

Список литературы

1. Распоряжение Правительства РФ от 2 декабря 2021 г. № 3427-р «Об утверждении стратегического направления в области цифровой трансформации образования, относящейся к сфере деятельности Министерства просвещения РФ». URL: <https://www.garant.ru/products/ipo/prime/doc/403075723/> (дата обращения: 15.12.2025).
2. Распоряжение Правительства РФ от 16 июля 2020 г. № 1845-р «Об утверждении методических рекомендаций по порядку формирования и ведения региональных информационных систем, указанных в части 14 статьи 98 Федерального закона «Об образовании в Российской Федерации», в том числе по порядку предоставления родителям (законным представителям) детей сведений из них». URL: <https://www.garant.ru/products/ipo/prime/doc/74299773/> (дата обращения: 15.12.2025).
3. Статья 98. Информационные системы в системе образования Федерального закона от 29.12.2012 N 273-ФЗ (ред. от 15.12.2025) «Об образовании в Российской Федерации». URL: https://www.consultant.ru/document/cons_doc_LAW_140174/07b2a433c35195c28c56a221a970dc3ce333fade/ (дата обращения: 15.12.2025).
4. Постановление Правительства РФ от 13 июля 2022 г. N 1241 «О федеральной государственной информационной системе «Моя школа» и внесении изменения в подпункт «а» пункта 2 Положения об инфраструктуре, обеспечивающей информационно-технологическое взаимодействие информационных систем, используемых для предоставления государственных и муниципальных услуг и исполнения государственных и муниципальных функций в электронной форме». URL: <https://base.garant.ru/405000799/> (дата обращения: 15.12.2025).
5. Федеральный закон №156-ФЗ от 24.06.2025 «О создании многофункционального сервиса обмена информацией и о внесении изменений в отдельные законодательные акты Российской Федерации». URL: <https://www.garant.ru/products/ipo/prime/doc/412110426/> (дата обращения: 15.12.2025).

ОБЗОР АЛГОРИТМОВ ДЕТЕКЦИИ ЛИЦ И ИХ СРАВНИТЕЛЬНЫЙ АНАЛИЗ ДЛЯ РАЗРАБОТКИ ПРИЛОЖЕНИЯ СИСТЕМЫ УЧЁТА РАБОЧЕГО ВРЕМЕНИ СОТРУДНИКА

Чернышев О.Г.

ФГБОУ ВО «Мелитопольский государственный университет», Мелитополь,
e-mail: a.shapurov@melsu.ru

Научный руководитель: Шануров А. А.

Введение

В эпоху стремительной цифровизации бизнеса и повсеместной автоматизации процессов человеческие ресурсы становятся важнейшим активом любой организации. Эффективность управления персоналом напрямую зависит от точности и объективности данных о его деятельности, а основой для этого служит достоверный учет рабочего времени. Традиционные методы учета, такие как бумажные журналы или электронные таблицы с ручным вводом данных, а также простые системы на основе пропускных карт, не справляются с вызовами современного быстроразвивающегося предприятия. Они подвержены ошибкам, «припискам», «дружескому» учету времени коллегами («buddy punching»), требуют много времени на админи-

стрирование и не обеспечивают необходимого уровня достоверности и аналитики.

В этой связи разработка автоматизированной системы учета рабочего времени, основанной на биометрической идентификации сотрудников с использованием технологий компьютерного зрения, представляется исключительно актуальной и востребованной задачей.

Биометрическая идентификация по лицу – это метод, который, в отличие от пропускной карты, брелока или PIN-кода, невозможно передать, потерять, украсть или подделать без использования сложных высокотехнологичных средств. Это позволяет полностью устранить проблему «buddy punching», когда один сотрудник отмечает приход или уход за другого.

Внедрение такой системы обеспечит справедливые и равные для всех условия учета для всех сотрудников, минимизирует риски внутреннего мошенничества и повышает общий уровень корпоративной безопасности, ограничивая доступ в помещения только авторизованным сотрудникам.

Детекция лиц (Face Detection) является основополагающий и критически важный этап в разработке приложения для учёта рабочего времени сотрудников. Задача алгоритма – автоматическое обнаружение и локализация лиц на изображении или в видеопотоке. Эффективность и точность всей системы распознавания напрямую зависят от качества выполнения этого начального этапа.

