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.

Актуальность выполненного диссертационного исследования связана развитием метода построения протоколов защиты и аутентификации информации, обладающих повышенным уровнем безопасности. Научная новизна состоит в следующем:

1. Впервые предложен универсальный метод, построения протоколов защитных преобразований, сохраняющих требуемый уровень стойкости при появлении прорывного алгоритма решения задачи дискретного логарифмирования по простому модулю или задачи факторизации. Повышенный уровень безопасности таких протоколов обеспечивается тем, что вероятность появления за заданный временной интервал обоих из указанных алгоритмов существенно меньше вероятности появления одного из них.
2. На основе разработанного метода разработаны новые протоколы, решающие задачи открытого согласования секретного ключа, аутентификации удаленных пользователей, обеспечения конфиденциальности информации при ее передачи по открытым каналам связи, аутентификации источника электронных сообщений и документов.

Практическая значимость полученных автором результатов состоит в расширении арсенала протоколов защитных преобразований информации, пригодных для обеспечения информационной безопасности информационно-телекоммуникационных систем и информационных технологий. Достоверность научных результатов подтверждается применением апробированного математического аппарата, в частности задач факторизации и дискретного логарифмирования, отсутствием противоречий с другими опубликованными работами в данной области и их апробацией. Основные научные результаты опубликованы в 5 статьях, входящих в список ВАК.

Судя по автореферату недостатком выполненного исследования является то, что использованная формула интегрального показателя безопасности протоколов, поясняющая смысл понятия уровня безопасности использования протоколов защитных преобразований, не учитывает вероятность появления в ближайшем будущем вычислительных технологий, реализуемых с помощью квантовых компьютеров.

Указанное замечание не является принципиальными для выполненного исследования. Судя по автореферату, можно сделать вывод, что выполненное исследование является завершенным научным трудом и

полученные научные результаты дают основания для признания диссертационной работы соответствующей требованиям п.9 «Положения о присуждении учёных степеней», предъявляемых к кандидатским диссертациям, а автор диссертации Березин А.Н. заслуживает присуждения учёной степени кандидата технических наук по специальности 05.13.19 «Методы и системы защиты информации, информационная безопасность».

Генеральный директор
ООО «СофИТ лабс»,
кандидат технических наук Никехин Алексей Алексеевич

Сведения о составителе отзыва:
ФИО: Никехин Алексей Алексеевич
Учёная степень: кандидат технических наук
Место работы: ООО «СофИТ лабс»
Должность: генеральный директор
Почтовый адрес: Малый проспект В. О., д. 48/2, лит. А, БЦ "Навигатор", Санкт-Петербург, 199178
Телефон: +7 812 320 98 93
e-mail: anikekhin@sofitlabs.ru