VOICEKEY.PLATFORM

ЦРТ инновации

САНКТ-ПЕТЕРБУРГ
+7 (812) 325-88-48
stc-spb@speechpro.com

МОСКВА
+7 (495) 669-74-40
stc-msk@speechpro.com

WWW.SPEECHPRO.RU

О ПРОДУКТЕ

VoiceKey.PLATFORM — это программный комплекс мультимодальной биометрической аутентификации. Программный комплекс представляет собой технологическую платформу управления нагрузкой, поступающей в виде звука или фото, маршрутизацию к обработчикам данных, мониторингу состояния, хранения и защиты данных.

Принципы построения комплекса:

- Мультимодальность. Биометрическая аутентификация по голосу и лицу. Регистрация голосового и лицевого образца через мобильное приложение. Верификация в контакт центре, IVR системе, мобильном приложении или при общении с виртуальным ассистентом.
- Liveness. Обеспечение защиты от подделки биометрических образцов лица или подмены диктора.
- Выявление аномалий. Определяет мошенников и усиливает системы защиты от фрода.
- Безопасность данных. Обеспечена высоким уровнем защиты персональных данных.

Применение комплекса

VoiceKey.PLATFORM находит широкое применение в различных сферах, в том числе:

- в сфере предоставления услуг при построении систем голосового дистанционного обслуживания в контактных центрах, интерактивных сервисах и виртуальных ассистентах с голосовым управлением;
- в сфере финансов, межведомственного электронного взаимодействия, банковской сфере, телекоме и предоставления государственных услуг, в корпоративных информационных системах;
- в системах паспортного и визового контроля, в системах оказания государственных дистанционных услуг;
- в облачных решениях и системах национального уровня;
- в службах безопасности финансовых, телекоммуникационных и других организаций.

БИОМЕТРИЧЕСКИЕ ТЕХНОЛОГИИ

Голосовая биометрия

Голосовая биометрия («отпечаток» голоса) — это совокупность методов автоматической идентификации человека и подтверждения личности, основанных на признаках его собственного голоса. Частотные характеристики колебаний голосовых связок и спектральная структура речи помогают создать индивидуальную модель голоса, способную отразить даже диалект и ритмику речи диктора.

Технологии голосовой биометрии отличаются высокой степенью надёжности: невозможно взломать защиту методами социальной инженерии. Живой диалог с оператором гарантирует защиту от взлома через запись. Пока клиент объясняет цель своего звонка, система голосовой биометрии уже сможет верифицировать его. Кроме того, в отличие от паспортов, паролей, шифров и прочих традиционных способов подтверждения личности, характеристики голоса невозможно потерять, передать другому лицу, забыть, украсть или подделать.

Комплекс **VoiceKey.PLATFORM** применяет голосовую биометрию для различных задач:

- верификация при обращении в контакт-центр;
- верификация при обращении в IVR;
- идентификация пользователя по Чёрным и Белым спискам.

Сама технология имеет ряд преимуществ:

- Биометрическая проверка по голосу более надёжна, чем проверка человеком. В основе технологии ЦРТ лежат современные подходы на базе глубоких нейронных сетей (DNN) и CX-векторов.
- Безопасная верификация позволяет расширить набор предлагаемых через контакт-центр сервисов и привлечь новых клиентов.
- Регистрация биометрических образцов и последующая голосовая верификация осуществляются на основе свободного общения в фоновом режиме. Не требуется произносить специальные фразы или отвечать на вопросы.
- Биометрический шаблон можно построить для речи на любом языке, что позволяет использовать его во всем мире.
- Биометрическая система хранит не фотографии и записи голоса, а биометрические модели. Восстановить исходные фото или записи по моделям невозможно.

Для наиболее эффективной работы технологии голосовой биометрии следует соблюдать некоторые условия:

- Низкий уровень фонового шума;
- Один говорящий на аудиозаписи;
- Отсутствие технических помех устройства передачи звука.

Лицевая биометрия

Лицевая биометрия — это измерение и сравнение уникальных характеристик изображения лица человека.

Лицо — это также уникальный биометрический параметр человека. Как и другие параметры, лицо нельзя потерять, украсть или подделать. При этом использовать лицо для подтверждения личности — удобно и просто, для этого не требуется использование какого-то специализированного оборудования, и обладания специальными навыками.

В **VoiceKey.PLATFORM** лицевая биометрия используется для различных задач:

- идентификация пользователя по Чёрным и Белым спискам;
- верификация пользователя;
- определение живого пользователя по фото и видео.

Для достижение максимальных показателей точности в работе технологий, использующих лицевую биометрию, необходимо соблюдать требования к изображению лица:

- Положение головы на фото;
- Отсутствие тёмных очков;
- Лицо не должно быть закрыто волосами (допускается закрывать лоб);
- Выражение лица нейтральное;
- Лицо должно быть равномерно освещено, без бликов и теней.

Бимодальная биометрия

В **VoiceKey.PLATFORM** реализована технология бимодальной биометрии, которая заключается в одновременном использовании образцов голоса и изображения лица при построении биометрического шаблона человека.

Бимодальная биометрия обладает рядом значительных преимуществ, которые открывают широкие возможности применения этой технологии в массовом сегменте дистанционного обслуживания:

- голос и лицо — это уникальные биометрические идентификаторы человека, которые невозможно потерять, украсть или подделать;

- биометрическая защита более эффективна в сравнении с использованием паролей, PIN-кодов, смарт-карт и прочее, так как позволяет идентифицировать конкретного человека, а не устройство;
- одновременное использование образцов голоса и лица повышает точность аутентификации пользователя;
- для получения биометрического образца голоса или лица не требуется специальных устройств – достаточно только микрофона и камеры на компьютере или в смартфоне;
- пользователям не требуются специальные навыки и умения – технология бимодальной биометрии интуитивно понятна и проста в использовании;
- бимодальная биометрия — это новейшая, совершенствующаяся технология, вобравшая в себя все современные научные разработки в области распознавания лиц и речи.

