ОТЗЫВ

научного руководителя

на диссертацию Терехиной Ирины Юрьевны

«Методы выявления аномалий в условиях смеси технологических процессов, сопровождающих наблюдаемый объект», представленную на соискание ученой степени кандидата физико-математических наук по специальности 2.3.6 – «Методы и системы защиты информации, информационная безопасность»

В 2017 году Терёхина И.Ю. с отличием окончила ФГБОУ ВО «Московский государственный университет имени М.В. Ломоносова», факультет вычислительной математики и кибернетики и получила квалификацию магистра по программе «Математическое и программное обеспечение защиты информации», специальность «Прикладная математика и информатика». В 2021 году Терёхина И.Ю. окончила аспирантуру ФГБОУ ВО «Московский государственный университет имени М.В. Ломоносова», факультет вычислительной математики и кибернетики по направлению 10.06.01 «Информационная безопасность», получив квалификацию «Исследователь. Преподаватель исследователь». В настоящее время работает ассистентом на кафедре информационной безопасности факультета вычислительной математики и кибернетики ФГБОУ ВО «Московский государственный университет имени М.В. Ломоносова».

Диссертационная работа Терёхиной И. Ю. посвящена актуальной теме выявления аномалий, используя модели, построенные из последовательностей логов исполнения информационных технологий. В настоящее время разработано большое количество различных подходов к методам восстановления моделей рабочих процессов по логам выполнения информационных технологий. Основная идея метода выявления аномалий с использованием построенных моделей состоит в том, чтобы по текущим трассам лога определить отклонение от построенной модели. Такое отклонение соответствует аномалии в реализации текущего варианта

выполнения информационной технологии, описываемой моделью. Эффективное выявление аномалий предложенным способом возможно при отсутствии неоднозначности представления технологии в модели. Если возможна такая неоднозначность, то либо возрастает сложность отслеживания, либо появляется противоречие с условиями корректности представления технологии в виде представленной модели. Тогда надо отказаться от рассматриваемого подхода и перейти к другим методам модельного представления рассматриваемой технологии по наблюдаемым логам.

На первый взгляд использование богатого языка в построении модели позволяет надежно определять аномалии при выполнении информационных технологий. Однако исследование языка сетей Петри, который является богатым языком, показал нецелесообразность его использования в задаче выявления аномалий. Поэтому для дальнейшего исследования был выбран более бедный язык представления технологий в виде ациклических ориентированных графов (DAG). На этом пути удалось доказать однозначность построения моделей информационных технологий по логам и возможность выявления аномалий даже в случаях одновременной работы нескольких информационных технологий.

Апробация результатов диссертации проводилась на специальных семинарах «Компьютерная безопасность» под руководством д.ф.-м.н., проф. Грушо А.А., д.т.н., проф. Тимониной Е.Е. на факультете ВМК МГУ и семинаре “Компьютерная безопасность” под руководством к.ф.-м.н. Галатенко А.В., к.ф.-м.н. Александрова Д.Е., кафедры МаТИС механико-математического факультета МГУ. Кроме того Терёхина И.Ю. успешно выступила на следующих научных мероприятиях:

На научной конференции “Ломоносовские чтения – 2023”,

На четырнадцатом Международном Семинаре “Дискретная математика и ее приложения” имени академика О. Б. Лупанова, Москва, ФГБОУ ВО

“Московский государственный университет имени М. В. Ломоносова”, 20–24 июня 2022 год.

На специальном семинаре “Проблемы современных информационно-вычислительных систем” под руководством д.ф.-м.н., проф. В.А. Васенина, кафедры вычислительной математики механико-математического факультета МГУ, 7 марта 2023 год.

Результаты, выносимые на защиту, изложены в 4 статьях, опубликованных в научных изданиях из списка ВАК и входящих в базы цитирования Scopus, RSCI и РИНЦ, 3 из которых опубликованы в рецензируемых научных изданиях, рекомендованных для защиты в диссертационном совете МГУ имени М. В. Ломоносова по специальности 2.3.6 — Методы и системы защиты информации, информационная безопасность. В работах, написанных в соавторстве, Терехиной И.Ю. принадлежат результаты вошедшие в диссертацию.

В первой главе помещен обзор существующих результатов решений задачи построения модели процесса и задачи поиска аномалий.

Вторая глава посвящена использованию математических моделей в виде сетей Петри для решения задачи поиска аномалий. Показано, что решение задачи поиска аномалий с использованием модели в виде сети Петри возможно только для простых процессов без ветвлений (“ИЛИ”) и требований одновременного выполнения нескольких условий (“И”). С точки зрения задачи поиска аномалий, это обстоятельство свидетельствует о том, что для некоторого процесса наложение нескольких необходимых для дальнейшего поиска аномалий условий корректности приводит к переборной задаче и не гарантирует успешного результата. Тем самым строго сформулировать задачу поиска аномалий, используя для этого модель в терминах сети Петри, не всегда удается.

Третья глава посвящена построению моделей информационных технологий, используя аппарат ориентированных ациклических графов. Построены обобщения методов восстановления моделей рабочих процессов в

случаях реализации нескольких информационных технологий. Полученные результаты позволяют эффективно искать аномалии с помощью соответствия таким моделям информационных технологий.

В диссертации получены следующие основные результаты, выносимые на защиту.

1. Исследование возможности использования математических моделей в виде сетей Петри для решения задачи построения модели процесса и для решения задачи поиска аномалий.

2. Исследование возможности использования математических моделей в виде ациклических ориентированных графов (DAG) для решения задачи построения модели процесса и для решения задачи поиска аномалий.

3. Алгоритмы и соответствующие им оценки сложности выполнения по времени для решения задачи построения моделей нескольких процессов в виде ациклических ориентированных графов.

4. Алгоритмы и соответствующие им оценки сложности выполнения для решения задачи выявления аномалий в некоторой трассе при использовании моделей процессов в виде ациклических ориентированных графов. Обобщение предложенных алгоритмов и оценка сложности выполнения для случая, когда в трассе, проверяемой на наличие аномалий, содержатся данные нескольких процессов.

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 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.

По мнению руководителя, соискатель Терехина И.Ю. заслуживает присуждения ученой степени кандидата физико-математических наук по специальности 2.3.6. «Методы и системы защиты информации, информационная безопасность» (по физико-математическим наукам).

Научный руководитель:
д.ф.-м.н., профессор,
чл.-корр. Академии криптографии РФ
главный научный сотрудник ФИЦ ИУ РАН [redacted] А. А. Грушо

[redacted]