Цель исследования – изучить алгоритмы распознавания лиц и провести их сравнительный анализ для создания программного обеспечения, которое будет учитывать рабочее время сотрудников.

Материалы и методы исследования

В процессе исследования были проанализированы научные публикации и техническая документация, которые раскрывают принципы работы, архитектуру, а также преимущества и недостатки трёх основных классов алгоритмов, предназначенных для обнаружения лиц. Анализ носил сравнительный и аналитический характер. В ходе исследования были систематизированы и оценены следующие методы:

Алгоритм Виолы-Джонса (каскады Хаара). Были подробно изучены ключевые составляющие данного алгоритма: признаки Хаара для выявления контрастных особенностей, интегральное изображение для ускорения вычислений и каскадная структура классификаторов для быстрого отбраковки негативных регионов. В качестве практической реализации рассмотрена предобученная модель `haarcascade_frontalface_default.xml` из библиотеки OpenCV.

Метод HOG (Histogram of Oriented Gradients) с классификатором SVM. В этом методе для распознавания объектов используется дескриптор,

который строится на основе гистограмм направлений градиентов яркости в локальных областях изображения. Затем дескриптор нормализуется внутри блоков. Для принятия решений применяется линейный классификатор опорных векторов. В качестве примера реализации этого метода можно привести детектор из библиотеки Dlib.

Методы на основе глубоких нейронных сетей (DNN). Исследованы две основные архитектурные парадигмы: двухэтапные детекторы (например, Faster R-CNN) и одноэтапные детекторы (такие как SSD и YOLO). Особое внимание уделено оптимизированным для работы в реальном времени моделям (например, MobileNet-SSD). В качестве основного инструмента для применения данного класса методов рассмотрен DNN-модуль библиотеки OpenCV (cv2.dnn), который поддерживает загрузку предобученных моделей из фреймворков Caffe, TensorFlow и других. Конкретным примером является легковесная модель `opencv_face_detector_caffe_model`.

Для сравнительного анализа были выбраны следующие критерии:

1. Точность распознавания в различных условиях, включая освещение, ракурс и наличие препятствий.
2. Скорость работы алгоритма.
3. Требования к вычислительным ресурсам, таким как CPU и GPU.
4. Легкость интеграции в уже существующие программные продукты.

Результаты исследования и их обсуждение

Детекция лиц (Face Detection) представляет ключевую задачу компьютерного зрения, заключающаяся в автоматическом обнаружении и локализации лиц на цифровых изображениях

или в видеопотоке. Качество и эффективность этого этапа напрямую влияют на точность всей системы распознавания. В настоящее время для решения этой задачи широко применяются три класса алгоритмов: методы на основе признаков (каскады Хаара), на основе гистограмм ориентированных градиентов и на основе глубоких нейронных сетей. Сравнительный анализ их характеристик является основой для обоснованного выбора технологии для проекта.

1. *Алгоритм Виолы-Джонса (каскады Хаара – Haar Cascades)*. Данный алгоритм, предложенный в 2001 году, стал первым эффективным методом для детекции объектов в реальном времени [1]. Его работа основывается на трёх ключевых идеях (рис. 1):

1. Признаки Хаара (Haar-like Features) – это простые прямоугольные шаблоны, которые вычисляют разность сумм интенсивностей пикселей в белой и чёрной областях. Эти признаки позволяют эффективно выявлять контрастные особенности лица, такие как область глаз (тёмная) относительно переносицы (светлая) или вертикальные границы носа [2, с. 154].

2. Интегральное изображение (Integral Image) – это техника, позволяющая вычислять суммы интенсивностей в прямоугольных областях изображения за константное время, что обеспечивает высокую скорость расчёта большого количества признаков [1].

3. Каскадный классификатор (Cascade of Classifiers) – это алгоритм, основанный на последовательном применении простых классификаторов. Если область изображения не проходит через каждый этап, она сразу исключается из дальнейшего рассмотрения. Благодаря этому основное время тратится только на обработку областей-кандидатов, что обеспечивает высокую скорость работы [1].

