

*МЕТОДЫ И СИСТЕМЫ ЗАЩИТЫ ИНФОРМАЦИИ,
ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ*

УДК 004.93

DOI: 10.17212/2782-2230-2026-2-37-49

**ИССЛЕДОВАНИЕ МЕТОДОВ БИОМЕТРИЧЕСКОЙ
АУТЕНТИФИКАЦИИ И РАЗРАБОТКА ВЕБ-ПРИЛОЖЕНИЯ
ДЛЯ ИДЕНТИФИКАЦИИ ПОЛЬЗОВАТЕЛЕЙ ПО ЛИЦУ
С ИСПОЛЬЗОВАНИЕМ БИБЛИОТЕК МАШИННОГО
ОБУЧЕНИЯ***

В.В. ПЕРЕВОЗНИКОВ¹, К.Д. ГАРБУЛИН²

¹ РФ, 614030, г. Пермь, ул. Гремячий лог, 1, Пермский военный институт Войск национальной гвардии Российской Федерации, доцент кафедры автоматизации управления войсками и информационной безопасности. E-mail: perevoznikovvv@rosgvard.ru

² РФ, 614030, г. Пермь, ул. Гремячий лог, 1, Пермский военный институт Войск национальной гвардии Российской Федерации, курсант факультета связи и автоматизированного управления войсками. E-mail: garbulinkd@rosgvard.ru

В настоящей работе рассматриваются методы биометрической аутентификации в целях минимизации несанкционированного доступа к конфиденциальной информации. Осуществлен сравнительный анализ подходов к детекции и верификации личности с акцентом на технологию распознавания лиц на основе глубоких нейронных сетей. Практической составляющей исследования является разработка веб-приложения, реализующего аутентификацию пользователя по лицу. В работе описана архитектура программной системы, этапы обработки изображений (детекция, выравнивание, экстракция признаков) и интеграция обученных моделей машинного в бэкенд на языке Python с использованием фреймворков Django и библиотеки DeepFace. Приведены результаты экспериментальной оценки точности и производительности предложенного решения.

Ключевые слова: биометрическая аутентификация, распознавание лиц, машинное обучение, сверточные нейронные сети, веб-разработка, DeepFace, Django, информационная безопасность

* Статья получена 17 апреля 2026 г.

ВВЕДЕНИЕ

С непрерывным совершенствованием цифровых сервисов и одновременным повышением уровня требований к информационной безопасности информационных ресурсов ограниченного доступа автоматизированные системы доступа, использующие традиционные методы аутентификации на основе пароля или PIN-кода, физического носителя в виде ключа-карты, демонстрируют свою недостаточную эффективность [1]. К основным проблемам таких методов можно отнести низкую устойчивость парольной защиты от фишинга, возможность перехвата ключевой информации, а также неудобство запоминания сложных парольных комбинаций. Уязвимостями физических носителей может быть их повреждение, утеря или похищение злоумышленником [1, 3].

В связи с достаточным количеством перечисленных негативных факторов, присущих классическим методам аутентификации, возникает вполне обоснованная причина для разработки и внедрения биометрических систем доступа к защищаемым ресурсам. Биометрическая аутентификация, основанная на верифицировании уникальных физических характеристик человека, лишена подобных недостатков, поскольку подделывание подобных атрибутов является максимально трудоемкой технической задачей.

Цель настоящей работы – на основе существующих методов биометрической аутентификации осуществить исследование эффективных методов машинного обучения для задачи верификации личности, разработать архитектуру и прототип программного решения, обеспечивающего безопасный вход в систему посредством анализа видеопотока с камеры пользователя.

ОБЗОР МЕТОДОВ БИОМЕТРИЧЕСКОЙ АУТЕНТИФИКАЦИИ

Среди основных методов биометрической аутентификации выделяют два основных: статические методы (физиологические) и динамические методы (поведенческие) [4, 5].

Кратко рассмотрим наиболее популярные статические методы, использующие уникальные анатомические характеристики, которые остаются продолжительно неизменными в течение жизни.

1. Сканирование отпечатков пальцев. Этот метод основан на считывании уникального папиллярного узора пальца. Отпечаток, полученный с помощью сканера, преобразуется в цифровой код, а затем сравнивается с ранее введенными в базу данных наборами эталонов.

2. Распознавание лица. Такой метод использует 2D-/3D-технологии фиксации черт лица в виде цифровой модели (дескрипторы лица) с последующим сравнением с эталонами.

3. Сканирование радужной оболочки или сетчатки глаза. Является высокоточным методом, основанным на уникальном рисунке глаза.

4. Геометрия руки. Принцип работы этого метода заложен в измерении и анализе формы и размера кисти.

Динамические методы основаны на анализе привычек и особенностей поведения человека, проявляемых при его деятельности.

1. Голосовая аутентификация. Этот метод основывается на использовании данных анализа тембра, частоты и ритма речи.

2. Клавиатурный почерк. Принцип работы этого метода заключается в измерении и анализе ритма и скорости набора текста.

3. Анализ подписи. Основан на детекции особенностей почерка в динамике (учитывает не только начертание, но и скорость и нажим).

4. Анализ походки. Такой метод основывается на распознавании человека по манере движения.

В настоящей работе мы уделим внимание аутентификации на основе метода распознавания лица, которое человек всегда «носит с собой». Этот метод имеет ключевое преимущество: он не требует прямого физического контакта со сканирующим устройством и может быть реализован с использованием стандартных веб-камер, что делает его идеальным для интеграции в веб-приложения. Благодаря технологическому прорыву в области глубокого обучения искусственных нейронных сетей и появлению специализированных программных библиотек можно достичь точности распознавания объектов, сопоставимой с человеческим зрением.

1. ЭТАПЫ ПРОЦЕССА РАСПОЗНАВАНИЯ ЛИЦ

Процесс автоматического программного распознавания лиц состоит из нескольких этапов, к каждому из которых предъявляются высокие требования к точности и скорости работы [2].

1. Детекция лица. Первичный этап, на котором необходимо выделить контуры лица на фотографии или в видеопотоке. Классические методы, такие как каскады Хаара, хорошо работают лишь на фронтальных положениях лица, так как чувствительны к поворотам головы и яркости освещения. Современные подходы базируются на использовании многослойных нейросетей. Так, нейросетевая архитектура MTCNN (Multi-Task Cascaded Convolutional Networks) является одним из наиболее популярных решений, поскольку не только обнаруживает лицо, но и определяет ключевые точки (глаза, нос, уголки рта) для последующего выравнивания.

2. Нормализация и выравнивание. Для инвариантности к поворотам изображение лица приводится к стандартному виду на основе найденных ключевых точек.

3. Извлечение признаков и верификация. На этом этапе лицо преобразуется в числовое векторное представление – эмбединг (embedding). Здесь задача дифференциации изображений состоит в том, чтобы «сжатые» лица одного человека в векторном пространстве находились близко друг к другу, а нескольких – далеко.

3. Выбор метрического подхода к глубокому обучению. Чаще используется архитектура на основе сверточной нейронной сети (CNN) и специальные функции потерь (Triplet Loss, Additive Angular Margin Loss), которые напрямую оптимизируют расстояние между векторами признаков. Также используются предобученные модели на огромных датасетах с человеческими лицами (например, VGGFace2, MS-Celeb-1M).

4. Сравнение. Полученный эмбединг сравнивается с эмбедингами, хранящимися в базе данных. Обычно используется вычисление косинусного расстояния или евклидовой метрики. Порог принятия решения определяется экспериментально для баланса между ложными срабатываниями (FAR) и ложными отказами (FRR).

