

Отзыв

научного руководителя на диссертацию

Чередника Игоря Владимировича

«Использование бинарных функциональных сетей при
построении кратко транзитивных множеств блочных
преобразований»,

представленную на соискание ученой степени кандидата
физико-математических наук по специальности 05.13.19 —
«Методы и системы защиты информации, информационная
безопасность» (физико-математические науки).

В работе И. В. Чередника изучаются классы блочных преобразований, которые реализуются уникальной (для класса) бинарной функциональной сетью фиксированной ширины и параметризуются бинарной операцией. Базовое множество, на котором определены бинарные операции-параметры, может варьироваться. Подобные классы преобразований естественным образом возникают во многих узлах обработки и защиты информации и при этом на них, как правило, накладывается ряд дополнительных требований. Первым требованием является обратимость каждого преобразования из класса — это необходимо для корректной обработки данных в узлах защиты информации. Очевидным необходимым условием глобальной обратимости является обратимость параметра-операции по одной из переменных. Поэтому в работе рассматриваются два вида множеств параметров: квазигруппы (операция обратима по обоим переменным) и бинарные операции, обратимые по второй переменной. Второе требование вытекает из соображений обеспечения безопасности: класс преобразований должен действовать транзитивно, то есть для любой пары (вход, выход) должно существовать значение параметра, при котором соответствующая классу сеть преобразует данный вход в данный выход. Усилением условия транзитивности является условие k -кратной транзитивности, то есть возможность перевода любых k входов в любые k выходов. Построение классов преобразований, удовлетворяющих перечисленным условиям, позволит создавать новые защищенные узлы обработки информации. Таким образом, задача является **актуальной и практически значимой**.

Основной целью работы И. В. Чередника является исследование описанных классов преобразований. Возникают следующие подзадачи:

1. нахождение необходимых и достаточных условий, обеспечивающих обратимость каждого преобразования из класса независимо от выбора параметра ($\mathcal{R}$ -биективность в терминах работы);

2. создание эффективных методов проверки транзитивности и кратной транзитивности класса преобразований;
3. разработка алгоритмов построения $\mathcal{R}$ -биективных сетей, реализующих классы преобразований со свойством k -кратной транзитивности при заданном k ;
4. явное построение семейств $\mathcal{R}$ -биективных сетей, реализующих классы преобразований со свойством k -кратной транзитивности при заданном k .

Содержание диссертации отражает приведенные постановки. Диссертация состоит из введения, трех глав и заключения.

Во **введении** описываются цели работы, обосновывается актуальность и практическая значимость, приводятся основные результаты.

В **первой главе** вводятся основные понятия и исследуются вопросы $\mathcal{R}$ -биективности. Важным результатом здесь является теорема 1.2, в которой устанавливается критерий $\mathcal{R}$ -биективности и “нормальный вид” сети, реализующей класс $\mathcal{R}$ -биективных преобразований.

Во **второй главе** изучается вопрос о транзитивности. Доказывается ряд критериальных свойств транзитивных сетей (сводка таких свойств приведена в следствии 2.4), описывается конструкция, позволяющая преобразовать произвольную $\mathcal{R}$ -биективную сеть в сеть, реализующую классы транзитивных преобразований (теорема 2.10), явно указываются две конструкции сетей небольшой сложности (автор обозначает их Δ_n и Ψ_n), которые реализуют транзитивные классы преобразований.

Третья глава посвящена вопросу кратной транзитивности. Как и в случае второй главы, автору удалось получить критериальные свойства k -транзитивности (следствие 3.5), описать конструкцию, преобразующую произвольную $\mathcal{R}$ -биективную сеть в сеть, реализующую классы k -кратно транзитивных преобразований (теорема 3.14), и явно указать конструкции сетей ∇_n , гарантирующих кратную транзитивность.

В **заключении** перечисляются основные результаты диссертации.

Отдельно отметим технику доказательств. Автором разработан оригинальный аппарат разметок сетей, представляющий значительный интерес.

Содержание работы **свидетельствует** о том, что полученные в ходе ее создания **результаты являются новыми и вносят вклад в решение научной задачи** — построения транзитивных и k -кратно транзитивных классов преобразований для узлов обработки и защиты информации.

Практическая значимость полученных результатов состоит в возможности их применения при построении новых защищенных узлов обработки информации.

Основные результаты диссертации докладывались на Всероссийской конференции «Сибирская научная школа-семинар с международным участием “Компьютерная безопасность и криптография”» в 2017 и 2018 годах, на XXII научно-практической конференции «РусКрипто’2020», на специальных семинарах механико-математического факультета МГУ. По результатам исследований автором опубликовано 6 работ, включая четыре статьи в рецензируемых журналах из списка Scopus и/или Web of Science.

Достоверность и обоснованность результатов подтверждается:

- четкостью формулировок утверждений и строгостью представленных доказательств;
- апробацией на семинарах и конференциях;
- опубликованием основных результатов в рецензируемых журналах.

С учетом изложенного считаю, что **работа И. В. Чередника соответствует критериям, установленным в “Положении о присуждении ученых степеней в Московском государственном университете имени М.В. Ломоносова”, и рекомендуется к защите в диссертационном совете МГУ.05.01 ФГБОУ ВО МГУ по специальности 05.13.19 — методы и системы защиты информации, информационная безопасность, а ее автор, несомненно, заслуживает присуждения ему ученой степени кандидата физико-математических наук.**

Научный руководитель
кандидат физико-математических наук,
старший научный сотрудник
кафедры математической теории
интеллектуальных систем

А.В. Галатенко

Подпись старшего научного сотрудника А. В. Галатенко удостоверяю.

Декан механико-математического
факультета МГУ имени М.В.Ломоносова
д.ф.-м.н., профессор,
член-корреспондент РАН

А. И. Шафаревич