Московский институт электроники и математики им. А.Н. Тихонова

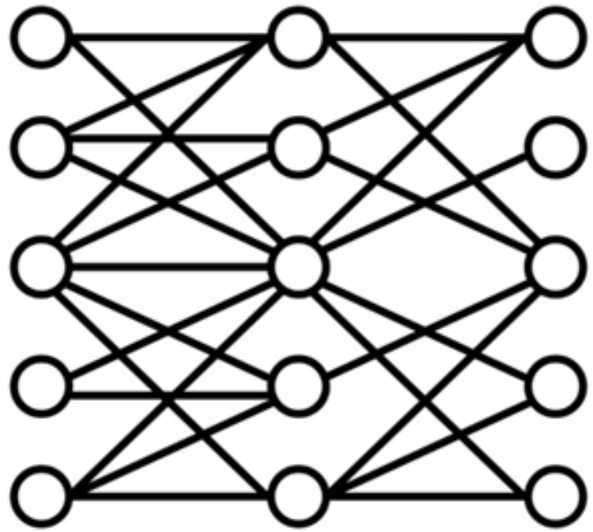
Кафедра информационной безопасности киберфизических систем

Москва 2025

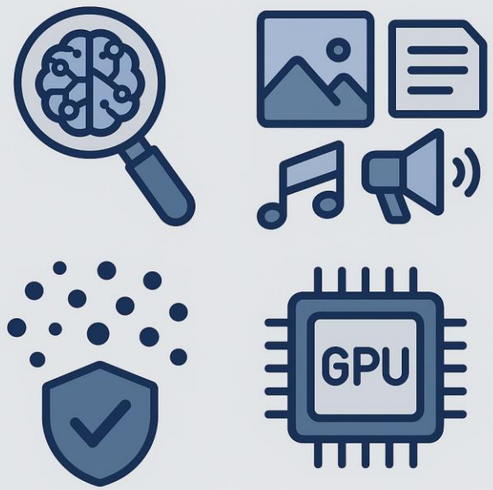
Изучение Deep Learning

Введение в Deep Learning с RapidMiner

Глубинное обучение — направление искусственного интеллекта, позволяющее решать задачи классификации изображений и анализа текста. RapidMiner предлагает инструменты для создания нейронных сетей без программирования.



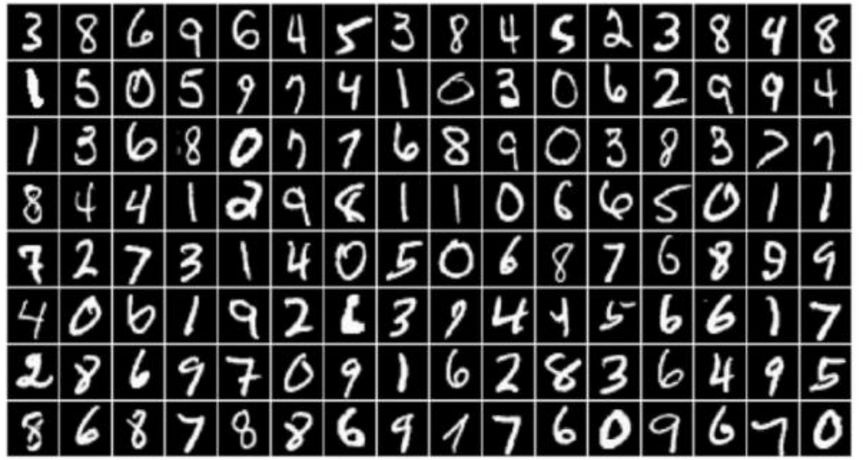
Преимущества Deep Learning



- Автоматическое извлечение признаков данных.
- Универсальность применения (изображения, текст, аудио).
- Устойчивость к шумным данным.
- Аппаратная поддержка GPU для ускорения обучения сетей.

Описание тестового набора данных MNIST

Будет рассмотрен набор MNIST, который состоит из 70 000 изображений рукописных цифр (0-9). Из них 60 000 предназначены для обучения, а 10 000 — для тестирования моделей. Изображения имеют размер 28×28 пикселей.



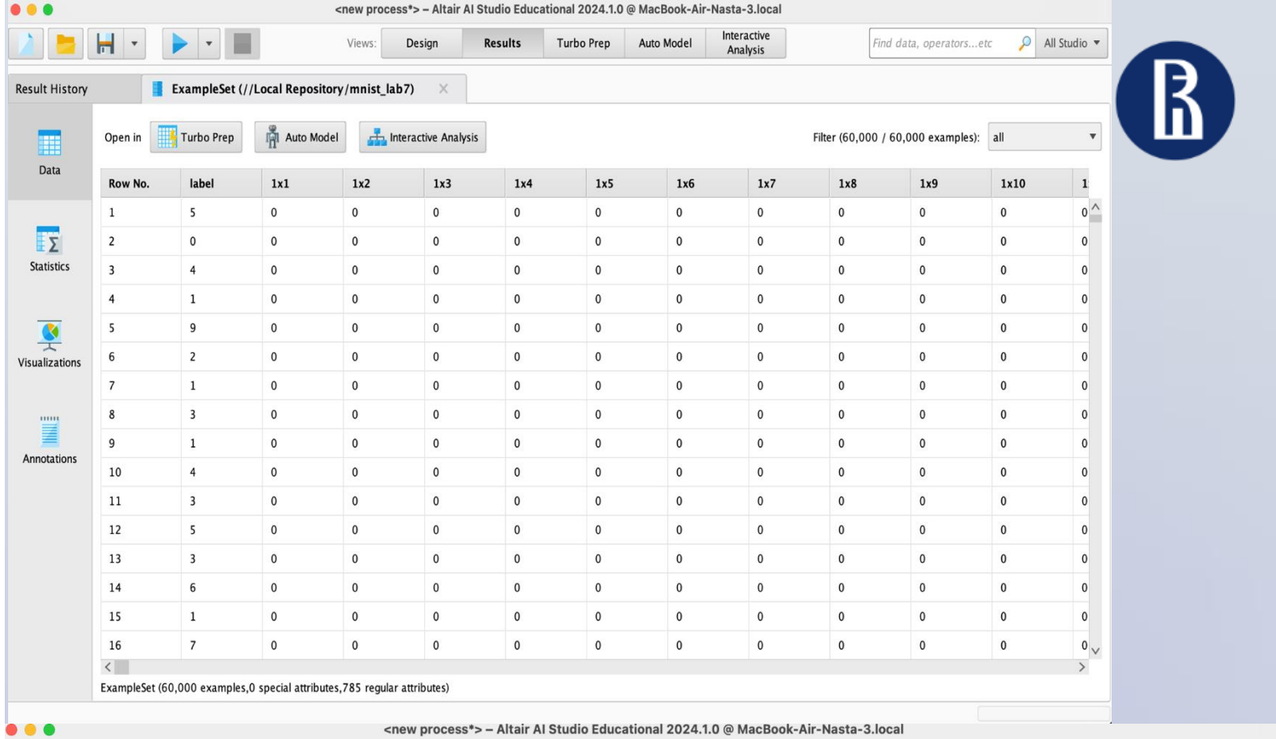
Почему рассматриваем набор MNIST

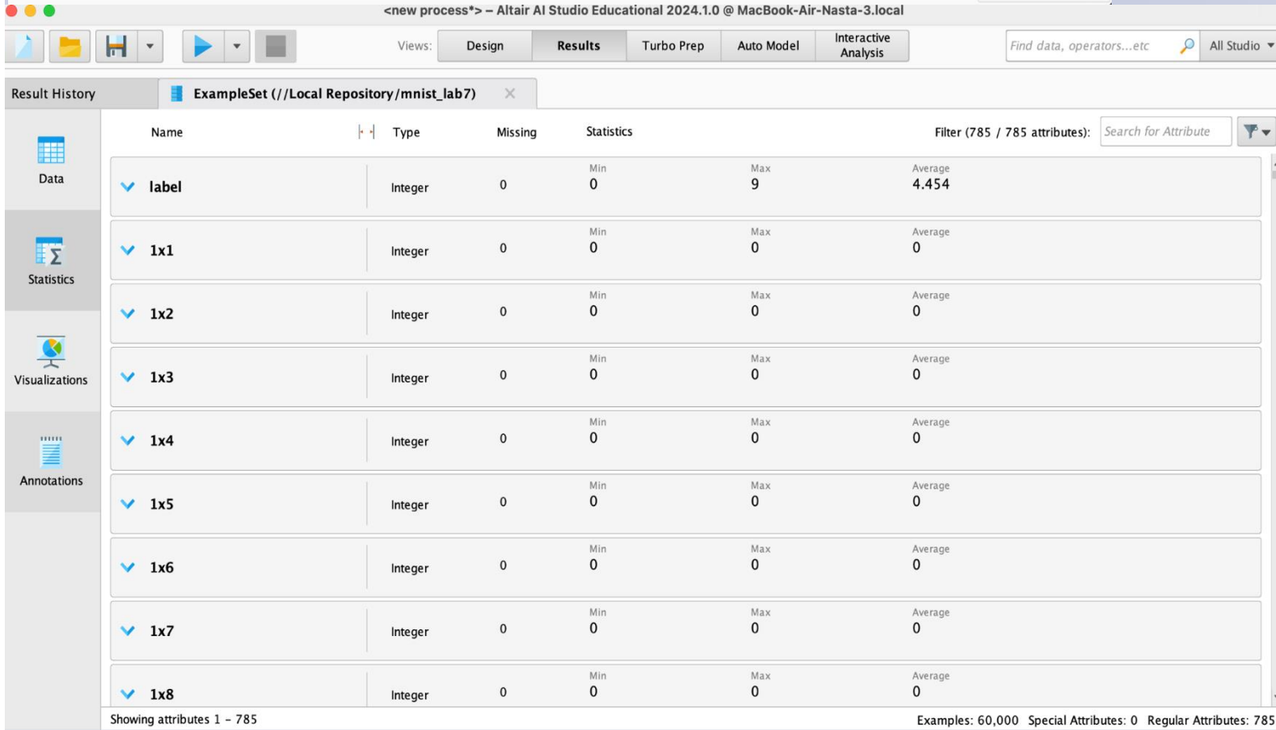
Будет рассмотрен набор MNIST, так как он прост и нагляден.

С его помощью можно продемонстрировать работу сети и быстро оценить эффективность различных алгоритмов.

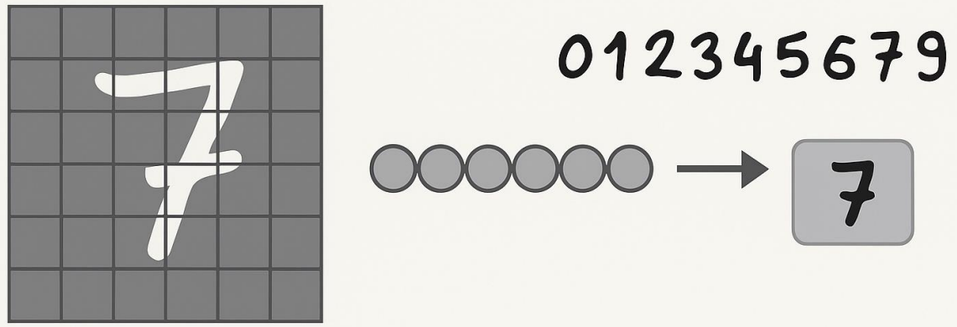
Работа с данными в RapidMiner

В RapidMiner данные MNIST загружаются через оператор Read CSV. После загрузки набор имеет 785 столбцов (784 признака пикселей и 1 столбец меток классов).





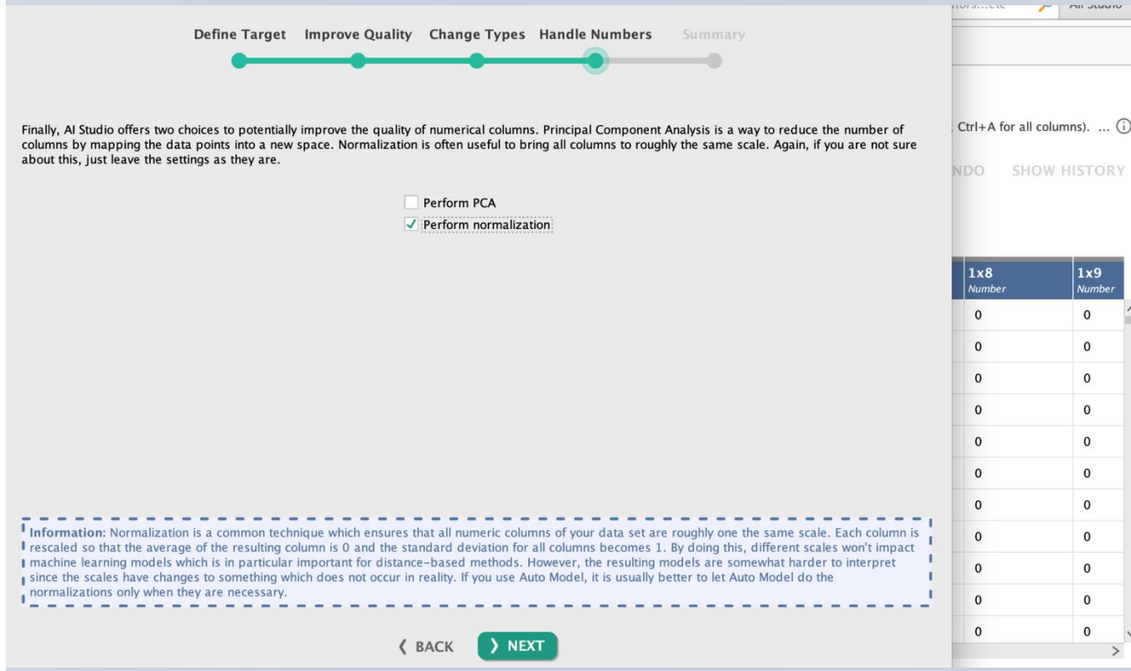
Структура данных MNIST



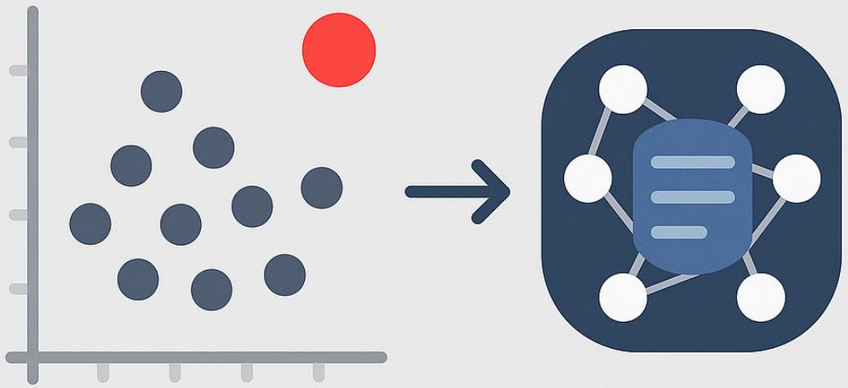
Каждое изображение представлено в виде вектора значений пикселей от 0 до 255. Целевая переменная (label) хранит классы цифр, отнесённые к каждому изображению.

Предобработка данных

Перед обучением сети необходима нормализация пикселей (до диапазона 0–1). Это повышает стабильность и скорость обучения. Дополнительно проверяется тип данных для корректной работы моделей.



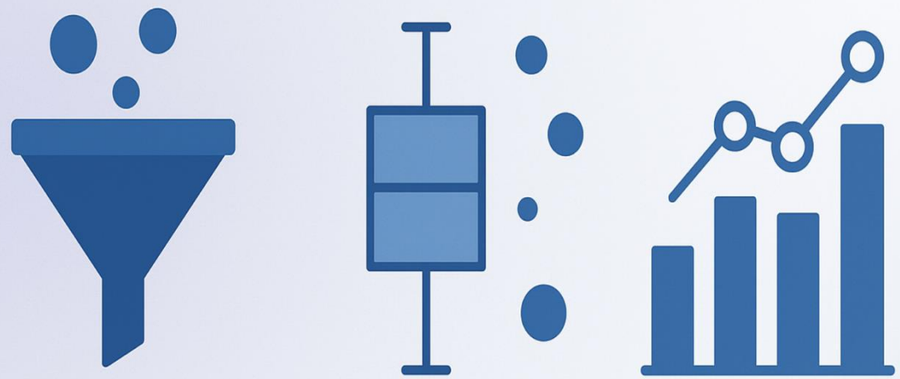
Удаление выбросов



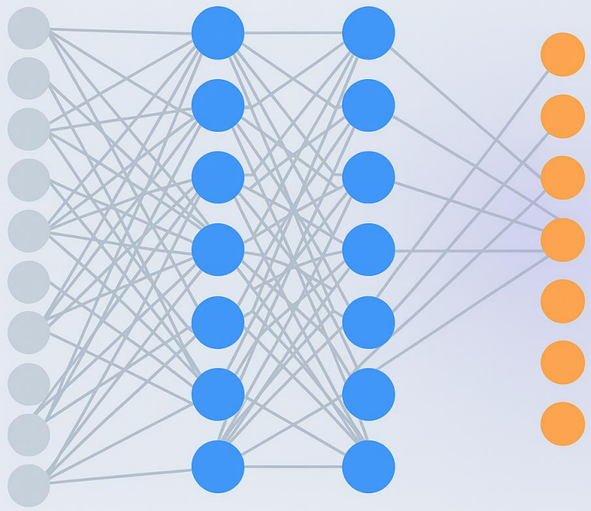
В реальных задачах могут встречаться выбросы — данные, значительно отличающиеся от остальных. В MNIST это не критично, но в других задачах необходимо проводить фильтрацию выбросов.