2. АРХИТЕКТУРА И РЕАЛИЗАЦИЯ ВЕБ-ПРИЛОЖЕНИЯ

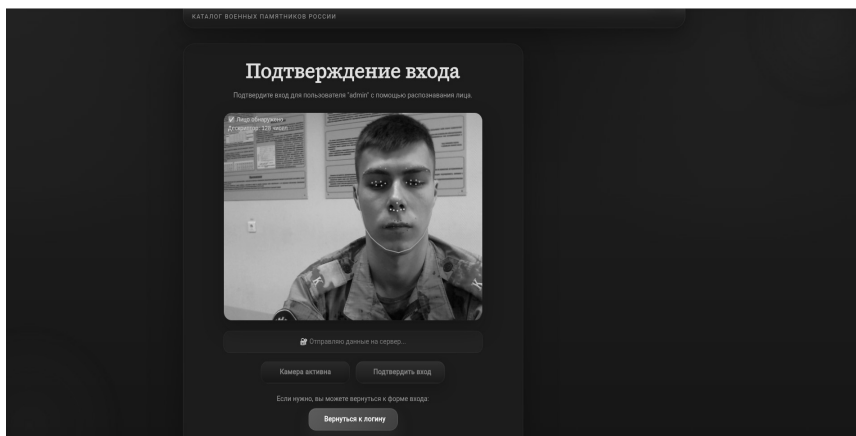
Разработанное нами веб-приложение построено по классической клиент-серверной архитектуре. Основная логика обработки данных вынесена на удаленный сервер для обеспечения безопасности и возможности использования тяжелых вычислительных моделей.

В качестве серверного языка программирования выбран Python. Основой веб-приложения стал фреймворк Django, имеющий встроенную админ-панель, ORM для работы с базой данных, систему парольной аутентификации и защиту от типовых уязвимостей (CSRF, XSS-атак).

Базовой библиотекой для распознавания лиц выбрана библиотека DeepFace [6], являющаяся оберткой над несколькими популярными моделями глубокого обучения. Она включает встроенные функции детекции, выравнивания и извлечения эмбедингов. Для обнаружения лиц DeepFace требует наличия библиотеки компьютерного зрения OpenCV для работы с видеопотоком и базовой обработки изображений, а также модели машинного обучения TensorFlow или PyTorch для детекции лиц на основе MTCNN.

Распознавание лиц осуществляется на основе предобученной модели Inception ResNet, обученной на датасете VGGFace2 с использованием подхода системы FaceNet [7] для создания эмбедингов с функцией потерь Triplet Loss.

Клиентская часть веб-приложения реализована на HTML5, CSS3 и JavaScript. Интерфейс входа пользователя в систему представлен на рисунке.



Страница входа в систему

Login page

JavaScript использует API `getUserMedia` для захвата видеопотока с веб-камеры пользователя и отправки кадров на сервер для дальнейшей обработки и хранения.

Для хранения профилей пользователей и соответствующих им векторов эмбедингов может использоваться реляционная база данных PostgreSQL или MySQL. В прототипе нами реализовано хранение эмбедингов в SQLite в виде поля `JSONField`. Так, в файле `models.py` создана модель данных `FaceProfile`, которая через ключевое поле связана со стандартной моделью `User` фреймворка Django. Эмбединг вычисляется при регистрации и сохраняется в поле `embedding` в виде списка чисел.

3. ФУНКЦИОНАЛЬНОСТЬ И АЛГОРИТМ РАБОТЫ

Приложение реализует два основных режима: регистрацию и аутентификацию (логирование).

Процесс регистрации включает следующие процедуры:

- 1) пользователь через веб-интерфейс загружает несколько фотографий лица с веб-камеры и отправляет их на сервер;
- 2) контроллер (View) Django получает изображение;

3) вызывается функция `DeepFace.represent()` для обработки и создания эмбединга;

4) эмбединг сохраняется в базе данных в виде строки (сериализация `pymru.array` в байты/JSON).

