

### **Отзыв научного руководителя**

на выпускную квалификационную работу студента Виноградова Михаила Викторовича,  
обучающегося по направлению 02.03.03 (Математическое обеспечение и  
администрирование информационных систем)

Тема выпускной квалификационной работы:

“Исследование уязвимости iOS tftp для применения в криминалистическом анализе”

Перед Михаилом Викторовичем задача была поставлена в ходе его трудовой деятельности в компании “Belkasoft”, одного из мировых лидеров в области цифровой криминалистики. Мобильные телефоны под управлением ОС iOS широко распространены и содержат массу личных данных об их пользователе, которые довольно сложно извлечь из-за хорошей защищённости системы от неавторизованного доступа. Эти личные данные (такие как данные геолокации или программ для обмена сообщениями) могут быть критичны для следствия, так что криминалистам приходится решать типично хакерские задачи, чтобы эти данные заполучить. Несколько облегчает работу то, что, как правило, уязвимости уже найдены и документированы “настоящими” хакерами, но использовать их для получения данных и интегрировать их в программный комплекс криминалистического анализа само по себе является сложной инженерной задачей. Ей и занимался Михаил Викторович в ходе работы над ВКР.

В ходе работы всё-таки пришлось подробно разобраться с уязвимостью “tftp”, поскольку за время работы над ВКР вышло несколько новых версий iOS, для которых использование уязвимости несколько отличалось. К счастью, уязвимости в новых версиях искались и документировались сторонними командами быстрее, чем это успевал делать Михаил Викторович, поэтому собственно обходить защиту iOS самостоятельно не потребовалось. Тем не менее, в ходе работы пришлось разбираться в низкоуровневом устройстве iOS (например, для открытия беспарольного SSH-соединения с устройством и временного отключения блокировки экрана). Также подсистема получения данных с телефона была интегрирована в продукт Belkasoft Evidence Center, что потребовало рефакторинга соответствующей части этого продукта, что, в свою очередь, потребовало некоторого объёма программирования на C# и демонстрации архитектурных навыков. Была выполнена апробация, показавшая, что программный компонент, разработанный Михаилом Викторовичем, позволяет получить с телефона гораздо больше данных, чем использовавшийся в Belkasoft Evidence Center ранее способ через получение резервной копии.

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

В ходе работы Михаил Викторович показал себя специалистом, способным от начала и до конца решить поставленную задачу. Результаты его ВКР были внедрены в систему Belkasoft Evidence Center, ещё в апреле релиз с функциональностью Михаила Викторовича стал доступен конечным пользователям, что для ВКР бакалавра очень хорошо. Связь с научным руководителем и консультантом поддерживалась регулярно (причём, по инициативе самого Михаила Викторовича), задачи решались в срок, текст работы был написан заблаговременно и, хотя изначально в нём присутствовало большое количество грамматических и стилистических ошибок, успел пройти несколько итераций

исправления и сейчас вполне адекватно излагает суть работы. Имеется положительный отзыв от консультанта. Считаю, что работа, безусловно, заслуживает оценки **"отлично"**.

Литвинов Юрий Викторович,  
к.т.н., доцент кафедры системного программирования СПбГУ

Дата: 19.05.2019

Подпись: Литв