Ордена Трудового Красного Знамени
Федеральное государственное бюджетное
образовательное учреждение высшего образования
«Московский технический университет связи и информатики»

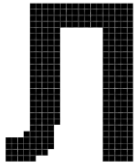
Зиядинов Вадим Валерьевич

Оптимизация помехоустойчивости и точности нейросетевого распознавания изображений

Москва – 2023

Актуальность темы исследований

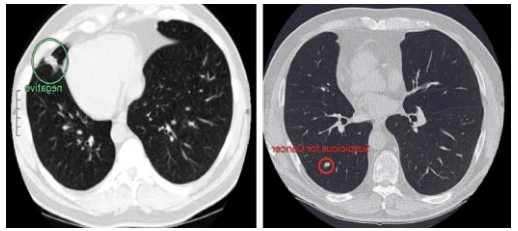
Распознавание символов



Распознавание рукописного текста

Распознавание автомобильных номеров

Распознавание патологий



Распознавание лиц

Выделение объектов интереса в видеопотоке

Подход – использование свёрточных нейронных сетей глубокого обучения

ТРУДНОСТИ:

1. Часто не обеспечивается приемлемая точность распознавания
2. Изображения с различной степенью искажения распознаются с разной точностью
3. Непонятно, как оценить оптимальность и робастность обученной нейронной сети

Современное состояние предметной области

Большинство исследований посвящено разработке новых архитектур и новым применениям сетей.

- точность распознавания изображений свёрточными сетями бывает низкой или недостаточной;
- на результаты работы нейронных сетей влияют искажения данных, в особенности высокочастотные искажения;
- не существует универсального подхода к оценке оптимальности и устойчивости обученной нейронной сети.

Существует несколько методов борьбы с чрезмерным снижением качества распознавания искажённых изображений, в частности,

1. Метод «Защитная дистилляция» предполагает использование двух или более сетей; эффективно для некоторых неопределенных угроз, но неэффективен против тонкой настройки высокочастотных атак;

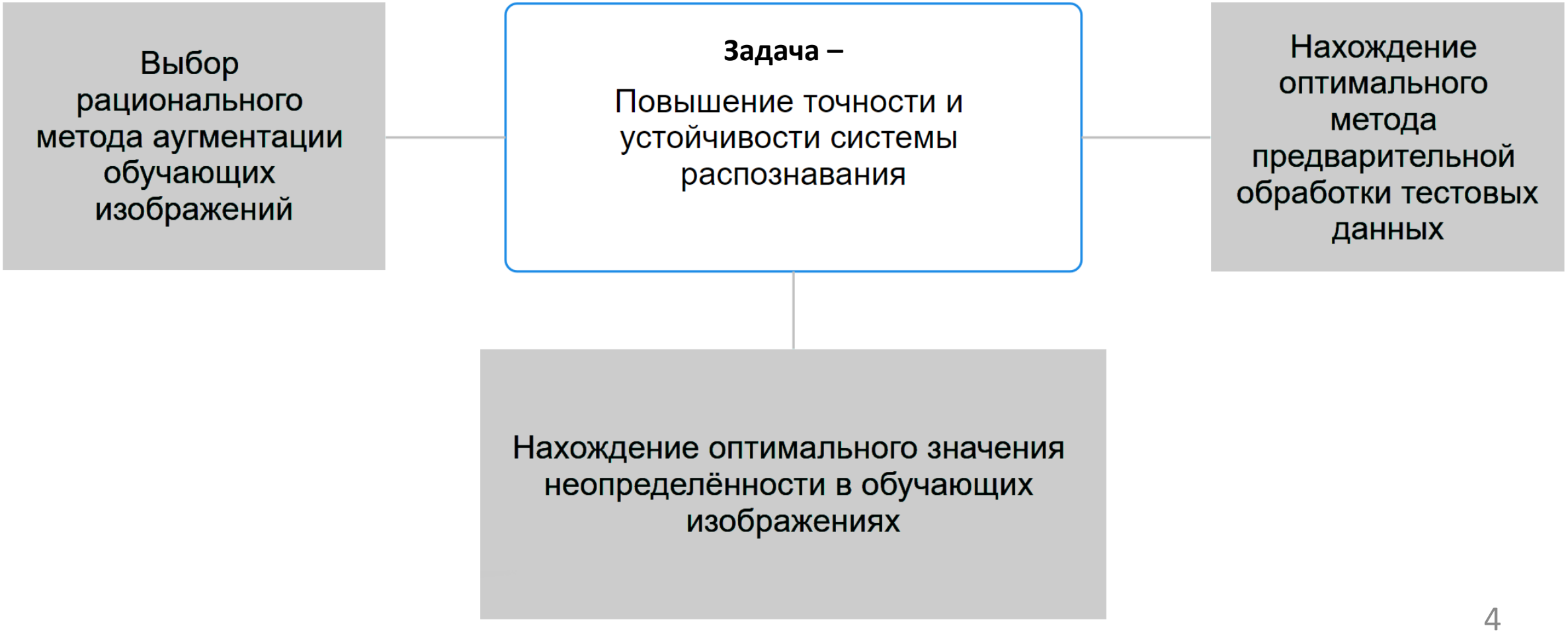
2. Градиентная регуляризация – трудно реализуема; количественная оценка стойкости к высокочастотным искажениям отсутствует;

3. Денойзеры - используются в основном для визуального улучшения качества изображения или повышения качества; не доказана эффективность против высокочастотных искажений; количественная оценка устойчивости недостаточна;

4. Генеративные состязательные сети эффективны для обнаружения состязательного шума; дискриминатор (важная часть GAN) также уязвим для тех же состязательных атак.

Цели и задачи

Цель диссертационного исследования – обеспечить повышение точности распознавания свёрточной нейронной сетью изображений при наличии в них искажений различной физической природы



Научная новизна

1. Доказательство существования оптимального значения неопределённости в *обучающих* изображениях, позволяющего достичь максимальной интегральной точности распознавания *тестовых* изображений с различными искажениями при заданном пороге минимальной точности распознавания получено автором впервые [1, 2].

2. Подход к повышению точности распознавания изображений, подвергнутых состязательным атакам, на основе низкочастотной фильтрации изображений в совокупности с предварительным обучением нейронной сети размытыми изображениями, предложен автором впервые [3].

[1] Ziyadinov V., Tereshonok M. Noise Immunity and Robustness Study of Image Recognition Using a Convolutional Neural Network // Sensors. 2022. Vol. 22, № 3. P. 1241.

[2] Ziyadinov V.V., Tereshonok M.V. Neural Network Image Recognition Robustness with Different Augmentation Methods // 2022 Systems of Signal Synchronization, Generating and Processing in Telecommunications (SYNCHROINFO). Arkhangelsk, Russian Federation: IEEE, 2022. P. 1–4.

[3] Ziyadinov, V.; Tereshonok, M. Low-Pass Image Filtering to Achieve Adversarial Robustness. Sensors **2023**, *23*, 9032. https://doi.org/10.3390/s23229032

Математическая постановка задачи диссертационного исследования

1) Нахождение оптимального значения неопределённости в обучающих изображениях

$$U_{TRopt} = \arg\left(\max\left(\sum_{U_{TS=0}}^{U_{TSmax}} P(U_{TS}, U_{TR})\right)\right)$$, где U_{TR} – значение неопределённости в обучающем наборе данных, U_{TS} – значение неопределённости в тестовом наборе данных

2) Выбор рационального метода аугментации обучающих изображений

$$p(U_{TR})_{opt} = \arg\left(\max\left(\sum_{U_{TS=0}}^{U_{TSmax}} P(U_{TS}, p(U_{TR}))\right)\right)$$, где $p(U_{TR})$ – закон распределения значений неопределённости в обучающем наборе данных

3) Нахождение оптимального метода предварительной обработки тестовых данных

$$F_{TSopt} = \arg\left(\max\left(\sum_{U_{TS=0}}^{U_{TSmax}} P(F_{TS}, U_{TS})\right)\right)$$, где F_{TS} – функция обработки тестовых данных

Положения, выносимые на защиту

1. Существует оптимальное значение неопределённости в *обучающих* изображениях, позволяющее достичь максимальной интегральной точности распознавания *тестовых* изображений с различными искажениями.

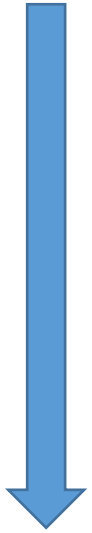
2. Оптимальное значение неопределённости в *обучающих* изображениях может быть оценено методом статистического моделирования. Использование обучающего набора данных с оптимальным значением неопределённости позволяет снизить вероятность ошибки распознавания в среднем в 20 раз по сравнению с использованием исходного набора изображений без дополнительных искажений.

3. Существует оптимальный способ аугментации *обучающих* изображений, позволяющий повысить интегральную точность распознавания *тестовых* изображений с различными искажениями при заданном пороге минимальной точности распознавания, без увеличения объёма обучающей выборки. Использование оптимального способа аугментации позволяет снизить вероятность ошибки распознавания в среднем на 60 % по сравнению с использованием исходного набора изображений без дополнительных искажений.

4. Низкочастотная фильтрация изображений в совокупности с предварительным обучением нейронной сети размытыми изображениями позволяет в среднем в 8,8 раз снизить вероятность ошибки распознавания изображений, подвергнутых состязательным атакам, по сравнению с использованием исходного набора изображений без дополнительных искажений.

АНАЛИЗ ВНЕШНИХ ХАРАКТЕРИСТИК СИСТЕМЫ ОБУЧЕНИЯ-РАСПОЗНАВАНИЯ

Возрастание информативности с точки зрения оценки робастности и оптимальности системы обучения-распознавания



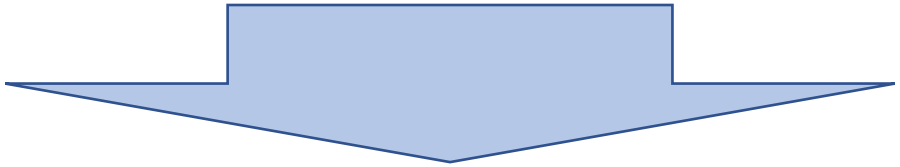
1. Точность распознавания фиксированной тестовой выборки сетью, обученной на фиксированной обучающей выборке – одно число, скаляр P_0

$$P_0 = \frac{M_{correct}}{M_{total}}$$

, где $M_{correct}$ – количество правильно распознанных изображений, M_{total} – общее количество изображений

2. Функция зависимости точности распознавания тестовых выборок от их неопределённости сетью, обученной на фиксированной обучающей выборке – одномерный массив $P(U_{TS})$

3. Функция зависимости точности распознавания тестовых выборок от их неопределённости и от неопределённости обучающих выборок – двумерный массив $P(U_{TR}; U_{TS})$



Зная $P(U_{TR}; U_{TS})$, можно определить $P(U_{TR})$ и P_0:

$$P(U_{TS}) = \frac{1}{N_{TR}} \cdot \sum_{U_{TR}} P(U_{TR}; U_{TS});$$

$$P_0 = \frac{1}{N_{TS}} \cdot \sum_{U_{TS}} P(U_{TS}),$$

где N_{TR} - количество наборов данных с различными значениями неопределенности для обучения U_{TR}, N_{TS} - количество наборов данных с различными значениями неопределенности тестовых данных U_{TS}.

Первое защищаемое положение

Существует **оптимальное** значение неопределённости в ***обучающих*** изображениях, позволяющее достичь **максимальной интегральной точности** распознавания ***тестовых*** изображений с **различными искажениями**.

План исследования по оценке внешних характеристик системы обучения-распознавания

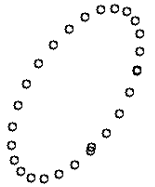
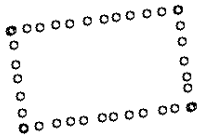
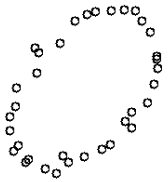
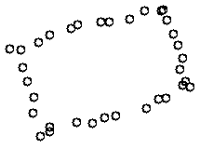
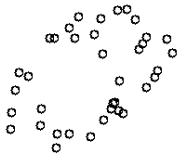
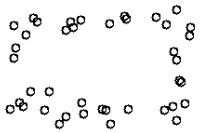
1. Выбрать модель изображений, удобную для экспериментов – подходят облака точек различных форм

2. На выбранной модели сгенерировать множество изображений для обучения и распознавания

3. Определить зависимость точности распознавания изображений от степени их искажения

4. Найти способ оптимизировать точность распознавания изображений

ПРИМЕР МОДЕЛИ:

	Эллипс	Прямоугольник
Низкая степень искажения		
Средняя степень искажения		
Высокая степень искажения		

Параметр, определяющий степень неопределённости

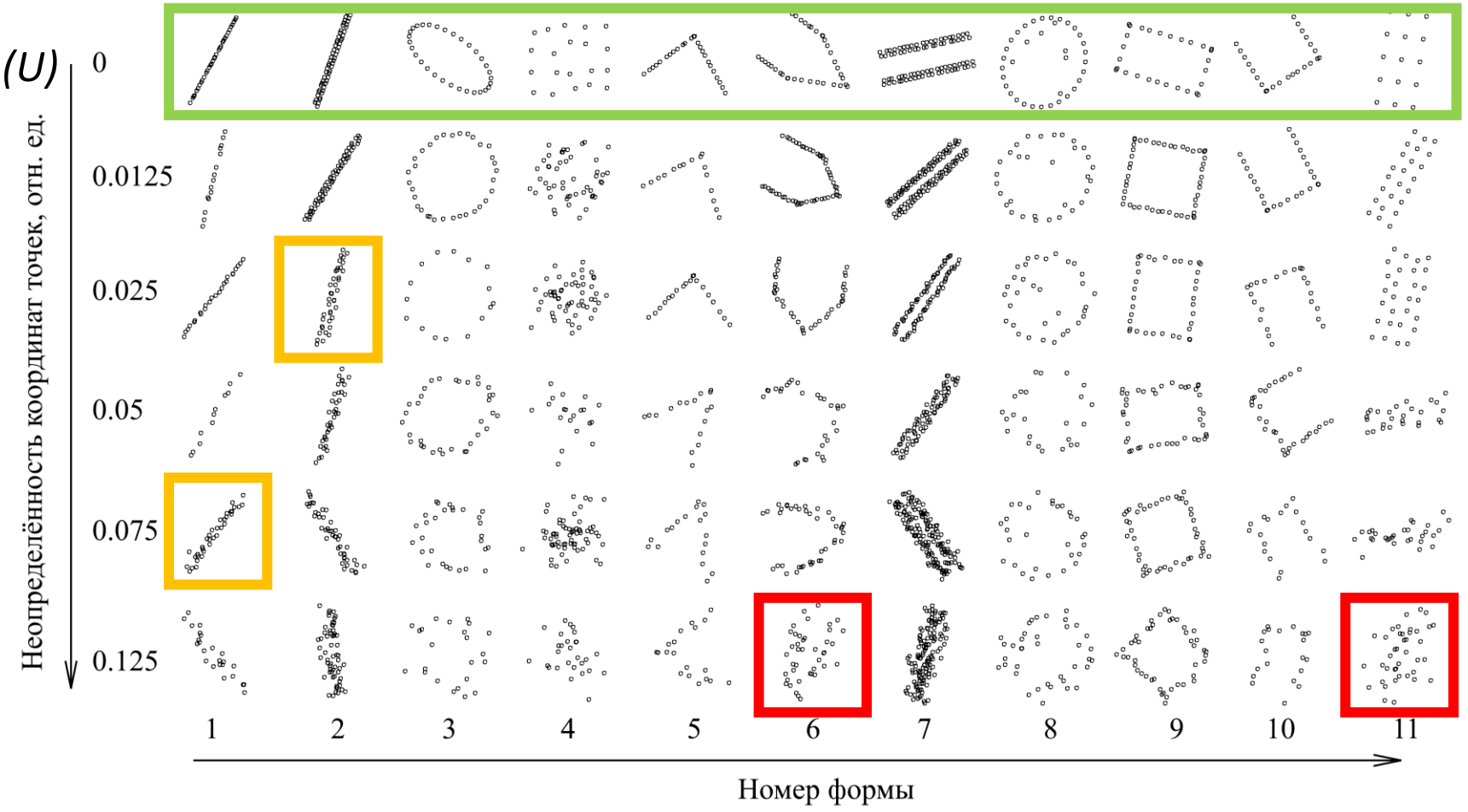
$U = \frac{d}{a}$, где d - среднеквадратическое отклонение положения точек, a - максимальный линейный размер всей фигуры.

Ziyadinov V.V., Tereshonok M.V., Moscow Technical University of Communications and Informatics. MATHEMATICAL MODELS AND RECOGNITION METHODS FOR MOBILE SUBSCRIBERS MUTUAL PLACEMENT // T-Comm. 2021. Vol. 15, № 4. P. 49–56.

Примеры сгенерированных изображений с разной степенью искажения

Задача: обеспечение корректного распознавания искажённых изображений

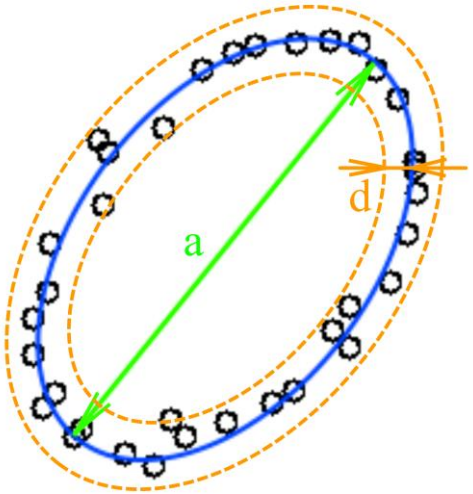
Пример: распознавание изображений с низкой плотностью точек, образующих скопления различной формы

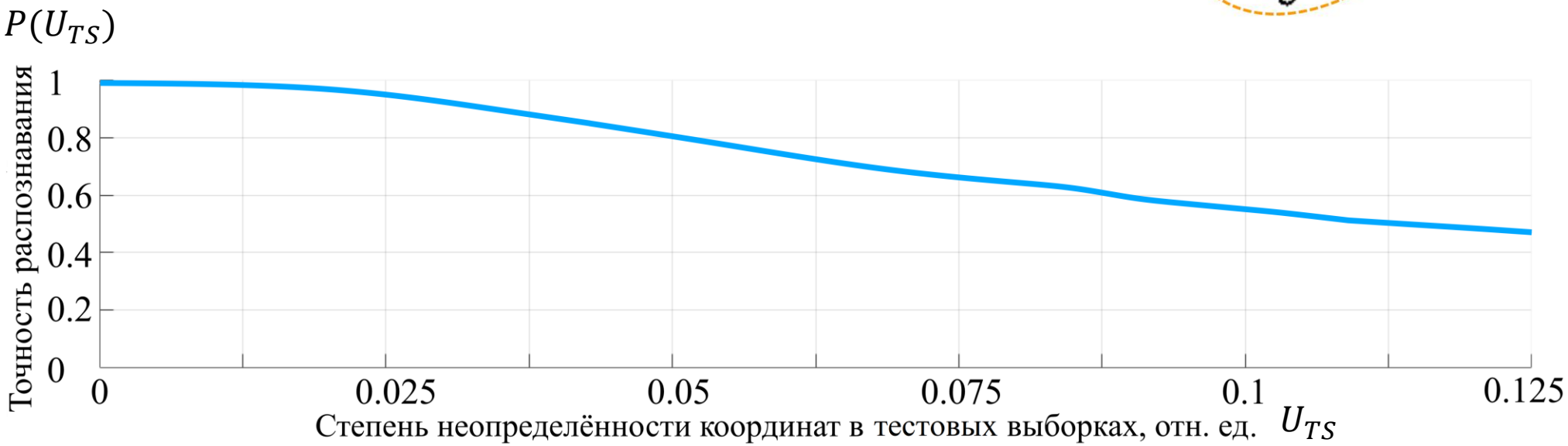


Видно, что неопределённость координат отдельных точек искажает изображение, однако формы скоплений сохраняют свои характерные черты

Способ оценки зависимости качества распознавания от неопределённости в тестовой выборке

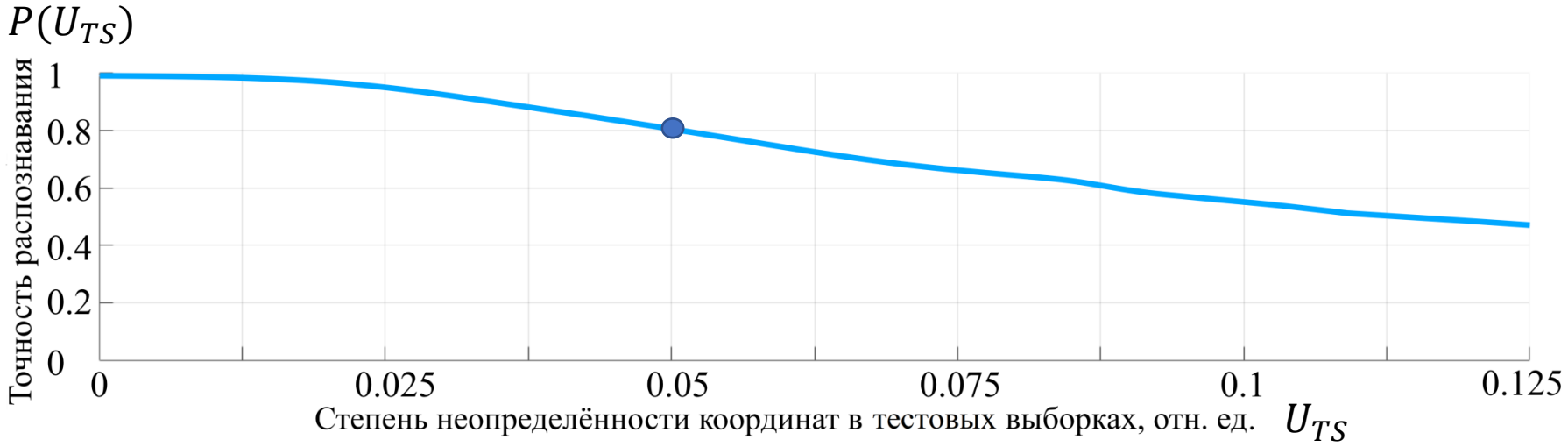
1. Сгенерировать обучающую выборку
2. Обучить нейронную сеть
3. Сгенерировать множество тестовых выборок с различной неопределённостью $U_{TS} = d/a$
4. Распознать все тестовые выборки и получить массив точности распознавания в зависимости от неопределённости $P(U_{TS})$



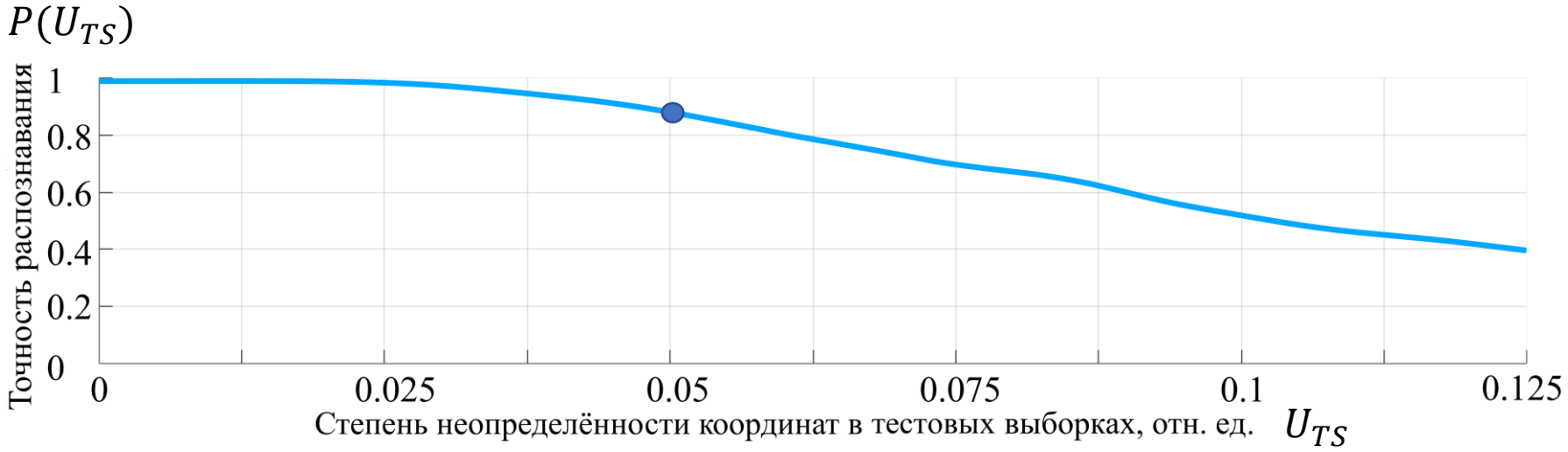


ИЗМЕНЕНИЕ КАЧЕСТВА РАСПОЗНАВАНИЯ ПРИ ВНЕСЕНИИ НЕОПРЕДЕЛЁННОСТИ В ОБУЧАЮЩУЮ ВЫБОРКУ

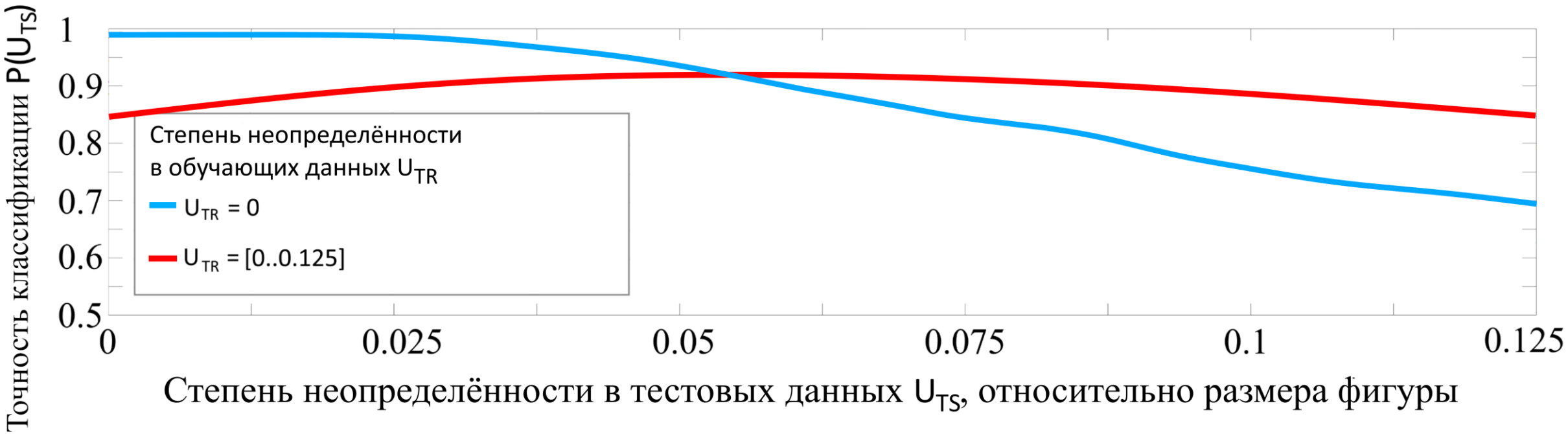
Обучение проведено на идеальных примерах (неопределённость равна нулю)



Обучение проведено на выборке со среднеквадратическим отклонением случайного разброса точек $U=d/a$=0.025, где *a* - максимальный линейный размер всей фигуры, *d* – среднеквадратическое отклонение точек



