

На правах рукописи



Сивак Мария Алексеевна

Робастное обучение нейронных сетей с простой архитектурой для решения задач классификации

Специальность 05.13.17 —
«Теоретические основы информатики»

Автореферат
диссертации на соискание учёной степени
кандидата технических наук

Новосибирск — 2022

Работа выполнена в Федеральном государственном бюджетном образовательном учреждении высшего образования «Новосибирский государственный технический университет».

Научный руководитель: доктор технических наук, доцент
Тимофеев Владимир Семенович

Официальные оппоненты: **Марков Николай Григорьевич**,
доктор технических наук, профессор,
Федеральное государственное автономное образовательное учреждение высшего образования «Национальный исследовательский Томский политехнический университет», отделение Информационных технологий, профессор;

Осипов Александр Леонидович,
кандидат технических наук, доцент,
Федеральное государственное бюджетное образовательное учреждение высшего образования «Новосибирский государственный университет экономики и управления "НИНХ"», кафедра Информационных технологий, доцент

Ведущая организация: Федеральное государственное бюджетное научное учреждение «Федеральный исследовательский центр информационных и вычислительных технологий» (Новосибирск)

Защита состоится 29 июня 2022 г. в 10:00 часов на заседании диссертационного совета Д 212.173.06 при Федеральном государственном бюджетном образовательном учреждении высшего образования «Новосибирский государственный технический университет» по адресу: 630073, Новосибирск, пр. К. Маркса, 20, I корпус, конференц-зал.

С диссертацией можно ознакомиться в библиотеке Новосибирского государственного технического университета и на сайте <http://www.nstu.ru>.

Автореферат разослан ___ мая 2022 года.

Ученый секретарь
диссертационного совета, к.т.н.

Фаддеев Андрей Владимирович

Общая характеристика работы

Актуальность темы исследования и степень ее разработанности.

В настоящее время исследователям в различных областях науки и техники приходится сталкиваться со все более сложными задачами. Нередки ситуации, когда у исследователя есть возможность получить достаточно большой объем данных, необходимых для решения той или иной практической задачи, но нет возможности программно реализовать эффективный алгоритм решения этой задачи в явном виде. В связи с этим большую популярность приобрела такая область информатики, как искусственный интеллект, и отдельный его раздел – машинное обучение. Особенность инструментов искусственного интеллекта заключается в том, что они работают за счет выделения статистических закономерностей в анализируемых данных, а не за счет выполнения непосредственных инструкций алгоритма.

Машинное обучение включает в себя множество инструментов, предназначенных для решения самого широкого круга задач, например для построения различных прогнозных моделей, разбиения данных на группы по определенному признаку, распознавания образов и др. Большой вклад в развитие этой области внесли такие известные зарубежные специалисты, как Самюэль А, Тьюринг А., Робертс Л., Dejong G. Нельзя недооценивать вклад в развитие этого направления, сделанный советскими и российскими учеными, авторами научных работ в области кибернетики и теории автоматического управления, такими как Китов А.И., Глушков В.Г., Ивахненко А.Г., Цыпкин Я.З.

Одним из наиболее известных инструментов машинного обучения сегодня являются искусственные нейронные сети (ИНС). Они используются повсеместно – от создания компьютерных игр и «умных» бытовых приборов до решения сложных наукоемких задач, требующих высокой точности получаемых результатов. Основоположниками в области нейронных сетей традиционно считаются Ф. Розенблатт, У. МакКаллок и У. Питтс. Дальнейшее развитие данная область получила благодаря Вербосу П.Дж., который считается автором алгоритма обратного распространения ошибки, использующегося при обучении нейронных сетей, а также Румельхарту Д.И. и Хинтону Дж.Е, которые популяризировали данный алгоритм. Здесь следует отметить также работы Галушкина А.И., Барцева С.И., Охонина В.А. – советских ученых, которые развивали идеи обучения нейронных сетей одновременно с западными специалистами и независимо от них. В практическом плане большое значение имели работы Минского М.Л. и Сейновски Т., носящие прикладной характер. Кроме того, говоря о развитии и популяризации нейронных сетей, нельзя не упомянуть таких специалистов, как Хайкин С. и Бишоп К.М. – авторов одних из общепризнанных в настоящее время работ, описывающих основы теории нейронных сетей.

Со временем стало ясно, что простые нейронные сети не всегда позволяют добиться высокой точности при решении задач, поскольку на практике в

подавляющем большинстве случаев анализируемые данные не являются идеальными – так или иначе в них присутствуют ошибки и нетипичные наблюдения, которые не подчиняются каким-то общим закономерностям. В связи с этим появился ряд работ за авторством Хопфилда Д.Д., Коско Б.Э, Лекуна Я., Elman J.L., Jordan M.I., в которых описывались более сложные модели нейронных сетей: рекуррентные нейронные сети, сети с памятью, сверточные нейронные сети. Такое развитие данной области со временем привело к формированию отдельного подраздела в машинном обучении – глубокого обучения (термин введен Хинтоном Дж. в 2006 году). Очевидно, что усложнение архитектуры нейронной сети влечет за собой рост вычислительной сложности алгоритмов обучения и, как следствие, увеличение или временных затрат на построение модели, или материальных затрат на приобретение более мощного аппаратного обеспечения.

В то же время в области прикладного статистического анализа данных получил широкое развитие робастный подход, позволяющий снизить негативное влияние нетипичных наблюдений без существенного усложнения архитектуры используемой модели. Значительный вклад в развитие этого направления внесли такие ученые, как Хьюбер П., Хампель Ф., Rousseeuw P., Денисов В.И., Смоляк С.А., Титаренко Б.П. Наиболее широко робастный подход используется в рамках регрессионного анализа. Устойчивые методы хорошо зарекомендовали себя при анализе зашумленных данных, поэтому представляется перспективным применить основные идеи робастного подхода при построении нейронных сетей. Кроме того, чтобы улучшить точность оценок, прогнозов и выводов, иногда в регрессионном анализе при сборе данных используют идеи теории планирования оптимального эксперимента. Представляется интересным исследовать эффекты от выбора различных планов эксперимента при подготовке данных для обучения нейронной сети.

Цель и задачи исследования. Целью данного исследования является разработка математического и алгоритмического обеспечения для построения робастных нейронных сетей, позволяющих корректно обрабатывать сильно зашумленные данные. Для достижения этой цели были поставлены и решены следующие задачи:

- исследовать применимость основных идей робастного подхода в области нейронных сетей;
- разработать, реализовать и исследовать алгоритм робастного обучения нейронных сетей с простой архитектурой;
- провести исследование устойчивости построенных нейронных сетей при анализе зашумленных данных и сформулировать рекомендации относительно настройки и использования робастных нейронных сетей, исследовать эффекты от использования различных планов эксперимента при обучении ИНС;

– разработать программный модуль, позволяющий строить робастные нейронные сети с произвольной простой архитектурой, и использовать его для решения задач прикладного характера.

Область исследования. Содержание диссертации соответствует п.5 области исследований «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» паспорта специальности 05.13.17 – «Теоретические основы информатики» (в области технических наук).

