

Отзыв научного руководителя

на выпускную квалификационную работу Даниила Фёдоровича Степырева,
обучающегося по направлению 02.03.03 (Математическое обеспечение и
администрирование информационных систем)

Тема выпускной квалификационной работы:
«Использование уязвимостей ОС Windows для повышения привилегий
пользователя в цифровой криминалистике»

Выпускная квалификационная работа Даниила Фёдоровича проходила по теме от компании Belkasoft, одного из ведущих разработчиков программного обеспечения для цифровой криминалистики. Даниилу Фёдоровичу было поручено исследовать известные уязвимости ОС Windows для повышения привилегий пользователей для того, чтобы реализовать их в продукте компании Belkasoft для извлечения защищённых данных с компьютеров подозреваемых. Все уязвимости известны, многие из них даже реализованы, так что о хакерстве в данной работе речи не идёт. Однако необходимо их протестировать на разных версиях Windows 7, 10 и 11, и внедрить их реализацию в программный продукт.

В ходе работы было детально рассмотрено четыре известные уязвимости, обнаруженные в 2021 году. Эксплуатация одной из них, наиболее применимой, была реализована в виде библиотеки на C++. Также был реализован на C# модуль повышения привилегий для Belkasoft Launcher, использующий данную библиотеку, и компонент, отвечающий за определение возможности применения уязвимости. Разработанные компоненты прошли внутреннее тестирование и попали в апрельский релиз Belkasoft Triage.

Даниил Фёдорович регулярно отчитывался о ходе работы, вёл детальные заметки о ходе исследований, текст был сдан вовремя. Анализ текста на наличие неправомерных заимствований показал, что текст неправомерных заимствований не содержит.

Даниил Фёдорович проявлял проактивность в рамках совместной работы, ответственно подходил к исследованию уязвимостей и особенностей их поведения на разных версиях целевых ОС. В процессе реализации компонент показал высокий уровень навыков программной инженерии, ключевые части компонент сопровождались тестами и документацией. Разработанная система на данный момент доступна клиентам Belkasoft, что демонстрирует сформированность компетенций Даниила Фёдоровича. Имеется акт о внедрении и положительный отзыв консультанта. Рекомендую оценку **«отлично»**.

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

Дата: 04.06.2022 года

Подпись: 