Antispoofing

Antispoofing — подсистема, детектирующая спуфинг-атаки.

Спуфинг-атака — попытка взлома голосовых биометрических систем, основанная на активных попытках фальсификации голосовых характеристик с целью получения несанкционированного доступа к защищаемой информации.

Примерами таких атак могут служить случаи, когда злоумышленник подаёт на вход синтезированный голос или создаёт аудиозапись из нарезанных фрагментов речи человека, за которого хочет себя выдать, или умышленно обрабатывает чей-либо или свой голос, изменяя цифровую запись.

Различают четыре вида спуфинг-атак:

- имперсонализация;
- повторное воспроизведение;
- преобразование речи;
- синтез речи.

Для обнаружения спуфинг-атак используется специализированный модуль. Основу модуля обнаружения составляет обученная и реализованная глубокая нейронная сеть. Модуль на вход получает фонограмму, а на выходе выдаёт единственное значение в диапазоне от 0 до 100.

Liveness

Компонент лицевого антиспуфинга предоставляет возможность анализировать изображения для поиска признаков наличия спуфинг-атак — злонамеренных попыток фальсифицировать данные, чтобы лицевой шаблон, созданный из этих фальсифицированных данных, был похож на лицевой шаблон какого-либо другого человека, что позволило бы злоумышленнику использовать этот лицевой шаблон для успешного прохождения верификации.

Во время проверки на liveness («живость») система определяет, взаимодействует ли она с «реальным» человеком или мошенником, использующим поддельный идентификатор: фотографию или видео лица, реалистичную маску.

Базовые процессы применения биометрии

Независимо от сценария применения, биометрическое распознавание включает несколько основных этапов.

- **Биометрическая регистрация**

Как в любой системе, обеспечивающей безопасность доступа, пользователю необходимо зарегистрироваться. В **VoiceKey.PLATFORM** пользователь должен оставить образцы своего голоса и/или лица. На основе биометрического образца система создает голосовой или лицевой шаблон пользователя и сохраняет его в базе данных.

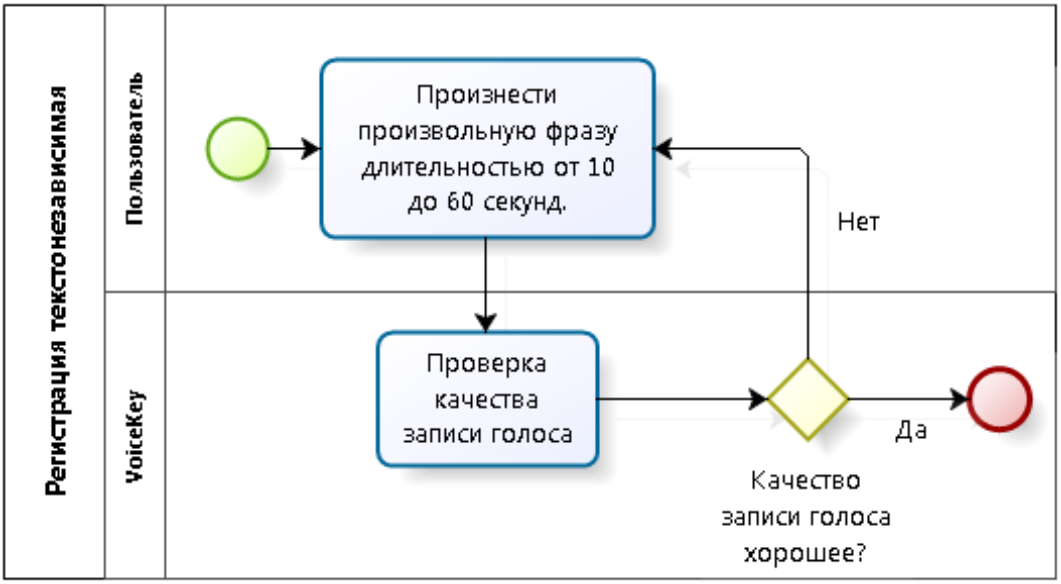
Для построения голосового шаблона требуется собрать 30 секунд чистой речи пользователя. Понятие «чистая речь» подразумевает речевые участки, содержащие биометрически значимую информацию, и пригодные для построения голосовых биометрических моделей. Данные речевые участки НЕ включают: акустические дефекты (щелчки, гудки, перегрузы, тональные помехи и т.п.), паузы (перерывы в речи), паралингвистические элементы (смех, кашель, вздох и т.п.), участки с низким соотношением сигнал-шум, оглушенные речевые участки (с преобладанием глухих согласных и оглушенных гласных).

Биометрические контрольные шаблоны (БКШ) содержатся в хранилище биометрических данных и связываются с идентификаторами пользователей в информационной системе заказчика. Позднее, при верификации или идентификации, именно с этими шаблонами будут сравниваться вновь предоставленные образцы голоса и лица пользователя.

В процессе создания голосового шаблона предусмотрены следующие возможности:

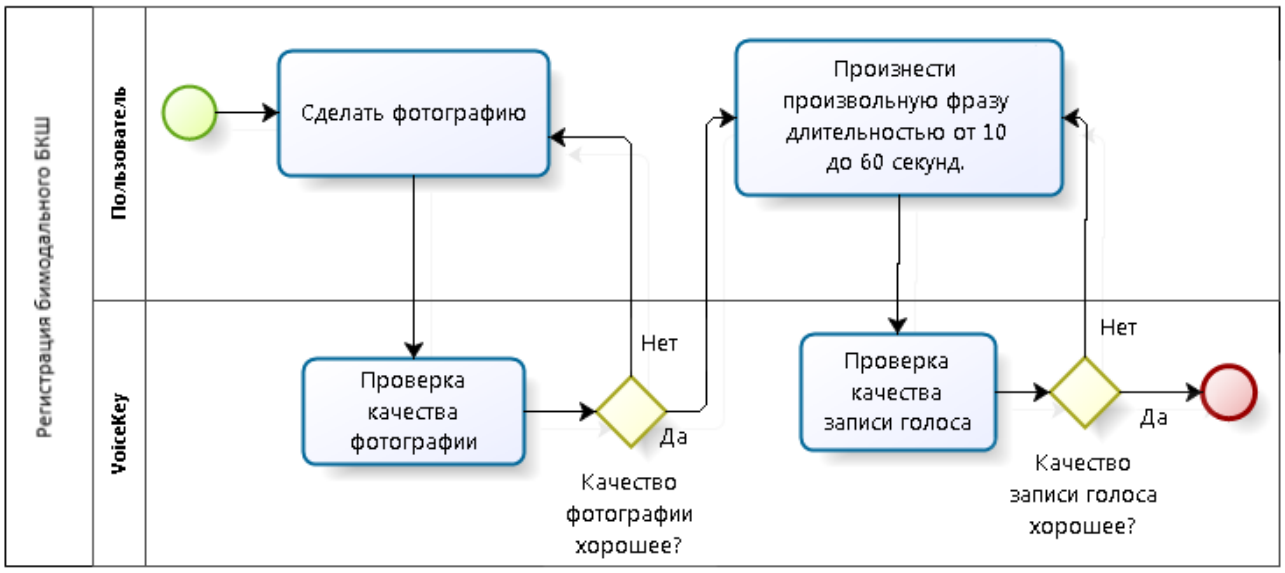
- Текстонезависимый голосовой шаблон

Текстонезависимый шаблон строится на основе записи голоса пользователя при произнесении им произвольного текста. Длительность записи свободной речи составляет не менее 10 и не более 60 секунд.



- Бимодальный биометрический шаблон

Для бимодальной биометрии последовательно создается лицевой шаблон пользователя по фотографии с изображением лица и голосовой шаблон пользователя с фонограммой.



Верификация пользователя

Верификация — это процедура подтверждения личности пользователя.

При биометрической верификации происходит сравнение биометрического контрольного шаблона, созданного при регистрации, с биометрическим шаблоном (БШ), который строится непосредственно в процессе верификации. В результате система выдает показатель схожести эталона и кандидата, на основе которого пользователю предоставляется или запрещается доступ для выполнения дальнейших действий.

Модуль голосовой верификации пользователей предусматривает следующие варианты:

- **Текстонезависимая верификация пользователя**. При текстонезависимой верификации сравнивается голосовой шаблон, построенный по свободной речи пользователя длительностью не менее 3 и не более 60 секунд, с текстонезависимым голосовым шаблоном пользователя, созданным при регистрации и хранящимся в базе данных системы.
- **Верификация пользователей по фотографии**. При верификации пользователь записывает видео, из которого произвольным образом выбирается кадр с изображением его лица. Лицевой шаблон, построенный по данному кадру, сравнивается с биометрическим контрольным шаблоном лица пользователя, созданным при регистрации биометрических данных пользователя в системе.
- **Мультимодальная верификация**. В различных сценариях биометрическая оценка может осуществляться отдельно по каждому из доступных биометрических методов (голосовая или лицевая биометрия) или формироваться одновременно по нескольким биометрическим методам (голосовая и лицевая биометрия).

- **Идентификация пользователя**

Идентификация — это процедура определения личности пользователя.

В процессе биометрической идентификации происходит сопоставление голосового и/или лицевого шаблона пользователя с массивом БКШ, хранящихся в базе данных системы.

- **Текстонезависимая биометрия**. Пользователь свободно общается с оператором контакт-центра или виртуальным ассистентом в системе самообслуживания. Система сравнивает голос пользователя с хранящимися в базе данных голосовыми шаблонами в «чёрных» или «белых» списках и определяет наиболее похожие.
- **Фотобиометрия**. Система делает фотографию пользователя с доступного устройства (камера на смартфоне, веб-камера на ноутбуке или ПК), сравнивает со всеми биометрическими шаблонами лиц из базы данных и определяет наиболее похожие.

Результатом идентификации является список пользователей, для которых показатель схожести биометрических контрольных шаблонов и биометрических шаблонов, построенный в процессе идентификации, превышает установленный порог.

Идентификацию на базе **VoiceKey.PLATFORM** рекомендуется применять для задач обнаружения мошенников при удалённом обслуживании клиентов.

- **Адаптация биометрического контрольного шаблона**

Для поддержания биометрических образцов голоса и лица в актуальном состоянии, с учётом естественного старения организма, особенностей канала и других факторов, **VoiceKey.PLATFORM** предоставляет возможность адаптации (обогащения) биометрического контрольного шаблона.

Адаптация БКШ происходит после успешного прохождения пользователем процесса верификации. Созданный на этапе верификации голосовой или лицевой шаблон объединяется с уже имеющимся контрольным шаблоном пользователя и сохраняется в базе данных.