Методы исследования. Для решения поставленных задач использовались методы и положения математического анализа, прикладной математической статистики, регрессионного анализа, теории планирования эксперимента, а также методы статистического моделирования и методы оптимизации.

Достоверность и обоснованность научных положений, рекомендаций и выводов обеспечивается корректным использованием методов исследования, а также подтверждением полученных выводов результатами вычислительных экспериментов, проведенных с использованием технологии статистического моделирования.

Научная новизна работы заключается в следующем:

- предложен общий подход к построению робастных нейронных сетей с простой архитектурой на основе идеи алгоритма обратного распространения ошибки;
- сформулированы рекомендации относительно выбора значений внутренних параметров робастных функций потерь, позволяющие ускорить процесс настройки и обеспечить более высокую точность работы нейронных сетей;
- исследована устойчивость построенных робастных нейронных сетей при анализе зашумленных данных, впервые показано влияние качества плана эксперимента на точность работы робастной нейронной сети.

Теоретическая значимость работы заключается в развитии методов машинного обучения, а именно в предложенной модификации алгоритма обратного распространения ошибки, а также в исследовании применимости робастных функций потерь в нейронных сетях. Данная модификация отличается от классического алгоритма обратного распространения ошибки использованием робастных функций потерь вместо квадратичной, что позволяет снизить негативное влияние нетипичных наблюдений, не исключая их из рассмотрения.

Практическая значимость работы заключается в повышении точности классификации при работе с зашумленными данными, а также в сокращении времени обучения нейронной сети. Для обеспечения возможности использования полученных результатов на практике был разработан кроссплатформенный программный модуль «RobustNN», функционал которого позволяет выбрать

функцию потерь, а также задать количество скрытых слоев и число нейронов на каждом слое. Данный программный модуль был зарегистрирован в виде объекта интеллектуальной собственности как программа для ЭВМ (№ гос. рег. 2021618329 от 26 мая 2021 г.) [11]. С использованием данного модуля решены две прикладные задачи технического характера: задача классификации нефтяных месторождений и задача определения положения проводника при коронарном стентировании.

Положения, выносимые на защиту. На защиту выносятся:

- модификация алгоритма обратного распространения ошибки, позволяющая построить и обучить робастную нейронную сеть с простой архитектурой;
- результаты исследования устойчивости построенных робастных нейронных сетей при анализе различных зашумленных данных и рекомендации по настройке параметров различных робастных нейронных сетей, результаты исследования точности работы робастных нейронных сетей при использовании различных планов эксперимента;
- программный модуль для построения робастных нейронных сетей с произвольной простой архитектурой «RobustNN»;
- результаты решения задачи классификации нефтяных месторождений.

Личный творческий вклад автора в совместных публикациях заключается в:

- исследовании применимости идей робастного подхода при построении нейронных сетей;
- разработке и реализации робастной модификации алгоритма обратного распространения ошибки;
- исследовании свойств построенных робастных нейронных сетей и формировании рекомендаций по их настройке;
- разработке программного модуля «RobustNN», позволяющего строить робастные нейронные сети с произвольной простой архитектурой, и использовании реализованных программных средств для решения прикладных задач.

Апробация результатов диссертации. Результаты работы докладывались на XIII Всероссийской научной конференции молодых ученых “Наука. Технология. Инновации” (НТИ-2019, г. Новосибирск, 2-6 декабря 2019 г.), XIV Всероссийской научной конференции молодых ученых “Наука. Технология. Инновации” (НТИ-2020, г. Новосибирск, 30 нояб.–4 дек. 2020 г.), XV Всероссийской научной конференции молодых ученых “Наука. Технология. Инновации” (НТИ-2021, г. Новосибирск, 6-10 декабря 2021 г.); на XIV международной научно-технической конференции «Актуальные проблемы электронного приборостроения» (АПЭП-2018, г. Новосибирск, 2-6 октября 2018 года); на XV международной научно-технической конференции «Актуальные проблемы электронного приборостроения» (АПЭП-2021, г. Новосибирск, 19-21 ноября 2021 года).

Разработанные методы и алгоритмы используются в работе Татарского научно-исследовательского и проектного института нефти публичного акционерного общества «Татнефть» имени В.Д. Шашина, а также в учебном процессе кафедры теоретической и прикладной информатики НГТУ, что подтверждено соответствующими актами о внедрении. Работа выполнена при финансовой поддержке РФФИ в рамках научного проекта № 20-37-90077, Министерства науки и высшего образования в рамках Госзадания (проект № FSUN-2020-0009), федеральной целевой программы «Исследования и разработки по приоритетным направлениям развития научно-технологического комплекса России на 2014-2020 годы» (проект № 075-15-2019-1853), а также в рамках выполнения научно-исследовательских работ по договору № 0750/2021/4150.

Публикации. По результатам диссертационного исследования опубликованы 12 печатных работ [1-12], в том числе: 3 статьи в изданиях, рекомендованных ВАК, 2 статьи в изданиях, индексируемых в международных базах данных Scopus и/или Web of Science, 2 свидетельства о регистрации программы для ЭВМ.

Объем и структура работы. Диссертация состоит из введения, 5 глав основного содержания, заключения, списка литературы и 3 приложений. Полный объем диссертации составляет 111 страниц, включая 18 рисунков и 18 таблиц. Список литературы содержит 105 наименований.

Основное содержание работы

Во введении обоснована актуальность темы диссертации, сформулированы цель и задачи исследования, определены научная новизна, теоретическая и практическая значимость работы, дано краткое содержание работы по главам.

Первая глава является обзорной. В разделе 1.1 описываются различные виды задач машинного обучения и подходы к их решению (как классические, так и робастные). Основная задача машинного обучения, которая рассматривается в данной работе, – задача классификации.

Пусть имеется конечное множество классов $Q = \{q_1, \dots, q_{|Q|}\}$, где q_k – непересекающиеся между собой классы, а также конечное множество объектов $X = \{X_1, \dots, X_{|X|}\}$. При этом каждый объект $X_m, m = 1, \dots, |X|$ можно описать вектором $x_m = \{x_{m1}, x_{m2}, \dots, x_{mY}\}$, состоящим из значений признаков этого объекта $x_{mi}, i = 1, \dots, Y$, где Y – количество признаков. Классифицировать объект значит указать для каждого объекта X_m класс q_k , к которому этот объект относится.

При решении задачи классификации, как правило, всё множество объектов X разделяется на обучающую и тестовую подвыборки, которые представляют собой два непересекающихся подмножества. Обучающая выборка $L = \{X_1, \dots, X_{|L|}\}$ представляет собой набор объектов, с помощью которого происходит обучение алгоритма классификации. Тестовая выборка $D =$

$\{X_{|L|+1}, \dots, X_{|X|}\}$ представляет собой набор объектов, на котором производится оценка точности работы алгоритма классификации.

В разделе 1.2 рассматривается определение нейронной сети, а также проанализированы различные виды ИНС. Искусственная нейронная сеть представляет собой структуру, которая состоит из простых элементов, называемых нейронами. Нейроны связаны друг с другом посредством однонаправленных каналов (ребер). У ребер есть весовые коэффициенты, за счет корректировки которых и происходит обучение модели. Будем называть простой нейронной сетью или нейронной сетью с простой архитектурой модель нейронной сети типа перцептрон. Одним из наиболее часто используемых вариантов этой архитектуры является многослойный перцептрон с одним скрытым слоем.

В разделе 1.3 приводится модель простой нейронной сети для задачи классификации. Представлен пример ИНС с одним скрытым слоем (рис. 1).

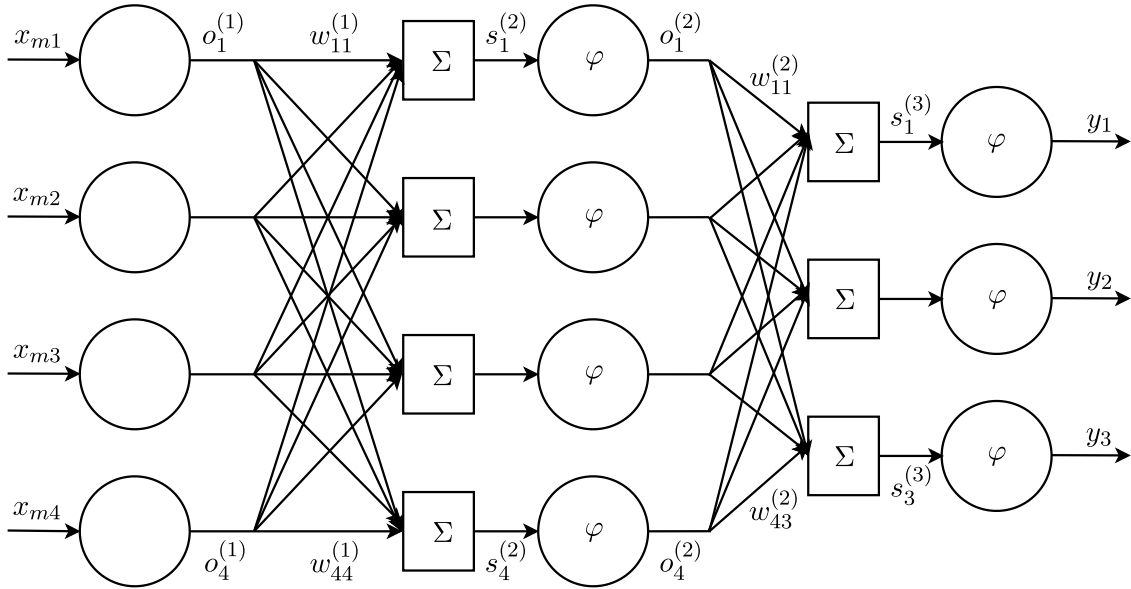


Рисунок 1 — Искусственная нейронная сеть с одним скрытым слоем

Данная сеть состоит из трёх слоев ($N = 3$). Входной слой сети, на который подаются признаки объекта X_m , включает в себя четыре нейрона, выходной — три (по одному для каждого класса q_k). Скрытый слой рассматриваемой сети состоит из четырёх нейронов. В качестве функции активации $\phi = \phi(z)$ в данной работе используется сигмоида:

$$\varphi(z) = \frac{1}{1 + e^z}.$$

Использованные на рис. 1 обозначения можно обобщить для более сложных нейронных сетей: y_k , $k = 1, \dots, |Q|$ — значения на выходном слое нейронной сети; $w_{ij}^{(n-1)}$, $i = 1, \dots, l^{(n-1)}$, $j = 1, \dots, l^{(n)}$ — вес между j -м нейроном слоя n и i -м нейроном слоя $n - 1$ ($l^{(n)}$ — количество нейронов на слое n); $s_j^{(n)}$ — входное значение j -го нейрона на слое n , определяемое на основе $o_i^{(n-1)}$ — выходных

значений нейронов на слое $n - 1$:

$$s_j^{(n)} = \sum_{i=1}^{l^{(n-1)}} w_{ij}^{(n-1)} o_i^{(n-1)}, n = 2, 3, \dots, N.$$

Если нейрон находится на входном слое, то для него будет выполняться

$$s_i^{(1)} = o_i^{(1)}.$$

Далее в п. 1.3.2 данного раздела описывается алгоритм обратного распространения ошибки. При использовании этого алгоритма обучение сети сводится к решению следующей задачи оптимизации:

$$E = \sum_{j=1}^{l^{(N)}} f(t_j, y_j) \rightarrow \min_{w_{ij}^{(1)}, \dots, w_{ij}^{(N-1)}},$$

где E – суммарная функция потерь, t_j – требуемый ответ на j -м выходе.

Обычно используется квадратичная функция потерь:

$$f(t_j, y_j) = \frac{1}{2}(y_j - t_j)^2. \quad (1)$$

Для минимизации суммарной функции потерь необходимо вычислить её производную по весам нейронной сети. В общем случае эта производная вычисляется в соответствии с

$$E'_{ji}^{(n)} = \delta_j^{(n)} o_i^{(n-1)},$$

где $\delta_j^{(n)}$ вычисляется следующим образом:

$$\delta_j^{(n)} = \frac{\partial E}{\partial o_j^{(n)}} \frac{\partial o_j^{(n)}}{\partial s_j^{(n)}} = \begin{cases} \frac{\partial f(y_j, t_j)}{\partial y_j} \varphi'(y_j), & n = N, \\ \left(\sum_{k=1}^{l^{(n+1)}} w_{jk}^{(n)} \delta_k^{(n+1)} \right) \varphi'(s_j^{(n)}), & \text{иначе.} \end{cases} \quad (2)$$

В п. 1.3.3 рассматриваются основные способы оценки точности работы построенной нейронной сети. Приводятся выражения для вычисления таких метрик, как *accuracy* ($\alpha(q_i)$), *precision* ($p(q_i)$), *recall* ($r(q_i)$). При решении задач множественной классификации обычно рассматриваются метрики α , p , r , представляющие собой средние арифметические значения метрик $\alpha(q_i)$, $p(q_i)$, $r(q_i)$, соответственно. Если значения метрик p и r совпадают, используют метрику *F1 – score*. Кроме того, в этом пункте рассматриваются такие критерии оценки качества, как ROC-кривые и AUC.

В разделе 1.4 рассматриваются особенности использования ИНС на практике. Описаны такие ситуации, как недообучение, переобучение, «паралич

сети». В разделе 1.5 проводится анализ существующих программных решений для построения ИНС. Рассмотрены наиболее известные фреймворки и программные комплексы, позволяющие построить и обучить модели нейронных сетей, описаны их преимущества и недостатки.

Анализ существующих методов решения задач машинного обучения, классического подхода к построению искусственных нейронных сетей, а также программных средств показал необходимость разработки и реализации общего подхода к построению робастных нейронных сетей, которые были бы устойчивы при анализе зашумленных данных.

