

# ТЕХНИЧЕСКИЕ НАУКИ

## ГОЛОСОВАЯ БИОМЕТРИЯ. АНАЛИЗ ИДЕНТИФИКАЦИОННЫХ СИСТЕМ

**БАРАШКО Елена Николаевна**

старший преподаватель

**ГАМАЮНОВ Дмитрий Владимирович**

студент

**ВЕРЕСКЛЯ Владислав Игоревич**

студент

ФГБОУ ВО «Донской государственный технический университет»  
г. Ростов-на-Дону, Ростовская область, Россия

*В данной статье предоставлены некоторые из передовых технологий голосовой биометрии, приведены сравнения основных ведущих технологий. Указана разница между текстозависимой и текстонезависимой технологиями. Уточнены многие термины связанные с голосовой биометрией.*

**Ключевые слова:** голосовая биометрия, текстозависимая, текстонезависимая, FAR, FRR, биометрические технологии.

**Б**иометрическая идентификация может решить проблему безопасности данных. Главным преимуществом использования биометрической идентификации вместо ряда паролей является низкий риск утери, кражи, взлома или подделки «ключа». Они также более устойчивы к публичным манипуляциям.

Рассмотрим одну из самых востребованных на сегодняшний день технологий идентификации личности – голосовую биометрию, измеряющую голос человека. Она незаменима для удаленного обслуживания клиентов, когда главным средством взаимодействия является голос, в первую очередь в автоматических голосовых меню и контакт-центрах.

Преимущества голосовой биометрии:

- никаких специальных сканеров не требуется – только обычный микрофон в телефоне или диктофон;

- не нужны специальные устройства – можно использовать любой диктофон (аналоговый или цифровой), мобильный или стационарный телефон (не менее 80 годов выпуска);

- никаких специальных навыков от пользователя не требуется.

Типы голосовой биометрии (аутентификации):

1. **Текстонезависимая** – определение личности клиента в условиях свободы слова не требует произнесения каких-либо специальных слов и выражений. Например, человек должен только произнести фразу или обсудить с оператором контакт-центра цель своего звонка.

2. **Текстозависимая** – для определения личности человека необходимо произнести строго определенную фразу. Этот тип голосовой биометрии делится на два типа:

**Текстовая аутентификация по статической парольной фразе.** Чтобы проверить вашу личность, вы должны сказать ту же фразу, которая была использована для регистрации голоса человека в системе.

**Текстовая аутентификация по динамической парольной фразе** – для проверки личности человека предлагается произнести фразу, состоящую из набора слов, произнесенных этим человеком при регистрации голоса в системе. Преимущество динамической парольной фразы от статического заключается в том, что каждый раз фраза меняется, что усложняет мошенничество с использованием голосовой записи человека (например, на диктофоне). Проблема технологии – некоторые люди не могут произносить звуки, голос может меняться из-за болезни и возраста. Кроме того, на точность аутентификации влияет шумовая обстановка вокруг человека (шум, реверберация).

VoiceKey.PLATFORM – это мультифункциональная биометрическая платформа для аутентификации при дистанционном обслуживании. В состав платформы входят следующие решения: VoiceKey.AGENT, VoiceKey.IVR, VoiceKey.-ONEPASS, Voice-Key.FRAUD.

В биометрии существуют наиболее устойчивые понятия – FAR(ошибочная скорость приема) и FRR(ошибочная скорость отбраковки). Первое

число указывает на вероятность ложного совпадения биометрических характеристик двух людей. Второе – возможность отказа в доступе лицу, имеющему доступ. Чем лучше система, тем

меньше значение FRR при тех же значениях FAR. Иногда используется сравнительная характеристика EER, определяющая точку пересечения FRR и дальних графов.

Таблица 1

### СРАВНЕНИЕ ТЕХНОЛОГИЙ ГОЛОСОВОЙ БИОМЕТРИИ

Название технологии	Условия тестирования	FRR %	FAR %
VoiceKey AGENT	Текстозависимое распознавание	2	1,0
VoiceKey.IVR	Текстозависимое распознавание	1	0,3
VoiceKey.FRAUD	Текстонезависимое распознавание	3	1,4
VoiceKey.OnePass	Текстозависимое распознавание	0.5	0.2

**Текстонезависимая аутентификация** – подтверждение личности происходит по спонтанной речи клиента, т. е. нам не важно, что говорит человек. Это самый долгий метод подтверждения – чистой речи абонента должно накопиться минимум 6-8 сек. Обычно этот способ применяется непосредственно во время общения абонента с оператором контактного центра, когда последнему нужно однозначно удостовериться, что абонент именно тот, за кого себя выдает.

Для верификации или аутентификации в текстонезависимых системах может использоваться практически любой фрагмент свободной звучащей речи достаточной длины, что делает их удобными с точки зрения пользователя. Такие системы незаменимы при решении полицейских задач: скрытая идентификация, криминалистическая идентификация, фоноучеты. Тем не менее, эта возможность усложняет реализацию текстонезависимых систем, понижает их надежность и скорость распознавания.

