Отзыв научного руководителя

на выпускную квалификационную работу Белошапкина Михаила Юрьевича, обучающегося по направлению 02.03.03 (Математическое обеспечение и администрирование информационных систем)
Тема выпускной квалификационной работы:
«Извлечение данных keychain из облачного хранилища iCloud»

Работа Михаила Юрьевича проходила по теме от компании «Цифровая корпоративная защита», одного из крупнейших российских разработчиков средств для цифровой криминалистики. Продукт Belkasoft X этой компании поддерживает сбор и обработку информации из очень большого количества источников, в частности, из Apple iCloud. Задачей Михаила Юрьевича стала поддержка извлечения из iCloud данных iCloud keychain. Обратим внимание, что, как и обычно в цифровой криминалистике, речь идёт не о «взломе» сервиса (что в случае iCloud keychain вряд ли в принципе реализуемо в рамках студенческой работы), а о получении данных в удобном для обработки виде при наличии возможности законно авторизоваться в сервисе. Задача актуальна, поскольку в iCloud keychain могут храниться пароли пользователя от множества сервисов, возможность их получать может быть очень важна для криминалиста.

В ходе работы Михаил Юрьевич выполнил обзор существующих инструментов и статей, научился пользоваться утилитами Burp Suite, SSL Kill Switch, Frida, выполнил дамп и анализ трафика в разных режимах получения keychain из iCloud. Было реализовано извлечение ключей из Escrow Proxy, дешифровка с их помощью значений из keychain с помощью библиотеки corecrypto. В итоге была реализована полная схема скачивания и расшифровки keychain, проведена апробация на тестовых учётных записях на трёх разных устройствах с разной версией iOS.

Михаил Юрьевич регулярно отчитывался о ходе работы, текст сдал раньше срока, но изначально изобилующий неточностями и опечатками. Замечания были поправлены к итоговой версии. Анализ текста на наличие неправомерных заимствований показал, что неправомерных заимствований текст не содержит.

Михаил Юрьевич в ходе работы получил ценные и редкие навыки цифровой криминалистики, разобрался в сложном протоколе и реализовал инструмент получения данных, однако не успел довести работу до продуктового состояния. Трудности с реализацией оставили слишком мало времени на оформление работы, в релиз функциональность не попала, что является большим минусом. Однако имеется положительный отзыв консультанта, где также отмечается пропуск сроков, но подчёркивается объём исследовательской части работы и утверждается, что студент получил много опыта и навыков и показал себя как опытный программист. Следуя мнению консультанта, рекомендую оценку «**отлично**».

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

Дата: 17.05.2023 года Подпись: