УДК 004.932.2

РАЗРАБОТКА ЛЕГКОВЕСНОГО АЛГОРИТМА ДЕТЕКЦИИ «ЖИВОСТИ» ЛИЦА (LIVENESS DETECTION) ДЛЯ СИСТЕМ ВЕБ-ИДЕНТИФИКАЦИИ

И.В. Андриалович
Заместитель декана по ИВР факультета компьютерного проектирования БГУИР, аспирант кафедры ИПиЭ
andryinna@bsuir.by

И.П. Галяк
Студент кафедры проектирования информационно-компьютерных систем ФКП БГУИР
haliak.ivanba@gmail.com

Е.А. Касперец
Студент кафедры инженерной психологии и эргономики БГУИР
kasperetsyevgeny@gmail.com

И.В. Андриалович
Окончила Белорусский государственный университет информатики и радиоэлектроники. Область научных интересов связана с исследованием проблем психологического выгорания профессорско-педагогического состава учреждений высшего образования.

И.П. Галяк
Студент кафедры проектирования информационно-компьютерных систем БГУИР. Область профессиональных интересов / исследований: бизнес-системный анализ, применение методов анализа данных и технологий искусственного интеллекта для оптимизации бизнес-процессов, и поддержки принятия решений.

Е.А. Касперец
Студент кафедры инженерной психологии и эргономики БГУИР. Область профессиональных интересов / исследований: языки программирования, искусственный интеллект, исследование инженерной психологии.

Аннотация. В статье рассматривается разработка легковесного алгоритма проверки «живости» лица в режиме реального времени, предназначенного для противодействия подделке биометрических данных в системах веб-идентификации. Предложенный метод базируется на анализе антропометрических точек лица с использованием алгоритмов компьютерного зрения. Данный подход позволяет снизить требованиях к аппаратным ресурсам, что делает его эффективной альтернативой ресурсоемким нейросетевым решениям.

Ключевые слова: детекция «живости», биометрическая аутентификация, компьютерное зрение, подделка биометрических данных, веб-идентификация, антропометрические точки лица.

Введение. В условиях глобальной цифровизации и перехода к удаленному обслуживанию в финансовом, государственном и корпоративном секторах, биометрическая аутентификация по лицу стала неотъемлемым компонентом комплексных систем безопасности. Однако рост вычислительных мощностей и совершенствование методов синтеза медиаконтента привели к резкому увеличению числа атак на подобные системы. Согласно действующему международному стандарту *ISO/IEC* 30107-1:2023, подобные угрозы классифицируются как предоставление системе биометрического захвата данных, целью которого является вмешательство в работу биометрической системы [1]. В рамках терминологии стандарта атаки могут осуществляться двумя типами субъектов: биометрическим самозванцем, который стремится быть распознанным как

конкретное другое лицо, известное системе, или биометрическим маскировщиком, чья цель – избежать распознавания или скрыть свои собственные характеристики без намерения имитировать кого-либо.

Несмотря на различие в мотивах злоумышленников, угроза в обоих случаях зачастую сводится к атаке на уровне предъявления (*Presentation Attack*), в частности непосредственно на сенсор захвата данных. В данной работе рассматривается противодействие этому типу атак. Ключевой контрмерой в данном случае выступает проверка «живости» (*liveness*). Под этим термином понимается измерение и анализ анатомических характеристик, а также непроизвольных или произвольных реакций с целью определения того, происходит ли сбор биометрических данных от живого субъекта, присутствующего в точке захвата. Методы проверки подлинности, основанные на этом принципе, являются подмножеством механизмов обнаружения атак (*Presentation Attack Detection – PAD*).

Современные реализации *PAD*-систем в большинстве случаев опираются на использование нейронных сетей для выявления артефактов подделанной биометрии. Несмотря на высокую точность, такие решения обладают недостатками в контексте веб-систем.

Во-первых, серверная обработка видеопотока вносит существенную задержку (*latency*), которая с учетом сетевых издержек может достигать 500–1000 мс, что является неприемлемым показателем для интерактивных пользовательских интерфейсов. Во-вторых, экономическая эффективность подобных решений при масштабировании крайне низка: производительность современных моделей на стандартных серверных *CPU* зачастую ограничена скоростью 5–15 кадров в секунду. Это вынуждает компании инвестировать в дорогостоящие *GPU*-ускорители для поддержания приемлемой производительности при обслуживании большого потока одновременных сессий верификации [2].

