Отзыв научного руководителя
о диссертации В. О. Миронкина «Явные формулы
для распределений характеристик итераций случайных отображений»,
представленной на соискание ученой степени
кандидата физико-математических наук
по специальности 05.13.19 – Методы и системы защиты информации,
информационная безопасность

В диссертации В. О. Миронкина изучаются свойства графов случайных отображений конечных множеств. В отличие от большого числа публикаций по этой теме, в которых доказывались предельные теоремы для графов равновероятных отображений, в диссертации рассматриваются графы неравновероятных случайных отображений специального вида, а именно, итераций одного или нескольких независимых равновероятных отображений. Такая структура отображений позволяет использовать их как более адекватные модели преобразований, реализуемых алгоритмическими методами защиты информации. Практической направленностью исследований обусловлены как круг изучаемых характеристик графов отображений, так и вид основных результатов: точные (пригодные для расчетов) формулы для распределений изучаемых характеристик.

Для двух основных моделей случайных отображений: k-кратной итерации одного равновероятного случайного отображения конечного множества S в себя и итерации k независимых равновероятных случайных отображений S в себя – получены явные формулы для распределений ряда практически важных характеристик:

длины отрезка апериодичности,
высоты произвольно выбранной вершины (расстояния от нее до цикла),
числа циклических вершин,
мощностей слоев (множеств вершин на заданном расстоянии от циклов),
вероятности принадлежности двух вершин одной связной компоненте,
мощности прообраза произвольно выбранной вершины,
вероятности возникновения коллизии.

Вывод точных формул проводится методами комбинаторной теории вероятностей и потребовал проведения глубокого анализа структуры графов изучаемых неравновероятных отображений.

Все основные результаты диссертации являются новыми.

В диссертации отмечены возможности практического применения результатов исследований для обоснования теоретической стойкости конкретных алгоритмических методов защиты информации и качества формируемых этими алгоритмами псевдослучайных последовательностей. Приведенные в диссертации теоретические результаты нашли практическое применение, что подтверждается двумя актами об их внедрении.

Результаты диссертации опубликованы в 9 статьях в рецензируемых журналах из списка ВАК, докладывались на различных семинарах и научных конференциях. В двух совместных публикациях (со мной и с В. Г. Михайловым) основные результаты получены диссертантом.

Диссертация В. О. Миронкина и мой многолетний опыт общения с ним позволяют сделать вывод о том, что В. О. Миронкин хорошо знаком с алгоритмическими методами защиты информации, владеет методами комбинаторной теории вероятностей и способен самостоятельно ставить задачи и проводить научные исследования.

Считаю, что диссертация «Явные формулы для распределений характеристик итераций случайных отображений» удовлетворяет всем требованиям «Положения о присуждении ученых степеней в Московском государственном университете имени М.В.Ломоносова», и рекомендую ее к защите в диссертационном совете МГУ.05.01 МГУ имени М.В.Ломоносова по специальности 05.13.19 – Методы и системы защиты информации, информационная безопасность (физико-математические науки).

Научный руководитель:
заведующий отделом
Математического института им. В. А. Стеклова
Российской академии наук,
доктор физико-математических наук

А.М.Зубков

06 сентября 2021 г.

Почтовый адрес: 119991, Москва, ул. Губкина, 8
Телефон: 8(499) 941-01-84
Адрес электронной почты: zubkov@mi-ras.ru