На правах рукописи

Перов Артём Андреевич

УНИВЕРСАЛЬНЫЙ МЕТОД ПОСТРОЕНИЯ РЕШАЮЩИХ ПРАВИЛ С ИСПОЛЬЗОВАНИЕМ СВЕРТОЧНЫХ НЕЙРОННЫХ СЕТЕЙ ДЛЯ АНАЛИЗА ГЕНЕРАТОРОВ ПСЕВДОСЛУЧАЙНЫХ ПОСЛЕДОВАТЕЛЬНОСТЕЙ НА ОСНОВЕ ИТЕРАТИВНЫХ БЛОЧНЫХ ШИФРОВ

Специальность 05.13.17 – Теоретические основы информатики

АВТОРЕФЕРАТ

диссертации на соискание ученой степени
кандидата технических наук по специальности

Красноярск – 2021

Работа выполнена в Федеральном государственном бюджетном образовательном учреждении высшего образования «Новосибирский государственный университет экономики и управления «НИНХ»

Научный руководитель: кандидат физико-математических наук, доцент **Пестунов Андрей Игоревич**

Официальные оппоненты: **Ложников Павел Сергеевич,** доктор технических наук, доцент, Федеральное государственное бюджетное образовательное учреждение высшего образования "Омский государственный технический университет", кафедра комплексной защиты информации, заведующий кафедрой

Елисеев Владимир Леонидович, кандидат технических наук, доцент, Федеральное государственное бюджетное образовательное учреждение высшего образования "Национальный исследовательский университет «МЭИ», кафедра управления и интеллектуальных технологий, доцент

Ведущая организация:
Федеральное государственное бюджетное учреждение науки Институт математики им. С. Л. Соболева Сибирского отделения Российской академии наук

Защита состоится «07» апреля 2021 года в 14.00 часов на заседании диссертационного совета Д 212.099.22, созданного на базе Сибирского федерального университета по адресу: 660074, г. Красноярск, ул. Киренского, 26, ауд. УЛК 112.

С диссертацией можно ознакомиться в библиотеке и на сайте Сибирского федерального университета по адресу http://www.sfu-kras.ru/

Автореферат разослан «___» февраля 2021 г.

Ученый секретарь
диссертационного совета Покидышева Людмила Ивановна

ОБЩАЯ ХАРАКТЕРИСТИКА РАБОТЫ

Актуальность и степень разработанности проблемы. Псевдослучайные последовательности имеют большое значение при решении многих задач, связанных с исследованием информационных моделей, анализом функционирования программно-аппаратных средств, обеспечением высоконадежной обработки информации, в том числе для целей ее передачи, хранения и защиты.

Особым классом генераторов псевдослучайных последовательностей являются генераторы с итеративной структурой, формирующие очередное псевдослучайное число посредством повторения относительно простого преобразования, называемого раундом, над входными данными несколько раз. Зачастую такие генераторы разрабатываются на основе итеративных блочных шифров в режиме счетчика (CTR).

Оценка качества генераторов обычно осуществляется через применение методов обнаружения закономерностей и отклонений от случайности в полученных псевдослучайных последовательностях. Выбор подходов к построению решающих правил для обнаружения таких закономерностей обусловлен итеративной структурой рассматриваемых генераторов. Для этого разрабатываются специальные решающие правила на основе так называемых различителей, предназначенных для распознавания псевдослучайных последовательностей, получаемых после разного количества раундов. При этом важной задачей является поиск максимального количества раундов, при котором такие правила способны отличить разные раунды друг от друга. Эффективные решающие правила на основе различителей представляют научный интерес как сами по себе, так и в комплексе, когда на их основе создаются алгоритмы вычисления неизвестных параметров генератора. В случае применения блочного шифра это могут быть секретные ключи.

Методы построения решающих правил на основе различителей можно условно разделить на два класса: аналитические и эмпирические (в основном статистические). Многие аналитические методы базируются на выявлении дифференциальных, линейных или интегральных признаков, описывающих свойства псевдослучайной последовательности после заданного числа раундов. Затем обнаружение закономерностей осуществляется через выявление этих свойств в сгенерированной последовательности.

Большой вклад в развитие аналитических методов построения решающих правил внесли зарубежные ученые A. Shamir, E. Biham, A. Biruykov, B. Schneier, M. Matsui, D. Wagner и др. Ими предложены разнообразные подходы к построению различителей и алгоритмов вычисления неизвестных параметров на их основе. Аналитические подходы позволяют строить решающие правила для большого количество раундов и находить уязвимости, проявляемые только на очень больших выборках или при наличии недоступных на практике вычислительных ресурсов (например, порядка 2^{128} элементарных операций или байт памяти). В работах Г.П. Агибалова, Б.А. Погорелова, М.А. Пудовкиной, Х.

Lai, J. Massey, K. Nyberg, S. Vaudenay и др. развиваются теории, описывающие те или иные свойства аналитически построенных решающих правил в общем виде, однако поскольку используемые в них признаки тесно связаны с конкретными генераторами, то аналитически построенные решающие правила не являются универсальными и эффективны только для целевого генератора.

Помимо аналитических методов построения решающих правил для обнаружения закономерностей в псевдослучайных последовательностях, полученных при помощи генераторов на основе итеративных блочных шифров, могут использоваться эмпирические статистические методы. В рамках таких методов решающие правила строятся на основе критериев, позволяющих отличить последовательность от случайной в ходе экспериментов на выборках, размер которых приемлем для расчетов. Так, в работах L. Knudsen предложена и для некоторых генераторов псевдослучайных последовательностей успешно применена универсальная методика вычисления неизвестных параметров генератора, где в качестве различителя выступает критерий хи-квадрат. Для малого числа раундов, когда для распознавания отклонения от равномерного распределения достаточно выборок, размеры которых относительно невелики, атака осуществляется экспериментально, а для большего числа раундов размер необходимой выборки экстраполируется аналитически на основе полученных экспериментальных данных. В рамках этого подхода Б.Я. Рябко, Ю.И. Шокиным, А.Н. Фионовым и др. предложены решающие правила на основе статистических тестов, использующих динамически изменяемые структуры, что позволило повысить их эффективность для ряда алгоритмов.

Достоинством решающих правил на основе статистических различителей является их универсальность, проявляющаяся в том, что по одной и той же схеме можно проанализировать серию генераторов псевдослучайных последовательностей без детального учета индивидуальных особенностей архитектуры каждого из них. При этом необходимость проведения экспериментальных расчетов накладывает ограничения на размер выборки, которую возможно обработать. Применение машинного обучения имеет потенциал добиться снижения размера выборки за счет более тонкого анализа паттернов, встречающихся в псевдослучайных последовательностях, полученных при варьируемом количестве раундов итеративного блочного шифра, на котором основан генератор.

Кроме того, решающие правила на основе статистических различителей далеко не всегда способны обнаруживать сложные паттерны в проверяемых выборках и использовать это при выявлении отклонений от случайности. Обычно решение принимается на базе интегральных накопительных характеристик, обновляемых после обработки очередного выборочного элемента, но не учитывающих многие корреляции.

Машинное обучение позволяет решать широкий спектр задач по реализации систем поддержки принятия решений, прогнозированию, оптимизации и распознаванию образов. Эти технологии уже применялись к исследованию генераторов псевдослучайных последовательностей на основе

итеративных блочных шифров, однако, в основном такие методы используют не только сгенерированные псевдослучайные числа, но и требуют дополнительных данных, полученных через побочные каналы (см. работы L. Lerman, G. Bontempi, B. Hettwer, S. Gehrer и др.).

M. Bernardi, P. Malacaria и др. показали, что глубокая нейронная сеть способна обучиться генерировать псевдослучайные последовательности так, чтобы они отвечали требованиям информационной безопасности и проходить ряд тестов на случайность. Наиболее эффективные решающие правила для обнаружения отклонений от случайности, вызванных скрытой в стего-изображениях информации, также активно используют именно машинное обучение, в частности, метод опорных векторов и ансамблевые классификаторы (см. работы J. Fridrich, A. Ker, M. Goljan, T. Pevny, J. Kodovsky, R. Bohme и др.). Такая информация может быть обнаружена за счет того, что она, хотя и незначительно, но нарушает статистические связи между соседними пикселями стего-контейнера.

Таким образом, применение методов машинного обучения имеет потенциал их использования в разработке решающих правил для обнаружения закономерностей и отклонений от случайности в псевдослучайных последовательностях, которые, с одной стороны, обладают универсальностью, а с другой – учитывают внутреннюю структуру итеративных генераторов.

Рабочая гипотеза исследования. Решающие правила на основе сверточных нейронных сетей могут позволить обнаруживать закономерности и отклонения от случайности в псевдослучайных последовательностях, полученных посредством генераторов на основе итеративных блочных шифров более эффективно, чем универсальные решающие правила на базе статистических тестов.

Целью диссертационной работы является разработка универсального метода построения решающих правил на основе сверточных нейронных сетей для обнаружения закономерностей и отклонений от случайности в псевдослучайных последовательностях, полученных посредством генераторов, созданных на основе итеративных блочных шифров.

Для достижения цели решались следующие **задачи**:

1. Разработать алгоритм обработки псевдослучайных последовательностей для представления их в формате, пригодном для обучения нейронной сети.

2. Разработать, алгоритмически описать и математически обосновать метод построения решающих правил для обнаружения закономерностей и отклонений от случайности в псевдослучайных последовательностях, полученных при помощи генераторов на базе блочных шифров.

3. Создать программные реализации разработанных алгоритмов и применить их к экспериментальному исследованию генераторов псевдослучайных последовательностей на базе современных итеративных блочных шифров; сравнить полученные результаты с результатами анализа

псевдослучайных последовательностей посредством универсальных решающих правил на основе статистических тестов.

4. Определить параметры генераторов на базе итеративных блочных шифров, обеспечивающие неотличимость полученных псевдослучайных последовательностей от равномерно распределенных случайных величин.

Объектом исследования являются генераторы псевдослучайных последовательностей на основе итеративных блочных шифров.

Предметом исследования являются решающие правила для обнаружения закономерностей в псевдослучайных последовательностях, полученных посредством генераторов с итеративной структурой.

Методы исследований. Методы машинного обучения, сверточные нейронные сети; аппарат теории вероятностей и математической статистики; технологии структурного и объектно-ориентированного программирования; инструментарий графического моделирования и визуализации данных.

Научная новизна диссертационной работы заключается в следующем.

1. Предложен и теоретически обоснован новый метод построения решающих правил на основе сверточных нейронных сетей для обнаружения закономерностей в псевдослучайных последовательностях, полученных с помощью итеративных генераторов. В отличие от аналитических подходов, которые предполагают анализ внутренней структуры конкретного генератора и поэтому не применимы к другим, новый метод универсален и позволяет строить решающие правила для любых итеративных генераторов. В то же время, в отличие от многих универсальных правил, основанных на статистических критериях и обрабатывающих выборочные значения отдельно друг от друга, нейронная сеть принимает для анализа всю выборку целиком, что дает возможность более точного обнаружения закономерностей.

2. Экспериментально подтверждена эффективность построенных решающих правил применительно к генераторам псевдослучайных чисел, основанных на итеративных блочных шифрах в режиме счетчика. Для ряда генераторов построенные решающие правила позволяют достичь лучших результатов по сравнению со статистическими тестами, в том числе, базирующимися на адаптивных кодах и структурах («стопка книг», порядковый тест и «адаптивный критерий хи-квадрат») и др. В частности, решающие правила позволяют обнаруживать закономерности (отклонения от равномерного распределения) при меньших объемах выборок и при большем количестве итераций генератора.

3. В результате применения построенных решающих правил для ряда генераторов на основе современных итеративных блочных шифров уточнены существующие оценки минимального количества итераций (раундов), которое требуется для обеспечения удовлетворительных статистических свойств псевдослучайных последовательностей, а также впервые получены новые оценки для тех генераторов, для которых таких оценок не существовало.

Положения, выносимые на защиту.

1. Метод построения универсальных решающих правил для обнаружения закономерностей в псевдослучайных последовательностях.
2. Теоретическое обоснование предложенного метода и результаты экспериментального исследования, подтверждающие его эффективность.
3. Оценки минимального количества раундов, требуемого для обеспечения удовлетворительных статистических свойств псевдослучайных последовательностей, полученных с помощью итеративных генераторов на основе блочных шифров.
4. Созданный на основе предложенного метода программный комплекс для анализа псевдослучайных последовательностей, полученных при помощи итеративных генераторов, основанных на блочных шифрах.

Личный вклад автора.

Все результаты, выносимые на защиту, получены автором лично.

Теоретическая значимость. Разработан новый универсальный метод построения решающих правил на основе сверточных нейронных сетей для анализа генераторов псевдослучайных последовательностей на основе итеративных блочных шифров. Метод имеет перспективу быть развитым в общий подход построения решающих правил для анализа любых генераторов на основе итеративных алгоритмов, в том числе хеш-функций и других.

Практическая значимость работы. Разработан программный комплекс для статистического анализа генераторов псевдослучайных последовательностей на базе итеративных блочных шифров при помощи решающих правил на основе сверточных нейронных сетей и универсальных статистических тестов. Для ряда генераторов определены параметры, обеспечивающие удовлетворительные статистические свойства получаемых псевдослучайных последовательностей и отсутствие закономерностей в них. Получены два свидетельства о регистрации программ для ЭВМ в Федеральной службе по интеллектуальной собственности.

Результаты диссертационной работы используются в образовательном процессе кафедры информационных технологий ФГБОУ ВО НГУЭУ и факультета информационных технологий ФГАОУ ВО НГУ, а также в практической деятельности компании «Акстел-Безопасность» и Научно-исследовательского института информационно-коммуникационных технологий (НИИ ИКТ).

Достоверность результатов обеспечена корректностью постановок задач, математическими доказательствами теоретических утверждений, экспериментальной проверкой теоретических результатов, сравнением полученных экспериментальных данных с эталонными.

Соответствие диссертации паспорту специальности. Содержание диссертации соответствует п. 5 «Разработка и исследование моделей и алгоритмов анализа данных, обнаружения закономерностей в данных и их извлечениях; разработка и исследование методов и алгоритмов анализа текста, устной речи и изображений», п. 7 «Разработка методов распознавания образов,

фильтрации, распознавания и синтеза изображений, решающих правил. Моделирование формирования эмпирического знания», п. 11 «Разработка методов обеспечения высоконадежной обработки информации и обеспечения помехоустойчивости информационных коммуникаций для целей передачи, хранения и защиты информации; разработка основ теории надежности и безопасности использования информационных технологий».

Апробация работы. Результаты диссертации докладывались и обсуждались на следующих конференциях и семинарах: XIV Международная научно-практическая конференция «Информационная безопасность», Таганрог (2015); Всероссийская конференция молодых ученых по математическому моделированию и информационным технологиям (2015, 2019 – получен диплом победителя конференции); Всероссийская научная конференция молодых ученых «Наука. Технологии. Инновации» (2015, 2016); Международная научная студенческая конференция МНСК, (2016, 2017); Научная сессия ИТФ НГУЭУ, секция «Информационная безопасность и защита информации», Новосибирск, (2015, 2016); конф. «Информационные технологии» в рамках науч. сессии НГУЭУ (2017, 2018); Конференция «Актуальные направления научной мысли: проблемы и перспективы», Новосибирск (2018); Всероссийская конференция «Сибирская научная школа-семинар с международным участием "Компьютерная безопасность и криптография"» SIBECRYPT (2019, 2020); 2019 International Multi-Conference on Engineering, Computer and Information Sciences (SIBIRCON), Новосибирск (2019); Международная научно-практическая конференция «Распределенные информационно-вычислительные ресурсы: Цифровые двойники и большие данные» (DICR 2019), Новосибирск (2019);

Научный семинар «Криптография и криптоанализ» (рук. к.ф.-м.н. Н.Н. Токарева, ИМ им. С.Л. Соболева СО РАН), 2019; Научный семинар Сибирского государственного университета телекоммуникаций и информатики (рук. д.т.н. А.Б. Мархасин), 2019; Объединенный семинар ИВТ СО РАН и НГУ «Информационные технологии» (рук. академик Ю.И. Шокин и к.ф.-м.н. А.В. Юрченко), 2020; Научный семинар кафедры «Комплексная защита информации» ОмГТУ (рук. д.т.н. П.С. Ложников), 2020.

Публикации.

По теме диссертации автором опубликовано 18 работ, из них 4 статьи в журналах ВАК, 2 публикации в Scopus/WoS, 11 публикаций в материалах международных и всероссийских конференций, 2 свидетельства о государственной регистрации программы для ЭВМ. Общий объем публикаций составляет 4.25 п.л., авторский вклад – 3.54 п.л.

Объем и структура диссертации.

Диссертационная работа состоит из введения, 3 глав основного содержания, списка использованных источников из 107 наименований и 12 приложений. Общий объем диссертации 153 страницы (основное содержание изложено на 124 страницах), включая 21 иллюстрацию и 12 таблиц.

ОСНОВНОЕ СОДЕРЖАНИЕ РАБОТЫ

Во **введении** обосновывается актуальность выбранной темы, определены цели и задачи исследования, раскрыта научная новизна работы и практическая значимость полученных результатов. Сформулированы положения, выносимые на защиту.

В **первой главе** представлен обзор исследований по теме диссертации. Рассмотрены современные направления развития машинного обучения, существующие архитектуры нейронных сетей и возможные сферы применения этих технологий для решения практически значимых задач. Проанализированы аналитические и статистические подходы к оцениванию итеративных генераторов псевдослучайных последовательностей, в том числе, на примере блочных шифров.

В качестве базовой архитектуры нейронной сети для реализации предлагаемого в настоящей диссертационной работе метода была выбрана Inception ResNet-v2. Помимо Inception ResNet-v2 применялись современные архитектуры EfficientNet и Inception V3. Данные модели являются одними из лидеров по показателю точности классификации изображений. Конечный выбор архитектуры Inception ResNet-v2 обоснован балансом между скоростью обучения и точностью категоризации изображений, что подтверждено в статье[1], где автор применял вышеописанные модели и устанавливал зависимость между числом параметров соответствующей модели и точностью определения, при этом выполняя экспертную оценку производительности. Погрешность в рамках экспериментов настоящей работы варьировалась в рамках допустимой и существенно не повлияла на полученные результаты. Так, EfficientNet-B7 показала точность категоризации на 5% выше Inception V3, однако в эксперименте на контрольной выборке разница по точности не превосходила 1.5%.

Таким образом, базовой моделью для последующих экспериментов выбрана Inception ResNet-v2, базовая архитектура которой приведена на рисунке 1.

На входе выполняется свертка 7x7 с 64 выходными каналами. Далее следует слой с максимальной сверткой 3x3, который на выходе уменьшает высоту и ширину входного изображения в 4 раза. После этого на ветках А и Б происходит одномерная свертка с увеличением каналов обработки изображения. Для исключения резкого снижения размерности данных используется сверточный слой подвыборки. На последнем этапе используется несколько одномерных сверток для наиболее точного формирования паттернов каждой генерируемой псевдослучайной последовательности.

---

[1] **Mingxing T., Quoc V. Le** EfficientNet: Rethinking Model Scaling for Convolutional Neural Networks // Proceedings of the 36th International Conference on Machine Learning. Long Beach, California, 2019.

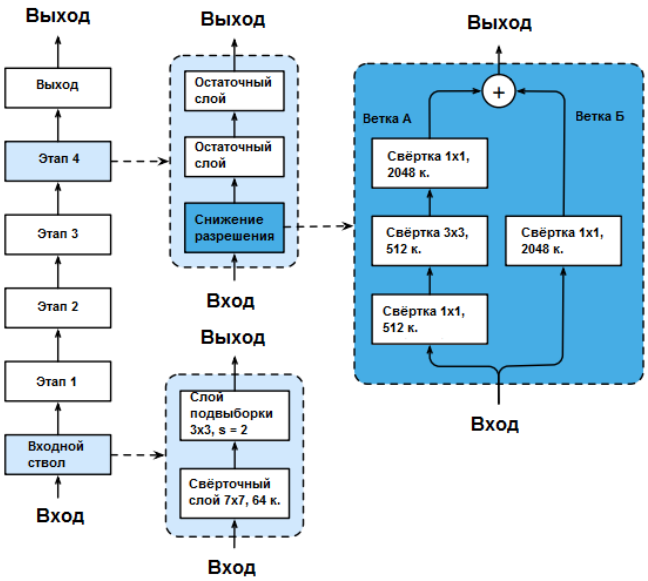

Рисунок 1 – архитектура сверточной нейронной сети Inception ResNet-v2

Во **второй главе** приводится описание метода построения решающих правил на основе сверточных нейронных сетей для анализа итеративных генераторов псевдослучайных чисел. Предлагаемый метод основан на различении графических эквивалентов псевдослучайных последовательностей, полученных посредством генераторов на основе итеративных блочных шифров.

Идея предлагаемого метода возникла в результате наблюдения следующей закономерности: преобразованная в растровое изображение выходная последовательность итеративного блочного шифра, полученная на малом числе раундовых преобразований, имеет выраженную текстуру (паттерн), которая с увеличением числа раундов изменяется в сторону равномерно шумного изображения. На рисунке 2 приведен пример изменения графического эквивалента последовательности (далее – отображения) на примере итеративного блочного шифра Simon.

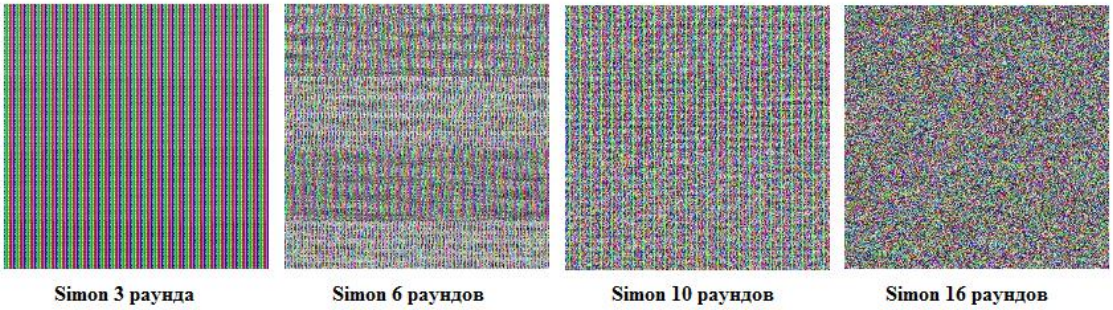

Рисунок 2 – демонстрация изменений текстуры генерируемых последовательностей при разном числе раундов (на примере итеративного блочного шифра Simon)

Из рисунка 2 видно, что последовательности на каждом из раундов обладают определенными паттернами, и эти изображения могут быть отличимы даже визуально. Согласно некоторым исследованиям, глубокие сверточные нейронные сети, решающие задачи классификации графических изображений, превзошли результаты человека еще в 2015 году и имеют очень высокие показатели точности. Основываясь на данной идее, предлагается метод

построения решающих правил, основанный на применении сверточной нейронной сети.