Роль TurboPrep в предобработке

TurboPrep в RapidMiner облегчает предварительную обработку данных: позволяет быстро нормализовать признаки, фильтровать выбросы и визуализировать распределения классов.



Архитектура полносвязной сети (FCN)

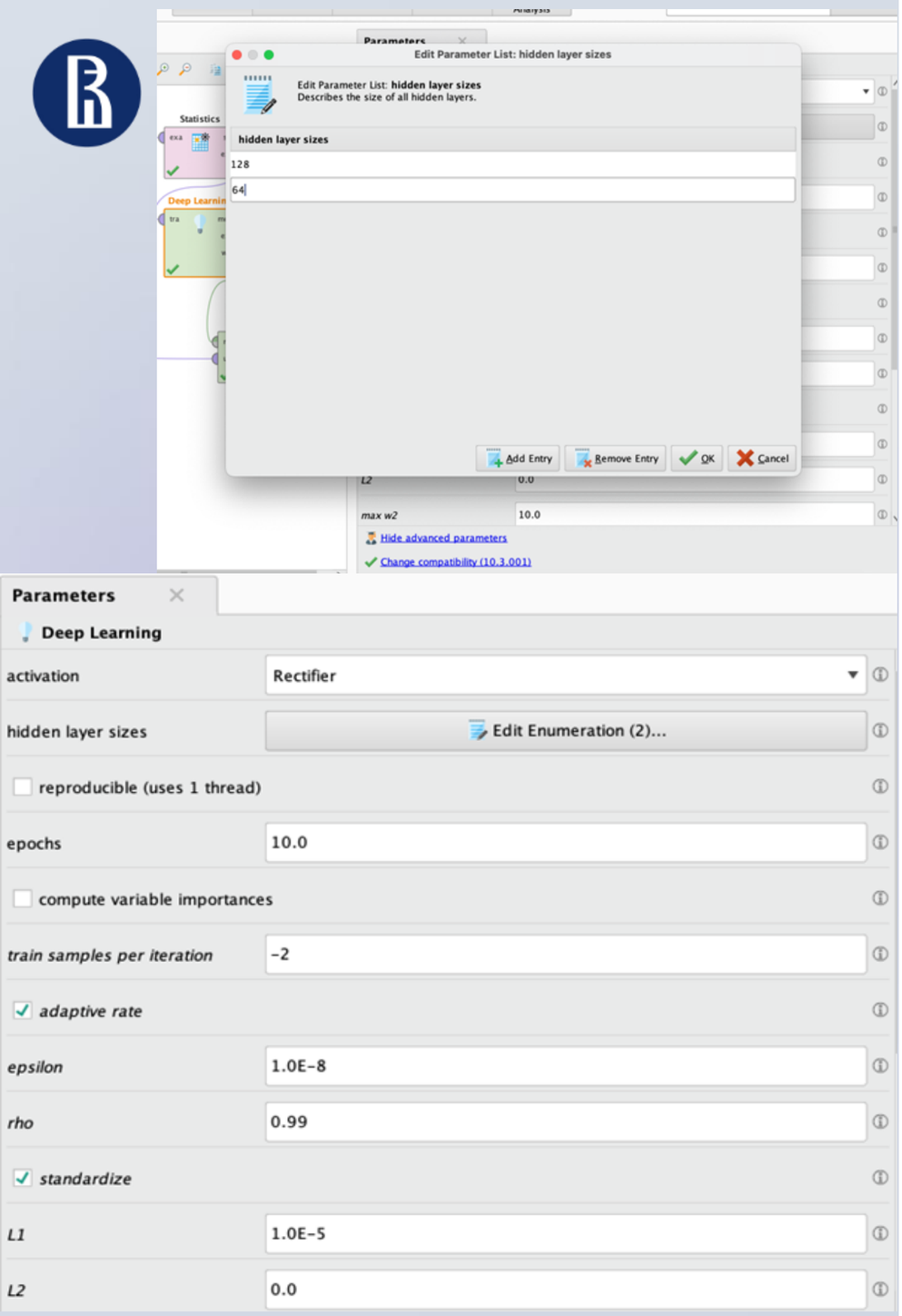


FCN состоит из:

- входного слоя (784 нейрона по числу пикселей);
- скрытых слоёв с несколькими нейронами;
- выходного слоя с 10 нейронами для классов (функция активации — Softmax).

Выбор функции активации

Наиболее распространённые функции активации — ReLU и Tanh. ReLU предпочтительна за скорость обучения и простоту вычислений, Tanh иногда показывает большую точность на небольших наборах.

