РЕЦЕНЗИЯ
на выпускную квалификационную работу обучающегося СПбГУ
Тарасовой Полины Максимовны
по теме «Восстановление виртуального адресного пространства процесса в Windows 10»

В выпускной квалификационной работе рассматривается метод восстановления виртуального адресного пространства процесса в Windows 10. Работа опирается на уже реализованные методы восстановления адресного пространства Windows 7 x86/x64 применительно к адресному пространству Windows 10. Описывается структура организации процессов в памяти. Производится сравнение различных методов детектирования и поиска этих структур. Описываются отличия структуры организации процессов в памяти Windows 7 и Windows 10 и проблемы, вызванные ими. Дается обзор существующих решений по данной проблеме. Отдельное внимание уделяется механизму виртуализации памяти и трансляции виртуальных адресов для архитектуры x86 PAE. Описывается метод обработки недействительных блоков памяти и, в качестве примера, рассматривается теоретический алгоритм получения виртуального адресного пространства для конкретной архитектуры. С помощью анализа находится сигнатура для поиска EPROCESS структур в памяти Windows 10, на основе которого строится метод для их идентификации и производится уточнение границ пользовательского адресного пространства. Приводятся результаты интеграции метода в продукт Belkasoft Evidence Center. Описывается методика и результаты тестирования работы метода.

В введении автором обосновывается актуальность данной проблемы и приводятся сценарии применения предложенных методов в сфере компьютерной криминалистики.

В работе были выявлены следующие недостатки:

1. Имеются грамматические и синтаксические ошибки в тексте работы, а также во многих местах наблюдается неаккуратность в её оформлении.
2. В работе часто встречаются глубоко проработанные технические описания различных механизмов организации памяти, относящиеся к проблеме, но выбивающиеся из основного повествования.
3. В ходе работы встречаются аббревиатуры, которые никак не поясняются.
4. После нахождения сигнатуры структуры EPROCESS и выбора её для применения в сигнатурном методе поиска этих структур в п.4.1, не производится обоснования использования именно этого метода и его сравнения с другими приведенными ранее методами.
5. В работе не приводятся преимущества реализованного метода восстановления виртуального адресного пространства по сравнению с существующими решениями.

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

На основании вышеизложенного можно заключить, что выпускная квалификационная работа соответствует основным требованиям, предъявляемым к выпускной квалификационной работе бакалавра, и заслуживает оценки «отлично».

«____»_____ 20 г. _____ _____
Подпись *ФИО*