Предлагаемый метод имеет два основных сценария. Общая схема работы представлена на рисунке 3. *Сценарий анализа, основанный на сравнении соседних раундов* одного и того же алгоритма, предполагает обучение нейронной сети на последовательностях, полученных при каждом из раундов до полного числа раундов генератора.

Эталонный сценарий выполняет аналогичные сравнения генерируемых последовательностей, однако выборка на каждом раунде сравнивается с последовательностью при полном числе раундов (в экспериментах предлагалось сравнение с полнораундовым шифром AES, использующим 14 раундов для 256-битного ключа).

Для функционирования предлагаемого метода необходимо выполнить обучение сверточной нейронной сети. Ниже представлен псевдокод *алгоритма 1*, описывающий процесс обучения.

Алгоритм 1. Обучение сверточной нейронной сети

Шаг 1: **Функция** ОбучитьНейронную Сеть(*Cipher, r, M*)
Cipher – итеративный блочный генератор;
r – число раундов генератора, на котором проводится тест;
M – размер обучающего множества;
Шаг 2: Сгенерировать *M* выборок с помощью генератора Cipher и получить $\tilde{y}^r = (\tilde{y}_1^r, \dots, \tilde{y}_M^r)$
Шаг 3: **Если** выбран «эталонный сценарий», **то** Сгенерировать *M* выборок с помощью генератора *AES14* и получить $\tilde{y}^{rand} = (\tilde{y}_1^{rand}, \dots, \tilde{y}_M^{rand})$
Иначе если выбран сценарий «соседних раундов» **то** Сгенерировать *M* выборок с помощью генератора Cipher и получить $\tilde{y}^{r+1} = (\tilde{y}_1^{r+1}, \dots, \tilde{y}_M^{r+1})$
Шаг 4: Преобразовать сгенерированные множества выборок $\tilde{y}^r$ **и** ($\tilde{y}^{rand}$**или** $\tilde{y}^{r+1}$) в изображения. Полученные множества обозначим $y^r = (y_1^r, \dots, y_M^r)$, $y^{rand} = (y_1^{rand}, \dots, y_M^{rand})$, $y^{r+1} = (y_1^{r+1}, \dots, y_M^{r+1})$
Шаг 5: Обучить нейронную сеть различать изображения из обучающих выборок y^r **и** (y^{rand} **или** y^{r+1}).
Шаг 6: **Вернуть** НейронныйСеть^r(image), которая будет относить image к 0 (случайной) или 1 (неслучайной) последовательности.

При проведении исследований предлагаемым методом, как и в тестах из главы 3, на вход алгоритма рекомендуется подавать максимально неслучайную последовательность: в режиме счетчика (counter mode, CTR) возможна подача порядковых чисел или одного и того же одинакового числа. Выполняя шифрование при разном числе раундов в режиме CTR, получаем выборку выходных последовательностей блочных шифров со статистическими свойствами различной степени случайности. На *шаге 2-3* приведенного алгоритма 1 с помощью системы «УНИБЛОКС-2015» выполняется такое шифрование. На *шаге 4* сгенерированные псевдослучайные последовательности преобразуются в формат растровых графических изображений для того чтобы нейронная сеть корректно выполнила процесс обучения. Преобразование

последовательностей в графический формат производится автоматизировано с помощью разработанной программной утилиты на языке C++. Утилита выполняет конвертацию текстового файла (или опционально – потоковой последовательности) в BMP файл с глубиной 24 бита, где каждая компонента палитры RGB кодируется 8 битами (палитра содержит 256 цветов). Принцип преобразования заключается в последовательном присваивании компонентам палитры RGB значений считываемых байт из генерируемой последовательности.

После преобразования последовательностей с помощью разработанной на языке C++ утилиты TxtToIMG Utility и формирования выборки уже на уровне изображений происходит переобучение последнего слоя сверточной нейронной сети на графические эквиваленты (*шаг 5 алгоритма 1*). В процессе обучения нейронная сеть запоминает основные паттерны, характерные для генерируемых последовательностей при разном числе раундов, которые использует для последующей категоризации.

После выполнения процесса обучения, выполняется распознавание сгенерированных последовательностей. В зависимости от выбранного сценария на контрольной выборке нейронная сеть сравнивает последовательности на соседних раундах (или сравнивает последовательности при выбранном раунде с «эталоном», например, полнораундовым AES), подсчитывает процент верных решений при определении принадлежности элемента контрольной выборки к тому или иному множеству. С увеличением числа раундов и, соответственно, улучшением статистических свойств, модель увеличивает значение E (E – число ошибок, допущенных моделью при определении принадлежности). *Алгоритм 2* описывает процесс статистического тестирования методом MLSA.

Алгоритм 2. Общая схема решающих правил, построенных с помощью предлагаемого метода

Шаг 1: **Функция** РаспознатьПоследовательность(*x*, *Cipher*, *r*)
x – запрошенная последовательность;
Cipher – итеративный блочный генератор;
r – число раундов генератора;
Шаг 2: Выбрать размер обучающей выборки *M*
Шаг 3: НейроннаяСеть^r(image) = ОбучитьНейроннуюСеть(*Cipher*, *r*, *M*)
Шаг 4: Представить выборку *x* в виде изображения *image*
Шаг 5: *Result*:=НейроннаяСеть^r(*image*)
Шаг 6: **Если** *Result* = 0, **то вернуть** «выборка случайна»
иначе если *Result* = 1, **то вернуть** «выборка неслучайна»

Одной из задач предлагаемого алгоритма является нахождение значения параметра R_{min} – минимального числа раундов, при котором обеспечиваются удовлетворительные статистические свойства. Алгоритм 3 описывает процесс поиска R_{min}.

Алгоритм 3. Определение параметра R_{min}

Шаг 1: **Функция** Вычислить R_{min}(*Cipher*)
Шаг 2: Для всех r = $\overline{1, R}$
НейроннаяСеть^r = ОбучитьНейроннуюСеть(*Cipher*, *r*, *M*)
Шаг 3: $x^r = (x_1^r, \ldots, x_N^r)$
Шаг 4: **Пока** ($E_0 + E_1 \in [M - \delta_\alpha, M + \delta_\alpha]$)
Выполнять ($E_0 + E_1$) := ВычислитьОшибку(*Cipher*)
r:=r+1; R_{min} := r;
Шаг 5: **Вернуть** R_{min}

Общая схема предлагаемого метода представлена на рисунке 3.

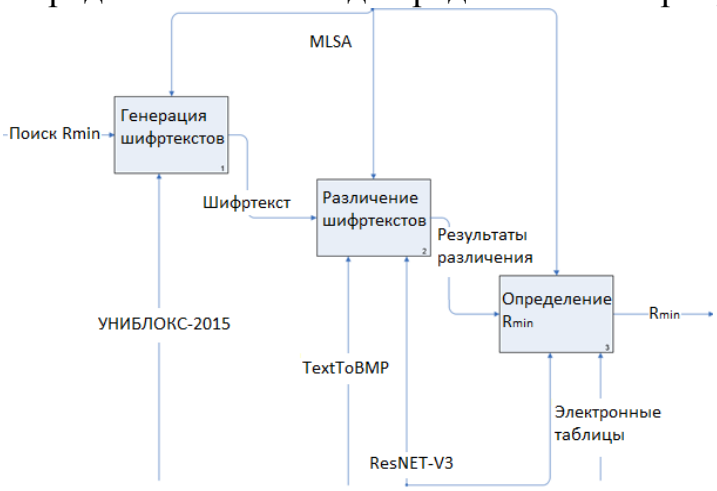

Рисунок 3 – общая схема метода MLSA

Эффективность решающих правил, построенных с помощью предлагаемого метода (способность нейронной сети отличать выходные последовательности генераторов при различном числе раундов друг от друга и от случайных последовательностей), оценивалась через долю верных решений нейронной сети на элементах контрольной выборки.

