тели, которая при произведении порядка 2^{664} требует 10^{23} операции; и функция определения модульной экспоненты по фиксированному основанию, для решение которой необходимо определить значение дискретного логарифма, что не имеет на данный момент эффективного алгоритма (при этом не существует доказательств, что такого алгоритма нет) [2]. Обе из описанных ранее однонаправленных функций используются в алгоритме RSA, что во многом поддерживает его криптостойкость.

Если описывать алгоритм RSA обобщённо, то существует несколько основополагающих логических точек: во-первых, это выбор некоторого множества исходных данных, а именно двух больших простых чисел (вполне логично, что для реализации криптосистемы необходимы алгоритмы генерации больших чисел и тестов на простоту); во-вторых, это нахождение произведения двух больших простых чисел; в-третьих, поиск двух множителей, произведение которых является мультипликативным обратным единице по модулю функции Эйлера для ранее найденного произведения; в-четвёртых, непосредственно шифрование, основанное на нахождение модульной экспоненты.

В ходе исследования было создано программное средство и выполнен сопутствующий этому процессу алгоритмический анализ с точки зрения программирования.

Разработанный шифратор обладает функционалом, необходимым для осуществления обратимого преобразования некоторого текста, а именно: генерация открытого и секретного ключа, причём открытый ключ автоматически заносится в соответствующие поля для шифрования информации; непосредственное шифрование и дешифрование некоторой текстовой информации, а также удаление пробелов открытого текста, для уменьшения объема шифртекста. Для шифрования некоторого текста, необходимо выполнить генерацию ключа или вставить ранее сгенерированный ключ, после чего нажать на кнопку «Encrypt», дешифрование выполняется благодаря использованию секретного ключа и нажатию на кнопку «Decrypt». Шифрование возможно для всех символов как латинского, так и кириллического алфавитов, цифр и всех необходимых пунктуационных и арифметических знаков, что описывает достаточное множество символов для шифрования и дешифрования большинства как русских, так и английских текстов, с возможностью считывания информации из текстовых файлов и занесения в файл.

Заключение. Результатом разработки является программное средство, позволяющее генерировать секретный и открытый ключи шифра, выполняющее обратимое преобразование текста с помощью алгоритма шифрования RSA, в основе которого используются числа 9-того порядка, при избыточности шифртекста 1/15. В ходе исследования были изучены и программно реализованы алгоритмы Евклида, Ферма, Миллера-Рабина для больших чисел. Разработанный шифратор может быть использован для проведения обратимого преобразования небольших текстов с целью создания ЭЦП, шифрования и дешифрования текстов с учётом избыточности шифртекста, а также для изучения принципа асимметричных криптосистем в учреждениях образования в качестве учебного материала.

1. Алфёров, А.П. Основы криптографии [Текст] / А.П. Алфёров, А.Ю. Зубов, А.С. Кузьмин, А.В. Черемушкин. – М.: «Гелиос АРВ», 2002. – 480 с.
2. Романец, Ю.В. Защита информации в компьютерных системах и сетях [Текст] / Ю.В. Романец, П.А. Тимофеев, В.Ф. Шаньгин. – М.: «Радио и связь», 2001. – 376 с.

ВОЗМОЖНОСТЬ ПОСТРОЕНИЯ ВЕБ-ПРИЛОЖЕНИЙ НА ОСНОВЕ ГЕНЕРАТИВНОЙ СОСТЯЗАТЕЛЬНОЙ СЕТИ

Рыльков А.В.,
студент ВГУ имени П.М. Машерова, г. Витебск, Республика Беларусь
Научный руководитель – ***Маркова Л.В.,*** *канд. физ.-мат. наук, доцент*

Нейросети умеют распознавать изображения и не только, но генерация самостоятельных решений для них практически не возможна. Однако, относительно недавно, данная проблема была решена исследователями из университета Монреаля. Они разработали генеративную состязательную сеть (далее GAN) [1]. Анализ возможностей сети GAN и области ее применения является актуальной задачей.

Цель исследования – анализ работы GAN, примеров её использования и целесообразности её применения для разработки веб приложений.

Материал и методы. В качестве материалов анализировались статьи о создании, принципах работы и примерах использования генеративной состязательной сети, а так же, непосредственно, веб-приложения построенные на её основе. При проведении исследований применялись методы анализа, синтеза, обобщения и классификации.

Результаты и их обсуждение. Генеративная состязательная сеть представляет собой мощный тип нейронной сети, используемой для бесконтрольного машинного обучения. Она состоит из двух конкурирующих моделей, генератора и дискриминатора, которые противостоят друг другу.

Эта сеть отлично подходит для манипулирования изображениями и их генерации, но также может быть использована для таких задач, как генерация последовательности нот и, соответственно, полноценной мелодии, а также, например, для прогнозирования поведения частиц, моделирования распределения темной материи.

GAN довольно новая технология – она была впервые представлена в 2014 году [1]. Её разработали для решения некоторых проблем с аналогичными нейронными сетями, включая машину Больцмана и автоэнкодеры с целью оптимизации потребляемых ресурсов, в первую очередь уменьшения объема используемой памяти.

Для того, чтобы понять как работает GAN, можно привести следующую аналогию. Существует картина и мастер-фальсификатор, который хочет создать дубликат картины. Для этого фальсификатор изучает технологию создания картины оригинальным художником. Одновременно "следователь" пытается поймать фальсификатора, используя "догадку" о правилах, которые изучает фальсификатор.

