УДК 004.056.53
DOI 10.18413/2411-3808-2019-46-1-148-160

# РАЗРАБОТКА ИНТЕЛЛЕКТУАЛЬНОЙ СИСТЕМЫ БИОМЕТРИЧЕСКОЙ ИДЕНТИФИКАЦИИ ПОЛЬЗОВАТЕЛЯ

# THE DEVELOPMENT OF INTELLIGENT BIOMETRIC IDENTIFICATION SYSTEM USER

**С.Н. Девицына[1], Т.А. Елецкая[1], Т.Н. Балабанова[2], Н.Н. Гахова[2]**
**S.N. Devitsyna[1], T.A. Eletskaya[1], T.N. Balabanova[2], N.N Gakhova[2]**

[1)] Севастопольский государственный университет,
Россия, 299053, г. Севастополь, ул. Университетская, 33
[2)] Белгородский государственный национальный исследовательский университет,
Россия, 308015, г. Белгород, ул. Победы, 85

[1)] Sevastopol State University,
33 Universitetskaya St, Sevastopol, 299053, Russia
[2)] Belgorod National Research University,
85 Pobeda St, Belgorod, 308015, Russia

E-mail: sndevitsyna@sevsu.ru, toma.eletskaya@mail.ru, sozonova@bsu.edu.ru

**Аннотация**
Биометрические методы являются эффективным инструментом идентификации личности и применяются для верификации субъекта, защиты от несанкционированного доступа, контроля явки сотрудника на работу, поиска преступников, выявления террористов. В статье приведен обзор современных биометрических методов идентификации личности, показаны их преимущества и недостатки, а также примеры использования в различных сферах деятельности. Проведен анализ статистических данных и сделано сравнение точности разных методов биометрической идентификации по показателям FRR (False Rejection Rate) и FAR (False Acceptance Rate), характеризующим надежность идентификации. В результате в качестве идентификатора было выбрано изображение лица. Для повышения точности идентификации использованы возможности нейросетевых технологий. Приведен пример программной реализации интеллектуальной системы идентификации пользователя по изображению лица. Основное отличие от существующих решений состоит в одновременном применении нескольких инструментов машинного обучения при подготовке и обработке изображений. Разработанное решение использует две нейросети для разных задач, что делает точность идентификации выше по сравнению с аналогичными решениями для того же типа биометрики.

**Abstract**
Biometrical methods are the effective tool for people identification and are used to verify the person, protect against unauthorized access, control the employee attendance, search for criminals, identify terrorists. The article provides an overview of modern biometric methods of identification, explain their advantages and disadvantages, as well as examples of their use in various fields. The analysis of statistical data and a comparison of the accuracy of different methods of biometric identification indicators according to FRR (False Rejection Rate) and FAR (False Acceptance Rate) which are the measures of reliability identification is also done. As a result, the face image was chosen as the identifier. To improve the accuracy of identification, the neural networks were used. An example of software implementation of an intelligent system of user identification by foto is given. The main difference from existing solutions is the simultaneous use of several machine learning tools during the images preparation and processing. The developed solution uses two neural networks for different tasks, which makes the identification accuracy higher in comparison with competitor solutions on the same type of biometrics.

**Ключевые слова**: информационные технологии, информационная безопасность, искусственный интеллект, биометрия, идентификация, биометрические технологии, распознавание образов.
**Keywords**: information technology, information security, artificial intelligence, biometrics, identification, biometric technologies, pattern recognition.

## Введение

Современный уровень развития информационных технологий, а также более высокие требования к обеспечению информационной безопасности привели к тому, что традиционные средства идентификации – логины, коды, ключи, карты доступа – перестают быть эффективными, что влечет за собой не только материальный ущерб компании из-за действий злоумышленников, но и не обеспечивает требуемую безопасность личности в информационном пространстве. Требования персонализации и активное внедрение smart-технологий в технических системах и даже на бытовом уровне (например, Smart Home – Умный Дом, IoT – Интернет вещей) привели к необходимости использования более совершенных и надежных механизмов идентификации. Технологии аутентификации переходят на новый уровень развития – используются сложные методы верификации субъекта на основе комбинации различных идентификаторов, алгоритмов, протоколов. На первое место среди требований обеспечения безопасного доступа к объекту выходят точность идентификации и эффективность.

*Точность* идентификации определяется двумя показателями: вероятностью отказа доступа человеку, имеющего допуск (ошибки I рода), и вероятностью ложного совпадения биометрических характеристик двух людей (ошибки II рода). Кроме того, к характеристикам биометрических систем идентификации относятся: устойчивость к муляжу (имитации биометрики), скорость работы, простота использования, стоимость системы. *Эффективность* – это соотношение между достигнутым результатом (правильной идентификацией) и использованными для идентификации субъекта ресурсами системы (ГОСТ Р ИСО/МЭК 19795-1-2007).

## Основная часть

Особенностью биометрических систем является то, что процедура получения, хранения и использования для идентификации биометрических данных является сложной, что приводит к дороговизне реализующих ее технических устройств. Биометрики уникальны, их не нужно запоминать, как пароль, они всегда с субъектом.

Биометрические данные делятся на две группы: физиологические и поведенческие. К первой группе относят: ДНК; отпечаток пальца (дактилоскопические данные); цифровое изображение лица в 2D или 3D-проекции; рисунок радужной оболочки глаза; рисунок сетчатки глаза; рисунок вен руки, голос; геометрию кисти руки; форму уха и др. Поведенческими являются: динамика подписи; клавиатурный почерк; походка; голос. Рассмотрим особенности реализации различных методов биометрической идентификации [Мальцев, 2018; Кухарев, 2001; Вакуленко и др., 2006].

Самым распространенным методом биометрической идентификации является *дактилоскопическая экспертиза*. Для снятия отпечатка пальца применяют как традиционный метод – с использованием краски, так и современный – получение электронного отпечатка с помощью сканера. Специальные сенсоры делают высококачественный цифровой снимок папиллярного узора пальца, который потом преобразуется в код, хранящийся в базе данных. Данный метод является недорогим, быстрым и точным, кроме того, на рынке имеется большое количество сканеров отпечатков и специализированных программ. Современные сканеры имеют расширенный функционал, например, могут учитывать рельеф линий, силу нажатия и температуру, эти дополнительные параметры применяют для исключения возможности подделки биометрических данных. Недостатком метода является то, что на пальцах часто возникают порезы и царапины, которые могут затруднить либо сделать

идентификацию непригодной. Кроме того, специфика отдельных видов деятельности (например, химическое производство) делает дактилоскопию невозможной, а метод – непригодным для идентификации субъекта.

Второй по популярности метод – идентификация *по геометрии лица*. Популярность метода обусловлена тем, что он часто используется в криминалистике для определения местоположения преступника, выявления террористов. Метод основан на распознавании лиц, попадающих в кадр при использовании систем видеонаблюдения. Такие системы широко используются в местах большого скопления людей: на вокзалах, в метро, в аэропортах.

Тем не менее данный метод биометрической идентификации имеет плохие статистические показатели, его эффективность зависит от параметров видеокамеры, освещения, скорости перемещения и удаленности объекта наблюдения, он чувствителен к мимике. Появление современных методов распознавания образов и создания 3D-изображений привело к улучшению качественных показателей данного метода, но вместе с тем – и к дороговизне оборудования.

Идентификация *по радужной оболочке глаз* многими экспертами признается наиболее точным способом установления личности. Рисунок радужной оболочки практически не изменяется в течение жизни человека, для проведения процедуры идентификации не требуется физический контакт с устройством, так как считывание производится на комфортном расстоянии от глаз. Сканеры захватывают изображение, оцифровывают его и передают в устройство сравнения, которое сравнивает изображение с базой данных и выявляет соответствие. Данные системы обладают высокой надежностью, быстротой и точностью. Недостаток – точность метода зависит от разрешения камеры, а также дороговизна оборудования. Тем не менее из-за высокой точности метода такие системы используются организациями, в сферу деятельности которых входит работа с секретными документами.

Самыми лучшими показателями по точности распознавания обладает *метод сканирования сетчатки глаза*. У данных систем самый низкий процент отказа, поэтому их чаще всего используют на особо секретных объектах для реализации систем контроля доступа и идентификации сотрудников. Метод основан на получении изображения рисунка кровеносных сосудов на задней стенке глаза. Недостатки метода: сложная процедура получения рисунка сосудов оптической системой требует достаточно долгой неподвижности исследуемого субъекта, что вызывает дискомфорт. Стоимость систем достаточно высокая. Требуется большое время для получения и обработки изображения.

*Метод распознавания по рисунку вен руки* является достаточно точным, обладает высокой достоверностью. Кроме того, данную характеристику сложно подделать, ведь, чтобы получить изображение, требуется использовать специальную инфракрасную камеру и программу, преобразующую изображение в код. Эта технология – одна из самых новых. Недостатки метода: некоторые заболевания могут привести к изменению рисунка вен, сканеры чувствительны к солнечным лучам и галогеновым лампам.

Для выбора вида биометрики для создания интеллектуальной системы идентификации пользователя проведем сравнительную оценку рассмотренных методов.

Основные показатели надежности биометрической системы (по ГОСТ Р ИСО/МЭК 19795-1-2007) – это ошибки I и II рода, коэффициенты FAR и FRR: False Acceptance Rate (FAR) – ошибочное подтверждение (принятие решения «чужой = свой», вероятность несанкционированного допуска) и False Rejection Rate (FRR) – ошибочный отказ (принятие решения «свой = чужой», вероятность ложного задержания). Сравнение точности разных методов биометрической идентификации можно провести, используя показатели FRR и FAR.

Эффективность определения показателей зависит от условий тестирования.

В табл. 1 приведены данные исследований эффективности биометрических методов [Биометрическая система на мобильном телефоне. 2018. URL: https://habr.com/post/236209/ (дата обращения 30.10.2018 г.)].

Таблица 1
Table 1

Значение показателей точности биометрических методов идентификации
Value of indicators of accuracy of biometric methods of identification

| Биометрический признак | Тест | Условия тестирования | FRR | FAR |
|---|---|---|---|---|
| Отпечатки пальцев | FVC 2006 | неоднородная популяция, включая работников ручного труда и пожилых людей | 2,2% | 2,2% |
| Лицо | MBE 2010 | полицейская база фотографий | 4,0% | 0,1% |
| Голос (ООО «ЦРТ») | NIST 2012 | текстонезависимое распознавание | 3% | 1% |
| Радужная оболочка глаз | ICE 2006 | контролируемое освещение, широкий диапазон качества | 1,1% | 0,1% |

Важно учесть, что вероятности ошибочного отказа и ошибочного подтверждения связаны друг с другом, а качество процедуры распознавания определяется их соотношением: идентификация тем точнее, чем меньше значение FRR при одинаковых значениях FAR. Для оценки точности вводят коэффициент EER (равный уровень ошибок) – это коэффициент, при котором становятся эквивалентными ошибка подтверждения и ошибка отказа. Из этого следует, что точность биометрической системы тем выше, чем меньше коэффициент EER. Для определения точности метода идентификации, как численного параметра, допустимое значение FAR фиксируется (то есть задается «порог» совпадения биометрик двух субъектов, рис. 1), а значение FRR становится интегральным критерием точности.

