Отзыв научного руководителя

на магистерскую диссертацию работу студентки кафедры системного программирования СПбГУ

Соковиковой Светланы Алексеевны

Тема выпускной квалификационной работы:

“Верификация контрактов в криптовалюте Ethereum”

Поиск уязвимостей в смарт-контрактах криптовалюты Ethereum является одной из наиболее актуальных задач компьютерной безопасности. Программы, которые работают в публичной блокчейн-сети, имеют дело непосредственно с деньгами клиентов. Тем важней становится своевременное нахождение возможных сценариев атаки на смарт-контракты и предотвращение возможных хищений.

В работе студентки представлен прототип программы по верификации смарт-контракта. инструмент предназначен для поиска наиболее опасных видов уязвимостей - перевызываемость функций контрактов и недостаточная защищенность деструктора. В качестве технологии поиска уязвимостей используется программа верификации темпоральных моделей spin, которая в 2002 году получила награду ACM System Software Award. Полученные результаты должны быть использованы на практике при более глубоком анализе массива смарт-контрактов основной сети Ethereum.

В ходе работы студентка самостоятельно изучила предметную область. Произвела сбор данных по инструментам верификации, типам уязвимостей смарт-контрактов, самостоятельно выучила язык Promela, Solidity, ассемблер EVM, освоила методику верификации на основе SPIN.

Проверка ВКР на предмет наличия/отсутствия неправомерных заимствований показала, что работа неправомерных заимствований не содержит.

В ходе работы студентка активно взаимодействовала с научным руководителем, своевременно выполняла поставленные задачи, проявляла самостоятельность, оперативно устраняла выявленные замечания к работе. Считаю, что работа заслуживает оценку “**отлично**”.

д. ф.-м. н., проф. Терехов А.Н.

Дата: 31/05/19

Подпись: