МИНОБРНАУКИ РОССИИ
Федеральное государственное бюджетное образовательное учреждение
высшего образования
«САРАТОВСКИЙ НАЦИОНАЛЬНЫЙ ИССЛЕДОВАТЕЛЬСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ ИМЕНИ Н.Г. ЧЕРНЫШЕВСКОГО»

Кафедра теоретических основ компьютерной безопасности и криптографии

Классификация образов нейронными сетями

АВТОРЕФЕРАТ
дипломной работы

студента 6 курса 631 группы
специальности 10.05.01 Компьютерная безопасность
факультета компьютерных наук и информационных технологий
Романова Игоря Константиновича

Научный руководитель
доцент
_____ И. И. Слеповичев
22.01.2022 г.

Заведующий кафедрой
д. ф.-м. н., доцент
_____ М. Б. Абросимов
22.01.2022 г.

Саратов 2022

ВВЕДЕНИЕ

В настоящее время информационные технологии это неотъемлемая часть жизни человека в целом. Одним из аспектов современных технологий в области обработки и исследованиях информации является машинное обучение. Особое внимание уделяется такому аспекту машинного обучения, как искусственные нейронные сети [1].

Большие объемы данных перестали быть редкостью, и нейронные сети теперь имеют возможность обучаться комплексно и эффективно. Также применяются новые архитектурные решения, большим успехом в области классификации изображений пользуются сверточные нейронные сети [5]. Еще одним усовершенствованием в разработке сетей является подход переноса обучения, позволяющий экономить ресурсы и получать высокоточные результаты [9]. Разработки нейронных сетей в современном мире давно вышли из рамок только научного исследования и уже повсеместно внедряются в коммерческие проекты.

Математическое обоснование работоспособности нейронных сетей в качестве аппроксиматоров сложных функций было исследовано еще в прошлом веке. Также опытным путем выявлена эффективность именно сверточных сетей в задачах, связанных с изображениями. Современные специалисты отмечают успешное применение подхода переноса обучения в проблеме классификации.

Цель данной дипломной работы – построение нескольких моделей нейронных сетей, исследование эффективности каждой из них, анализ полученных результатов.

Для достижения поставленной цели необходимо решить следующие задачи:

- изучить основы построения нейронных сетей;
- рассмотреть алгоритмы обучения сетей;
- выбрать задачу классификации и подходящие данные для неё;
- выбрать несколько подходов к решению задачи классификации;

- программно реализовать выбранные подходы к решению задачи классификации;
- собрать полученные экспериментальные данные;
- проанализировать эффективность каждого подхода.

Дипломная работа состоит из введения, 2 разделов, заключения, списка использованных источников и 3 приложений. Общий объем работы – 42 страниц, из них 27 страниц – основное содержание, включая 11 рисунков, список использованных источников из 16 наименований.

КРАТКОЕ СОДЕРЖАНИЕ

Первый раздел содержит необходимые теоретические сведения касающиеся искусственных нейронных сетей. Здесь приводятся основные определения и обозначения, используемые далее в дипломной работе.

Первый раздел включает в себя такие аспекты рассматриваемой темы как:

- архитектура искусственной нейронной сети;
- обучение искусственной нейронной сети;
- алгоритмы обучения;
- вероятностные подходы к обучению.

Второй раздел «Задача классификации» вводит четкую постановку задачи, реализованной в практической части работы. Вводятся такие понятия как признаки, карты признаков, свертка, подвыборка, нормализция и перенос обучения.

Вначале общие сведения о классификации изображений. Допустим, у нас есть какое-то множество объектов U, каждый объект обладает набором признаков $X(U)$, также имеется множество классов Y, на которые мы и хотим поделить наше множество объектов.

В нашем случае, U - это изображения, $X(U)$ - это какие-либо признаки изображения, например, пиксели, а классами изображения Y могут быть такие классы, как изображение человека, дома, машины и так далее.

В конечном итоге, задачей машинного обучения является построение функции $F: X \to Y$, которая будет отображать объекты в классы, то есть говорить о принадлежности объекта конкретному классу. Будем называть данную функцию решающей [4].

Нам понадобиться обучающая выборка D, которая будет выглядеть следующим образом $D = \{ x_i; y_i \}$. Наш набор содержит пары $(x_i; y_i)$, где для каждого изображения x_i нам уже известен его класс y_i.

На основе выборки D построим решающую функцию, которая мало ошибается на объектах обучающего набора. Предполагаем, что в будущем

построенная функция будет достаточно хорошо классифицировать объекты не из D.

Как было сказано ранее, для обучения нам нужно будет определить функцию ошибки, формально $E(D,F) = \sum(F(x_i) \neq y_i)$. Учитываем неверные ответы ИНС и обрабатываем их.

Наша задача - это минимизация функции ошибки. Добиваемся мы этого путем изменения весов входов нейронов. Возможно, тем же самым обратным распространением ошибки, находя производные функции ошибки и двигаясь в обратном направлении, тем самым, стремясь к минимуму функции.

На практике, для решения задачи классификации отлично показали себя сверточные нейронные сети. Принцип их действия заключается в том, что нейроны взаимодействуют не отдельно с каждым пикселем изображения, а сразу с какой-то окрестностью пикселей. Таким образом, существенно уменьшается количество весов, ускоряется обучение и распознавание, уменьшаются шансы переобучить сеть на входном множестве.

Подробнее, у каждого пикселя есть своя окрестность, допустим, восемь его соседей. Тогда каждый нейрон будет иметь девять весов, по одному на каждого соседа и плюс еще на сам пиксель, на котором находимся. Поэлементно перемножаем каждый элемент окрестности на ядро свертки, так называется набор весов, складываем и получаем выход на новый слой. Также, используется не один канал преобразования, а несколько, для выявления разных признаков [6]. Количество весов на одном слое сети будет равно произведению количеству весов в ядре на количество каналов преобразования, формула (4).

$$N_w = Ker * Chanels, \quad (4)$$

где N_w – общее количество весов на одном слое;

Ker – количество весов в одном ядре;

$Chanels$ – количество каналов преобразования.

Действие такой сети можно описать как переход от простых признаков на более сложные с каждым слоем свертки. Сеть не имеет обратных связей, обучается, как правило, методом обратного распространения ошибки.

Для уменьшения размерности изображения используется операция подвыборки (рис. 7).

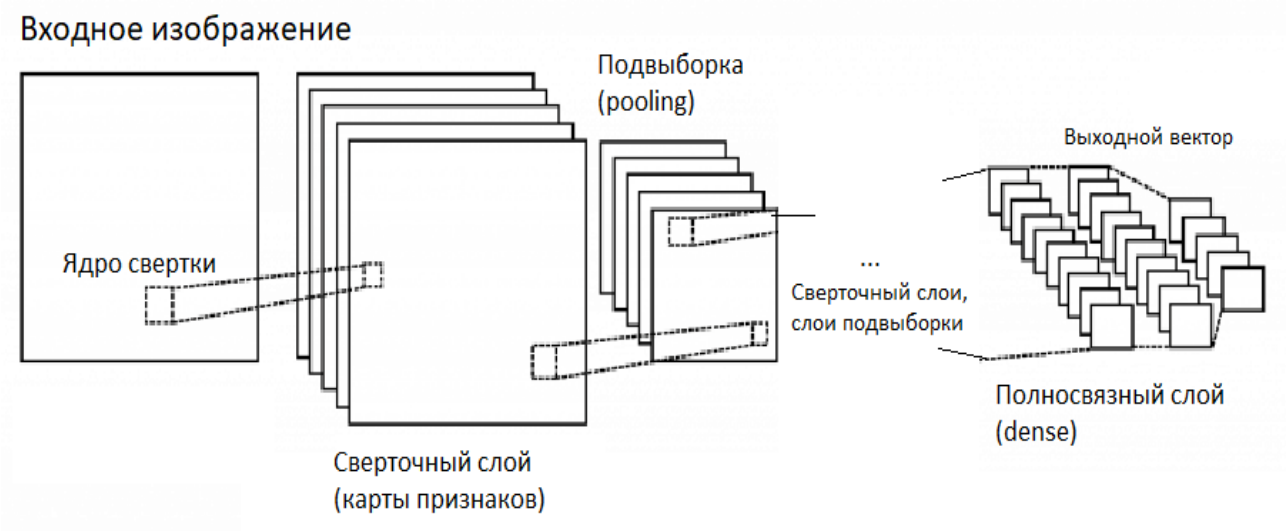

Рисунок 7 – Свертка изображения, 5 ядер свертки, 25 весов в каждом [5]

В нашей работе используются три входных канала изначально, так как входными данными являются изображения в формате jpg с палитрой цветов RGB. На каждый цвет свой слой изображения. Отметим, что перед обработкой изображения необходимо нормализовать все цвета, то есть все значения входного слоя, формула (5).

$$f(p, min, \max) = \frac{p - min}{\max - min}, \quad (5)$$

где f – функция нормализации;

p – значение конкретного цвета пикселя (от 0 до 255);

$min, \max$ – минимальное и максимальное значение пикселя.

Операция свертки представляет собой поочередный проход ядром свертки по всем пикселям конкретного слоя. Текущий пиксель и его окрестность умножаются на соответствующие веса ядра свертки, результаты суммируются, и на выходе получается новое значение, новой карты признаков.

Для хороших результатов распознавания, даже с использованием сверточных нейронных сетей, требуется большое количество специально подобранных примеров обучения. Также к сложностям, возникающим в процессе решения новой задачи классификации, можно отнести трудоемкий процесс настройки многочисленных параметров сети и необходимость в больших вычислительных мощностях для обработки изображений и обучения.

Эти задачи можно упростить использованием метода Transfer Learning. Метод заключается в том, что вместо предварительного отбора большой обучающей выборки и долгого процесса обучения, в модель добавляется заранее обученная сеть в качестве слоя. Сеть выбирается опытным путем, основным требованием к такой сети является то, что она должна быть заранее обучена на очень большом количестве обучающих примеров [10].

Такой подход позволяет уменьшить затраты на создание новой модели и достигает отличных результатов, превосходя в точности многие популярные сети (рис. 8). На рисунке диаграммы обозначают точность вычисления трех сетей (BiT, SOTA, ILSVRC-2012 [9]) на различных наборах данных. Графики показывают изменение точности распознавания в зависимости от количества входных примеров на класс, от 1 до 100.