Целью данной работы является разработка метода активного обнаружения атак для веб-интерфейсов, лишенного указанных недостатков. В основу предлагаемого решения положен интерактивный анализ точек лица пользователя в режиме реального времени. Система генерирует случайную последовательность заданий (повороты головы, моргание, изменение мимики) – и оценивает корректность их выполнения с помощью легковесного математического аппарата компьютерного зрения, что позволяет проводить проверку на серверах без специализированного оборудования.

Теоретический базис и используемый стек технологий. В основе разработанного алгоритма лежит комбинация классических методов компьютерного зрения, что обеспечивает повышение производительности на стандартном *CPU* без привлечения специализированных ускорителей. Сам же физический процесс детекции представляет собой машину проверки состояний, которая в режиме реального времени выполняет потоковую обработку видеоданных. Для каждого кадра последовательно производятся следующие операции: локализация лица, определение координат его антропометрических точек, расчет набора числовых дескрипторов (коэффициентов открытости глаз, рта и углов поворота головы) и сравнение этих дескрипторов с пороговыми значениями, соответствующими требуемому на данном этапе действию.

Ключевым этапом всего процесса является выделение антропометрических точек лица (*Facial Landmarks*). Для решения этой задачи выбрана библиотека *Dlib* и реализованный в ней метод, использующий предварительно обученную модель, которая захватывает положение ключевых точек на основе анализа изображения. Данный подход позволяет определять координаты 68 ключевых точек, очерчивающих контуры челюсти, бровей, носа, глаз и губ (рисунок 1). Выбор в пользу *Dlib* обусловлен фокусом на производительность на центральном процессоре и достаточной точностью для решения поставленных задач [3, 4].

Рисунок 1. 68 точек лица, обнаруживаемых библиотекой *dlib*

После получения массива координат 68 точек, система переходит к расчету набора числовых дескрипторов, отражающих текущее состояние мимики и положения головы пользователя. Для количественной оценки моргания и закрытия глаз применяется коэффициент соотношения сторон глаза (*Eye Aspect Ratio – EAR*) [5]. Данный коэффициент численно выражает отношение суммы расстояний между вертикальными точками-ориентирами глаза к расстоянию между его горизонтальными точками-ориентирами. Такое соотношение остается стабильным при открытом глазе и стремительно снижается к нулю при его закрытии, что делает его индикатором моргания. По аналогии с *EAR*, для детекции улыбки введен коэффициент соотношения сторон рта (*Mouth Aspect Ratio – MAR*), который вычисляется схожим образом, оценивая степень открытия рта относительно его ширины.

Для выполнения наиболее сложной части проверки – отслеживания поворотов головы – используется метод оценки пространственного положения объекта (*Head Pose Estimation*). Данная задача сводится к классической проблеме *Perspective-n-Point* (*PnP*) и решается с помощью одноименного алгоритма (*SolvePnP*) из библиотеки *OpenCV* [6]. Метод находит ориентацию объекта в 3D-пространстве путем сопоставления набора его эталонных трехмерных точек (в данном случае – обобщенная 3D-модель лица) с их двумерными проекциями на изображении. В результате алгоритм вычисляет векторы вращения и смещения, которые затем преобразуются в углы Эйлера: рыскание (*yaw*), тангаж (*pitch*) и крен (*roll*). Анализ угла рыскания (*yaw*) позволяет системе определить, повернул ли пользователь голову влево или вправо в соответствии с полученной инструкцией.

Программная реализация и архитектура системы. Архитектура разрабатываемой системы базируется на клиент-серверном взаимодействии, оптимизированном для потоковой обработки видеоданных в веб-интерфейсе. Согласно представленной диаграмме (рисунок 2) последовательности обработки кадра, цикл начинается на стороне клиента (браузера), где с помощью интерфейса *getUserMedia* осуществляется захват видеопотока с веб-камеры пользователя. Для минимизации нагрузки на канал связи и обеспечения совместимости с протоколом *HTTP*, каждый значимый кадр подвергается преобразованию в формат *Base64*. Передача данных на сервер, реализованный на базе микрофреймворка *Flask*, осуществляется посредством асинхронных *POST*-запросов. Такой подход позволяет реализовать концепцию «тонкого клиента», где все ресурсоемкие вычисления, связанные с анализом биометрии, выносятся на серверную сторону, обеспечивая стабильную работу системы даже на мобильных устройствах с ограниченной вычислительной мощностью.

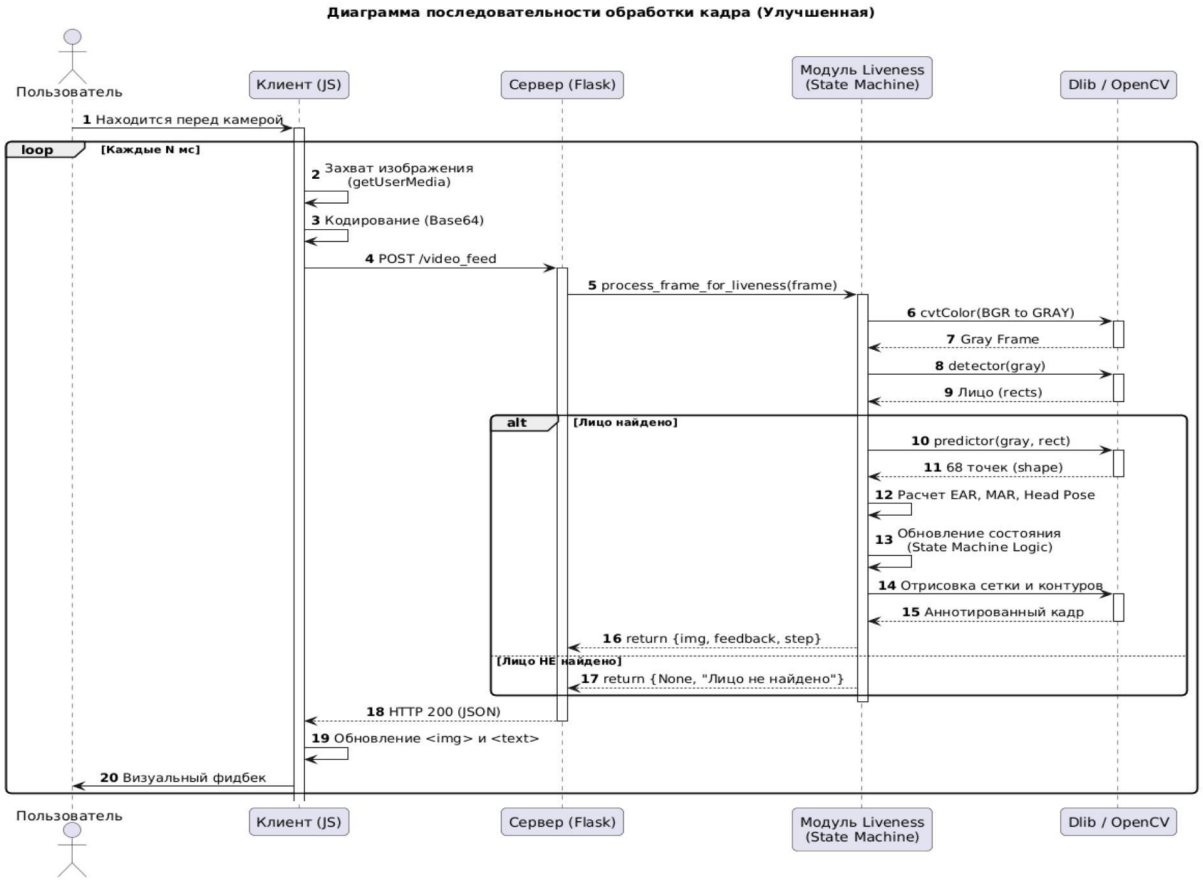

Рисунок 2. Диаграмма последовательности обработки кадра

Центральным элементом логики работы сервера выступает модуль «*Liveness State Machine*», управляющий последовательностью этапов проверки. Процесс верификации разделен на ряд последовательных состояний: от первичной локализации лица до анализа специфических команд (повороты головы, моргание, мимические реакции). Переход к каждому следующему этапу возможен только при условии успешного выполнения текущего задания, что контролируется путем непрерывного сопоставления расчетных дескрипторов (*EAR, MAR, Yaw*) с эталонными пороговыми значениями.

Подобный подход исключает возможность подмены биометрических данных статическими изображениями или заранее записанными видеофрагментами, так как система требует динамической реакции в ответ на случайно сгенерированные инструкции.

Для удобства взаимодействия с клиентом предложена подсистема визуальной обратной связи. В процессе анализа кадра модуль захвата антропометрических точек не только вычисляет математические показатели, но и формирует аннотированное изображение. На исходный видеопоток в режиме реального времени накладывается адаптивная сетка из 68 ключевых точек и контуры основных черт лица. Визуализация процесса детекции служит инструментом взаимодействия с пользователем: она позволяет субъекту корректировать положение головы относительно камеры и освещенности, а также подтверждает, что система корректно распознает его биометрические характеристики. После завершения обработки кадра сервер возвращает клиенту *JSON*-объект, содержащий текущий статус проверки, текстовую инструкцию и модифицированный кадр с наложенной графикой для отображения в браузере.

