

ОТЗЫВ

официального оппонента **Елисеева Владимира Леонидовича**

на диссертацию **Перова Артёма 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»

Актуальность диссертационного исследования Артёма Андреевича Перова обосновывается значительным вниманием, которое в настоящее время уделяется разработке методов обработки информации для обеспечения помехоустойчивости и безопасности использования информационных технологий при передаче, хранении и защите информации. При этом большое значение имеют исследования, связанные с методами машинного обучения и обнаружения закономерностей в данных. Это обуславливает пристальное изучение соответствующих разделов науки и техники и поиск новых более эффективных методов исследования в этих областях. К современным весьма востребованным подходам анализа данных относятся методы машинного обучения, в частности, с использованием сверточных глубоких искусственных нейронных сетей, примененных автором в своем диссертационном исследовании.

Изучение статистических свойств генераторов псевдослучайных последовательностей на основе блочных шифров и близких к ним хэш-функций является важнейшим аспектом их эффективного применения. Диссертация А.А. Перова развивает данную тему и предлагает методы оценки качества генераторов псевдослучайных последовательностей на основе итеративных блочных шифров с помощью подходов машинного обучения, упрощающих в ряде аспектов анализ качества случайности генерируемой последовательности.

Основная идея диссертации заключается в применении сверточной нейронной сети, традиционно используемой для анализа изображений и обученной на выявлении типовых паттернов, в качестве различителя, позволяющего решить, имеется ли закономерность между раундами блочного

шифра или нет? Применение построенного решающего правила позволяет обоснованно ограничить число раундов блочного шифра и обеспечить более эффективное использование исследуемого блочного шифра в режиме CTR в качестве генератора псевдослучайной последовательности чисел без потери качества этой последовательности. Данная идея может быть применена в различных сценариях, а также для различных блочных шифров. Универсальность инструмента, лежащего в основе различителя закономерностей – сверточной нейросети – позволяет использовать метод построения решающих правил для генераторов псевдослучайных последовательностей на основе различных блочных шифров.

Предложенные подходы к оценке качества псевдослучайной последовательности сопоставляются со стандартом de-facto в области генераторов случайных чисел – тестами NIST. Проведенные в диссертации теоретические и экспериментальные исследования позволяют убедиться в обоснованности разработанного метода и хорошем качестве анализа псевдослучайных последовательностей, в некоторых случаях превосходящего тесты NIST по эффективности в части меньшего объема используемой выборки.

В качестве эффективного критерия качества блочного шифра с раундовыми преобразованиями автор сформулировал положение о минимальном количестве раундов, которое позволяет сделать преобразование блочного шифра неотличимым от случайного. Эта граница R_{min} , по мнению автора, может быть получена разными способами, продемонстрированными в диссертации. Для ряда шифров R_{min} составляет меньшее количество раундов, чем реализовано в шифре, что позволяет сделать предположение о снижении количества раундов без потери стойкости криптографического преобразования и, следовательно, качества получаемой случайной последовательности.

Наиболее значимыми результатами диссертации следует признать:

- 1) Новый универсальный метод анализа псевдослучайной последовательности, создаваемой с помощью итеративных блочных шифров, в части построения решающих правил для обнаружения отклонений от равномерного распределения;
- 2) Теоретическое обоснование метода построения решающих правил;
- 3) Обширное исследование генераторов псевдослучайных последовательностей, созданных на базе итеративных блочных шифров;

- 4) Формулировка показателя качества генератора на базе итеративных блочных шифров через минимальное число раундов, обеспечивающих заданные статистические свойства псевдослучайных последовательностей;
- 5) Программный комплекс для анализа псевдослучайных последовательностей, генерируемых с помощью итеративных блочных шифров, и реализующий разработанные решающие правила.

Достоверность результатов подтверждается применением методов теории вероятностей, методов математической статистики и обоснованным использованием методов машинного обучения с использованием глубоких сверточных нейронных сетей, а также экспериментальным сопоставлением с существующими методами анализа качества случайных последовательностей.

В диссертации 153 страницы, из них введение, три главы и заключение занимают 124 страницы, имеются 21 иллюстрация и 12 таблиц.

