

Л.И. Покидышевой Д 212.099.22
660074, г. Красноярск, ул. Киренского, 26, СФУ

ОТЗЫВ
на автореферат диссертации
Перова Артема Андреевича

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

Диссертация А.А. Перова посвящена применению сверточных нейронных сетей к анализу генераторов псевдослучайных последовательностей с особенной (итеративной) структурой. Генераторы такого типа могут строиться на основе блочных шифров, хеш-функций и других алгоритмов, состоящих из раундов (итераций). Псевдослучайные последовательности, в свою очередь, широко применяются во многих разделах информатики, в том числе, при исследовании процессов создания, накопления и обработки информации, а также при создании аппаратных и программных средств автоматизации.

В своей работе А.А. Перова показал, что для некоторых итеративных генераторов псевдослучайных последовательностей применение нейронных сетей позволяет либо сократить размер выборки, требуемой для обнаружения закономерностей и отклонений от случайности в генерируемых последовательностях, либо увеличить число раундов (итераций генератора), для которого удается обнаружить такие отклонения по сравнению с решающими правилами на основе других эмпирических методов. Важным свойством предложенного в диссертации метода построения решающих правил является его универсальность, т.е. применимость к широкому спектру генераторов без необходимости глубокого анализа их внутренней структуры (как это требуется, например, при применении аналитических методов).

Исходя из положений, сформулированных в автореферате, можно заключить, что структура диссертации выстроена последовательно и логично. Автореферат диссертации содержит все необходимые разделы и характеризуется четкостью изложения цели, задач и результатов исследования.

Тем не менее, в работе имеются следующие недостатки:

1. Из текста автореферата сложно понять, что чем обусловлен выбор такого нетипичного термина, как «сценарий» при описании предлагаемого метода. Например, возникает вопрос, почему автор не выносит каждый сценарий в отдельный метод или, скажем, не параметризует этот метод.
2. В автореферате (стр. 7) декларируется об использовании результатов диссертационной работы в ряде организаций, однако отсутствует описание того было внедрено и результаты внедрения.

Обозначенные замечания не являются критичными и не снижают теоретической и практической ценности диссертации, результаты которой представлены в печатных работах и аprobированы на семинарах и конференциях достаточно полно.

В целом, автореферат позволяет сделать вывод о том, что диссертация 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» выполнена на высоком уровне, представляет собой завершенное исследование, отвечает требованиям ВАК, а ее автор, Перов Артем Андреевич, заслуживает присуждения ученой степени кандидата технических наук по специальности 05.13.17 – Теоретические основы информатики.

Главный научный сотрудник,
ФГБУН «Институт проблем управления им. В. А.
Трапезникова РАН»,
д-р техн. наук, профессор
Тел.: +7 495 198-17-20, доб. 1625
E-mail: mrv@ipu.ru

Мещеряков
Роман
Валерьевич

10.03.2021



Адрес: 117997, г. Москва, ул. Профсоюзная, д. 65, ИПУ РАН
Тел.: +7 495 334-89-10; Факс: +7 495 334-93-40, +7 499 234-64-26
E-mail: dan@ipu.ru
Сайт: www.ipu.ru