УКД 004.7

В.М. Сливницин, Д.В. Кочкин
Вологодский государственный университет

РАЗРАБОТКА НЕЙРОСЕТЕВОЙ СИСТЕМЫ ВИДЕОАНАЛИТИКИ ДЛЯ АВТОМАТИЗИРОВАННОГО РАСПОЗНАВАНИЯ ПОТЕНЦИАЛЬНО ОПАСНЫХ СИТУАЦИЙ В ОБЩЕСТВЕННЫХ УЧРЕЖДЕНИЯХ

В статье представлена разработка нейросетевой системы видеоаналитики для автоматизированного распознавания потенциально опасных ситуаций в общественных учреждениях. Основное внимание уделено применению методов глубокого обучения (YOLOv8) для идентификации подозрительных людей и оружия в режиме реального времени. Описаны архитектура и алгоритмы системы, а также проведено тестирование, показавшее точность распознавания на уровне 80 %. Разработка направлена на повышение безопасности посетителей и персонала в общественных учреждениях. Рассматриваются возможности масштабирования и дообучения нейронной сети для повышения точности и расширения распознаваемых объектов.

Нейросетевые системы, видеоаналитика, безопасность, компьютерное зрение, машинное обучение, YOLOv8, Python, распознавание угроз, глубокое обучение.

Введение

Обеспечение безопасности в общественных учреждениях с высокой проходимостью является важной задачей в условиях роста социальной напряженности. Традиционные методы видеонаблюдения, основанные на ручном мониторинге, обладают значительными ограничениями и не всегда позволяют оперативно реагировать на потенциальные угрозы, такие как скрытие лица или ношение оружия. Это создает необходимость внедрения интеллектуальных систем видеоаналитики, использующих методы глубокого обучения для автоматизированного выявления опасных ситуаций в режиме реального времени [1–3].

Цель работы заключается в разработке системы видеоаналитики, способной в режиме реального времени распознавать:

1. Лица, закрытые капюшонами или масками.
2. Наличие оружия (пистолеты, ножи и т.д.).

Постановка задачи

Основная задача заключается в разработке системы видеоаналитики, обеспечивающей корректное и качественное распознавание потенциально опасных ситуаций в общественных учреждениях. Система должна быть масштабируемой для работы с большим количеством видеопотоков [4, 5]. Для достижения этого необходимо:

1. Провести анализ существующих решений в области видеоаналитики и методов детекции угроз.

2. Разработать архитектуру системы, обеспечивающую высокую точность распознавания (более 80 %) и скорость обработки (более 25 кадров в секунду).

3. Сформировать и аннотировать датасет, включающий видеозаписи с маркировкой скрытых лиц (маски, капюшоны) и наличия оружия.

4. Реализовать прототип системы с использованием современных технологий (YOLOv8, Python, OpenCV).

5. Провести тестирование системы для оценки корректности распознавания, устойчивости к различным условиям (освещение, ракурсы) и производительности.

6. Обеспечить возможность масштабирования системы для работы с множеством камер.

Архитектура системы

Разработанная нейросетевая система видеоаналитики реализована на основе модульного подхода, обеспечивающего высокую производительность, масштабируемость и адаптивность к условиям эксплуатации [6, 7]. Структурная схема системы представлена на рисунке 1.

Система начинается с модуля захвата видеопотока, интегрированного с IP-камерами через стандартные протоколы RTSP/HTTP. Входящие данные преобразуются в последовательность кадров с разрешением 1280×720 пикселей и частотой 25 кадров в секунду, после чего подвергаются предобработке [8]. На этом этапе выполняется нормализация яркости, коррекция разрешения и снижение шумов с применением алгоритма Non-Local Means Denoising, что повышает стабильность работы последующих модулей при изменении условий освещенности [9].

Детекция объектов реализована на базе модели YOLOv8m (средняя версия), дообученной на кастом-

ном датасете для распознавания двух классов: «скрытое лицо» (капюшоны, маски, балаклавы) и «оружие» (огнестрельное и холодное оружие). Выбор YOLOv8 обусловлен его высокой точностью и скоростью обработки, что критично для реального времени. Архитектурные улучшения, такие как SPPF-блоки и Anchor-Free детекция, обеспечивают эффективное использование ресурсов GPU при работе с мелкими и частично скрытыми объектами [10]. Для интеграции с системой использован фреймворк PyTorch с оптимизацией вычислений через CUDA.

Постобработка данных включает фильтрацию ложных срабатываний и анализ событийной логики. Для минимизации ошибок применен алгоритм временной устойчивости, требующий подтверждения тревоги в трех последовательных кадрах. Дополнительно реализован трекинг объектов на базе DeepSORT, отслеживающий траектории движения и идентифицирующий потенциально опасные сценарии, например одновременное присутствие «скрытого лица» и «оружия» в кадре. Реализация алгоритмов постобработки выполнена на Python с использованием библиотек NumPy и SciPy для работы с временными рядами.