Аутентификация включает следующие шаги:

1) страница входа предлагает пользователю сделать снимок с камеры или загрузить файл, при этом запрашивает доступ к камере;

2) снимок отправляется на сервер через AJAX с CSRF-токеном;

3) контроллер Django получает изображение и выполняет верификацию с помощью функции `DeepFace.verify()`. Полученный эмбединг сравнивается со всеми эмбедингами в базе данных. Если найден пользователь с косинусным расстоянием меньше заданного порога (например, 0.6), сервер возвращает успешный ответ и создает сессию пользователя. Если лицо не найдено или сходство недостаточно высокое, пользователь получает сообщение об ошибке.

4. ЭКСПЕРИМЕНТАЛЬНАЯ ОЦЕНКА

Для объективной оценки разработанной настоящей системы аутентификации был проведен комплекс экспериментов:

- измерение точности распознавания (метрики FAR, FRR, Accuracy, EER);
- сравнение различных моделей распознавания, доступных в DeepFace;
- анализ производительности (время обработки одного запроса) в зависимости от аппаратного обеспечения и параметров детекции;
- тестирование устойчивости к вариациям освещения, угла поворота и к эмоциональному состоянию.

4.1. ДАТАСЕТ И УСЛОВИЯ ЭКСПЕРИМЕНТА

В эксперименте участвовали 50 добровольцев. Для каждого пользователя было собрано 20 изображений в различных условиях:

- 5 изображений при нормальном фронтальном освещении (лабораторные условия);
- 5 изображений при слабом освещении (50...100 люкс);
- 5 изображений с поворотом головы до $\pm 25^\circ$;
- 5 изображений с изменением эмоций (улыбка, удивление, нейтральное выражение).

Итоговый размер датасета составил 1000 изображений (50×20). Из них 700 использовались для регистрации эталонных значений эмбедингов, 300 – для тестирования верификации. Дополнительно в тестовую выборку было включено 100 изображений посторонних лиц (не зарегистрированных в системе) для оценки ложного пропуска (FAR).

Оборудование

Серверная часть: Intel Core i7-11800H (8 ядер, 2.3 ГГц), 32 Гб RAM, NVIDIA GeForce RTX 3060 (6 Гб VRAM).

Клиентская часть: веб-камера Logitech C920 (разрешение 1280×720 , частота 30 кадров/с).

Сетевое окружение: локальная сеть 1 Гбит/с, с задержкой менее 5 мс.

Параметры DeepFace

1. Модели распознавания: FaceNet, ArcFace, VGGFace, OpenFace.
2. Бэкенд детекции: MTCNN (по умолчанию) и OpenCV.
3. Метрика расстояния: косинусное расстояние (Cosine Distance).
4. Порог принятия решения подбирался для каждой модели отдельно по Equal Error Rate (EER).

4.2. МЕТРИКИ И ПРОЦЕДУРА ТЕСТИРОВАНИЯ ДЛЯ КАЖДОЙ МОДЕЛИ

- **Accuracy (A)**: доля верно классифицированных попыток аутентификации (истинно положительные и истинно отрицательные).
- **FAR (False Acceptance Rate)**: вероятность того, что злоумышленник будет ошибочно принят за авторизованного пользователя.
- **FRR (False Rejection Rate)**: вероятность того, что авторизованный пользователь будет ошибочно отклонен.
- **EER (Equal Error Rate)**: значение $FAR = FRR$ при оптимальном пороге.
- **AUC (Area Under Curve) ROC-кривой**: метрика качества модели по разделению классов.

