

Ильина Ольга Викторовна

**Повышение устойчивости и точности нейросетевого обнаружения  
искажённых объектов при видовом мониторинге**

Специальность 2.2.13

Радиотехника, в том числе системы и устройства телевидения

**АВТОРЕФЕРАТ**

диссертации на соискание учёной степени

кандидата технических наук

Работа выполнена в Ордена Трудового Красного Знамени федеральном государственном бюджетном образовательном учреждении высшего образования «Московский технический университет связи и информатики» (МТУСИ).

**Научный руководитель:** **Терешонок Максим Валерьевич** – доктор технических наук, профессор, начальник НИЧ МТУСИ.

**Официальные оппоненты:** **Гладышев Анатолий Иванович** – доктор технических наук, профессор, директор по перспективным проектам и науке АО «Концерн «Калашников».

**Доленко Сергей Анатольевич** – кандидат физико-математических наук, заведующий лабораторией адаптивных методов обработки данных научно-исследовательского института ядерной физики имени Д.В. Скобельцына Московского государственного университета имени М.В. Ломоносова.

**Ведущая организация:** Акционерное общество «Научно-исследовательский институт точных приборов» (АО «НИИ ТП»).

Защита диссертации состоится «17» декабря 2026 года в 11:00 на заседании диссертационного совета по защите докторских и кандидатских диссертаций 55.2.002.01 при Ордена Трудового Красного Знамени федеральном государственном бюджетном образовательном учреждении высшего образования «Московский технический университет связи и информатики» по адресу: 111024, г. Москва, ул. Авиамоторная, д. 8-а, МТУСИ, ауд. А-211.

С диссертацией можно ознакомиться в библиотеке и на сайте МТУСИ:  
<https://dis.mtuci.ru/upload/srd/Dis-IlinaOV/dis-IlinaOV.pdf>

Автореферат разослан «15» октября 2026 г.

Учёный секретарь

диссертационного совета 55.2.002.01

кандидат технических наук, доцент

В.М. Сахарчук

## ОБЩАЯ ХАРАКТЕРИСТИКА РАБОТЫ

**Актуальность темы исследования.** В последние годы активно развиваются технологии видового мониторинга, основанные на дистанционном зондировании Земли, что обеспечивает получение больших объемов изображений земной поверхности с высоким пространственным разрешением. Визуальный анализ таких данных востребован при мониторинге транспортных средств, объектов инфраструктуры и природных территорий. Объем и сложность поступающих данных обуславливают необходимость автоматизации их обработки и применения нейросетевых методов обнаружения объектов. Современные исследования подтверждают широкое применение глубокого обучения и нейросетевых моделей обнаружения объектов для анализа аэрофото- и спутниковых изображений. При этом для изображений дистанционного зондирования характерны сложный фон, высокая вариативность масштаба, ориентации и формы объектов, а также наличие большого числа мелких объектов на одном изображении.

Обнаружение объектов является одной из ключевых задач компьютерного зрения и заключается в одновременном определении пространственного положения объектов на изображении, класса этих объектов и оценки показателя уверенности своего предсказания. Для задач видового мониторинга особенно важна возможность автоматического обнаружения множества объектов различного размера и ориентации. Развитие методов нейросетевого обнаружения объектов позволило существенно повысить эффективность автоматического анализа подобных данных, однако перенос достигнутых результатов в реальные условия эксплуатации остается сложной задачей.

Эффективность нейросетевых моделей обнаружения объектов может существенно снижаться при ухудшении качества входных изображений. При формировании аэрофотоснимков на качество данных влияют шумы, размытие, изменения освещенности, атмосферные явления, особенности оптической системы и другие факторы. В исследованиях по робастности моделей обнаружения объектов показано, что современные модели могут значительно

терять эффективность при воздействии естественных искажений, причем снижение качества зависит как от типа, так и от интенсивности искажения.

Дополнительную проблему представляет сдвиг распределения данных между условиями обучения и эксплуатации нейросетевой модели. Изменение характеристик входных изображений относительно обучающего распределения может приводить к снижению обобщающей способности модели и ухудшению качества обнаружения объектов. В связи с этим повышение робастности нейросетевых моделей обнаружения объектов к изменениям условий формирования изображений является важным направлением современных исследований.

Наряду с естественными искажениями нейросетевые системы видового мониторинга подвержены преднамеренным состязательным воздействиям. В частности, состязательные патч-атаки позволяют локально изменять изображение таким образом, чтобы нарушать работу модели обнаружения объектов. Для аэрофотоснимков показана практическая реализуемость физических состязательных патч-атак: специально оптимизированные и напечатанные патчи могут быть размещены на реальных объектах и приводить к существенному снижению эффективности их обнаружения на снимках с воздуха. Аналогичная уязвимость продемонстрирована для систем обнаружения людей в задачах видеомониторинга.

Таким образом, современные системы видового мониторинга должны обеспечивать не только высокую точность обнаружения объектов в стандартных условиях, но и устойчивость к изменению характеристик входных данных и преднамеренным воздействиям. Разработка методов повышения точности и робастности нейросетевого обнаружения объектов при естественных искажениях и состязательных атаках является актуальной научной задачей, имеющей практическое значение для систем дистанционного зондирования Земли, транспортного мониторинга и других приложений компьютерного зрения.

**Степень разработанности темы исследования.** Важный вклад в развитие тематики робастности искусственных нейронных сетей внесли С.А. Доленко,

А.И. Гладышев, М.В. Терешонок, В.В. Зиядинов, И.В. Оселедец, I.J. Goodfellow, C. Szegedy, D. Hendrycks.

Существенный прогресс в области обнаружения объектов на изображениях связан с развитием глубоких сверточных нейронных сетей и появлением современных архитектур обнаружения объектов, среди которых наибольшее распространение получили двухэтапные обнаружители объектов семейства R-CNN и одноэтапные архитектуры семейства YOLO. Эти архитектуры заложили основу современных систем обнаружения объектов, обеспечивающих высокую точность и скорость обработки изображений. В последние годы данные архитектуры успешно применяются в задачах дистанционного зондирования Земли, интеллектуального транспорта, автономной робототехники и видового мониторинга, однако их эффективность существенно снижается при отклонении условий эксплуатации от условий обучения вследствие сдвига домена, возникающего при изменении распределения входных данных.