Интерфейс взаимодействия обеспечивает визуализацию результатов через наложение bounding boxes и текстовых меток на видеопоток с использованием библиотеки OpenCV. Для интеграции с внешними системами безопасности разработан REST API, передающий тревожные события в формате JSON и активирующий звуковые оповещения. Все инциденты фиксируются в базе данных PostgreSQL с привязкой к временным меткам для последующего аудита.

Масштабируемость системы обеспечена контейнеризацией (Docker) и распределением нагрузки между несколькими графическими ускорителями.

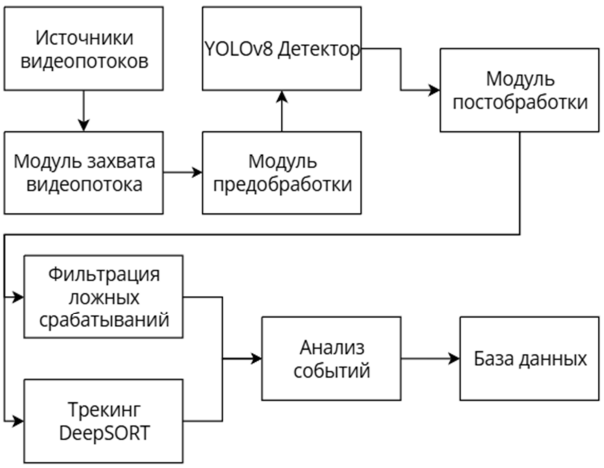

Рис. 1. Блок-схема архитектуры системы

Обучение модели

Процесс обучения модели YOLOv8m осуществлялся с использованием облачной платформы Roboflow для подготовки датасета и Google Colab для проведения экспериментов. Исходный датасет включал 9450 изображений, собранных из открытых источников: CCTV-записей общественных учреждений, симулированных сцен с участием актеров и публично доступных баз данных (Kaggle) [11]. На платформе Roboflow выполнена разметка объектов двух классов «скрытое лицо» и «оружие» с помощью инструмента автоматической полигональной аннотации и последующей ручной верификации. Для повышения качества данных применены встроенные функции Roboflow:

1. Балансировка классов (устранение дисбаланса через oversampling для класса «оружие»).

2. Синтетическая аугментация: добавление искусственных объектов оружия на изображения с использованием технологии Generative Adversarial Networks (GAN).

3. Предобработка: автообрезание, нормализация гистограмм, преобразование в формат YOLOv8 Pytorch.

Итоговый датасет после аугментации составил 14 200 изображений, разделенных на обучающую (70 %), валидационную (20 %) и тестовую (10 %) выборки. Обучение проводилось в Google Colab на GPU Tesla T4 (16 ГБ VRAM) с использованием библиотеки Ultralytics для YOLOv8. Гиперпараметры настроены через конфигурационный файл:

– Размер пакета (batch size): 16 (ограничение VRAM).

– Количество эпох: 30.

– Оптимизатор: SGD с моментом (momentum=0.9).

– Скорость обучения (learning rate): 0.01 с расписанием OneCycleLR.

– Аугментация в реальном времени: поворот (±25°), масштабирование (±30 %), мозаика (mosaic= 0.5), HSV-коррекция (насыщенность ±50 %).

Интеграция с Roboflow позволила автоматизировать конвейер данных: экспорт в формате YOLOv8, генерация аугментированных версий и управление версиями датасета. Для ускорения обучения в Colab использовано кэширование данных на Google Drive.

На рисунок 2 представлены кривые обучения, отражающие динамику метрик точности (mAP@0.5, mAP@0.5-0.95) и потерь (train/val loss). Модель достигла максимального mAP@0.5 ≈ 80 % на валидационной выборке к 30-й эпохе, после чего процесс обучения был завершен.

Потери на обучении (box_loss ≈ 1.5, cls_loss ≈ 1.0, dfl_loss ≈ 1.7) и валидации (box_loss ≈ 1.8, cls_loss ≈ 2.0, dfl_loss ≈ 2.0) демонстрируют устойчивую сходимость без признаков переобучения.