ИЗМЕНЕНИЕ ТОЧНОСТИ РАСПОЗНАВАНИЯ ПРИ РАЗЛИЧНОМ УРОВНЕ НЕОПРЕДЕЛЁННОСТИ В ОБУЧАЮЩЕЙ ВЫБОРКЕ

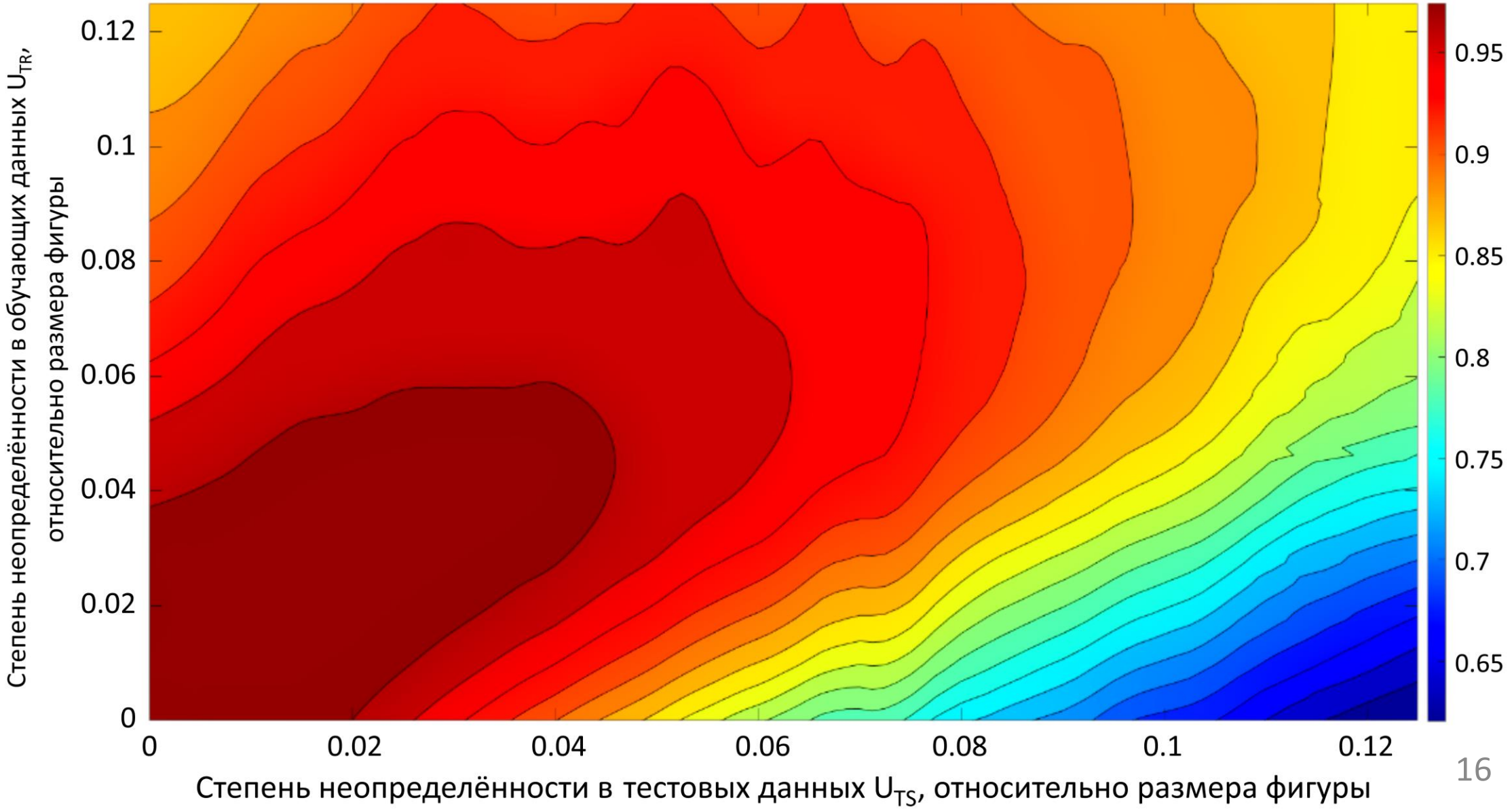


Анализ графиков показывает, что с ростом неопределённости в обучающих данных растёт точность распознавания данных с большой неопределённостью и падает точность распознавания данных с малой неопределённостью

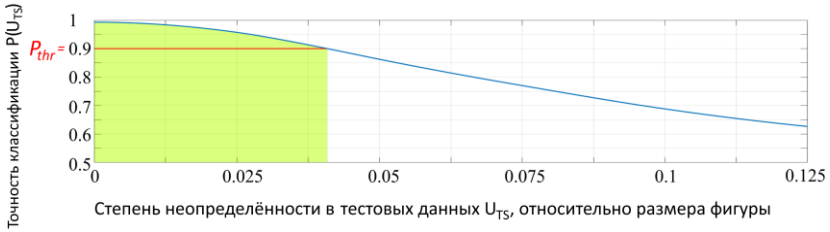
Второе защищаемое положение

Оптимальное значение неопределённости в ***обучающих*** изображениях **может быть оценено** методом статистического моделирования. Использование обучающего набора данных с оптимальным значением неопределённости позволяет снизить вероятность ошибки распознавания в среднем в 20 раз по сравнению с использованием исходного набора изображений без дополнительных искажений.

ГРАФИК ЗАВИСИМОСТИ ТОЧНОСТИ РАСПОЗНАВАНИЯ ИЗОБРАЖЕНИЙ ОТ СТЕПЕНИ НЕОПРЕДЕЛЁННОСТИ В ТЕСТОВЫХ И ОБУЧАЮЩИХ ДАННЫХ U_{TR} И U_{TS}



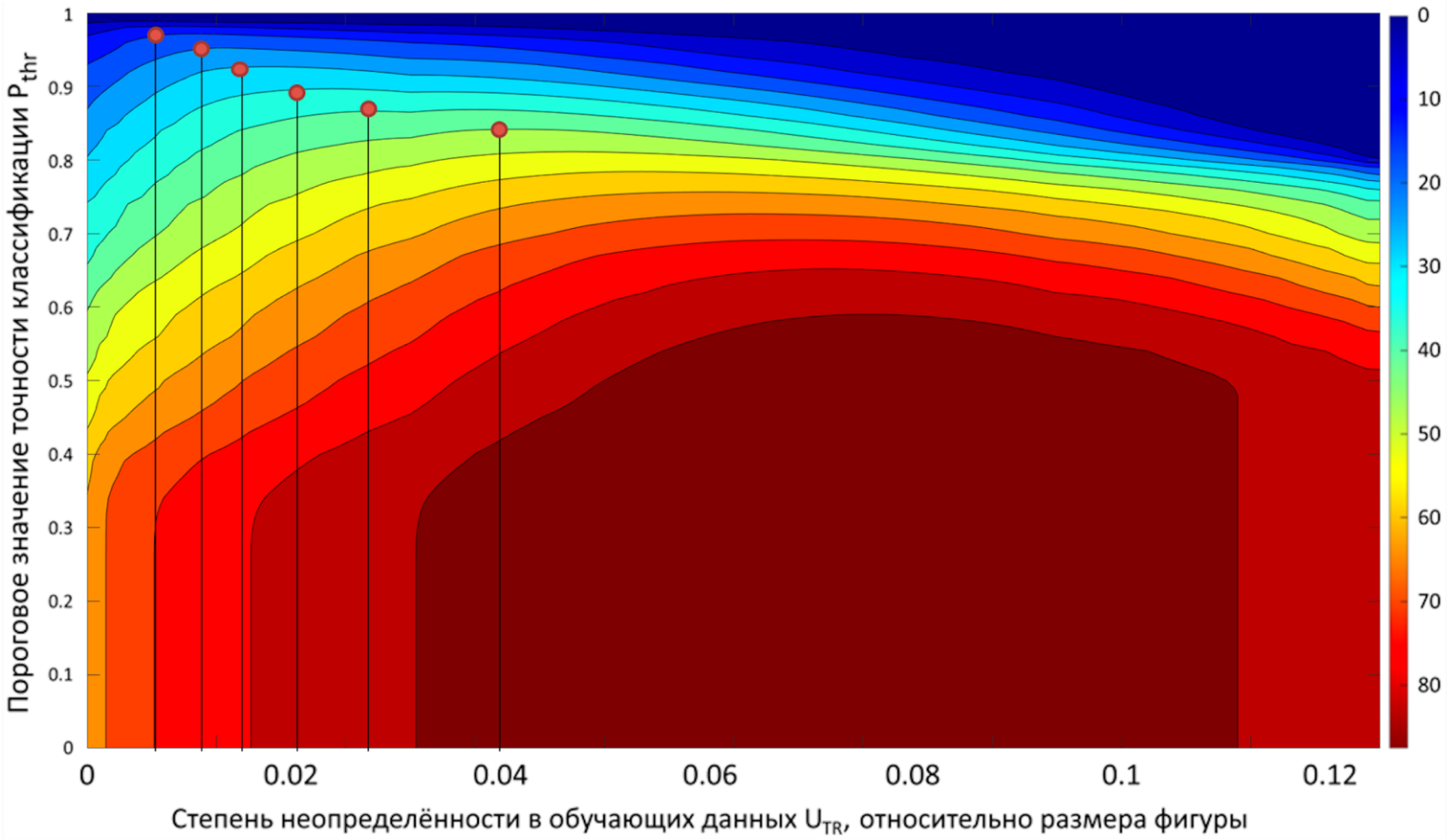
$$Q(P_{thr}) = \sum_{U_{TS}=U_{TS}^{\min},P\geq P_{thr}}^{U_{TS}=U_{TS}^{\max},P\geq P_{thr}} P(U_{TS})$$



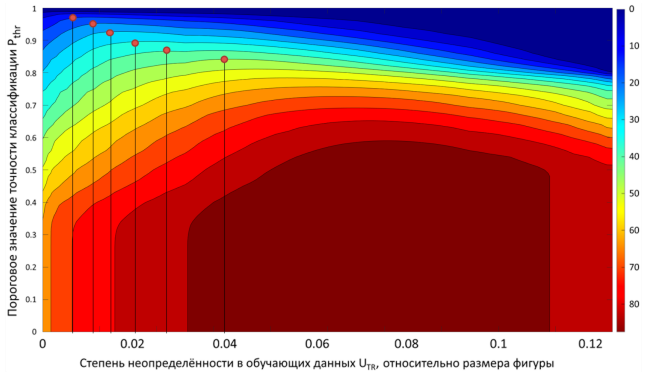
Качество работы системы оценивается:

- с точки зрения максимально возможной точности классификации
- с точки зрения устойчивости системы к неопределенности

$$Q(U_{TR};P_{thr}) = \sum_{U_{TS}=U_{TS}^{\min},P\geq P_{thr}}^{U_{TS}=U_{TS}^{\max},P\geq P_{thr}} P(U_{TR};U_{TS})$$

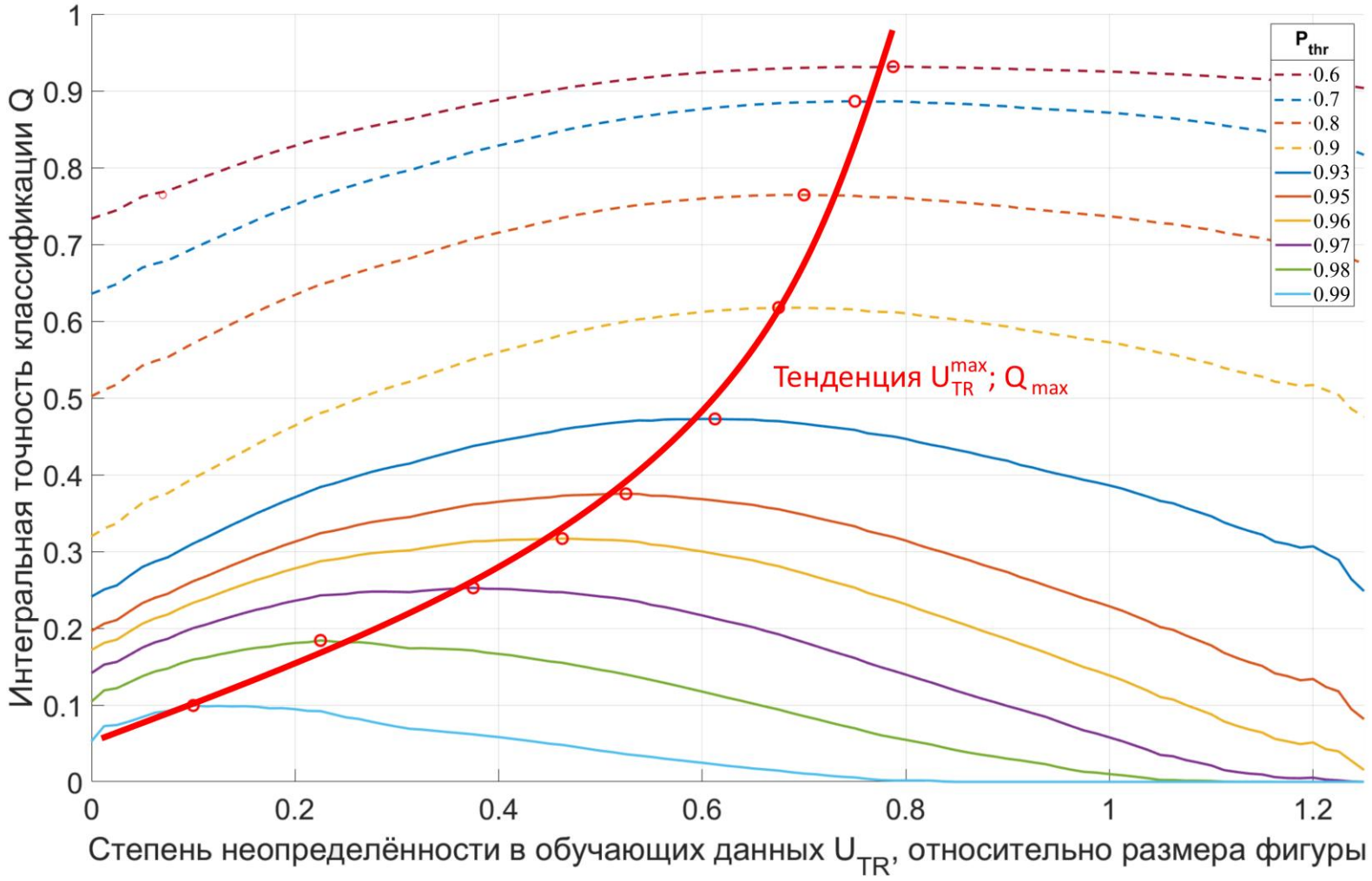


Оптимальное значение неопределённости в обучающих данных

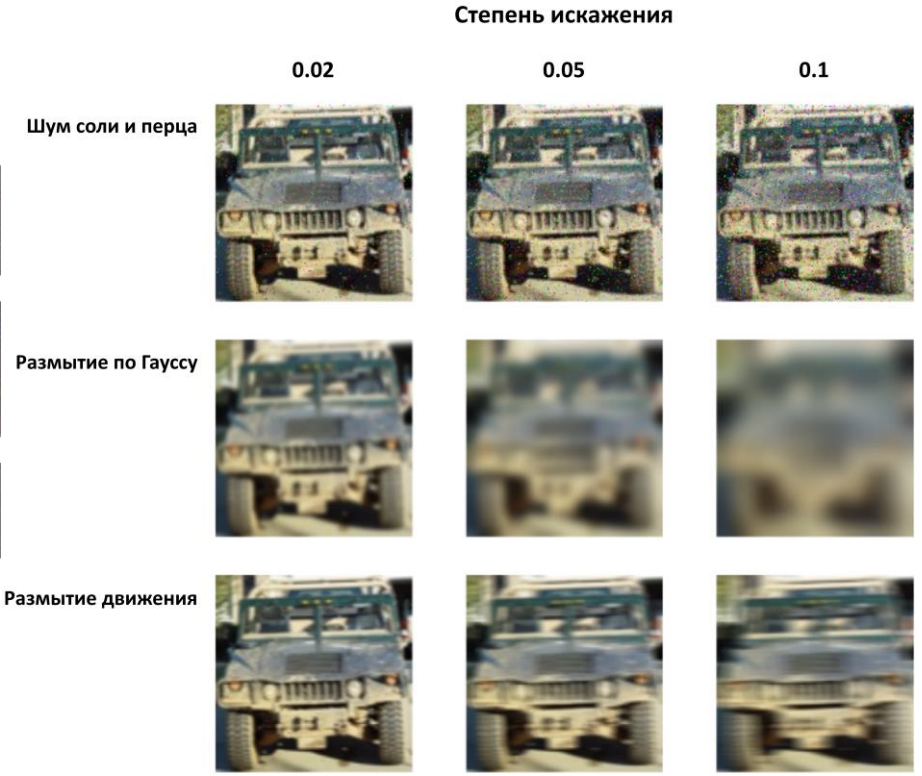


Обучение сети с оптимальным значением U_{TR} для фиксированного значения P_{thr} значительно повышает интегральную точность распознавания по сравнению с обучением сети на идеальном наборе данных ($U_{TR} = 0$).