Надежность применения биометрии

Надежность алгоритмов биометрии определяется двумя ключевыми понятиями:

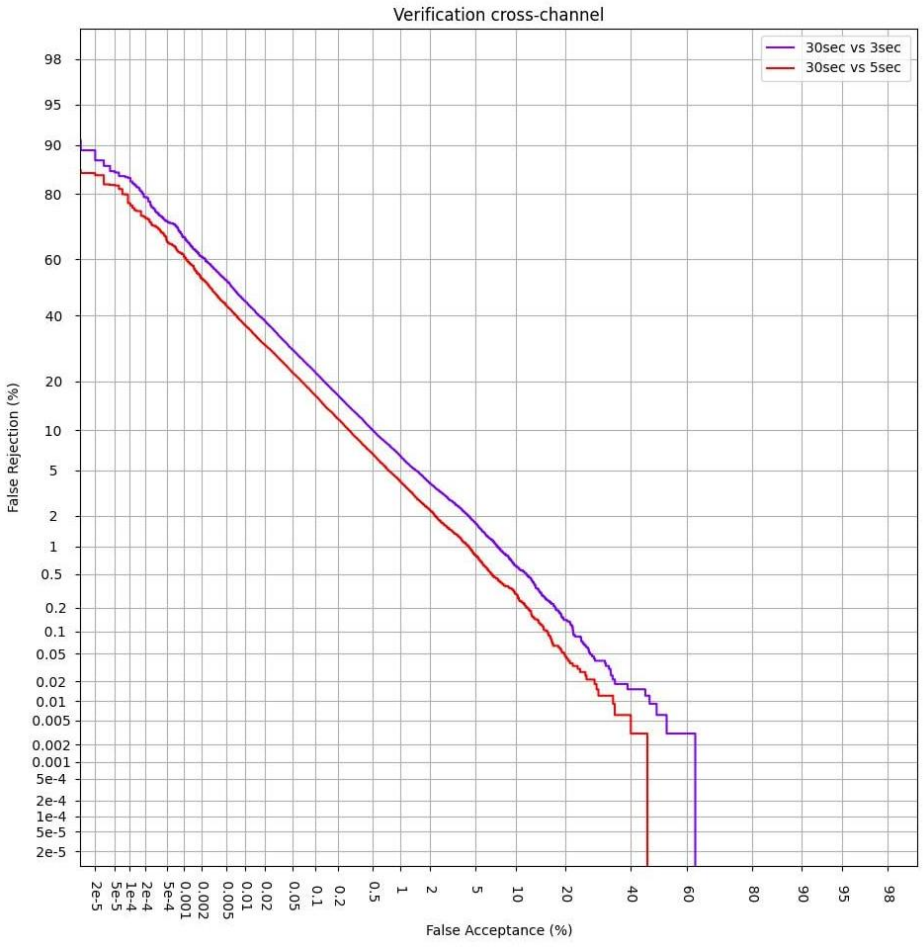
- ошибка ложного недопуска (False Rejection Rate, FRR) — вероятность отклонить зарегистрированного клиента;
- ошибка ложного допуска (False Acceptance Rate, FAR) — вероятность принять постороннего человека за клиента.

Для оценки точности биометрических систем принято использовать характеристические кривые, которые устанавливают зависимость между FRR и FAR.

Ниже приведены графики для различных сценариев применения биометрии.

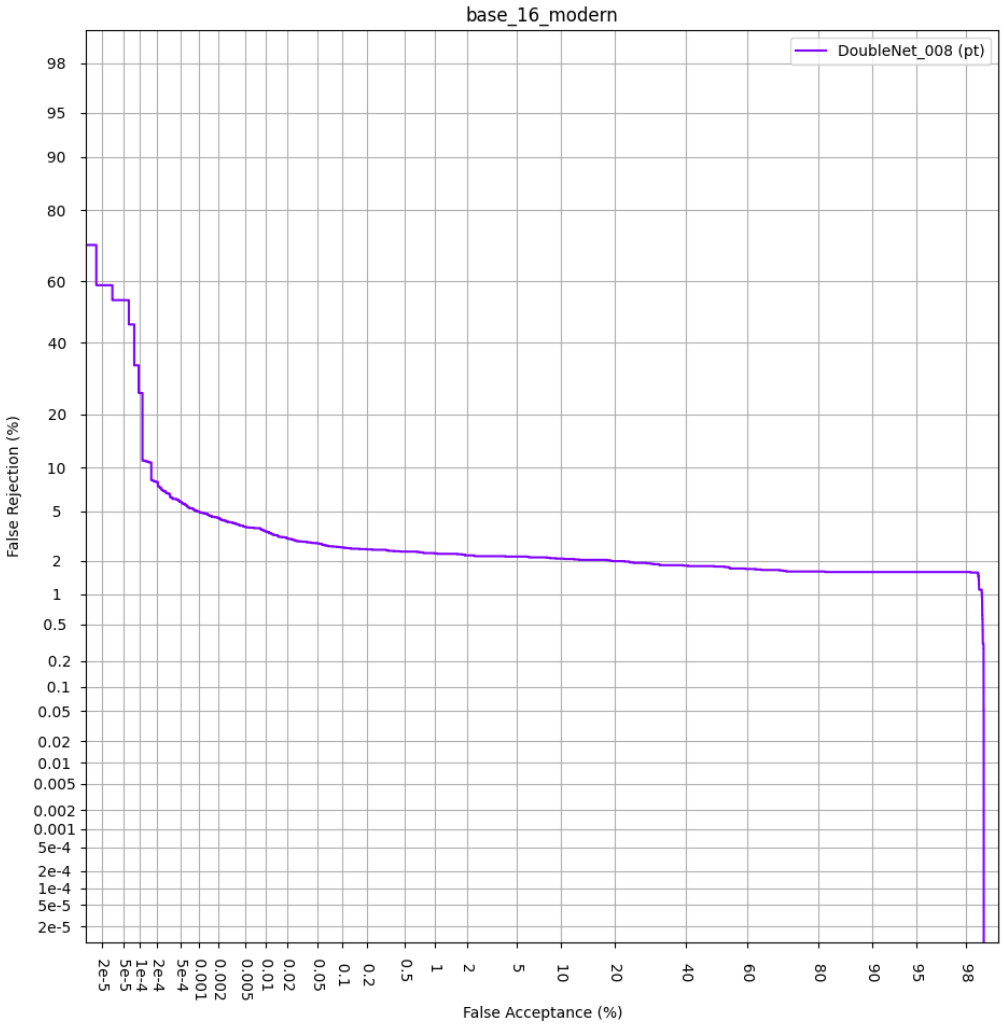
- **Текстонезависимая голосовая биометрия**

