программ», представленную на соискание ученой степени кандидата физико-математических наук по специальности 05.13.11 — математическое и программное обеспечение вычислительных машин, комплексов и компьютерных сетей

Актуальность темы

Крупные программные системы на языке программирования Си составляют значительную часть системного программного обеспечения, которое лежит в основе широкого спектра информационных систем и программно-аппаратных платформ. Ошибки и уязвимости информационной безопасности, которые своевременно не удалось обнаружить в таких Си-программах, уже приводили к крупным убыткам и другим нежелательным последствиям. Программная инженерия предлагает разные подходы для повышения надежности и защищенности программных продуктов, в основе которых лежит систематическая работа по выделению требований к программам и контролю за их соблюдением за счет верификации.

В зависимости от этапа жизненного цикла программной системы и особенностей ее устройства на практике применяются различные комбинации методов верификации. В данной работе рассматривается задача проверки требований к модулям крупных программных систем на языке программирования Си при помощи инструментов верификации моделей программ. Несмотря на успехи, достигнутые в последнее время в развитии и применении инструментов верификации моделей программ, уровень трудоемкости и требования к квалификации инженеров все еще не позволяют применять современные инструменты для верификации крупных программных систем на языке Си, за исключением ряда узких приложений таких, как,

например, верификация драйверов операционных систем или встраиваемое программное обеспечение.

Целью диссертационной работы является развитие методов верификации крупных программных систем на языке программирования Си с использованием инструментов верификации моделей программ для сокращения трудозатрат и времени, необходимых для выполнения верификации. Для достижения данной цели предлагается автоматизировать декомпозицию программных систем на модули и синтез моделей окружения.

Достоверность полученных результатов и новизна диссертационного исследования

Научной новизной обладают следующие результаты диссертационной работы:

- Метод декомпозиции программных систем на языке программирования Си на модули.
- Метод спецификации моделей окружения для модулей программных систем на языке программирования Си на основе параллельной композиции систем переходов и доказательство теоремы об изоморфизме множеств достижимых ошибочных состояний спецификации и результата ее трансляции на язык Си.
- Метод автоматизированного синтеза моделей окружения для модулей программных систем на языке программирования Си, позволяющий выполнять адаптацию процесса синтеза для проверки разных видов требований к Си-программам с различной архитектурой.

Достоверность полученных в диссертационной работе результатов подтверждается апробацией как на научно-практических международных конференциях и семинарах, так и публикациями в рецензируемых журналах, а также использованием обоснованных научных методик проведения научных

исследований и экспериментальным подтверждением свойств предложенных методов на практике.

Обоснованность научных положений, выводов и рекомендаций

Обоснованность научных положений и выводов подтверждается анализом российских и зарубежных научных работ в области разработки и использования инструментов верификации моделей программ. Научные результаты диссертационного исследования обсуждены на международных конференциях, изложены в 11 публикациях, а ряд реализаций методов защищены свидетельствами о регистрации программ для ЭВМ.

По теме диссертации автором было опубликовано 11 работ, и которых 9 опубликованы в изданиях списка ВАК, а 6 входят в международную систему цитирования Scopus. По результатам работы автором было получено 4 свидетельства государственной регистрации программ для ЭВМ.

Научная и практическая значимость результатов исследования

Предложенные в данной работе методы реализованы в системе верификации Klever, предназначенной для проверки требований при помощи инструментов верификации моделей Си-программ. Система имеет открытый исходный код, а результаты ее практического применения подтверждают возможность выявления ошибок в модулях крупных программных систем. Изложенные в данной работе методы являются полезными как при проектировании и реализации новых специализированных систем верификации, так и для дальнейшего развития методов модульной верификации крупных программных систем на языке Си.

Замечания и недостатки по диссертационной работе

В работе имеются следующие отдельные недостатки, а именно.

1. Метод автоматизированной декомпозиции подразумевает ручную работу по определению модулей, но в работе не представлены подходы, которые могли бы облегчить эту деятельность для инженера, кроме как для

непосредственно рассмотренных в работе BusyBox и Linux. Специфицирование правил, целей и лучших практик облегчило бы прикладное применение подхода в промышленности.

2. Не совсем понятно, каким образом предполагается учесть возможные ошибки при специфицировании окружения, которое требует большой ручной работы, не предложено методик тестирования. Ошибки в этом процессе могут существенно повлиять на вердикт системы. Анализ возможности, вероятности и последствий их появления (влияния на вердикт) представляется необходимым компонентом реальной системы промышленного уровня.
3. В работе недостаточно обосновывается использование единственно рассмотренной модели синхронизации как «рандеву между парами моделей сценариев». В частности, вопрос полноты охвата ей всех возможных сценариев параллельного исполнения и асинхронных событий во внешних средах не рассмотрен.
4. В работе не представлены рекомендации по разработке специализированных построителей моделей сценариев, которые требуются для верификации программных систем с событийно-ориентированным устройством.

Заключение

Указанные недостатки не влияют на общую положительную оценку диссертационной работы. Считаю, что диссертационная работа И. С. Захарова является законченной научно-квалификационной работой, которая обладает актуальностью, научной новизной и практической значимостью.

Результаты диссертационного исследования соответствуют паспорту специальности 05.13.11 – «Математическое и программное обеспечение вычислительных машин, комплексов и компьютерных сетей». Автореферат полно и правильно отражает содержание диссертационной работы.

Диссертационная работа И. С. Захарова выполнена в соответствии с положением ВАК РФ о присуждении ученых степеней, утвержденного Постановлением Правительства РФ №842 от 24.09.2013, а ее автор, Захаров Илья Сергеевич заслуживает присуждения ему ученой степени кандидата физико-математических наук по специальности 05.13.11 – «Математическое и программное обеспечение вычислительных машин, комплексов и компьютерных сетей».

Официальный оппонент
доктор физико-математических наук, профессор,
ректор Автономной некоммерческой организации
высшего образования «Университет Иннополис» А.Г. Тормасов

26 09 2019 г.