По теме диссертации автором опубликовано 18 работ, в которых отражены основные результаты исследований, из них 4 статьи опубликованы в журналах из перечня ВАК, 2 публикации сделаны в изданиях, индексируемых в Scopus/WoS, 11 публикаций представлены в материалах международных и всероссийских конференций. Имеются 2 свидетельства о государственной регистрации программы для ЭВМ.

Материалы диссертации полностью отражают её объем и сложность проделанной автором работы. Автореферат диссертации полностью соответствует ее содержанию.

Замечания

- 1) В обзоре практически полностью обойдено вниманием применение нейронных сетей для реализации криптографических преобразований. В частности, не упомянуты так называемые хаотические нейросети, а также синтез шифров с помощью соревновательных нейросетей. Есть также неупомянутые работы по криптоанализу с использованием искусственных нейронных сетей (например, R. Focardi, F. Luccio «Neural Cryptanalysis of Classical Ciphers», 2018).
- 2) Выбор архитектуры Inception ResNet-v2 в первой главе производится раньше изложения разработанного метода, поэтому обоснование выглядит чужеродно в подразделе, в котором рассматривается

машинное обучение в криптографии и информационной безопасности. Это тем более неуместно, что обоснование выбора Inception ResNet-v2 затем повторяется во второй главе с большими подробностями.

- 3) В выводах к первой главе особо отмечено значимое определение R_{min} , однако это обозначение впервые появляется во второй главе.
- 4) Следует отметить некоторые неточности, связанные с упоминаемыми в тексте диссертации стандартами на блочные шифры. В частности, ГОСТ Р 34.12–2015 в настоящее время заменен на ГОСТ Р 34.12–2018, а под обозначением AES14, видимо, следует понимать 14-раундовый AES, то есть, AES256.
- 5) Некоторые утверждения, ссылающиеся на предыдущий опыт, даются без ссылок и иных пояснений об их происхождении. Например, на стр. 46: «Практика проведения статистического анализа классическими методами показывает, что если на вход итеративного генератора подаётся случайная последовательность, то результаты статистического анализа могут быть некорректны».
- 6) Некоторые упоминаемые в тексте суждения не могут быть поняты однозначно. Например, на стр.55 в предложении «Эталонный сценарий предполагает наличие последовательности, которая обладает удовлетворительными статистическими свойствами» неясно, что такое «удовлетворительные статистические свойства». На стр.57 неясно, что такое «абсолютно объективные результаты»: «в противном случае результаты тестирования могут не быть абсолютно объективными». На стр. 58 сообщается о том, что «корректный выбор алгоритмов-оппонентов позволил получить результаты, сопоставимые с результатами, полученными с помощью группы тестов NIST», не уточняя, что же такое «корректный выбор».
- 7) В некоторых местах нумерация таблиц, рисунков и ссылок на них не соответствуют друг другу (например, на стр. 50 и стр. 57).

Диссертация Артёма Андреевича Перова соответствует паспорту специальности 05.13.17 – «Теоретические основы информатики» и является завершённой научно-квалификационной работой, содержащей новые результаты в актуальной сфере науки и техники, полученные с помощью современных подходов интеллектуального анализа данных.

По моему мнению, 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» соответствует требованиям п.9 «Положения о присуждении ученых степеней» постановления Правительства Российской Федерации от 24.09.2013 г. №842, а её автор Перов Артём Андреевич достоин присуждения ученой степени кандидата технических наук по специальности 05.13.17 – «Теоретические основы информатики».

Официальный оппонент:

Доцент кафедры

Управления и интеллектуальных технологий

ФГБОУ ВО «НИУ «МЭИ»,

кандидат технических наук



Елисеев Владимир Леонидович

Дата: 11.03.2021

Тел.: +7 (916) 914-9889

Эл. почта: vlad-eliseev@mail.ru

Лорись уростоверлю

Почтовый адрес: 111250, Москва, ул. Красноказарменная, д.13а

Тел.: +7 (495) 362-74-07

Эл. почта: ui@mpei.ru

Сайт: <http://uii.mpei.ru>



ЗАМЕСТИТЕЛЬ НАЧАЛЬНИКА
УПРАВЛЕНИЯ ПО РАБОТЕ С ПЕРСОНАЛОМ