Во второй главе рассматриваются вопросы построения робастных нейронных сетей. В разделе 2.1 выполняется исследование применимости различных робастных функций потерь (см. табл. 1) в нейронных сетях. Здесь и далее используются следующие обозначения для робастных функций потерь: f_1 – Эндрюса, f_2 – Уэлша, f_3 – Хьюбера, f_4 – Рамсея, f_5 – «Fair», f_6 – Коши, f_7 – биквадратная Тьюки, f_8 – Geman-McCluer, f_9 – Мешалкина, f_{10} – Charbonnier, f_{11} – Тьюки, f_{12} – Хампеля.

Таблица 1 – Робастные функции потерь и их производные

f_i	Функция потерь $\rho(z)$	Производная $\rho'(z)$
f_1	$\begin{cases} \beta(1 - \cos \frac{z}{\beta}), & z < \pi\beta \\ 2\beta, & z \geq \pi\beta \end{cases}$	$\begin{cases} \sin \frac{z}{\beta}, & z < \pi\beta \\ 0, & z \geq \pi\beta \end{cases}$
f_2	$1 - \exp(-\frac{1}{2}(\frac{z}{\beta})^2)$	$\frac{1}{\beta^2}z \exp(-\frac{1}{2}(\frac{z}{\beta})^2)$
f_3	$\begin{cases} \frac{1}{2}z^2, & z \leq \beta \\ \beta z - \frac{1}{2}\beta^2, & z > \beta \end{cases}$	$\begin{cases} z, & z \leq \beta \\ -\beta, & z < -\beta \\ \beta, & z > \beta \end{cases}$
f_4	$\frac{1}{\beta^2}(1 - (1 + \beta z) \exp(-\beta z))$	$z \exp\{-\beta z \}$
f_5	$\beta^2 \left(\frac{ z }{\beta} - \ln \left(1 + \frac{ z }{\beta} \right) \right)$	$\frac{z}{(1+ z /\beta)}$
f_6	$\ln(\frac{1}{2}(\frac{z}{\beta})^2 + 1)$	$\frac{z}{\frac{1}{2}z^2 + \beta^2}$
f_7	$\begin{cases} \frac{z^6}{6\beta^4} - \frac{z^4}{2\beta^2} + \frac{z^2}{2}, & z < \beta \\ \frac{\beta^2}{6}, & z \geq \beta \end{cases}$	$\begin{cases} \frac{z^5}{\beta^4} - \frac{2z^3}{\beta^2} + z, & z < \beta \\ 0, & z \geq \beta \end{cases}$
f_8	$\frac{z^2/\beta}{1+z^2/\beta}$	$\frac{2z}{\beta(1+z^2/\beta)^2}$
f_9	$\beta^{-1}(1 - \exp(\frac{-\beta z^2}{2}))$	$\exp(\frac{-\beta z^2}{2})z$
f_{10}	$\sqrt{(\frac{z}{\beta})^2 + 1}$	$\frac{1}{\beta^2} \frac{z}{\sqrt{z^2/\beta^2 + 1}}$
f_{11}	$\begin{cases} z^2, & z \leq \beta \\ \beta^2, & z > \beta \end{cases}$	$\begin{cases} 2z, & z < \beta \\ 0, & z \geq \beta \end{cases}$

Таблица 1 – продолжение

f_i	Функция потерь $\rho(z)$	Производная $\rho'(z)$
f_{12}	$\left\{ \begin{array}{ll} z^2, & 0 \leq z \leq \eta \\ \eta^2 + \eta(z - \eta), & \eta < z \leq \beta \\ \eta^2 + 2\eta(\beta - \eta) - \\ - \frac{\eta(\gamma - z)^2}{\gamma - \beta} + & \beta < z \leq \gamma \\ + \eta(\gamma - \beta), & \\ \eta^2 + 2\eta(\beta - \eta) + & \\ + \eta(\gamma - \beta), & \gamma < z \end{array} \right.$	$\left\{ \begin{array}{ll} 2z, & 0 \leq z \leq \eta \\ \mathit{sign}(z)2\eta, & \eta < z \leq \beta \\ \frac{2\eta}{\gamma - \beta}(\gamma - z) \cdot \\ \cdot \mathit{sign}(z), & \beta < z \leq \gamma \\ 0, & \gamma < z \end{array} \right.$

Предлагаемая модификация алгоритма обратного распространения ошибки заключается в замене квадратичной функции потерь на робастную. При этом необходимо учесть, что используемая функция потерь должна быть непрерывно дифференцируемой. Рассматриваемые производные робастных функций потерь также приводятся в табл. 1.

Очевидно, что производные робастных функций потерь Рамсея, Коши, Geman-McCluer, «Fair», Charbonnier, Уэлша и Мешалкина при $\beta > 0$ являются непрерывными на множестве действительных чисел \mathbb{R} , следовательно, эти функции потерь могут быть использованы в алгоритме обратного распространения ошибки. Производные функций потерь Хьюбера, Эндрюса, Хампеля, Тьюки и биквадратная функция потерь Тьюки имеют предполагаемые точки разрыва. В связи с этим были сформулированы и доказаны два утверждения, показывающие возможность использования этих функций при обучении ИНС.

Утверждение 2.1. Робастные функции потерь Хьюбера, Эндрюса, Хампеля и биквадратная функция потерь Тьюки имеют непрерывные производные и могут быть использованы в алгоритме обратного распространения ошибки.

Утверждение 2.2. Робастная функция потерь Тьюки не удовлетворяет ограничению алгоритма обратного распространения ошибки.

Таким образом, для дальнейших исследований были выбраны все робастные функции потерь из табл. 1, кроме функций потерь Тьюки и Хампеля. Последняя не рассматривалась из-за необходимости настройки трех параметров, что привело бы к увеличению вычислительных затрат. Более подробный анализ робастных функций потерь представлен в [6].

В разделе 2.2 предлагается робастная модификация алгоритма обратного распространения ошибки, подробно изложенная в [1]. Было сформулировано и доказано следующее утверждение, позволяющее построить эту модификацию.

Утверждение 2.3. Использование робастной функции потерь вместо квадратичной функции потерь (1) в алгоритме обратного распространения ошибки приведет к изменению только тождества (2).

Это тождество примет вид

$$\delta_j^{(n)} = \frac{\partial E}{\partial o_j^{(n)}} \frac{\partial o_j^{(n)}}{\partial s_j^{(n)}} = \begin{cases} \frac{\partial f_R(y_j, t_j)}{\partial y_j} \varphi'(y_j), & n = N, \\ \left(\sum_{k=1}^{l^{(n+1)}} w_{jk}^{(n)} \delta_k^{(n+1)} \right) \varphi'(s_j^{(n)}), & \text{иначе,} \end{cases} \quad (3)$$

где $f_R(y_j, t_j) = \rho(y_j - t_j)$ – любая функция из табл. 1, кроме функций потерь Хампеля или Тьюки.

Доказанное утверждение позволило построить модификацию алгоритма обратного распространения ошибки путем замены (2) на (3), оставляя без изменений большинство шагов алгоритма. При этом за счет использования различных функций потерь был получен класс совершенно новых нейронных сетей, которые могут быть использованы для решения различного рода задач, например для анализа образовательных [3] или текстовых [5, 10] данных.