Результаты экспериментов и оценка эффективности. Для тестирования разработанного алгоритма создан веб-интерфейс, позволяющий провести экспериментальную оценку как эффективности системы, так и удобства ее использования

(рисунок 3). Пользовательский интерфейс спроектирован с учетом минимизации когнитивной нагрузки на пользователя. Центральную область занимает видеопоток с веб-камеры, где вспомогательный овальный контур помогает пользователю правильно позиционировать лицо. В правой части экрана расположен пошаговый индикатор этапов проверки, который в реальном времени отображает текущий прогресс. Под видеопотоком выводится текстовая обратная связь, содержащая как инструкции для следующего действия (например, «Поверните голову ВЛЕВО»), так и служебные сообщения (например, «Лицо не найдено»). Такая компоновка предоставляет возможность взаимодействия и позволяет пользователю получать обратную связь об эффективности своих действий в рамках процесса верификации.

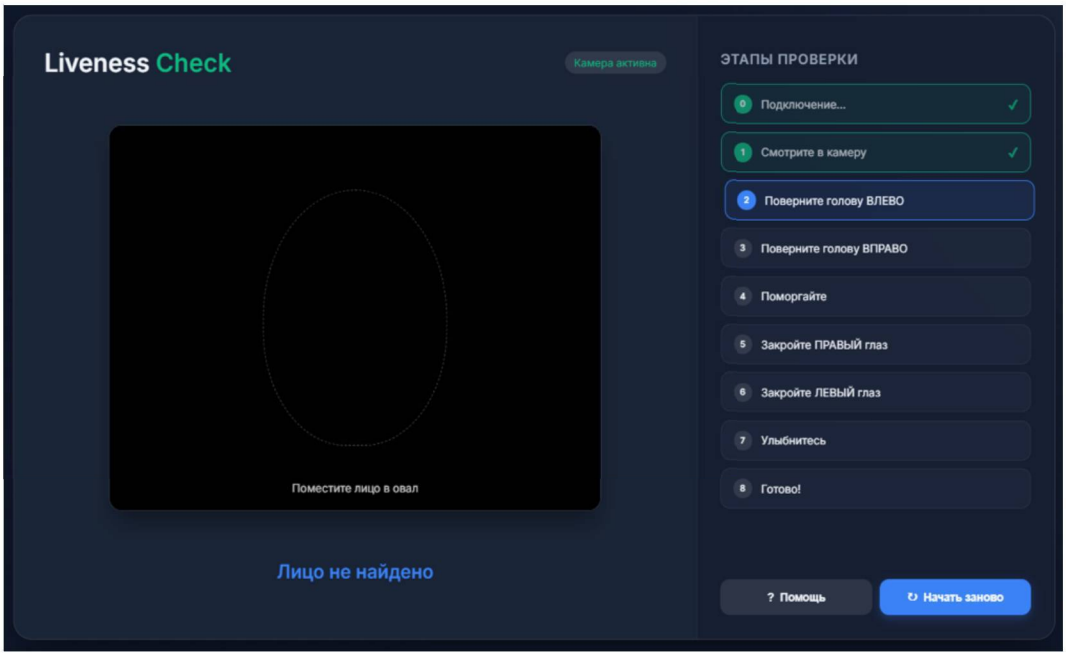

Рисунок 3. Пользовательский интерфейс системы верификации

В ходе апробации подобраны пороговые значения для каждого из контролируемых биометрических параметров. Задачей на данном этапе являлся поиск баланса между устойчивостью системы к атакам на предъявление и минимизацией ложных отказов в обслуживании (*False Rejection Rate, FRR*).

Оптимальные значения, используемые в финальной версии системы, приведены в таблице 1.

Таблица 1. Пороговые значения параметров для машины состояний

Этап проверки	Контролируемый параметр	Пороговое значение
Фиксация в центре	Угол рыскания (*Yaw*)	±30 градусов
Поворот влево/вправо	Угол рыскания (*Yaw*)	> +25 / < -25 градусов
Моргание	Коэффициент *EAR*	< 0.24
Закрытие одного глаза	Коэффициент *EAR* (закрытый)	< 0.24
Улыбка	Коэффициент *MAR*	> 0.40

Тестирование подтвердило эффективность разработанного подхода по двум ключевым направлениям: безопасность и производительность. В ходе тестирования проверена устойчивость системы к основным типам 2D-атак на предъявление: алгоритм успешно идентифицировал и блокировал попытки прохождения верификации с использованием статичных артефактов (распечатанные фотографии) и динамических артефактов (воспроизведение видеозаписей на экранах мобильных устройств). Одновременно с этим, оценка производительности показала, что средняя латентность обработки одного кадра на стандартном серверном *CPU* (*Intel Core i5*) находится в диапазоне 30–40 мс. Такой низкий показатель позволяет поддерживать до 25 одновременных сессий верификации в реальном времени на одном процессорном ядре, что подтверждает высокую архитектурную эффективность для высоконагруженных веб-сервисов.