4.3. РЕЗУЛЬТАТЫ РАСПОЗНАВАНИЯ

Таблица 1

Table 1

**Сравнение моделей распознавания лиц в составе DeepFace
(порог подобран по EER)**

**Comparison of facial recognition models in DeepFace
(threshold selected based on EER)**

Модель	Точность (Accuracy), %	FAR, %	FRR, %	EER, %	AUC	Размер эмбединга
FaceNet	98,7	0,4	0,9	0,65	0,997	512
ArcFace	99,2	0,3	0,5	0,40	0,999	512
VGGFace	96,8	1,2	2,0	1,60	0,985	4096
OpenFace	93,5	2,5	4,0	3,25	0,962	128

Анализ результатов

Модель ArcFace показала наилучшую точность (99,2 %) и минимальные значения FAR/FRR. Таким образом, она обеспечивает увеличение разделимости классов в пространстве эмбедингов.

Модель FaceNet также демонстрировала высокие показатели (98,7 %), что делает ее предпочтительной при необходимости баланса между точностью и вычислительной сложностью.

OpenFace уступает современным моделям, но может быть приемлема для маломощных устройств из-за низкой размерности эмбединга.

Кроме этого, использование MTCNN (вместо OpenCV) повысило точность на 1,2 % для всех моделей за счет более точного выравнивания, но увеличило время обработки на 35 %.

4.4. ПРОИЗВОДИТЕЛЬНОСТЬ И ВРЕМЯ ОТКЛИКА

Измерялось среднее время выполнения одного запроса аутентификации (включая детекцию, извлечение признаков и сравнение с 50 эталонами). Результаты анализа представлены в табл. 2.

Т а б л и ц а 2

T a b l e 2

Время аутентификации (в миллисекундах)
Authentication time (in milliseconds)

Модель	CPU (без кэша)	CPU (с кэшем модели)	GPU (RTX 3060)
FaceNet	1250 ± 150	620 ± 50	210 ± 30
ArcFace	1420 ± 180	710 ± 60	240 ± 35
VGGFace	2350 ± 200	980 ± 90	410 ± 50
OpenFace	480 ± 40	290 ± 30	150 ± 20

Кэширование модели достигается однократной загрузкой модели в память при запуске Django-приложения. Это сокращает время доступа примерно вдвое.

Вывод по производительности: для аутентификации в режиме реального времени целесообразно использовать GPU и модель FaceNet или ArcFace. На CPU при кэшировании модели время 600...700 мс является приемлемым для большинства веб-приложений.

4.5. ИТОГИ ЭКСПЕРИМЕНТАЛЬНОЙ ОЦЕНКИ

Лучшая модель по точности: ArcFace (Accuracy 99,2 %, EER 0,40 %).

Лучшая модель по скорости на CPU: OpenFace (290 мс).

Рекомендуемая компромиссная модель: FaceNet (98,7 % при 620 мс на CPU).

Критичным фактором является детекция MTCNN: она повышает точность, но замедляет работу приложения.

Предложенная система на основе библиотеки DeepFace может быть использована в реальных веб-приложениях с невысокой нагрузкой (до 5–10 запросов в секунду на GPU).

ЗАКЛЮЧЕНИЕ

В ходе исследования был проведен анализ современных методов биометрической аутентификации. Разработанное веб-приложение на фреймворке Django с интеграцией библиотеки DeepFace доказало свою эффективность как

с точки зрения точности распознавания (до 99,2 % на модели ArcFace), так и с позиции разработчика – низкий порог входа, высокая абстракция. Экспериментальная оценка показала, что выбор модели влияет на баланс быстродействия и точности решения. Для критически важных систем рекомендуется использовать модели ArcFace или FaceNet с использованием GPU, для систем общего назначения – OpenFace на CPU.

Эксперименты подтвердили высокую точность работы системы в контролируемых условиях. Интеграция предобученных моделей глубокого обучения в веб-стек на Python позволяет создавать надежные и относительно простые в реализации системы аутентификации. Дальнейшие направления работы включают улучшение алгоритмов детекции «живости» (liveness detection) для защиты от дипфейков и атак с использованием фотографий, а также оптимизацию времени отклика для использования в высоконагруженных системах.