Теорема. Пусть n – размер контрольной выборки и α – уровень значимости решающего правила, тогда при $\tilde{\delta}(n, \alpha) = \frac{Q_{\alpha/2}}{2\sqrt{n}}$, где $Q_{\alpha/2} = F_{0,1}^{-1}\left(1 - \frac{\alpha}{2}\right)$ – квантиль стандартного нормального распределения уровня $1 - \frac{\alpha}{2}$, выполняется

$$\tilde{S}_n \subset [{}^1/_2 - \tilde{\delta}(n, \alpha); {}^1/_2 + \tilde{\delta}(n, \alpha)] \leq \alpha.$$

Доказательство. Введем следующие случайные величины для $i = \overline{1, n}$.

$$\eta_i = \begin{cases} 1 - \text{нейронная сеть приняла верное решение на } i\text{ом изображении}, \\ 0 - \text{нейронная сеть ошиблась}. \end{cases}$$

Тогда количество верных решений нейронной сети (S_n) и их долю ($\tilde{S}_n$) на всей контрольной выборке можно определить следующим образом:

$$S_n = \sum_{i=1}^{n} \eta_i, \ \tilde{S}_n = S_n / n.$$

Найдем теперь такое $\tilde{\delta}$ (n, α), что при $\tilde{\boldsymbol{S}}_{\boldsymbol{n}} \subset [{}^{1}/_{2} - \tilde{\delta}(n,\alpha); {}^{1}/_{2} + \tilde{\delta}(n,\alpha)]$ можно было бы сделать вывод о том, что нейронная сеть способна отличать сгенерированные и случайные последовательности друг от друга эффективнее простого угадывания. Пусть

$$\boldsymbol{S}_{\boldsymbol{n}}^{*} = \frac{S_n - ES_n}{\sqrt{DS_n}}, \quad (1)$$

где ES_n и DS_n – соответственно математическое ожидание и дисперсия S_n.

Из центральной предельной теоремы следует, что $P\,(S_n^* \subset [-\delta; \delta]) \approx F_{0,1}(\delta) - F_{0,1}(-\delta)$, где $F_{0,1}(\cdot)$ – функция стандартного нормального (гауссовского) распределения.

Пусть $Q_{\alpha/2} = F_{0,1}^{-1}\left(1 - \frac{\alpha}{2}\right)$ – квантиль стандартного нормального распределения уровня $1 - \frac{\alpha}{2}$, тогда $P\left(S_n^* \subset \left[-Q_{\alpha/2}; Q_{\alpha/2}\right]\right) \approx 1 - \alpha$.

Если нейронная сеть неспособна отличать графические эквиваленты сгенерированных и неотличимых от случайных последовательностей друг от друга, то все случайные величины η_i будут иметь распределение Бернулли с параметром 1/2, т.е. $P(\eta_i = 1) = P(\eta_i = 0) = 1/2$, поскольку результат работы нейронной сети будет равносилен случайному угадыванию. Следовательно, ES_n = n/2, DS_n = n/4, а формулу (1) можно преобразовать к виду

$$S_n^* = \frac{S_n - n/2}{\sqrt{n}/2} = \frac{2S_n - n}{\sqrt{n}}. \quad (2)$$

Далее из (2) получаем, что $\tilde{\delta}$ (n, α) = $\frac{Q_{\alpha/2}}{2\sqrt{n}}$. **Теорема доказана.**

Например, при α = *0.01* величина $Q_{0.01/2}$ равна 2.59, и при таких значениях $\tilde{\delta}$(0.01; 200) = 0.09, и $\tilde{\delta}$(0.01; 2000) = 0.03

Основным преимуществом предлагаемого метода является возможность использования выборки меньшей, чем требуется для классических статистических тестов. Экспериментальное обоснование эффективности предлагаемого метода приведено в главе 3. За счет подхода нейронных сетей к классификации графических изображений, при котором анализируется не каждое текущее значение счетчика как при тестировании классическими методами, а определяются общие паттерны всей выборки, ее объем может не превышать $2^{21.9}$ бит информации.

В **третьей главе** представлено экспериментальное исследование предложенного метода и обоснование его эффективности.

Параграф 3.1 посвящен постановке задачи статистического тестирования итеративных генераторов.

В **параграфе 3.2** приведены результаты экспериментов методом MLSA. Для проведения экспериментов предлагаемым методом выполнялось конфигурирование модификации архитектуры нейронной сети Inception ResNet-v2. В ходе исследования варьировались следующие параметры:

– Image size (размер изображения): параметр, определяющий размер выборки. Для различения были использованы изображения 400 на 400 пикселей. Увеличение этого параметра замедляет процесс обучения при минимальном увеличении показателей точности.

– Batch size (размер партии): параметр устанавливает количество изображений, между которыми модель нейронной сети производит поиск общих признаков за итерацию. Экспериментально найден параметр равный 32 изображениям. Уменьшение параметра для большинства алгоритмов (за исключением KATAN64 и KTANTAN64) означало снижение точности распознавания. Значительное увеличение размера партии приводит к уменьшению производительности и потенциальному переобучению нейронной сети, что также ведет к снижению точности распознавания.

– Input shape – параметр, определяющий число нейронов на входном слое сети. В данном случае это число напрямую связано с размером изображения, так как принцип работы сверточной нейронной сети по распознаванию изображений заключается в сложении соседних пикселей и поиске объединяющих признаков от общего к частному.

Предложенные значения параметров позволили обеспечить требуемое соотношение между точностью категоризации отображений и скоростью обучения нейронной сети. Реализация предложенного метода выполнена на языке Python с использованием программных библиотек для машинного обучения TensowFlow и FastAI.

На рисунке 4 представлен график зависимости процента верных решений, принятых моделью нейронной сети при попытке различения по сценарию «соседних раундов» от их числа для генератора псевдослучайных последовательностей на основе блочного шифра Simon (красный график) и эталонного сценария (синий график).

Рисунок 4 – график верных решений для шифра Simon

Необходимо отметить, что с ростом числа раундов количество верных решений нейронной сети стремится к значению 0.5. Это связано с тем, что с улучшением статистических свойств блочного шифра модель нейронной сети совершает большее число ошибок при попытке отличить элементы выборок соседних раундов.

Для алгоритма Simon было найдено, что на 15 раунде (для тестов «стопка книг» и комплекса тестов NIST) достигается значение R_{min}.

Значение R_{min}, найденное классическими тестами, совпадает с моментом, когда процент верных решений сверточной нейронной сети становится приближен к 0.5. Такое поведение нейронной сети объясняется тем, что на большом числе раундов последовательности становятся неотличимыми от равномерно распределенных и слабо отличаются друг от друга, заставляя модель работать как подбрасывание монеты.

Отличительной особенностью предлагаемого метода тестирования является то, что для классических статистических тестов выборки соседних раундов слабо отличимы друг от друга: на рисунке 4 представлен график зависимости пройденных тестов NIST (выполнялось 15 тестов на 10 ключах) от числа раундов. Из графика видно, что рассматриваемый алгоритм Simon как на 3, так и на 4 раунде проходит одинаковое число статистических тестов, тогда как модель нейронной сети в 92% случаев (рисунок 5) на контрольной выборке отличает последовательности при 3 раундах от 4.