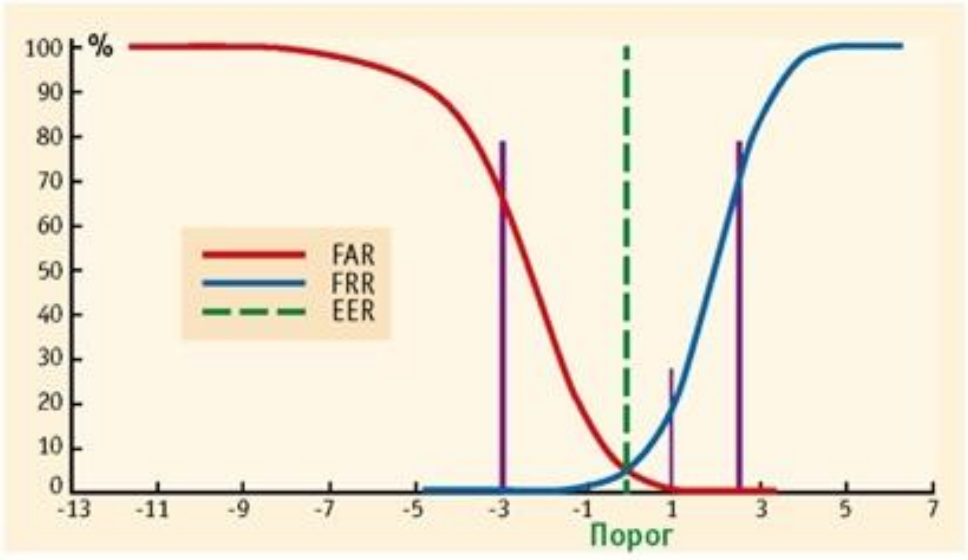


Рис. 1. Графики FAR и FRR [Михайлов и др., 2015]
Fig. 1. Graphs of FAR and FRR

По результатам статистических исследований строят характеристические кривые – ROC-кривые (Receiver Operating Characteristic), или кривые рабочих характеристик РХ, которые показывают зависимость между ВЛНС – вероятностью ложного несовпадения (false non-match rate; FNMR) и ВЛС – вероятностью ложного совпадения (false match rate; FMR). ROC – это заданная с помощью параметров функция порога принятия решения, в которой учитываются попытки злоумышленника (вероятность ложно-положительных решений, ось *x*) и попытки легитимного пользователя (вероятность истинно-положительных решений, ось *y*), как показано на рис. 2.


Рис. 2. Пример ROC-кривой (кривой рабочих характеристик) [Михайлов и др., 2015]
Fig. 2. An example of a ROC curve (performance curve)

Для того чтобы сравнить эксплуатационные характеристики различных биометрических систем, используемых в одинаковых условиях, или одной биометрической системы, используемой в различных условиях окружающей среды, применяют кривые рабочих характеристик (ROC), из-за их свойства не зависеть от порога.

Таким образом, выбор требуемого соотношения между показателями FAR и FRR является неким компромиссным решением, принятие которого зависит от многих факторов, например, численности персонала компании, и, соответственно, размера баз данных, методов ограничения доступа, применяемых компанией, целей идентификации субъектов. Для решения такой задачи используют кривые КОО – компромиссного определения ошибки (detection error trade-off curve; DET curve). Кривые КОО представляют собой модификацию кривой рабочих характеристик. Ось *x* кривых компромиссного определения ошибок – это значения вероятностей ложноположительных ошибок, а ось y – значения ложноотрицательных ошибок. Таким образом, используя кривую КОО, можно построить графики вероятностей ошибок сравнения (ВЛНС (FNMR) в зависимости от ВЛС (FMR)), вероятностей ошибок принятия решения (ВЛНД (FRR) в зависимости от ВЛД (FAR)) и вероятностей идентификации на открытом множестве (ВЛОИ в зависимости от ВЛПИ). Пример кривых компромиссного определения ошибки представлен на рис. 3 (по ГОСТ Р ИСО/МЭК 19795-1-2007).


Рис. 3. Пример кривых DET некоторого набора систем A-F
Fig. 3. Example of DET curves of some set of A-F systems

Методики получения ROC-кривых различны. Выбор методики тестирования зависит от обстоятельств тестирования, алгоритма и условий проведения тестов, сценария используемой системы, количества тестируемых и других факторов. В свою очередь, тип тестирования определяется применяемой методикой. Существуют технологическое, сценарное и операционное тестирование. Поэтому результаты анализа одной и той же системы идентификации, полученные по разным методикам тестирования, могут значительно отличаться. Таким образом, эффективность системы биометрической идентификации является интегрированным показателем, зависящим от процента правильной идентификации и затраченного на минимизацию ошибок ресурса.

Приблизительные значения точности в режиме операционного тестирования для основных биометрических методов приведены в [Вакуленко и др., 2006] и показаны в табл. 2.

Таблица 2
Table 2

Точность (в процентах) биометрических методов [Вакуленко и др., 2006]
Accuracy (percentage) of biometric methods

| Метод | 3D Лицо | 2D Лицо | Отпечаток пальца* (один палец) | | | | Радужная оболочка |
|---|---|---|---|---|---|---|---|
| FAR | FRR A4Vision | FRR (лучший 2D-алгоритм) | FRR сканер 1 | FRR сканер 2 | FRR сканер 3 | FRR сканер 4 | FRR (лучший сканер)** |
| $10^{-3}$ (0,1%) | 0,2 | 19 | 0,4 | 1,5 | 5 | 8 | 4,7 |
| $10^{-4}$ (0,01%) | 1 | 28 | 1 | 2 | 7 | 10 | 5,3 |
| $10^{-5}$ (0,001%) | 1,5 | - | 1,3 | 3 | 8 | 14 | 6 |
| * См. FpVTE 2003 results (http://fpvte.nist.gov);<br>** см. IBG ITIRT 2005, p.92, Figure 66 Cross-Visit Recognition Comparison Results (Single-Attempt). | | | | | | | |

Вероятность ложного распознавания зависит от количества субъектов. В больших базах данных ошибки совпадения биометрик выше, например, при количестве субъектов 2000 и более, ни один из биометрических методов не удовлетворяет по точности. Поэтому рекомендуется использовать многокритериальные системы для идентификации (двойная, тройная верификация), например, отпечатки нескольких пальцев, комбинации «голос – форма лица» и т. п.

Появление «мультимодальных» методов биометрической идентификации путем одновременного использования 2D- и 3D-изображений лица приводит к обеспечению требуемой точности идентификации при базах данных размером до десяти тысяч лиц. Кроме того, в системах распознавания образов в настоящее время широко используются интеллектуальные средства [Biometrics, 2016; Одинец Д.Н., 2018; Васильев, 2017; Васильев и др., 2015; Советов и др., 2013; Еременко и др., 2014]. В частности, в системах компьютерного зрения для обучения системы применяют нейросетевые технологии. В результате сравнения показателей надежности методов биометрической идентификации принято решение в качестве биометрики использовать изображение лица. В данной статье в качестве примера интеллектуального средства распознавания пользователя по изображению лица будет приведено описание системы, созданной Т. Елецкой с использованием инструментов Python и нейросетевых технологий. Система названа «ZORGO» (в переводе с эсперанто – «Смотритель»).

## О разработке

Данная разработка реализует удобное хранилище для данных в формате HDF5 и применяет компьютерное зрение для анализа изображений. При создании интеллектуального средства идентификации были использованы: DLIB, HDF5, OpenCv, NumPY, face_recognition.

