

## 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».

Актуальность диссертационной работы И.И. Лапикова определяется тем, что решается задача построения новых методов компрометации генераторов псевдослучайных последовательностей, используемых при построении систем защиты информации. Данная проблематика рассматривается в разрезе возможности сведения задачи анализа класса генераторов ПСП к системам линейных неравенств с  $k$ -значными неизвестными.

Объектом диссертационного исследований являются системы целочисленных неравенств, возникающих в задачах информационной безопасности.

Предметом диссертационного исследования являются методы решения систем линейных неравенств в действительной и дискретной областях.

Цель диссертационного исследования определена автором как построение и реализация алгоритмов решения систем линейных неравенств в методе разделяющих плоскостей. Для достижения цели потребовалось решение ряда алгоритмических задач.

Основные результаты диссертационного исследования Лапикова И.И. нашли отражение в 10 научных статьях, и которых 7 статей в журналах из списка ВАК и 1 статья в издании, индексируемом в Scopus.

Положения (основные результаты) диссертации, выносимые на защиту и содержащие научную новизну:

1. Адаптивный алгоритм решения систем линейных неравенств с  $k$ -значными неизвестными, развивающий метода эллипсоидов Хачияна.
2. Пространственно-декомпозиционный алгоритм, основанный на геометрическом распараллеливании адаптивного алгоритма эллипсоидов.
3. Экспериментальное доказательство возможности применения разработанных алгоритмов для решения широкого класса прикладных задач, включая анализ узлов защиты информации, сводящихся к решению систем линейных неравенств с  $k$ -значными неизвестными.
4. Способ применения адаптивного алгоритма эллипсоидов для восстановления линейной рекурренты над кольцом  $\mathbb{Z}_2^m$ , реализованной линейным регистром сдвига с трехчленным законом обратной связи, по подряд

идущим знакам ее старшей координатной последовательности, который позволил дать оценку расстояния единственности задачи.

5. Применение модифицированного метода эллипсоидов Хачияна для характеристики  $k$ -значной пороговой функции.

По автореферату диссертации можно сделать следующие замечания:

1. Понятие коэффициента пространственной декомпозиции впервые упоминается на стр. 13, а его определение дано только на стр. 15.

2. В автореферате не раскрыта сущность модификации метода эллипсоидов Хачияна, используемого для характеристики  $k$ -значной пороговой функции.

Указанные замечания носят рекомендательный характер и не снижают общую положительную оценку диссертационной работы.

Судя по автореферату, представленная диссертационная работа, удовлетворяет требованиям ВАК РФ, предъявляемым к кандидатским диссертациям, представляет собой успешно завершённое научно-квалификационное исследование, имеющее важное теоретическое и практическое значение, а ее автор – Лапиков Игорь Игоревич безусловно заслуживает присуждения ученой степени кандидата технических наук по специальности 05.13.19 – «Методы и системы защиты информации, информационная безопасность».

Заместитель директора научно-исследовательского института радиоэлектронных средств Юго-западного государственного университета, кандидат технических наук (05.13.01 – Системный анализ, управление и обработка информации (по отраслям)). 305040 г. Курск, ул. 50 лет Октября, 94; тел. +7 (904) 525–25-05; e-mail: ub3wcl@yandex.ru



Шиленков Егор Андреевич

«30» апреля 2019 г.



Михайлова Е.А.

Специалист по кадрам  
Шиленков