Таким образом, можно сделать вывод о том, что решающие правила, построенные по предлагаемому методу и работающие по сценарию различения соседних раундов, для целого ряда шифров способны эффективнее отличать последовательности, чем группа классических статистических тестов.

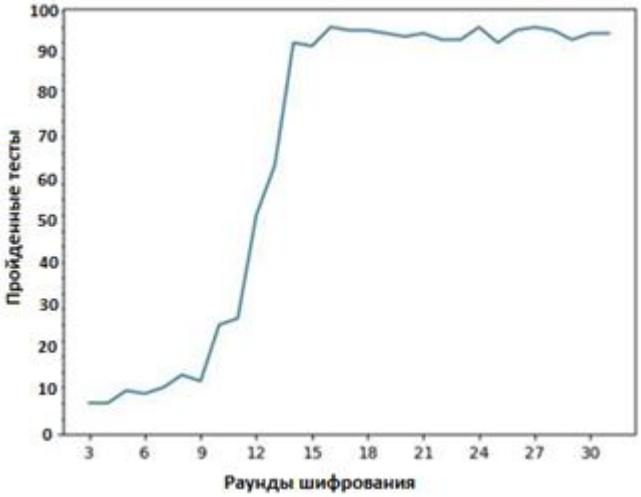

Рисунок 5 – график зависимости пройденных статистических тестов NIST от числа раудов на примере шифра Simon

В таблице 1 приведены значения процента верных решений нейронной сети при различении соседних раундов генераторов псевдослучайных последовательностей на основе блочных шифров. Жирным выделены значения раундов, на которых значение доли верных решений попадает в доверительный интервал $[M - \delta_\alpha, M + \delta_\alpha]$ из алгоритма 3 и соответствуют числу R_{min}.

Из алгоритма 1 следует, что если N = 500 и α= 0.01, то $\delta = 0.06$, таким образом, при попадании значения S'^r_n в интервал [0.44;0.56] будем считать значение $r = R_{min}$.

Алгоритм 4 описывает экспериментальное обоснование предлагаемого метода MLSA на примере «эталонного сценария».

Таблица 1 – значения правильных решений нейронной сети

В строках указаны исследуемые генераторы на основе блочных шифров. В столбцах указаны номера раундов, которые пыталась отличить друг от друга нейронная сеть по «эталонному сценарию». Жирным и подчеркнутым шрифтом выделены значения при которых достигается значение R_{min}.

Раунд / ***Шифр***	***3***	***4***	***5***	***6***	***7***	***8***	***9***	***10***	***11***	***12***	***13***	***14***	***15***	***16***	***17***
AES	**49**	46	49	46	51	53	49	51	50	-	-	-	-	-	-
CLEFIA	82	60	**51**	46	52	53	49	51	50	46	52	53	49	51	50
DESXL	**52**	48	51	46	53	50	-	-	-	-	-	-	-	-	-
HIGHT	94	87	68	73	67	64	58	**49**	51	50	53	49	46	53	50
IDEA	**54**	51	47	49	51	50	46	-	-	-	-	-	-	-	-
KLEIN	**51**	53	49	51	50	46	49	51	50	46	51	55	46	49	51
LED	100	**54**	50	50	46	53	50	46	49	51	50	46	49	51	49
mCrypton	92	60	**49**	51	53	49	51	50	49	-	-	-	-	-	-
MIBS	**53**	49	51	50	46	49	51	50	46	51	49	51	50	46	49
Noekeon	**52**	49	51	50	53	49	46	53	49	51	50	53	49	-	-
Piccolo	99	62	**59**	46	52	53	49	51	50	46	52	53	49	46	52
Present	100	100	87	72	60	**49**	46	51	53	49	51	50	53	49	51
Sea	100	100	96	93	74	60	58	**47**	51	50	46	51	55	46	50
Simon	100	100	100	100	100	99	98	97	91	82	70	59	**52**	53	52
Speck	100	99	99	89	72	59	**47**	51	50	46	51	55	46	50	47
Twine	100	94	97	95	77	62	**48**	46	52	53	49	51	50	46	52
XTEA	**49**	46	49	46	51	53	49	51	50	53	49	51	46	50	46
LBlock	100	99	95	91	74	58	**52**	53	50	46	49	51	53	48	53
RC5	100	72	**53**	46	49	51	50	46	51	55	-	-	-	-	-
RC6	79	66	**48**	47	51	50	53	49	46	53	49	51	50	50	53
MARS (FM)	54	49	51	50	53	49	-	-	-	-	-	-	-	-	-
MARS (FC)	46	52	53	49	51	50	46	52	53	49	51	50	47	52	-
MARS (BM)	68	**47**	51	50	46	51	-	-	-	-	-	-	-	-	-
CAST-128	100	89	**56**	**49**	51	50	53	49	46	53	49	51	49	51	-

Алгоритм 4. Схема экспериментального обоснования эффективности построенных решающих правил на примере «эталонного сценария»

Шаг 1: **Функция** ВычислитьОшибку (*Cipher*,*r*)
Шаг 2: Выбрать размер обучающей выборки *M*
Шаг 3: НейроннаяСеть^r(image) = ОбучитьНейроннуюСеть (*Cipher*, *r*, *M*)
Шаг 4: Выбрать количество контрольных выборок *N*
Шаг 5: Сгенерировать *N* контрольных выборок с помощью генератора *AES14* и получить $\tilde{x}^{rand} = (\tilde{x}_1^{rand}, \dots, \tilde{x}_N^{rand})$
Шаг 6: Сгенерировать *N* контрольных выборок с помощью генератора Cipher и получить $\tilde{x}^{r} = (\tilde{x}_1^{r}, \dots, \tilde{x}_N^{r})$
Шаг 7: Преобразовать сгенерированные множества выборок $\tilde{x}^{rand}$ **и** $\tilde{x}^{r}$ в изображения. Полученные множества обозначим соответственно $x^{rand} = (x_1^{rand}, \dots, x_M^{rand})$ и $x^{r} = (x_1^{r}, \dots, x_M^{r})$.
Шаг 8: Экспериментально определить ошибку первого рода $E_0 = \#\{x_i^{rand} |$ Нейронная сеть$^r(x_i^{rand} = 1\}$ Экспериментально определить ошибку второго рода $E_1 = \#\{x_i^{rand} |$ Нейронная сеть$^r(x_i^{rand} = 1\}$
Шаг 9: Вернуть E_0, E_1

По аналогичной схеме выполняется обоснование эффективности для сценария различения соседних раундов.

В **параграфе 3.3** приведено описание системы «УНИБЛОКС-2015», которая решает одну из важных проблем при построении решающих правил, объединяя алгоритмы, реализованные различными разработчиками под единым программным интерфейсом. Необходимость разработки такой информационной системы для построения решающих правил обусловлена отсутствием подобного универсального средства тестирования алгоритмов, которое бы имело в своем составе набор отлаженных блочных шифров, имеющих единый интерфейс. Наличие большого количества открытых исходных кодов и криптографических библиотек от разных разработчиков не решает эту проблему. На рисунке 6 представлена архитектура предлагаемой системы в виде диаграммы классов.