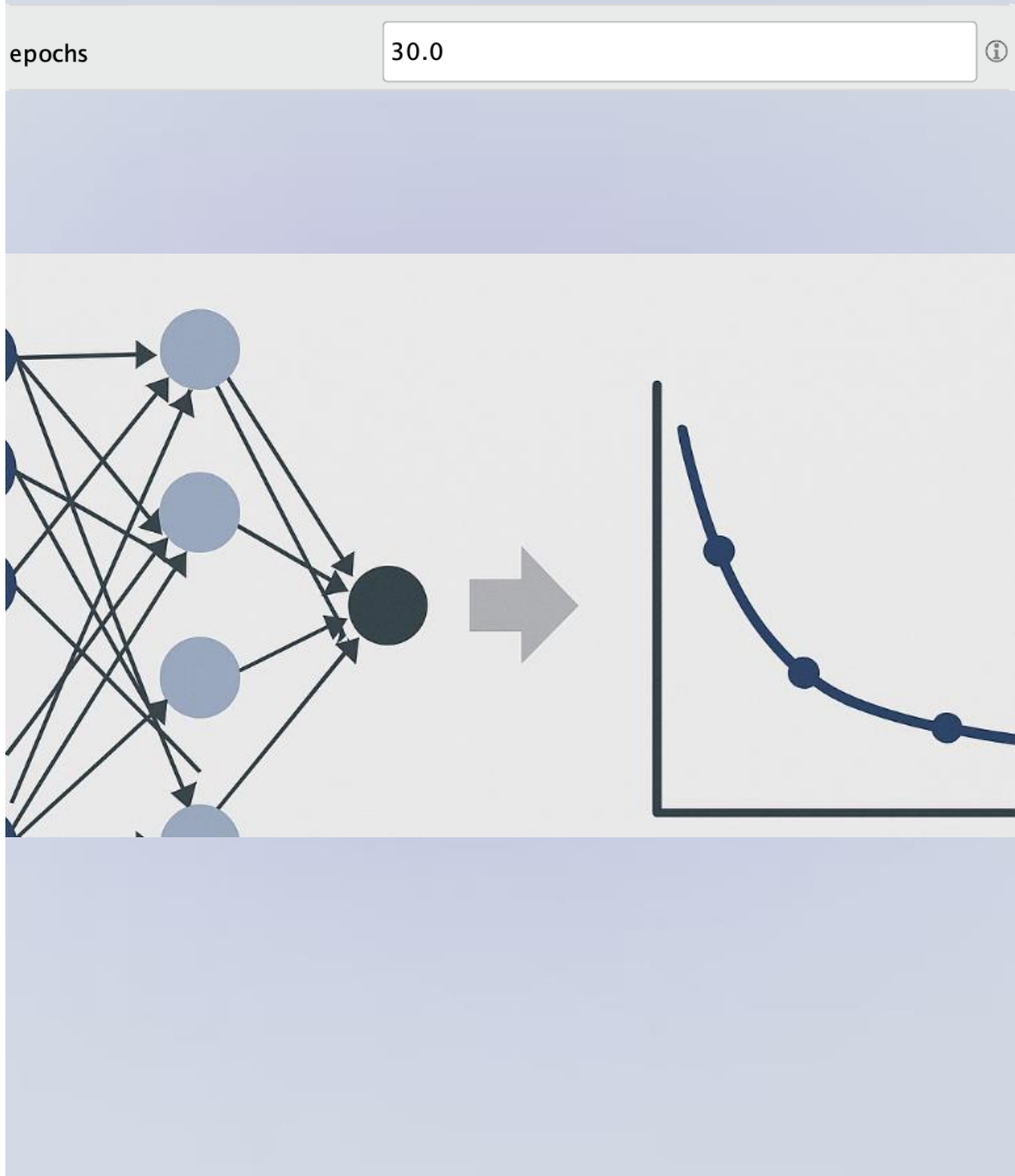


Настройки оператора Deep Learning

- Число нейронов в скрытых слоях (например, [128,64]).
- Функция активации (ReLU).
- Параметры оптимизации (adaptive rate, epsilon, rho).
- Регуляризация (L1, L2) для борьбы с переобучением.

Понятие эпох в обучении

Эпоха (epoch) — это один полный проход нейронной сети через весь набор данных. Обычно используются 10–30 эпох, увеличение числа эпох улучшает точность, но увеличивает риск переобучения.



Оценка качества обучения

Table View Plot View

accuracy: 97.44%

	true 5	true 0	true 4	true 1	true 9	true 2	true 3	true 6	true 7	true 8	class preci...
pred. 5	1587	2	0	2	4	1	29	3	0	15	96.59%
pred. 0	3	1759	0	0	3	10	4	9	1	5	98.05%
pred. 4	6	0	1715	3	15	4	1	5	6	4	97.50%
pred. 1	1	0	2	2008	1	4	2	3	5	6	98.82%
pred. 9	9	6	25	1	1677	2	8	0	16	9	95.66%
pred. 2	1	1	3	15	1	1774	19	1	7	8	96.94%
pred. 3	12	0	0	6	9	6	1736	1	1	9	97.53%
pred. 6	8	1	2	1	0	0	0	1783	0	7	98.95%
pred. 7	2	1	5	7	12	14	9	0	1828	3	97.18%
pred. 8	5	3	1	3	8	7	22	2	2	1673	96.93%
class recall	97.12%	99.21%	97.83%	98.14%	96.94%	97.37%	94.86%	98.67%	97.96%	96.20%	

