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»

Современные методы машинного обучения и, в частности, свёрточные нейронные сети решают очень широкий спектр задач. Данный инструмент находит своё применение и в задачах информационной безопасности, например, реализуя автоматизированный тест Тьюринга при прохождении авторизации в различных информационных сервисах.

В представленной Перовым А.А. работе существенно изменен подход к статистическому анализу выходных последовательностей. Автор разработал метод построения решающих правил, который отличается от предложенных ранее. Методы, основанные на математическом аппарате, работают за счёт анализа каждого следующего входного значения. Предлагаемый автором метод не анализирует каждое конкретное значение, а используя идею преобразования результатов работы генератора в единую структуру (изображение), анализирует выборку целостно. Предлагаемый Перовым А.А. метод перспективен по той причине, что свёрточные нейронные сети постоянно прогрессируют по метрикам точности классификации, что соответственно позволит развивать предлагаемый метод в дальнейшем и получать новые научные результаты.

В результате работы автором получены новые результаты:

1. Предложен алгоритм обработки псевдослучайных последовательностей, полученных с помощью генераторов на базе итеративных блочных шифров, с целью их представления в формате, который подходит для обучения нейронной сети.

2. Предложен новый универсальный метод построения решающих правил на основе свёрточных нейронных сетей для обнаружения закономерностей и отклонений от случайности в псевдослучайных последовательностях, полученных с помощью генераторов на основе итеративных блочных шифров.

3. Приведены результаты экспериментов, которые в ряде случаев превосходят ранее опубликованные либо по размерам выборки, либо по числу итераций преобразования открытого текста.

4. Разработан программный комплекс, реализующий предлагаемый в диссертационной работе метод.

Особенно необходимо отметить п.3: автор действительно превзошёл некоторые ранее опубликованные результаты, что подтверждается ключевыми ссылками на научные статьи в самом тексте автореферата.

Работа прошла апробацию на различных научных семинарах, и результаты исследований опубликованы в достаточном объеме в научных журналах и тезисах конференций, а также получены свидетельства о регистрации программ ЭВМ.

Из автореферата не совсем понятно: почему в качестве эталона псевдослучайной последовательности выбран алгоритм-генератор на базе шифра AES?

Несмотря на выявленный недостаток, содержание автореферата позволяет утверждать, что диссертационная работа Перова А.А. «Универсальный метод построения решающих правил с использованием сверточных нейронных сетей для анализа генераторов псевдослучайных последовательностей на основе итеративных блочных шифров» выполнена на высоком научном уровне и представляет собой законченное научное исследование, а её автор, Перов А.А. заслуживает присуждения учёной степени кандидата технических наук по специальности 05.13.17 – Теоретические основы информатики.

Доцент кафедры информационных технологий ФГБОУ ВО «Сочинский государственный университет», канд. техн. наук, доцент
E-mail: rav@sutr.ru

Ревнивых Александр Владимирович

Тел.: +7-929-263-7777

10.03.2021 г.

354000, Краснодарский край, г. Сочи, ул. Пластунская, 94

Подпись Ревнивых А.В.
Заверяю
Начальник УК
Ляпина Н.Г.