ОТЗЫВ

на автореферат диссертации Березина Андрея Николаевича «Методы повышения уровня безопасности защитных преобразований информации», представленной к защите на соискание ученой степени кандидата технических наук по специальности 05.13.19 – Методы и системы защиты информации, информационная безопасность.

Обеспечение информационной безопасности информационно-телекоммуникационных систем представляется важной задачей, при решении которой широко используются защитные преобразования информации, основанные на вычислительной трудности задач факторизации и дискретного логарифмирования в простом поле. С целью повышения уровня безопасности алгоритмов и протоколов указанного типа ранее был предложен подход к построению защитных алгоритмов таким образом, чтобы их взлом требовал решения обеих упомянутых задач, однако применяемый в известных в научной литературе метод позволил реализовать алгоритмы цифровой подписи. Для построения в рамках этого подхода других типов защитных алгоритмов и протоколов требовался другой конструктивный метод, который и был разработан в ходе диссертационного исследования Березина А. Н. В диссертации разработанный метод применен для построения достаточно широкого круга разнотипных защитных преобразований, обладающих повышенным уровнем безопасности, что обусловливает актуальность темы диссертационного исследования и полученных результатов.

Автореферат дает вполне ясное представление о структуре и содержании диссертации, а также об основных полученных результатах и их научной новизне, которая состоит в следующем:

1. Предложен метод построения алгоритмов и протоколов, нарушение безопасности которых требует одновременного решения задачи факторизации и задачи дискретного логарифмирования по простому модулю.
2. Разработаны новые протоколы аутентификации объектов и субъектов информационных процессов, обладающие повышенным уровнем безопасности.
3. Разработаны новые протоколы защитного преобразования информации, обладающие повышенным уровнем безопасности.
4. Разработаны новые протоколы электронной цифровой подписи различных типов (индивидуальной, коллективной, групповой, слепой), обладающие повышенным уровнем безопасности, в которых устранены недостатки известных аналогов.

Таким образом, научные результаты, полученные автором, расширяют арсенал алгоритмических средств защиты информации, обладающих повышенным уровнем безопасности.

Практическая значимость работы заключается в возможности использования полученных научных результатов для совершенствования существующих средств защиты информации и проектировании новых.

По содержанию автореферата необходимо сделать следующее замечание. В Таблице 1 автореферата приведены оценки интегрального параметра безопасности, но нигде не поясняется, откуда берутся значения вероятности появления прорывных алгоритмов решения вычислительно задач, положенных в основу разработанных алгоритмов и протоколов.

Указанное замечание не является принципиальным. Выполненное диссертационное исследование является законченной научно-исследовательской работой, обладающей научной новизной и практической значимостью, и соответствует требованиям «Положения о присуждении ученых степеней» ВАК РФ, предъявляемым к кандидатским диссертациям, а её автор заслуживает присуждения ученой степени кандидата технических наук по специальности 05.13.19 – Методы и системы защиты информации, информационная безопасность.

Доцент кафедры ИнИБ,
к.т.н. М. Л. Глухарев

Сведения о составителе отзыва:
ФИО: Глухарев Михаил Леонидович
Учёная степень: кандидат технических наук
Место работы: ФГБОУ ВО «Петербургский государственный университет путей сообщения Императора Александра I»
Должность: доцент
Почтовый адрес: 190031, Санкт-Петербург, Московский пр., 9
Телефон: 8 (812) 310-34-72
e-mail: mlgluharev@yandex.ru