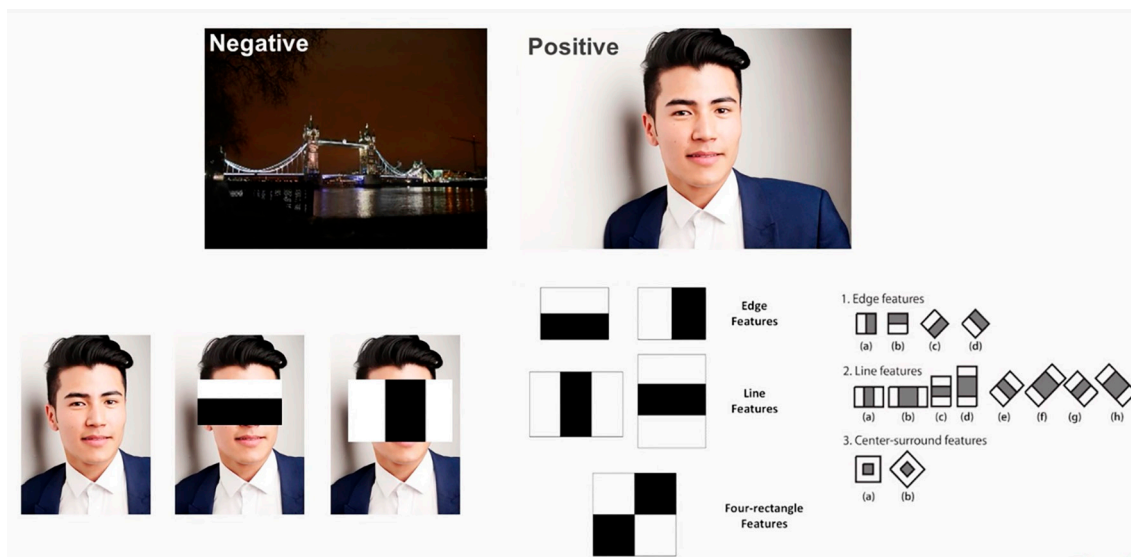


Рис. 1. Алгоритм Виолы-Джонса (каскады Хаара – Haar Cascades) [7]

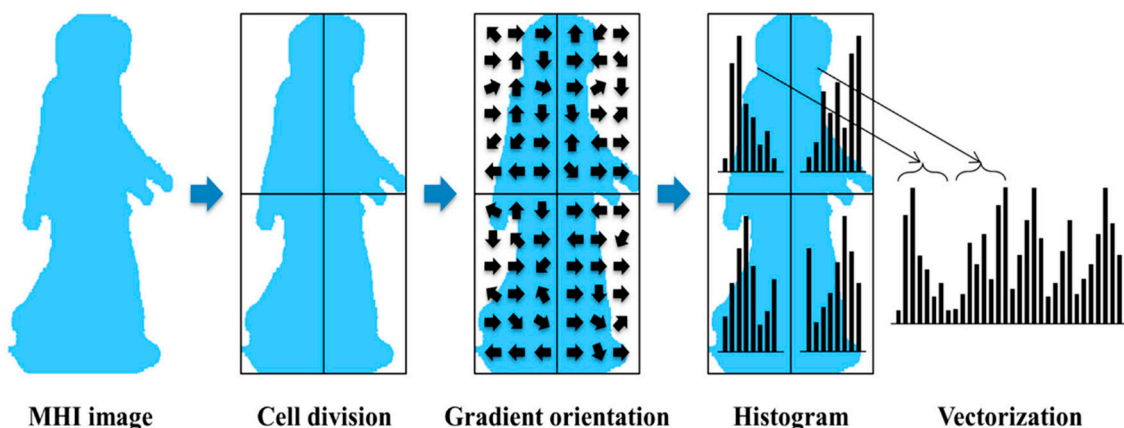


Рис. 2. Метод гистограммы ориентированных градиентов [8]

Преимущества метода включают высокую скорость работы на CPU, простоту реализации и наличие предобученных моделей во многих библиотеках, включая OpenCV (haarcascade_frontalface_default.xml). Основные недостатки – низкая устойчивость к изменениям ракурса (оптимизирован для фронтальных лиц), чувствительность к сложному фону и освещению, а также более низкая точность по сравнению с современными методами на основе глубокого обучения.

2. Метод гистограммы ориентированных градиентов (HOG – Histogram of Oriented Gradients). HOG был первоначально разработан для детекции пешеходов, но успешно адаптирован для лиц в комбинации с классификатором опорных векторов [3, с. 101]. Алгоритм не использует непосредственно интенсивность пикселей, а анализирует структуру объекта (рис. 2).

