ОТЗЫВ

на автореферат диссертации Синева В.Е.
«Методы построения и разработка практичных протоколов групповой подписи и алгебраических алгоритмов защитных преобразований», представленной на соискание ученой степени кандидата технических наук

В настоящее время все большая часть деятельности человека осуществляется с применением средств информационных и коммуникационных технологий, что обусловливает необходимость особого внимания к обеспечению информационной безопасности и достоверности электронных документов. Практика применения современных механизмов электронной цифровой подписи (ЭЦП) выявила ряд серьезных проблем, препятствующих расширению ее применения. Соответственно, не подлежит сомнению актуальность диссертационной работы Синева В.Е., посвященной разработке новых методов разработки практичных протоколов групповой подписи и алгоритмов реализации защитных преобразований.

Анализ автореферата позволяет сделать вывод, что соискателем на основе структурного и функционального анализа разработаны методы и алгоритмы, позволяющие на единой методологической основе реализовать эффективные протоколы групповой подписи и алгоритмы реализации защитных преобразований, пригодные для аппаратной и программной реализации в средствах защиты информации.

Наиболее существенными научными результатами диссертационного исследования, полученными лично Синевым В.Е., следует признать разработку протокола утверждаемой групповой ЭЦП, а также разработку методов построения протоколов коллективной и комбинированной коллективной ЭЦП, обеспечивающих практически важное расширение функциональности протоколов коллективной подписи.

Достоверность полученных результатов обеспечена обоснованностью принятых допущений и корректностью исходных математических положений.

Значимость полученных научных результатов заключается в том, что разработанные методы и алгоритмы обеспечивают возможность повысить уровень информационной безопасности средств информационных и коммуникационных технологий за счет повышения достоверности групповой электронной цифровой подписи.

Полученные при выполнении диссертационного исследования результаты, достаточно полно освещены в 14 публикациях, среди которых пять в рецензируемых изданиях, входящих в перечень ВАК РФ. Следует отметить достаточную апробацию результатов на научно-технических конференциях различного уровня.

В качестве замечаний и недостатков автореферата следует отметить:

1) недостаточное отражение условий и фактических данных экспериментальной проверки полученных результатов;

2) недостаточное внимание к вопросам программной реализации разработанных методов и алгоритмов.

Тем не менее, указанные замечания носят локальный характер и не оказывают существенного влияния на общую высокую оценку научной значимости и практической ценности выполненного диссертационного исследования.

На основе содержания автореферата диссертации Синева Валерия Евгеньевича «Методы построения и разработка практичных протоколов групповой подписи и алгебраических алгоритмов защитных преобразований», представленной на соискание ученой степени кандидата технических наук, ее можно считать отвечающей требованиям ВАК МОН РФ (п.п. 9, 10, 11, 13, 14 «Положения о порядке присуждения ученых степеней», утвержденного постановлением Правительства Российской Федерации от 24 сентября 2013 г. № 842), а ее автора заслуживающим присуждения ученой степени кандидата технических наук по специальности 05.13.19 – Методы и системы защиты информации, информационная безопасность.

Профессор кафедры систем управления и
вычислительной техники ФГБОУ ВО
«Калининградский государственный т
университет» доктор педагогических н
кандидат технических наук, заслужен
работник высшей школы РФ, профес

горь Давидович

«08» 12 2017 г.

236022 Калининград, Советский пр. 1
тел. (4012) 995942, idru@yandex.ru

Подпись И.Д. Рудинского заверяю.
Ученый секретарь ФГБОУ ВО «КГТУ»