

**Отзыв на автореферат диссертации
Терёхиной Ирины Юрьевны на тему
«Методы выявления аномалий в условиях смеси технологических процессов,
сопровождающих наблюдаемый объект», представленной на соискание ученой
степени кандидата физико-математических наук по специальности 2.3.6 –
«Методы и системы защиты информации, информационная безопасность»**

Целью диссертационной работы Терёхиной И.Ю. является разработка моделей и алгоритмов для решения задачи поиска аномалий в условиях функционирования нескольких процессов, имеющих техническую природу.

Актуальность полученных в диссертационной работе результатов обусловлена необходимостью постоянного решения задачи контроля корректности работы информационных систем любого уровня и сложности, если в системе присутствует журналирование (сбор логов) происходящих в системе событий. Поиск аномалий с использованием построенной модели/множества моделей информационной системы (процесса, в терминах диссертации), как определение несоответствия поступающей трассы (исполнения процесса, в терминах диссертации) этой модели, является актуальной задачей информационной безопасности и допускает большое количество возможных применений и конкретизаций. Возможными прикладными применениями результатов диссертации могут быть как поиск нетипичного использования некоторого сервиса пользователем web-приложения, так и поиск аномалий в системных вызовах ключевых системных приложений.

Диссертационная работа вносит вклад в изучение широко известной задачи мониторинга технологических процессов. Предложенные в диссертации математические модели могут быть использованы для практического решения задач выявления и предупреждения вторжений в компьютерных системах.

К тексту автореферата имеется ряд замечаний.

1. В нескольких случаях в тексте автореферата содержится упоминание разработанных алгоритмов, однако детального описания алгоритмов не приводится. При этом в самом тексте диссертации алгоритмы описываются и помимо временной сложности дается оценка и на сложность по памяти.
2. В тексте автореферата содержатся мелкие опечатки.

Перечисленные замечания носят редакционный характер и не затрагивают научной сути диссертации.

Учитывая все вышеизложенное, считаю, что Терёхина И.Ю. заслуживает присуждения ученой степени кандидата физико-математических наук по специальности 2.3.6 – «Методы и системы защиты информации, информационная безопасность».

Директор по информационной
безопасности
Яндекс

Александр Васильевич Каледя

28 октября 2024

119034, Москва, Льва Толстого, 16
Тел.: +7 (926) 275-14-11, e-mail: kaleda@yandex-team.ru