Ученому секретарю
диссертационного совета
Д 212.267.22 при НИ ТГУ
Тренькаеву В.Н.
634050, г. Томск, пр. Ленина 36

на автореферат диссертации 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

Развитие информационно-телекоммуникационных технологий неизбежно приводит к возникновению новых угроз обеспечения безопасности информации, и, следовательно, вызывает необходимость разработки и совершенствования методов защиты. Многие подходы, лежащие в основе методов защиты информации, основаны на итерационных функциях, которые применяются, например, при построении кодов аутентификации, функций хеширования, алгоритмов шифрования и т.д. В связи с этим актуальной проблемой является исследование итерационных функций с целью разработки общих математических методов, предназначенных для выявления уязвимостей в системах защиты информации, основанных на этих функциях.

В диссертации Пудовкиной М.А. рассмотрена и решена проблема совершенствования и применения методов и средств защиты информации в процессе ее сбора, хранения, обработки, передачи и распространения и обеспечения информационной безопасности цифровых объектов от внешних и внутренних угроз хищения, разрушения и/или модификации информации математическими методами в информационных системах.

Считаю, что соискателем получены следующие научные результаты:

1. Обнаружена общая связь комбинаторно-алгебраических свойств отдельных преобразований, составляющих итерационную функцию, с наличием потенциальных уязвимостей блочных шифров, что является существенно важным для задач совершенствования математических методов защиты информации.

2. Предложен способ описания структур алгоритмов блочного шифрования, использующий разбиения t-грамм множества X (t=1,2), наличие которых может свидетельствовать об уязвимостях средств защиты информации в информационно-телекоммуникационных сетях.

3. Описаны подстановочные и комбинаторные свойства групп, порожденных разными множествами преобразований, составляющих итерационную

функцию. Проанализированы связи алгебраических свойств таких групп и введенных метрик, задающих анализируемые структуры.

Работа достаточно полно опубликована: 51 научная публикация, в том числе в 14 журналах из списка ВАК Российской Федерации и в 6 печатных изданиях, индексируемых Web of Science и Scopus. Результаты исследования докладывались на достаточном количестве научных конференций различного уровня.

Тем не менее, к автореферату имеются следующие замечания:

1. Из текста автореферата неясно, какая связь существует между APN-подстановками и p_G-структурами.
2. На странице 24 автореферата имеется опечатка в фразе о s-боксах алгоритма SAFER.
3. Пункт 6 научной новизны, сформулированный на странице 9 автореферата, не отражен в тексте автореферата.

Замечания не влияют на общую положительную оценку работы и не опровергают ее основных положений. Автореферат написан математически корректным языком и хорошо структурирован. Как часть выполненной научной работы автореферат отражает компетентность соискателя в области проводимых исследований и хорошее владение современными математическими методами.

Диссертация Пудовкиной М.А. на тему «Комбинаторно-алгебраические структуры итерационных функций в системах защиты информации» является законченной научно-квалификационной работой, содержащей решение актуальной научной проблемы повышения уровня защищенности информационных систем математическими методами удовлетворяет требованиям ВАК при Минобрнауки РФ, предъявляемым к диссертациям по специальности 05.13.19 - Методы и системы защиты информации, информационная безопасность (физико-математические науки), а её автор Пудовкина Марина Александровна заслуживает присуждения ученой степени доктора физико-математических наук.

Доктор технических наук, профессор, профессор РАН
проректор по научной работе и инновациям,
заведующий кафедрой безопасности информационных систем,
ФГБОУ ВО «Томский государственный университет
систем управления и радиоэлектроники»
(специальность 05.13.01 – системный анализ, управление и обработка информации)
Р. В. Мещеряков

18.04.2017

Мещеряков Роман Валерьевич
Адрес: 634050, г. Томск, пр. Ленина, 40
Тел.: +7 (382-2) 51-43-02
E-mail: mrv@tusur.ru