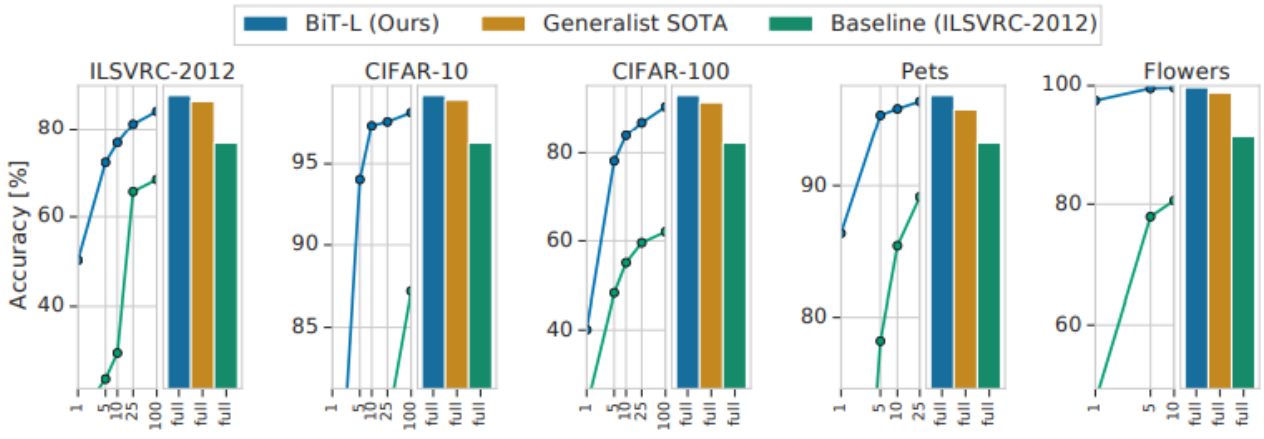

Рисунок 8 – Результаты применения модели Big Transfer на различных наборах данных [9]

Конечно, такой подход осуществим не во всех классах задач машинного обучения, но в области распознавания изображений с небольшим количеством классов изображений, Big Transfer (BiT) показывает наилучшие результаты.

Результаты обучения первой сверточной сети, слой нормализации, 3 сверточных слоя, 2 полносвязных слоя, на рисунке 9.