График качества голосовой биометрии для gen6_v5 для регистрации 30 секунд чистой речи против 5 и 3 секунд чистой речи для верификации.

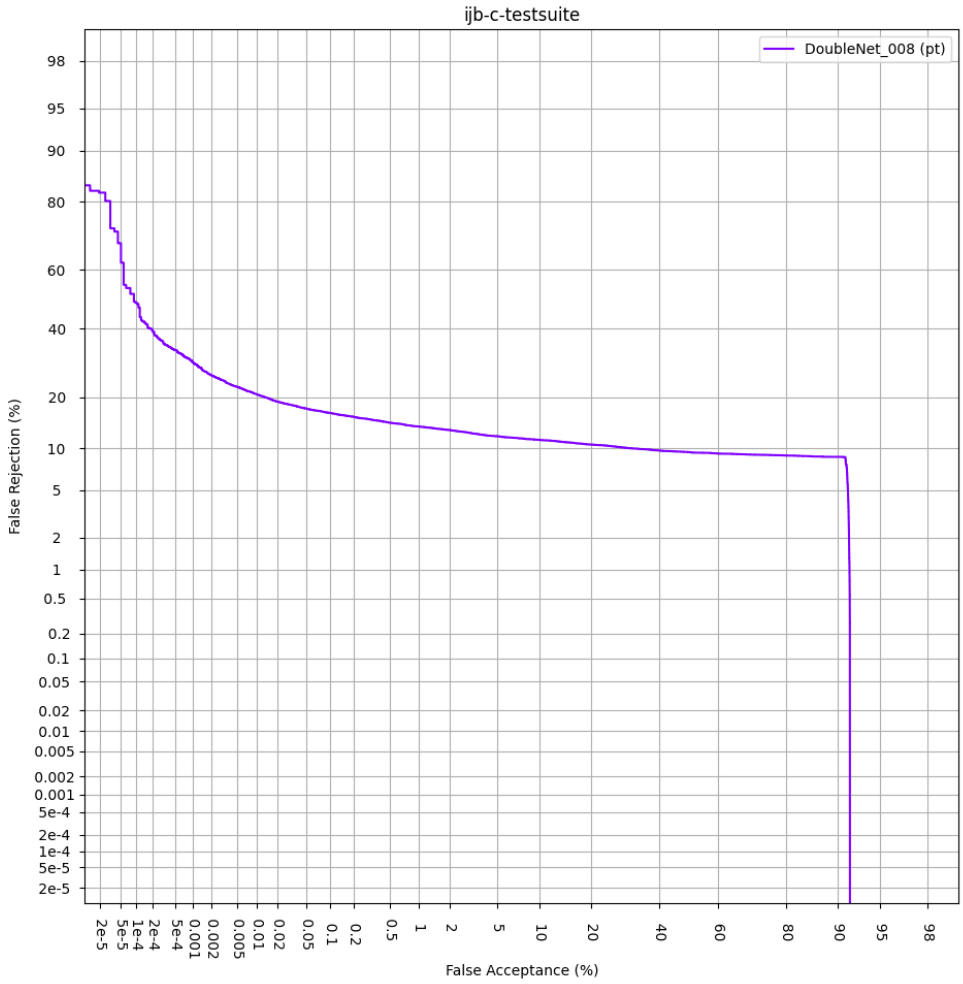


Лицевая биометрия

Графики качества Face SDK для алгоритма DoubleNet_008 в сценарии mugshot (на базах base_16) и в сценарии wild (база IJB-C).