Например, для P_{thr} = 0,9 значение Q_{max} превышает Q_0 на 94% (Q_{max} = 0,62 получено при U_{TR} = 0,068, а Q_0 = 0,32 - при U_{TR} = 0).



ОБУЧЕНИЕ СВЁРТОЧНЫХ НЕЙРОННЫХ СЕТЕЙ НА ЗАШУМЛЕННЫХ ЕСТЕСТВЕННЫХ ИЗОБРАЖЕНИЯХ



Для АБГШ ***U = σ / DR***, *где σ – среднеквадратичное отклонение значений (яркостей) пикселей.*

Для шума соли и перца ***U = E / (h·w)***, *где E – количество искаженных пикселей,* ***h*** *– разрешение по высоте,* ***w*** *- разрешение по ширине.*

Для размытия по Гауссу и размытия движения ***U = σ / min(h, w)***, *где* ***σ*** *– среднеквадратичное отклонение фильтра Гаусса,* ***h*** *– разрешение по высоте,* ***w*** *- разрешение по ширине.*

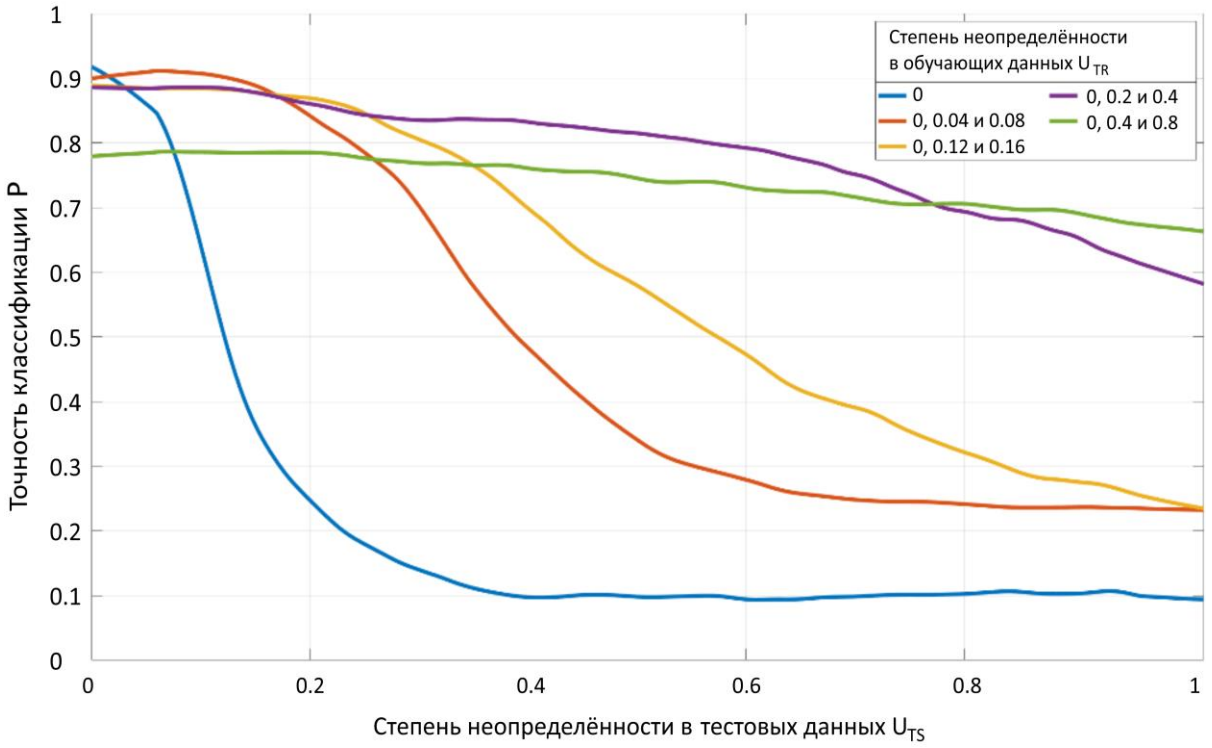
НАБОРЫ ДАННЫХ ДЛЯ ОБУЧЕНИЯ:

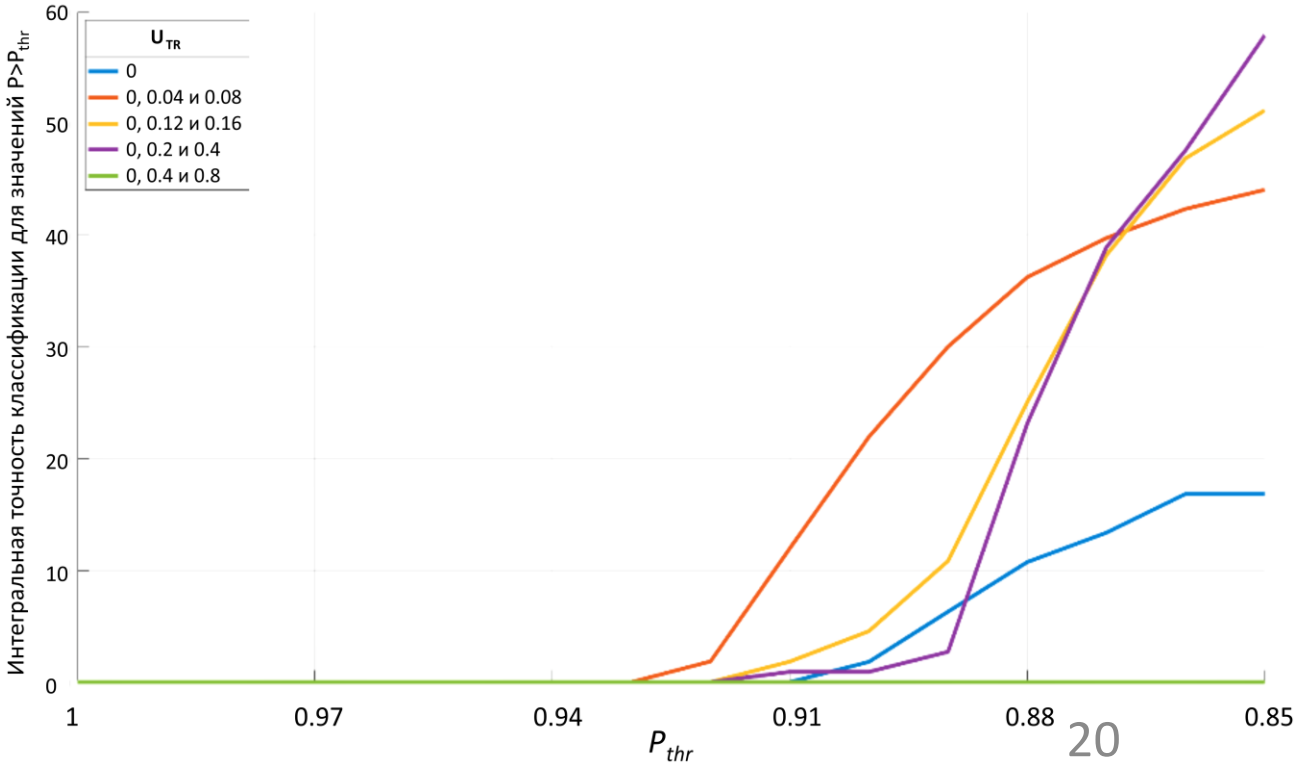
1. U_{TR} = 0 (шум не добавлялся).
2. Разделен на три части, содержащие равное количество изображений; в первой части U_{TR} = 0, во второй части U_{TR} = 0,04, в третьей части U_{TR} = 0,08.
3. Третий набор данных был разделен на три части, содержащие равное количество изображений; в первой части U_{TR} = 0, во второй части U_{TR} = 0,12, в третьей части U_{TR} = 0,16.
4. Четвертый набор данных был разделен на три части, содержащие равное количество изображений; в первой части U_{TR} = 0, во второй части U_{TR} = 0,2, в третьей части U_{TR} = 0,4.
5. Пятый набор данных был разделен на три части, содержащие равное количество изображений; в первой части U_{TR} = 0, во второй части - U_{TR} = 0,4, в третьей части - U_{TR} = 0,8.

использованы для обучения пяти независимых СНС с идентичной структурой

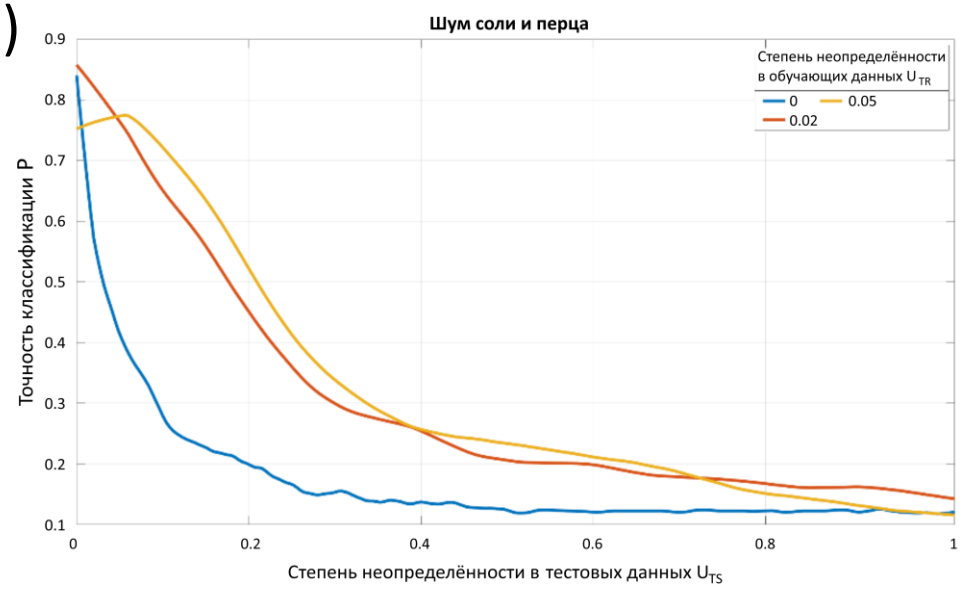
Обучение на зашумленных естественных изображениях (АБГШ)

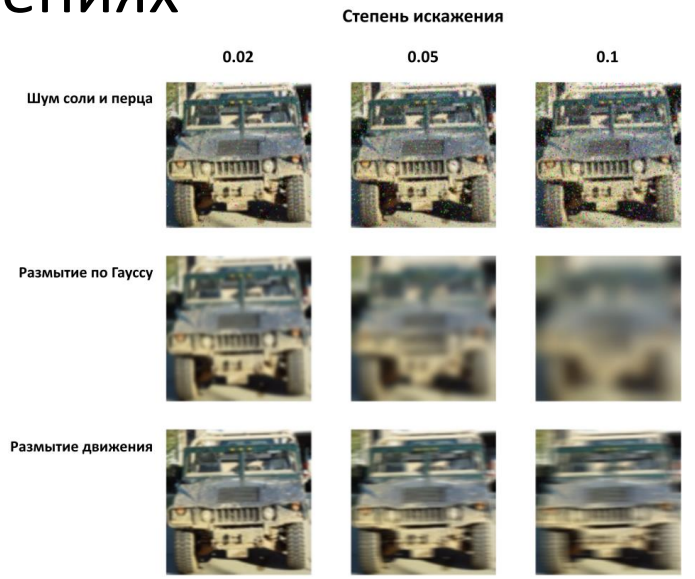
Умеренная степень искажений в наборах обучающих данных U_{TR} является оптимальной для обучения нейронных сетей и для последующего распознавания зашумленных изображений

