РАЗРАБОТКА ИНТЕЛЛЕКТУАЛЬНОЙ СИСТЕМЫ АВТОМАТИЗИРОВАННОГО КОНТРОЛЯ ДОСТУПА НА ОСНОВЕ ВИДЕОКАМЕР И ТЕХНОЛОГИЙ РАСПОЗНАВАНИЯ ЛИЦА

Анарбаев Жавлон Даврон угли
магистрант кафедры «Искусственный интеллект и анализ данных»

Аннотация. *В статье представлены результаты разработки и экспериментальной проверки интеллектуальной системы автоматизированного контроля доступа, основанной на биометрическом распознавании лица в режиме реального времени. Система реализует четыре модели идентификации: DLIB, FaceNet, ArcFace и авторскую гибридную модель Hybrid AI. Разработан оригинальный шестиэтапный конвейер обработки биометрических данных, включающий геометрическое выравнивание лица, накопление скользящего буфера из пяти кадров, комплексную подсистему защиты от атак подделкой (anti-spoofing) на основе LBP-текстурного анализа, оценки резкости изображения и анализа цвета кожи в пространстве YCrCb, а также двухуровневый механизм принятия решений. Экспериментальное тестирование проводилось на выборке из 15 участников (300 испытаний, 5 условий). Средняя точность гибридной модели составила 88.0% при FRR = 5.0% и FAR = 1.7%. Подсистема anti-spoofing обеспечила блокировку 78.9% атак подделкой без применения специализированного оборудования.*

Ключевые слова: *распознавание лица, биометрия, контроль доступа, глубокое обучение, ArcFace, FaceNet, anti-spoofing, LBP, гибридная модель, Flask, SQLite.*

Abstract. *This paper presents the development and experimental verification of an intelligent automated access control system based on real-time face recognition. The system integrates four identification models: DLIB, FaceNet, ArcFace, and an original Hybrid AI model. A novel six-stage biometric data processing pipeline is proposed, incorporating geometric face alignment, temporal averaging over a five-frame sliding buffer, a composite anti-spoofing subsystem combining LBP texture analysis, Laplacian sharpness estimation, and YCrCb skin colour verification, as well as a two-level decision mechanism. Experimental evaluation was conducted on 15 participants (300 trials, 5 conditions). The hybrid model achieved an average accuracy of 88.0% with FRR = 5.0% and FAR = 1.7%. The anti-spoofing subsystem blocked 78.9% of presentation attacks without specialised hardware.*

Keywords: *face recognition, biometrics, access control, deep learning, ArcFace, FaceNet, anti-spoofing, LBP, hybrid model, Flask, SQLite.*

1. ВВЕДЕНИЕ

Задача автоматизированного управления физическим доступом к охраняемым объектам приобретает возрастающую практическую значимость в условиях цифровизации организационных процессов. Традиционные идентификаторы — RFID-карты, PIN-коды, механические ключи — не обеспечивают достаточного уровня защиты: они могут быть скопированы, переданы третьим лицам или утрачены. Биометрические методы идентификации, основанные на неотчуждаемых физиологических признаках личности, лишены указанных недостатков. По данным MarketsandMarkets, объём мирового рынка систем распознавания лиц достиг 5.01 млрд долларов США в 2022 году и прогнозируется на уровне 12.67 млрд к 2028 году при среднегодовом темпе роста 16.3% [1].

Среди биометрических модальностей распознавание лица занимает особое место благодаря сочетанию бесконтактности, высокой практичности и приемлемой точности. Внедрение методов глубокого обучения обеспечило качественный скачок: современные модели FaceNet [2] и ArcFace [3] достигают точности 99.63% и 99.83% соответственно на эталонном датасете LFW. Тем не менее практическое применение данных методов в реальных системах контроля доступа сопряжено с рядом нерешённых проблем: деградацией точности в условиях недостаточного освещения и частичного закрытия лица, а также уязвимостью к атакам подделкой посредством фотографий и видеозаписей.