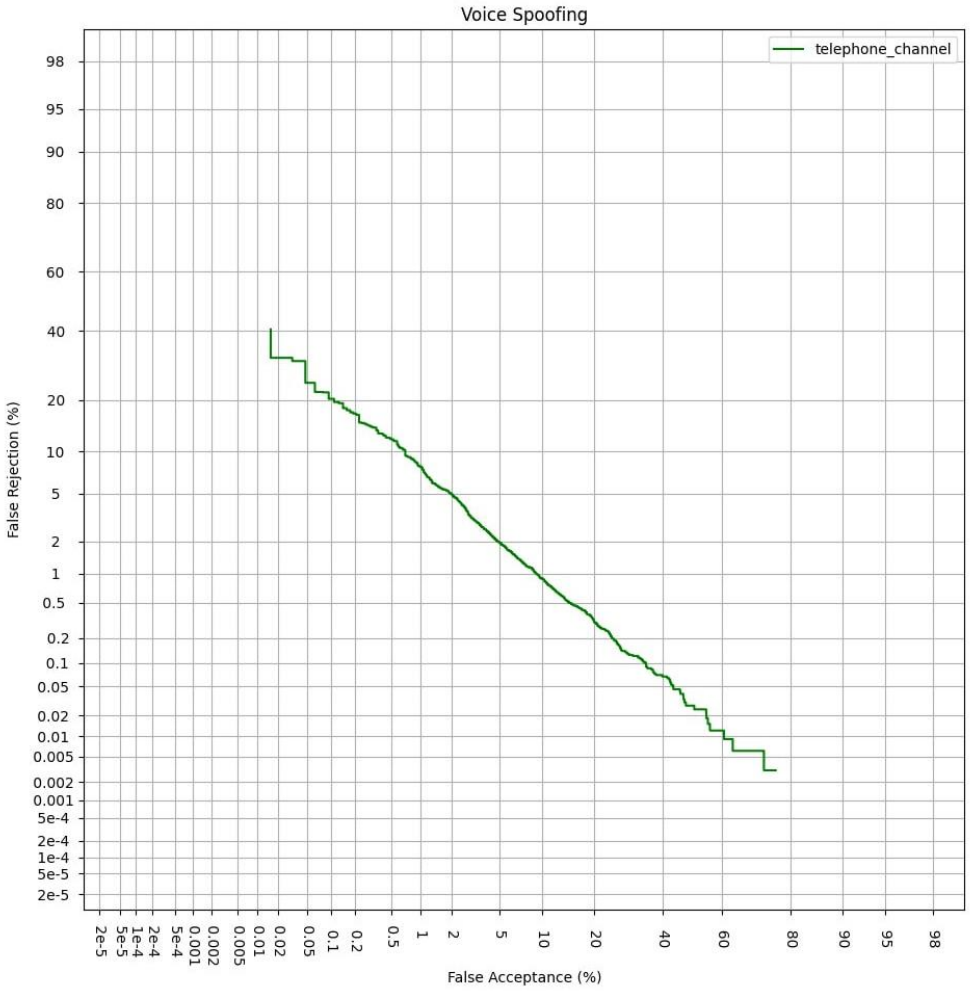
Сценарий mugshot применяется для фотографий, соответствующих требованиям полного фронтального типа. Данный тип изображения включает целиком голову (как правило, с волосами), шею и плечи. Данный тип изображения лица предназначен для долговременного хранения информации об изображении лица; его используют в качестве фотографии для паспорта, водительского удостоверения и т.д.).



Сценарий wild, в свою очередь, применяется для фотографий различного расширения, как правило, на таких изображениях присутствует только голова, положение и поворот головы имеет широкие диапазоны, также допускается частичное перекрытие лица волосами, руками. Данные изображения могут быть получены в фотожурналистских целях, с камер видеонаблюдения.

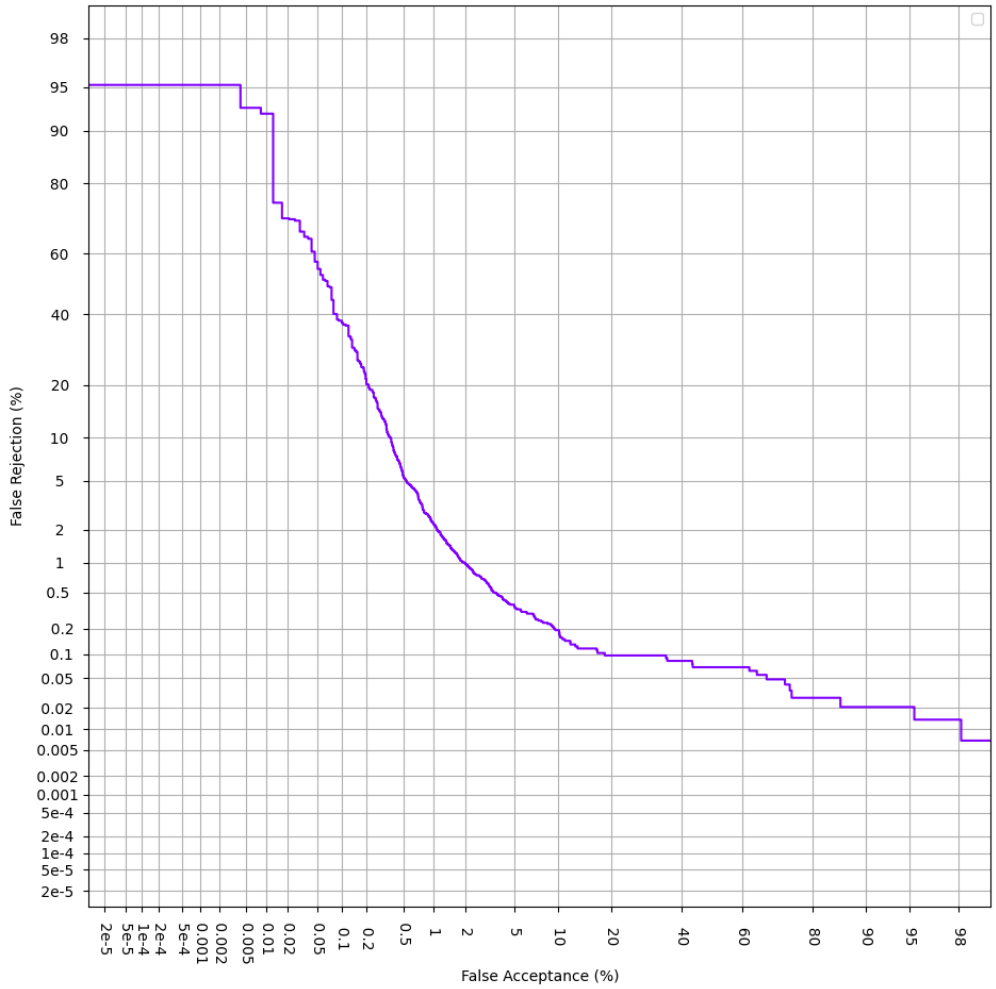
Голосовой антиспуфинг

График качества технологии Voice Antispoofing для 5 секунд чистой речи.