DLIB представляет собой универсальную кроссплатформенную программную библиотеку, написанную на языке программирования C++. Для реализации были взяты две предварительно обученные на лицах нейросети DLIB: dlib_face_recognition_resnet_model_v1.dat.bz2 (GitHub dlib-models). Нейросети реализуют разные задачи. Первая нейросеть определяет на фото лицо человека. Для этого используется набор данных, представляющих координаты уголков глаз и рта. Если нейросеть находит лицо на фото, она передает выделенное по координатам изображение лица второй нейросети. Вторая нейросеть также предварительно обучена на изображениях лиц людей. Ее задача – преобразовать лицо в набор числовых данных размерностью 128 признаков. Таким образом, используя комбинацию двух нейросетей, из фото лица получаем массив данных – чисел длиной 128, с которыми система потом работает для установления личности (идентификации).

HDF5 (Hierarchical Data Format – иерархический формат данных) – название формата файлов, разработанного для хранения большого объема цифровой информации. Свободно распространяемый пакет HDF состоит из библиотеки, утилиты командной строки, исходных текстов для тестирования, интерфейса для Java и Java-программы для просмотра HDF-файлов. Поддерживается Python.

При распознавании, когда имеется сохраненный экземпляр изображения лица (массив данных), происходит сравнение нового массива, извлеченного этой нейросетью, и уже существующего экземпляра. Для каждого пользователя хранятся данные не более чем о десяти изображениях лица. Идентификатором для массива является UUID4 (рис. 4).

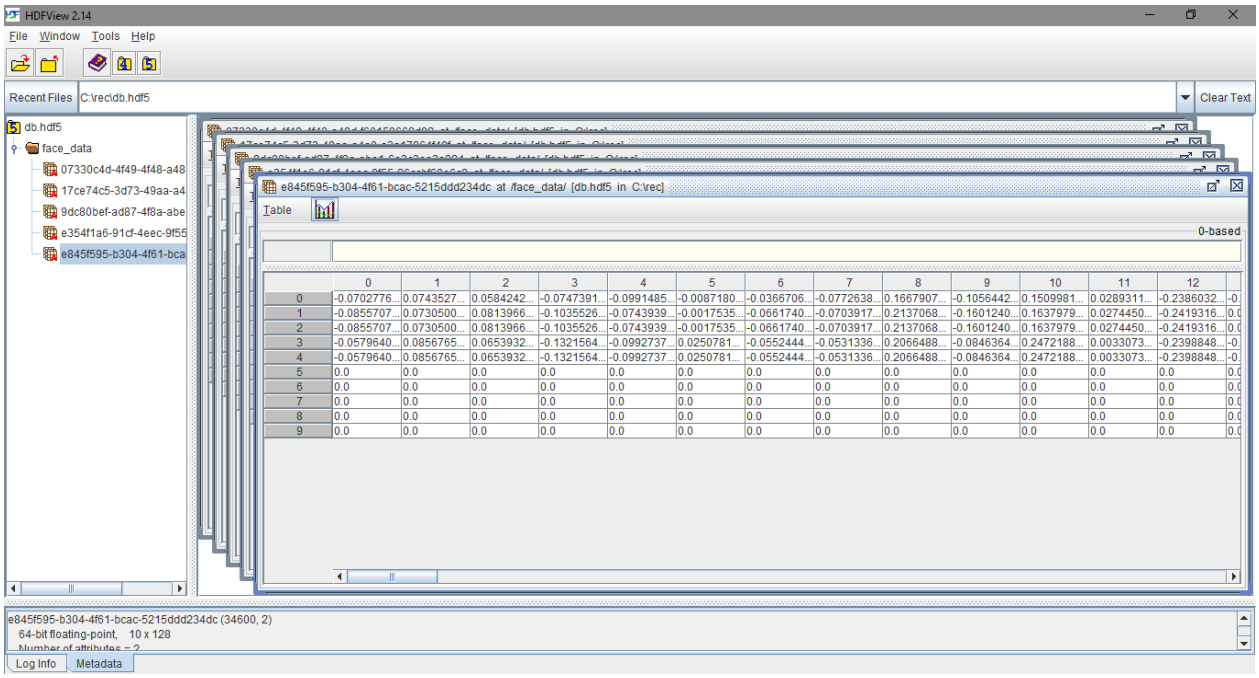


Рис. 4. Идентификатор для массива UUID4
Fig. 4. The identifier for the array UUID4

UUID (universally unique identifier) – это стандарт идентификации, используемый в создании программного обеспечения, является частью среды распределенных вычислений DCE (Distributed Computing Environment).

Для обработки видео используется библиотека компьютерного зрения с открытым исходным кодом OpenCV (Open Source Computer Vision Library), которая реализована на C/C++ и разрабатывается для Python, Java, Ruby, Matlab, Lua и других языков.

NumPy – библиотека с открытым исходным кодом для языка программирования Python. Возможности: поддержка многомерных массивов; поддержка высокоуровневых математических функций, предназначенных для работы с многомерными массивами.

Face_recognition – это прослойка для Python, позволяющая использовать написанную на C++ DLIB (установка производится с помощью pip, что будет рассмотрено ниже).

Для создания интеллектуальной системы идентификации использовались математические методы: нахождение коэффициента корреляции, метрическая разность.

*Подготовка к запуску и работа с программой.* Для запуска данной программы необходимо:

1) Установить Python 3.6 в каталог C: \Python36.

2) При помощи пакетного менеджера «pip» устанавливаем необходимые библиотеки:

- dlib – библиотека на C++, которая реализует нейросети и face_recognition;
- numpy – методы линейной алгебры и массивы;
- hdf5py – библиотека для работы с файлами стандарта HDF5;
- OpenCV – библиотека компьютерного зрения.

3) Начало работы с программой.

Исходные файлы для работы с программой (рис. 5):

- adduser.py; Recognize.py – программы, которые представляют пользовательский функционал;
- adduser – ярлык, запускающий программу adduser.py;
- webcam – запускает recognize.py в режиме вебкамеры;
- access – запускает recognize.py в текстовом режиме;
- improcessing.py – используется для обработки изображений с помощью face_recognition (которая, в свою очередь, применяется для DLIB). В данном файле реализован интерфейс, с помощью которого производится ввод данных в модуль predictor;
- predictor.py – ядро системы, которое отвечает за поиск и сравнение лиц по базе данных HDF5. Ключевым методом является «predict_face» – данный метод возвращает список лиц, похожих по параметрам с передаваемым изображением.