Принцип работы HOG заключается в следующем: изображение делится на небольшие ячей-

ки, и для каждой из них строится гистограмма направлений градиентов яркости, также известных как ориентации краев. Эти локальные гистограммы затем нормализуются внутри более крупных блоков для компенсации изменений освещённости. Полученный дескриптор HOG описывает форму и контуры объекта [3, с. 103].

Полученный вектор признаков подаётся на вход линейного классификатора SVM, который обучается отличать лицо от не-лица. В сравнении с каскадами Хаара, HOG обычно демонстрирует более высокую точность и лучшую устойчивость к изменению освещения благодаря нормализации градиентов. Однако этот метод, как правило, требует больше вычислительных ресурсов и работает медленнее, чем каскады Хаара, особенно при работе с большими изображениями. Реализация HOG для детекции лиц доступна, например, в библиотеке Dlib.

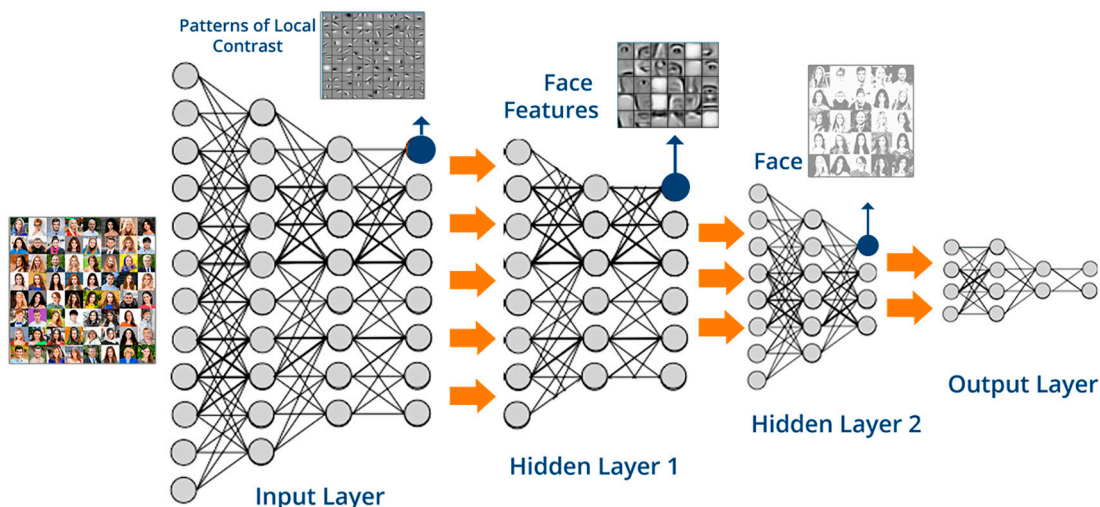


Рис. 3. Deep Neural Networks (Глубокие нейронные сети) [9]

3. Методы на основе глубоких нейронных сетей (DNN – Deep Neural Networks). Современный этап развития детекции лиц связан с применением сверточных нейронных сетей (Convolutional Neural Networks, CNN) и более сложных архитектур [4, с. 17]. Эти методы можно разделить на две основные категории: двухэтапные (two-stage) и одноэтапные (one-stage) детекторы (рис. 3).

Двухэтапные детекторы, такие как Faster R-CNN, работают в два этапа: сначала они выделяют области, которые могут содержать объекты (Region Proposal Network), а затем классифицируют каждый регион и уточняют его границы. Этот подход обеспечивает высокую точность, но требует больше времени для обработки изображений [5, с. 123].

Одноэтапные детекторы (например, SSD – Single Shot MultiBox Detector, YOLO – You Only Look Once): Они прогнозируют координаты ограничивающих рамок (bounding boxes) и вероятности классов непосредственно за один проход по сети. Эти детекторы обеспечивают оптимальный баланс между скоростью и точностью и наиболее пригодны для работы в реальном времени [5, с. 125].

