Отзыв

на автореферат диссертации Нестеренко Алексея Юрьевича на тему: «Математические методы обеспечения защищенного взаимодействия средств защиты информации», представленной на соискание ученой степени доктора физико-математических наук по специальности 2.3.6 – «Методы и системы защиты информации, информационная безопасность»

В диссертационной работе Нестеренко А. Ю. решается актуальная проблема построения и обоснования безопасности криптографических протоколов, применяемых для защиты информационно-телекоммуникационных сетей связи, автоматизированных систем управления, а также, для защиты критической информационной инфраструктуры Российской Федерации.

В диссертационной работе автор сосредоточил основное внимание на решении ряда сложных математических задач:

- задаче уточнения трудоемкости вычисления дискретных логарифмов в группах точек эллиптических кривых,
- задаче построения режима работы блочных шифров, реализующего шифрование с одновременной выработкой кодов целостности.

Среди вынесенных на защиту положений наибольшую значимость, по мнению рецензента, имеют следующие результаты:

- верхняя оценка числа шагов алгоритма дискретного логарифмирования, основанного на методе Госпера поиска двух совпадающих элементов числовой последовательности;
- теорема о существовании алгоритма дискретного логарифмирования в группе точек эллиптической кривой, использующего информацию о мультипликативном порядке неизвестного;
- понятие «слабого» ключа и оценка средней трудоемкости алгоритма дискретного логарифмирования в группе точек эллиптической кривой;
- алгоритм вычисления явного представления эндоморфизмов эллиптических кривых;
- формы эллиптических кривых, обеспечивающие минимальную трудоемкость вычисления предъявленных эндоморфизмов;
- усиленные, по сравнению с ГОСТ Р 34.10-2012, требования к параметрам эллиптических кривых, а также алгоритм построения таких параметров;
- метод локальной аутентификации пользователей средств защиты информации, основанный на алгоритме представления действительных чисел специального вида в виде систематической дроби по заданному основанию.
- новый класс ключевых функций хеширования, представляющих собой линейные формы от перестановок на множестве кодов аутентификации;

Приведенные в автореферате результаты являются новыми и имеют важные практические приложения при проведении криптографических исследований средств защиты информации.

К тексту автореферата имеются следующие замечания.

1. Описания алгоритмов поиска длин циклов и оценки величины кратности точки эллиптической кривой в Теореме 1.3 загромождают автореферат.
2. Чрезвычайно большое количество ссылок, более 100 наименований, на предыдущих авторов порождает необоснованное сомнение в новизне результатов диссертации.
3. Формализованная модель отражена в автореферате чрезвычайно скупо, что не позволяет оценить ее практическую ценность и, по мнению автора рецензии, является лишней и в самой диссертации.
4. Отсутствует информация о результатах верификации упомянутой модели на примере нескольких, используемых на практике протоколов. Для квалификационной работы достаточно и приведенных математических результатов, имеющих несомненную криптографическую ценность

Судя по автореферату указанные замечания не снижают общего положительного впечатления от диссертационной работы.

Диссертация соответствуют паспорту научной специальности 2.3.6 «Методы и системы защиты информации, информационная безопасность» (физико-математические науки) и является существенным продвижением в решении крупной научной проблемы обеспечения безопасности средств криптографической защиты информации.

Учитывая все вышеизложенное, считаю, что Нестеренко Алексей Юрьевич заслуживает присуждения ученой степени доктора физико-математических наук по специальности 2.3.6 – методы и системы защиты информации, информационная безопасность.

Доктор физико-математических наук,
действительный член Академии Криптографии РФ,
Заместитель генерального директора
Акционерного общества «КБ «Корунд-М»»
Баранов Александр Павлович
Адрес:
115230, Москва, Электролитный проезд,
Дом 9, кор.1.
Тел. +7(916) 204-61-51.
E-mail: baranov.ap@yandex.ru

Подпись Баранова А.П. Заверяю