Для проведения текстонезависимой идентификации существует два подхода. Первый заключается в том, что по акустическим признакам речевого сигнала для каждого диктора строятся статистические модели. Идентификация в данном случае представляет собой вычисление отклонения случайного вектора от модельных распределений и

принятие решений происходит с заданным порогом допуска. Второй подход основан на создании в рамках одной системы гендеро- и каналозависимых подсистем, функционирующих на отдельных наборах речевых признаков.

Подводя итоги, можно сказать, что текстозависимая архитектура более надежна в наше время, чем та же текстонезависимая, основными причинами такого вывода являются показатели FRR и FAR.

Тестирование показало, что самой надежной технологией на 2018 г. является технология VoiceKey.ONEPASS, главными преимуществами которой являются:

- решение VoiceKey.ONEPASS позволит пользователю максимально быстро и безопасно авторизоваться в любом мобильном приложении;

- нет необходимости держать в голове огромное количество паролей и идентификаторов. Образцы голоса и лица, которые требуются для подтверждения личности пользователя, можно легко получить, используя камеру и микрофон практически любого современного телефона;

- VoiceKey.ONEPASS за несколько секунд сфотографирует, запишет голос и произведет верификацию личности пользователя без необходимости для него совершать какие-либо дополнительные действия.

### СПИСОК ЛИТЕРАТУРЫ

1. Дунаев Д.Ю. Кратко о биометрических технологиях. – URL: <http://sec4all.net/modules/myarticles/article.php?storyid=149/>.
2. Ивантер Э.В. Коросов А.В. Элементарная биометрия. – Петрозаводск: Изд-во ПетрГУ, 2010. – 104 с.
3. Исавев С. Речевые технологии. Голосовая биометрия для чайников на примере работы в контактном центре. – URL: <https://habr.com/ru/company/speechpro/blog/205880/>.

## VOICE BIOMETRY ANALYSIS OF IDENTIFICATION SYSTEMS

**BARASHKO Elena Nikolaevna**  
Senior Lecturer  
**GAMAYUNOV Dmitry Vladimirovich**  
student  
**VERESKLA Vladislav Igorevich**  
student  
Don State Technical University  
Rostov-on-Don, Rostov Region, Russia

*This article provides some of the advanced technologies of voice biometrics, provides a comparison of the main leading technologies. The difference between text-dependent and text-independent technologies is indicated. Clarified many terms related to voice biometry.*

**Keywords:** voice biometrics, text-dependent, text-independent, FAR, FRR, biometric technology.

## НОВЫЕ СИСТЕМЫ ПОИСКА И РАСПОЗНАВАНИЯ ЛИЦ

**БАРАШКО Елена Николаевна**  
старший преподаватель кафедры «Информационные технологии»  
**КРУЖИЛИН Кирилл Дмитриевич**  
студент  
ФГБОУ ВО «Донской государственный технический университет»  
г. Ростов-на-Дону, Ростовская область, Россия

*Раскрытие понятия распознавания лиц, описание современных технологий, основанных на 2 основных способах распознавания, сравнительная характеристика и выявление лучшего программного обеспечения.*

**Ключевые слова:** распознавание лиц, FaceID, DeepFace, FaceNet, технология, программа.

**И**нформационные системы поиска и распознавания применяются в различных сферах жизнедеятельности человека. Распознавание лиц – это автоматическая локализация человеческого лица на изображении или видео и, при необходимости, идентификация личности человека на основе имеющихся баз данных.

Существуют два способа распознавания лиц:

- геометрическое сравнение;
- эталонное сравнение.

*Геометрическое сравнение* основано на определении элементов лица, таких как: глаза, нос, рот, подбородок и др. Лицо может быть распознано, даже когда индивидуальные черты видны недостаточно. Идея подхода заключается в нахождении относительного положения и собственных характеристик отдельных элементов лица. К настоящему моменту были разработаны такие программы, которые способны запоминать положения маленьких черт, что способствует ментальному точному распознаванию.

**Эталонное сравнение** подразумевает под со-

бой построение изображения в виде массива байтов – величин интенсивности и сравнивается в подходящей метрике с эталоном – целым лицом.

К 1993 г. было заявлено о существовании нескольких алгоритмов, правильно решающих задачу поиска и распознавания лиц в среде с минимальным числом ограничений.

Одним из главных примеров данной технологии является функция *FaceID*, созданная и разработанная Apple для iPhone и iPad Pro в 2017 г. Система позволяет использовать биометрическую аутентификацию для разблокировки устройства, осуществления платежей и доступа к конфиденциальным данным, а также обеспечивает подробное отслеживание выражений лица для Animoji и других функций.

Специально разработанная камера True-Depth сравнивает лицо пользователя с картинкой, хранящейся в памяти айфона. Она создает 3D-снимок вашего лица, а при входе в систему сверяет лицо со снимком. Проектор точек проецирует на ваше лицо 30 тысяч невидимых инфракрасных точек, а инфра-