Отзыв

научного руководителя на магистерскую диссертацию

Полубеловой Марины Игоревны

“Компиляция сертифицированных F*-программ в робастные Web-приложения”

Вопрос надёжности программ становится всё более актуальным. Одна из областей, где обеспечение надёжности особенно востребовано — это передача данных в различных сетях, например, в сети Internet, что требует разработки различных криптографических протоколов и примитивов. Сложность заключается в том, что даже при наличии надёжного алгоритма, скажем, шифрования, никто не застрахован от ошибок в его программной реализации. Один из подходов, призванных решить данную проблему — сертифицированное программирование, позволяющее доказывать соответствие программы и её формальной спецификации. Однако, для этого используются специализированные системы, такие как Coq, Agda, использующие специализированные языки, в то время, как для практического применения в Web-приложениях, необходимы компоненты, реализованные на JavaScript. Таким образом, возникает необходимость создания транслятора из специализированного языка в язык общего назначения. При этом необходимо гарантировать, что данный транслятор сохраняет семантику исходной программы.

Один из представителей языков, позволяющих доказывать формальные свойства программ — это язык F*, разрабатываемый совместно INRIA и Microsoft Research. Однако, данный язык не позволяет исполнять программы. Таким образом, задача, поставленная перед М.И. Полубеловой — создания транслятора из F* в JavaScript, что должно позволить создавать надёжные Web-приложения. Данная работа инициирована в ходе стажировки М.И. Полубеловой в INRIA, в команде F* и выполнялась при непосредственном сотрудничестве с данной командой.

В ходе работы М.И. Полубелова проявила самостоятельность как в изучении необходимых материалов, так и при работе над решением. Изучены новые области, такие как сертификационное программирование и язык F*, некоторые алгоритмы шифрования. Продемонстрированы не только инженерные навыки, но и хорошая математическая подготовка, которая потребовалась при формализации алгоритмов шифрования, на которых проводилась апробация.

Текст диссертации аккуратный, в достаточной мере отражает проделанную работу.

В ходе работы над диссертацией был сделан доклад на конференции SYRCoSE-2016, часть результатов опубликована в журнале “Труды Института системного программирования РАН”, входящем в список ВАК. Исходный код разработанного транслятора находится в основном репозитории проекта F*. Считаю, что работа заслуживает оценки «отлично».

К.ф.-м.н., доцент кафедры информатики СПбГУ
Григорьев Семён Вячеславович