Отзыв научного руководителя

на выпускную квалификационную работу студента Небогатикова Ивана Юрьевича, обучающийся по направлению 02.03.03 (Математическое обеспечение и администрирование информационных систем)

Тема выпускной квалификационной работы:

“Мониторинг работы операционной системы в реальном времени на основе гипервизора”

Методы фильтрации системных вызовов, которые использует антивирус КОДА для поиска вредоносного ПО, считаются операционной системой подозрительными. Kernel Patch Protection, защищающий ядро Windows, не позволяет менять обработчик системных вызовов и мешает основной функциональности КОДЫ. Помимо этого, антивирус устанавливается в потенциально опасную среду, где другие программы могут пытаться читать чужие файлы, не имея к ним доступа, искать и выгружать системы защиты.

Перед Иваном Юрьевичем была поставлена цель защитить КОДУ от описанных проблем.

В ходе работы Иван Юрьевич изучил, подробно описал основные векторы атак на антивирус, изучил существующие техники защиты ПО, в том числе на основе гипервизора, реализовал систему защиты системы КОДА от выгрузки, перетирания файлов и завершения работы сервиса драйвера. Созданное решение было протестировано на производительность и показало хорошие результаты. Реализация встроена в КОДУ и протестирована с ней, текущие и потенциальные угрозы были устранены.

Результаты работы были представлены на конференции СПИСОК 2019.

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

В процессе работы Иван Юрьевич активно взаимодействовал с научным руководителем, своевременно выполнял поставленные задачи, проявлял самостоятельность и демонстрировал хорошие технические навыки. Считаю, что работа заслуживает оценки “отлично”.

Ханов Артур Рафаэльевич,
старший преподаватель кафедры системного программирования СПбГУ

Дата: Подпись:_____