Настоящая работа посвящена разработке интеллектуальной системы контроля доступа, интегрирующей четыре модели биометрической идентификации, оригинальный алгоритм обработки на основе гибридной модели и подсистему защиты от атак подделкой, функционирующую на стандартной RGB-камере без специализированного оборудования.

2. ОБЗОР ЛИТЕРАТУРЫ

Задача автоматического распознавания лиц исследуется с начала 1990-х годов. Turk и Pentland [4] предложили метод Eigenfaces на основе анализа главных компонент (PCA), достигавший точности 60–70% на ограниченных выборках. Belhumeur et al. [5] расширили подход, применив линейный дискриминантный анализ (LDA — метод Fisherfaces) для максимизации межклассовой вариативности. Ojala et al. [6] ввели дескриптор локальных бинарных шаблонов (LBP), обеспечивший устойчивость к вариациям освещения; комбинация LBP с методом опорных векторов (SVM) обеспечивала точность до 87%.

Переход к нейросетевым методам ознаменовался работой Taigman et al. (DeepFace, 2014) [7], достигших 97.35% на LFW. Schroff et al. (FaceNet, 2015) [2] предложили функцию потерь Triplet Loss, обучающую сеть в метрическом пространстве, и достигли 99.63%. Принципиально новый подход предложен Deng et

al. (ArcFace, 2019) [3]: аддитивный угловой зазор в функции потерь (формула 1) создаёт геодезические границы между классами, что обеспечивает точность 99.83%.

$$L = -(1/N)\ \Sigma\ log\ [\ e^{(s\cdot cos(\theta\_yi + m))} / (e^{(s\cdot cos(\theta\_yi+m))} + \Sigma\_\{j\neq yi\}\ e^{(s\cdot cos\ \theta\_j))}\ ] \quad (1)$$

где s — масштабный коэффициент (s = 64), m — аддитивный угловой зазор (m = 0.5 рад), θ_yi — угол между вектором признаков и весовым вектором целевого класса.

Проблема защиты от атак подделкой рассматривалась в работах Boulkenafet et al. [8], применивших LBP-текстурный анализ, и Liu et al. [9], предложивших подход на основе глубокого обучения. Детектирование и выравнивание лиц посредством каскадных свёрточных сетей (MTCNN) описано в работе Zhang et al. [10].

Вместе с тем анализ литературы свидетельствует об отсутствии комплексных решений, объединяющих сравнительный анализ нескольких нейросетевых моделей, многоэтапный конвейер гибридной обработки и подсистему anti-spoofing в едином функционирующем программном комплексе. Данный пробел определяет научную нишу настоящего исследования.

3. АРХИТЕКТУРА РАЗРАБОТАННОЙ СИСТЕМЫ

Разработанная система реализована в виде трёхуровневого клиент-серверного приложения. Серверная часть построена на веб-фреймворке Flask (Python) и предоставляет REST API для взаимодействия с клиентским одностраничным приложением (SPA). Хранение данных осуществляется в реляционной СУБД SQLite, включающей четыре таблицы: users (пользователи), embeddings (биометрические шаблоны), access_log (журнал событий) и test_results (результаты тестирования).

В систему интегрированы четыре модели биометрической идентификации, характеристики которых приведены в таблице 1. Для каждой модели реализованы независимые функции извлечения биометрического дескриптора и вычисления метрики сходства. Это обеспечивает возможность параллельного использования моделей и их сравнительного анализа в рамках единого интерфейса.

Таблица 1 — Характеристики реализованных моделей распознавания лиц

Модель	Библиотека	Вектор	Метрика	Порог θ
DLIB	face_recognition (ResNet-34)	128D	$1 - \|\|a - b\|\|_2$	0.55
FaceNet	facenet-pytorch + MTCNN	512D	(cos(a,b) + 1) / 2	0.65
ArcFace	InsightFace (ONNX RT)	512D	(cos(a,b) + 1) / 2	0.60

Hybrid AI	Собственная (ArcFace / FaceNet)	512D	Cosine + двухуровневое решение	0.55 (MED) / 0.80 (HIGH)

4. ГИБРИДНАЯ МОДЕЛЬ HYBRID AI

Основным научным результатом настоящей работы является оригинальная гибридная модель Hybrid AI, реализующая шестиэтапный конвейер обработки биометрических данных.