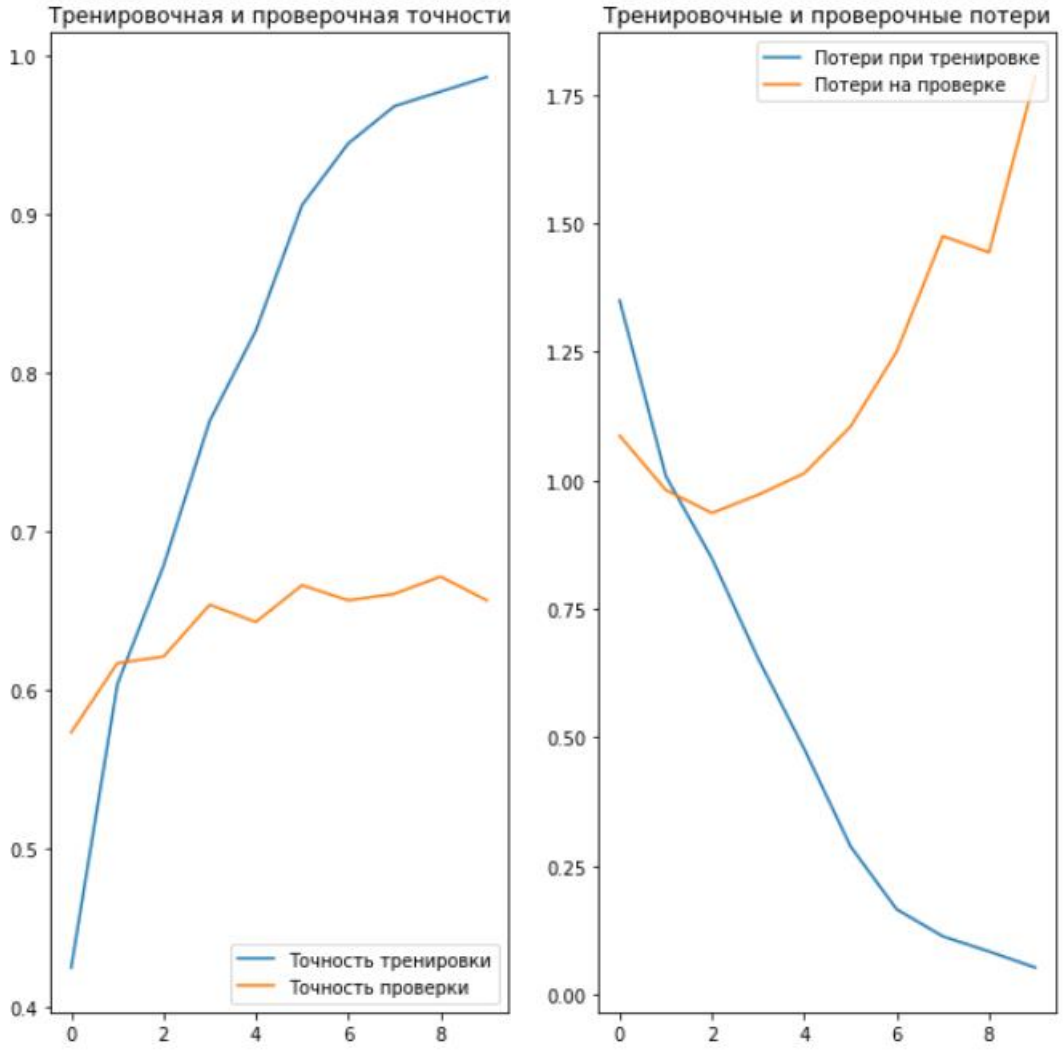

Рисунок 9 – Результаты обучения

Результаты обучения второй сверточной сети, 3 сверточных слоя, слой исключений, слой дополнения входных данных, слой нормализации и 2 полносвязных слоя, на рисунке 10.