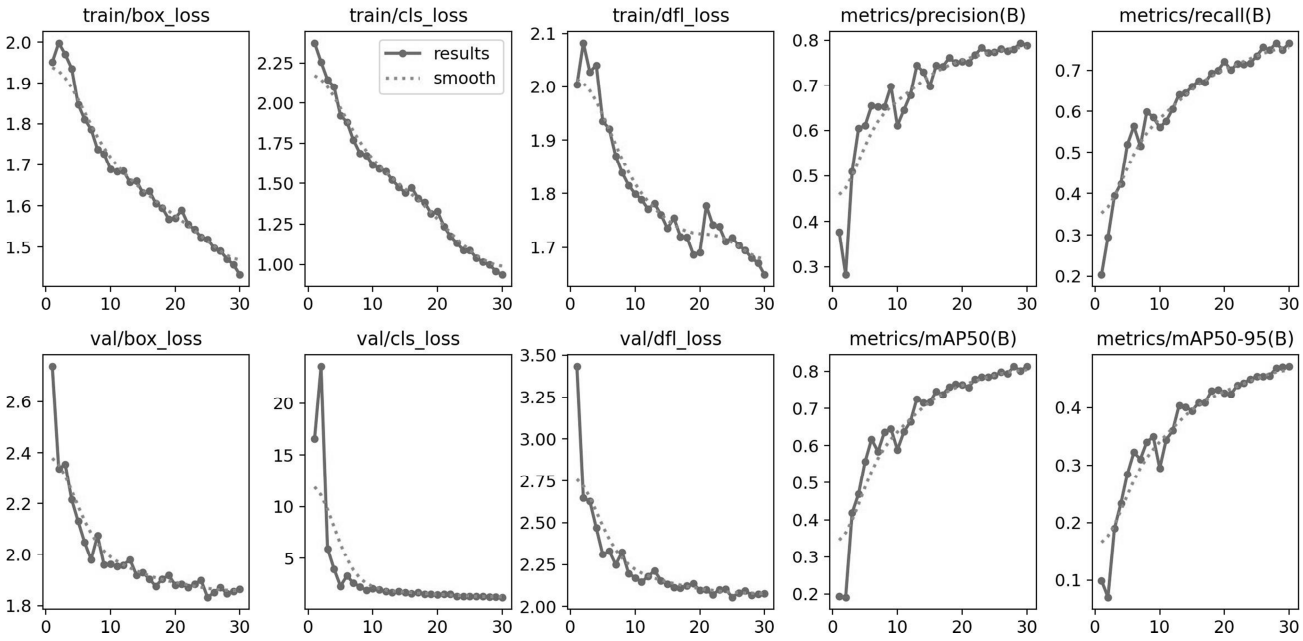

Рис. 2. Метрики и потери

Тестирование

Для финальной проверки использовалась выделенная тестовая выборка (1420 изображений), не участвовавшая в обучении и валидации. Результаты оценки представлены в таблице.

Таблица

Результаты тестирования системы на выделенной выборке

Метрика	Скрытое лицо	Оружие	Среднее
Точность (Precision)	83.2 %	77.5 %	80.4 %
Полнота (Recall)	81.7 %	75.8 %	78.8 %
mAP@0.5	84.1 %	78.3 %	81.2 %

Анализ показал, что основная доля ошибок (18 %) связана с детекцией мелких объектов (ножи в руках, пистолеты в карманах), ложными срабатываниями на предметы, имитирующие оружие (мобильные телефоны, строительные инструменты), частично скрытыми лицами (капюшоны в профиль, маски с прозрачными вставками).

Система интегрирована в прототип приложения на Python с использованием библиотек OpenCV (обработка видео) и FastAPI (REST-интерфейс). Для визуализации результатов разработан GUI. Система успешно детектирует объекты в реальном времени, накладывая bounding boxes и метки на видео.

Результаты

Разработанная система видеоаналитики продемонстрировала высокую эффективность в ходе тестирования. На выделенной тестовой выборке (1420 изображений) была достигнута средняя точность (mAP@0.5) 81,2 % при скорости обработки 25 кадров в секунду, что соответствует требованиям реального времени. Модель успешно распознает объекты в сложных условиях: при частичном перекрытии лиц (капюшоны, маски), малом размере оружия и динамичных ракурсах.

Система интегрирована в прототип приложения с графическим интерфейсом, который визуализирует детекцию в реальном времени, а также в REST API для взаимодействия с внешними системами безопасности. Благодаря обработке в реальном времени система мгновенно генерирует тревожные уведомления, сокращая время между обнаружением угрозы и действиями служб безопасности. Например, при детекции оружия или скрытого лица оповещение поступает оператору в течение менее одной секунды, что существенно ускоряет реакцию.

Заключение

В работе предложена нейросетевая система видеоаналитики для автоматического обнаружения потенциально опасных ситуаций в общественных учреждениях. На базе YOLOv8m разработана модель, сочетающая точность, скорость и низкие аппаратные требования.

Для дальнейшего развития можно добавить:

1. Расширение датасета синтетическими данными для улучшения детекции в ИК-спектре и при низком разрешении.

2. Добавление классов «агрессивные жесты» и «оставленные предметы».