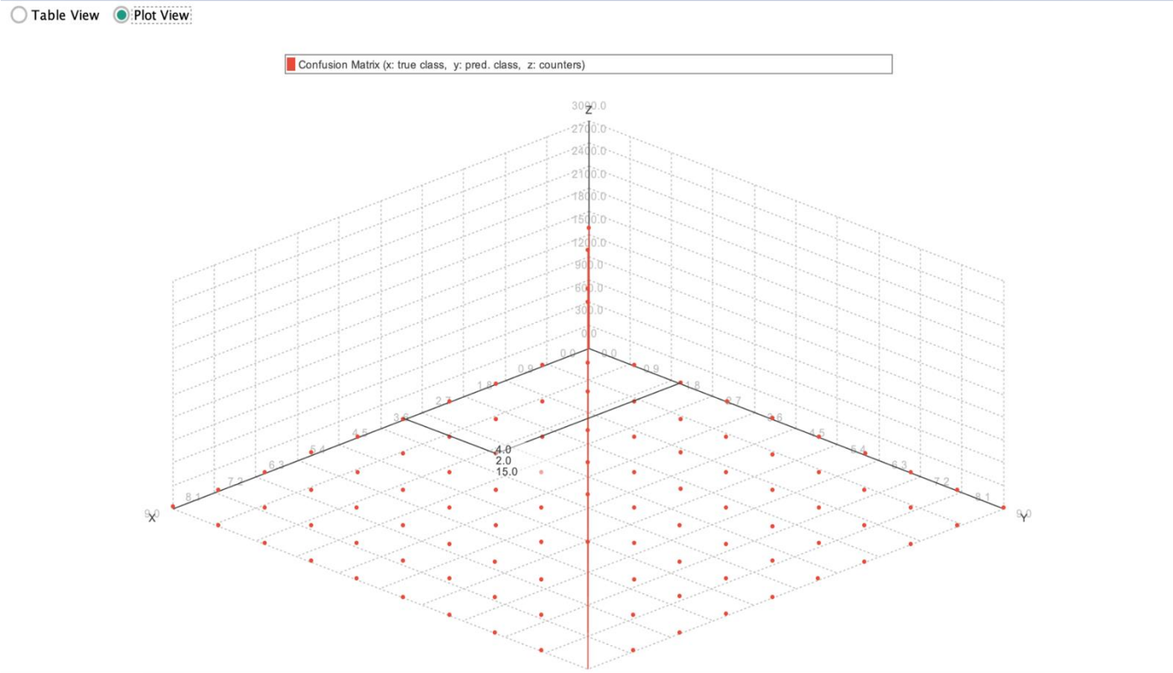
classification_error: 2.56%

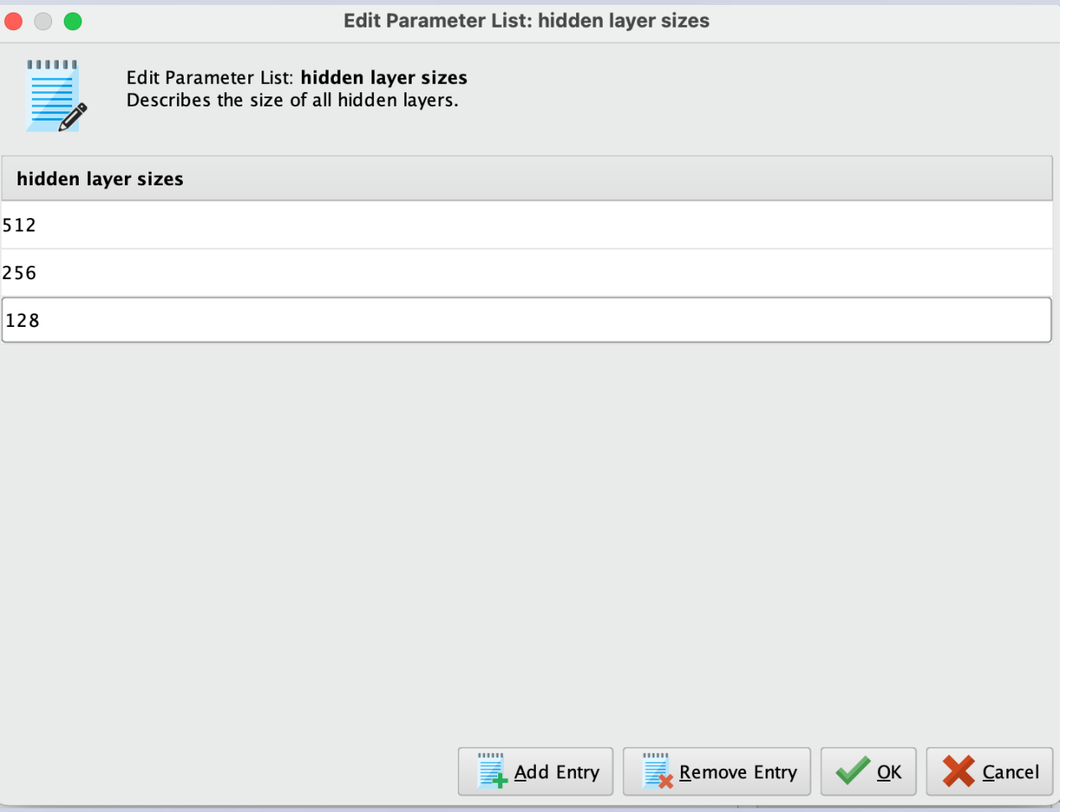
	true 5	true 0	true 4	true 1	true 9	true 2	true 3	true 6	true 7	true 8	class preci...
pred. 5	1587	2	0	2	4	1	29	3	0	15	96.59%
pred. 0	3	1759	0	0	3	10	4	9	1	5	98.05%
pred. 4	6	0	1715	3	15	4	1	5	6	4	97.50%
pred. 1	1	0	2	2008	1	4	2	3	5	6	98.82%
pred. 9	9	6	25	1	1677	2	8	0	16	9	95.66%
pred. 2	1	1	3	15	1	1774	19	1	7	8	96.94%
pred. 3	12	0	0	6	9	6	1736	1	1	9	97.53%
pred. 6	8	1	2	1	0	0	0	1783	0	7	98.95%
pred. 7	2	1	5	7	12	14	9	0	1828	3	97.18%
pred. 8	5	3	1	3	8	7	22	2	2	1673	96.93%
class recall	97.12%	99.21%	97.83%	98.14%	96.94%	97.37%	94.86%	98.67%	97.96%	96.20%	

RapidMiner позволяет оценивать модели через показатели: accuracy (точность), precision (точность положительных прогнозов), recall (полнота выявления классов), classification error (доля ошибок классификации).

Матрица ошибок (Confusion Matrix)

Матрица ошибок позволяет увидеть, какие цифры модель путает чаще всего. Это даёт возможность точечно улучшать архитектуру нейросети и параметры её обучения.