Раздел 2.3 посвящен исследованию влияния плана эксперимента на точность работы робастной нейронной сети. Рассматривалась задача бинарной классификации, в рамках которой каждый объект X_m описывался двухкомпонентным вектором значений признаков $x_m = \{x_{m1}, x_{m2}\}$. Предполагалось, что при сборе данных исследователь мог контролировать значения признака x_{m2} и проводились два эксперимента, каждый из которых включает в себя 500 наблюдений (по 250 для каждого класса). План первого эксперимента состоял из двух возможных значений признака x_{m2} и выглядел следующим образом:

$$\xi^{(1)} = \begin{Bmatrix} 10 & 20 \\ r_1 & r_2 \end{Bmatrix},$$

где $r_i > 0$ – число наблюдений для i -го возможного значения признака x_{m2} ; $r_1 + r_2 = 500$. План второго эксперимента состоял из 11 возможных значений признака x_{m2} и выглядел следующим образом:

$$\xi^{(2)} = \begin{Bmatrix} 10 & 11 & 12 & 13 & 14 & 15 & 16 & 17 & 18 & 19 & 20 \\ r_1 & r_2 & r_3 & r_4 & r_5 & r_6 & r_7 & r_8 & r_9 & r_{10} & r_{11} \end{Bmatrix},$$

где $\sum_{i=1}^{11} r_i = 500$; $r_i > 0$. В результате моделирования были получены два набора данных, для каждого из которых дополнительно выполнялось добавление выбросов для признака x_{m1} :

$$\tilde{x}_{m1} = x_{m1} + \epsilon_{m1}, \quad (4)$$

где ϵ_{m1} – независимые и одинаково распределенные случайные ошибки. Эти ошибки имели следующую функцию распределения:

$$F_1(x) = (1 - \lambda)F_1(x, 0, \sigma_{11}) + \lambda F_2(x, 0, \sigma_{12}), \quad (5)$$

где $F_j(x, 0, \sigma_{1j})$, $j = 1, 2$ – функция нормального распределения с нулевым математическим ожиданием и дисперсией σ_{1j}^2 , $\lambda \in [0, 1]$ – параметр смеси, играющий роль доли засоряющих наблюдений. В данном случае задавались не сами значения дисперсий $\sigma_{11}^2, \sigma_{12}^2$, а соответствующие им значения уровня шума. Уровень шума определяется следующим образом:

$$\rho_{ij} = \frac{\sigma_{ij}}{c} 100\%, \quad (6)$$

где c^2 – дисперсия незашумлённой выборки.

При моделировании выбросов в данной задаче полагалось, что дисперсия σ_{11}^2 соответствовала уровню шума $\rho_{11} = 30\%$, а дисперсия σ_{12}^2 – уровню шума $\rho_{12} = 120\%$. Значение доли засоряющих наблюдений λ полагалось равным 0,25.

Для решения рассматриваемой задачи использовалась робастная ИНС с функцией потерь Хьюбера (параметр функции потерь $\beta = 0,5$) и одним скрытым слоем, имеющая следующую архитектуру: по 2 нейрона на входном и на выходном слое, 3 нейрона на скрытом.

Для оценки точности работы нейронных сетей использовалась метрика α , значение которой фиксировалось при числе эпох обучения h , равном 2, 5, 10, 50, 100 и далее до 1000 эпох с шагом в 100. Для обоих наборов данных выполнялось по 50 вычислительных экспериментов (в ходе каждого вычислительного эксперимента 100 раз проводилось обучение нейронной сети с разным начальным приближением для весов), результаты которых затем усреднялись. Полученные результаты приводятся на рис. 2.

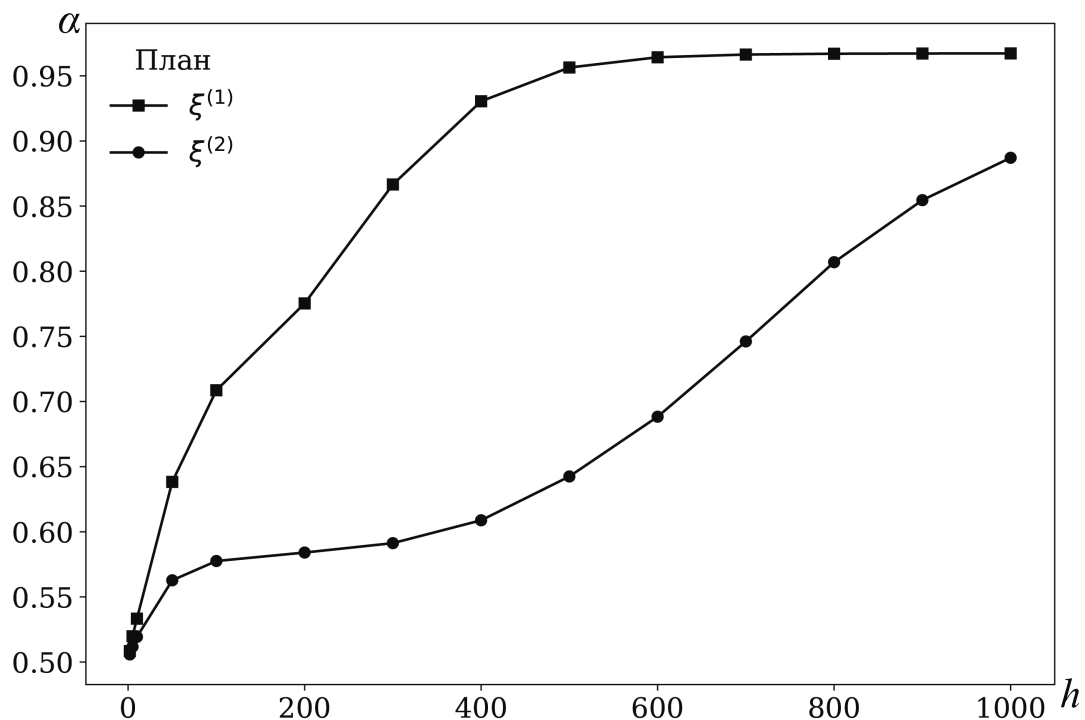


Рисунок 2 — Точность работы нейронных сетей для планов $\xi^{(1)}$ и $\xi^{(2)}$

Из рис. 2 видно, что для плана эксперимента $\xi^{(1)}$ точность работы робастной нейронной сети, начиная с 500 эпох обучения, достигает значения 0,95

по метрике α и фактически перестает изменяться. В то же время для плана эксперимента $\xi^{(2)}$ точность работы нейронной сети по метрике α не превышает значение 0,90 даже на 1000 эпох обучения. В связи с этим для плана $\xi^{(2)}$ проводилось дополнительно еще 50 вычислительных экспериментов, в ходе которых нейронная сеть обучалась в течение 2000 эпох. Однако даже на 2000 эпох точность работы нейронной сети по метрике α достигла только значения 0,93.

Проведенные исследования позволяют сделать вывод о том, что для плана эксперимента $\xi^{(1)}$ процесс обучения нейронной сети проходит быстрее, чем для плана $\xi^{(2)}$, а сам план $\xi^{(1)}$ является более качественным.

