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

Компьютерно-техническая экспертиза (КТЭ) в последнее десятилетие стала одним из самых востребованных видов криминалистических экспертиз. Основная цель КТЭ обнаружение и выявление информации (текстовых, графических, видео- или аудиофайлов). При этом в большинстве случаев требуется определить, какие действия и в какое время пользователь совершал с данной информацией. Проведение такого рода экспертного исследования осложняется отсутствием проверенных и научно обоснованных методик. Для того чтобы убедиться в правильности сделанных выводов эксперт в каждом отдельном случае вынужден проводить эксперименты с целью изучения закономерностей изменений компьютерной системы. Таким образом, разработка алгоритма проведения анализа временных отметок (ВО), математической модели изменения ВО и методики восстановления последовательности файловых операций (ФОп) является **актуальной задачей**.

В диссертационной работе получены следующие новые **научные результаты**

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,

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;

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

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).

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

проблемные вопросы. Следует указать следующие вопросы, требующие пояснения:

1 В работе описывается фальсификация временных отметок файла путем применения специальных программных средств, однако отсутствует упоминание о возможности изменения пользователем системного времени.

2. Диссертационное исследование строится соискателем с использованием понятия «изоморфный», однако строгого определения, когда системы можно считать изоморфными в автореферате не приводится.

3. В автореферате не приведены скоростные характеристики разработанного программного обеспечения.

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

Заключение. Таким образом, диссертация Князевой Наталии Сергеевны является завершенной научно-квалификационной работой, в которой изложены новые научно обоснованные технические решения, внедрение которых вносит значительный вклад в развитие методов проведения компьютерных 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.

Ведущий инженер-программист ООО «АГОМАТ»
кандидат технических наук, доцент
_____Сутямов Евгений Владимирович

24 ноября 2021 г

Тел.· +79097914592
e-mail: radio@tis-dialog.ru
Адрес организации: 238326, Калининградская обл. Гурьевский р-н, пос. Малое Луговое, ул. Селецкая, д. 15

Подпись Сутямова Евгения Владимировича заверяю
Генеральный директор ООО «АЛГОМАТ»
доктор технических наук, профессор
_____Иванов Владимир Анатольевич