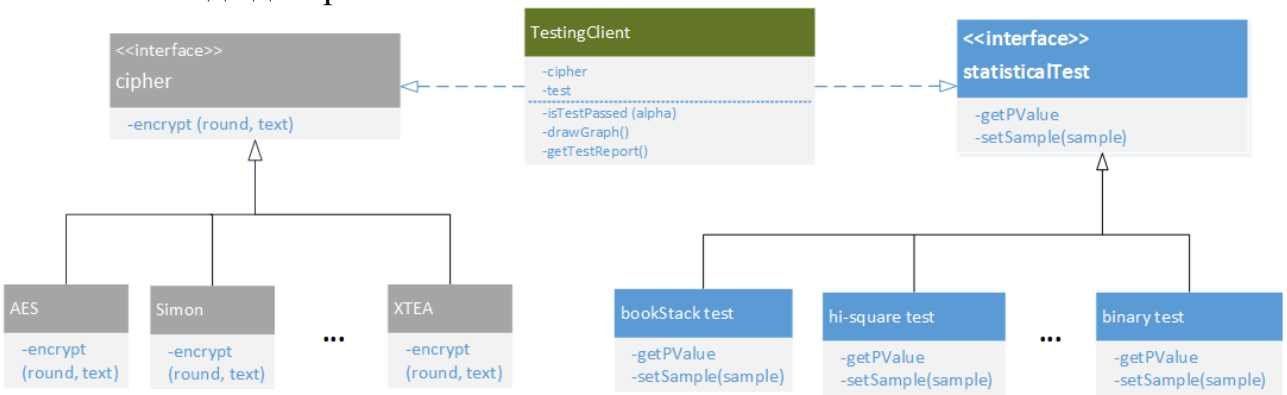

Рисунок 6 – диаграмма классов системы «УНИБЛОКС-2015».

Система позволяет осуществлять взаимодействие генераторов псевдослучайных чисел на основе итеративных блочных шифров и статистических тестов. В систему интегрировано более 25 шифров и 17 статистических тестов. С помощью разработанных на языке Python скриптов система координирует работу шифров и статистических тестов и позволяет формировать отчеты о тестировании, а также автоматизировать построение графиков зависимости статистических свойств от числа раундов для каждого протестированного генератора. Представлены основные подходы к реализации предлагаемой системы. Изложены требования к системе и реализация приемов объектно-ориентированного программирования, которые применялись при разработке. Описывается решение проблем разных длин ключей и блоков для различных программных реализаций итеративных блочных шифров.

В **параграфе 3.4** описан статистический тест «стопка книг» и результаты экспериментов. Эффективность теста заключается в возможности находить отклонения от случайности на большем числе раундов генератора чем некоторые другие известные статистические тесты.

В **параграфе 3.5** приводится описание теста «Адаптивный критерий хи-квадрат», позволяющего находить отклонения от случайности на выборках меньших, чем при использовании классического критерия хи-квадрат. Параграф содержит описание программной реализации теста, а также результаты проведенных экспериментов.

В **параграфе 3.6** приводится краткое описание 15 статистических тестов NIST и особенности реализации в разработанной информационной системе. Изложены некоторые особенности реализации функционала по автоматической генерации отчетов о тестировании и построении графиков зависимостей пройденных тестов от числа раундов.

Проверка тестами NIST считается пройденной, если значение пройденных тестов в соответствии с критерием хи-квадрат превышает вычисленное по формуле:

$$\chi 2 = \sum_{i=1}^{k} \frac{(v_i - np_i)^2}{np_i}$$

где v – успешно пройденные тестирования, а все $np_i = 150$ (15 тестов проводятся на 10 разных ключах). Экспериментально найдено, что при $v_i = 126$ значение $\chi 2 = 3.841$, что соответствует уровню значимости $\alpha = 0.05$. Из этого следует, что при 126 пройденных тестах вероятность корректного определения случайности выходной последовательности шифра равна 95%.

В таблице 2 приведены результаты тестирования рассмотренных в диссертационной работе алгоритмов с помощью всех предложенных методов и тестов.

Таблица 2 – результаты применения решающих правил, построенных согласно предлагаемому методу, к анализу генераторов псевдослучайных чисел на основе итеративных блочных шифров (жирным выделены шифры, для которых новые решающие правила позволяют достичь лучших результатов по сравнению с ранее опубликованными работами: либо увеличить R_{min}, либо уменьшить размер выборки)

Шифр – название шифра, на основе которого создан генератор. *R* – полное число раундов шифра. R_{min} *(NIST)* – минимальное число раундов, определенное тестами NIST (лучший из всех тестов по результатам экспериментов). R_{min} *BS* – минимальное число раундов определенное тестом «стопка книг». R_{min} $\chi 2$– минимальное число раундов определенное тестом «адаптивный критерий $\chi 2$», $R_{min(other)}$ – минимальное значение опубликованное другими авторами, R_{min} *MLSA* – минимальное число раундов определенное методом MLSA.

Шифр	***R***	R_{min} ***(NIST)*** 2^{27}	R_{min} ***BS*** (2^{24})	R_{min} $\chi 2$ (2^{24})	R_{min}***(other)***	R_{min} ***MLSA*** $(2^{21.9})$
CAST-128[2]	***16***	***4***	***3***	***3***	***3***(2^{31})	***5***
IDEA[2]	***8.5***	***2***	***2***	***2***	***2***(2^{108})	***2***
LBlock[3]	***32***	***8***	***8***	***7***	***8***(2^{26})	***9***
Simon[4]	***32-72***	***14***	***12***	***12***	***12***(2^{36})	***15***
Speck[4]	***22-34***	***8***	***6***	***6***	***6***(2^{31})	***9***
RC5[5]	***12***	***5***	***5***	***5***	***5***(2^{28})	***5***
RC6[2]	***20***	***5***	***5***	***5***	***5***(2^{29})	***5***
AES	10-14	3	4	4	-	3
CLEFIA	18-26	6	6	6	-	5
DESXL	8	6	2	4	-	3
HIGHT	32	9	10	10	-	10
KATAN64	254	32	30	31	-	31
KLEIN	12-20	3	4	4	-	3
KTANTAN64	254	32	30	31	-	31
LED	32-48	4	4	4	-	4
Mcrypton	12	6	6	3	-	5
MIBS	32	3	2	1	-	2

Шифр	***R***	R_{min} ***(NIST)*** 2^{27}	R_{min} ***BS*** (2^{24})	R_{min} $\chi 2$ (2^{24})	R_{min}***(other)***	R_{min} ***MLSA*** $(2^{21.9})$
NOEKEON	16	3	2	2	-	2
Piccolo	25-31	6	6	5	-	5
PRESENT	31	10	9	8	-	8
SEA	51	10	10	10	-	10
Twine	36	9	9	9	-	9
XTEA	32	3	3	3	-	3

Таким образом, предлагаемый метод построения решающих правил показывает результаты, сопоставимые с известными статистическими тестами, используя при этом меньшую длину выборки (во всех экспериментах методом MLSA использована выборка $2^{21.9}$ бит), а для ряда шифров получены результаты, превосходящие ранее полученные (в таблице выделены жирным и серым цветом).

ЗАКЛЮЧЕНИЕ

В соответствии с поставленной целью и задачами исследования были получены следующие результаты.

1. Разработан 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. Исследуемые псевдослучайные последовательности преобразуются в их графические эквиваленты, которые в свою очередь используются для обучения сверточной нейронной сети и последующей классификации.

2. Предложен новый универсальный метод построения решающих правил на основе сверточных нейронных сетей для обнаружения закономерностей и отклонений от случайности в псевдослучайных последовательностях, полученных с помощью генераторов на основе итеративных блочных шифров. Универсальность нового метода состоит в том, что он позволяет создавать решающие правила для генераторов, базирующихся на любых итеративных блочных шифрах. Достоинством таких решающих правил, в сравнении со многими правилами на основе универсальных статистических критериев, является более тонкая настройка правил под конкретный генератор. В то же время, они не требуют анализа внутренней структуры генератор, в отличие от аналитических подходов.