Большое количество исследований посвящено повышению робастности моделей компьютерного зрения к естественным искажениям изображений. Наиболее распространёнными направлениями являются аугментация обучающих данных, обучение на изображениях с различными видами деградации, предварительное восстановление изображений, а также разработка специализированных архитектур, менее чувствительных к шуму и размытию. Существенный вклад в развитие данного направления внесли исследования, в которых сформированы современные подходы к оценке робастности моделей глубокого обучения. Вместе с тем большинство существующих работ посвящено задачам классификации изображений, тогда как вопросам повышения устойчивости нейросетевых моделей обнаружения объектов к совместному воздействию различных естественных искажений уделено значительно меньше внимания.

Отдельным направлением исследований является защита нейросетевых моделей от состязательных воздействий. После фундаментальных работ Ian Goodfellow и Aleksander Madry были предложены многочисленные методы

повышения устойчивости моделей, основанные на состязательном обучении, локализации патчей, использовании сегментационных и генеративных моделей, а также сертифицированных алгоритмах защиты.

Несмотря на большое количество исследований в области повышения робастности нейросетевых моделей компьютерного зрения, большинство существующих работ рассматривает отдельные виды естественных искажений либо ориентировано на задачи классификации изображений. Недостаточно исследованы вопросы формирования оптимального распределения уровней искажений, вносимых в процесс обучения моделей обнаружения объектов, адаптивной предварительной обработки изображений, согласованной со статистическими характеристиками обучающих изображений, а также повышения устойчивости моделей одновременно к преднамеренным состязательным атакам без модификации нейросетевой архитектуры.

**Целью диссертационной работы** является повышение точности и робастности (устойчивости) функционирования нейросетевых моделей обнаружения объектов в условиях воздействия естественных искажений и преднамеренных состязательных атак при видовом мониторинге.

**Научная задача** исследования состоит в разработке комплекса методов повышения точности и робастности нейросетевого обнаружения объектов в условиях естественных и преднамеренных искажений входных изображений при видовом мониторинге.

Для достижения поставленной цели и решения научной задачи в работе были решены следующие **частные задачи**:

1. Разработка способа формирования обучающего набора данных для повышения устойчивости модели обнаружения объектов при видовом мониторинге.

2. Разработка метода адаптивной предварительной обработки изображений при видовом мониторинге.

3. Разработка метода локализации и удаления состязательных патч-атак на изображениях при видовом мониторинге.

**Научная новизна работы.** В диссертационной работе исследование проводится для видового мониторинга, где изображения характеризуются наличием объектов, существенно различающихся по масштабу и пространственному расположению на изображении. В отличие от классификации, где оценивается корректность определения класса изображения, задача обнаружения одновременно требует определить наличие объекта, корректно классифицировать его и локализовать его местоположение. Перенос результатов, полученных для классификации, на задачу обнаружения объектов не является непосредственным, поскольку эти задачи имеют разные критерии качества и по-разному реагируют на искажения входных изображений.

Научная новизна диссертационной работы заключается в разработке методов повышения точности и робастности нейросетевого обнаружения объектов при естественных и искусственных искажениях при сохранении высокой точности обнаружения объектов на неискажённых изображениях. Впервые для рассматриваемой задачи предложен способ формирования обучающего набора изображений, заключающийся в целенаправленном добавлении искажённых изображений с заданным распределением уровней искажений; разработан адаптивный метод предварительной обработки изображений на основе оценки их статистической неоднородности; а также разработан метод локализации и удаления состязательных патч-атак на основе реконструкции изображения и анализа карты ошибок.

**Теоретическая значимость** работы заключается в развитии математического аппарата глубокого обучения и теории робастного компьютерного зрения в условиях искажающих воздействий на входные изображения. Результаты диссертационного исследования углубляют теоретическую базу систем искусственного интеллекта для дальнейшего проектирования защищенных и помехоустойчивых систем компьютерного зрения.

**Практическая значимость** работы заключается в повышении точности обнаружения объектов на тестовых изображениях, что может быть использовано

в различных практических приложениях. Практическая значимость подтверждена актом использования результатов диссертационной работы в МТУСИ при выполнении НИОКР.

**Методология и методы исследования:** методы численного моделирования, теории вероятностей, математической статистики, теории машинного обучения, теории искусственного интеллекта, цифровой обработки изображений.

**Объектом исследования** являются глубокие свёрточные нейронные сети, решающие задачу обнаружения объектов на изображении.

**Предметом исследования** являются характеристики устойчивости и робастности глубоких свёрточных нейронных сетей, решающих задачу обнаружения объектов.

#### **Положения, выносимые на защиту:**

1. Разработанный способ обучения модели обнаружения объектов, основанный на формировании обучающего набора изображений с использованием искаженных изображений, обеспечивает увеличение метрики полноты обнаружения на тестовых данных более чем в 2 раза при воздействии аддитивного белого гауссова шума (отношение сигнал/шум от -8 до 0 дБ) и при воздействии гауссова размытия с радиусом от 6 до 12 пикселей по сравнению с моделью, обученной на неискаженных изображениях.

2. Разработанный адаптивный метод предварительной обработки изображений, обеспечивающий автоматический выбор режима фильтрации на основе оценки статистической неоднородности входного изображения, совместно с разработанным методом робастного обучения позволяет повысить интегральную оценку помехоустойчивости модели в 1,4 раза по сравнению с исходной моделью.

3. Разработанный метод локализации и удаления состязательных патч-атак, основанный на реконструкции изображения и анализе локальных статистических характеристик карты ошибок реконструкции, увеличивает значение метрики

качества обнаружения mAP с 46,8% до 81,0% при сохранении высокой точности обнаружения на изображениях без атак (mAP = 93,5%).

**Степень достоверности.** Достоверность полученных результатов подтверждается обоснованием используемого математического аппарата, а также верификацией разработанных методов на общедоступных наборах тестовых изображений.

