ОТЗЫВ ОФИЦИАЛЬНОГО ОППОНЕНТА

на диссертационную работу Захарова Ильи Сергеевича

«Методы декомпозиции систем и моделирования окружения программных модулей для верификации Си-программ»,

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

На сегодняшний день разрабатывается множество программных систем, объем кода которых составляет сотни тысяч или миллионы строк кода. Код многих из этих систем является открытым. Одной из наиболее известных таких систем, разработанной на языке Си, является ядро операционной системы Linux. Открытость кода дала возможность разработчикам со всего мира создавать на его основе новые программные продукты. К некоторым из таких продуктов предъявляются особенно высокие требования надежности и безопасности, не принятые во внимание разработчиками системы, взятой за основу.

Ключ к выполнению этих требований лежит в применении формальных методов верификации, позволяющих получить математическое обоснование соответствия программы предъявляемым к ней требованиям. Однако еще не существует метода верификации, который позволил бы автоматически получать такие обоснования для программных систем с большим объемом кода. Современные инструменты, нацеленные на максимальную автоматизацию процесса верификации, способны работать с программами, размер кода которых не превышает нескольких десятков тысяч строк. Обеспечить применимость таких инструментов к программным системам большего размера можно на основе достаточно ясной идеи, лежащей в основе диссертации: разбить систему на модули и верифицировать их по-отдельности, упрощенно представляя для каждого модуля воздействия на него со стороны оставшейся части системы. Однако реализация этой идеи

сопряжена со множеством трудностей. Диссертационная работа является шагом в преодолении этих трудностей, что определяет ее несомненную *актуальность*.

Основной практический результат работы видится в том, что автор разработал и реализовал в программной системе методы автоматизированного разбиения Си-программ на модули и автоматизированного создания моделей окружения модулей. Ручное решение этих задач сопряжено с рядом проблем. Монолитный стиль программного кода на языке Си многих систем делает задачу выделения модулей достаточно сложной. Задача же разработки моделей окружения модулей для целей верификации требует особого внимания, так как недостаточно детальные модели окружения могут свести на нет все усилия по верификации, поскольку многие ошибки останутся необнаруженными.

В то же время, разработанные в диссертации методы не являются универсальными, что автор верно отмечает и оставляет возможности для ручного вмешательства в процесс разбиения программы на модули и создания моделей окружения модулей. Следует отметить, что собственно верификация модулей, полученных на основе методов, разработанных в диссертации, осуществляется с помощью сторонних инструментов, реализующих метод проверки моделей. С развитием этих инструментов применимость и результативность методов, предложенных в диссертации, будет увеличиваться.

При всех своих достоинствах, работа не свободна и от некоторых недостатков. Во второй главе представлены основные для работы метод автоматизированного разбиения программной системы на модули и метод синтеза моделей окружения модулей. Однако отсутствуют математические описания алгоритмов, реализующих разработанные методы. Словесные описания скорее во многом определяют требования к алгоритмам и в

некоторой степени обсуждают возможные пути решения задач, возникающих при реализации методов, нежели предлагают и анализируют конкретные алгоритмические решения.

Иногда используются термины, определение которых дано в тексте только позднее первого использования. Так, термин «спецификация декомпозиции» впервые встречается на странице 49 и используется на последующих страницах, а поясняется только на странице 57. Работа содержит достаточно большое количество опечаток и мелких ошибок (в том числе пунктуационных).

Приведенные замечания не ставят под сомнение ценность работы в целом. Научные положения, выводы и рекомендации, сформулированные в диссертации вполне обоснованы и достоверны, что подтверждается реализацией разработанных методов в системе верификации Klever с открытым исходным кодом, разрабатываемой в Институте системного программирования им. В.П. Иванникова РАН, и их применением для верификации существующих программных систем: ядра Linux и апплетов проекта BusyBox. Научной новизной обладают метод автоматизированной декомпозиции Си-программ на модули, метод задания сценариев для моделей окружения получаемых модулей и метод автоматизированного синтеза моделей окружения для модулей. Основные результаты диссертации прошли апробацию на российских и зарубежных научно-технических конференциях и опубликованы, в том числе в изданиях, входящих в перечень ВАК РФ. Автореферат полно отражает содержание диссертации.

Таким образом, можно заключить, что работа отвечает всем требованиям, предъявляемым к кандидатским диссертациям положением ВАК РФ о порядке присуждения ученых степеней, 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
кандидат технических наук,
разработчик-исследователь
АО «Лаборатория Касперского»
Россия, Москва, 125212
Ленинградское шоссе, д.39А, стр.3
БЦ «Олимпия Парк»

Буренков Владимир Сергеевич

19 апреля 2019 г.