ОТЗЫВ ОФИЦИАЛЬНОГО ОППОНЕНТА

о диссертационной работе Князевой Наталии Сергеевны «Разработка методики идентификации последовательности внешних воздействий на динамическую систему, изоморфную конечному автомату (на примере восстановления последовательности файловых операций в операционной системе)», представленную на соискание ученой степени кандидата технических наук по специальности 2.3.1. Системный анализ, управление и обработка информации.

Диссертационная работа Н.С. Князевой посвящена одной из важных задач компьютерной криминалистики — определению характера работы пользователя с файлами в исследуемой системе. В ОС семейства Windows каждое действие пользователя фиксируется в тех или иных системных файлах: системном реестре, журналах событий, файлах конфигурации, файлах гибернации и подкачки, системных каталогах, таблицах файловых систем FAT и NTFS и т.д. Применительно к задаче восстановления последовательности операций, совершенных пользователем над файлами, используется анализ временных отметок, хранимых в таблицах файловых систем. Однако информация по изменению временных отметок имеет разрозненный характер. Методики и алгоритмы, позволяющие автоматизировать анализ временных отметок, не обнаружены. Возможным решением данных проблем является разработка алгоритма проведения экспериментов для формирования базы знаний о механизмах изменений временных отметок файлов и разработка методики восстановления последовательности файловых операций. Именно эти задачи поставлены в работе Н.С. Князевой, что определяет ее высокую актуальность.

Диссертация состоит из введения, 4 глав, заключения, списка использованных источников из 86 наименований и 7 приложений.

В первой главе проведен анализ современного состояния предметной области, на основе обзора работ отечественных и зарубежных ученых.

Во второй главе описаны инструментарий и разработанный алгоритм исследования изменений временных отметок в ОС Windows. Определены закономерности в изменении временных отметок при совершении файловых операций. Проведен анализ признаков подделки временных отметок и описаны следы, позволяющие обнаружить их фальсификацию.

Третья глава посвящена разработке модели изменения значений временных отметок и методики восстановления хронологии файловых операций. Представлены результаты экспериментальной проверки адекватности модели.

В четвертой главе описаны разработанная функция, реализующая методику восстановления файловых операций, и рекомендации по использованию временных отметок, хранящихся во внутренней структуре файла, для уточнения результатов автоматизированного анализа.

Структура диссертации соответствует логике и последовательности решения соискателем поставленной научной задачи. Рукопись написана грамотно, хорошим научным языком. Автореферат соответствует содержанию диссертации. Публикации в достаточной степени отражают содержание диссертации.

К числу новых и наиболее значимых результатов, полученных в ходе выполнения работы, по мнению оппонента, относятся:

1. Разработка алгоритма проведения экспериментального исследования, позволяющего выявлять закономерности изменения временных отметок при совершении файловых операций в ОС Windows.

2. Создание обобщенной математической модели, позволяющей осуществлять расчет возможных состояний временных отметок при совершении различных операций над файлами.

3. Разработка методики восстановления последовательностей файловых операций, которая сопоставляет возможные последовательности файловых операций и варианты состояний временных отметок файлов.

Использование проверенных литературных данных, современного математического аппарата, апробированного программного продукта и компьютерного эксперимента обеспечивают достоверность полученных автором результатов. Их обобщения представляются весьма обоснованными, поскольку сделаны с использованием известных правил логики, прошли достаточную общественную апробацию и хорошо вписываются в общую систему знаний, накопленную в данной научно-технической области.

В то же время представленная диссертационная работа не свободна от недостатков. К ним можно отнести следующее:

1. Основные результаты диссертационной работы получены для случая, когда пользователь не изменял временные отметки с помощью, например, шестнадцатеричного редактора. Применима ли предложенная методика при подобных действиях пользователя?

2. Недостаточно подробно описана методика восстановления последовательности файловых операций в случае обновления версий (сборок) ОС Windows.

3. Разработанная программа (функция) Retro.m написана в программной среде Matlab, что может вызвать трудности при ее практическом использовании экспертом в случае отсутствия на его компьютере программного обеспечения Matlab.

Высказанные замечания не носят принципиального характера. Представленная диссертационная работа является важным законченным исследованием, выполненным по чрезвычайно актуальной тематике. В работе получен ряд новых значимых результатов, которые расширяют научное знание в области компьютерной криминалистики. Результаты работы Князевой Н.С. имеют несомненное практическое значение в части разработки программы, позволяющей в автоматическом режиме восстанавливать хронологию файловых операций, а также в части рекомендаций по использованию дополнительных временных отметок для уточнения результатов автоматического анализа. Научные положения диссертации в достаточной степени опубликованы, получили апробацию на научно-технических (или научно-практических) конференциях и внедрены в учебный процесс.

Таким образом, диссертация Князевой Наталии Сергеевны полностью соответствует требованиям п. 9 Положения о присуждении ученых степеней в УрФУ[1], предъявляемым к кандидатским диссертациям, а ее автор, Князева Наталия Сергеевна, заслуживает присуждения ученой степени кандидата технических наук по специальности 2.3.1. Системный анализ, управление и обработка информации.

Официальный оппонент:
Доктор физико-математических наук, профессор
Декан факультета компьютерных наук
ФГБОУ ВО «Омский государственный университет им. Ф.М. Достоевского»
Тел.: +7 (3812) 64-83-11
e-mail: guts@omsu.ru
Адрес: 644077, г. Омск, проспект Мира, д. 55-А

Гуц Александр Константинович

12.11.2021

(подпись) (дата)

Подпись Гуц Александра Константиновича заверяю:

Рогалева Ольга Сергеевна

12.11.2021

(подпись) (дата)

1 ФГАОУ ВО «Уральский федеральный университет имени первого Президента России Б.Н. Ельцина»