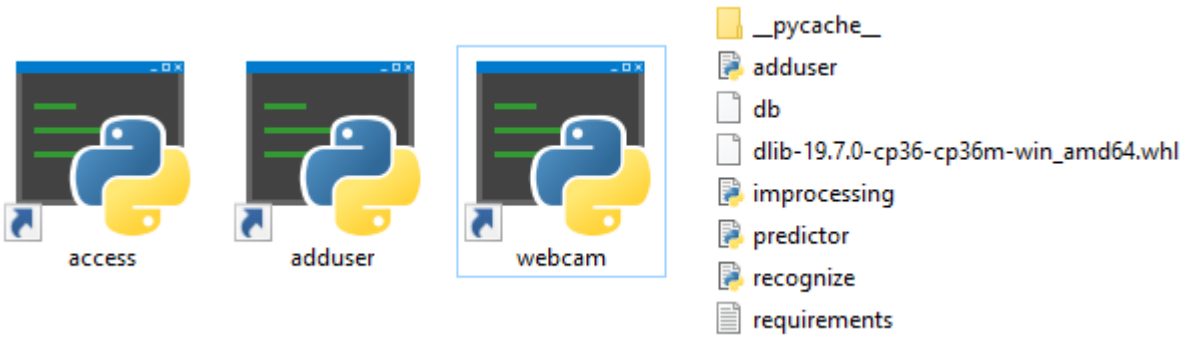


Рис. 5. Исходные файлы для работы с программой
Fig. 5. Source files for working with the program

4) Работа с программой.

Открываем программу «adduser» для добавления нового пользователя: вводим имя (tomaE) и смотрим в камеру (рис. 6). Система делает снимок лица с помощью вебкамеры.

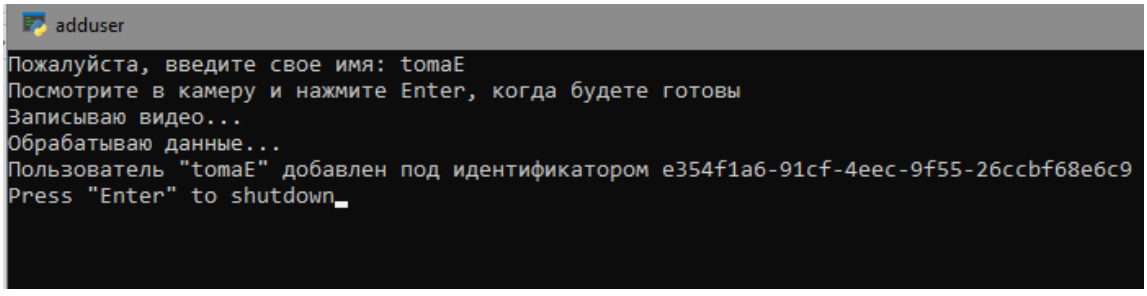


Рис. 6. Окно программы «adduser»
Fig. 6. The window of the program «adduser»

Далее открываем программу «acess» и получаем доступ к системе (рис. 7). Благодаря «adduser» система уже имеет данные о введенном имени и изображении лица.

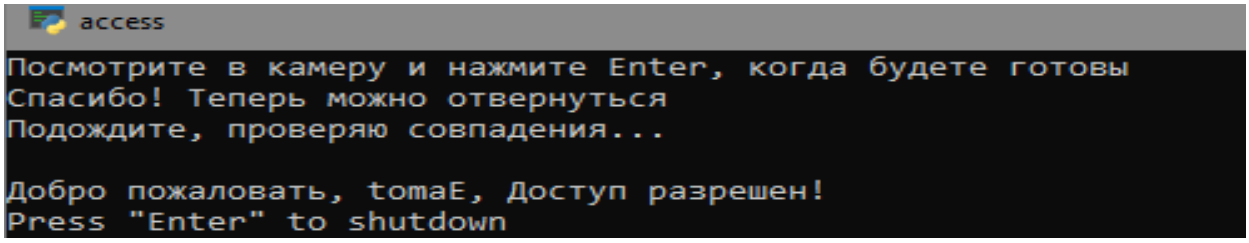


Рис. 7. Успешное получение доступа к системе
Fig. 7. Successful access to the system

Если данные в систему не занесены, она запретит доступ (рис. 8).

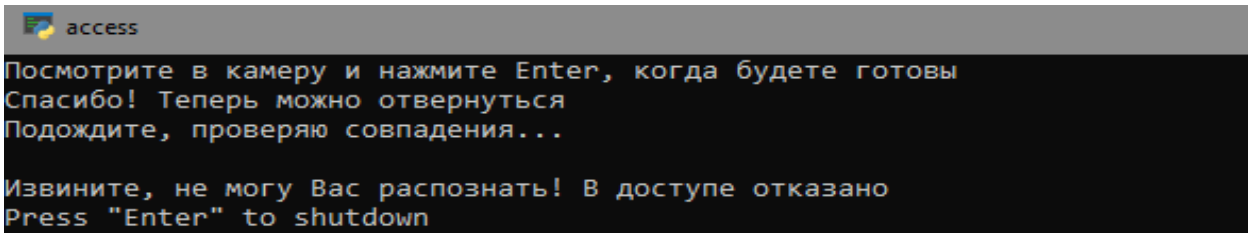


Рис. 8. Отказ в доступе
Fig. 8. Denial of access

Запускаем «webcam». На экране появляется видеоизображение пользователя, и программа, в случае идентификации, выделяет область лица рамкой зеленого цвета, в которой указывается имя пользователя (рис. 9).

