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»

Диссертация Лапикова И.И. посвящена рассмотрению актуальной научно-технической задачи анализа уязвимостей систем защиты информации с применением разработанного алгоритма решения систем линейных неравенств. В центре внимания проводимых исследований естественно оказались генераторы псевдослучайных последовательностей, функционирование которых либо естественно приводит к системам линейных неравенств, либо такие системы могут быть сформированы специальными процедурами сведения.

Структура диссертации отражает порядок проведения исследований, когда на первом этапе рассматриваются методы сведения задач дискретной математики к системам линейных ограничений, далее анализируется метода эллипсоидов, предложенный Л.Г. Хачияном для нахождения действительных решений и строится новый адаптивный алгоритм поиска дискретных решений и на прикладном этапе исследований анализируется применение адаптивного алгоритма к целому спектру практических задач анализа различных систем защиты информации.

Из содержания автореферата следует, что целью исследования Лапикова И.И. является повышение уровня информационной безопасности вновь создаваемых систем и обоснование возможностей обнаружения уязвимостей в уже существующих системах.

Научная новизна работы заключается в том, что для достижения поставленной цели автором разработан новый адаптивный алгоритм, созданный на базе идей алгоритма Хачияна и унаследовавший для ряда прикладных задач его полиномиальную сложность.

Теоретическое значение диссертации заключается и в теоретической разработке отдельных алгоритмических приемов, сформировавших адаптивный алгоритм, и в теоретических результатах, относящихся к его применению, в частности, в задаче нахождения начального состояния линейного регистра сдвига, реализующего линейную рекурренту над кольцом, по знакам старшего разряда, которое позволило дать оценку расстоянию единственности.

Достоверность теоретических положений работы обосновывается применением математических методов в сочетании с результатами экспериментальных исследований.

Практическая значимость диссертации определяется расширением арсенала методов обеспечений информационной безопасности за счет включения в него адаптивного алгоритма эллипсоидов и применения его в конкретных прикладных задачах. Практическое значение алгоритма подтверждается двумя актами о внедрении и двумя свидетельствами о регистрации программ для ЭВМ в Федеральном институте промышленной собственности.

На основании сведений из автореферата, результаты соискателя с достаточной полнотой опубликованы в 10 статьях, из которых 7 – в журналах из перечня ВАК РФ, докладывались и обсуждались на семинарах, а также российских и международных конференциях.

Автореферат диссертации изложен ясным и доступным для понимания языком, аргументация положений, утверждений и выводов ясна и убедительна.

Отмечая несомненные достоинства работы, следует отметить ряд недостатков.

1. В диссертации введен коэффициент линейного расширения текущего эллипсоида равный $\left(1+\frac{1}{16n^2}\right)$ для сохранения искомого решения внутри эллипсоида после округления параметров из-за ограниченности разрядной сетки вычисления, однако для выбора этого коэффициента не приведено достаточных оснований.
2. Полиномиальная сложность задачи распознавания k-значной пороговой функции базируется на исходном алгоритме эллипсоидов и не требует использования адаптивного алгоритма, поэтому этот результат можно было бы включить во вторую главу диссертации.
3. Разработанную методику нахождения начального заполнения линейного регистра сдвига с трехчленным законом по подряд идущим знакам выходной последовательности было бы интересно использовать для изучения строения близких заполнений, порождающих длинные отрезки совпадающих знаков старшей координатной последовательности.

В целом, указанные недостатки не снижают научной и практической ценности диссертации и не меняют в целом благоприятной ее оценки. Изучение автореферата свидетельствует о том, что цель диссертации достигнута, поставленная научная задача решена на высоком уровне.

Вывод. Диссертация Лапикова Игоря Игоревича представляет собой законченную научно-квалификационную работу, в которой получили развитие новые методы решения актуальных задач информационной безопасности.

Диссертация Лапикова И.И. по научному содержанию, глубине, полноте выполненных исследований, а также по объему полученных результатов соответствует требованиям «Положения о порядке присуждения ученых степеней», утвержденного постановление Правительства РФ от 24 сентября 2013 года №842, а ее автор, Лапиков Игорь Игоревич, заслуживает присуждения ему ученой степени кандидата технических наук по специальности 05.13.19 «Методы и системы защиты информации, информационная безопасность».

Профессор кафедры систем информационной безопасности ФГБОУ ВО «Воронежский государственный технический университет», доктор технических наук, доцент (05.13.01 – Системный анализ, управление и обработка информации), 394006 г. Воронеж, ул. 20 лет Октября, 84. Рабочий телефон: 8 (473) 252-34-20; e-mail: mnac@comch.ru

_____ Разинкин Константин Александрович

«27» 05 2019 г.