# ОТЗЫВ

на автореферат диссертационной работы Александрова Дмитрия Евгеньевича «Сложность распознавания принадлежности слова регулярному языку в системах обнаружения вторжений», представленной на соискание учёной степени кандидата физико-математических наук по специальностям 05.13.17 — теоретические основы информатики и 05.13.19 — методы и системы защиты информации, информационная безопасность.

Проверка принадлежности слова регулярному языку является одной из ключевых задач в области активного аудита. С помощью регулярных языков задаётся множество злоумышленных действий, и для проверки безопасности текущего состояния требуется определить, принадлежит ли входное слово (например, сетевой пакет или последовательность записей регистрационного журнала) этому языку. В частности, подсистема, решающая описанную задачу, встраивается в сетевое оборудование. Как правило, такая подсистема реализуется как конечный детерминированный автомат, диаграмма переходов которого хранится во внешней памяти. В результате проблема оптимизации пространственной сложности становится ключевой, так как пространственно сложные регулярные языки приводят к автоматам, диаграмма Мура которых не помещается в отведённую память.

В работе Д.Е. Александрова выбирается класс пространственно сложных регулярных выражений вида $.*R_1.*R_2.*$, достаточно часто встречающийся на практике. В частности, довольно большое число таких выражений имеется в широко распространённой системе активного аудита snort. Объединение n таких выражений в худшем случае приводит к автомату с числом состояний, экспоненциальным по n. Автор предлагает метод уменьшения пространственной сложности за счёт склейки выражений, то есть замены объединения $.*R_1.*R_2.*$ и $.*R_3.*R_4.*$ на выражение $.*(R_1|R_3).*(R_2|R_4).*$. Основная часть работы посвящена исследованию свойств предложенного метода, как с теоретической точки зрения (выведены оценки

на число состояний распознающего автомата до и после применения метода, оценена погрешность), так и с практической точки зрения (вычислены точные значения выигрыша в числе состояний и погрешности для выражений из системы snort). Новизна предлагаемых Д.Е. Александровым решений связана, во-первых, с малоисследовательностбю подхода, основанного на модификации регулярных выражений (традиционно исследователи пытаются изменять распознающее устройство, добавляя к конечным детерминированным абстрактным автоматам ту или иную функциональность), так и наличием математической, теоремной части (в подавляющем большинстве работ по уменьшению пространственной сложности авторы ограничиваются экспериментальной проверкой эффективности).

Таким образом, решаемая в работе задача весьма актуальна, полученные результаты являются новыми и представляют несомненный теоретический и практический интерес.

К сожалению, автор не привёл оценок эффективности комбинирования предлагаемого метода и существующих подходов, описанных во второй главе, хотя возможность совмещения методов описана во введении.

Сделанное замечание не снижает положительной оценки представленной работы. В целом, насколько можно судить по автореферату, диссертация является существенным вкладом в решение важной научно-технической проблемы и вполне удовлетворяет требованиям, предъявляемым к кандидатским диссертациям, а её автор Д.Е. Александров заслуживает присуждения искомой учёной степени.

Рецензент – д.т.н., проф., профессор кафедры прикладной математики и кибернетики Петрозаводского государственного университета

Кузнецов В.А.

Подпись руки Кузнецов В.А.

УДОСТОВЕРЯЮ.

Уч. секретарь ученого совета

«28» марта 2015 г.