ОТЗЫВ ОФИЦИАЛЬНОГО ОППОНЕНТА

кандидата технических наук Правикова Дмитрия Игоревича на диссертационную работу 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.

Актуальность темы исследования

В ходе расследования компьютерных инцидентов типовой задачей, решаемой специалистом, является ретроспективный анализ файловых объектов (файлов, каталогов, ярлыков) с целью восстановления последовательности действий пользователя. Данная задача решается путем исследования метаданных файловых объектов, к которым в первую очередь следует отнести временные отметки (ВО). Практика проведения компьютерных исследований показывает, что по соотношениям ВО можно определять ряд значимых файловых операций (ФОп). К текущему моменту специалистами накоплен некоторый раздел знаний о причинно-следственных связях между ФОп и изменениями ВО файлов, но попыток формализации этих знаний до сих пор не предпринималось. Отсутствие научно обоснованных методик и алгоритмов проведения ретроспективного анализа не позволяет автоматизировать процесс восстановления и требует высокой квалификации специалиста.

В этой связи изучение закономерностей изменения ВО, разработка модели изменения ВО и методики восстановления последовательности ФОп является актуальной научной и практической задачей.

Научная новизна полученных результатов

В диссертационной работе получены следующие новые научные результаты:

разработан алгоритм анализа изменения ВО, выявляющий полный набор закономерностей изменения ВО при совершении ФОп в ФС NTFS во всех версиях ОС Windows;

обоснована гипотеза изоморфизма динамики изменения ВО файлов и динамики изменения состояний конечного автомата, на основании которой предложена математическая модель изменения значений ВО при совершении ФОп в ОС Windows;

разработана методика восстановления последовательностей ФОп, которая решает обратную задачу путем адаптации алгоритма обхода в глубину к особенностям решаемой задачи.

Обоснованность и достоверность научных положений, сформулированных в диссертации

Обоснованность и достоверность научных результатов исследования обеспечивается применением корректных исходных данных, апробированных методов исследований, проверкой непротиворечивости и адекватности положений и выводов, экспериментальными данными, полученными при апробации программного обеспечения, реализующего методику восстановления последовательности ФОп.

Результаты исследования опубликованы в 6 научных работах, 5 из которых в ведущих рецензируемых журналах, рекомендованных ВАК РФ и Аттестационным советом ФГАОУ ВО «Уральский федеральный университет имени первого Президента России Б. Н. Ельцина» (УрФУ).

Степень обоснованности и достоверности научных положений, выводов и рекомендаций соответствует требованиям к научным квалификационным работам.

Практическая значимость результатов диссертации

Практическая значимость результатов диссертации заключается в разработке программы, позволяющей в автоматическом режиме проводить анализ ВО, расположенных внутри файловой записи, и восстанавливать хронологию ФОп. Разработаны рекомендации по использованию ВО, хранящихся во внутренней структуре файла, для повышения количества восстанавливаемых ФОп.

Оценка содержания диссертации и ее оформления

Диссертационная работа содержит 110 страниц основного текста (всего 156 с.), 72 рисунка и 19 таблицы. Она состоит из введения, четырех глав, заключения, списка сокращений и условных обозначений, списка литературы из 86 наименований, 7 приложений.

Структура квалификационной работы логически выдержана. Материал излагается последовательно. Ключевые позиции сопровождаются графическим материалом, а также таблицами и формулами.

Автореферат отражает содержание и основные выводы диссертационной работы.

Замечания и вопросы по работе

Вместе с этим следует отметить некоторые замечания и вопросы по работе:

1. В работе отмечается, что дальнейшим направлением исследования является разработка методики восстановления последовательности ФОп с учетом возможной модификации системного времени. Говоря другими словами, возможна ситуация, когда злоумышленник целенаправленно стремиться внести искажения во ВО с целью потенциального влияния на результаты КЭ. Тем не менее, даже на

текущем этапе исследования возможно определение ситуации, когда полученная картина ВО не могла быть сформирована ФОп в штатном режиме. Отмечаемая ситуация важна с точки зрения проведения экспертизы, но на данном этапе она даже не описана.

2. Как можно понять из работы, есть ряд ситуаций, в которых определить последовательность ФОп возможно только с определенной вероятностью. Вместе с тем, оценка данных вероятностей не приводится.
3. В автореферате на стр. 15 есть ссылка на таблицу 0. Вместе с тем, таблицы с таким номером в автореферате нет.

Сделанные замечания не влияют на полученные научные результаты и не снижают научной ценности работы.

Заключение по работе

Исследовательская работа изложена грамотным научно-техническим языком, в полной мере отвечает требованиям по актуальности, научной новизне, практической значимости, личному вкладу автора, отражению результатов в публикациях, а также полностью соответствует п. 9 Положения о присуждении ученых степеней в УрФУ и специальности 2.3.1. Системный анализ, управление и обработка информации. Автор диссертации Князева Наталия Сергеевна заслуживает присуждения ученой степени кандидата технических наук по специальности 2.3.1. Системный анализ, управление и обработка информации.

Официальный оппонент:

Кандидат технических наук
Советник генерального директора
Акционерное общество «ИБ Реформ»
Тел.: +7 (499) 390-79-05
e-mail: dip@ib-reform.ru
Адрес: 117587 г. Москва, Варшавское шоссе, 125, строение 1

Правиков Дмитрий Игоревич

29.11.2021

(подпись) (дата)

Подпись Правикова Дмитрия Игоревича заверяю:

Генеральный директор Сердюк Тимур Владимирович