Этап 1. Детектирование лица. Применяется каскадный классификатор Хаара (OpenCV), настроенный с параметрами scaleFactor = 1.1, minNeighbors = 5, minSize = (60, 60) пикселей.

Этап 2. Геометрическое выравнивание. По координатам центров глаз (c_1, c_2) вычисляется угол наклона головы и применяется аффинное преобразование поворота:

$$\alpha = \arctan(\ (c_2.y - c_1.y) / (c_2.x - c_1.x)\ ),\quad |\alpha| > 2^\circ \ \rightarrow \text{вращение} \quad (2)$$

Этап 3. Извлечение биометрического вектора. Используется ArcFace (при наличии) или FaceNet в качестве резервного. Вектор нормализуется до единичной длины.

Этап 4. Накопление и усреднение кадров. Скользящий буфер размером N = 5 накапливает последовательные векторы. Усреднённый дескриптор вычисляется как нормализованное среднее:

$$\hat{e} = \text{normalize}(\ \Sigma_{k\in B}\ e_k / |B|\ ),\quad 1 \le |B| \le 5 \quad (3)$$

Применение формулы (3) снижает влияние случайных шумов и мимических вариаций, повышая стабильность идентификации.

Этап 5. Anti-spoofing. Для обнаружения атак подделкой разработана комплексная метрика живости лица S_anti, объединяющая три независимых признака:

$$S\_anti = 0.4 \cdot S\_lbp + 0.3 \cdot S\_blur + 0.3 \cdot S\_skin \quad (4)$$

где S_lbp — нормализованная энтропия Шеннона гистограммы LBP-кодов (формула 5); S_blur — нормализованная дисперсия оператора Лапласа (формула 6); S_skin — доля пикселей с компонентами YCrCb в диапазоне живой кожи: Cr ∈ [133, 173], Cb ∈ [77, 127] (формула 7).

$$S\_lbp = \min(1, H(LBP)/7),\quad H = -\Sigma\ p_k \log_2 p_k \quad (5)$$

$$S\_blur = \min(1, \text{Var}(\nabla^2 I) / 500) \quad (6)$$

$$S\_skin = 0.5 \cdot [Cr \in [133,173]] + 0.5 \cdot [Cb \in [77,127]] \quad (7)$$

По итогам вычисления S_anti формируется вердикт: LIVE ($S \ge 0.65$), UNCERTAIN ($0.40 \le S < 0.65$) или SPOOF ($S < 0.40$).

Этап 6. Двухуровневое принятие решения. Доступ предоставляется при выполнении одного из двух условий:

$$\text{access} = 1:\ \text{score} \ge 0.80\ \ И\ \ \text{verdict} \ne \text{SPOOF}\quad (\text{HIGH confidence}) \quad (8)$$

access = 1: $0.55 \leq score < 0.80$ И verdict = LIVE (MEDIUM) (9)

access = 0: verdict = SPOOF (блокировка независимо от score) (10)

5. МЕТОДОЛОГИЯ ЭКСПЕРИМЕНТАЛЬНОГО ТЕСТИРОВАНИЯ

Тестирование системы проводилось в соответствии с требованиями стандарта ISO/IEC 19795-1:2006 на выборке из 15 участников. Каждый участник прошёл регистрацию с захватом 7–10 фотографий при нормальном освещении (≥ 200 лк), после чего выполнялась серия из 20 попыток идентификации — по 4 попытки на каждое из пяти условий тестирования. Итоговая выборка составила 300 испытаний.