Чтобы отобразить это на архитектуру GAN, предполагаем, что фальсификатор – это генераторная сеть, которая изучает распределение классов, в то время как следователь – это дискриминаторная сеть, которая изучает границы между этими классами.

Генеративные состязательные сети могут использоваться для целого ряда различных применений.

Одним из лучших примеров является проект Google Brain. Еще в 2016 году исследователи использовали GAN для разработки метода шифрования,[2].

В этом проекте использовались 3 нейронные сети – Алиса, Боб и Ева. Задача Алисы состояла в том, чтобы послать Бобу зашифрованное сообщение. Боб должен был расшифровать это сообщение, а Ева – перехватить его.

Сообщения Алисы были легко перехвачены Евой. Тем не менее, благодаря состязательной работе Евы, Алиса начала разрабатывать свою собственную стратегию шифрования – потребовалось 15 000 запусков для Алисы, чтобы успешно зашифровать сообщение, которое могло быть расшифровано Бобом, чтобы Ева не могла его перехватить.

GAN также используется для создания новых лекарств. Нейронные сети могут обучаться на существующих препаратах и предлагать новые синтетические химические структуры, улучшающие уже существующие препараты.

GAN предлагает некоторые действительно захватывающие возможности в области искусственного интеллекта,[3]. Есть два ключевых преимущества этой системы: GAN решает проблему генерации данных, когда их недостаточно изначально и они не требуют человеческого надзора.

Такой подход имеет решающее значение как с точки зрения эффективности запуска моделей, так и с точки зрения реальных данных, которые мы хотим использовать. Эти данные могут быть низкого качества или иметь проблемы конфиденциальности, как, например, многие медицинские данные.

Заключение. Таким образом, в результате данного исследования, можно сделать вывод о том, что использование генеративной состязательной сети для решения задач, требующих самостоятельной генерации данных без непосредственного человеческого надзора, является крайне практичным и актуальным решением. Так как GAN позволяет генерировать данные похожие на сущности из реального мира в области изображений, музыки, речи, прозы и так далее. Что касается использования GAN при разработке веб-приложений, тут многое

зависит от направленности приложения. Например, при создании приложения, цель которого – генерация фотографий, приближенных к реальным изображениям, использование GAN является крайне целесообразным. И, наоборот, в случае, когда в приложении нет необходимости генерации данных, GAN практически не используется.

1. Neurohive [Электронный ресурс] Режим доступа: https://neurohive.io/ru/osnovy-data-science/gan-rukovodstvo-dlja-novichkov/
2. РОСКОМСВОБОДА [Электронный ресурс] Режим доступа: https://roskomsvoboda.org/22487/
3. Evergreen [Электронный ресурс] Режим доступа: https://evergreens.com.ua/ru/articles/gan.html

ПРИМЕНЕНИЕ ТЕОРИИ НЕСТАЦИОНАРНОЙ ТЕПЛОПРОВОДНОСТИ ДЛЯ ПРОГНОЗИРОВАНИЯ ПРОДОЛЖИТЕЛЬНОСТИ ТЕПЛОВЫХ ОПЕРАЦИЙ В ПРОИЗВОДСТВЕ ПИЩЕВОЙ ПРОДУКЦИИ

Смагина М.Н.[1], Терешкова Е.Р.[2],
[1]аспирант Могилевского государственного университета продовольствия
[2]студентка 3-го курса Могилевского государственного университета продовольствия,
г. Могилев, Республика Беларусь
Научный руководитель – ***Смоляк А.А.,*** *канд. техн. наук, доцент*

Одной из проблем при подготовке студентов в вузах является умение применять теоретические знания фундаментальных наук в реализации отдельных прикладных задач. Так, студенты технологических специальностей изучают теорию тепломассообмена, но не понимают, как применять ее в производственной деятельности. Между тем, например запекание мясных полуфабрикатов является не только технологическим процессом, но в гораздо большей степени теплофизическим процессом, характер протекания которого определяется прежде всего законами теплообмена. Важнейшим для технологов, но трудно поддающемуся расчету показателем эффективности тепловой обработки пищевой продукции, является продолжительность процесса. Предлагаемые методики аналитического определения продолжительности тепловых операций сложны и нуждаются в корректировке. Отсутствие комплексного подхода по изучению факторов интенсификации тепловой обработки и невозможность прогнозирования ее продолжительности не позволяют рационально осуществлять производственный процесс. Решение указанной задачи позволит повысить эффективность тепловой обработки, приведет к повышению потребительских характеристик готовой продукции и повышению эффективности оперативного планирования производства.

Материалы и методы. Рекомендуется два способа определения длительности процесса: по темпу нагрева и по интенсивности теплоподвода.

Дифференциальное уравнение теплопроводности при отсутствии внутренних источников теплоты имеет вид [1, 2]:

$$\frac{\partial t}{\partial \tau} = a[\frac{\partial^2 t}{\partial x^2} + \frac{\partial^2 t}{\partial y^2} + \frac{\partial^2 t}{\partial z^2}], \quad (1)$$

где t – температура, К; τ – время, с;

Уравнение (1) имеет бесчисленное множество решений. Для выделения единственности их решения необходимо задать состояние системы в начале процесса (начальные условия) и характер взаимодействия между рассматриваемой системой и окружающей средой (граничные условия).

Уравнение теплопроводности в безразмерной форме для одномерной задачи имеет следующий вид [1, 2]:

$$\frac{\partial \Theta}{\partial Fo} = \frac{\partial^2 \Theta}{\partial \xi^2}, \quad (2)$$

где Θ – безразмерная температура тела; ξ – безразмерная координата; *Fo* – число Фурье.