АКЦИОНЕРНОЕ ОБЩЕСТВО
АО НИИ «РУБИН»
“НАУЧНО-ИССЛЕДОВАТЕЛЬСКИЙ ИНСТИТУТ
“Р У Б И Н”

Кантемировская ул., д. 5, Санкт-Петербург, 194100, тел.: (812) 670-89-89, факс: (812) 596-35-81, e-mail: inforubin@rubin-spb.ru
ИНН/КПП 7802776390/780201001, ОГРН 1127847043720, ОКПО 07542394

Экз. № 1

Утверждаю
еститель генерального директора
«НИИ «Рубин» по научной работе
д ческих наук
В.И. Курносов
› _ __ 2017 г.

ОТЗЫВ

на автореферат диссертационной работы Синева Валерия Евгеньевича «Методы построения и разработка практичных протоколов групповой подписи и алгебраических алгоритмов защитных преобразований», представленной к защите на соискание ученой степени кандидата технических наук по специальности 05.13.19 – Методы и системы защиты информации, информационная безопасность.

АКТУАЛЬНОСТЬ ТЕМЫ ДИССЕРТАЦИОННОЙ РАБОТЫ

Алгоритмы и протоколы электронной цифровой подписи (ЭЦП) в настоящее время достаточно широко используются в информационных технологиях, как математическая база придания юридической силы электронным сообщениям и электронным документам. Практика применения информационных технологий связана с достаточно разнообразными вариантами создания, обработки, передачи и хранений электронных документов, имеющих юридическую значимость. Это обстоятельство обусловило интерес исследователей к разработке протоколов ЭЦП специального вида – протоколов слепой ЭЦП, агрегированной ЭЦП, коллективной ЭЦП, групповой ЭЦП и др. Последние два тип протоколов ЭЦП представляет существенный интерес для практики, однако недостатки известных протоколов групповой подписи ограничивает их внедрение в практику. Направленность темы диссертационного исследования на разработку практичных протоколов групповой ЭЦП, внедрение которых может быть осуществлено с использованием имеющейся на практике инфраструктуры открытых ключей, определяет актуальность темы диссертационной работы.

НАУЧНАЯ НОВИЗНА И ПРАКТИЧЕСКАЯ ЗНАЧИМОСТЬ

Новыми научными результатами выполненного исследований являются:

1. Разработка протокола групповой ЭЦП, основанной на вычислительной трудности одновременного решения задачи факторизации и задачи дискретного логарифмирования и использующего стандартную инфраструктуру открытых ключей.

2. Разработка метода построения протоколов коллективной ЭЦП для групповых подписантов, обеспечивающая фиксированный размер для произвольного числа групповых подписантов (коллегиальных органов, осуществляющих подписывание электронных документов).

3. Разработка метода построения протоколов комбинированной коллективной ЭЦП, обеспечивающая фиксированный размер для произвольного числа групповых подписантов и произвольного числа индивидуальных подписантов.

4. Разработка на основе предложенных методов протоколов новых типов.

5. Разработка нового алгебраического псевдовероятностного алгоритма защитного преобразования, отличающегося от известных представлением шифруемых сообщений в виде элементов конечного расширенного поля, заданного в явной векторной форме.

Перечисленные результаты имеют и существенную практическую значимость, прежде всего при решении конкретных задач обеспечения информационной безопасности, а также в учебном процессе.

ДОСТОВЕРНОСТЬ ПОЛУЧЕННЫХ РЕЗУЛЬТАТОВ

Достоверность результатов работы подтверждается корректностью постановки задач, применением апробированных аппарата и методов математической статистики, теории вероятности, теории чисел, криптографии.

При анализе содержания диссертации можно сделать вывод о том, что полученные результаты соответствуют теме, цели и задачам исследования, методически увязаны друг с другом, обладают научной новизной и практической значимостью и, судя по автореферату, прошли достаточную апробацию. Выводы сформулированы грамотно и логически связаны с содержанием работы и позволяют уяснить ее основные положения, научные результаты и практическую значимость. По результатам выполненного исследования опубликовано достаточное число научных работ, включая 5 статей в журналах из списка ВАК.

ВЫВОДЫ И РЕКОМЕНДАЦИИ:

1. Судя по автореферату, диссертационная работа Синева Валерия Евгеньевича является законченной научно-исследовательской работой.

Судя по автореферату к недостаткам диссертационной работы можно отнести следующие:

- недостаточно полно рассмотрены сценарии практического применения предложенных протоколов;
- отсутствует разработка программного прототипа, реализующего разработанные протоколы.

Тем не менее, указанные замечания не снижают теоретическую и практическую ценность научных положений, выносимых на защиту, и личный вклад автора.

2. В целом диссертационное исследование «Методы построения и разработка практичных протоколов групповой подписи и алгебраических алгоритмов защитных преобразований» представляется завершенной научной работой, обладающей научной новизной, практической и теоретической значимостью, соответствует требованиям «Положения о присуждении ученых степеней», предъявляемым к кандидатским диссертациям, а её автор, Синев Валерий Евгеньевич, заслуживает присуждения ученой степени кандидата технических наук по специальности 05.13.19 – «Методы и системы защиты информации, информационная безопасность».

Отзыв обсужден и одобрен на заседании секции № 1 НТС АО «НИИ «Рубин», протокол № 15 от 22 ноября 2017 года.

Отзыв подготовили:

Главный специалист отдела безопасности и защиты информации,
кандидат технических наук (20.01.09 – «Военные системы управления и связи»)

Щукин Анатолий Николаевич

Главный научный сотрудник,
кандидат технических наук (05.12.21 – «Радиотехнические системы специального назначения, включая технику СВЧ и технологию их производства»), доцент

Добросельский Михаил Анатольевич