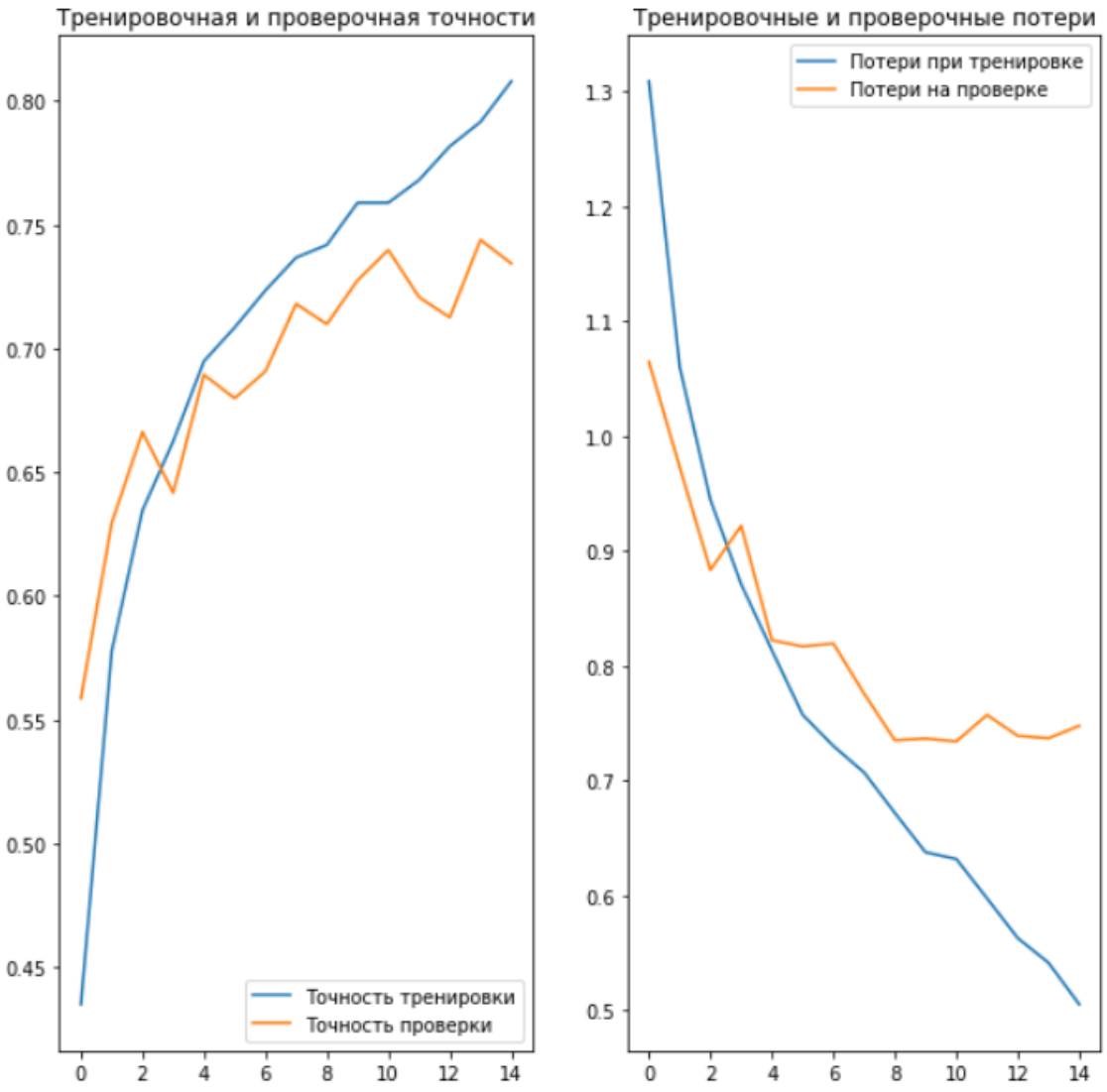

Рисунок 10 – Результаты обучения измененной CNN

Результаты обучения модели BiT, имплементирована заранее обученная на CIFAR-10 сверточная сеть ResNet50, на рисунке 11.

По горизонтали эпохи, по вертикали совмещено точность и потери. Результаты показывают, что точность на тренировочном и контрольном множествах превышают 95%. Значения потерь на тренировочном и контрольном множествах приблизительно совпадают. Это говорит нам о том, что достигнуты отличные результаты точности распознавания, переобучения не наблюдается.