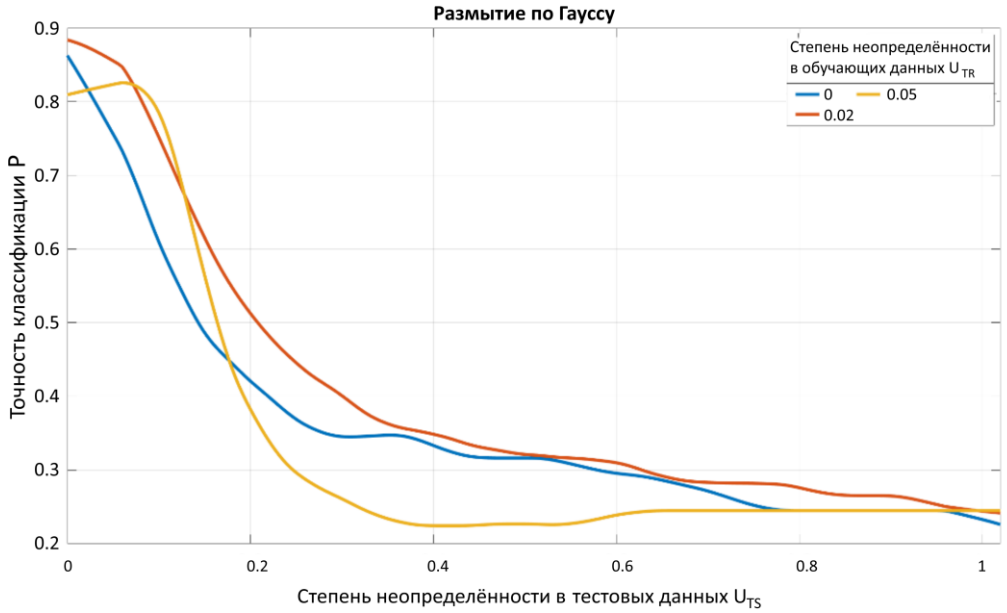


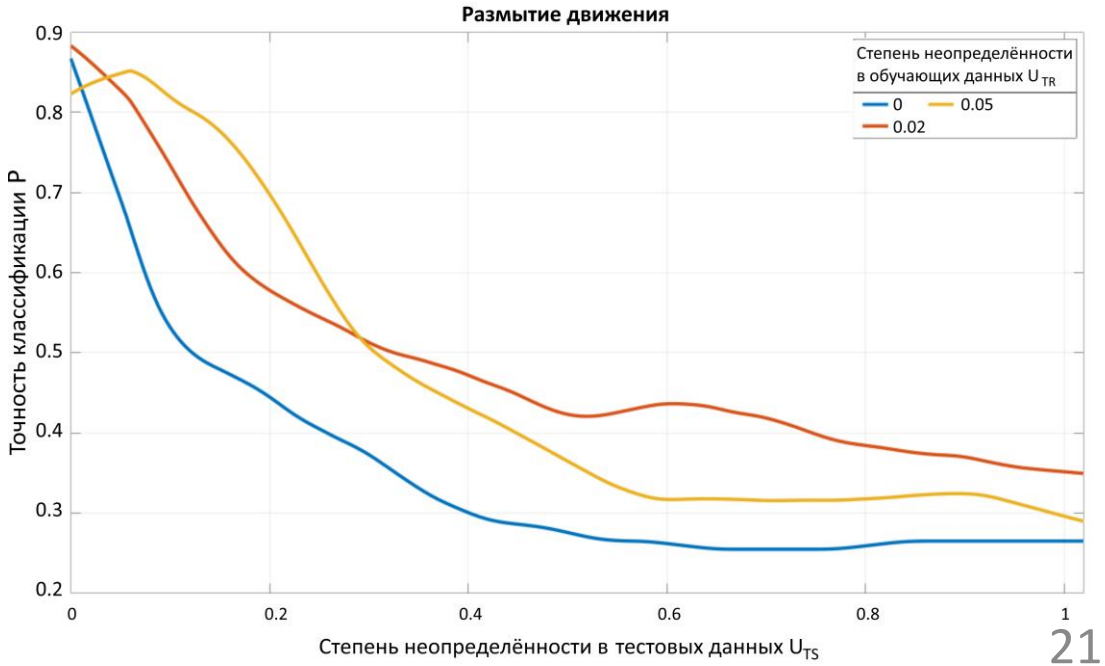


Обучение на зашумленных естественных изображениях (шум соли и перца, гауссовым размытием и размытием движения)









Третье защищаемое положение

Существует оптимальный способ **аугментации *обучающих*** изображений, позволяющий повысить интегральную **точность распознавания *тестовых*** изображений с различными искажениями при заданном пороге минимальной точности распознавания, без увеличения объёма обучающей выборки. Использование оптимального способа аугментации позволяет снизить вероятность ошибки распознавания в среднем в 2.5 раза по сравнению с использованием исходного набора изображений без дополнительных искажений.

Наборы обучающих данных

Исследуется влияние методов расширения обучающих наборов данных на примере **размытия по Гауссу**

$$I_{blur}(x,y) = \sum_{m=-k}^{k}\sum_{n=-k}^{k} G_{2d}(m,n)\cdot I(x-m,y-n)$$, где k – размеры фильтра

$$G_{2d}(x,y,\sigma) = \frac{1}{2\pi\sigma^2} e^{-\frac{x^2+y^2}{2\sigma^2}}$$

Рассмотрены следующие наборы данных:

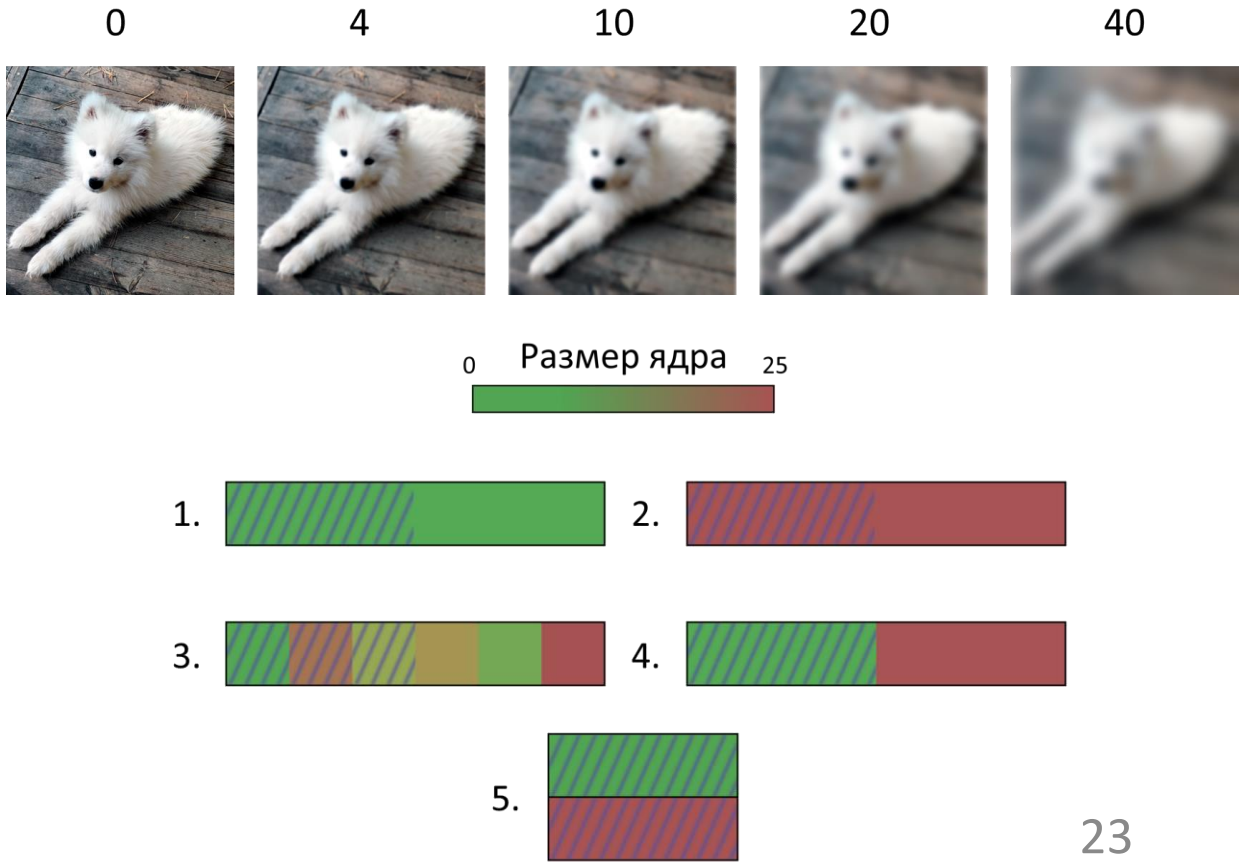
1) Классический набор изображений для обучения – без использования искажённых изображений.

2) В обучающем наборе все изображения искажены с размером окна = 25.

3) Для каждого из изображений в обучающем наборе размер окна искажения задавался случайно в диапазоне от 0 до 25.

4) Использовалась половина изображений из исходного набора (обозначенная штриховкой) - без искажений, а также другая половина (обозначенная сплошным цветом) - с искажением при размере окна = 25.

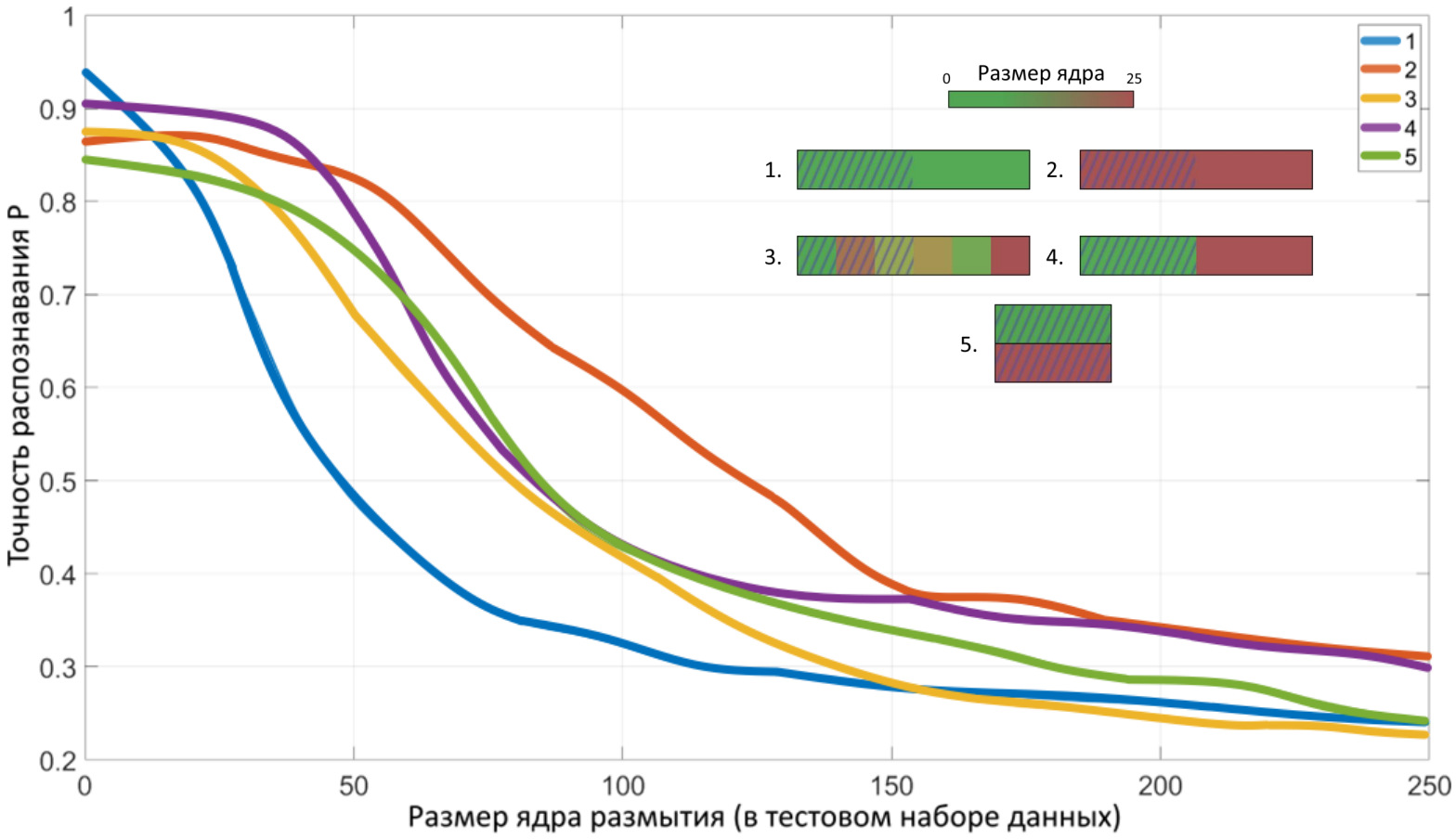
5) Использовалась половина изображений из исходного набора (обозначенная штриховкой) дважды – без искажений и с искажением при размере окна = 25.



Результаты

- Обучены пять экземпляров нейронной сети
- Получены кривые помехоустойчивости (зависимость точности распознавания от интенсивности искажений тестовых изображений)

Использование набора данных без аугментации приводит к



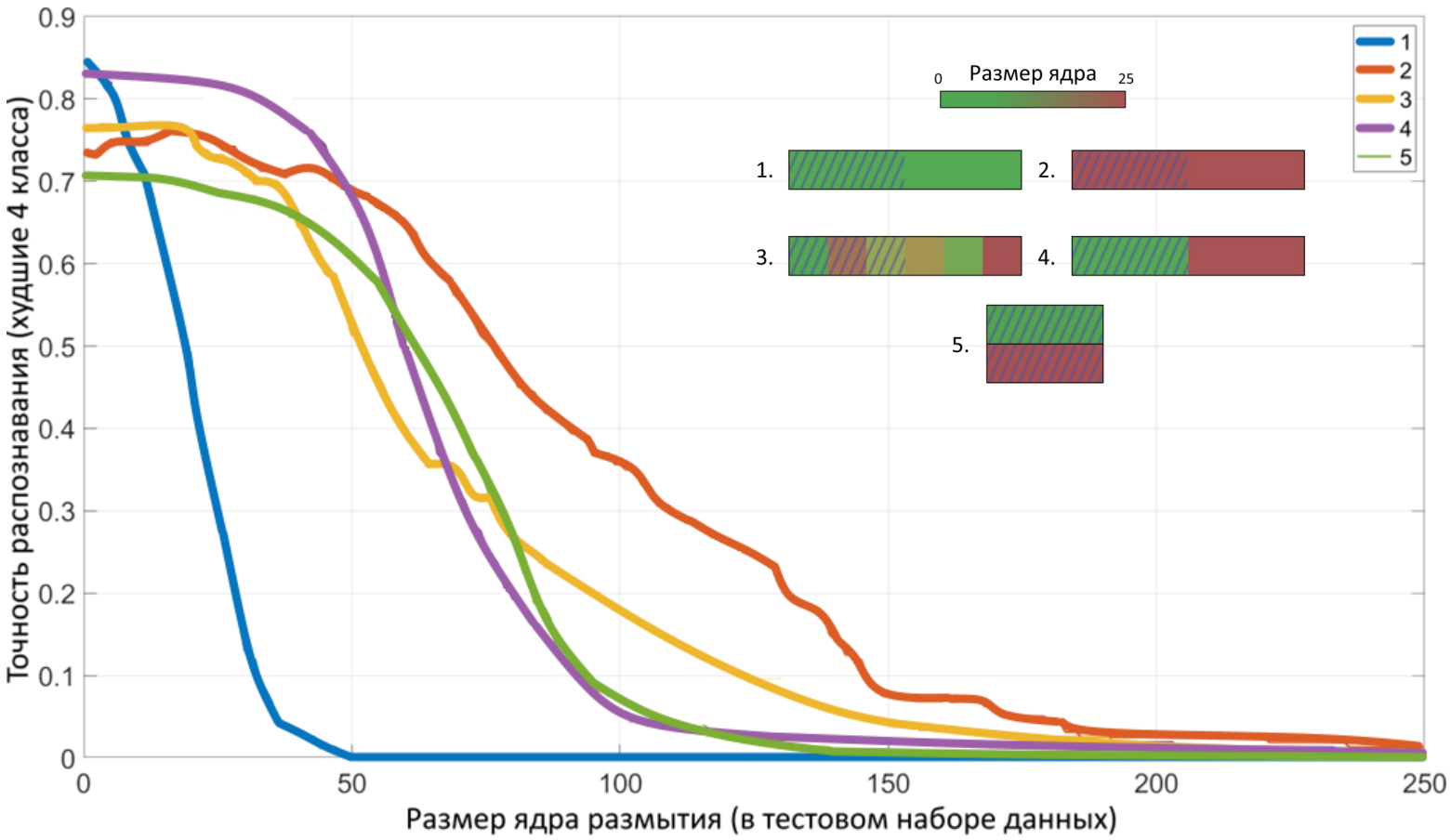
Низкая точность распознавания размытых изображений

Быстрое снижение точности распознавания изображений с ростом размеров фильтра Гаусса

Результаты

Для демонстрации скорости снижения точности распознавания также получены данные о точности распознавания наихудших четырех классов.

