**ОТЗЫВ**
**научного консультанта**
**о диссертации на соискание учёной степени доктора физико-математических наук Нестеренко Алексея Юрьевича на тему «Математические методы обеспечения защищенного взаимодействия средств защиты информации» по специальности 2.3.6 «Методы и системы защиты информации, информационная безопасность»**

В диссертации Нестеренко А.Ю. решена важная практическая проблема построения и математического обоснования безопасности криптографических протоколов, применяемых для обеспечения защищенного обмена информацией по открытым каналам связи, в частности, для защиты критической информационной инфраструктуры Российской Федерации.

Несмотря на практический характер проблемы, результаты диссертации тесно пересекаются с классическими исследованиями в области алгоритмической теории чисел, алгебры и теории вероятностей. Для получения обоснованных оценок безопасности Нестеренко А.Ю. рассматривает хорошо известную, сложную задачу разработки эффективного алгоритма вычисления индексов в группе точек эллиптической кривой, определенной над конечным простым полем, также рассматриваются задачи вычисления явного вида эндоморфизмов эллиптических кривых и выбора параметров эллиптических кривых, обеспечивающих высокий уровень защиты информации.

Для выработки случайных значений, используемых в средствах криптографической защиты информации, Нестеренко А.Ю. предлагается использовать классический подход, основанный на представлении значений иррациональных чисел специального вида в виде систематических дробей в заданной системе счисления. Для обоснования свойств такого типа генераторов Нестеренко А.Ю. решается задача восстановления неизвестных параметров чисел по заданным рациональным приближениям.

При решении указанных задач Нестеренко А.Ю. были получены, в частности, следующие результаты:

- доказана теорема о существовании алгоритма вычисления индексов в группе точек эллиптической кривой, использующего информацию о мультипликативном порядке неизвестного;

- предложен алгоритм вычисления явного представления эндоморфизмов эллиптических кривых; построены формы эллиптических кривых, обеспечивающие минимальную трудоемкость вычисления предъявленных эндоморфизмов; доказана теорема о представлении натуральных чисел значениями многочленов в точках мнимого квадратичного

поля; предложен способ применения доказанной теоремы для реализации алгоритма вычисления кратной точки на эллиптической кривой;

- доказана теорема об оценках неизвестных коэффициентов действительных чисел специального вида, предложены алгоритмы их восстановления по известному рациональному приближению, доказаны утверждения о невозможности применения предложенных алгоритмов для построения более точных рациональных приближений.

Диссертация Нестеренко А.Ю. представляет собой крупное научное достижение в области математических методов защиты информации. Разработанные в ней методы являются новыми, актуальными и востребованными при проведении сертификационных испытаний средств криптографической защиты информации. Все выносимые на защиту результаты получены Нестеренко А.Ю. лично, а глубина проработанности демонстрирует высочайшую квалификацию в выбранной им области исследований.

Считаю, что диссертация Нестеренко Алексея Юрьевича «Математические методы обеспечения защищенного взаимодействия средств защиты информации» отвечает всем требованиям, установленным Московским государственным университетом имени М.В. Ломоносова к диссертациям на соискание учёной степени доктора физико-математических наук. Рекомендую присудить её автору - Нестеренко Алексею Юрьевичу - ученую степень доктора физико-математических наук по специальности 2.3.6 «Методы и системы защиты информации, информационная безопасность».

Научный консультант
доктор физико-математических наук
(специальность 01.01.06 -
Математическая логика, алгебра и теория чисел)
доцент, профессор кафедры математического анализа
механико-математического факультета ФГБОУ ВПО
«Московский государственный университет им. М.В. Ломоносова»

119991, Москва, Ленинские горы, д.1,
механико-математический факультет,
кафедра математического анализа;
vgchirskii@yandex.ru, +7 (495) 939-18-01

Чирский Владимир Григорьевич