Лицевой антиспуффинг (liveness)

График качества технологии Face Liveness при проверке изображения лица, полученного с камеры смартфона, веб-камеры.



Производительные характеристики

▸ Лицевая биометрия

В таблице ниже приведены производительные характеристики* на 2 процессорах Intel® Xeon CPU E5-2620 v4.

	Время, мс
Создание модели	305
Сравнение 1 к 1	0,077
Сравнение 1 к 1000	0,786
Сравнение 1 к 10 000	1,69
Сравнение 1 к 100 000	22,79

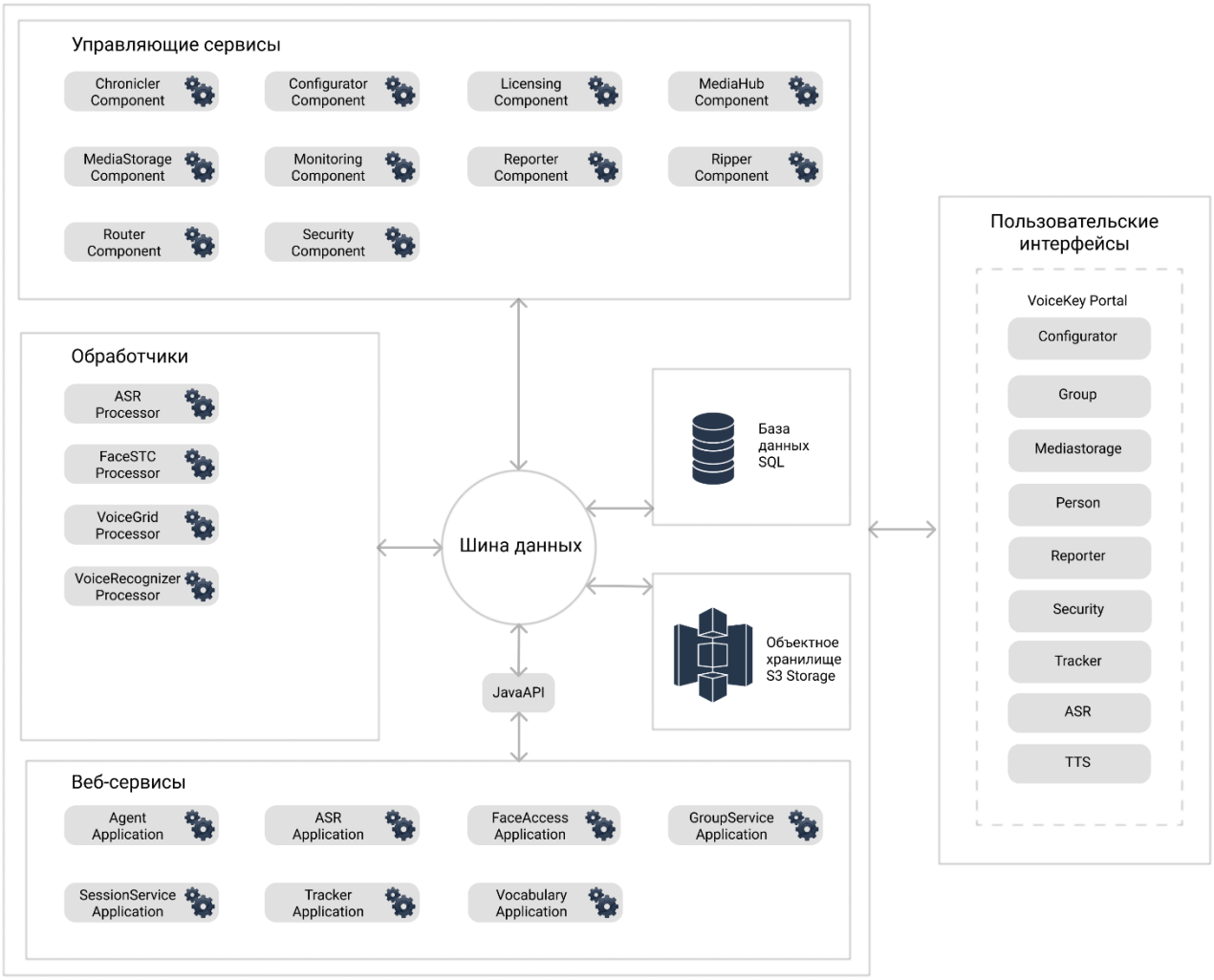
▸ Текстонезависимая биометрия

В таблице ниже приведены производительные характеристики* на 1-м ядре процессора Intel® Xeon® CPU E5-2683 v4 2.1 GHz.

	Время, с
Создание модели (из аудиозаписи длительностью 60 с)	1
Сравнение 1 к 1	0,04
Сравнение 1 к 1000	40
Сравнение 1 к 10 000	400

* Испытание производительных характеристик производилось в лабораторных условиях без учёта нагрузки стороннего ПО на систему.

АРХИТЕКТУРА VOICEKEY.PLATFORM



Комплекс **VoiceKey.PLATFORM** имеет двухуровневую архитектуру.

Базовым уровнем комплекса является технологическая платформа, в состав которой входят:

- сервисы,
- обработчики,
- хранилище данных.

Сервисы обрабатывают запросы, поступающие от веб-сервисов, распределяют их между обработчиками и управляют передачей сообщений между компонентами.

Обработчики обеспечивают выполнение поступивших в технологическую платформу запросов.

Хранилище данных состоит из двух сегментов: хранилище биометрических данных и хранилище медиаданных. Хранилище биометрических данных используется для регистрации, хранения биометрических контрольных шаблонов персон. Хранилище медиаданных используется для сохранения исходных, использовавшихся для построения биометрических шаблонов, аудиозаписей и фотографий.