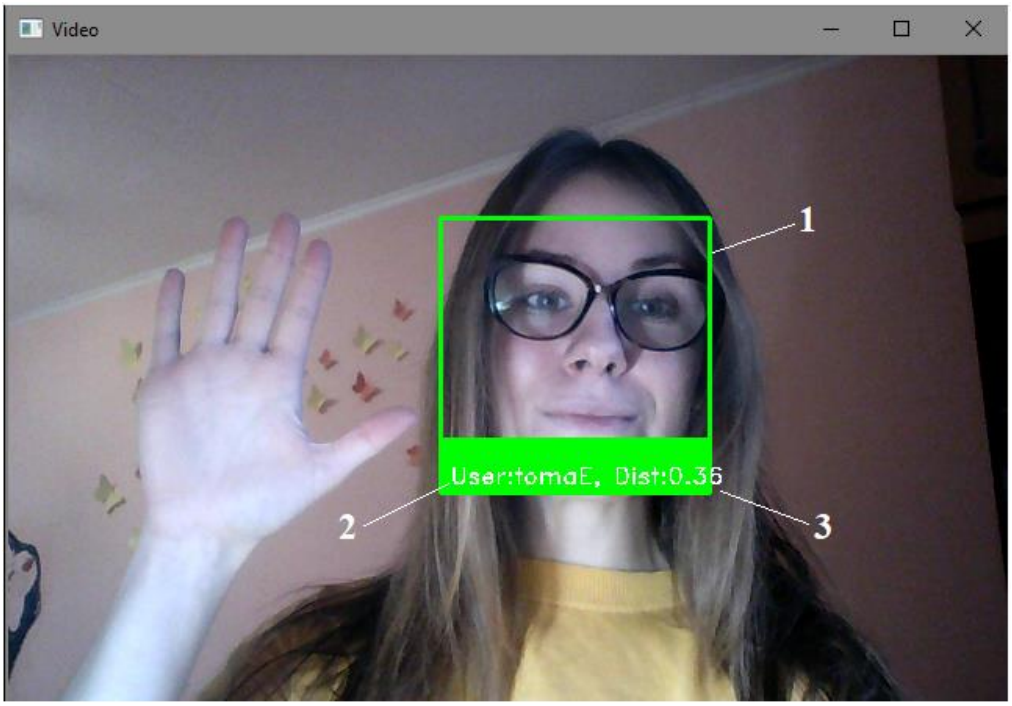


Рис. 9. Окно программы «webcam» с распознанным пользователем: 1 – рамка, выделяющая область лица на видеоизображении; 2 – User: имя пользователя; 3 – Dist:0.36 – метрическое расстояние
Fig. 9. The program window is "webcam" with the recognized user: 1 – frame that highlights the area of the face on the video image; 2 – User: username; 3 – Dist: 0.36 – metric distance

Чем меньше метрическое расстояние, тем точнее совпадение. Если значение больше 0.5, то система не распознает пользователя, рамка становится красной и имя пользователя сменяется на «Unknown» (пользователь неизвестен) (рис. 10).

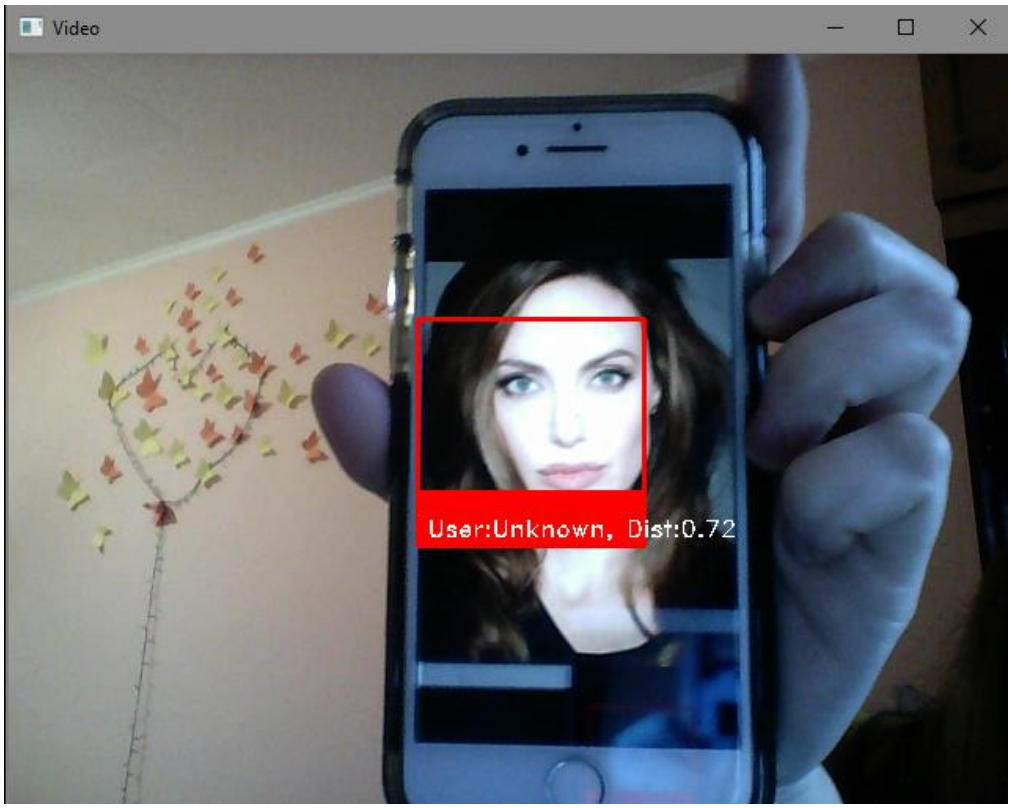


Рис. 10. Нераспознанный пользователь
Fig. 10. Unrecognized user

Сеть была обучена «с нуля» на наборе данных около трех миллионов лиц, который является производным от нескольких свободно распространяемых наборов данных.

Биометрические системы идентификации личности широко применяются на предприятиях для защиты от несанкционированного доступа, контроля явки сотрудника на работу, учета рабочего времени. Кроме гражданских систем, биометрия широко используется спецслужбами для поиска преступников и выявления террористов. С июля 2018 г. принято решение использовать биометрический паспорт в банковской сфере для защиты банковской тайны, контроля доступа, идентификации клиентов при получении кредитов и совершении финансовых операций в банкоматах. Методы сканирования лица широко применяются в местах массового скопления людей для проведения антитеррористических мероприятий. Начато внедрение биометрических систем идентификации в образовательных и медицинских учреждениях, на транспорте (в составе платежной системы), в системах электронного голосования. Применение данных технологий способствует обеспечению как безопасности личности в информационном пространстве, так и безопасности бизнеса, науки и государства в целом. Поэтому предложенная разработка является актуальной и востребованной.

## Результаты и их обсуждение

Традиционные идентификаторы постепенно вытесняются более надежными и точными системами, основанными на биометрической идентификации личности. Как показал анализ, наиболее точными являются системы биометрической идентификации, использующие в качестве биометрики ДНК, рисунок радужной оболочки и сетчатки глаза.