**Апробация результатов.** Материалы диссертационной работы были доложены и одобрены на пяти научно-технических конференциях:

- 2022 Systems of Signal Synchronization, Generating and Processing in Telecommunications (SYNCHROINFO-2022), Архангельск, Россия, 29 июня – 01 июля 2022 г.;

- 2023 Intelligent Technologies and Electronic Devices in Vehicle and Road Transport Complex (TIRVED), Москва, Россия, 15 – 17 ноября 2023 г.;

- Научно-исследовательский семинар по физике наноструктур, атомной и молекулярной физике, Москва, Россия, 8 сентября 2022 года;

- Научно-исследовательский семинар по физике наноструктур и квантовым технологиям, Москва, Россия, 27 августа 2026 года;

- Международная конференция «Квантовые вычисления на сверхпроводниках», Сколково, Россия, 3 сентября 2026 года.

**Публикации результатов.** По теме диссертации было опубликовано 13 работ. Из них 3 работы опубликованы в журналах из белого списка и проиндексированы в международных базах данных Web of Science и Scopus, 2 работы опубликованы в журналах из Перечня ВАК, ещё 2 работы проиндексированы в международной базе данных Scopus, получено 6 свидетельств о государственной регистрации программ для ЭВМ.

**Реализация и внедрение результатов.** Разработанные в ходе диссертационного исследования методы и способы использованы в НИР «Шеренга-2020», СЧ ОКР «5P17K302-МТУСИ» и НИР «Лакмус-СПП», выполненных и выполняемых в рамках Государственных контрактов в МТУСИ с 2018 года по настоящее время.

**Личный вклад.** Все выносимые на защиту научные результаты получены соискателем лично. Из работ, опубликованных в соавторстве, в диссертацию включена только та их часть, которая получена лично соискателем.

**Соответствие паспорту научной специальности.** Диссертация соответствует пункту 11 «Разработка информационных технологий, в том числе цифровых, а также с использованием нейронных сетей для распознавания сигналов, изображений и речи в интеллектуальных радиотехнических, робототехнических системах технического зрения» паспорта научной специальности 2.2.13 «Радиотехника, в том числе системы и устройства телевидения».

**Объем и структура работы.** Текст диссертационной работы изложен на 112 печатных страницах и включает введение, четыре раздела, заключение, список сокращений и условных обозначений, список терминов, список литературы и приложения (на 8 печатных страницах). Список литературы содержит 97 наименований. В работе представлены 23 рисунка и 1 таблица.

## СОДЕРЖАНИЕ РАБОТЫ

**Первый раздел** посвящен обзору предмета исследований. Рассмотрены существующие методы обнаружения и распознавания объектов на изображениях при видовом мониторинге, описаны существующие метрики оценки качества робастности модели обнаружения объектов на изображениях. Проведен анализ существующих способов обучения нейросетевых систем, решающих задачу компьютерного зрения для устранения влияния естественных искажений, а также анализ существующих способов устранения влияния искусственных преднамеренных искажений, таких как состязательные патч-атаки.

Анализ существующих методов повышения устойчивости показал, что большинство исследований ориентировано на задачи классификации изображений и основано на аугментации изображений, предварительном восстановлении изображений, модификации архитектуры нейронной сети и обучении на искаженных изображениях. Для защиты от состязательных патч-атак применяются методы состязательного обучения, сегментации и удаления патчей,

реконструкции изображений и сертифицированной защиты, однако многие из них характеризуются зависимостью от конкретного типа атаки, повышенными вычислительными затратами и необходимостью дополнительного обучения.

В результате исследования выявлены следующие проблемы:

- снижение качества нейросетевого обнаружения объектов при воздействии естественных искажений, изменяющих статистические характеристики входных изображений;

- недостаточная изученность влияния способа формирования обучающего набора изображений на робастность моделей нейросетевого обнаружения объектов, в частности зависимости устойчивости модели от распределения интенсивности естественных искажений;

- отсутствие адаптивного механизма предварительной обработки изображений, позволяющего выбирать метод фильтрации в зависимости от типа и характера искажения без изменения архитектуры и повторного обучения нейросетевой модели обнаружения объектов;

- уязвимость нейросетевых моделей обнаружения объектов к преднамеренным состязательным патч-атакам, способным существенно снижать качество обнаружения объектов.

На основании проведенного анализа сформулирована научная задача разработки методов повышения точности и робастности нейросетевых моделей обнаружения объектов при воздействии естественных и преднамеренных состязательных искажений. Определены границы исследования, предусматривающие сохранение фиксированной архитектуры модели обнаружения объектов и повышение её устойчивости за счет формирования обучающего набора изображений, адаптивной предварительной обработки входных изображений и применения внешнего метода локализации и удаления состязательных патч-атак.

**Во втором разделе** исследовано влияние аддитивного белого гауссова шума и гауссова размытия на качество и робастность нейросетевых моделей обнаружения объектов на аэрофотоснимках Земли. Для исследования шумового

воздействия рассмотрены модели, обученные на неискаженных, умеренно зашумленных (отношение сигнал/шум выше нуля) и избыточно зашумленных изображениях (отношение сигнал/шум ниже нуля), при этом показано, что включение изображений с умеренным уровнем шума позволяет повысить полноту обнаружения более чем в 2 раза в области низких отношений сигнал/шум от -8 до 0 дБ по сравнению с обучением на неискаженных изображениях, тогда как избыточное зашумление обучающего набора изображений приводит к снижению полноты обнаружения.

Для исследования влияния гауссова размытия предложен способ формирования обучающего набора изображений, в котором интенсивность размытия отдельных изображений задается полунормальным распределением с параметром  $\sigma_{\text{обуч.}}^{\text{размыт.}}$ :

$$d = |\hat{d}|, \quad (1)$$

где

$$\hat{d} \sim N\left(0, \left(\sigma_{\text{обуч.}}^{\text{размыт.}}\right)^2\right), \quad (2)$$

где  $N\left(0, \left(\sigma_{\text{обуч.}}^{\text{размыт.}}\right)^2\right)$  – нормальное распределение с нулевым математическим ожиданием и стандартным отклонением  $\sigma_{\text{обуч.}}^{\text{размыт.}}$ .