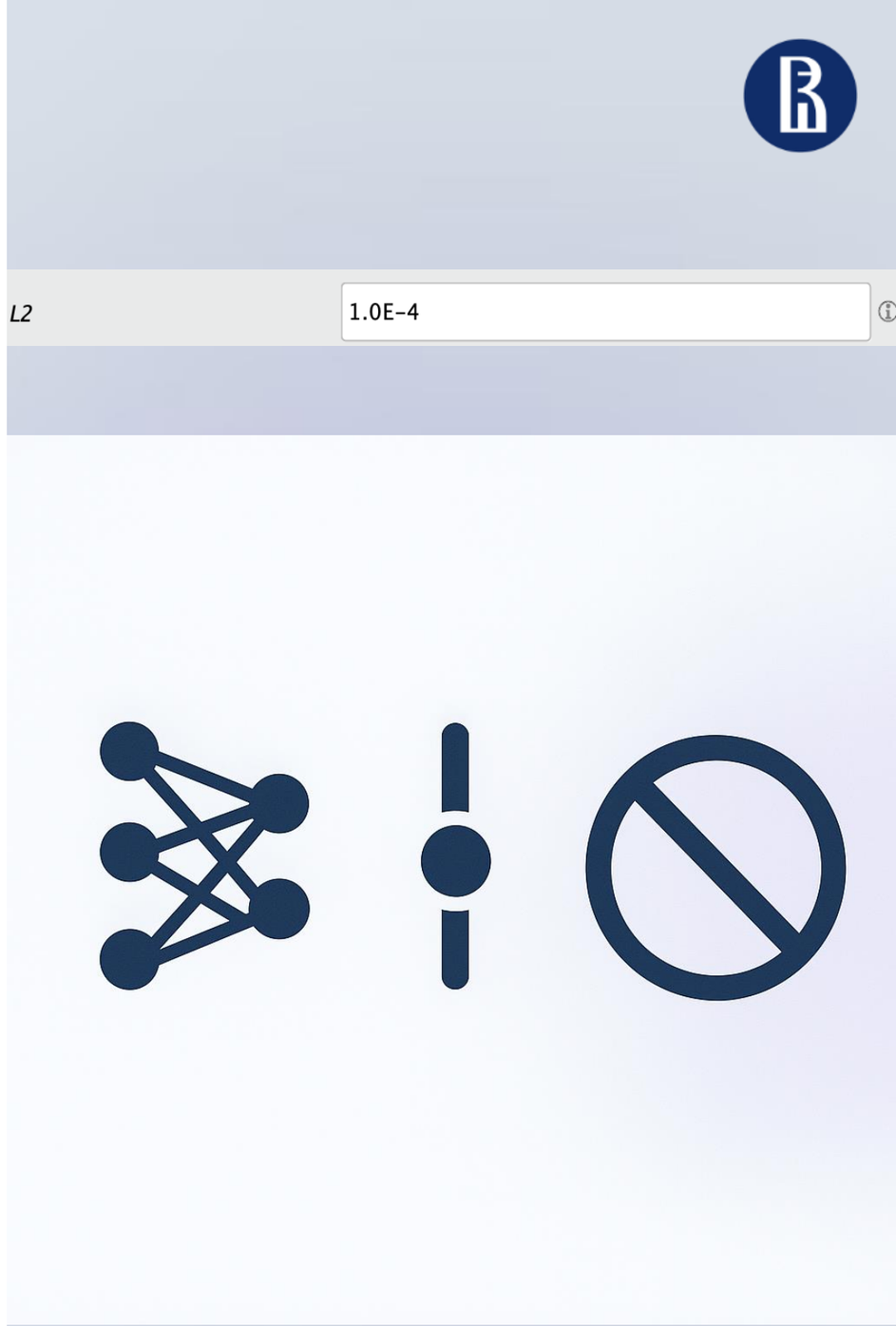


Эксперименты с архитектурой сети

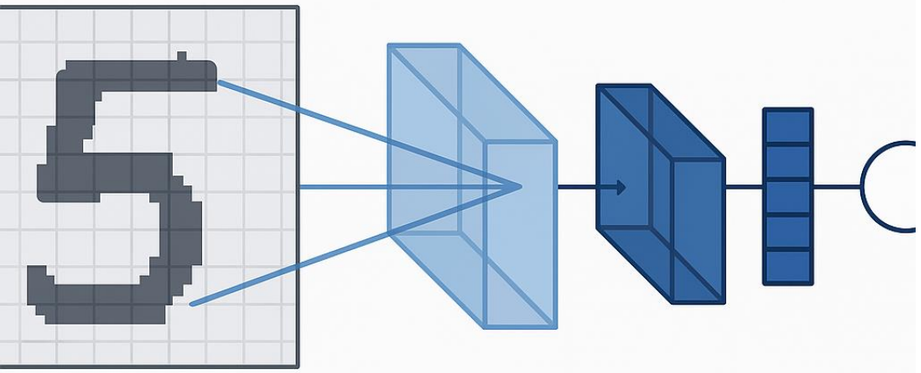
Изменяя число нейронов и слоёв (например, 128→256→512), можно повысить точность модели. Однако увеличение слоёв увеличивает время обучения и риск переобучения.

Эксперименты с регуляризацией

Регуляризация (L1, L2) ограничивает веса сети, предотвращая переобучение. Подбор параметров регуляризации (например, увеличение L2) помогает улучшать обобщающие свойства модели.



