

ОТЗЫВ

на автореферат диссертации Николаева Максима Владимировича
«О сложности решения некоторых обобщений задачи дискретного
логарифмирования», представленной на соискание учёной степени
кандидата физико-математических наук
по специальности 05.13.19 — «Методы и системы защиты информации,
информационная безопасность» (физико-математические науки)

Диссертация посвящена актуальным проблемам исследования трудоемкости решения двумерной задачи дискретного логарифмирования и задачи дискретного логарифмирования для групп с эффективными автоморфизмами. Для этих задач Николаевым М.В. предложен способ оптимизации алгоритма Годри-Шоста. Автором разработана методика выбора оптимальных параметров алгоритма и, таким образом, построены наиболее эффективные в настоящее время алгоритмы.

Особый интерес, на мой взгляд, вызывают результаты диссертации, касающиеся задачи дискретного логарифмирования в интервале. За счет использования разработанной диссертантом модификации алгоритма Годри-Шоста, удалось понизить наилучшую известную оценку средней трудоемкости решения указанной задачи, что является существенным научным достижением.

Достоверность результатов диссертационной работы обеспечивается строгим математическим доказательством утверждений и подтверждается их согласованностью с данными, полученными в ходе вычислительных экспериментов.

Считаю, что диссертационная работа Николаева М.В. является самостоятельным завершённым исследованием. Результаты автора опубликованы в научных журналах, индексируемых базами Scopus и Web of Science.

Представленная работа соответствует требованиям «Положения о порядке присуждения ученых степеней в Московском государственном

университете имени М.В. Ломоносова», предъявляемым к кандидатским диссертациям, а ее автор Николаев М.В., несомненно, заслуживает присуждения ему искомой степени кандидата физико-математических наук по специальности 05.13.19 «Методы и системы защиты информации, информационная безопасность» (физико-математические науки).

Фролов Александр Борисович,
доктор технических наук,
профессор, кафедра математического
моделирования ФГБОУ ВО
"Национальный исследовательский
университет "МЭИ"

21 мая 2018 г.

Подпись Фролова А.Б. удостоверяю.



ЗАМЕСТИТЕЛЬ НАЧАЛЬНИКА
УПРАВЛЕНИЯ ПО РАБОТЕ С ПЕРСОНАЛОМ
Л.И.ПОЛЕВАЯ