Отзыв официального оппонента
о диссертационной работе Терёхиной Ирины Юрьевны
«Методы выявления аномалий в условиях смеси
технологических процессов, сопровождающих наблюдаемый объект»,
представленной на соискание учёной степени
кандидата физико-математических наук по специальности 2.3.6 –
методы и системы защиты информации, информационная безопасность

Актуальность темы диссертации

Задачи контроля корректности работы информационных систем обречены на долгое время оставаться в фокусе внимания подразделений информационной безопасности всех уровней. Диссертационная работа Терёхиной И. Ю. связана с одним из аспектов указанного направления – выявлением аномалий в работе систем по записям (логам, отчётам, истории) о выполняемых или выполнявшихся процессах. Системы, процессы, записи в рамках сложившейся теории принято представлять абстракциями на языке множеств, графов, автоматов и т.п. Таким образом, любой результат допускает широкое многообразие конкретизаций. Например, задача рассматриваемой работы может допускать конкретизацию – выявление (нелегальных) каналов утечки информации из охраняемого сегмента информационной системы. Сегодня подразделения по анализу поведения информационной системы на основе истории ее работы (английский термин – process mining) имеют ведущие мировые, а также российские корпорации.

Новизна научных результатов

В диссертационной работе предпринят систематический анализ подходов к построению моделей по записям процессов для выявления аномалий с использованием сетей Петри. Построен универсальный пример процесса, для которого каждая из пяти рассматриваемых моделей обладает каким-то из естественно определяемых признаков некорректности. Обоснован вывод о том, что сети Петри в общем случае не являются подходящим инструментом для решения задачи поиска аномалий.

Автором также изучен и расширен альтернативный подход, связанный с построением по записи процесса ациклического ориентированного графа достаточно общего вида. В рамках этой модели предложены алгоритмы и выполнены оценки сложности решения задачи выявления аномалий при различных предположениях относительно входных данных, в частности, при множественности процессов в записи. Полученные оценки указывают на возможность эффективной практической реализации.

Указанные результаты представляют несомненный интерес и, насколько можно судить, являются новыми.

Замечания к диссертации

- Обращает на себя внимание то, что в списке литературы все источники англоязычные, кроме одной книги (причём переводной с английского) и одной лекции. Однако в формате диссертации было бы уместно также осветить работы отечественных учёных по анализу информационных систем и реконструкции технологических процессов. Всё-таки у нас в стране даже есть лаборатории, которые занимаются исключительно этой тематикой.

- Основной результат №5 работы формулируется забавно и банально: «Показано, что не каждая математическая модель описания реального процесса является подходящей для эффективного решения задач информационной безопасности…»

- Для полноты картины было бы неплохо, если бы пример из главы 2, на котором «не работают» сети Петри, был промоделирован методами главы 3. Тем более что главе 3 недостаёт иллюстративного материала.

- На с. 102 диссертации есть отсылка к теореме Ф. Холла, но не сказано, о какой из теорем Холла идёт речь.

- Корректность предлагаемого алгоритма 3.4 не проверяется и никак не комментируется.

- Отсутствует логическая связность в формулировках теорем и следствий из главы 3. На примере теоремы 3.3 – шаблон для всех формулировок (комментарий – *курсивом*):

Теорема 3.3. Пусть задан лог L для s процессов. Пусть s процессов имеют попарно различные начальные действия. [*Ещё какие-то s процессов?*] Тогда сложность построения s конформных графов составляет ..., в зависимости от свойств лога L. [*Графов, конформных чему? Процессам? Каким? Каждому процессу один граф, или одному процессу 3 графа, другому 10, третьему ни одного и т.д.?*]

Кроме того, теорема 3.1 начинается так: Пусть задан лог L для s процессов. Пусть выполнены условия Лемм 3.1, 3.2, 3.3. [*Общее условие всех лемм: в логе только один процесс. Причём в лемме 3.3 это единственное условие. Значит, s=1?*]

Последние замечания, хотя и снижают общее впечатление от работы, всё же являются легко исправимыми и не отменяют её результаты.

Заключение по диссертации

Основные результаты диссертационной работы являются новыми, снабжены теоретическим обоснованием. Они своевременно опубликованы в печатных работах автора, в том числе, в журналах, входящих в перечень изданий, рекомендованных для защит в диссертационных советах МГУ. Содержание автореферата с надлежащей полнотой отражает содержание диссертационной работы. Результаты диссертации прошли апробацию на нескольких научных конференциях и семинарах. Они могут быть востребованы специалистами, работающими в области информационной безопасности.

Диссертационная работа «Методы выявления аномалий в условиях смеси технологических процессов, сопровождающих наблюдаемый объект» отвечает требованиям пп. 2.1–2.5 «Положения о присуждении учёных степеней в МГУ им. М.В. Ломоносова», предъявляемым к диссертациям на соискание учёной степени кандидата наук. Считаю, что автор диссертации Терёхина Ирина Юрьевна заслуживает присуждения учёной степени кандидата физико-математических наук по специальности 2.3.6 – «методы и системы защиты информации, информационная безопасность».

Официальный оппонент: Сергеев Игорь Сергеевич

начальник лаборатории
ФГУП «НИИ «Квант», д.ф.-м.н.

14 октября 2024 г.

Подпись Сергеева Игоря Сергеевича заверяю
Зам. начальника отдела кадров ФГУП «НИИ «Квант». О.Н. Дудко