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.

Защитные преобразования информации и протоколы электронной цифровой подписи (ЭЦП) играют важную роль в средствах обеспечения информационной безопасности телекоммуникационных систем. Направленность диссертационного исследования на развитие этих областей определяет актуальность темы выполненного исследования.

Автореферат диссертации дает достаточно полное представление о ее содержании в целом. Как следует из автореферата в диссертационной работе получены следующие основные результаты:

- разработан метод построения протоколов групповой ЭЦП трех типов, целесообразность которых определяется возможностью их внедрения в практику на основе уже имеющейся инфраструктуры открытых ключей;
- разработан метод построения алгебраических алгоритмов псевдо вероятностного защитного преобразования, обладающего более высокой производительностью по сравнению с известными алгоритмами такого типа;
- разработан новый алгоритм псевдо вероятностного защитного преобразования и новые протоколы групповой ЭЦП;
- предложен новый алгебраический алгоритм псевдо вероятностного шифрования защищенный от атак с принуждением открытия ключа шифрования.

Эти результаты обладают научной новизной, имеют существенную значимость для теории и практики. Основные положения достаточно полно представлены в 5 статьях, опубликованных в журналах из списка ВАК.

Основные замечания по работе, которые можно сделать на основе автореферата:

1. Тема диссертации не раскрывает особенностей исследования, которые предполагается выполнить в работе.
2. Цель работы сформулирована нечетко – неясно, что такое «функциональность преобразований» и вообще, чем отличается данная работа от других многочисленных исследований по данным направлениям.
3. Объединение в одной диссертации различных улучшений цифровой подписи, а также защиты методов шифрования от атак с принуждением раскрытия действующего ключа, представляется чрезмерным – хватило бы и одной части, а вторую можно было бы оставить и для другого соискателя.
4. В автореферате не раскрываются некоторые сокращения (например: ЗФ, ЗДЛ), а также не определены некоторые термины, которые нельзя признать общеизвестными даже специалистам по защите информации (алгебраические защитные преобразования – имеется в виду шифры например, AES?; неотказуемость от электронных сообщений; псевдо вероятностное шифрование – имеется в виду гомофонное шифрование?)
5. Список публикаций достаточно впечатляющий, однако обращают на себя внимание следующие его особенности:
   - все работы из перечня ВАК, кроме одной, выполнены в соавторстве, а степень личного вклада автора диссертации в автореферате не отмечена;
   - три из пяти работ 8-9 летней давности;
   - в списке «Другие публикации» из восьми работ пять имеют объем одна страница – достаточно ли этого для изложения научного материала?

Несмотря на сделанные выше замечания, которые в большинстве своем связаны с оформлением автореферата, представляется что в целом выполненное диссертационное исследование является завершенной научно-исследовательской работой, имеющей научную новизну, значимость для

теории и практики. Особенно хочется отметить свободное владение автором сложным математическим аппаратом, который, однако, является необходимым для решения поставленных задач.

Вывод: 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.

Почётный профессор кафедры защищённых систем связи СПбГУТ,
доктор технических наук, профессор,
заслуженный работник высшей школы РФ, член IEEE on IT,

Коржик Валерий Иванович

«11» декабря 2017 г.

Организация:
Федеральное государственное бюджетное образовательное учреждение высшего образования "Санкт-Петербургский государственный университет телекоммуникаций им. проф. М.А. Бонч-Бруевича", www.sut.ru
Почтовый адрес: 193232, Санкт-Петербург, пр. Большевиков д.22, корп.1
Телефон: (812) 326-31-50
Эл. почта: rector@sut.ru