ЗАКЛЮЧЕНИЕ

экспертной комиссии диссертационного совета Д.002.199.01 по кандидатской диссертации Синева Валерия Евгеньевича «Методы построения практичных протоколов групповой подписи и алгебраических алгоритмов защитных преобразований», научный руководитель – д.**т.н., профессор, заведующий лабораторией криптологии ФГБУН СПИИРАН Молдовян Н.А.**

Экспертная комиссия диссертационного совета Д.002.199.01 в составе: д.т.н., проф. Осипов В.Ю. (председатель), д.т.н., проф. Воробьев В.И., д.т.н., проф. Котенко И.В. после ознакомления с кандидатской диссертацией Синева Валерия Евгеньевича «Методы построения практичных протоколов групповой подписи и алгебраических алгоритмов защитных преобразований» сделала вывод о том, что диссертационная работа Синева В.Е. посвящена решению актуальной научной задаче, включающей разработку метода повышения безопасности протокола утверждаемой групповой ЭЦП; разработку метода построения протокола утверждаемой групповой ЭЦП, свободной от использования вспомогательных открытых ключей; разработку методов построения коллективной ЭЦП для групповых подписантов и комбинированной коллективной ЭЦП; разработку метода повышения производительности алгебраических алгоритмов защитного преобразования.

Целью исследования является расширение функциональности и повышение уровня безопасности протоколов обеспечения неотрекаемости от электронных сообщений (и электронных документов) и алгоритмов защитных преобразований. Значительная практическая значимость и недостаточная научная проработка проблемы определили выбор темы, ее актуальность, цель, задачи, основные направления и содержание диссертационного исследования.

Практическую значимость исследования составляют разработанные в диссертации методы и алгоритмы, которые обеспечивают решение актуальной научно-технической задачи повышения безопасности и расширения функциональности протоколов коллективной и групповой ЭЦП, повышения производительности алгебраических алгоритмов защитных преобразований. Результаты исследования внедрены в образовательном учреждении и использованы в производственной деятельности предприятия, предоставляющего практические услуги в области технологии ЭЦП.

Достоверность и обоснованность научных положений, основных выводов и результатов диссертации обеспечиваются всесторонним анализом состояния исследований в данной области на сегодняшний день, формальными доказательствами, вычислительным экспериментом, апробацией основных теоретических положений диссертации в печатных трудах и докладах на российских и международных научных и научно-практических конференциях.

Материалы и основные результаты кандидатской диссертации Синева В.Е. удовлетворяют паспорту специальности: 05.13.19 – «Методы и системы защиты информации, информационная безопасность», по которой диссертационному совету Д.002.199.01 предоставлено право проведения защит диссертаций.

Основные научные результаты диссертации удовлетворяют требованиям, предусмотренным пунктами 11 и 13 Положения о присуждении ученых степеней: по материалам диссертационной работы опубликовано 13 научных работ, в том числе 5 статей, из которых 5 статей в периодических журналах, рекомендованных ВАК (журналы: «Вопросы защиты информации», «Информационно-управляющие системы», «Известия СПбГЭТУ «ЛЭТИ»).

Недостоверные сведения о работах, в которых изложены основные научные результаты диссертации, опубликованных соискателем ученой степени, отсутствуют.

Текст диссертации, представленной в диссертационный совет, идентичен тексту диссертации, размещенной на сайте СПИИРАН.

Объем оригинального текста диссертационной работы составляет не менее 89%; цитирование оформлено корректно. Требования, установленные пунктом 14 Положения о присуждении ученых степеней, соблюдены: заимствованного материала, использованного в диссертации без ссылки на автора либо источник заимствования, не обнаружено; научных работ, выполненных соискателем ученой степени в соавторстве, без ссылок на соавторов, не выявлено.

Комиссия предлагает:

1. Принять кандидатскую диссертацию Синева В.Е. к защите на диссертационном совете Д.002.199.01 как соответствующую профилю диссертационного совета по специальности 05.13.19 – Методы и системы защиты информации, информационная безопасность.
2. В качестве официальных оппонентов назначить специалистов по данной проблеме: д.т.н. Александрову Е.Б., д.т.н., проф. Татарникову Т.М.
3. В качестве ведущей организации утвердить акционерное общество «Научно-исследовательский институт «ВЕКТОР»
4. Разрешить Синеву В.Е. опубликовать автореферат и утвердить список рассылки авторефератов.
5. Защиту диссертации назначить на «21» декабря 2017 г.

Члены комиссии: проф. Осипов В.Ю.

проф. Воробьев В.И.

проф. Котенко И.В.