ОТЗЫВ

на автореферат диссертации Лапикова Игоря Игоревича на тему «Построение и реализации алгоритмов решения систем целочисленных неравенств в методе разделяющих плоскостей», представленную на соискание ученой степени кандидата технических наук по специальности 05.13.19 – «Методы и системы защиты информации, информационная безопасность».

Судя по автореферату, диссертация Лапикова Игоря Игоревича посвящена разработке методов компрометации генераторов псевдослучайных последовательностей и вносит значительный вклад в алгоритмическое направление дискретной математики, развивая новый подход к решению систем линейных неравенств с дискретными неизвестными, к которым может быть сведен анализ определенного класса генераторов ПСП. Сохраняя итеративную базу полиномиального алгоритма Хачияна, построенный новый адаптивный алгоритм в определенных в диссертации условиях сохраняет и полиномиальную оценку сложности, качественно отличаясь от ранее известных методов направленного перебора.

Положительные стороны нового авторского алгоритма позволяют применить его в решении целого ряда прикладных задач в области информационной безопасности, прежде всего, как это показано в диссертации, при анализе генераторов псевдослучайных последовательностей.

Изначально теоретическая новизна адаптивного алгоритма приводит к тому, что все результаты его практического применения являются новыми и представляют значительный интерес для практических приложений. Следует отметить также общую ориентацию диссертации на развитие методов пороговой логики при решении задач информационной безопасности, что в полной мере отвечает современным тенденциям совершенствования элементной базы и перехода к высокоскоростным методам обработки и передачи информации. В этой связи пороговые элементы представляют особый интерес, благодаря возможности их реализации непосредственно в среде-носителе сигнала с высоким быстродействием.

К достоинствам диссертации в теоретической области следует отнести непосредственно сам новый адаптивный алгоритм с авторскими правилами остановки, локализации исходной области поиска предложенным способом распараллеливания. К важным теоретическим результатам следует отнести также установленную в работе полиномиальную сложность задачи распознавания пороговой k-значной функции.

Из наиболее значимых практических результатов можно, прежде всего, выделить применения адаптивного алгоритма при анализе комбинирующего генератора и в задаче восстановления линейной рекурренты над кольцом, по отрезку подряд идущих знаков ее старшей координатной последовательности, с получением оценки расстояния единственности задачи.

Вместе с тем, в автореферате диссертации хотелось бы отметить следующие недостатки.

1) Из текста автореферата не ясно, каким образом осуществляется переход от булевых систем линейных уравнений к системам неравенств с действительными коэффициентами.
2) В автореферате нечётко указаны границы применения разработанных методов для различных типов генераторов псевдослучайных последовательностей (например, для генератора с неравномерным движением или для генератора Мерсена).

В целом автореферат представляет собой целостное системное изложение результатов проведенных научных исследований. Из автореферата видно, что диссертация соответствует специальности 05.13.19 – «Методы и системы защиты информации, информационная безопасность» по профилю технических наук, ее результаты являются новыми и актуальными для информационной безопасности. Исходя из изложенного можно заключить, что диссертация Лапикова И.И. удовлетворяет всем требованиям ВАК РФ, предъявляемым к кандидатским диссертациям, а ее автор заслуживает присуждения ученой степени кандидата технических наук.

Директор ООО «НИЦ супер-ЭВМ и нейрокомпьютеров», доктор технических наук, профессор (05.13.11 – Математическое и программное обеспечение вычислительных машин, комплексов и компьютерных сетей, 05.13.15 – Вычислительные машины комплексы и компьютерные сети) 347900 Ростовская область, г. Таганрог, пер. Итальянский д. 106; тел. +7 (8634) 612–111; e-mail: levin@superevm.ru

_____ Левин Илья Израилевич

«14» мая 2019 г.

Подпись Левина И.И. заверяю

Начальник отдела кадров