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.

Постоянное развитие современных автоматизированных информационно-телекоммуникационных систем, расширение спектра решаемых ими задач обуславливает перманентный характер актуальной задачи обеспечения высокого уровня информационной безопасности современных информационно-телекоммуникационных систем, в том числе систем, использующих защитные преобразования, рассматриваемые в диссертации. С целью повышения уровня безопасности упомянутых систем автором предлагается новый подход к их построению и совокупность новых алгоритмов и протоколов защитных преобразований на основе вычислительной сложности задач факторизации и дискретного логарифмирования.

Следует отметить, что подход к построению протоколов защитных преобразований различного вида на основе сложности одновременного решения двух вычислительно трудных задач представляет интерес, т.к. в случае появления в будущем некоторого прорывного решения одной из задач (факторизации или дискретного логарифмирования) не произойдет критического снижения стойкости такой системы. Сам по себе подход, заключающийся в комбинировании задач факторизации и дискретного логарифмирования по простому модулю, не является новым. В тоже время, как показывает автор, известные технические решения имеют ограниченное применение и для синтеза алгоритмов и протоколов защитных преобразований других типов требуется разработка других методов. В качестве универсального метода, применимого для синтеза алгоритмов и протоколов, взлом которых

требует одновременного решения задачи факторизации и задачи дискретного логарифмирования по простому модулю, в диссертации предлагается и обосновывается использование задачи дискретного логарифмирования по трудно факторизуемому модулю, простые делители которого удовлетворяют определённым требованиям.

На основе предложенного метода разработаны следующие протоколы:

1. Электронной цифровой подписи (ЭЦП).
2. Коллективной ЭЦП.
3. Утверждаемой групповой ЭЦП.
4. Интерактивной аутентификации.
5. Двухшаговой аутентификации.
6. Согласования ключей по открытому каналу связи.
7. Защитного преобразования информации.
8. Коммутативного защитного преобразования информации.
9. Стойкого защитного преобразования информации по ключам малого размера.
10. Слепой ЭЦП.
11. Слепой коллективной ЭЦП.

Известные ранее в научно-технической литературе методы построения протоколов на основе задач факторизации и дискретного логарифмирования не позволяют построить такое разнообразие протоколов, применяемых для решения широкого спектра практических задач по обеспечению информационной безопасности в информационно-телекоммуникационных системах.

По содержанию автореферата необходимо сделать следующие замечания.

1. Текст автореферата не позволяет полностью оценить все достоинства и недостатки разработанных протоколов. В частности протокол утверждаемой групповой подписи описан излишне кратко, хотя он представляется весьма интересным с практической точки зрения.

2. Обозначения, используемые при описании разработанных протоколов, раскрыты недостаточно полно.

Указанные недостатки не снижают научную и практическую ценность выполненного диссертационного исследования. В целом, судя по автореферату, можно сделать вывод о том, что представленная диссертация представляет собой законченное научное исследование, содержащее результаты, имеющие теоретическую и практическую значимость, соответствует положениям ВАК РФ, предъявляемым к работам на соискание ученой степени кандидата технических наук. Автор, Березин Андрей Николаевич, заслуживает присуждения ученой степени кандидата технических наук по специальности 05.13.19 – Методы и системы защиты информации, информационная безопасность.

Зам. директора по науке СПбФ ИЗМИРАН
д. т. н, профессор А.Г. Коробейников

Санкт-Петербургский филиал
Федерального государственного
бюджетного учреждения науки
Института земного магнетизма,
ионосферы и распространения
радиоволн им. Н.В.Пушкова
Российской академии наук

199034, г. Санкт-Петербург,
Менделеевская линия, д.1;
тел.: 8 (812) 323-28-07
e-mail: Korobeynikov_A_G@mail.ru