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 учёной степени кандидата технических наук по специальности 05.13.17 – «Теоретические основы информатики»

В диссертационной работе Перова А.А. предлагается новый метод анализа генераторов псевдослучайных последовательностей. Исследование выполнено на стыке нескольких актуальных научных направлений: искусственного интеллекта, теории информации, информационной безопасности. Предлагается несколько нестандартное применение свёрточных нейронных сетей, в частности архитектуры Inception V3, ResNet-v2 и EfficientNet, которые обычно применяются для классификации цифровых изображений. Автор трансформирует объекты исследования в графические эквиваленты и в ходе экспериментов выполняет их различение с помощью нейросети.

В своей работе автор решает несколько задач:

1. Разработка алгоритма обработки псевдослучайных последовательностей для конвертации их в формат, пригодный для обучения свёрточной нейронной сети.

2. Алгоритмическое описание и математическое обоснование нового метода построения решающих правил для обнаружения закономерностей и отклонений от случайности в псевдослучайных последовательностях.

3. Программная реализация предлагаемого метода и сопутствующих средств.

4. Определение параметров рассматриваемых генераторов, при которых обеспечивается неотличимость от равномерно распределенных величин.

Универсальность предлагаемого метода, отмеченная в названии, заключается в том, что подобное исследование может быть проведено для любого типа итеративных генераторов, хеш-функций, булевых функций, что позволяет работе иметь перспективы развития.

Несмотря на наличие научной и практической значимости полученных результатов, по автореферату можно сделать следующие замечания:

1. На стр. 19 для проверки прохождения тестов автор приводит формулу для вычисления статистики хи-квадрат, однако описание элементов

этой формулы проведено не совсем точно. В частности, нет информации, что есть k, с другой стороны в описании представлена переменная v, вместо которой в формуле присутствует v_i . Попытка проведения вычислений с приведенными в описании значениями (150 и 126) привели к указанному ответу при одном слагаемом, т.е. при k=1. О каком числе степеней свободы в этом случае идет речь?

2. На рис. 4 приведены три линии, при этом в описании речь идет только о двух. Прямая линия, проходящая примерно из левого верхнего угла в правый нижний, никак не описывается и ее смысл не ясен.

Сделанные замечания носят локальный характер и не ставят под сомнение основные результаты диссертационной работы. Считаю, что работа Перова А.А. «Универсальный метод построения решающих правил с использованием сверточных нейронных сетей для анализа генераторов псевдослучайных последовательностей на основе итеративных блочных шифров» представляет собой законченное научное исследование, выполненное на современном научном уровне, содержит новые результаты, полученные лично автором, имеет внутреннее единство и согласованность и отвечает требованиям "Положения о присуждении ученых степеней" (п. 9-11, 13, 14) для кандидатских диссертаций, а её автор Перов Артём Андреевич заслуживает присуждения искомой степени кандидата технических наук по специальности 05.13.17 - "Теоретические основы информатики".

Профессор кафедры теоретической
и прикладной информатики Новосибирского
государственного технического университета,
д.т.н, доцент Тимофеев В.С.

Согласен на обработку персональных данных.

Тимофеев Владимир Семенович,
630072, Новосибирск, пр. К. Маркса, 20,
Организация: Новосибирский государственный технический университет,
+7(383)346-37-54, email: v.timofeev@ccfit.nstu.ru

Подпись
ЗАВЕРЯЮ
Начальник ОК
17.03.2021 г.
О. К. Пустовалова