

## ОТЗЫВ НАУЧНОГО РУКОВОДИТЕЛЯ

на диссертационное исследование Лапикова Игоря Игоревича

на тему:

«Построение и реализация алгоритмов решения систем целочисленных неравенств в методе разделяющих плоскостей», представленную к защите на соискание ученой степени кандидата технических наук по специальности 05.13.19 – «Методы и системы защиты информации, информационная безопасность».

Диссертационная работа Лапикова И.И. посвящена построению новых методов решения систем неравенств с дискретными неизвестными. Сводимость к таким системам неравенств широкого круга нелинейных систем дискретных уравнений делает данное направление исследований исключительно важным и актуальным для расширения методов анализа узлов защиты информации в целом.

В основу исследования положено изучение возможности адаптации к дискретным задачам полиномиального алгоритма эллипсоидов, в исходной редакции предложенного Хачияном Л.Г. в 1979 году для нахождения действительных решений систем линейных неравенств с целочисленными коэффициентами. Необходимо подчеркнуть, что возможность такой адаптации изначально исключено сдержано или даже негативно оценивалась специалистами в этой области. Причины такой оценки вызваны непосредственно самой логикой полиномиального алгоритма, на каждой итерации которого в качестве текущего решения рассматривается центр очередного эллипсоида, описанного вокруг полуэллипсоида предыдущей итерации и имеющего действительные координаты, в отличие от желательных дискретных. Кроме того, целью алгоритма Хачияна является попадание в произвольную точку, лежащую в многограннике решений системы линейных неравенств без учета близости к дискретным точкам. И, наконец, еще одной причиной в этом ряду специалистами отмечалась ожидаемая сложность выполнения разовой итерации алгоритма и анонсированное большое их число, требующееся для вынесения решения о совместности, либо несовме-

стности системы. Столь подробный обзор ожидаемой сложности адаптации алгоритма эллипсоидов Хачияна к решению систем линейных неравенств с дискретными неизвестными подчеркивает всю сложность задач, стоящих перед автором в процессе проведения исследований и написания диссертации.

Тем не менее, основные задачи, стоящие перед автором, ему удалось успешно решить и достичь тех целей, которые стояли перед ним в процессе написания диссертации. Важнейшей среди них следует признать разработку адаптивного алгоритма эллипсоидов, нацеленного на нахождение непосредственно дискретных решений систем линейных неравенств. На базе этого адаптивного алгоритма был разработан пространственно-декомпозиционный алгоритм, включающий распараллеливание построенного адаптивного алгоритма для снижения временной сложности.

Далее было проведено масштабное экспериментальное исследование, доказывающее корректность и результативность предложенных алгоритмов. Экспериментальные исследования позволили получить эмпирические оценки сложности разработанных алгоритмов, что позволило сравнить их эффективность с возможными альтернативными методами, прежде всего – эвристическими и установить, что большинству показателей в рамках конкретного применения разработанные алгоритмы следует признать предпочтительными.

Следующий этап исследования, имеющий не только теоретический, но и прикладной интерес, связан с применением адаптивного алгоритма для решения ряда конкретных практических задач, сводящихся к анализу систем линейных неравенств. Среди них можно выделить целый ряд задач по нахождению параметров фильтрующих генераторов различной природы с пороговой функцией выхода.

Самостоятельный серьезный интерес представляет применение адаптивного алгоритма эллипсоидов для восстановления линейной рекурренты над кольцом  $Z/2^m$  с трехчленным рекуррентным законом. Использование разработанного алгоритма позволило не только находить начальное заполнение по последовательности подряд идущих знаков старшего разряда, но и вывести оцен-

ку расстояния единственности с её обстоятельной экспериментальной проверкой. Еще одним ярким достижением работы, имеющим большое значение для пороговой логики, как самостоятельного направления дискретной математики, следует признать применение метода эллипсоидов для характеристики пороговой функции и доказательство того факта, что задача распознавания имеет полиномиальную сложность.

Для получения перечисленных результатов автору пришлось провести углубленное исследование алгоритмической природы метода эллипсоидов, усовершенствовать критерий отбраковки, уточнить параметры исходной локализации и правило поведения на заключительном этапе нахождения решения либо объявления о несовместности.

В целом в диссертации решен целый ряд сложных теоретических задач, направленных на построение новых алгоритмов решения систем линейных неравенств с  $k$ -значными неизвестными.

Практическое значение диссертации определяется нацеленностью построенных алгоритмов на решение прикладных задач информационной безопасности, сводящихся к решению систем линейных неравенств с дискретными неизвестными.

Все основные результаты диссертации с достаточной полнотой опубликованы в 10 печатных изданиях, 7 из которых входят в перечень ВАК РФ, издавались на всероссийских, ведомственных научных конференциях. Диссертация в полной мере соответствует специальности 05.13.19 по профилю технических наук.

При проведении научных исследований Лапиков И.И. проявил целеустремленность, настойчивость, показал себя сложившимся специалистом, способным самостоятельно ставить и решать сложные задачи в области дискретной и непрерывной математики, теории алгоритмов и их практических приложений.

Так как разработанные в диссертации алгоритмы открывают новое направление в решении систем линейных неравенств с  $k$ -значными неизвестными, то автору удалось затронуть далеко не все возникающие при этом вопросы и

рассмотреть лишь некоторые из возможных практических приложений. Этим замечанием определяются и недостатки работы. В алгоритмической области можно рекомендовать для найденных эмпирических оценок параметров вывести теоретические, позволяющие установить их зависимости от исходных данных. Кроме того, можно значительно расширить область практического применения результатов диссертации за счет рассмотрения большего числа прикладных задач. Здесь, в качестве примера можно указать задачу проверки реализуемости  $k$ -значной функции с помощью нелинейной поверхности фиксированной степени, которая также сводится к решению систем линейных неравенств. Однако эти недостатки скорее определяют направления дальнейших исследований и не меняют общего положительного впечатления от работы.

Подводя итог изложенному, делаю вывод о том, что представленная диссертация удовлетворяет всем требованиям, предъявляемым ВАК к кандидатским диссертациям, а ее автор, Лапиков Игорь Игоревич, достоин присвоения ученой степени кандидата технических наук по специальности 05.13.19 – «Методы и системы защиты информации, информационная безопасность».

**Научный руководитель:**

Член-корреспондент Академии криптографии Российской Федерации, ФГКНУ «Академия криптографии Российской Федерации», 121552, г. Москва, ул. Ярцевская, дом 30, профессор, доктор технических наук, специальность 05.13.17 «Теоретические основы информатики»

*В.Г. Никонов*

В.Г. Никонов

25 октября 2018 г.

Подпись Никонова В.Г. заверяю

Управляющий делами аппарата президиума Академии криптографии  
Российской Федерации

26 октября 2018 г.



А.А. Тюкин