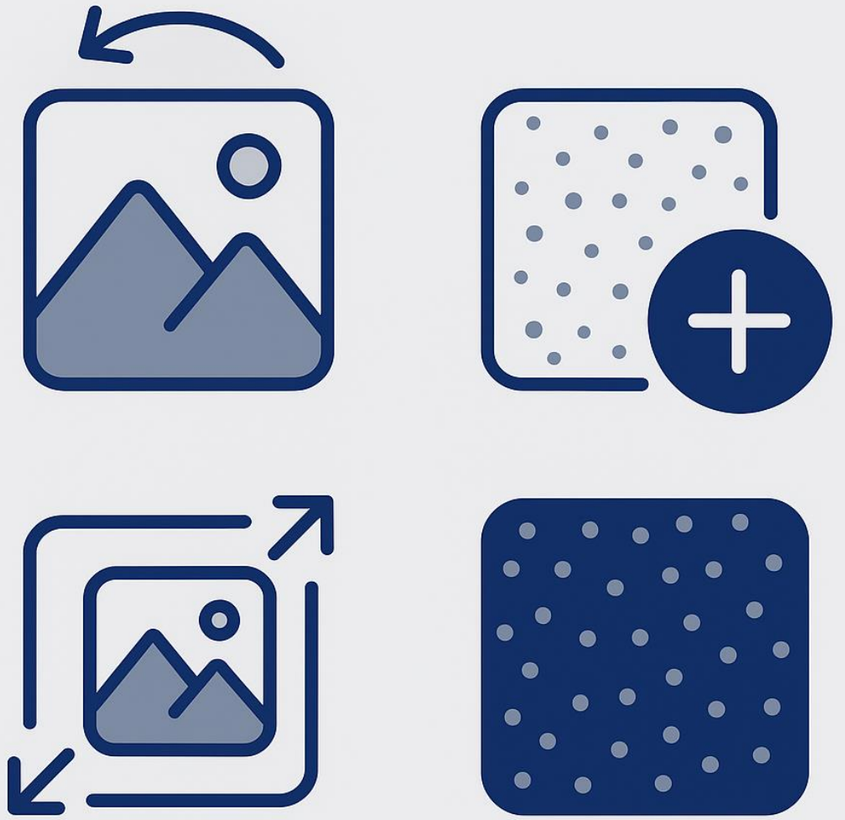
Сверточные нейронные сети (CNN)



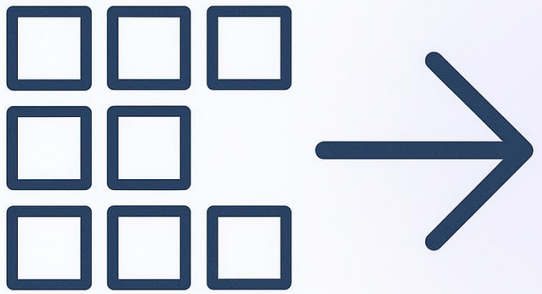
CNN эффективно используются для анализа изображений. Они автоматически извлекают важные признаки, достигая точности более 99% на MNIST. RapidMiner также поддерживает создание CNN.

Аугментация данных

Аугментация (вращение, добавление шума, масштабирование) увеличивает количество обучающих примеров и улучшает устойчивость нейросети к изменениям исходных изображений.



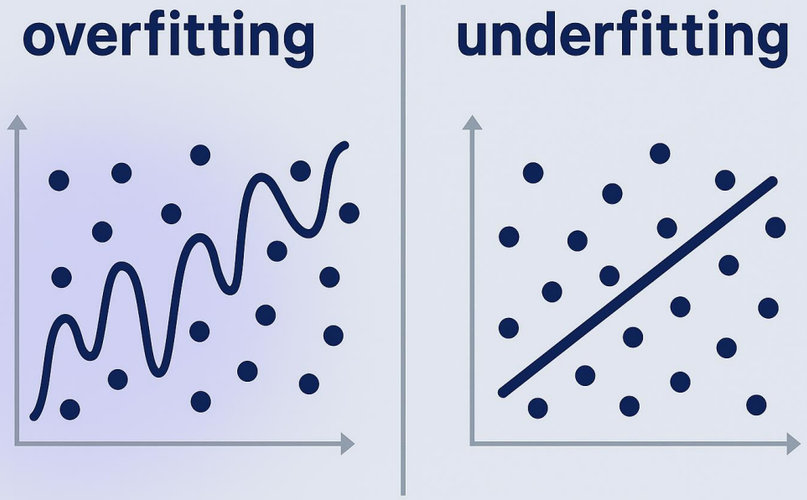
Подбор гиперпараметров (Grid Search)



Подбор гиперпараметров (количество слоёв, нейронов, скорость обучения) проводится автоматизировано, например, с помощью метода Grid Search, позволяя найти оптимальную архитектуру сети.

Проблемы переобучения и недообучения

- Переобучение: модель хорошо работает только на тренировочных данных.
- Недообучение: модель недостаточно обучена. Необходим баланс: правильный подбор слоёв, нейронов и эпох.

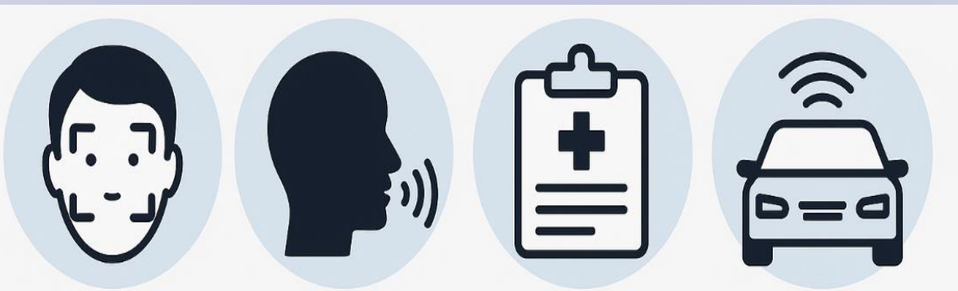


Использование GPU в обучении сетей

Графические процессоры (GPU) ускоряют обучение нейронных сетей, сокращая время вычислений. RapidMiner совместим с GPU, что значительно упрощает работу с крупными наборами данных.

Примеры применения Deep Learning

Deep Learning применяется в распознавании лиц и речи, анализе медицинских изображений, автопилотах, финансовых прогнозах и персонализированных рекомендациях, подтверждая универсальность технологии.



Заключение

RapidMiner позволяет изучить и эффективно применять глубокие нейросети для решения реальных задач без программирования, создавая мощные инструменты анализа изображений и данных в целом.