ОТЗЫВ

на автореферат диссертации

КНЯЗЕВОЙ НАТАЛИИ СЕРГЕЕВНЫ

на тему: «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

Ущерб, наносимый преступлениями, совершаемыми с использованием средств компьютерной техники, практически не поддается оценке. При этом с каждым годом не только стремительно растет число преступлений подобного рода, но и увеличивается их масштаб. При расследовании компьютерного преступления назначается компьютерно-техническая экспертиза (КТЭ). Одной из важнейших задач КТЭ является восстановление последовательности операций, совершенных пользователем над файлами. Для решения этой задачи исследуется служебная информация, регистрируемая в файловой системе компьютера, в том числе временные отметки (ВО) файлов. Обеспечение достоверности и глубины восстановления цепочки файловых операций (ФОп) требуют большого объема ручной работы и высокой квалификации специалиста. При этом количество обрабатываемых пользователем файлов таково, что эффективное восстановление последовательности ФОп для каждого из них оказывается невозможным

Актуальность темы исследования обусловливается потребностью в изучении закономерностей изменения ВО при различных действиях над файлами и создании методики восстановления последовательности ФОп по ВО, а также реализующего эту методику программного обеспечения, адаптированного для использования в практической деятельности эксперта-криминалиста.

Научная новизна исследования состоит в разработке математической модели изменения значений ВО, основанной на гипотезе изоморфизма файловой системы динамической системе, и созданной на основе модели методике восстановления последовательностей ФОп.

Практическая значимость диссертации заключается в создании программы, позволяющей в автоматическом режиме проводить анализ ВО и восстанавливать хронологию ФОп. Практическую значимость имеют также выработанные практические рекомендации по использованию ВО, хранящихся во внутренней структуре файла, для повышения количества восстанавливаемых ФОп.

Судя по автореферату, автором вывполнен большой объем теоретической работы: предложен алгоритм проведения исследования механизмов изменения ВО, исследованы программы, которые позволяют умышленно модифицировать ВО файлов, разработана модель изменения значений ВО, основанная на

найденных закономерностях изменений ВО, подтверждена экспериментально адекватность модели. Результаты диссертационного исследования прошли достаточно широкую апробацию; положения, выносимые на защиту, своевременно опубликованы. Материал, представленный в автореферате, позволяет судить о содержании и качестве диссертационной работы.

Недостатки работы. Ограниченный объем автореферата, к сожалению, не позволил его автору подробно осветить все проблемы диссертационного исследования.

Так, не вполне ясно, почему в таблице 1 на стр. 10 говорится о 12 внешних ВО, а в таблице 2 (стр. 11, 12) представлены изменения только 8 внешних ВО.

Рекомендации по использованию ВО, хранящихся во внутренней структуре файла, описаны не подробно, поэтому трудно оценить их практическую значимость.

На стр. 15 имеется опечатка: ссылка на табл. 0.

Указанные выше замечания не носят принципиального характера и не снижают общего положительного впечатления о диссертационном исследовании.

Заключение. Структура представленной работы соответствует логике научного исследования. Автореферат написан ясным научным языком и отражает суть проведенных изысканий. Результаты диссертационного исследования можно квалифицировать как решение актуальной научно-технической задачи в сфере совершенствования методов проведения КТЭ. Основные положения диссертации своевременно и в достаточной степени опубликованы. Выносимые автором на защиту научные положения представляются достоверными.

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.

Заместитель начальника отдела криминалистической техники и специальных программных комплексов ООО «ЛАН-ПРОЕКТ»
Кандидат физико-математических наук
Романюк Анатолий Валентинович _____ 15.11.2024
(подпись) (дата)

Тел.: +7 495 926-12-75
e-mail: a.romanyuk@lan-project.ru
Адрес организации: 123103, г. Москва, пр. Маршала Жукова д. 74, корп. 1

Подпись Романюка А.В. заверяю:
Заместитель генерального директора ООО «ЛАН-ПРОЕКТ»
Ипатов Е.Е. _____ 15.11.2024
(подпись) (дата)