ОТЗЫВ ОФИЦИАЛЬНОГО ОППОНЕНТА

доктора технических наук, профессора Никульчева Евгения Витальевича, профессора кафедры КБ-14 «Цифровые технологий обработки данных» Института комплексной безопасности и специального приборостроения, 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.

1. Актуальность темы исследования

Тема диссертация является, несомненно, актуальной. Действительно, представить манипуляцию с файлами как динамическую систему с изменяющимися динамическими и временными параметрами, характеристиками, которые могут быть оценены и измерены, является очень интересной научно гипотезой. Данный подход может иметь важное значение для формирования интерфейсов (наиболее употребляемых из несколько альтернативных путей манипуляции с файлами, такие как использование контекстного меню, сочетания клавиш и т.д.); оптимизации систем хранения действий пользователя, а также при проведении компьютерно-технических экспертиз при выявлении несанкционированных действий с файлами. Именно на последнее и направлены основные исследования представленной работы.

2. Оценка содержания диссертации

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

Во введении обоснована актуальность и определена степень разработанности темы диссертационной работы, определены цель и задачи, указаны научная новизна, теоретическая значимость, перечислены методы исследования, сформулированы научные положения, выносимые на защиту.

В первой главе проведен анализ современного состояния предметной области, основанный на результатах исследований отечественных и зарубежных исследователей и ученых. Автор рассматривает сущность временных отметок, проводит обзор имеющихся программных средств просмотра и анализа временных

отметок (ВО) и делает обоснованный вывод о целесообразности системного подхода и построению динамических моделей. На основе анализа предметной области автор формулирует цель и задачи исследования.

Вторая глава посвящена экспериментальному исследованию механизмов изменения ВО. Предложен алгоритм и программный инструментарий. По результатам диссертационного исследования автор строит таблицу изменений ВО, которая позволяет восстанавливать последнюю, совершенную над файлом операцию. Отдельно рассмотрен вопрос фальсификации ВО.

В третьей главе автор обосновывает выбор конечного автомата для описания процесса изменения ВО при осуществлении пользователем файловых операций (ФОп). Представлена разработанная модель изменения значений ВО, проводится проверка ее адекватности. Автором предложена методика восстановления хронологии ФОп, основанная на использовании алгоритма обхода в глубину.

Четвертая глава посвящена описанию функции, разработанной на основе методики восстановления ФОп. Приведены рекомендации по практическому использованию. Представлены примеры восстановлении последовательности ФОп с использованием разработанной функции.

В заключении представлены основные научные и практические результаты исследований, полученные в ходе выполнения диссертационной работы.

3. Научная новизна результатов

Дадим оценку заявленной в диссертационной работе результатов, имеющих научную новизну.

«1. Впервые предложена математическая модель изменения значений ВО при совершении ФОп в ОС Windows, основанная на гипотезе изоморфизма динамики изменения ВО файлов и динамики изменения состояний конечного автомата.»

Действительно, предложенная модель является оригинальной, однако использование термина «изоморфизм», на мой взгляд, не совсем является уместным. Речь идет о математическом моделировании – когда исходному явлению ставится в соответствие модель, адекватно отражающая моделируемые процессы. Изоморфизм подразумевает отображение всех функциональных свойств, файловая система существует и для других целей, не учитываемых модели (потому что они и не нужны в данном случае). Наверное, здесь возникла некоторая путаница с термином «изоморфность графов». Таким образом, результат имеет место, он обоснован, но в формулировке его в диссертации слово изоморфизм требует уточнения.

«2. Впервые разработан алгоритм анализа изменения ВО, отличающийся специальной подготовкой ВО файлов и выявляющий полный набор закономерностей изменения ВО при совершении ФОп в ФС NTFS во всех версиях ОС Windows на заданных пространствах ФОп и типов файлов.»

Основной результат, позволивший получить важные научные и практические результаты на основе введенной модели. Алгоритм основан на новых научных положениях и построенных математических моделях.