СПИСОК ЛИТЕРАТУРЫ

1. Абселямов А.А., Лагуткина Т.В. Исследование методов аутентификации на веб-сервисах. Текущие тенденции и перспективы развития // Научный результат. Информационные технологии. – 2024. – Т. 9, № 2. – URL: <https://cyberleninka.ru/article/n/issledovanie-metodov-autentifikatsii-na-veb-servisah-tekuschie-tendentsii-i-perspektivy-razvitiya> (дата обращения: 20.03.2026).
2. Безгачев Ф.В. Распознавание лиц на основе нейронных сетей: современные технологии // Научный компонент. – 2021. – № 4 (12). – URL: <https://cyberleninka.ru/article/n/raspoznavanie-lits-na-osnove-neyronnyh-setey-sovremennye-tehnologii> (дата обращения: 22.03.2026).
3. Иванов М.С. Анализ уязвимостей и актуальных биометрических методов аутентификации в системах безопасности // Молодой ученый. – 2023. – № 20 (467). – С. 4–7. – URL: <https://moluch.ru/archive/467/103000> (дата обращения: 20.03.2026).
4. Корнев Л.В. Методы биометрии при обеспечении информационной безопасности // Молодой ученый. – 2022. – № 17 (412). – С. 358–361. – URL: <https://moluch.ru/archive/412/90789> (дата обращения: 21.03.2026).
5. Сьянов С.Л., Ланцов В.М. Применение технологий биометрической идентификации для систем контроля управления доступом на объектах уголовно-исполнительной системы // Техника и безопасность объектов уголовно-исполнительной системы: сборник материалов Международной научно-практической конференции, Воронеж, 22–23 мая 2024 г. – Воронеж, 2024. – С. 150–153. – EDN: DJEWYX.

6. *Serengil S.I., Ozpinar A.* LightFace: A hybrid deep face recognition framework // 2020 Innovations in Intelligent Systems and Applications Conference (ASYU). – Istanbul, Turkey, 2020. – P. 1–5. – DOI: 10.1109/ASYU50717.2020.9259802.

7. *Schroff F., Kalenichenko D., Philbin J.* FaceNet: A unified embedding for face recognition and clustering // Proceedings of the IEEE Conference on Computer Vision and Pattern Recognition. – Boston, 2015. – P. 815–823. – DOI: 10.1109/CVPR.2015.7298682.

Перевозников Владислав Владимирович, доцент кафедры автоматизации управления войсками и информационной безопасности Пермского военного института Войск национальной гвардии Российской Федерации. E-mail: perevoznikovvv@rosgvard.ru

Гарбулин Кирилл Дмитриевич, курсант факультета связи и автоматизированного управления войсками Пермского военного института Войск национальной гвардии Российской Федерации. E-mail: garbulinkd@rosgvard.ru

DOI: 10.17212/2782-2230-2026-2-37-49

Research of biometric authentication methods and development of a web application for facial user identification using machine learning libraries*

V.V. Perevoznikov¹, K.D. Garbulin²

¹ Perm Military Institute of the Russian National Guard Troops, 1 Gremyachiy Log Street, Perm, 614030, Russian Federation, associate Professor of the Department of Troop Command and Information Security Automation. E-mail: perevoznikovvv@rosgvard.ru

² Perm Military Institute of the Russian National Guard Troops, 1 Gremyachiy Log Street, Perm, 614030, Russian Federation, cadet of the Faculty of Communications and Automated Troop Command. E-mail: garbulinkd@rosgvard.ru

This paper examines biometric authentication methods for minimizing unauthorized access to confidential information. A comparative analysis of approaches to identity detection and verification is conducted, with a focus on facial recognition technology based on deep neural networks. The practical component of the study is the development of a web application implementing user facial authentication. The paper describes the software system architecture,

* Received 17 April 2026.

image processing stages (detection, alignment, feature extraction), and the integration of trained machine learning models into a Python backend using the Django framework and the DeepFace library. The results of an experimental evaluation of the accuracy and performance of the proposed solution are presented.

