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.

Задачи аутентификации авторства электронных документов и защиты электронных сообщений от несанкционированного ознакомления играют существенную роль в информационных технологиях. Первая задача решается с использованием протоколов электронной цифровой подписи (ЭЦП). Практические потребности привели к построению протоколов ЭЦП различных типов, включая протоколы групповой подписи, однако известные протоколы не предусматривают использования стандартных индивидуальных открытых ключей, что ограничивает области применения таких проколов. Вторая задача решается путем выполнения защитного преобразования информации. Реализация новых механизмов защиты информации предоставляется алгебраическими алгоритмами псевдовероятностного защитного преобразования. Известные алгоритмы такого типа имеют сравнительно низкую производительность, что ограничивает области их применения. Тема диссертационной работы направлена на поиск методов построения и разработку протоколов ЭЦП и алгоритмов и защитного преобразования, свободных от указанных недостатков, что определяет ее актуальность.

Автореферат дает хорошее представление о содержании выполненного исследования. В ходе диссертационной работы получены следующие основные результаты:

-предложен метод построения протоколов коллективной ЭЦП для групповых подписантов;

-предложен метод построения протоколов комбинированной коллективной ЭЦП для групповых и индивидуальных подписантов;

-предложен метод повышения производительности алгебраических алгоритмов псевдовероятностного защитного преобразования;

-на основе предложенных методов разработаны алгоритмы и протоколы, перспективные для практического применения.

Перечисленные результаты обладают научной новизной, значимостью для теории и практики, прошли достаточную апробацию и достаточно полно изложены в пяти статьях, опубликованных в журналах из списка ВАК.

Судя по автореферату, недостатком диссертационной работы является отсутствие детального рассмотрения конкретных потенциальных приложений разработанных протоколов и связанных с ними моделей нарушителя.

Указанный недостаток не является принципиальным, а выполненное диссертационное исследование является завершенной научно-исследовательской работой, имеющей научную новизну, практическую и теоретическую значимость. Диссертация соответствует 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.

Зам. директора по науке

д.т.н., профессор А.Г. Коробейников

07.12.2017

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

Юридический адрес: 199034, Россия, Санкт-Петербург, Университетская наб, д.5, лит. Б.

Email: Korobeynikov_A_G@mail.ru

Телефон: 8-812-3232807