Заключение. В ходе исследования разработан и программно реализован легковесный алгоритм активной проверки «живости» (*Active Liveness Detection*), основанный на комбинации методов компьютерного зрения. Предложенный метод, использующий машину состояний для анализа динамики антропометрических точек лица (*EAR, MAR, Head Pose*), продемонстрировал свою эффективность в противодействии атакам с использованием фото и видео.

Проведенные эксперименты подтвердили, что система обладает достаточно высокой производительностью на стандартном серверном оборудовании, что делает ее экономически выгодным и легко масштабируемым решением. Работа доказывает, что классические алгоритмы компьютерного зрения остаются актуальным и конкурентоспособным инструментом для решения задач биометрической безопасности, предлагая практическую альтернативу глубокому обучению.

В качестве направлений для дальнейшего развития можно выделить интеграцию в систему дополнительных пассивных проверок (например, анализ текстуры кожи) для противодействия более сложным 3D-атакам, а также адаптивную настройку пороговых значений в зависимости от условий освещения.

Список литературы

[1] ISO/IEC 30107-1:2023. Information technology – Biometric presentation attack detection – Part 1: Framework. – Geneva: International Organization for Standardization, 2023. – 23 p.

[2] Ren Y. Performance Analysis of Deep Learning Workloads on Leading-edge Systems. – Upton: Brookhaven National Laboratory, 2020. – 15 p.

[3] Amos B. The 68 landmarks detected by dlib library. – Режим доступа: https://www.researchgate.net/figure/The-68-landmarks-detected-by-dlib-library-This-image-was-created-by-Brandon-Amos-of-CMU_fig2_329392737 – Дата доступа: 07.03.2026.

[4] Dlib C++ Library. – Режим доступа: http://dlib.net/ – Дата доступа: 07.03.2026.

[5] Liveness Detection in Face Recognition: A Review. – Режим доступа: https://pmc.ncbi.nlm.nih.gov/articles/PMC9044337/ – Дата доступа: 07.03.2026.

[6] OpenCV Documentation: Camera Calibration and 3D Reconstruction (solvePnP). – Режим доступа: https://docs.opencv.org/4.x/d5/d1f/calib3d_solvePnP.html – Дата доступа: 07.03.2026.

Авторский вклад

Андриалович Инна Владимировна – руководство и постановка задачи исследования, формирование структуры статьи.

Галяк Иван Павлович – разработка алгоритма детекции «живости» лица, проектирование математической модели анализа антропометрических дескрипторов (EAR, MAR, Head Pose Estimation), программная реализация серверной логики системы на базе Flask и OpenCV, интеграция алгоритмов машинного зрения в решение.

Касперец Евгений Александрович – проектирование пользовательского интерфейса и архитектуры взаимодействия клиент-серверной системы, разработка клиентской части приложения, проведение экспериментального тестирования, анализ корректности работы системы при различных сценариях использования.

EVALUATION OF THE EFFECTIVENESS OF GENERATIVE POLICY IN OPTIMIZING DESIGN DECISIONS

I.V. Andryalovich
Deputy Dean of the Faculty of Computer Design of BSUIR, postgraduate student of the Department of IP&E
andryinna@bsuir.by

I.P. Haliak
BSUIR student, Department of Information Computer Systems
haliak.ivanba@gmail.com

Y.A. Kaspiarets
BSUIR student, Department of Engineering Psychology and Ergonomics
kasperetsyevgeny@gmail.com

Abstract. The article explores the development of a lightweight real-time face liveness detection algorithm designed to counter biometric data spoofing in web-based authentication systems. The proposed method is based on analyzing facial anthropometric landmark dynamics using classical computer vision algorithms. This approach significantly reduces hardware resource requirements, offering an efficient alternative to computationally expensive deep learning-based solutions.

Keywords: liveness detection, biometric authentication, computer vision, biometric spoofing, web-based authentication, facial landmarks.