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.

Протоколы электронной цифровой подписи (ЭЦП) достаточно широко используются в информационных технологиях. При этом практика выдвигает задачу расширения функциональности протоколов цифровой подписи для обеспечения возможности решения новых задач с применением протоколов ЭЦП. Представляют практический интерес протоколы коллективой и групповой ЭЦП, однако их практическое применение ограничивается рядом недостатков, свойственных известным протоколам такого типа. Устранение недостатков известных протоколов обеспечит расширение применения механизмов ЭЦП в информационных технологиях и возможность решения новых практических задач с помощью последних. Направленность темы диссертационного исследования на разработку протоколов групповой ЭЦП, практическое использование которых может быть реализовано на основе стандартной инфраструктуры открытых ключей, обеспечивает их практичность и определяет актуальность выполненного исследования.

Новыми научными результатами выполненного исследований являются:

1. Разработка метода построения протоколов коллективной ЭЦП для групповых подписантов, в качестве каждого из которых выступает коллегиальный орган.

2. Разработка метода построения протоколов комбинированной коллективной ЭЦП для индивидуальных и групповых подписантов.

На основе предложенных методов разработаны протоколы с фиксированным размером подписи, который не зависит от числа подписантов, а число последних может быть произвольным. При этом разработанные протоколы могут быть использованы на практике, используя

уже имеющуюся и действующую на практике инфраструктуру открытых ключей.

Полученные в диссертации результаты имеют практическая и теоретическую значимость. Судя по автореферату результаты диссертационного исследования прошли достаточную апробацию.

Выполненное диссертационное исследование представляется завершенной научной работой, обладающей научной новизной, практической и теоретической значимостью, и 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.

Профессор кафедры «Комплексное обеспечение информационной безопасности»
Федеральное государственное бюджетное образовательное учреждение высшего образования «Государственный университет морского и речного флота имени адмирала С.О. Макарова»
д.т.н., профессор Ныркov Анатолий Павлович

Почтовый адрес - 198035, г. Санкт-Петербург, ул. Двинская, 5/7
Телефон – (812) 748-96-41
Адрес электронной почты – kaf_koib@gumrf.ru

«29» 11 2017 г.