Вместе с тем данные системы являются дорогостоящими и не всегда могут быть использованы для систем контроля доступа компании.

Применение «мультимодальных» методов биометрической идентификации приводит к повышению точности работы системы. Следующим этапом развития технологий биометрической идентификации является внедрение интеллектуальных средств, работающих в условиях неполной достоверности и неопределенности информации, и способных использовать механизмы нечеткой логики и нейросетевые технологии для реализации процедур идентификации/верификации субъектов.

Достоинством разработанной интеллектуальной системы идентификации «ZORGO» является то, что точность распознавания практически не зависит от мимики, наличия на лице очков, усов, бороды. Основное отличие от существующих решений состоит в одновременном применении нескольких инструментов машинного обучения при подготовке и обработке изображений. Разработанное решение использует две нейросети для разных задач, что делает точность работы выше по сравнению с аналогичными решениями. Первая нейросеть занимается извлечением области лица из предоставляемых изображений. Она использует метод обнаружения лица по пяти точкам (брови, глаза, нос, рот, челюсть) на основе метода гистограмм-ориентированных градиентов (HOG или Histogram of Oriented Gradients) [Mahpod et al., 2018]. HOG-распределение используется в качестве признаков для определения лиц. Градиенты (производные x и y) изображения полезны, потому что величина градиентов велика по краям и углам (области резких изменений интенсивности), так как края и углы содержат гораздо больше информации о форме объекта, чем плоские области.

Основные преимущества используемого метода:

- самый быстрый метод для CPU;
- работает очень хорошо для фронтальных и слегка не фронтальных граней;
- облегченная модель по сравнению с существующими (CNN, Haar Cascade);
- работает при небольшой окклюзии.

Недостатки:

- основным недостатком является то, что не обнаруживаются маленькие лица, поскольку сеть обучена при минимальном размере лица 80×80;
- ограничительная рамка часто исключает часть лба и даже часть подбородка;
- не очень хорошо работает при значительной окклюзии;
- не работает для боковой грани и экстремальных нефронтальных граней, например, взгляд вниз или вверх [Vikas Gupta, 2018; Satya Mallick, 2016].

Вторая нейросеть используется для непосредственного преобразования данных о лицах в числовые векторы. Эта модель представляет собой сеть ResNet с 27 сверхточными слоями. Она является версией сети ResNet-34 [Kaiming He et al., 2015] с несколькими удаленными слоями и уменьшением количества фильтров на слой вдвое.

Хотелось бы отметить, что разработанная система идентификации «ZORGO» распознает лица с фотографии (печатный формат, фото с экрана телефона) так же качественно, как и через камеру ПК. Вместе с тем данный фактор является уязвимостью, так как при помощи фото можно «обмануть» систему и получить доступ без согласия пользователя. Поэтому предлагаемая разработка может быть использована, например, в системах видеонаблюдения для выявления и идентификации разыскиваемых людей.

## Список литературы
## References

1. ГОСТ Р ИСО/МЭК 19795-1-2007. Национальный стандарт Российской Федерации «Автоматическая идентификация. Идентификация биометрическая. Эксплуатационные испытания и протоколы испытаний в биометрии. Часть 1. Принципы и структура». Automatic identification. Biometrics. Biometric performance testing and reporting. Part 1. Principles and framework. Дата введения 01.01.2009.

GOST R ISO/IEC 19795-1-2007 Automatic identification. Biometrics. Biometric performance testing and reporting. Part 1. Principles and framework [Avtomaticheskaya identifikaciya. Identifikaciya biometricheskaya. EHkspluatacionnye ispytaniya i protokoly ispytanij v biometrii. CHast' 1. Principy i struktura]. Date of introduction 01.01.2009 (in Russian).

2. Мальцев А. 2018. Современные биометрические методы идентификации. URL: https://habr.com/post/126144 (дата обращения 30.10.2018).

Mal'cev A. 2018. Sovremennye biometricheskie metody identifikacii [Current biometric methods of identification]. Availableat: https://habr.com/post/126144 (accessed 30 Oktober 2018) (in Russian).

3. Кухарев Г.А. 2001. Биометрические системы. Методы и средства идентификации личности человека. М., Политехника, 240.

Kuharev G.A. 2001. Biometricheskie sistemy. Metody i sredstva identifikacii lichnosti cheloveka [Biometric system. Methods and means of identification of a person]. Moscow, Politekhnika, 240 (in Russian).

4. Вакуленко А., Юхин А. 2006. Биометрические методы идентификации личности: обоснованный выбор. BYTEmag.ru, 1(89). URL: https://www.bytemag.ru/articles/detail.php?ID=9077 (дата обращения 29.10.2018).

Vakulenko A., Yuhin A. 2006. Biometricheskie metody identifikacii lichnosti: obosnovannyj vybor [Biometric methods of identification: reasonable choice]. BYTEmag.ru, 1(89). Availableat: https://www.bytemag.ru/articles/detail.php?ID=9077/ (accessed 29 Oktober 2018) (in Russian).

5. Михайлов А.А., Колосков А.А., Дронов Ю.И. 2015. Основные параметры биометрических систем. Журнал «Алгоритм Безопасности», 5. URL: https://algoritm.org/arch/arch.php (дата обращения 30.10.2018).

Mihajlov A.A., Koloskov A.A., Dronov Yu.I. 2015. Basic parameters of biometric systems [Osnovnye parametry biometricheskih sistem]. Algoritm Bezopasnosti [The Security Algorithm], 5. Availableat: https://algoritm.org/arch/arch.php (accessed 30 Oktober 2018) (in Russian).

6. Биометрическая система на мобильном телефоне. 2018. URL: https://habr.com/post/236209/ (дата обращения 30.10.2018 г.).

Biometricheskaya sistema na mobil'nom telephone [Biometric system on mobile phone]. 2018. Availableat: https://habr.com/post/236209 (accessed 30 Oktober 2018) (in Russian).

7. Одинец Д.Н. 2018. Способы построения систем идентификации личности по биометрическим параметрам. Информационные технологии в системе образования, агропромышленности, биржевой системе. Защищенные информационные системы органов государственного управления и социальной сферы. Белорусский институт системного анализа и информационного обеспечения научно-технической сферы. URL: http://www.belisa.org.by/pdf/PTS2005/151-157.pdf (дата обращения: 13.11.2018).