Для анализа способности модели локализовать транспортные средства на аэрофотоснимках Земли были подготовлены следующие модели: модель, обученная на исходном (без искажений) обучающем наборе изображений ( $\sigma_{\text{обуч.}}^{\text{размыт.}} = 0$ ); модели, обученные на изображениях, которые искажены в соответствии с правилом (2) с параметром  $\sigma_{\text{обуч.}}^{\text{размыт.}} = 1$ ,  $\sigma_{\text{обуч.}}^{\text{размыт.}} = 2$ ,  $\sigma_{\text{обуч.}}^{\text{размыт.}} = 3$ ,  $\sigma_{\text{обуч.}}^{\text{размыт.}} = 4$  и  $\sigma_{\text{обуч.}}^{\text{размыт.}} = 5$  соответственно. На рисунке 1 представлены кривые зависимости усредненной полноты AR перечисленных выше моделей от различной степени искажений тестового набора изображений  $\sigma_{\text{тест}}^{\text{размыт.}}$ .

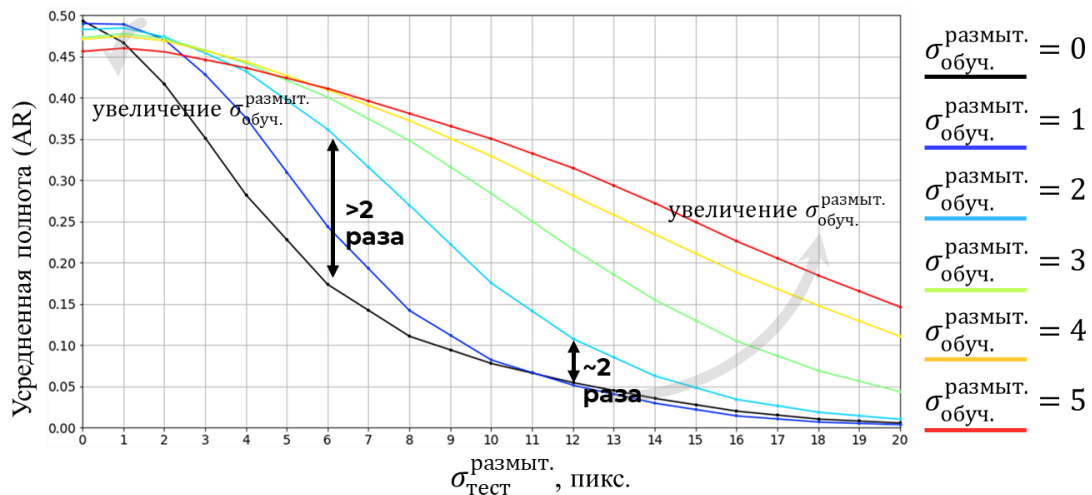


Рисунок 1 – Графики зависимости усредненной полноты AR от  $\sigma_{\text{тест}}^{\text{размыт.}}$  для моделей с параметром  $\sigma_{\text{обуч.}}^{\text{размыт.}} = 0$  (черная кривая),  $\sigma_{\text{обуч.}}^{\text{размыт.}} = 1$ ,  $\sigma_{\text{обуч.}}^{\text{размыт.}} = 2$ ,  $\sigma_{\text{обуч.}}^{\text{размыт.}} = 3$ ,  $\sigma_{\text{обуч.}}^{\text{размыт.}} = 4$  и  $\sigma_{\text{обуч.}}^{\text{размыт.}} = 5$  (синяя, голубая, зеленая, желтая и красная кривые соответственно)

Из рисунка 1 видно, что при обучении и тестировании ГСНС на неискаженных изображениях ( $\sigma_{\text{обуч.}}^{\text{размыт.}} = 0$ ) показывает наивысшую метрику усреднённой полноты, но с увеличением степени размытия тестовых изображений  $\sigma_{\text{тест}}^{\text{размыт.}}$  качество обнаружения быстро падает. В случае увеличения разброса степени искажений в обучающем наборе изображений (т.е. с увеличением  $\sigma_{\text{обуч.}}^{\text{размыт.}}$ ) видно, что уровень усредненной полноты анализируемой модели уменьшается медленнее при больших значениях  $\sigma_{\text{тест}}^{\text{размыт.}}$ , однако, на исходных (без искажений) изображениях оценка качества обнаружения заметно падает.

Для оценки полноты обнаружения моделью локализации объектов используется метрика перекрытия истинного объекта с лучшей предсказанной ограничивающей рамкой – IoU. На рисунке 2 представлены контурные графики для моделей с параметром  $\sigma_{\text{обуч.}}^{\text{размыт.}} = 0$ ,  $\sigma_{\text{обуч.}}^{\text{размыт.}} = 1$ ,  $\sigma_{\text{обуч.}}^{\text{размыт.}} = 2$ ,  $\sigma_{\text{обуч.}}^{\text{размыт.}} = 3$ ,  $\sigma_{\text{обуч.}}^{\text{размыт.}} = 4$  и  $\sigma_{\text{обуч.}}^{\text{размыт.}} = 5$ , на которых интенсивностью красного цвета показана доля правильно обнаруженных и локализованных транспортных средств на аэрофотоснимках Земли от метрики перекрытия IoU. Данные карты показывают, что чем точнее предсказаны ограничивающие рамки, т.е. чем выше их метрика

перекрытия с истинными объектами IoU, тем выше на контурных графиках будет отображаться интенсивнее красный цвет.