---

[2] **Лысяк А.С., Рябко Б.Я., Фионов А.Н.** Анализ эффективности градиентной статистической атаки на блоковые шифры RC6, MARS, CAST-128, IDEA, Blowfish в системах защиты информации // Вестник СибГУТИ. 2013. №1. С.85-109

[3] **Пестунов А.И.** Предварительная оценка минимального числа раундов легковесных шифров для обеспечения их удовлетворительных статистических свойств // ПДМ. Приложение. 2015. №8. С. 66-68

[4] **Сосков А.С., Рябко Б.Я.** Применение атаки различения на легковесные блочные шифры, основанные на ARX-операциях // Вычислительные технологии. 2019. №3. С.106-116

[5] **Рябко Б.Я, Монарёв В.А**. Новый тип атак на блоковые шифры // Проблемы передачи информации. 2005. т.14, вып. 4. С.97-107

3. Экспериментально показано, что решающие правила, построенные с использованием предложенного в диссертации метода для ряда генераторов псевдослучайных последовательностей, позволяют обнаруживать закономерности и отклонения от случайности при меньших размерах выборок или при большем числе раундов, чем при использовании решающих правил на базе универсальных статистических тестов.

4. Разработан программно-аппаратный комплекс для статистического анализа генераторов псевдослучайных чисел на основе итеративных блочных шифров, включающий более 50 генераторов, а также решающие правила на основе статистических тестов и сверточных нейронных сетей. Программный комплекс содержит инструменты, обеспечивающие эффективную интеграцию программных реализаций генераторов псевдослучайных последовательностей и решающих правил для их анализа с последующим формированием формированием отчетов (в том числе в графическом виде). Программный комплекс спроектирован таким образом, чтобы обеспечить его расширяемость с целью дальнейшей интеграции новых генераторов с итеративной структурой и решающих правил для их анализа.

ОПУБЛИКОВАННЫЕ РАБОТЫ АВТОРА ПО ТЕМЕ ДИССЕРТАЦИИ

Издания из Перечня ВАК ведущих рецензируемых научных изданий для опубликования основных научных результатов диссертаций:

1. Пестунов А.И. О некоторых направлениях научных исследований в области криптоанализа симметричных алгоритмов / А.И. Пестунов, **А.А. Перов**, Т.М. Пестунова // Вестник НГУЭУ. 2016. №3. С. 290-298.

2. **Перов А.А.** Статистическое тестирование современных итеративных блочных шифров с помощью программной библиотеки «УНИБЛОКС-2015» / **А.А. Перов**, А.И. Пестунов // Инновации в жизнь. 2016. №2 (17). С. 89-97.

3. **Перов А.А.** Применение статистических тестов NIST для анализа выходных последовательностей блочных шифров / **А.А. Перов** // Научный вестник НГТУ. 2019. №3 (76). С. 87-96.

4. **Перов А.А.** О возможности применения сверточных нейронных сетей к построению универсальных атак на итеративные блочные шифры / **А.А. Перов,** А.И. Пестунов // Прикладная дискретная математика. 2020. №3 (49). С. 46-57. (индексируется в **Scopus** и **Web of Science**)

Сборники научных трудов, индексируемые в Scopus и/или Web of Science:

5. **Perov A.** Using Machine Learning Technologies for Carrying out Statistical Analysis of Block Ciphers / A. Perov // Proceedings International Multi-Conference on Engineering, Computer and Information Sciences (SIBIRCON). 2019. P. 851-854.

Другие издания:

6. Пестунов А.И. Программная библиотека для статистического анализа итеративных блочных шифров / А.И. Пестунов, **А.А. Перов** // Информационное противодействие угрозам терроризма. 2015. №24. С. 197-202.

7. **Перов А.А.** Программная библиотека для статистического анализа итеративных блочных шифров и исследование легковесных алгоритмов с ее помощью / **А.А. Перов** // Наука. Технологии. Инновации. : сб. науч. тр. – Новосибирск, 2015. Ч. 2. С. 107-109

8. Пестунов А.И. Анализ статистических свойств легковесных блочных шифров с помощью специализированной программной библиотеки / А.И. Пестунов, **А.А. Перов** // Материалы XVI Всероссийской конференции молодых ученых по математическому моделированию, Красноярск, 28-30 октября 2015 г. Новосибирск: ИВТ СО РАН, 2015. С. 98

9. **Перов А.А.** Статистический анализ выходных последовательностей малоресурсных блочных алгоритмов шифрования / **А.А. Перов** // Материалы 54-й международной научной студенческой конференции МНСК-2016, Новосибирск, 16-20 апреля 2016 г. Новосибирск: ИПЦ НГУ, 2016. С. 81.

10. **Перов А.А.** Концепция информационно-аналитической системы для статистического анализа симметричных криптографических алгоритмов / **А.А. Перов** // Наука. Технологии. Инновации. : сб. науч. тр. – Новосибирск, 2016. – Ч. 1. – С. 44-45.

11. **Перов А.А.** Архитектура информационно-аналитической системы для анализа статистических свойств симметричных криптоалгоритмов / **А.А. Перов** // Материалы 55-й международной научной студенческой конференции МНСК-2017, Новосибирск, 17-20 апреля 2017 г. – Новосибирск: ИПЦ НГУ, 2017 – С. 43.

12. **Перов А.А.** Об использовании технологий машинного обучения для проверки статистических свойств симметричных криптографических алгоритмов / **А.А. Перов** // Прикладная дискретная математика. Приложение. 2019. №12. С. 232-235.

13. **Перов А.А.** Анализ возможностей применения технологий искусственного интеллекта к задачам статистического анализа блочных шифров / **А.А. Перов** // Тезисы XX Всероссийской конференции молодых ученых по математическому моделированию и информационным технологиями, Новосибирск, 28 октября - 01 ноября 2019 г. Новосибирск: ИВТ СО РАН, 2019. С. 72-73

14. **Перов А.А.** Алгоритм статистического анализа блочных шифров с использованием технологий машинного обучения / **А.А. Перов** // сб. тр. Международной научно-практической конференции «Распределенные

информационно-вычислительные ресурсы» DICR-2019, Новосибирск, 03-06 декабря 2019 г. – Новосибирск: ИВТ СО РАН, 2019. С. 153-156.

15. Пестунов А.И. Информационная система для автоматизации процесса создания и проверки письменных заданий по дисциплине «Криптографические методы защиты информации» / Пестунов А.И., **А.А. Перов** // ст. в сб. труд. конф. «Актуальные проблемы научной мысли: проблемы и перспективы», Новосибирск, 19-21 марта 2018 г. – Новосибирск: Новосибирский государственный университет экономики и управления «НИНХ», 2018. С. 234-238.

16. **Перов А.А.** Построение различителей для итеративных блочных шифров на основе нейронных сетей/ **А.А. Перов,** А.И. Пестунов // Прикладная дискретная математика. Приложение. 2020. №13. С. 54-56.

Свидетельства о государственной регистрации программы для ЭВМ:

17. Пестунов А.И. Унифицированная программная библиотека для статистического анализа итеративных блочных шифров «Униблокс-2015» / А.И. Пестунов, **А.А. Перов**, Т.М. Пестунова // М.: Роспатент. Свидетельство о государственной регистрации программы для ЭВМ №2015662092, от 17.11.2015.

18. **Перов А.А.** Программный комплекс для статистического анализа и оценки стойкости итеративных блочных шифров при помощи сверточных нейронных сетей «Нейроблокс-2020» / **Перов А.А.**, Пестунов А.И. // М.: Роспатент. Свидетельство о государственной регистрации программы для ЭВМ №2020618202, от 07.08.2020.