Отзыв

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

Восстановление хронологии файловых операций играет важную роль при проведении компьютерно-технических экспертиз. Известны несколько путей проведения такого рода исследования: анализ журналов событий, журнала транзакций (logfile) или временных отметок, которые для каждого объекта файловой системы NTFS хранятся в главной файловой таблице MFT. В случае, когда интересуемый файл просуществовал в системе значительное время, за которое события в журнале транзакций перезаписались, единственным источником информации для восстановления хронологии операций остаются временные отметки файла. Недостатками существующих методов анализа временных отметок является мало изученность механизма их обновления, возможность их подделки с помощью специального программного обеспечения и отсутствие инструмента, позволяющего автоматизировать подобный анализ. Поэтому, задачи диссертационного исследования, связанные с разработкой алгоритма проведения экспериментов для выявления закономерностей изменений временных отметок и методики восстановления последовательности файловых операций, являются актуальными.

Научная новизна работы заключается в предложенном автором алгоритме проведения экспериментального исследования влияния файловых операций на изменения временных отметок, а также в разработанной модели, описывающей изменения значений временных отметок. Результаты диссертационной работы: авторская методика восстановления последовательности файловых операций и реализующая ее функция могут быть внедрены в программные комплексы, предназначенные для криминалистического исследования компьютерных систем.

В качестве замечаний следует указать, что четвертая глава в автореферате на фоне первых трех недостаточно подробно описана; приведено мало примеров применения разработанной функции. Однако, сделанные замечания, в целом, не снижают общую позитивную оценку диссертации, выполненной на хорошем научном и техническом уровнях.

Полученные автором результаты обладают научной новизной и практической значимостью, представляются достоверными, а выводы и заключения — обоснованными. Автореферат грамотно оформлен, теоретические и экспериментальные материалы диссертации излагаются последовательно и обоснованно. Соискатель располагает достаточным количеством научных работ по тематике исследований. Полученные результаты

в необходимой степени апробированы и внедрены в практическую деятельность и учебный процесс.

Диссертационная работа соответствует п. 9 Положения о присуждении ученых степеней в УрФУ и специальности 2.3.1. Системный анализ, управление и обработка информации, а ее автор Князева Наталия Сергеевна заслуживает присуждения ученой степени кандидата технических наук по специальности 2.3.1. Системный анализ, управление и обработка информации.

Ведущий инженер-программист отдела Инфраструктуры Кабинета УЦ АО «ПФ «СКБ Контур»
Лыкошев Алексей Николаевич _____ 24.11.2021
(подпись) (дата)
Тел.: +7 902 263 88 01
e-mail: lykoshev@gmail.com
Адрес организации: 620036, г. Екатеринбург, ул. Малопрудная, д. 5

Подпись Лыкошева Алексея Николаевича заверяю:
Ведущий специалист отдела информационной безопасности АО «ПФ «СКБ Контур»
Нестеров Андрей Вениаминович _____ 24.11.2021
(подпись) (дата)