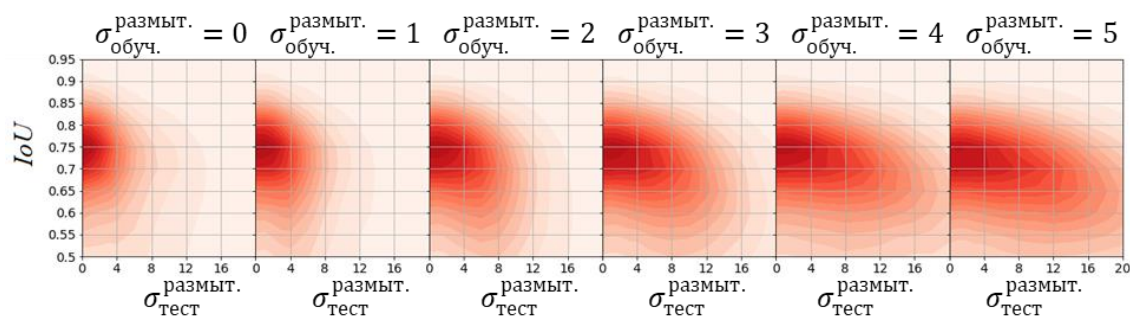


Рисунок 2 – Контурные графики зависимости доли правильно обнаруженных и локализованных транспортных средств на аэрофотоснимках от метрики их перекрытия с истинными объектами для моделей с параметром  $\sigma_{\text{обуч.}}^{\text{размыт.}} = 0$ ,  $\sigma_{\text{обуч.}}^{\text{размыт.}} = 1$ ,  $\sigma_{\text{обуч.}}^{\text{размыт.}} = 2$ ,  $\sigma_{\text{обуч.}}^{\text{размыт.}} = 3$ ,  $\sigma_{\text{обуч.}}^{\text{размыт.}} = 4$  и  $\sigma_{\text{обуч.}}^{\text{размыт.}} = 5$  при различных уровнях размытия тестовых изображений

Из анализа рисунка 2 следует, что избыточное размытие обучающих изображений, несмотря на рост усредненной полноты AR, приводит к нежелательным результатам в виде снижения меры перекрытия границ предложенных нейронной сетью регионов интереса с истинными объектами на изображении. В результате проведённого моделирования удалось экспериментально показать, что эффективной аугментацией обучающих изображений может быть их размытие части с интенсивностью, описываемой положительной ветвью распределения Гаусса. Выбор дисперсии этого распределения (и, соответственно, доли искажённых изображений и уровня их искажений в обучающем наборе) обусловлен двумя конкурирующими процессами – ростом усредненной полноты AR и снижением меры перекрытия границ предложенных нейронной сетью регионов интереса с истинными объектами на изображении по мере увеличения дисперсии уровня размытия. В частности, достаточно эффективная модель, обученная на наборе изображений с параметром разброса уровней размытия  $\sigma_{\text{обуч.}}^{\text{размыт.}} = 2$ , демонстрирует прирост полноты обнаружения более, чем в 2 раза при уровнях искажения тестовых изображений в диапазоне  $6 \leq \sigma_{\text{тест}}^{\text{размыт.}} \leq 12$ , по сравнению с обученной на неискажённых изображениях.

В третьем разделе экспериментально показано, что робастность, сформированная при обучении нейросетевой модели обнаружения объектов на изображениях с гауссовым размытием, не переносится на искажения иной природы, а именно – АБГШ. Это объясняется тем, что гауссово размытие приводит преимущественно к подавлению высокочастотных компонент изображения, тогда как аддитивный белый гауссов шум, напротив, увеличивает уровень высокочастотных составляющих. Следовательно, механизмы компенсации данных видов искажений существенно различаются.

В данном разделе предложена схема адаптивной предварительной обработки изображений при видовом мониторинге, упрощенная схема которой представлена на рисунке 3.

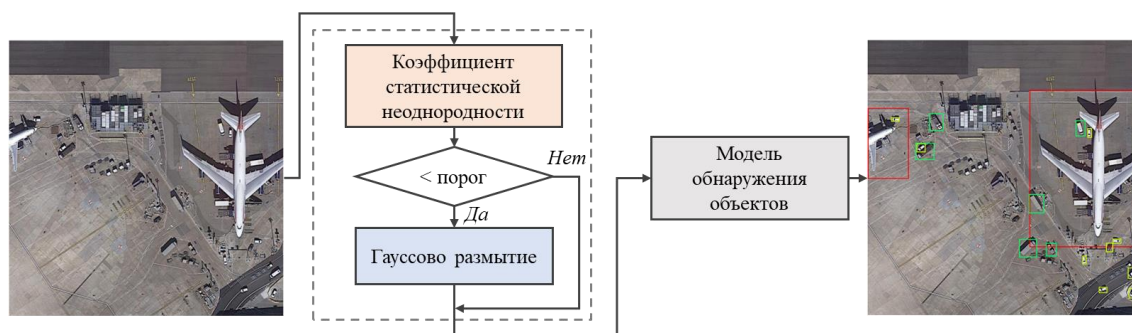


Рисунок 3 – Упрощенная схема разработанного адаптивного метода повышения устойчивости модели обнаружения объектов на искаженных изображениях

В соответствии с предложенной схемой, перед входом в модель обнаружения объектов изображение поступает в блок расчета коэффициента статистической неоднородности. В случае, если полученный коэффициент меньше определенного порогового значения, изображение считается зашумленным и его необходимо передать на вход гауссова фильтра с предопределённым радиусом размытия, который выполняет роль фильтра нижних частот и снижает влияние высокочастотных составляющих на изображении. В ином случае, считается, что на изображении нет значительного шума и нет необходимости выполнять предварительное размытие. Использование гауссова фильтра обусловлено тем, что он эффективно подавляет высокочастотную составляющую аддитивного белого гауссова шума при низкой вычислительной

сложности, что особенно важно для систем видового мониторинга, функционирующих в режиме, близком к реальному времени.

В данной работе используется интегральная оценка кривой помехоустойчивости, которая представляет собой среднее значение площадей под кривыми метрики качества обнаружения средней усредненной точности  $mAP$  (от англ. mean Average Precision) для дискретного множества значений стандартных отклонений гауссова размытия и АБГШ и значений радиуса гауссова ядра в тестовом наборе изображений. Для расчета площади под кривой помехоустойчивости в настоящем исследовании используется следующая формула:

$$AUC = \sum_{i=0}^N mAP_i \cdot \Delta\sigma_i \quad (3)$$

где  $N$  – количество интервалов, на которые делится анализируемая кривая;

$\Delta\sigma_i$  – ширина отрезка с индексом  $i$  по оси абсцисс анализируемой кривой;

$mAP_i$  – величина  $mAP$  в середине отрезка с индексом  $i$ .

Тогда, используя формулу (3), получим формулу интегральной оценки кривой помехоустойчивости:

$$S = \frac{AUC_{\text{размыт.}} + AUC_{\text{АБГШ}}}{2} \quad (4)$$

где  $AUC_{\text{размыт.}}$  – площадь под кривой величины качества обнаружения  $mAP$  от степени размытия изображений в тестовом наборе изображений  $mAP(\sigma_{\text{тест}}^{\text{размыт.}})$ ;

$AUC_{\text{АБГШ}}$  – площадь под кривой величины качества обнаружения  $mAP$  от степени зашумления изображений в тестовом наборе изображений  $mAP(\sigma_{\text{тест}}^{\text{АБГШ}})$ .