В третьей главе приводятся результаты исследования работоспособности робастных нейронных сетей при анализе различных зашумленных данных. В разделе 3.1 выполняется настройка моделей и даются рекомендации по выбору значений параметров робастных функций потерь.

Для исследований использовался набор данных «Ирисы Фишера», состоящий из 150 объектов. Каждый ирис $X_m, m = 1, \dots, 150$ описывается 4 признаками $x_{mi}, i = 1, \dots, 4$ и классом $q_k, k = 1, 2, 3$. Моделирование выбросов выполнялось для 3 и 4 признаков аналогично (4), (5).

На первом этапе исследований необходимо было определить наилучшие значения параметра β робастных функций потерь (такие значения, при которых точность работы сети была бы наиболее высокой). Для этого значения параметра варьировались на различных интервалах $(\beta_{min}, \beta_{max}]$, границы и шаг разбиения которых определялись посредством проведения предварительного исследования.

Сначала для всех выбранных в разделе 2.1 робастных функций потерь параметры рассматривались на интервале $(0, 0; 20, 0]$ с шагом разбиения 0,01, значение доли засоряющих наблюдений полагалось $\lambda = 0,25$, значение метрики α фиксировалось на 500 эпохах обучения. Для каждого значения β проводилось по 10 вычислительных экспериментов, результаты которых затем усреднялись. После проведения предварительного исследования для всех функций потерь была скорректирована правая граница интервалов (для функций потерь Эндрюса, Рамсея, Мешалкина и биквадратной Тьюки $\beta_{max} = 5,0$, для функций потерь Коши и Charbonnier $\beta_{max} = 7,0$, для функций потерь «Fair» и Geman-McCluer $\beta_{max} = 10,0$, для функции потерь Хьюбера $\beta_{max} = 1,0$, для Уэлша – $\beta_{max} = 8,0$), а также для ряда функций – шаг разбиения (0,05 для функции потерь Хьюбера и 0,5 для функций потерь «Fair» и Geman-McCluer). Для функции Geman-McCluer дополнительно рассматривались значения $\beta = 20, 50, 100$, так как было отмечено улучшение точности работы нейронной сети с ростом значения параметра.

Далее исследования проводились следующим образом. Значение λ изменялось от 0,05 до 0,40 с шагом в 0,05. Для каждого значения λ при всех β из указанных интервалов с заданным шагом разбиения вычислялось значение

метрики α и фиксировалось при различном числе эпох, в течение которых проходило обучение нейронной сети (50, 100 и далее до 1000 с шагом в 100 эпох). В ходе исследований для каждой робастной сети проводилось по 100 вычислительных экспериментов, результаты которых затем усреднялись. По результатам исследований были определены рекомендованные интервалы значений параметров при различном числе эпох обучения сети (табл. 2). Аналогичные исследования проводились для остальных функций потерь.

Таблица 2 — Рекомендованные интервалы значений параметров робастных функций потерь

$f_R(t_j, y_j)$	100 эпох	101–300 эпох	301–500 эпох	>500 эпох
Эндрюса	[1,5; 2,9]	[4,7; 5,0]	[4,7; 5,0]	[4,7; 5,0]
Уэлша	[0,5; 2,1]	[0,5; 2,1]	[2,3; 3,2]	[3,5; 4,6]
Хьюбера	[0,4; 0,55]	[0,2; 0,35]	[0,2; 0,35]	[0,2; 0,35]
Рамсея	[0,6; 1,0]	[0,8; 1,7]	[0,8; 1,7]	[0,8; 1,7]
«Fair»	[0,5; 1,5]	[0,5; 1,5]	[0,1; 0,5]	[0,1; 0,5]
Биквадратная Тьюки	[1,5; 1,7]	[1,3; 1,6]	[1,2; 1,5]	[1,2; 1,4]
Коши	[0,7; 1,3]	[2,4; 3,3]	[3,6; 5,2]	[5,2; 6,9]
Geman-McCluer	[2,0; 5,0]	[9,5; 10]	>20	>20
Charbonnier	[1,2; 1,7]	[2,2; 2,7]	[2,8; 3,3]	[2,8; 3,8]
Мешалкина	[1,4; 2,2]	[1,8; 3,3]	[2,2; 3,8]	[3,8; 4,9]

На основе полученных результатов были даны рекомендации относительно выбора значения параметра робастных функций потерь для ИНС с одним скрытым слоем. Для функции потерь Хьюбера значение параметра $\beta \geq 1$ выбирать не следует – в этом случае она будет полностью совпадать с квадратичной функцией. Для функций потерь Эндрюса, Рамсея, Коши, Charbonnier и Мешалкина значение параметра следует постепенно увеличивать с ростом числа эпох, однако слишком большие значения β могут негативно сказаться на точности классификации. Для функции потерь «Fair» и для биквадратной функции потерь Тьюки, наоборот, с ростом числа эпох обучения следует уменьшить значение β . Для функции потерь Geman-McCluer при малом числе эпох (до 300) можно выбирать β на интервале [2,0; 10,0], с ростом числа эпох – больше 20. Более подробно настройка робастных нейронных сетей описана в [2, 8, 9].

На рис. 3 продемонстрирована полученная зависимость точности классификации от значения параметра β для нейронной сети с функции потерь Charbonnier при различном числе эпох обучения и доли засоряющих наблюдений $\lambda = 0,25$. Нетрудно заметить, что с ростом числа эпох обучений возрастает и наилучшее значение параметра функции, например, для 100 эпох $\beta = 1,5$, а для 500 эпох $\beta = 3,0$. Однако слишком большие значения параметра приводят к снижению точности работы нейронной сети.