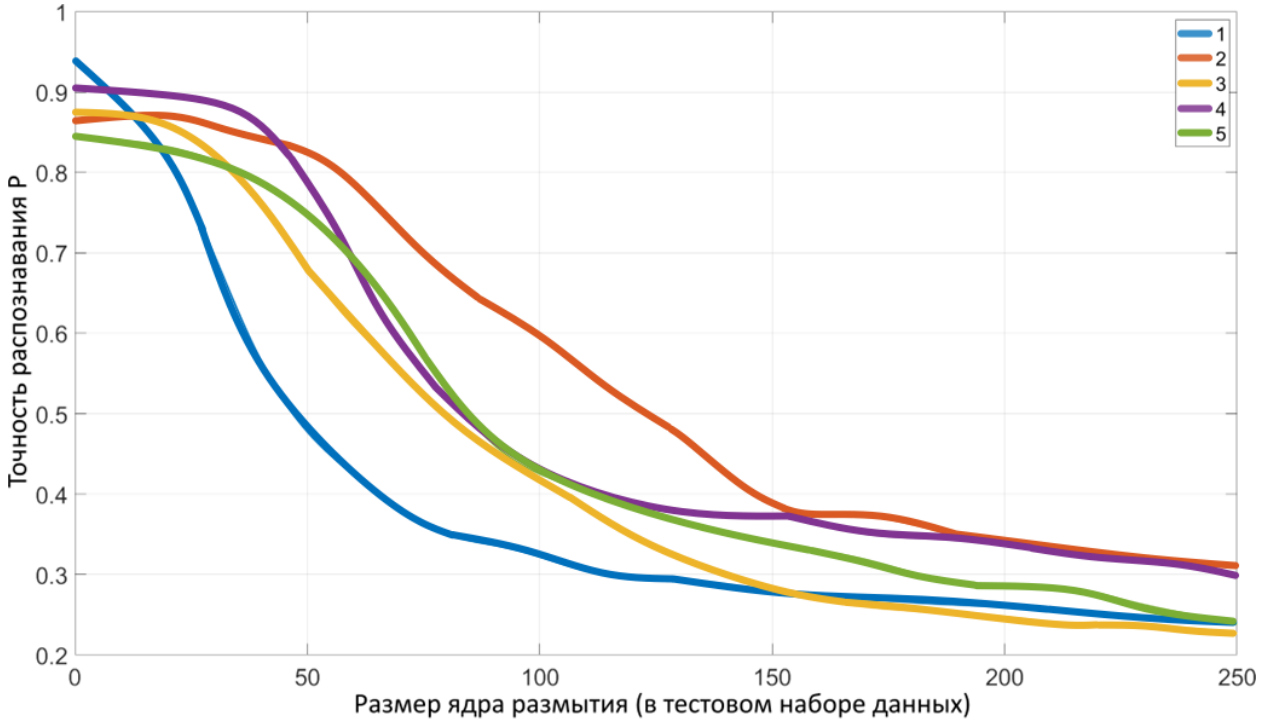
Полученные графики демонстрируют, что метод аугментации 4 (половина изображений из исходного набора - без искажений, половина - с искажением при размере окна = 25%) позволяет получить наилучший результат:

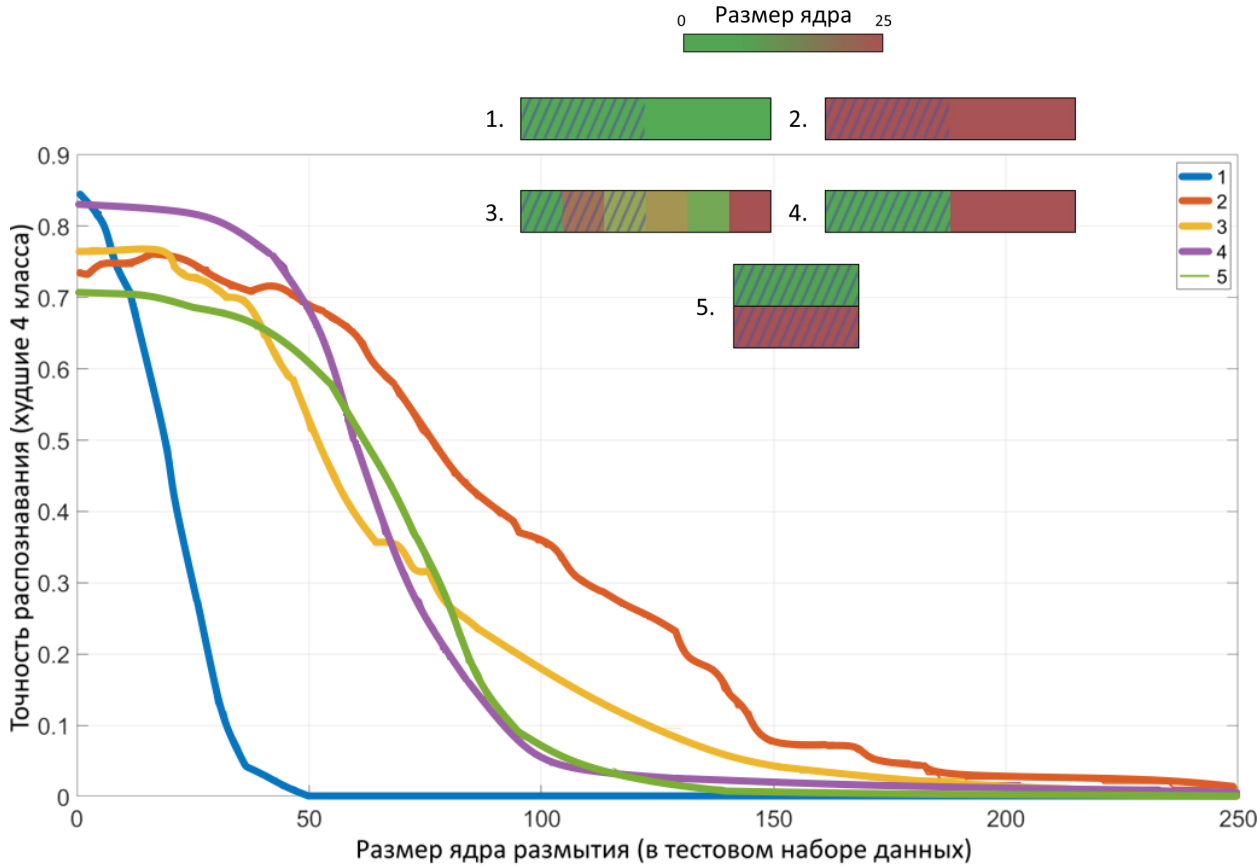


Высокая точность распознавания неискаженных изображений

Медленное снижение точности распознавания с увеличением интенсивности искажений

Результаты





Низкая точность распознавания размытых изображений

Быстрое снижение точности распознавания изображений с ростом размеров фильтра Гаусса

Высокая точность распознавания неискаженных изображений

Медленное снижение точности распознавания с увеличением интенсивности искажений

Четвертое защищаемое положение

Низкочастотная фильтрация изображений в совокупности с предварительным обучением нейронной сети размытыми изображениями позволяет в среднем в 8,8 раз снизить вероятность ошибки распознавания изображений, подвергнутых состязательным атакам, по сравнению с использованием исходного набора изображений без дополнительных искажений.

Состязательные примеры в физическом мире

- Тепловые шумы матриц камер
- Аберрации оптических элементов
- Плохое фото
- Дрожание камеры
- Погодные условия - туман, дождь, снег и т.д.
- Сжатие данных с потерями

Кукуруза
(молоток, орех, рука)

Банан
(кукуруза)

Сарай
(гора, трава, руины)

Маяк
(камень, мост)

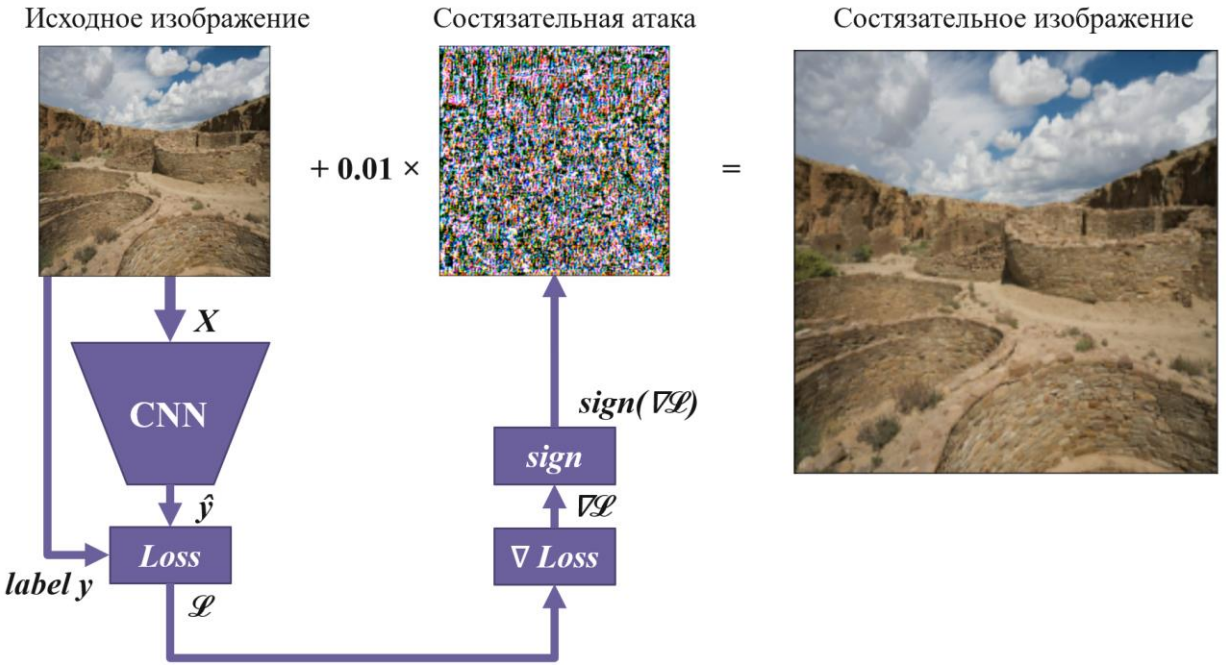
Стиральная машина
(люк)

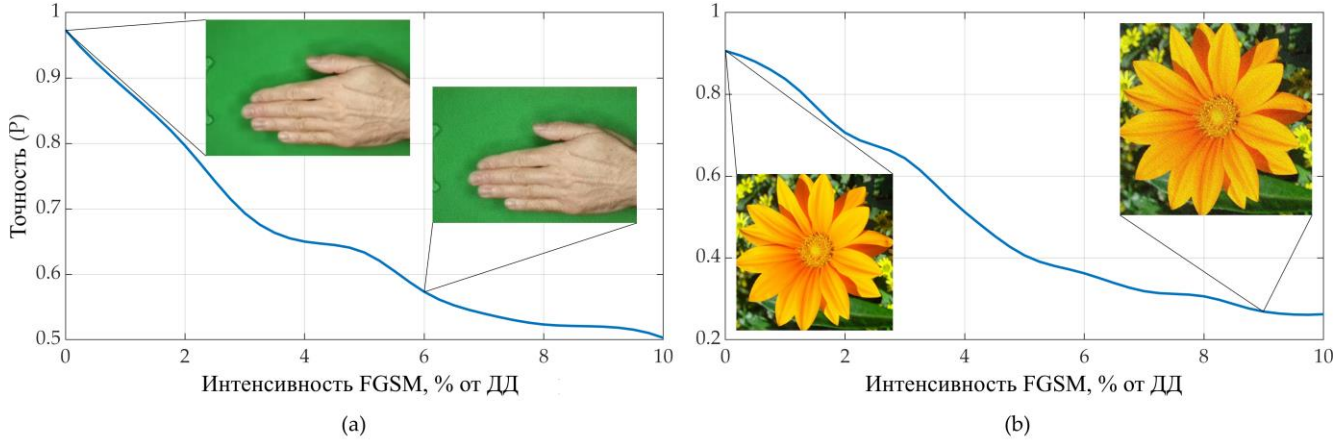
Вулкан
(поезд, дым)

Цепь
(ручка-молоток)

Зонт
(флаг)