Keywords: biometric authentication, facial recognition, machine learning, convolutional neural networks, web development, DeepFace, Django, information security

REFERENCES

1. Abselyamov A.A., Lagutkina T.V. Issledovanie metodov autentifikatsii na veb-servisakh. Tekushchie tendentsii i perspektivy razvitiya [Investigation of authentication methods on web services. current trends and development prospects]. *Nauchnyi rezul'tat. Informatsionnye tekhnologii = Research Result. Information Technologies*, 2024, vol. 9, no. 2. Available at: <https://cyberleninka.ru/article/n/issledovanie-metodov-autentifikatsii-na-veb-servisah-tekushchie-tendentsii-i-perspektivy-razvitiya> (accessed 20.03.2026).
2. Bezgachev F.V. Raspoznavanie lits na osnove neironnykh setei: sovremennye tekhnologii [Face recognition based on neural networks: modern technologies]. *Nauchnyi komponent*, 2021, no. 4 (12). (In Russian). Available at: <https://cyberleninka.ru/article/n/raspoznavanie-lits-na-osnove-neyronnyh-setey-sovremennye-tehnologii> (accessed 22.03.2026).
3. Ivanov M.S. Analiz uyazvimostei i aktual'nykh biometricheskikh metodov autentifikatsii v sistemakh bezopasnosti [Analysis of vulnerabilities and current biometric authentication methods in security systems]. *Molodoi uchenyi = Young Scientist*, 2023, vol. 20, no. 467, pp. 4–7. Available at: <https://moluch.ru/archive/467/103000> (accessed 20.03.2026).
4. Kornev L.V. Metody biometrii pri obespechenii informatsionnoi bezopasnosti [Biometric methods in information security]. *Molodoi uchenyi = Young Scientist*, 2022, vol. 17, no. 412, pp. 358–361. Available at: <https://moluch.ru/archive/412/90789> (accessed 21.03.2026).
5. S'yanov S.L., Lantsov V.M. [Application of biometric identification technologies for access control systems in penal facilities]. *Tekhnika i bezopasnost' ob'ektov ugovovno-ispolnitel'noi sistemy* [Technology and safety of penal system facilities]. Collection of materials from the International scientific and practical conference. Voronezh, 2024, pp. 150–153. (In Russian).
6. Serengil S.I., Ozpinar A. LightFace: A hybrid deep face recognition framework. *2020 Innovations in Intelligent Systems and Applications Conference (ASYU)*, Istanbul, Turkey, 2020, pp. 1–5. DOI: 10.1109/ASYU50717.2020.9259802.

7. Schroff F., Kalenichenko D., Philbin J. FaceNet: A unified embedding for face recognition and clustering. *Proceedings of the IEEE Conference on Computer Vision and Pattern Recognition*, Boston, 2015, pp. 815–823. DOI: 10.1109/CVPR.2015.7298682.

Для цитирования:

Перевозников В.В., Гарбулин К.Д. Исследование методов биометрической аутентификации и разработка веб-приложения для идентификации пользователей по лицу с использованием библиотек машинного обучения // Безопасность цифровых технологий. – 2026. – № 2 (121). – С. 37–49. – DOI: 10.17212/2782-2230-2026-2-37-49.

For citation:

Perevoznikov V.V., Garbulin K.D. Issledovanie metodov biometricheskoi autentifikatsii i razrabotka veb-prilozheniya dlya identifikatsii pol'zovatelei po litsu s ispol'zovaniem bibliotek mashinnogo obucheniya [Research of biometric authentication methods and development of a web application for facial user identification using machine learning libraries]. *Bezopasnost' tsifrovyykh tekhnologii = Digital Technology Security*, 2026, no. 2 (121), pp. 37–49. DOI: 10.17212/2782-2230-2026-2-37-49.