3. Оптимизация модели для работы на edge-устройствах, таких как Jetson Nano, с использованием квантования INT8 для повышения производительности.

Результаты работы подтверждают, что система может стать основой для интеллектуальных систем безопасности, сокращающих зависимость от человеческого фактора.

Литература

1. Душин, И. Объектная видеоаналитика реального времени / И. Душин // Открытые системы. СУБД. – 2019. – № 4. – С. 8. – ISSN 1028-7493.

2. Махонин, М. Н. разработка системы распознавания товаров на базе нейронных сетей / М. Н. Махонин, Д. В. Кочкин // Школа практических инноваций – инженерному бизнесу региона : материалы Всероссийской научно-практической конференции памяти профессора Александра Николаевича Шичкова, Вологда, 19 января 2024 года. – Вологда : Вологодский государственный университет, 2024. – С. 177–182. – EDN FDCYXL.

3. Махонин, М. Н. Детектор товаров на базе нейронной сети / М. Н. Махонин, Д. В. Кочкин // Интеллектуально-информационные технологии и интеллектуальный бизнес (ИНФОС-2024) : материалы Пятнадцатой Международной научно-технической конференции (Вологда, 27–28 июня 2024 г.). – Вологда : Вологодский государственный университет, 2024. – С. 22-25. – EDN KWRTYN.

4. Принципы построения самоорганизующихся информационно-телекоммуникационных систем / А. А. Суконщиков, А. Н. Швецов, И. А. Андрианов, Д. В. Кочкин // Вестник Череповецкого государственного университета. – 2021. – № 1 (100). – С. 56–67. – DOI 10.23859/1994-0637-2021-1-100-4. – EDN FUTTMS.

5. Ситуационные интеллектуальные системы поддержки принятия решений / А. Н. Швецов, А. А. Суконщиков, Д. В. Кочкин, И. А. Андрианов. – Курск : Закрытое акционерное общество "Университетская книга", 2018. – 251 с. – ISBN 978-5-907049-26-0. – EDN OSGGJV.

6. Кочкин, Д. В. Проектирование и конструирование программного обеспечения : учебное пособие / Д. В. Кочкин, А. Н. Швецов. – Вологда : Вологда, 2023. – 127 с. – ISBN 978-5-907606-66-1. – EDN JCEZKE.

7. Распределенные интеллектуальные информационные системы и среды / А. Н. Швецов, А. А. Суконщиков, Д. В. Кочкин [и др.] ; под редакцией А. Н. Швецова и А. А. Суконщикова. – Курск : Закрытое акционерное общество "Университетская книга", 2017. – 197 с. – ISBN 978-5-9909988-3-4. – EDN YNAOSP.

8. Яковлева, М. В. Исследования возможностей по внедрению интеллектуальных систем видеоаналитики в образовательных учреждениях / Яковлева М. В., Низовая А. А. // Информатизация в цифровой экономике. – 2023. – Т. 4, № 2. – С. 105–118.

9. Тихановский, Г. С. Исследование возможностей применения алгоритмов глубокого обучения и компьютерного зрения в задаче классификации грибов и ягод / Г. С. Тихановский, Д. В. Кочкин // Вестник Вологодского государственного университета. Серия: Технические науки. – 2023. – № 4 (22). – С. 41–46. – EDN UVJLNG.

10. Созыкин, А. В. Обзор методов обучения глубоких нейронных сетей / А. В. Созыкин // Вестник Южно-Уральского государственного университета. Серия: Вычислительная математика и информатика. – 2017. – Т. 6, № 3. – С. 28–59. – ISSN 2305-9052, eISSN 2410-7034. – DOI: 10.14529/cmse170303.

11. Ян Лекун. Как учится машина. Революция в области нейронных сетей и глубокого обучения / Ян Лекун. – Москва : Альпина нон-фикшн, 2021. – 454 с.

V.M. Slivnitsyn, D.V. Kochkin
Vologda State University

DEVELOPMENT OF NEURAL NETWORK VIDEO ANALYTICS SYSTEM FOR AUTOMATED RECOGNITION OF POTENTIALLY DANGEROUS SITUATIONS IN PUBLIC INSTITUTIONS

The article presents the development of a neural network video analytics system for automated recognition of potentially dangerous situations in public institutions. The main focus is on the use of deep learning methods (YOLOv8) for identifying suspicious people and weapons in real time. The architecture and algorithms of the system are described, and testing is conducted, which showed recognition accuracy at the level of 80%. The development is aimed at improving the safety of visitors and personnel in public institutions. The possibilities of scaling and additional training of the neural network to improve accuracy and expand the number of recognizable objects are considered.

Neural network systems, video analytics, security, computer vision, machine learning, YOLOv8, Python, threat recognition, deep learning.