На рисунке 4 представлены значения интегральной оценки кривой помехоустойчивости, рассчитанной по формуле (4), полученные при определенном радиусе гауссова размытия  $\sigma_{\text{адаптивн.}}^{\text{размытие}}$ , применяемом в адаптивной системе для моделей с параметром  $\sigma_{\text{обуч.}}^{\text{размыт.}} = 0$ ,  $\sigma_{\text{обуч.}}^{\text{размыт.}} = 1$ ,  $\sigma_{\text{обуч.}}^{\text{размыт.}} = 2$ ,  $\sigma_{\text{обуч.}}^{\text{размыт.}} = 3$  и  $\sigma_{\text{обуч.}}^{\text{размыт.}} = 4$ .

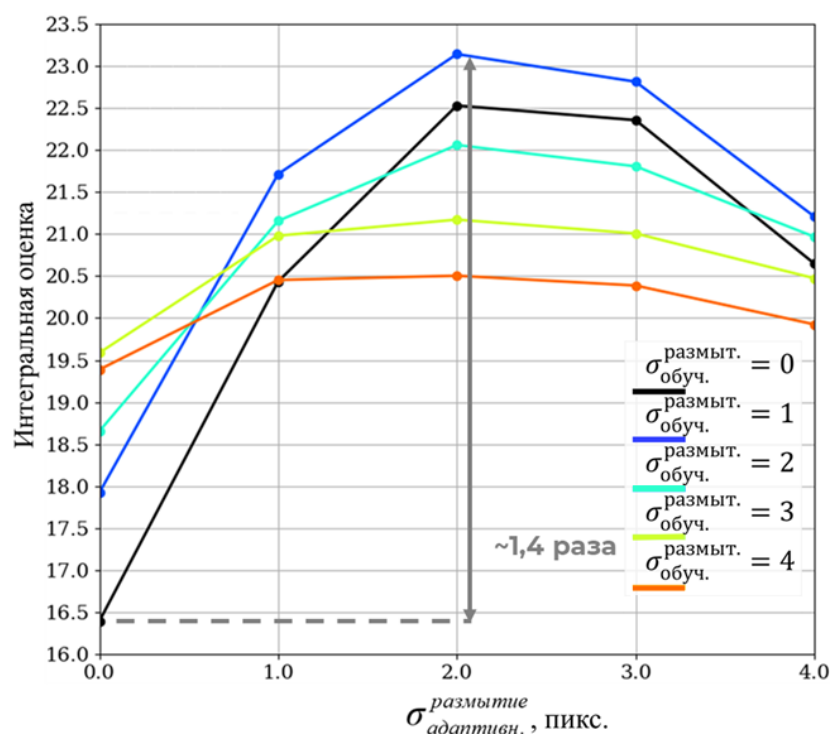


Рисунок 4 – Интегральная оценка кривой помехоустойчивости в зависимости от радиуса гауссова размытия, используемого в адаптивной схеме для моделей с параметром  $\sigma_{\text{размыт.}}^{\text{размыт.}} = 0$ ,  $\sigma_{\text{размыт.}}^{\text{размыт.}} = 1$ ,  $\sigma_{\text{размыт.}}^{\text{размыт.}} = 2$ ,  $\sigma_{\text{размыт.}}^{\text{размыт.}} = 3$  и  $\sigma_{\text{размыт.}}^{\text{размыт.}} = 4$

Из рисунка 4 видно, что использование предложенной адаптивной схемы с предопределенным радиусом размытия в этой адаптивной схеме приводит к росту величины интегральной оценки кривой помехоустойчивости. Однако существует некоторое критическое значение данного радиуса размытия, выше которого интегральная оценка кривой помехоустойчивости начинает падать. Также из данного рисунка видно, что применение только адаптивной схемы (черная кривая для модели с параметром  $\sigma_{\text{размыт.}}^{\text{размыт.}} = 0$ ) или при использовании только обучения на сформированном обучающем наборе изображений ( $\sigma_{\text{размытие адаптивн.}} = 0$ ) не приводит к тем результатам, которые получаются при их сочетании.

Также из полученных результатов видно, что модель, обученная на наборе изображений с параметром искажения  $\sigma_{\text{размыт.}}^{\text{размыт.}} = 1$ , в сочетании с предложенной адаптивной системой с параметром  $\sigma_{\text{размытие адаптивн.}} = 2$ , дает наивысшую оценку интегральной величины кривых помехоустойчивости.

В результате данного исследования предложен метод повышения робастности системы нейросетевого обнаружения объектов на аэрофотоизображениях. Данный метод состоит из двух этапов. Первый этап включает в себя аугментацию обучающих изображений, заключающуюся в добавлении размытых изображений, степень размытия которых задается генератором случайных величин с полунормальной функцией распределения с параметром стандартного отклонения  $\sigma_{\text{обуч.}}^{\text{размыт.}} = 1$ . Второй этап представляет собой адаптивную схему, состоящую из блока оценки статистической неоднородности на входном изображении и гауссова фильтра с радиусом размытия  $\sigma_{\text{адаптивн.}}^{\text{размытие}} = 2$ , позволяющего подавить высокочастотные шумовые составляющие изображения. Разработанный метод приводит к повышению интегральной оценки кривой помехоустойчивости в 1,4 раза по сравнению с исходной моделью обнаружения объектов без использования разработанного способа формирования обучающего набора изображений и адаптивной предварительной обработки.

Таким образом, разработанный метод позволяет существенно повысить устойчивость нейросетевой модели обнаружения транспортных средств одновременно к гауссову размытию и аддитивному белому гауссову шуму без модификации архитектуры модели обнаружения объектов.