«3. Разработана автоматическая методика восстановления последовательностей ФОп, которая впервые решает обратную задачу путем адаптации алгоритма обхода в глубину к особенностям решаемой задачи.»

Формулировка «автоматическая методика» вызывает вопросы: Чем автоматическая методика отличается от алгоритма? Как организована оценка сходимости? Какие условия эффективности методики? и т.д. Хотя, понятно, что именно хотела сказать соискатель, необходимо дать более четкое представление об ограничениях и предположениям, позволившим решить обратную, то есть некорректную задачу.

4. Обоснованность и достоверность научных положений, сформулированных в диссертации

Обоснованность и достоверность научных результатов исследования подтверждается корректным использованием математических методов и моделей, адекватных теоретическим и экспериментальным задачам исследования, а также их согласованностью с результатами, полученными другими авторами.

Результаты исследования опубликованы в 6 научных работах, 5 из которых в ведущих рецензируемых журналах, рекомендованных ВАК РФ и Аттестационным советом УрФУ.

5. Практическая значимость результатов диссертации

Практическая значимость заключается в разработке программы, позволяющей в автоматическом режиме восстанавливать хронологию ФОп, и рекомендаций по использованию ВО, хранящихся во внутренней структуре файла, для повышения количества восстанавливаемых ФОп. Полученные результаты внедрены в ФГАОУ ВО «Уральский федеральный университет имени первого Президента России Б.Н. Ельцина (г. Екатеринбург, Россия); в ООО «Уральский центр систем безопасности» (г. Екатеринбург, Россия); в Екатеринбургский научно-технический центр ФГУП «НПП «Гамма» (г. Екатеринбург, Россия).

6. Замечания по диссертации

1. Представленные результаты могут быть применены и в других областях – проектирования информационных систем, следовало бы рассмотреть эти возможности.

2. Разработанный в главе 2 программный инструментарий, мог бы быть вынесен в основные результаты и положения, выносимые на защиту как экспериментальный стенд, позволяющий строить введенные модели.

3. На с.78-79 диссертации «в результате анализа таблицы переходов выявлен ряд закономерностей», при этом не указано каким образом эти закономерности выявлены и является приведенный список полным или исчерпывающим.

Указанные замечания направлены на совершенствование работы и не снижают общего положительного впечатления от диссертации.

7. Общая характеристика работы

Исследования проведены в значительном объеме, логически выстроены, включают как теоретические аспекты, так и экспериментальную проверку.

В целом диссертационная работа Князевой Наталии Сергеевны хорошо и логично структурирована, соответствует требованиям, предъявляемым к научным работам. Иллюстрации выполнены на высоком научном и оформительском уровне. Автореферат соответствует диссертации.

8. Заключение по работе

Таким образом, диссертация Князевой Наталии Сергеевны «Разработка методики идентификации последовательности внешних воздействий на динамическую систему, изоморфную конечному автомату (на примере восстановления последовательности файловых операций в операционной системе)» является завершенной научно-квалификационной работой, в которой изложены новые научно обоснованные технические решения, внедрение которых вносит значительный вклад в развитие методов моделирования и мониторинга файловых операций в целях экспертиз.

Полученные автором результаты диссертации выглядят достоверно. Выводы обоснованы и своевременно опубликованы. Публикации и автореферат диссертации отражают основное содержание диссертации

Диссертация изложена грамотным научно-техническим языком, в полной мере отвечает требованиям по актуальности, научной новизне, практической значимости, 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:
Доктор технических наук, профессор
Профессор кафедры КБ-14 «Цифровых технологий обработки данных»
ФГБОУ ВО «МИРЭА – Российский технологический университет»
Тел.: + 7 (499) 215-65-65
e-mail: nikulchev@mail.ru
Адрес: 119454, г. Москва, проспект Вернадского, д. 78

15.11.2021

Никульчев Евгений Витальевич

(подпись) (дата)

заверяю
специалист
ления кадров
О.Ю. Васильева