

УТВЕРЖДАЮ

Директор ОАО «КБ Радар» –
управляющая компания холдинга
«Системы радиолокации»

И.С. Садовский

22.12.2022



ОТЗЫВ

на автореферат диссертации Кондратёнка Никиты Васильевича «Свойства теоретико-числовых и криптографических алгоритмов в дедекиндовых кольцах», представленной на соискание ученой степени кандидата физико-математических наук по специальности 01.01.06 – математическая логика, алгебра и теория чисел

Актуальность диссертационного исследования обусловлена расширением применения криптографии в современных информационно-вычислительных системах, необходимостью использования различных алгоритмов защиты информации, повышением их криптостойкости и, как следствие, усложнением.

Предложены новые подходы к исследованию экстремальных свойств цепочек делений в факториальных кольцах, что позволило автоматизировать проверку соответствующих теорем для факториальных и квадратичных колец.

Научная значимость диссертационной работы заключается:

в полученных новых критериях простоты идеалов в дедекиндовых кольцах;

полученных новых методах исследования экстремальных свойств алгоритма Евклида в факториальных кольцах.

Практическая значимость диссертационной работы заключается в полученных результатах исследования свойств криптосистемы RSA в дедекиндовых кольцах и возможности повышения ее криптостойкости в указанных кольцах.

Достоверность результатов подтверждается корректным применением математического аппарата и строгой аргументацией принятых допущений.

В качестве **недостатка** можно отметить то, что в автореферате не приведены результаты сравнения стойкости криптографических алгоритмов в дедекиндовых кольцах и, к примеру, в кольце гауссовых чисел, применяемых в настоящее время в криптосистемах RSA.

Материал, представленный в автореферате, свидетельствует о том, что диссертационная работа Кондратёнка Н.В. является законченной квалификационной работой, соответствующей требованиям Высшей аттестационной комиссии Республики Беларусь.

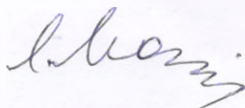
Указанный выше недостаток не снижает научную и практическую значимость диссертационной работы, а ее автор заслуживает присуждения ученой степени кандидата физико-математических наук по специальности 01.01.06 – математическая логика, алгебра и теория чисел.

Эксперт:

Главный научный сотрудник
службы фундаментальных и прикладных исследований
ОАО «КБ Радар» – управляющая компания холдинга
«Системы радиолокации»
доктор технических наук, профессор

Л.Н. Марков

21.12.2022 г.



Я, *Марков Лев Николаевич*, даю согласие на обработку моих персональных данных, связанную с защитой диссертации и оформлением аттестационного дела *Кондратёнка Никиты Васильевича*

Марков Лев Николаевич

