ОТЗЫВ

на автореферат диссертации 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

Широкое распространение знаний в сфере информационных технологий наряду с легкой доступностью программного инструментария, предназначенного для неправомерных действий, увеличивают численность компьютерных инцидентов. В связи с ростом компьютерных правонарушений повышается интерес к созданию новых методов и алгоритмов проведения компьютерных исследований. Однако одним из нерешенных вопросов остается определение истории появления интересуемых файлов. В настоящее время существует ряд исследований по тематике восстановления последовательности файловых операций (ФОп) по временным отметкам (ВО) файлов, но отсутствие научно обоснованных и поддающихся автоматизации методик, не позволяет использовать данные исследования на практике.

Таким образом, тема диссертации, посвященная разработке методики идентификации последовательности внешних воздействий на динамическую систему (на примере восстановления последовательности файловых операций в операционной системе), является актуальной.

Основные научные результаты, полученные автором:

1. Разработан алгоритм проведения экспериментальных исследований процесса изменений внешних ВО, в результате использования которого выявлены и обобщены в таблицу закономерности изменений ВО при совершении ФОп.

2. Представлена модель, описывающая закономерности процесса изменения ВО, в виде конечного автомата, где состояниями являются множество состояний ВО файлов, а входным алфавитом — множество совершаемых ФОп.

3. Предложена методика восстановления последовательности ФОп, позволяющая достоверно восстанавливать последовательность ФОп и определять последнюю совершенную над файлом операцию.

4. Разработана и протестирована функция, позволяющая автоматизировать методику восстановления хронологии ФОп, что значительно сокращает временные затраты при исследовании большого количества файлов.

Достоверность результатов подтверждается корректным применением методов математического моделирования и проведением натурных

при проверки адекватности представленной математической модели изменения значений ВО.

По материалам диссертации опубликовано 6 научных работ, из них 5 научных статей в рецензируемых изданиях, определенных ВАК РФ и Аттестационным советом УрФУ, в том числе 2 статьи в изданиях, индексируемых в международной цитатно-аналитической базе Scopus. Полученные результаты в необходимой и достаточной степени апробированы, а их внедрение в практическую деятельность подтверждено актами.

По автореферату есть замечание, которое не снижает общую положительную оценку работы: из материалов автореферата не понятно, как и зачем проводится анализ внутренних временных отметок.

Автореферат написан понятным научным языком, используемые научные и специальные термины обоснованы. Для текста автореферата характерны целостность, связность и смысловая завершенность. Приведенные таблицы и рисунки обоснованы, выполнены в соответствии с нормативными требованиями. Исследовательская работа в полной мере отвечает требованиям по актуальности, научной новизне, практической значимости.

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.

Исполнительный директор ООО «Элкомсофт»
Каталов Владимир Юрьевич _____ 23.11.2021
(подпись) (дата)

Тел.: 985-998-68-20
e-mail: katalov@elcomsoft.com

Адрес организации: 129085, г. Москва, Звездный бульвар, 21, офис 615

Подпись Каталова Владимира Юрьевича заверяю:

Генеральный директор ООО «Элкомсофт»
Шплатов Александр Николаевич _____ 23.11.2021
(подпись) (дата)

ПЕЧАТЬ