Искусственные состязательные атаки



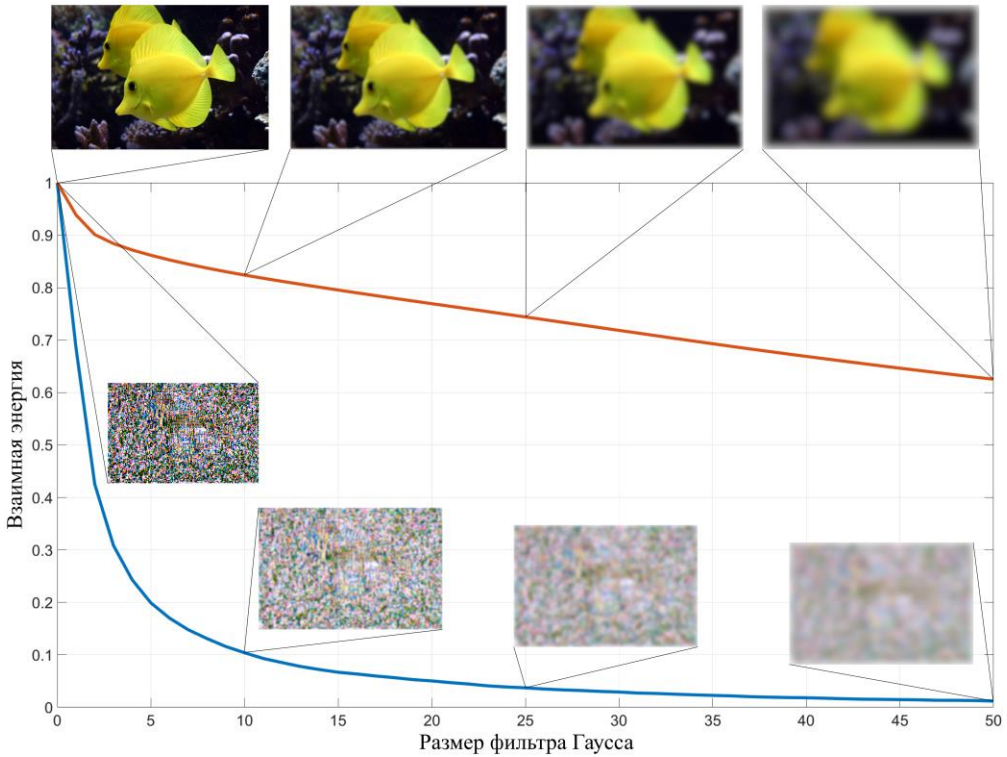


FGSM (Fast Gradient Sign Method) – на данный момент один из самых распространённых методов построения состязательной атаки [25]. Суть метода заключается в добавлении к исходному изображению некоторого неслучайного вектора, направление которого совпадает с градиентом функции потерь. Добавочный вектор FGSM можно представить как:

$$\eta=\varepsilon\cdot\mathrm{sgn}(\nabla_x J(\theta,x,y)),$$

где θ – параметры атакуемой модели нейронной сети,
x – входной вектор (изображение),
y – истинный класс вектора x (если есть),
J(θ, x, y) – функция потерь, используемая для обучения модели нейронной сети,
ε – коэффициент, выбираемый эмпирически,
∇x – градиент в пространстве изображения.

Разработанный метод противодействия высокочастотным искажениям



Предложен метод противостояния высокочастотным шумам, основанный на принципах, заимствованных из радиотехнических систем – фильтрация зашумлённых изображений с помощью низкочастотного фильтра Гаусса. Фильтрация изображений позволяет достаточно эффективно подавить высокочастотный шум, но одновременно размывает изображение, снижает его чёткость.

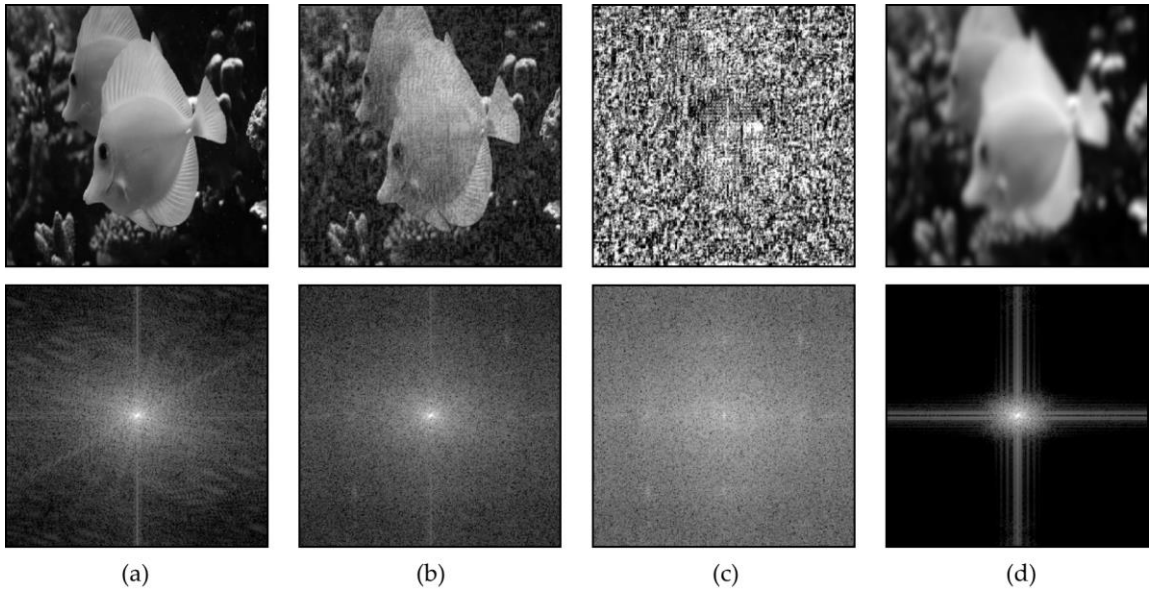
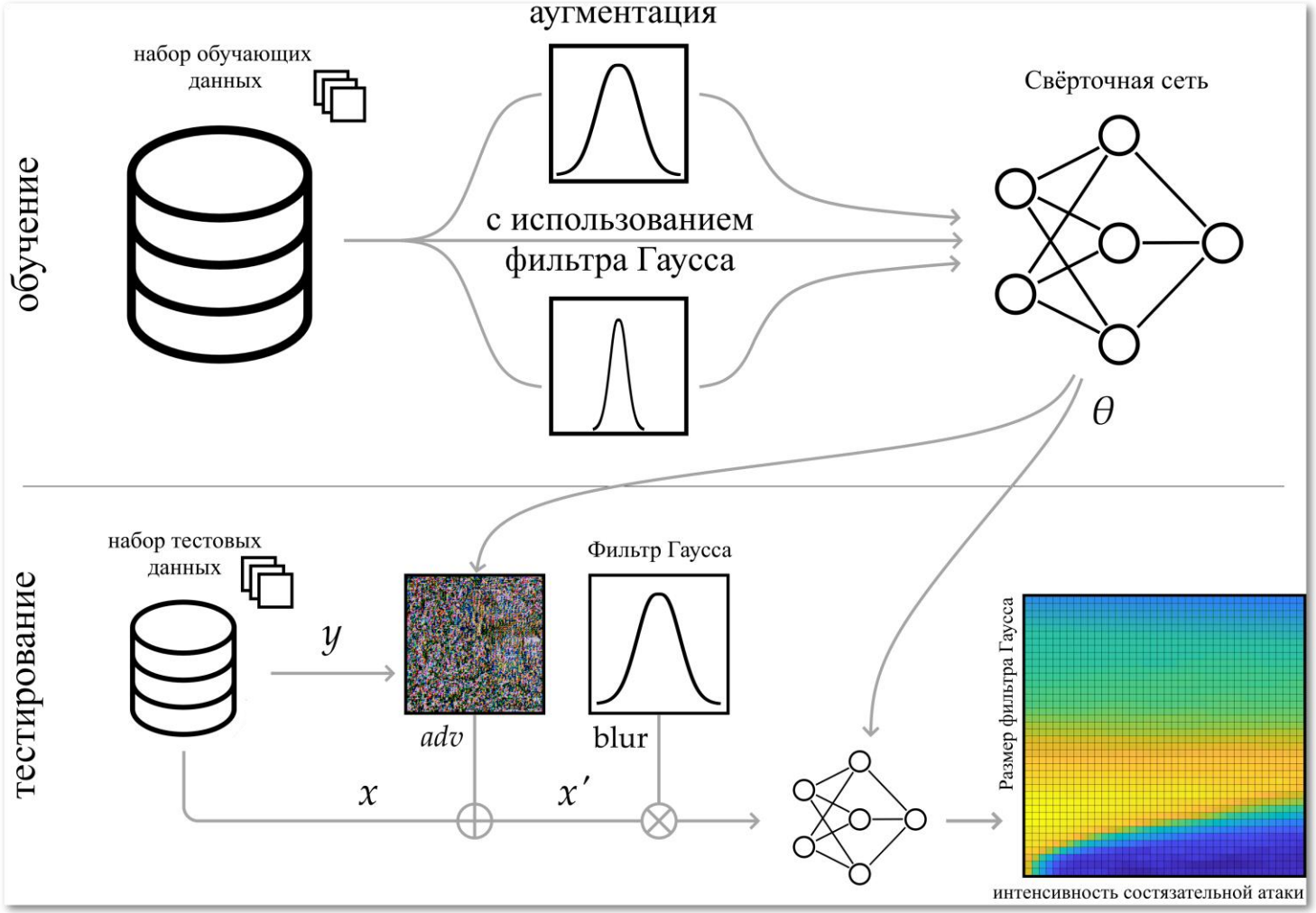


Схема алгоритма

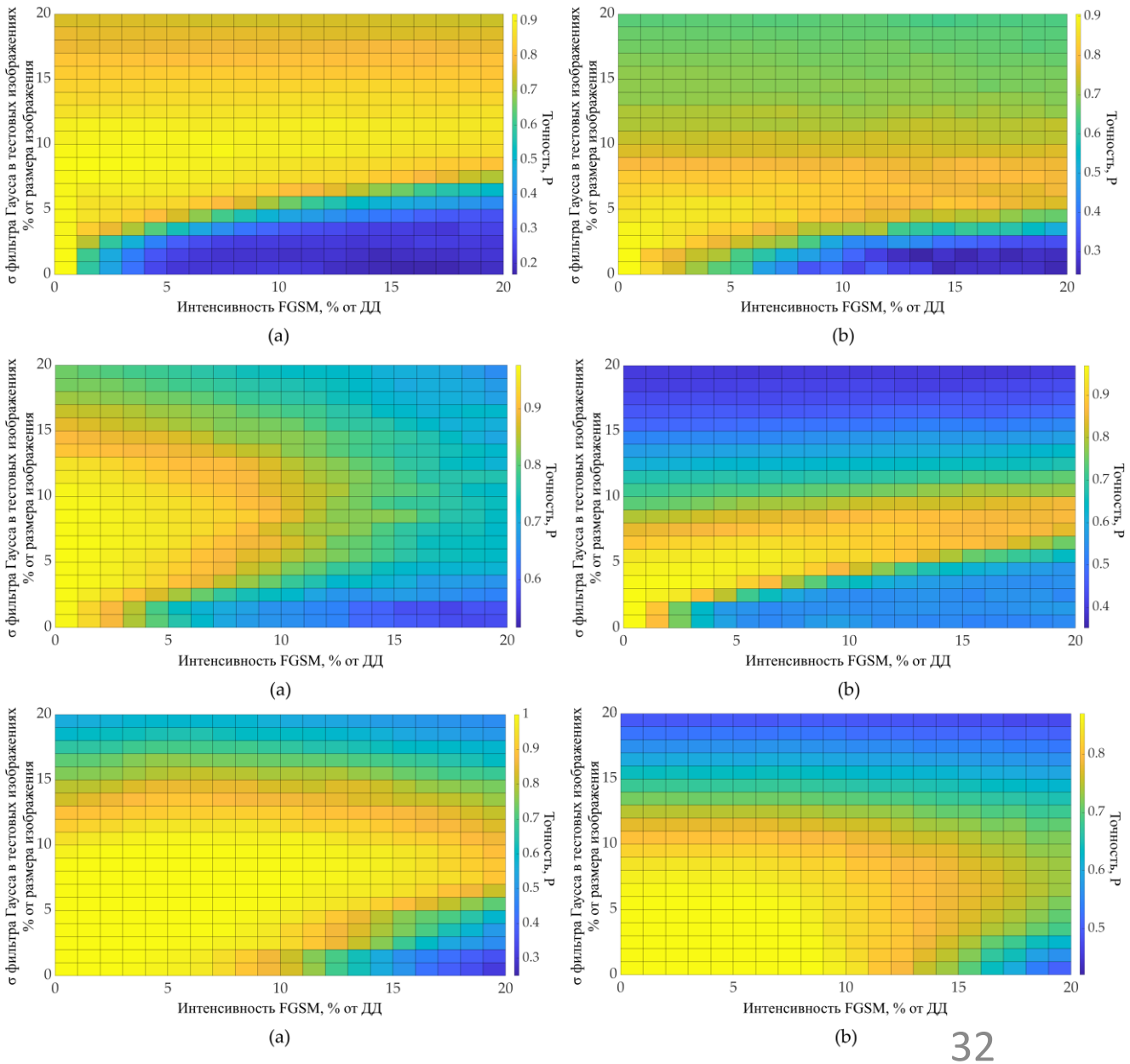
Состязательные изображения подвергаются фильтрации и поступают на нейронную сеть, предварительно обученную с учётом необходимости последующего распознавания размытых данных. Применение фильтра Гаусса позволяет значительно снизить влияние высокочастотного компонента изображения, включающего состязательную атаку, прочие высокочастотные шумы (например, импульсные или тепловые шумы для натуральных изображений) и мелкие детали изображения. При этом общая структура изображений меняется менее значительно.

Применение подобного метода является разменом общей точности распознавания (незначительно снижается) на точность распознавания изображений с внесенными целевыми искажениями (значительно возрастает).



Результаты работы алгоритма

- На графиках показана зависимость точности распознавания изображений от интенсивности атаки FGSM и от размера фильтра Гаусса.
- При обработке состязательных тестовых изображений с применением фильтра Гаусса точность возрастает.
- Полученные результаты являются репрезентативными для более сложных архитектур СНС.



