

**ОТЗЫВ**  
официального оппонента **Ложникова Павла Сергеевича**  
на диссертацию **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

**Актуальность диссертационного исследования**

Диссертация Перова Артема Андреевича посвящена применению нейронных сетей для построения решающих правил, используемых при анализе итеративных генераторов псевдослучайных чисел на основе блочных шифров.

Псевдослучайные последовательности и методы их генерации играют важную роль во многих задачах информатики, кибернетики и информационных технологий. Они используются в теоретических и прикладных исследованиях всевозможных информационных моделей, при исследовании функционирования аппаратных и программных средств автоматизации, при анализе данных различного рода и при решении ряда других задач. Особенность итеративных генераторов, являющихся объектом настоящего диссертационного исследования, состоит в том, что они состоят из простых итераций (раундов), позволяющих находить баланс между производительностью и качеством получаемых псевдослучайных чисел.

Помимо значимости объекта исследования (генераторов псевдослучайных последовательностей) актуальность темы диссертации А.А. Перова обусловлена значимостью основного инструмента исследования – нейронных сетей, которые являются одним из важнейших разделов сферы искусственного интеллекта. Данная технология является приоритетной в ряде нормативных документов, принятых в России за последние годы и описывающих стратегические приоритеты страны в отношении информационных технологий: Национальная технологическая инициатива (2014 г.), Национальная программа «Цифровая экономика РФ» (2018 г.), Национальная стратегия развития искусственного интеллекта на период до 2030 года (2019 г.). Содержание этих документов указывает на то, что исследование соискателя актуально и своевременно.

## **Основная идея диссертации**

Основная идея диссертации, которая лежит в основе предложенного в метода, состоит в следующем. Псевдослучайные последовательности при различном количестве раундов (итераций блочного шифра) конвертируются в растровые изображения, называемыми автором «графическими эквивалентами», которые затем используются для обучения сверточной нейронной сети.

В диссертации сформулирована и подтверждена гипотеза о том, что разработанные решающие правила на основе сверточных нейронных сетей в определенных случаях могут позволить обнаруживать закономерности и отклонения от случайности в псевдослучайных последовательностях, полученных посредством генераторов на основе итеративных блочных шифров, более эффективно, чем некоторые ранее известные универсальные решающие правила. При этом, соискателем выявлены как случаи, когда предложенный метод оказывается эффективнее, а когда – нет.

Двумя основными показателями эффективности решающих правил являются минимальный размер выборки и максимальное число раундов (итераций) генератора, при которых с помощью решающего правила оказывается возможным обнаружить отклонения от случайности.

Предложенный в диссертации метод основан на том, что представленные в виде своих графических эквивалентов псевдослучайные последовательностей имеют различные паттерны (иначе говоря, графические эквиваленты обладают отличной друг от друга текстурой), зависящие от числа раундов и от шифра, на основе которого создан генератор. С увеличением количества перемешивающих итераций (раундов) эти паттерны меняются и все больше становятся схожи с равномерным шумом, в котором отсутствуют какие-либо закономерности.

Основная идея диссертации представляет собой оригинальное применение сверточных нейронных сетей к известной задаче обнаружения закономерностей и отклонений от равномерного распределения в псевдослучайных последовательностях. Предложенный метод сочетает в себе, с одной стороны, универсальность решающих правил на основе статистических тестов, а с другой – способен проанализировать выборку целиком и принять решение не только на основе одного интегрального критического значения, а по аналогии с классификацией графических изображений находит взаимосвязи в целой выборке.

В работе показано, что для некоторых генераторов можно либо уменьшить размер выборки, либо увеличить число раундов, при котором удается обнаружить отклонения.

Предложенный метод построения решающих правил является универсальным в том смысле, что он может быть применим для генераторов псевдослучайных последовательностей на основе *любых* итеративных блочных шифров. В то же время, хочется отметить, что предложенный метод потенциально применим не только для генераторов на основе блочных шифров, но и для практически любых других генераторов, обладающих итеративной структурой. Данный факт свидетельствует о том, что работа имеет перспективы развития. Потенциально метод может быть расширен с целью применения к генераторам на основе хеш-функций и других итеративных алгоритмов.