**В четвертом разделе** предложен метод локализации и удаления состязательных патч-атак на изображениях при видовом мониторинге, который позволяет повысить устойчивость нейросетевой модели обнаружения объектов к искусственным воздействиям (патч-атакам) без модификации ее архитектуры. Разработанный метод основан на идее обнаружения и устранения аномалии на входных изображениях. В качестве аномалий в данной работе рассматриваются локализованные в пространстве изображения фрагменты (патч-атаки), которые отличаются от тех же фрагментов на доброкачественных изображениях, т.е. изображениях без добавления патч-атак.

Упрощенная схема метода локализации и удаления состязательных патч-атак на изображениях представлена на рисунке 5.

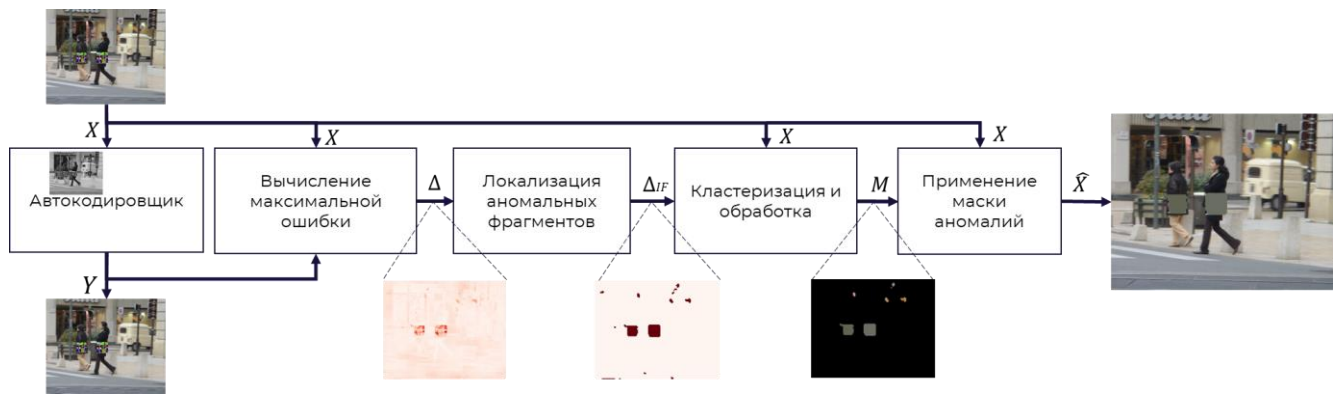


Рисунок 5 – Упрощенная схема метода локализации и удаления состязательных патч-атак на изображениях

В таблице 1 представлен сравнительный анализ качества разработанного метода и существующих аналогов (Segment and Complete (SAC) и Patch-Agnostic Defense (PAD)) в задачах защиты моделей обнаружения объектов от состязательных патч-атак.

Таблица 1 – Метрика качества детектора объектов mAP (%) в режиме состязательной патч-атаки для различных методов защиты. Наивысшие показатели выделены жирным

| Методы защиты        | mAP без добавления атак, % | mAP с добавлением атак, % |
|----------------------|----------------------------|---------------------------|
| -                    | 93,3                       | 46,8                      |
| SAC                  | 93,3                       | 53,7                      |
| PAD                  | 92,7                       | 76,9                      |
| <b>Разработанный</b> | <b>93,5</b>                | <b>81,0</b>               |

Результаты, представленные в таблице 1, показывают, что разработанный метод обеспечивает наилучшее качество обнаружения объектов среди рассмотренных методов защиты. В частности, на наборе изображений INRIA-Person при отсутствии атаки значение метрики mAP составляет 93,5%, а при наличии состязательной патч-атаки – 81,0%, что превышает результаты методов SAC и PAD.

Визуализация результатов работы модели обнаружения объектов на нескольких примерах из набора изображений INRIA-Person, подвергшихся состязательной патч-атаке, представлена на рисунке 6. Зеленые рамки

представляют обнаруженные объекты категории «человек», при этом в верхнем левом углу каждой рамки отображается оценка объектности. В левой колонке показаны результаты обнаружения без использования разработанного метода локализации и удаления состязательных патч-атак, в то время как в правой колонке показан результат работы модели обнаружения объектов с использованием разработанного метода.



Рисунок 6 – Визуализация результата работы модели обнаружения объектов на нескольких примерах из набора изображений INRIA-Person, подвергшихся состязательной патч-атаке

В результате исследования разработан метод снижения влияния состязательных патч-атак на систему нейросетевого обнаружения объектов. Предложенный метод включает глубокую сверточную нейронную сеть, алгоритм локализации аномальных областей и алгоритм их кластеризации и последующей обработки.

## ЗАКЛЮЧЕНИЕ

В ходе выполнения диссертационной работы получены следующие основные результаты.

1. Проведен анализ современных методов нейросетевого обнаружения объектов, существующих метрик оценки качества и робастности, а также способов повышения устойчивости моделей компьютерного зрения к естественным и искусственным искажениям. Установлено, что существующие методы не обеспечивают достаточной устойчивости моделей обнаружения объектов к совокупному воздействию различных видов естественных искажений и состязательных патч-атак без существенного увеличения вычислительных затрат или модификации архитектуры нейронной сети, что определило направление дальнейших исследований.

2. Разработан способ формирования обучающего набора изображений для обучения модели обнаружения объектов, суть которого заключается в использовании изображений, содержащих естественные искажения различной интенсивности. Экспериментально установлено, что повышение устойчивости определяется не только наличием искажённых изображений в обучающем наборе изображений, но и законом распределения уровней искажений. Показано, что введение аддитивного белого гауссова шума в обучающий набор изображений позволяет увеличить полноту обнаружения более чем в 2 раза в области низких ОСШ (от -8 до 0 дБ). В том числе показано, что использование полунормального распределения уровней искажений в обучающем наборе изображений позволяет повысить усредненную полноту обнаружения более чем в 2 раза при воздействии гауссова размытия при радиусе размытия в диапазоне от 6 до 12 пикселей. Данные результаты подтверждают эффективность разработанного метода.

3. Разработан метод адаптивной предварительной обработки изображений, основанный на статистической оценке неоднородности входного изображения и автоматическом выборе режима фильтрации. Предложенный метод объединяет разработанный способ формирования обучающего набора изображений и адаптивную предварительную обработку, что обеспечивает повышение интегральной оценки помехоустойчивости системы обнаружения объектов в 1,4 раза одновременно при воздействии гауссова размытия и аддитивного

белого гауссова шума по сравнению с исходной моделью без изменения архитектуры нейросетевой модели обнаружения объектов.