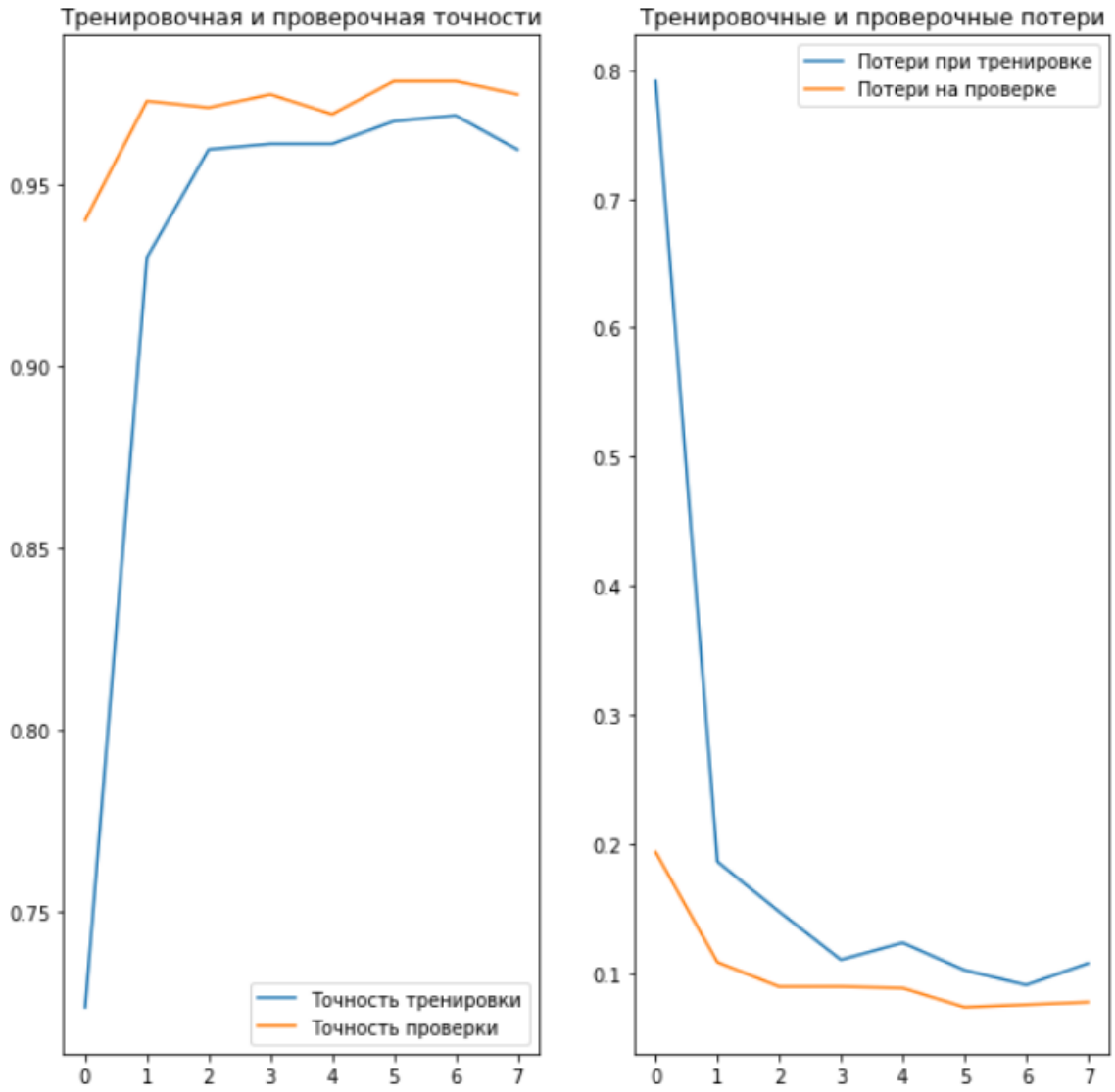

Рисунок 11 – Результаты обучения модели BiT

Можно заметить, что точность на проверочном множестве выше, чем на тренировочном множестве. Данное явление имеет несколько объяснений. Во-первых, даже в первых двух моделях замечалось нечто подобное на первых эпохах обучения, это связано с наличием слоя dropout. Так как на тренировочном множестве с некоторой вероятностью обнуляются правильные ответы. Во-вторых, проверочное множество не подвержено случайным изменениям, в отличие от тренировочного множества изображений, в котором объекты случайным образом поворачиваются, отражаются и масштабируются перед проходом через сеть.

ЗАКЛЮЧЕНИЕ

В дипломной работе было рассмотрено несколько подходов к решению задачи классификации. Выбранные для более детального исследования архитектуры были реализованы в программном виде. Три модели были обучены на одном и том же наборе входных данных. Полученные результаты дают представление об эффективности некоторых подходов в решении задачи классификации изображений.

Также в ходе работы были исследованы универсальные надстройки в искусственных нейронных сетях. Особую роль в работе занимают алгоритмы и методы несущие случайный характер. Подобные случайные модули или решения не являются в явном виде хаосом, а включаются в свою очередь в нужные места программы или в необходимые этапы разработки. Случайные аспекты модели выполняют конкретные действия, преследуют поставленные перед ними задачи по улучшению качества распознавания.

В первом разделе также рассмотрены исторические сводки по нейронным сетям и некоторые общие положения в мире нейронных сетей и глубокого обучения.

Во втором разделе дипломной работы описаны практические детали, такие как количество параметров, изменяющихся в процессе обучения. Также описаны математические формулы для вычисления функции потерь, для вычисления слоя нормализации. Подробный анализ полученных результатов в данном разделе работы может указать на плюсы и минусы каждого из подходов решения задачи классификации.

Использованные модели дают различные точности классификации, начиная от 63% и до 97%. Применение тех или иных методик может быть обусловлено обстоятельствами. Но в работе делается акцент на то, что с применением переноса обучения высокие показатели точности и низкие показатели функции потерь могут быть получены путем, не требующим высоких временных или вычислительных затрат.

Эффективные способы решения в данной работе показывают высокие результаты точности, актуальные для современности. Перенос обучения достигает аналогичных 95-98% точностей и в других задачах классификации. Хотя стоит отметить, что подход имеет некоторые ограничения.

Таким образом, все поставленные задачи полностью решены, а, следовательно, цель дипломной работы достигнута.