Преимущества DNN-методов неоспоримы: они обеспечивают наивысшую точность детекции, высокую устойчивость к окклюзиям частичному перекрытию лица (окклюзиям), изменению ракурса, масштаба и освещённости. Современные сети обучаются на огромных наборах данных таких как WIDER FACE, что позволяет им обобщать сложные закономерности. Главный недостаток – высокие требования к вычислительным ресурсам. Для обеспечения скорости, приемлемой для реального времени, часто требуется использование графических процессоров (GPU). Тем не менее, существуют оптимизированные легковесные модели такие как MobileNet-SSD, способные работать и на CPU.

При выборе алгоритма распознавания для конкретной системы необходимо учитывать три ключевых параметра: точностью, скоростью и ресурсоёмкостью. Для разрабатываемой системы учёта рабочего времени, где приоритетом является надёжная фиксация событий, наиболее предпочтительным является использование современных методов на основе глубоких нейронных сетей (DNN). Несмотря на повышенные требования к вычислительным ресурсам, ключевые преимущества DNN – высочайшая точность и устойчивость к изменениям ракурса, освещения и наличию аксессуаров – критически важны для обеспечения надёжности системы в реальных, неидеальных условиях офисной среды [4, с. 17].

Использование DNN-модуля библиотеки OpenCV (cv2.dnn) предоставляет уникальную возможность объединить передовую точность

нейросетевых моделей, таких как MobileNet-SSD или OpenPose и удобство интеграции в выбранный технологический стек. Данный модуль поддерживает загрузку предобученных моделей из популярных фреймворков, включая TensorFlow, Caffe, PyTorch, PyCharm, что избавляет от необходимости их сложного обучения с нуля [6]. Для нивелирования повышенной вычислительной нагрузки можно выбрать оптимизированную, легковесную модель например, `opencv_face_detector_caffemodel`, которая поставляется с OpenCV и специально разработана для баланса скорости и качества на CPU. Таким образом, выбор в пользу DNN-детектора в OpenCV является разумным решением для создания надёжной и технологически современной системы, отвечающей строгим требованиям к точности. При условии правильного выбора конкретной архитектуры нейронной сети, DNN-детектор в OpenCV станет основой для создания высокоточного и современного решения.

Выводы

Проведённый сравнительный анализ алгоритмов распознавания лиц наглядно демонстрирует, что методы на основе глубоких нейронных сетей значительно превосходят классические подходы, такие как Haar Cascades, HOG, по ключевому для нашего проекта параметру – точности распознавания в разнообразных условиях. Хотя DNN-методы предъявляют более высокие требования к вычислительным ресурсам, использование оптимизированных предобученных моделей через DNN-модуль OpenCV позволяет успешно применять их на стандартном CPU, что подтверждается практикой внедрения. Таким образом, выбор в пользу DNN-детектора, являющегося стратегическим решением, направленным на обеспечение максимальной надёжности и устойчивости системы биометрического учёта к внешним факторам, таким как освещение, ракурс. Это напрямую влияет на выполнение нефункционального требования по низкому проценту ложных отказов. Классические алгоритмы, как Haar Cascades сохраняют свою актуальность благодаря своей скорости и простоте, однако для решения поставленной задачи с высокими требованиями к достоверности приоритет отдаётся передовой нейросетевой методологии.

Список литературы

1. Viola P., Jones M. Rapid Object Detection using a Boosted Cascade of Simple Features // Proceedings of the 2001 IEEE Computer Society Conference on Computer Vision and Pattern Recognition (CVPR). 2001. Vol. 1. URL: <https://ieeexplore.ieee.org/document/990517> (дата обращения: 15.12.2025).
2. Брэдки Г., Келер Дж., Бэхук Э. Освой самостоятельное компьютерное зрение на языке Python за 24 часа / пер. с англ. Москва: Вильямс, 2022. 432 с.
3. Павлов С. С., Федоров А. И. Методы и алгоритмы детектирования лиц в видеопотоке в реальном времени // Известия ЮФУ. Технические науки. 2021. № 5 (214). С. 98–110.

4. Бобина М. А., Волков С. К. Сравнительный анализ алгоритмов распознавания лиц в условиях неидеального освещения // Информационные технологии и вычислительные системы. 2023. № 2. С. 12–24.

5. Шаров В. И., Новикова Т. П. Применение библиотеки OpenCV для задач компьютерного зрения в образовательных проектах // Современные информационные технологии и ИТ-образование. 2022. Т. 18, № 1. С. 120–129.

