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

В современных информационных технологиях протоколы электронной подписи (ЭП) играют важную роль, которая состоит в подтверждении целостности и авторства электронных документов и сообщений, циркулирующих в информационных системах. Разнообразие типов задач, решаемых с использованием механизма ЭП, стимулировало появление протоколов групповой подписи. Однако практическое внедрение известных протоколов групповой ЭП на основе имеющейся на практике инфраструктуры открытых ключей (ИОК), ориентированной на широкое применение протоколов индивидуальной ЭП, является проблематичным. Тема диссертации «Методы построения и разработка практичных протоколов групповой подписи и алгебраических алгоритмов защитных преобразований», связанная с разработкой методов построения протоколов групповой подписи, ориентированной на использование уже развернутой на практике стандартной ИОК, представляется актуальной.

В диссертационном исследовании получены следующие основные результаты, обладающие научной новизной:

- разработан метод построения протоколов формирования единой ЭП, удостоверяющей то, что связанный с нею электронный документ подписан заданным набором групповых подписантов, причем размер подписи не зависит от их числа;
- разработан протокол коллективной ЭП для групповых подписантов;
- разработан метод построения протоколов формирования единой ЭП фиксированного размера, которая разделяется одним или более индивидуальных подписантов и одним или более групповых подписантов;
- разработан протокол комбинированной коллективной ЭП для индивидуальных и групповых подписантов;
- разработан алгебраический метод псевдовероятностного защитного преобразования, отличающихся представлением двух одновременно шифруемых сообщений в виде элементов конечного поля, заданного в явной векторной форме.

Данные результаты обладают научной новизной, теоретической и практической значимостью и прошли достаточную аппробацию.

Автореферат дает хорошее представление о содержании выполненного исследования и полноте изложения основных результатов в статьях, опубликованных в журналах из списка ВАК РФ.

Судя по автореферату, к недостаткам диссертационной работы можно отнести следующее: отсутствие разработанного программного прототипа, с помощью которого разработанные протоколы и алгоритмы могли быть протестированы экспериментально, и использование нестандартизованного термина «электронная цифровая подпись».

Указанные недостатки не являются принципиальными.

В целом диссертационное исследование «Методы построения и разработка практичных протоколов групповой подписи и алгебраических алгоритмов защитных преобразований» представляется завершенной научно-исследовательской работой, имеющей научную новизну, практическую и теоретическую значимость, и соответствующей требованиям «Положения о присуждении ученых степеней» ВАК РФ, 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.

Доцент кафедры «Информатика и информационная безопасность» Федерального государственного бюджетного образовательного учреждения высшего образования «Петербургский государственный университет путей сообщения Императора Александра I», кандидат технических наук

Глухарев Михаил Леонидович

190031, Санкт-Петербург, Московский просп., д. 9.
телефон: +78123103472
e-mail: kaa.pgups@yande›

пись руки
М.Л. Глухарева
оверяю.
ментовед отдела кадров сотрудников
М.В. Афонина
11 » 12 2017 г.