ОТЗЫВ

на автореферат диссертации Перова Артёма Андреевича «Универсальный метод построения решающих правил с использованием сверточных нейронных сетей для анализа генераторов псевдослучайных последовательностей на основе итеративных блочных шифров», представленной на соискание ученой степени кандидата технических наук по специальности 05.13.17 – Теоретические основы информатики

Получение псевдослучайных последовательностей, неотличимых от случайных и обладающих большим периодом, является важной задачей при построении вычислительных сетей. Искусственные нейронные сети получили на данный момент широкое распространение и успешно используются при решении различных задач. Диссертация Перова Артёма Андреевича посвящена применению свёрточных нейронных сетей к задаче статистического анализа генераторов псевдослучайных чисел, построенных на базе блочных шифров с итеративной (раундовой) структурой. В связи с этим считаю, что избранная тема диссертации актуальна.

А. А. Перовым предложен оригинальный подход к построению решающих правил на основе свёрточных нейронных сетей для обнаружения закономерностей и отклонений от случайности в псевдослучайных последовательностях, полученных посредством указанных генераторов. Соискателю удалось построить такие решающие правила, которые выявляют отклонения от случайности эффективнее некоторых других аналогов для генераторов на базе ряда блочных шифров. В ходе работы разработан и реализован расширяемый программный комплекс для статистического анализа генераторов псевдослучайных чисел на основе итеративных блочных шифров, включающий более 50 генераторов, а также решающие правила на основе статистических тестов и свёрточных нейронных сетей.

Все выносимые на защиту результаты являются новыми. Достоверность и обоснованность полученных результатов подтверждается их

теоретическим обоснованием, наличием публикаций в рецензируемых изданиях, а также апробацией результатов на ведущих конференциях в соответствующей области.

Автореферат свидетельствует о том, что структура диссертации отвечает поставленной цели и основным задачам. Материалы проведенного исследования изложены логично и последовательно.

Из недостатков текста автореферата можно отнести указание иностранных авторов только на английском языке, отсутствие нескольких запятых (например, с. 11 «для того, чтобы»), отсутствие курсива и полужирный шрифт в некоторых формулах.

Считаю, что отмеченные недостатки не снижают значимости работы и общего качества автореферата.

На основании автореферата можно заключить, что диссертационное исследование А. А. Перова на тему «Универсальный метод построения решающих правил с использованием сверточных нейронных сетей для анализа генераторов псевдослучайных последовательностей на основе итеративных блочных шифров» является завершённым научным исследованием, соответствует требованиям ВАК, поэтому считаю, что соискатель Перов Артём Андреевич достоин присуждения ему учёной степени кандидата технических наук по специальности 05.13.17 – Теоретические основы информатики.

Доцент кафедры теоретических основ компьютерной безопасности и криптографии ФГБОУ ВО «СГУ имени Н.Г. Чернышевского», кандидат физико-математических наук

Жаркова Анастасия Владимировна

15.03.2024

Тел.: +7 (8452) 21-36-19
E-mail: ZharkovaAV3@gmail.com

Адрес: 410012, г. Саратов, ул. Астраханская, 83
Телефон ректора: +7(8452) 26-16-96
E-mail: rector@sgu.ru
Сайт: https://www.sgu.ru/

Подпись удостоверяю
Ученый секретарь
доцент М.В. Федусенко
«15» 03 2024