Определены пять условий тестирования: (1) нормальное освещение — базовое условие; (2) слабое освещение (30–50 лк); (3) маска / частичное закрытие лица; (4) очки / аксессуары; (5) поворот головы на 20–35°. Вычислительная платформа: Intel Core i5, 8 ГБ ОЗУ, без GPU-ускорения.

Для оценки качества системы использовались следующие метрики: точность (Accuracy), коэффициент ложного пропуска (FRR), коэффициент ложного принятия (FAR) и F1-мера. Равновесная точка ошибок (EER) определялась как значение порога θ^*, при котором $FAR(\theta^*) = FRR(\theta^*)$.

6. РЕЗУЛЬТАТЫ И ИХ ОБСУЖДЕНИЕ

Результаты тестирования точности распознавания при каждом условии приведены в таблице 2. Во всех пяти условиях гибридная модель Hybrid AI демонстрирует наивысшую точность, превосходя ближайшего конкурента (ArcFace) в среднем на 2.3 процентных пункта.

Таблица 2 — Точность распознавания (Accuracy, %) по условиям тестирования

Условие тестирования	DLIB	FaceNet	ArcFace	Hybrid AI
1. Нормальное освещение	88.3	91.7	93.3	**95.0**
2. Слабое освещение	71.7	80.0	83.3	**86.7**
3. Маска	55.0	73.3	81.7	**83.3**
4. Очки / аксессуары	75.0	83.3	86.7	**88.3**
5. Поворот головы	68.3	78.3	83.3	**86.7**
Среднее значение	**71.7**	**81.3**	**85.7**	**88.0**

Наиболее сложным условием для всех моделей оказалось наличие маски. Точность DLIB при данном условии снизилась до 55.0%, что исключает применение данной модели в сценариях с обязательным ношением средств защиты лица. Устойчивость гибридной модели при маске (83.3%) обусловлена геометрическим

выравниванием, сохраняющим информацию об области глаз, и механизмом усреднения кадров.

Сводные показатели качества всех моделей приведены в таблице 3.

Таблица 3 — Сводные показатели качества моделей (нормальное освещение)

Модель	Accuracy ср.	FRR (%)	FAR (%)	t_avg (мс)	F1-мера
DLIB	71.7	11.7	6.7	**87**	0.738
FaceNet	81.3	8.3	3.3	213	0.831
ArcFace	85.7	6.7	1.7	167	0.876
Hybrid AI	**88.0**	**5.0**	**1.7**	318	**0.901**

Результаты тестирования подсистемы anti-spoofing (90 испытаний по трём типам атак) представлены в таблице 4.

Таблица 4 — Результаты тестирования подсистемы anti-spoofing

Тип атаки	Тестов	SPOOF (корр.)	Точность блок. (%)
Распечатанная фотография	30	26	**86.7**
Видео на экране смартфона	30	24	**80.0**
Фото высокого разрешения (планшет)	30	21	70.0
Итого / среднее	**90**	**71**	**78.9**

Наибольшую сложность для подсистемы anti-spoofing представляет атака посредством фотографии высокого разрешения на планшете (70.0% корректных блокировок). Это объясняется высоким качеством дисплея, имитирующего текстуру кожи: средний показатель S_lbp для данного сценария составил 0.55, что приближается к пороговому значению живой кожи. Перспективным направлением преодоления указанного ограничения является интеграция анализа оптического потока (детекция моргания).

Для модели ArcFace было проведено дополнительное исследование зависимости FRR и FAR от порогового значения θ. Установлено, что равновесная точка ошибок (EER) достигается при $\theta^* \approx 0.55$, что соответствует $FRR \approx FAR \approx 5.0\%$. Рабочее значение $\theta = 0.60$, применяемое по умолчанию, смещает рабочую точку в сторону снижения FAR (до 1.7%) за счёт умеренного роста FRR (до 6.7%), что соответствует требованиям безопасности систем контроля доступа.