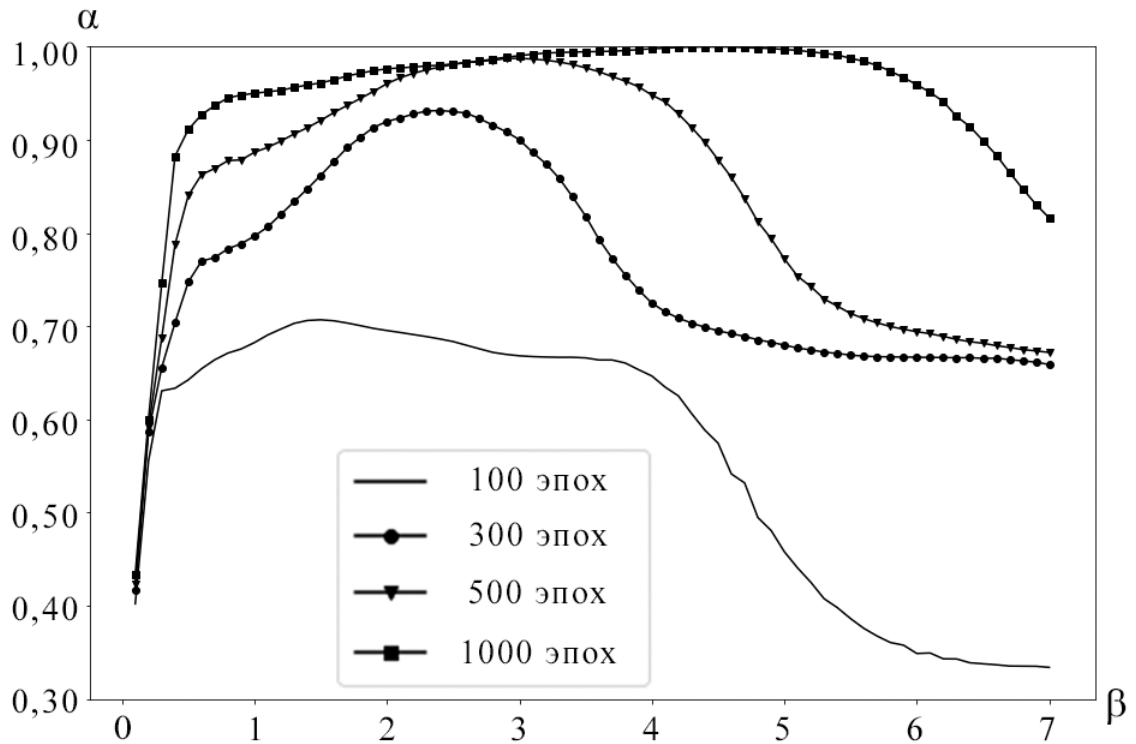


Рисунок 3 — Зависимость наилучшего значения параметра функции потерь Charbonnier от числа эпох обучения

В разделе 3.2 приводятся результаты исследования устойчивости построенных робастных нейронных сетей и сравнения их точности работы с точностью работы классической ИНС (с квадратичной функцией потерь). Набор данных использовался тот же, что и на предыдущем этапе исследований. Значения метрики α фиксировались при 100, 300 и 500 эпохах обучения для всех λ на отрезке $[0,05; 0,40]$ с шагом в 0,05. Всего выполнялось по 100 вычислительных экспериментов. Результаты исследований для 100 и 500 эпох обучения и значений доли засоряющих наблюдений $\lambda = \{0,05; 0,10; 0,35; 0,40\}$ приводятся в табл. 3 (f_q — квадратичная функция потерь).

Из табл. 3 видно, что при 100 эпохах обучения точность и скорость работы робастных нейронных сетей сопоставимы с классической. Однако даже при небольшой доле засоряющих наблюдений ($\lambda = 0,05$) с ростом числа эпох обучения до 500 робастные сети начинают работать точнее классической в среднем на 4,2%, а значение метрики α для всех робастных ИНС превышает 0,94. С ростом λ до 0,10 робастные ИНС обучаются быстрее и показывают точность в среднем на 8,1% выше, чем классическая нейронная сеть. При этом наименьшее значение метрики $\alpha = 0,898$ достигается для функции потерь «Fair», наибольшее ($\alpha = 0,956$) — для функций потерь Charbonnier и Уэлша. При работе с сильно зашумленными выборками (доля выбросов $\lambda = 0,35$ и $\lambda = 0,40$) робастные сети работают точнее в среднем на 11-12%, а в некоторых случаях (для функций потерь Коши, Charbonnier, Geman-McCluer) выигрыш в точности достигает 15%.

В разделе 3.3 приводятся результаты исследования точности работы построенных нейронных сетей при различном числе объектов в наборе данных. На

этом этапе использовались синтетические наборы данных, структура которых была аналогична набору «Ирисы Фишера». Рассматривались наборы данных из 150, 450, 600 и 900 объектов, при $\lambda = 0,25$. Для робастных функций потерь значения параметра β выбиралось согласно данным ранее рекомендациям. Точность работы нейронных сетей фиксировалась после 100, 300 и 500 эпох обучения.

Таблица 3 — Точность классификации при различной доле выбросов

λ	0,05		0,10		0,35		0,40	
h	100	500	100	500	100	500	100	500
f_1	0,766	0,966	0,723	0,927	0,696	0,925	0,693	0,937
f_2	0,770	0,968	0,723	0,956	0,696	0,960	0,694	0,954
f_3	0,767	0,943	0,719	0,913	0,677	0,908	0,690	0,907
f_4	0,771	0,950	0,722	0,916	0,687	0,913	0,692	0,918
f_5	0,769	0,951	0,722	0,898	0,689	0,900	0,691	0,899
f_6	0,769	0,968	0,723	0,957	0,696	0,960	0,694	0,954
f_7	0,770	0,945	0,721	0,912	0,679	0,901	0,690	0,899
f_8	0,767	0,967	0,723	0,955	0,696	0,959	0,694	0,952
f_9	0,770	0,945	0,721	0,915	0,678	0,899	0,691	0,909
f_{10}	0,769	0,967	0,723	0,956	0,695	0,960	0,694	0,954
f_q	0,750	0,914	0,716	0,835	0,656	0,818	0,670	0,803

Исследования показали, что увеличение числа объектов со 150 до 450 зачастую не сказывается на точности работы нейронных сетей негативным образом (а в случае классической ИНС точность даже увеличилась на 3,1%), а дальнейшее увеличение числа объектов приводит к снижению точности работы нейронных сетей. Так, по сравнению с набором, состоящим из 450 объектов, при использовании робастных сетей точность классификации для набора из 600 объектов снизилась примерно на 1%, а для набора из 900 объектов – на 2%. Для классической ИНС с ростом числа объектов с 450 до 600 точность снизилась на 1,1%, а с ростом числа объектов с 600 до 900 – еще на 1,8%. По сравнению с классической ИНС наибольший выигрыш в точности дали ИНС с функциями потерь Уэлша, Коши и Geman-McCluer, наименьший – с функцией потерь Рамсея и биквадратной функцией потерь Тьюки. Более подробно результаты данного этапа исследований представлены в [7].

В четвертой главе описывается разработанный программный модуль для построения робастных нейронных сетей «RobustNN».

В разделе 4.1 приводятся общие сведения о программном модуле. Он реализован с использованием языка программирования Python 3.6 и является кроссплатформенным. Минимальные системные требования для работы с модулем: IBM PC-совместимый ПК с ОЗУ не менее 1 Гб, ОС Windows 7/8/8.1/10/11, либо ОС Linux семейства Debian/Red Hat, интерпретатор языка Python 3.6, установленный модуль numpy.

В разделе 4.2 описываются основные классы и методы модуля. Модуль включает в себя два класса: класс `RobustLayer`, позволяющий задать отдельный слой нейронной сети, и класс `RobustNet`, использующийся для объединения слоев в модель. Программный модуль «`RobustNN`» позволяет:

- создавать отдельные слои, задавать их параметры (число входов и выходов на слое, вид функции активации), объединять слои в модель;
- выбирать функцию потерь, используемую при обучении модели;
- осуществлять обучение модели в течение требуемого числа эпох;
- сохранять и загружать построенную модель;
- проводить оценку качества модели на основе различных метрик;
- получать ответ от обученной модели для конкретного объекта.

В разделе 4.3 показано, как использовать программный модуль для организации работы в различных режимах: в режиме обучения модели, оценки качества модели и получения ответа для конкретного объекта.