Результаты работы алгоритма

- Оптимальный размер фильтра:

$$\sigma_{opt} = \arg\left(\max\left(\sum_{I_{FGSM}=0}^{I_{FGSM}^{max}} P_{LPF}(\sigma, I_{FGSM})\right)\right)$$

где σ_{opt} – оптимальный размер фильтра, P_{LPF} – точность распознавания, полученная с применением низкочастотного фильтра Гаусса, I_{FGSM} – интенсивность состязательной атаки, I_{FGSM}^{max} – максимальное значение интенсивности состязательной атаки.

Выигрыш в точности $G = \frac{(1-P_{no\ LPF})}{(1-P_{LPF})}$, где $P_{no\ LPF}$ – точность распознавания, полученная без применения низкочастотного фильтра Гаусса

Нейронная сеть и Набор данных	**Интенсивность FGSM**	**Точность распознавания с FGSM и без LPF** $P_{no\ LPF}$	**Точность распознавания с FGSM и LPF** P_{LPF}	**Оптимальный размер НЧ фильтра**	**Выигрыш точности G**
SimConvNet (Natural Dataset)	5	0.206	**0.913**	10	9.1
	10	0.206	**0.9**		7.9
	20	0.1875	**0.894**		6.7
SimConvNet (RPS)	5	0.738	**0.947**	8	4.9
	10	0.66	**0.879**		2.8
	20	0.576	**0.738**		1.6
EfficientNet (ImageNet)	15	0.699	**0.781**	7	1.4
	20	0.481	**0.72**		1.9
EfficientNet (Natural Dataset)	5	0.977	**1**	7	∞
	10	0.814	**0.996**		46.5
	20	0.25	**0.881**		6.3

Основные результаты исследования

1. Разработанные математические модели генерации изображений и обучения-тестирования свёрточной сети позволяет точно оценить характеристики устойчивости СНС к искажениям. Выявлена зависимость точности распознавания от меры неопределённости в тестовом наборе данных. Для корректно работающей модели при увеличении степени неопределённости в тестовых данных точность распознавания монотонно убывает. При внесении чрезмерных искажений в обучающий набор проявляется неоптимальность обучения.

2. Проанализирована точность распознавания множества наборов данных с различными степенями неопределенности и получена зависимость точности распознавания от степени искажений в обучающем наборе данных. Существование оптимальной степени искажений в обучающем наборе данных было предположено и доказано для различных типов изображений и шумов. Показано, что определение этого оптимума может быть выполнено с помощью статистического моделирования. Полученные результаты применимы к СНС с распространёнными структурами и различным типам искажений в данных. Использование обучающего набора данных с оптимальным значением неопределённости позволяет снизить вероятность ошибки распознавания в среднем в 20 раз по сравнению с использованием исходного набора изображений без дополнительных искажений.

3. Получена зависимость точности распознавания от интенсивности размытия по Гауссу для нейронных сетей, обученных с использованием различных методов аугментации. Доказано, что существует оптимальный способ аугментации обучающего набора данных, позволяющий снизить вероятность ошибки в среднем в 2.5 раза по сравнению с использованием исходного набора изображений без дополнительных искажений.

4. Предложен метод повышения устойчивости глубоких свёрточных нейронных сетей к высокочастотным атакам. Показано, что влияние состязательной атаки с увеличением граничной частоты фильтра Гаусса снижается быстрее, чем качество исходного изображения. Выигрыш в точности, достигаемый при использовании предложенного метода, в любом случае составляет не менее 1,4, средний выигрыш в точности составляет 8,8 раз.

Использование и реализация результатов диссертации, их теоретическая значимость и практическая ценность

Разработанные в ходе диссертационного исследования методы, алгоритмы, программы и методики их применения **использованы и реализованы** в:

1) НИР «Шеренга-2020»,
2) СЧ ОКР «5Р17К302-МТУСИ»,
выполненных по Государственному заказу в МТУСИ в 2018 — 2022 гг.
Использование результатов диссертационного исследования в перечисленных работах позволило существенно повысить технические характеристики разрабатываемых изделий.

Теоретическая значимость результатов диссертационного исследования обусловлена вкладом в развитие исследований робастности и устойчивости методов искусственного интеллекта к внешним воздействиям, в том числе представлением метода нахождения оптимума количества искажений в обучающих данных, а также метода противостояния высокочастотным искажениям.

Практическая ценность результатов диссертационного исследования состоит в том, что они могут быть использованы в различных системах распознавания образов и технического зрения, реализованных на разнообразных аппаратных платформах, в том числе и с крайне ограниченными вычислительными ресурсами.

Публикации по теме диссертации

Статьи в журналах, индексируемых в базах данных Web of Science и Scopus

1. Ziyadinov, V. V. Convolutional Neural Network Training Optimization for Low Point Density Image Recognition / V. V. Ziyadinov, P. S. Kurochkin, M. V. Tereshonok // Journal of Communications Technology and Electronics. – 2021. – Vol. 66, No. 12. – P. 1363-1369. – DOI 10.1134/S1064226921120202.
2. Ziyadinov, V. и др. A Survey on Symmetrical Neural Network Architectures and Applications // Symmetry. 2022. Т. 14. № 7. С. 1391.
3. Ziyadinov, V. Noise Immunity and Robustness Study of Image Recognition Using a Convolutional Neural Network / V. Ziyadinov, M. Tereshonok // Sensors. – 2022. – Vol. 22, No. 3. – DOI 10.3390/s22031241.
4. Ziyadinov V., Tereshonok M. Low-Pass Image Filtering to Achieve Adversarial Robustness // Sensors. 2023. Т. 23. № 22. С. 9032. https://doi.org/10.3390/s23229032

Статьи в журналах из списка ВАК

1. Зиядинов, В. В. Оптимизация обучения сверточных нейронных сетей при распознавании изображений с низкой плотностью точек / В. В. Зиядинов, П. С. Курочкин, М. В. Терешонок // Радиотехника и электроника. – 2021. – Т. 66, № 12. – С. 1207-1215. – DOI 10.31857/S0033849421120202.
2. Ziyadinov V.V., Tereshonok M.V., Moscow Technical University of Communications and Informatics. MATHEMATICAL MODELS AND RECOGNITION METHODS FOR MOBILE SUBSCRIBERS MUTUAL PLACEMENT // T-Comm. 2021. Vol. 15, № 4. P. 49–56. DOI: 10.36724/2072-8735-2021-15-4-49-56
3. Зиядинов, В. В. Обнаружение автомобильных заторов с использованием кластерного анализа данных геолокации / В. В. Зиядинов, А. Б. Талалаев, М. В. Терешонок // Труды Научно-исследовательского института радио. – 2022. – № 2. – С. 28-39. – DOI 10.34832/NIIR.2022.9.2.003.

Материалы конференций, индексируемые в базах данных Web of Science и Scopus

1. Ziyadinov, V. V. Analytical Survey on MANET and VANET Clusterisation Algorithms / V. V. Ziyadinov, M. V. Tereshonok // 2020 Systems of Signal Synchronization, Generating and Processing in Telecommunications, SYNCHROINFO 2020, Svetlogorsk, 01–03 июля 2020 года. – Svetlogorsk, 2020. – P. 9166120. – DOI 10.1109/SYNCHROINFO49631.2020.9166120.
2. Ziyadinov, V. V. Neural Network Image Recognition Robustness with Different Augmentation Methods / V. V. Ziyadinov, M. V. Tereshonok // Systems of Signal Synchronization, Generating and Processing in Telecommunications. – 2022. – Vol. 5, No. 1. – P. 441-444. – DOI 10.1109/SYNCHROINFO55067.2022.9840987.

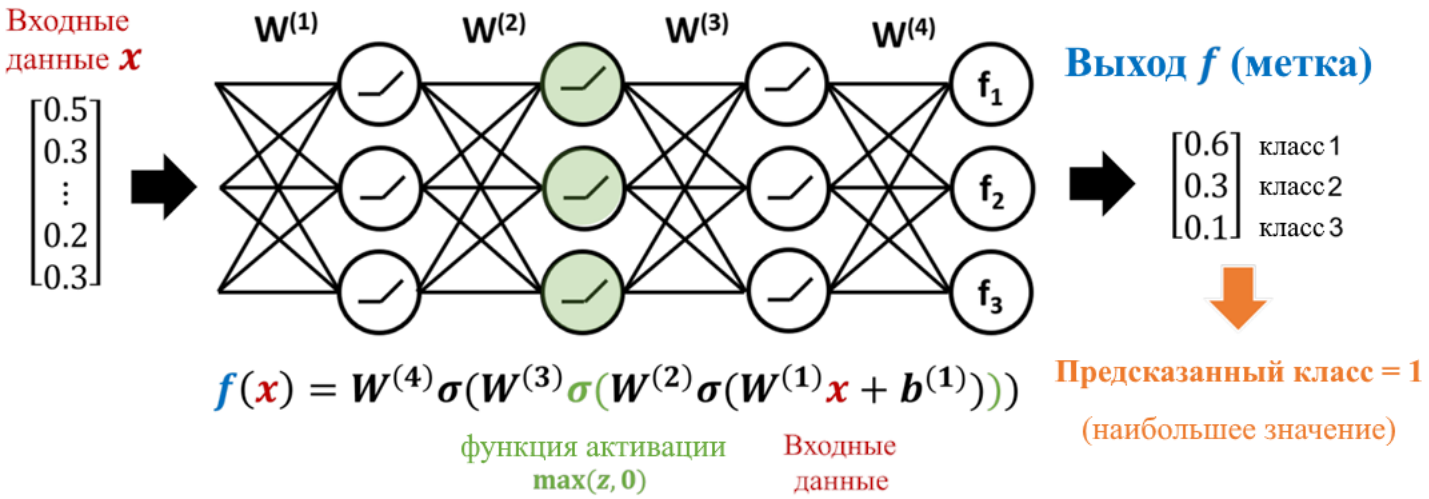
Авторские свидетельства

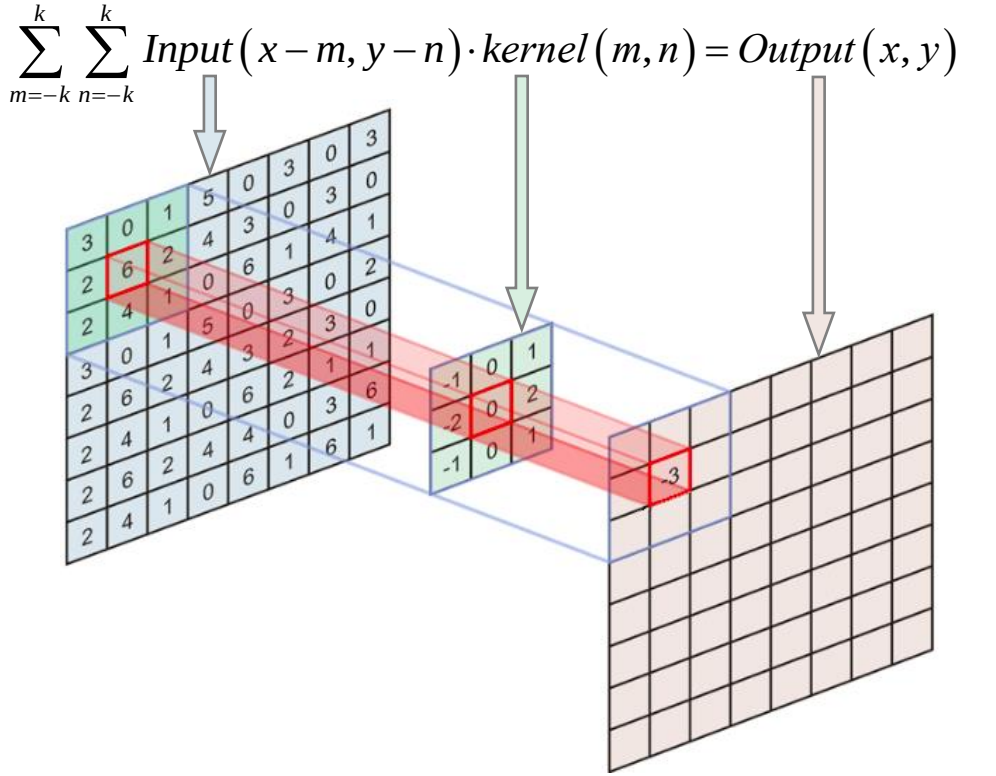
1. Свидетельство о государственной регистрации программы для ЭВМ № 2022660463 РФ. Программа сравнительного анализа и визуализации результатов работы свёрточных нейронных сетей : опубл. 03.06.2022.
2. Свидетельство о государственной регистрации программы для ЭВМ № 2020660537 РФ. Моделирование типов взаимного расположения абонентов сетей мобильной связи : опубл. 04.09.2020.
3. Свидетельство о государственной регистрации программы для ЭВМ № 2022660552 РФ. Программа моделирования шума в реальных изображениях и генерации обучающих выборок для систем распознавания : опубл. 06.06.2022.
4. Свидетельство о государственной регистрации программы для ЭВМ № 2022660553 РФ. Программа оценки результативности работы алгоритмов кластеризации : опубл. 06.06.2022.
5. Свидетельство о государственной регистрации программы для ЭВМ № 2022660554 РФ. Программа визуализации характеристик обучения свёрточных нейронных сетей для определения оптимальных параметров обучающих выборок при требуемой минимальной точности классификации : опубл. 06.06.2022.
6. Свидетельство о государственной регистрации программы для ЭВМ № 2021619356 РФ. Программа для оптимизации работы свёрточных нейронных сетей : опубл. 08.06.2021.
7. Свидетельство о государственной регистрации программы для ЭВМ № 2021619626 РФ. Программа генерации обучающих выборок для систем распознавания изображений с низкой плотностью точек : опубл. 15.06.2021.

Прочие публикации

1. Зиядинов, В. В. Математические модели и методы распознавания взаимного расположения мобильных абонентов / В. В. Зиядинов, М. В. Терешонок // Технологии информационного общества : Сборник трудов XIV Международной отраслевой научно-технической конференции, Москва, 18–19 марта 2020 года. – Москва: ООО "Издательский дом Медиа паблишер", 2020. – С. 157-159.

Спасибо за внимание!





На иллюстрации:
x – номер столбца на входном и выходном изображениях,
y – номер строки на входном и выходном изображениях,
k = 1, размер ядра свёртки равен 3×3


Flipping
Rotating
Cropping
Original
Color distortion
Sharpening
Random erasing