Отзыв официального оппонента
на диссертацию на соискание ученой степени кандидата физико-математических наук Терёхиной Ирины Юрьевны на тему: «Методы выявления аномалий в условиях смеси технологических процессов, сопровождающих наблюдаемый объект» по специальности 2.3.6. «Методы и системы защиты информации, информационная безопасность»

Актуальность темы диссертации

Поиск и анализ нарушений информационной безопасности как правило начинается с поиска аномалий в данных мониторинга (логах) процессов выполнения информационных технологий. Известным подходом в решении таких задач является выявление отклонений от известной модели выполнения таких процессов. Исследованию подлежит выбор модели, которая позволяет выявлять аномалии в логах и имеет допустимую трудоемкость при построении модели конкретных информационных технологий. Математическое обоснование правильного выбора модели является актуальной задачей в обеспечении информационной безопасности. Результаты диссертации Терехиной И.Ю. могут использоваться специалистами в области информационной безопасности.

Первая глава работы посвящена обзору и анализу существующих методов и подходов для решения задачи построения модели процесса и поиска аномалий. Описана мотивация выбора условий корректности для модели процесса.

Вторая глава работы посвящена исследованию математической модели в виде выделенного класса сетей Петри для моделирования рабочего процесса.

Проведен анализ совместимости свойств надежности и запрета последовательного выполнения в сети; конструкций синхронизации и выбора; полнота лога рабочего процесса для рассматриваемой сети; сохранение в сети отношения каузальности между переходами. Показаны несколько теорем и приведены результаты. В частности, делается акцент на проблеме формирования полного лога, суть которой сводится к тому, что если в модели

имеются параллелизм или циклы, то количество трасс, которое может породить модель, стремится к бесконечности.

Третья глава посвящена методам и алгоритмам для решения задачи поиска аномалий наличия нескольких эталонных процессов. Получены оценки сложности построения формальных моделей для процессов в зависимости от свойств логов. Приведена оценка сложности принятия решения о поступающей трассы относительно уже имеющихся построенных моделей. Показано, что с помощью системы различных представителей можно эффективно выделять траектории множества различных процессов. Исследована возможность использования математических моделей в виде ацикличных ориентированных графов для решения задач построения модели процесса поиска аномалий.

Научная новизна, обоснованность и достоверность результатов диссертации

В диссертации Терехиной И.Ю. исследованы возможности построения и использования для поисков аномалий моделей процессов на основе сетей Петри и моделей на основе ориентированных ациклических графов. Модели на основе сетей Петри обладают большими возможностями в описании информационных технологий. Однако в диссертации доказано, что использовать эти модели для поиска аномалий в процессах нельзя из-за возможной неоднозначности. Эти результаты являются новыми. Достоверность этих результатов следует из построенных математических доказательств.

Модели процессов на основе ориентированных ациклических графов подходят для поиска аномалий. Автор диссертации доказала, что решение этих задач возможно, когда в одной трассе лога встречаются следы нескольких различных процессов. Бесспорно, оригинальным является результат, где использована теорема Ф. Холла о системах различных представителей.

Для моделей на основе ориентированных ациклических графов получены оценки сложности алгоритмов выявления аномалий.

Несмотря на то, что в диссертационной работе использовались результаты других авторов, положения, выносимые на защиту доказаны автором лично.

Результаты диссертации докладывались на профильных семинарах, а также опубликованы в 6 публикациях, 3 из которых опубликованы в рецензируемых научных изданиях, рекомендованных к защите в диссертационном совете МГУ им. М.В. Ломоносова по специальности 2.3.6.

Автореферат адекватно отражает основные положения диссертации Терёхиной И.Ю.

Замечания к диссертации

1. В первой главе автор диссертации привел обзор определений аномалий. Нельзя сказать, что получилось четкое изложение вопроса, но главное в том, что автор нигде не использует именно это определение. Всюду используется простое определение, а именно, аномалия рассматривается как отклонение от модели.

2. Формулировка теоремы 2.2 не содержит условия из которых следует логически выводимое заключение. Это противоречит общепринятому определению понятия «теорема».

3. В главе 3 не приведено ни одного примера, когда в одной трассе встречаются следы хотя бы двух или нескольких процессов.

Заключение

Несмотря на указанные замечания, отмечу, что они не умаляют значимости диссертационного исследования. Основные результаты диссертации являются новыми и достаточно обоснованными, вносят вклад в развитие научного направления. Диссертация отвечает требованиям, установленным Московским государственным университетом имени М.В.Ломоносова к работам подобного рода. Содержание диссертации соответствует специальности 2.3.6 «Методы и системы защиты информации,

информационная безопасность» (по физико-математическим наукам), а также критериям, определенным пп. 2.1-2.5 Положения о присуждении ученых степеней в Московском государственном университете имени М.В. Ломоносова. Диссертация Терехиной И.Ю. оформлена согласно требованиям Положения о совете по защите диссертаций на соискание ученой степени кандидата наук, на соискание ученой степени доктора наук Московского государственного университета имени М.В. Ломоносова.

Считаю, что Терёхина Ирина Юрьевна заслуживает присуждения ученой степени кандидата физико-математических наук по специальности 2.3.6 «Методы и системы защиты информации, информационная безопасность».

Официальный оппонент:

доктор технических наук, профессор
президент, директор института
системной интеграции и безопасности

ФГАОУ ВО «Томский государственный университет систем управления и радиоэлектроники»

Шелупанов Александр Александрович

Дата: 14.10.2024

Специальность, по которой официальным оппонентом
защищена диссертация:
05.13.01 – «Системный анализ, управление и обработка информации (по отраслям)»

Адрес места работы:
634050, г. Томск, пр. Ленина, д. 40
ФГАОУ ВО «Томский государственный университет систем управления и радиоэлектроники»
Подпись Шелупанова А.А. удостоверяю

Ученый секретарь