Odinecz D.N. 2018. Sposoby` postroeniya sistem identifikacii lichnosti po biometricheskim parametram [Methods of construction of systems of identification of the personality on biometric parameters]. Informacionny`e texnologii v sisteme obrazovaniya, agropromy`shlennosti, birzhevoj sisteme. Zashhishhenny`e informacionny`e sistemy` organov gosudarstvennogo upravleniya i social`noj sfery`. Belorusskij institut sistemnogo analiza i informacionnogo obespecheniya nauchno-texnicheskoj sfery`. Availableat: http://www.belisa.org.by/pdf/PTS2005/151-157.pdf (accessed 13 November 2018) (in Russian).

8. Васильев В.И. 2017. Интеллектуальные системы защиты информации: учеб. пособие. М., «Издательство «Инновационное машиностроение»», 34–73.

Vasil'ev V.I. 2017. Intellektual'nye sistemy zashchity informacii: ucheb. posobie [Intelligent information security systems]. M., «Izdatel'stvo «Innovacionnoe mashinostroenie»», 34–73 (in Russian).

9. Васильев В.И. и др. 2015. Технологии скрытой биометрической идентификации пользователей компьютерных систем (обзор). В.И. Васильев, П.С. Ложников, А.Е. Славко, А.В. Еременко. Вопросы защиты информации, 3. URL: https://elibrary.ru/item.asp?id=24833962 (дата обращения: 14.11.2018).

Vasil'ev V.I. et al. 2015. Tekhnologii skrytoj biometricheskoj identifikacii pol'zovatelej komp'yuternyh sistem (obzor) [Technologies of hidden biometric identification of users of computer systems (review)]. V.I. Vasil'ev, P.S. Lozhnikov, A.E. Slavko, A.V. Eremenko. Voprosy zashchity informacii, 3. Available at: https://elibrary.ru/item.asp?id=24833962 (accessed 14 November 2018) (in Russian).

10. Советов Б.Я. 2013. Интеллектуальные системы и технологии: Учебник. Б.Я. Советов, В.В. Цехановский, В.Д. Чертовской. М., ИЦ Академия, 320.

Sovetov B.Ya. 2013. Intellektual'nye sistemy i tekhnologii: Uchebnik [Intelligent systems and technologies]. B.Ya. Sovetov, V.V. Cekhanovskij, V.D. Chertovskoj. M., IC Akademiya, 320 (in Russian).

11. Еременко А.В. и др. 2014. Разграничение доступа к информации на основе скрытого мониторинга действий пользователей в информационных системах: скрытая идентификация. Еременко А.В., Левитская Е.А., Сулавко А.Е., Самотуга А.Е. Вестник Сибирской государственной автомобильно-дорожной академии. СибАДИ. Омск, СибАДИ, 6(40): 92–101. URL: https://elibrary.ru/item.asp?id=22863118 (дата обращения: 15.11.2018).

Eremenko A.V. et al. 2014. Razgranichenie dostupa k informacii na osnove skrytogo monitoringa dejstvij pol'zovatelej v informacionnyh sistemah: skrytaya identifikaciya [Differentiation of access to information on the basis of hidden monitoring of user actions in information systems: hidden identification]. Eremenko A.V., Levitskaya E.A., Sulavko A.E., Samotuga A.E. Vestnik Sibirskoj gosudarstvennoj avtomobil'no-dorozhnoj akademii. SibADI. Omsk, SibADI, 6(40): 92–101. Availableat: https://elibrary.ru/item.asp?id=22863118 (accessed 15 November 2018) (in Russian).

12. Балабанова Т.Н., Чижов И.И., Голощапова В.А., Стецюк Т.С. 2012. Градиентная обработка изображений на основе вариационного метода оценки производных. Научные ведомости БелГУ. Сер. Экономика. Информатика, 7(126): 166–173.

Balabanova T.N., Chizhov I.I., Goloshapova V.A., Stetsyuk T.S. Gradient processing of images on the basis of the variational method of estimating derivatives. BSU Scientific Bulletin. Ser. Economy. Computer science. 2012. 7(126): 166–173.

13. Жиляков Е.Г., Черноморец А.А., Болгова Е.В. Об информационных подобластях пространственных частот изображений. Научные ведомости БелГУ. Сер. Экономика. Информатика, 23(244): 87–93.

Zhilyakov E.G., Chernomorec A.A., Bolgova E.V. Ob informacionnyh podoblastyah prostranstvennyh chastot izobrazhenij. Nauchnye vedomosti BelGU. Ser. Ehkonomika. Informatika, 23(244): 87–93.

14. A Journal of the International Biometric Society: Biometrics. 2016. Aim and Scope. URL: http://www.biometrics.tibs.org/ (дата обращения: 30.10.2018).

15. Projects hosted on GitHub: dlib-models. dlib_face_recognition. 2017. URL: https://github.com/davisking/dlib-models (дата обращения: 01.11.2018).

16. Hierarchical Data Format. 2018. URL: https://ru.wikipedia.org/wiki/Hierarchical_Data_Format (дата обращения: 02.11.2018).

17. UUID. 2018. URL: https://ru.wikipedia.org/wiki/UUID (дата обращения: 02.11.2018).

18. NumPy. 2018. URL: https://ru.wikipedia.org/wiki/NumPy (дата обращения: 02.11.2018).

19. Mahpod S et al. 2018. Facial Landmark Point Localization using Coarse-to-Fine Deep Recurrent Neural Network. Shahar Mahpod, Rig Das, Emanuele Maiorana, Yosi Keller, Patrizio Campisi. arXiv:1805.01760v2 [cs.CV]. URL: https://arxiv.org/pdf/1805.01760.pdf (дата обращения: 18.12.2018).

20. Vikas Gupta. 2018. Face Detection. LearnOpenCV. URL: https://www.learnopencv.com/face-detection-opencv-dlib-and-deep-learning-c-python (дата обращения: 08.11.2018).

21. Satya Mallick. 2016. Histogram of Oriented Gradients. LearnOpenCV. URL: https://www.learnopencv.com/histogram-of-oriented-gradients (дата обращения: 09.11.2018).

22. Kaiming He et al. 2015. Deep Residual Learning for Image Recognition. Kaiming He, Xiangyu Zhang, Shaoqing Ren, Jian Sun. arXiv:1512.03385v1 [cs.CV]. URL: https://arxiv.org/pdf/1512.03385.pdf (дата обращения: 12.11.2018).