ОТЗЫВ

на автореферат диссертационной работы

Пудовкиной Марины Александровны

«Комбинаторно-алгебраические структуры итерационных функций в системах защиты информации», представленной на соискание ученой степени доктора физико-математических наук по специальности 05.13.19 – Методы и системы защиты информации, информационная безопасность (физико-математические науки).

На современном этапе защита передаваемой и обрабатываемой информации криптографическими методами стала чрезвычайно необходимой во всех сферах деятельности государства и общества. Должны быть обеспечены такие аспекты безопасности информации, как ее конфиденциальность, целостность, стойкость к подмене и ряд других.

В настоящее время в основу многих криптографических алгоритмов защиты информации заложен итерационный принцип, реализуемый итерационной функцией. Широкое распространение итерационной функции в криптографических средствах вызвано эффективностью ее аппаратной и программной реализацией. В настоящее время она обычно используется в функциях хеширования, кодах аутентичности сообщений, поточных и блочных алгоритмах шифрования.

Практика показывает, в частности, что алгоритм блочного шифрования, лежащий в основе многих систем криптографической защиты, обладает уязвимостью. Она проявляется в том, что особенности открытого сообщения проявляются в зашифрованном тексте. Иными словами, криптографические алгоритмы, использующие итерационные функции не обладают необходимой криптографической стойкостью и уязвимы к атакам.

Методы анализа итерационной функции с целью выявления уязвимых мест криптоалгоритмов в настоящее время не развиты в достаточной степени и требуют разработки. В связи с этим, тема диссертационной работы Пудовкиной М.А., посвященной разработке универсального способа исследования структур итерационных криптографических функций, существование которых, прежде всего, вызвано комбинаторно-алгебраическими свойствами, является актуальной.

В диссертации решена проблема разработки универсального математического способа задания и исследования структур (названных в работе p_G-структурами), основанного на исследовании комбинаторно-алгебраических свойств преобразований итерационной криптографической функции. При этом решен ряд сложных математических задач, и получены научные результаты, обладающие безусловной научной новизной и практической значимостью.

Результаты диссертационной работы были применены в ходе выполнения НИР в ООО «СТЦ» при анализе систем закрытия данных, в которых используется алгоритм блочного шифрования AES, для поиска возможных уязвимостей, основанных на существовании различных нетривиальных p_G-структур, что было подтверждено актом о внедрении диссертационных результатов.

Все результаты диссертационной работы Пудовкиной М.А. являются новыми, строго доказанными, опубликованы в рецензируемых печатных изданиях из перечня ВАК РФ. Они прошли достаточную апробацию на семинарах и конференциях различных уровней, в том числе и международных.

По автореферату следует отметить следующие замечания:

1. Обоснованию актуальности темы диссертации и истории вопроса вместе со списком известных источников отведено 8 страниц, что, безусловно, ограничило возможность автора по изложению сути решенных задач;

2. К сожалению, в автореферате не приведены сведения, показывающие результаты применения разработанных p_G-структур к известным алгоритмам блочного шифрования;

3. В автореферате отсутствуют количественные характеристики разработанного способа анализа XSL-алгоритмов блочного шифрования в сравнении с разностным методом.

Отмеченные недостатки носят методический характер и не влияют на положительную оценку работы.

Судя по автореферату, представленные диссертационные результаты могут быть квалифицированы как научное достижение в области методов и системы защиты информации, информационной безопасности.

Диссертационная работа «Комбинаторно-алгебраические структуры итерационных функций в системах защиты информации» отвечает всем требованиям, предъявляемым ВАК к докторским диссертациям по специальности 05.13.19 – Методы и системы защиты информации, информационная безопасность (физико-математические науки), а ее автор, Пудовкина Марина Александровна, заслуживает присуждения ей ученой степени доктора физико-математических наук.

Заместитель начальника отдела связи
Общества с ограниченной ответственностью
«Специальный Технологический Центр»
доктор технических наук (специальность 20.01.09
«Системы управления, в том числе связь в Вооруженных Силах),
профессор по кафедре автоматического
засекречивания связи

Чесноков Михаил Николаевич

«18» апреля 2017 г.

Наименование организации: Общество с ограниченной ответственностью «Специальный Технологический Центр» (ООО «СТЦ»).

Адрес ООО «СТЦ»: Гжатская ул., д. 21, лит. Б, оф. 53, г. Санкт-Петербург, 195220.

Телефон: (812) 244-33-13, тел./факс (812) 535-77-00, (812) 535-58-16

Электронная почта: E-mail: office@stc-spb.ru.

Веб-сайт: http://www.stc-spb.ru/

Подпись Чеснокова Михаила Николаевича заверяю.

Начальник отдела кадров ООО «СТЦ»

Общество с ограниченной ответственностью «Специальный Технологический Центр» СТЦ Санкт-Петербург

Н.И. Герасимова