4. Разработан метод локализации и удаления состязательных патч-атак, основанный на реконструкции входного изображения и анализе локальных статистических характеристик карты ошибок реконструкции. Предложенный метод не требует модификации архитектуры модели обнаружения объектов и повторного обучения при появлении новых типов состязательных воздействий. Экспериментально показано, что применение разработанного метода увеличивает значение метрики mAP в условиях состязательной патч-атаки с 46,8% до 81,0%, при этом на изображениях без атак значение mAP сохраняется на уровне 93,5%, что превосходит результаты существующих методов защиты.

Полученные результаты доказывают обоснованность положений, выносимых на защиту, а также подтверждают, что цель диссертационной работы достигнута, а поставленная научная задача решена.

Разработанные методы могут быть использованы при создании интеллектуальных систем видового мониторинга, функционирующих в условиях естественных и искусственных искажений изображений, включая системы дистанционного зондирования Земли, автономные транспортные средства и другие системы компьютерного зрения, предъявляющие повышенные требования к надёжности обнаружения объектов.

Перспективы дальнейших исследований связаны с разработкой универсальных методов повышения робастности нейросетевых моделей к более широкому спектру естественных и искусственных искажений, исследованием совместного воздействия нескольких типов деградации изображений при решении задач компьютерного зрения.

## **СПИСОК РАБОТ, ОПУБЛИКОВАННЫХ АВТОРОМ ПО ТЕМЕ ДИССЕРТАЦИИ**

**Статьи в журналах, проиндексированных в международных базах  
данных Web of Science и Scopus:**

1. Ilina, O. A survey on symmetrical neural network architectures and applications / O. Ilina, V. Ziyadinov, N. Klenov, M. Tereshonok. // *Symmetry*. – 2022. – Т. 14, № 7. – С. 1391. – DOI: 10.3390/sym14071391.

2. Ilina, O. V. Robustness study of a deep convolutional neural network for vehicle detection in aerial imagery / O. V. Ilina, M. V. Tereshonok. // *Journal of Communications Technology and Electronics*. – 2022. – Т. 67, № 2. – С. 164–170. – DOI: 10.1134/S1064226922020048.

3. Ilina, O. Increasing neural-based pedestrian detectors' robustness to adversarial patch attacks using anomaly localization / O. Ilina, M. Tereshonok, V. Ziyadinov. // *Journal of Imaging*. – 2025. – Т. 11, № 1. – С. 26. – DOI: 10.3390/jimaging11010026.

#### **Статьи в журналах из Перечня ВАК:**

1. Ильина, О.В. Способ локализации состязательных патч-атак / О.В. Ильина // *Вестник связи*. – 2026. – № 9. – С. 26–33.

2. Демин, А. Д. Исследование влияния адаптации диаграмм направленности антенн на эффективность сетевого уровня AD НОС сети радиосвязи / А. Д. Демин, М. В. Терешонок, О. В. Ильина. // *T-Comm: Телекоммуникации и транспорт*. – 2025. – Т. 19, № 4. – С. 4–11. – DOI 10.36724/2072-8735-2025-19-4-4-11.

#### **Свидетельства о государственной регистрации программ для ЭВМ:**

1. № 2024689957 Российская Федерация. Программный модуль для локализации и удаления состязательных патч-атак на цветных изображениях для решения задач компьютерного зрения : № 2024689563 : заявл. 28.11.2024 : опубл. 11.12.2024 / О. В. Ильина, М. В. Терешонок (правообладатель – МТУСИ)

2. № 2024612396 Российская Федерация. Программный комплекс для демонстрации работы свёрточной нейронной сети, решающей задачу распознавания состязательных изображений : № 2023689454 : заявл. 27.12.2023 : опубл. 31.01.2024 / О. В. Ильина, М. В. Терешонок, В. В. Зиядинов (правообладатель – МТУСИ)

3. № 2024610705 Российская Федерация. Программа для моделирования работы нейросетевой модели обнаружения объектов с использованием

адаптивной системы для повышения устойчивости на размытых и зашумленных цветных изображениях : № 2023689457 : заявл. 27.12.2023 : опубл. 12.01.2024 / О. В. Ильина, М. В. Терешонок (правообладатель – МТУСИ)

4. № 2024611339 Российская Федерация. Программный комплекс расчета внешних характеристик точности и устойчивости свёрточной нейронной сети к высокочастотным искажениям и оптимизации параметров предварительной обработки изображений : № 2023689369 : заявл. 27.12.2023 : опубл. 19.01.2024 / В. В. Зиядинов, О. В. Ильина, М. В. Терешонок (правообладатель – МТУСИ)

5. № 2022660463 Российская Федерация. Программа сравнительного анализа и визуализации результатов работы свёрточных нейронных сетей : № 2022619579 : заявл. 23.05.2022 : опубл. 03.06.2022 / В. В. Зиядинов, О. В. Ильина, М. В. Терешонок (правообладатель – МТУСИ)

6. № 2022660552 Российская Федерация. Программа моделирования шума в реальных изображениях и генерации обучающих выборок для систем распознавания : № 2022619577 : заявл. 23.05.2022 : опубл. 06.06.2022 / В. В. Зиядинов, О. В. Ильина (правообладатель – МТУСИ)

### **Прочие публикации**

1. Ilina, O. V. Study of deep convolutional neural network for vehicle localization on blurred aerial imagery / O. V. Ilina, M. V. Tereshonok. // В сборнике: 2022 Systems of Signal Synchronization, Generating and Processing in Telecommunications (SYNCHROINFO). – Архангельск, Россия, 2022. – С. 1–7. – DOI: 10.1109/SYNCHROINFO55067.2022.9840965

2. Ilina, O. V. Adaptive method to increase vehicle detection system robustness on blurred and noisy aerial images / O. V. Ilina, M. V. Tereshonok. // В сборнике: 2023 Intelligent Technologies and Electronic Devices in Vehicle and Road Transport Complex (TIRVED). – Москва, Россия, 2023. – С. 1–6. – DOI: 10.1109/TIRVED58506.2023.10332671