6. Документация библиотеки OpenCV. URL: <https://docs.opencv.org/4.x/> (дата обращения: 15.12.2025).

7. 25 Object Detection with HAAR Cascade Classifiers. URL: <https://www.youtube.com/watch?v=kThRJyQCW-8> (дата обращения: 15.12.2025).

8. Continuous Human Action Recognition Using Depth-MHI-HOG and a Spotter Model. URL: <https://www.mdpi.com/1424-8220/15/3/5197> (дата обращения: 15.12.2025).

9. Deep Learning Vs Machine Learning. URL: <https://k21academy.com/ai-ml/dl-vs-ml/> (дата обращения: 15.12.2025).

ОСОБЕННОСТИ МУЛЬТИМЕДИЙНЫХ ПАРКОВ КАК ОБЪЕКТА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Чикарь Л. А., Мозговенко А. А.

*ФГБОУ ВО «Мелитопольский государственный университет», Мелитополь,
e-mail: ya@amozgovenko.ru*

Задачи исследования:

1. Определить понятие «информационная безопасность».
2. Осуществить анализ существующих типов угроз.
3. Выявить интересы субъектов информационных отношений.
4. Провести анализ мер защиты.

Материалы и методы исследования

Исследования и публикации в области информационной безопасности мультимедийных парков:

1. Научная статья Ирины Владимировны Топчий «Мультимедийные технологии в современном музее как инструмент привлечения посетителей (на примере музея-заповедника «Ар-каим»)» (журнал «Знак: проблемное поле медиаобразования», 2024). В статье рассмотрены возможности использования мультимедийных технологий в пространстве музея, а также классификации таких технологий.

2. Исследование Т. В. Румянцевой «Роль медиапроектов при продвижении музея» (2024). Исследователь отмечает, что оригинальный медиа контент, основанный на уникальной экспозиции, может быть представлен в формате виртуального пространства музея в виде видеоролика или трейлера для популяризации его деятельности [2].

Основная цель – создать защиту информации и поддерживающей её инфраструктуры от случайных или преднамеренных воздействий, которые могут нанести ущерб владельцам или пользователям информации.

Результаты исследования и их обсуждение

Рассмотрим мультимедийный парк как объект информационной безопасности – обеспечение конфиденциальности, целостности и доступности информации в информационных системах, связанных с использованием мультимедийных технологий. Это связано с тем, что мультимедийные данные (изображение, видео, аудио) подвергаются угрозам, и необходимо минимизировать риски, прогнозировать возможные негативные воздействия и предотвращать их.

Виды целей информационной безопасности для мультимедийных парков:

1. Конфиденциальность – доступ к информации только у лиц, имеющих на это полномочия.
2. Целостность – блокировка несанкционированного изменения информации.
3. Доступность – возможность получить требуемую информационную услугу за приемлемое время.
4. Подлинность – полнота и общая точность информации.
5. Неотказуемость – возможность определить источник или авторство информации [1].

Эти цели важны, так как информационные системы создаются для получения определённых информационных услуг, и, если предоставить эти услуги пользователям становится невозможно, это наносит ущерб [3].

Все эти элементы связаны в единую сеть, обеспечивающую бесперебойное функционирование контента и сервисов, и именно эта взаимосвязанность определяет особую уязвимость подобной среды. Любое нарушение в одном из сегментов инфраструктуры может повлечь за собой цепную реакцию сбоев, затронуть критические активы и повлиять на доступность и целостность информации.

С точки зрения информационной безопасности мультимедийные парки относятся к категории объектов с повышенной степенью риска. Это объясняется их публичностью, открытым доступом для большого количества пользователей и разнообразием подключаемых устройств, зачастую использующих стандартные беспроводные интерфейсы и протоколы связи. Высокая плотность цифрового оборудования и использование множества каналов передачи данных (локальные сети, Wi-Fi, Bluetooth, NFC, IT-протоколы) создают широкое поле для потенциальных киберугроз. При этом специфика работы подобных учреждений требует постоянного взаимодействия с внешними источниками информации – облачными платформами, сервисами обновления контента, платёжными шлюзами и базами данных партнёров, что дополнительно увеличивает количество точек возможного воздействия.

Мультимедийные парки одновременно выполняют функции культурно-просветительско-