ОТЗЫВ НАУЧНОГО РУКОВОДИТЕЛЯ

на выпускную квалификационную работу студентки 4 курса
кафедры системного программирования СПбГУ
Тарасовой Полины Максимовны, обучающейся по направлению 010500 (02.03.03)
(математическое обеспечение и администрирование информационных систем)

Тема выпускной квалификационной работы:
«Восстановление адресного пространства процесса в Windows 10»

ОС Windows 10, являясь последней версией самой распространённой операционной системы от Microsoft, вполне предсказуемо наращивает количество своих инсталляций. Также вполне предсказуемо, что с выходом новой версии множество системных инструментов, использующих специфику прошлых версий Windows, перестали работать. Одной из сложностей в обновлении ПО является недостаточная документированность технических деталей и внутренних форматов, часть которых является закрытыми и в принципе не публикуются. Данная работа посвящена изучению форматов хранения данных в оперативной памяти Windows 10.

Перед студенткой Тарасовой П.М. стояла следующая задача: разработать метод восстановления адресного пространства процесса Windows 10 x86 PAE и реализовать этот метод, внедрив его в коммерческий продукт Belkasoft Evidence Center.

В ходе работы Полина Максимовна выполнила обзор существующих средств для анализа оперативной памяти, изучила недокументированные структуры памяти Windows 10 x86 PAE, нашла устойчивую сигнатуру для поиска процессов данной операционной системы, а также реализовала метод восстановления адресного пространства процесса.

В процессе работы Полина активно взаимодействовала с научным руководителем, своевременно выполняла поставленные задачи.

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

В ходе работы студентка внедрила указанный алгоритм в коммерческий продукт, обнаружила и исправила критические проблемы в целевом продукте. Среди недостатков работы можно упомянуть частые задержки на этапах изучения структур памяти и внедрения реализованного решения, а также написание текста работы в последний момент, что не позволило улучшить этот текст совместно с научным руководителем. Чуть большая оперативность в работе позволила бы Полине Максимовне реализовать восстановление процессов не только 32-, но и 64-битной версии Windows.

Вместе с тем, считаю, что работа выполнена на высоком профессиональном уровне и заслуживает оценки «отлично».

29 мая 2017г.

Губанов Юрий Александрович,
Ст. преп. каф. сист. прогр.
математико-механического
факультета СПбГУ