В пятой главе рассматривается решение двух практических задач. В разделе 5.1 приводятся постановка и результаты решения задачи классификации нефтяных месторождений. Разработанные по результатам решения алгоритмы вошли в программный модуль `Epsilon` [12].

Набор данных включал в себя 96 объектов нефтяных месторождений $X = \{X_1, \dots, X_{96}\}$, описываемых вектором признаков из 9 компонент. Классы объектов заранее определены не были – для этого использовались алгоритм *k*-средних и EM-алгоритм. Были получены два варианта кластеризации объектов, на основе которых были сформированы три класса объектов q_1, q_2, q_3 . Для обоих вариантов кластеризации была построена классическая нейронная сеть, а также три робастные сети: с функциями потерь Коши, Уэлша и биквадратной функцией потерь Тьюки. Оценка качества работы построенных сетей выполнялась на основе метрик α , p и r .

При первом варианте кластеризации качество работы классической и робастных ИНС было сопоставимым ($\alpha = 0,95, p = 0,945, r = 0,889$). При этом значения метрик $r(q_i)$ показали, что модели очень хорошо определяют объекты второго и третьего классов ($r(q_2) = r(q_3) = 1,0$), однако потенциально могут плохо обнаруживать объекты первого класса ($r(q_1) = 0,667$). Для второго варианта кластеризации робастные ИНС ($\alpha = 0,952, p = 0,967, r = 0,958$) работали точнее классической ($\alpha = 0,905, p = 0,939, r = 0,875$). Значения метрик $r(q_i)$ показали, что классическая модель гораздо хуже определяет объекты первого класса ($r(q_1) = 0,750$) и все модели потенциально могут не обнаружить какие-то объекты, относящиеся ко второму классу ($r(q_2) = 0,875$ для всех ИНС). Более подробные результаты решения данной задачи представлены в [4].

В разделе 5.2 приводятся постановка и результаты решения задачи определения местоположения проводника в кровеносном сосуде. Точность работы построенных ИНС с функцией потерь Эндрюса превысила 0,981 по метрике α .

Заключение

Основные результаты, полученные в данной работе:

1. Проведен анализ возможности использования идей робастного подхода при построении искусственных нейронных сетей. Сформулированы и доказаны два утверждения, показывающие возможность использования 12 робастных функций потерь в нейронных сетях, 10 из которых выбраны для дальнейших исследований.

2. Предложен общий подход к построению робастных нейронных сетей на основе алгоритма обратного распространения ошибки. Для этого сформулировано и доказано утверждение, позволяющее получить робастную модификацию алгоритма обратного распространения ошибки с использованием различных функций потерь, не меняя при этом основную логику алгоритма.

3. Выполнена настройка полученных робастных нейронных сетей, по результатам вычислительных экспериментов сформированы рекомендации относительно выбора значений параметров робастных функций потерь. Проведено исследование работоспособности построенных моделей при анализе различных зашумленных данных. Впервые продемонстрировано влияние качества плана эксперимента при обучении робастных нейронных сетей.

4. Разработан программный модуль для построения робастных нейронных сетей, позволяющий задать архитектуру модели, провести обучение нейронной сети и оценить качество ее работы.

5. С использованием робастных нейронных сетей решены две практические задачи: задача классификации нефтяных месторождений и задача определения местоположения проводника при коронарном стентировании.

Публикации автора по теме диссертации

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

1. Тимофеев, В. С. Робастная нейронная сеть с простой архитектурой / В. С. Тимофеев, М. А. Сивак // Сибирский журнал индустриальной математики. – 2021. – Т. 24, № 4. – С. 126–138.

2. Сивак, М. А. Настройка робастных нейронных сетей для решения задачи классификации / М. А. Сивак, В. С. Тимофеев // Доклады Томского государственного университета систем управления и радиоэлектроники. – 2021. – Т. 24, № 3. – С. 26–32.

3. Сивак, М. А. Система поддержки принятия решений для анализа образовательных данных в вузе / М. А. Сивак, В. М. Стасышин // Информатизация и связь. – 2019. – № 5. – С. 128–132.

Международные рецензируемые издания:

4. Oilfield Classification with Various Neural Networks / M. A. Sivak [et al.] // 2021 XV International Scientific-Technical Conference on Actual Problems Of Electronic Instrument Engineering (APEIE). – 2021. – P. 600–603.

5. *Skvortsova, E.B.* Statistical Methods in the Problem of Studying Apology Speech Formulas and Their Satellites in the English language / E.B. Skvortsova, Bochkarev A.I. Pepelyaeva M. A. // 2018 XIV International Scientific-Technical Conference on Actual Problems of Electronics Instrument Engineering (APEIE). Vol. 1. – 2018. – P. 33–36.

Другие издания:

6. *Сивак, М. А.* Исследование применимости робастных функций потерь в нейронных сетях / М. А. Сивак // Сборник научных трудов НГТУ. – 2020. – № 4. – С. 50–58.

7. *Сивак, М. А.* Классификация зашумленных данных при различных объемах выборки / М. А. Сивак // Наука. Технологии. Инновации : сб. науч. тр.: в 9 ч., Новосибирск, 6-10 дек. 2021 г. Ч. 2. – Изд-во НГТУ, 2021. – С. 277–279.

8. *Сивак, М. А.* Оптимизация работы робастной нейронной сети для задачи классификации / М. А. Сивак, В. С. Тимофеев // Наука. Технологии. Инновации : сб. науч. тр.: в 9 ч., Новосибирск, 30 нояб.-4 дек. 2020 г. Ч. 2. – Изд-во НГТУ, 2020. – С. 298–300.

9. *Сивак, М. А.* Построение робастных нейронных сетей с различными функциями потерь / М. А. Сивак, В. С. Тимофеев // Системы анализа и обработки данных. – 2021. – Т. 82, № 2. – С. 67–83.

10. *Сивак, М. А.* Применение нейронных сетей различной архитектуры для решения задачи фильтрации спама / М. А. Сивак, В. С. Тимофеев // Наука. Технологии. Инновации: сб. науч. тр.: в 9 ч., Новосибирск, 2-6 дек. 2019 г. Ч.2. – Изд-во НГТУ, 2019. – С. 231–232.

Свидетельства о государственной регистрации права для ЭВМ:

11. Модуль для построения робастных нейронных сетей (RobustNN) / М. Сивак, В. Тимофеев (Россия). – № 2021618329 ; заявл. 26.05.2021 ; опубли. 26.05.2021. – 1 с.

12. Модуль прогнозирования параметров добычи нефти системы Estimating Performance of System Investment in Long-term Oil production using Neuronet / В. Тимофеев [и др.] (Россия). – № 2020667173 ; заявл. 23.11.2020 ; опубли. 21.12.2020. – 1 с.

Подписано в печать 25.04.2022. Заказ №945
Формат 60×90/16. Усл. печ. л. 1.1. Тираж 100 экз.

Отпечатано в типографии

Новосибирского государственного технического университета
630073, г. Новосибирск, пр. К. Маркса, 20, тел. (383) 346-08-57