Закрытое акционерное общество
«Ассоциация специалистов информационных систем»
ЗАО «АСИС»
194100, Санкт-Петербург, ул. Кантемировская, д. 7
т/ф (812) 2955777
E-mail: info@spbissa.ru http://www.spbissa.ru

исх. № 03 от 01/02/2017
на № от 2017

Председателю диссертационного
Совета Д 002.199.01
Санкт-Петербургского института
информатики и автоматизации
Российской академии наук
199178, СПб, 14 л. В.О., д.39

ОТЗЫВ

на диссертационную работу

Березина Андрея Николаевича,

выполненную на тему:

«Методы повышения уровня безопасности защитных преобразований информации»,

представленную на соискание учёной степени кандидата технических наук

по специальности 05.13.19 – «Методы и системы защиты информации, информационная безопасность»

Современное общество не может эффективно существовать и развиваться без информационных систем, которые всё более интенсивно проникают во все сферы деятельности человека. Существенное место в функционировании информационно-телекоммуникационных систем занимает вопрос безопасности, неразрывно связанный с применением различного рода защитных преобразований информации.

Целью представленной диссертационной работы являлось повышение уровня информационной безопасности информационно-телекоммуникационных технологий путём создания набора практичных протоколов защитных преобразований информации, взлом которых требует одновременного решения задач факторизации (ЗФ) и задач дискретного логарифмирования (ЗДЛ) в простом поле.

Научная новизна работы, на наш взгляд, заключается в том, что в ходе исследования был предложен новый универсальный метод построения защитных преобразований информации на основе одновременного решения ЗФ и ЗДЛ.

Практическая значимость результатов исследования заключается в возможности применения разработанных протоколов при построении новых систем защиты информации, в том числе для обеспечения юридической значимости документов.

Достоинства работы, состоят в проведении автором множества исследований существующих методов построения защитных преобразований информации на основе задач факторизации и дискретного логарифмирования, что позволило глубоко изучить проблематику и предложить решение, ведущее в конечном итоге, к повышению эффективность защиты.

Анализ автореферата позволяет обратить внимание на ряд **недостатков:**

- в автореферате используется термин «электронная цифровая подпись», на момент защиты диссертации являющийся устаревшим;

- задачей исследования, как следует из автореферата, была разработка методов и алгоритмов защиты информации на этапах ее сбора, обработки, хранения, передачи и распространения. Далее в автореферате не рассмотрено: имеются ли отличия в применении разработанных алгоритмов на всех указанных этапах жизненного цикла информации;

- в цели работы в автореферате указано повышение уровня информационной безопасности информационно-телекоммуникационных технологий (ИТКТ), но не приведены критерии, в соответствии с которыми проводилась оценка;

- в автореферате наблюдается ряд ошибок орфографического и оформительского характера (неоднородное форматирование, использование формул в тексте, оформление таблиц и рисунков).

Указанные недостатки носят дискуссионный характер. Научная новизна и практическая значимость результатов диссертационного исследования достаточно высокая.

Диссертационная работа Березина А.Н. по актуальности, научной новизне, практической значимости и достоверности полученных результатов соответствует требованиям п. 9 «Положения о присуждении учёных степеней», утверждённого постановлением Правительства Российской Федерации от 24 сентября 2013г. №842. Автор, Березин Андрей Николаевич, **заслуживает** присуждения ему учёной степени **кандидата технических наук по специальности 05.13.19 – «Методы и системы защиты информации, информационная безопасность».**

Генеральный директор закрытого акционерного общества
«Ассоциация специалистов информационных систем»
кандидат технических наук доцент
1.02.2017г _____ Солодянников Александр Владимирович