7. ЗАКЛЮЧЕНИЕ

В настоящей работе разработана и экспериментально верифицирована интеллектуальная система автоматизированного контроля доступа, реализующая четыре модели биометрической идентификации по лицу. Основным научным результатом является оригинальная гибридная модель Hybrid AI, интегрирующая шестиэтапный конвейер обработки с механизмами геометрического выравнивания, многокадрового усреднения и комплексной защиты от атак подделкой.

Предложенная метрика живости S_anti (формула 4), объединяющая LBP-текстурный анализ, оценку резкости по Лапласиану и анализ цвета кожи в пространстве YCrCb, обеспечивает блокировку 78.9% атак подделкой без применения специализированного оборудования (3D-сенсоров, ИК-камер). Экспериментальное тестирование (300 испытаний, 5 условий, 15 участников) подтвердило превосходство гибридной модели: средняя точность 88.0%, F1 = 0.901, FAR = 1.7%.

Перспективы дальнейших исследований включают: (1) интеграцию детектора моргания на основе анализа оптического потока для повышения точности anti-spoofing; (2) реализацию GPU-ускорения с целью снижения времени отклика до 30–50 мс; (3) применение концепции отзываемых биометрических шаблонов (cancelable biometrics) для защиты персональных данных при производственном развёртывании.

СПИСОК ЛИТЕРАТУРЫ

1. MarketsandMarkets. Face Recognition Market — Global Forecast to 2028. — Northbrook: MarketsandMarkets Research, 2023. — 350 p.

2. Schroff F., Kalenichenko D., Philbin J. FaceNet: A unified embedding for face recognition and clustering // Proceedings of CVPR 2015. — P. 815–823.

3. Deng J., Guo J., Xue N., Zafeiriou S. ArcFace: Additive angular margin loss for deep face recognition // Proceedings of CVPR 2019. — P. 4690–4699.

4. Turk M., Pentland A. Eigenfaces for recognition // Journal of Cognitive Neuroscience. — 1991. — Vol. 3, No. 1. — P. 71–86.

5. Belhumeur P. N., Hespanha J. P., Kriegman D. J. Eigenfaces vs. Fisherfaces: Recognition using class-specific linear projection // IEEE Trans. PAMI. — 1997. — Vol. 19, No. 7. — P. 711–720.

6. Ojala T., Pietikäinen M., Harwood D. A comparative study of texture measures with classification based on feature distributions // Pattern Recognition. — 1996. — Vol. 29, No. 1. — P. 51–59.

7. Taigman Y., Yang M., Ranzato M., Wolf L. DeepFace: Closing the gap to human-level performance in face verification // Proceedings of CVPR 2014. — P. 1701–1708.

8. Boulkenafet Z., Komulainen J., Hadid A. Face anti-spoofing using speeded-up robust features and Fisher vector encoding // IEEE Signal Processing Letters. — 2017. — Vol. 24, No. 2. — P. 141–145.

9. Liu Y., Jourabloo A., Liu X. Learning deep models for face anti-spoofing // Proceedings of CVPR 2018. — P. 389–398.

10. Zhang K., Zhang Z., Li Z., Qiao Y. Joint face detection and alignment using multitask cascaded convolutional networks // IEEE Signal Processing Letters. — 2016. — Vol. 23, No. 10. — P. 1499–1503.

11. He K., Zhang X., Ren S., Sun J. Deep residual learning for image recognition // Proceedings of CVPR 2016. — P. 770–778.

12. King D. E. Dlib-ml: A machine learning toolkit // Journal of Machine Learning Research. — 2009. — Vol. 10. — P. 1755–1758.

13. Wang H., Wang Y., Zhou Z. et al. CosFace: Large margin cosine loss for deep face recognition // Proceedings of CVPR 2018. — P. 5265–5274.

14. ISO/IEC 19795-1:2006. Information technology — Biometric performance testing and reporting — Part 1: Principles and framework. — Geneva: ISO, 2006. — 56 p.

15. Goodfellow I., Bengio Y., Courville A. Deep Learning. — Cambridge: MIT Press, 2016. — 800 p.