**Наиболее значимыми результатами диссертации следует признать:**

1. Новый универсальный (не привязанный к конкретному генератору) метод построения решающих правил для обнаружения закономерностей и отклонений от равномерного распределения в псевдослучайных последовательностях, полученных с помощью генераторов на основе итеративных блочных шифров;
2. Теоретическое обоснование метода построения решающих правил, эффективность которого экспериментально показана для ряда генераторов псевдослучайных последовательностей, созданных на базе итеративных блочных шифров;
3. Экспериментально найденные значения минимального числа итераций (раундов) блочных шифров, на основе которых созданы генераторы, обеспечивающие удовлетворительные статистические свойства псевдослучайных последовательностей;
4. Программный комплекс для анализа псевдослучайных последовательностей, включающий серию различных решающих правил и множество существующих генераторов, на базе итеративных блочных шифров.

**Достоверность результатов** подтверждается теоретическим обоснованием предлагаемого метода, а также продемонстрированными практическими примерами, по которым можно отслеживать изменения текстур графических эквивалентов рассматриваемых последовательностей. В работе показано, что картина результатов, полученных при помощи предложенного метода в целом согласуется с результатами, полученными другими ранее известными методами.

Общий объем диссертации составляет 153 страницы. Основная часть, включающая введение, три главы, заключение и список литературы, изложена на 124 страницах и включает 21 иллюстрацию и 12 таблиц.

По теме диссертации автором опубликовано 18 работ, в которых материалы диссертации отражены достаточно полно, из них 4 статьи в журналах из Перечня ВАК, 2 публикации в Scopus/WoS (одна из этих двух статей также входит в Перечень ВАК), 11 публикаций в материалах международных и всероссийских конференций, 2 свидетельства о государственной регистрации программы для ЭВМ.

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

### **Замечания**

1. В тексте диссертации отсутствует обоснование того, почему размер выборки при анализе предложенным методом всегда один и тот же (равен  $2^{21.9}$ ), в то время как в других методах, используемых в работе, размер выборки варьируется.
2. Мало внимания уделено анализу внутренней архитектуры сверточной нейронной сети, которая применяется для построения решающих правил в рамках диссертации. Возможно, более тонкая настройка нейронной сети позволит повысить эффективность решающих правил.
3. В диссертации исследовано применение только одной нейронной сети (Inception ResNet-v2), хотя, логично было бы изучить, как ведут себя решающие правила, построенные на основе других нейронных сетей.
4. Из текста диссертации плохо понятно, почему при экспериментальном обосновании эффективности построенных решающих правил в основном используется только генератор на основе итеративного блочного шифра Simon (с. 42-43, 69-70), а результаты по остальным алгоритмам приведены только в таблицах на с. 71, 73-74.
5. В диссертации представлены только два акта о внедрении («Акстел-Безопасность» и «НИИ ИКТ»), хотя в автореферате на с. 7 говорится об использовании результатов в образовательном процессе ФГБОУ ВО НГУЭУ и ФГАОУ ВО НГУ.
6. В тексте диссертации имеются опечатки: с. 44 («отности»), с. 50 (повторяется слово «получен»), с. 101 («подразумевается»), с. 102 («просыходит»); есть замечания по оформлению текста: с. 11-12, 90, 115 (использование кавычек разного типа), с. 115-116 (отдельные источники литературы оформлены не единообразно с остальными).

## **Общее заключение по диссертации**

Отмеченные замечания не являются критическими и не снижают научной ценности диссертации.

Диссертация Перова Артема Андреевича соответствует паспорту специальности 05.13.17 – Теоретические основы информатики, обладает внутренним единством и является завершенной научно-квалификационной работой, в которой на основании выполненных автором исследований изложены новые научно обоснованные результаты в области теоретической информатики, имеющие важное прикладное значение. Научное направление, в рамках которого проведено данное диссертационное исследование актуально, современно и имеет перспективы развития.

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

### **Официальный оппонент:**

Заведующий кафедрой  
«Комплексная защита информации»,  
ФГБОУ ВО «Омский  
государственный технический  
университет»,  
д-р техн. наук, доцент

Ложников Павел Сергеевич

04.03.2021

Тел.: (3812) 21-77-02  
Эл. почта: [lozhnikov@mail.ru](mailto:lozhnikov@mail.ru)

Почтовый адрес: 644050, Сибирский федеральный округ, Омская область, г. Омск, Пр. Мира, д. 11, ОмГТУ  
Тел.: (3812) 65-34-07;  
Факс: (3812) 65-26-98;  
Эл. почта: [info@omgtu.ru](mailto:info@omgtu.ru);  
Сайт: <https://omgtu.ru/>