Информационное взаимодействие компонентов технологической платформы обеспечивает **шина данных**.

Прикладной уровень комплекса представлен набором отдельных программных решений, использующих функциональность технологической платформы для решения специфических задач. Каждое программное решение реализовано в виде веб-сервиса, предоставляющего прикладной программный интерфейс, выполненный в стиле архитектуры **REST**.

Взаимодействие веб-сервисов с технологической платформой осуществляется через программный интерфейс на языке **Java**.

В соответствии с требованиями к производительности и резервированию, модули комплекса могут устанавливаться на одном или нескольких серверах. Поддерживается работа как на физических, так и виртуальных серверах.

Комплекс **VoiceKey.PLATFORM** состоит из следующих модулей:

Управляющие сервисы

- **Chronicler Component** — компонент журналирования. Регистрирует события, возникающие в ходе работы компонентов программного комплекса **VoiceKey.PLATFORM**.
- **Configurator Component** — компонент конфигурации. Реализует функцию централизованного управления конфигурациями всех входящих в состав **VoiceKey.PLATFORM** компонентов.
- **Licensing Component** — менеджер лицензий. Реализует функцию универсального провайдера лицензий, который может работать как на основе HASP, так и на основе других потенциальных средств лицензирования.

  Менеджер лицензий обеспечивает централизованное хранение информации о приобретённых лицензиях и предоставление сведений о наличии или отсутствии лицензии на использование заданного сервиса.
- **MediaHub Component** — медиаконцентратор. Реализует функцию коммуникации внешнего источника медиаданных и целевых операционных сервисов для решения поставленной задачи
- **MediaStorage Component** — хранилище медиаданных, полученных во время регистрации клиентов.
- **Monitoring Component** — менеджер мониторинга. Реализует систему технологического мониторинга компонентов комплекса VoiceKey.PLATFORM.

  Monitoring Component регистрирует компоненты в системе мониторинга и собирает данные о технологическом состоянии компонентов комплекса.
- **Reporter Component** — компонент формирования отчётности. Отвечает за формирование отчётов по данным, собираемым в журналы регистрации событий в ходе функционирования программного комплекса.
- **Ripper Component** — модуль обработки медиаданных. Обеспечивает первичную обработку поступающих медиаданных:
  - извлечение звуковой дорожки из видеофайла;
  - перекодирование/передискретизация звука;
  - разбиение видеоряда на определённые кадры.
- **Router Component** — компонент маршрутизации. Управляет маршрутизацией сообщений между компонентами комплекса.
- **Security Component** — подсистема разграничения доступа. Реализует централизованное управление разграничением прав доступа пользователей к ресурсам VoiceKey.PLATFORM.

Веб-сервисы

- **Agent Application**: реализация программного решения **VoiceKey.AGENT**.
- **ASR Application**: реализация программного решения **VoiceKey.ASR**.
- **FaceAccess Application**: проверка живого пользователя.
- **GroupService Application**: управление группами персон.
- **SessionService Application**: управление сессиями.
- **Tracker Application**: реализация программного решения **VoiceKey.TRACKER**.
- **Vocabulary Application**: добавление словарей и отдельных слов для распознавания.

Обработчики запросов

- **ASR Processor** – обработчик запросов на распознавание речи. Реализует преобразование речи в текст.
- **FaseSTC Processor** — обработчик запросов верификации по изображению лица. Реализует проверку личности пользователя по фотографии и предоставляет функциональность определения живого пользователя по фото и видео.
- **VoiceGrid Processor** — обработчик запросов текстонезависимой верификации по голосу. Реализует проверку личности клиента по свободной речи, независимо от произносимых фраз.
- **VoiceRecognizer Processor** — обработчик запросов на распознавание речи. Реализует преобразование речи, используя технологию распознавания речи.

Шина данных

Компонент реализован на базе связующего программного обеспечения **RabbitMQ** и обеспечивает возможность организации асинхронной передачи потоков сообщений между подсистемами. Шина данных предоставляет возможность подписки на получение сообщений и гарантированной доставки сообщений от отправителя получателю.

Веб-интерфейсы

- **VoiceKey Portal** — пользовательский интерфейс для: Configurator Component, GroupService Application, MediaStorage Component, Reporter Component, Security Component, Tracker Application, Vocabulary Application.

Программные компоненты

Java API — интерфейс программирования на языке Java, через который **VoiceKey.PLATFORM** принимает запросы от прикладных систем (VoiceKey.AGENT и др.).

Комплекс **VoiceKey.PLATFORM** работает в пассивном режиме, то есть осуществляет какие-либо действия, включая приём аудиофайлов, видеофайлов, фотографий, их обработку, построение и сравнение биометрических шаблонов, только после получения соответствующего запроса от прикладной системы.

На базе **VoiceKey.PLATFORM** реализованы следующие программные решения:

- **VoiceKey.AGENT** позволяет верифицировать звонящего по голосу непосредственно во время разговора с оператором. Голос клиента сравнивается с его голосовым контрольным шаблоном, хранящимся в базе данных системы.
- **VoiceKey.ASR** обеспечивает встраивание возможностей распознавания речи в программное обеспечение, онлайн-сервисы, мобильные приложения и другие продукты. Позволяет преобразовать речь в текст с использованием технологий распознавания речи.
- **VoiceKey.FaceAccess** служит для встраивания возможностей проверки на живость в программное обеспечение, онлайн-сервисы, мобильные приложения и другие продукты.
- **VoiceKey.TRACKER** обеспечивает идентификацию по изображению лица и/или образцу голоса. Выполняет поиск и сравнение лиц по массивам фотографий и/или голосов по массивам аудиозаписей.

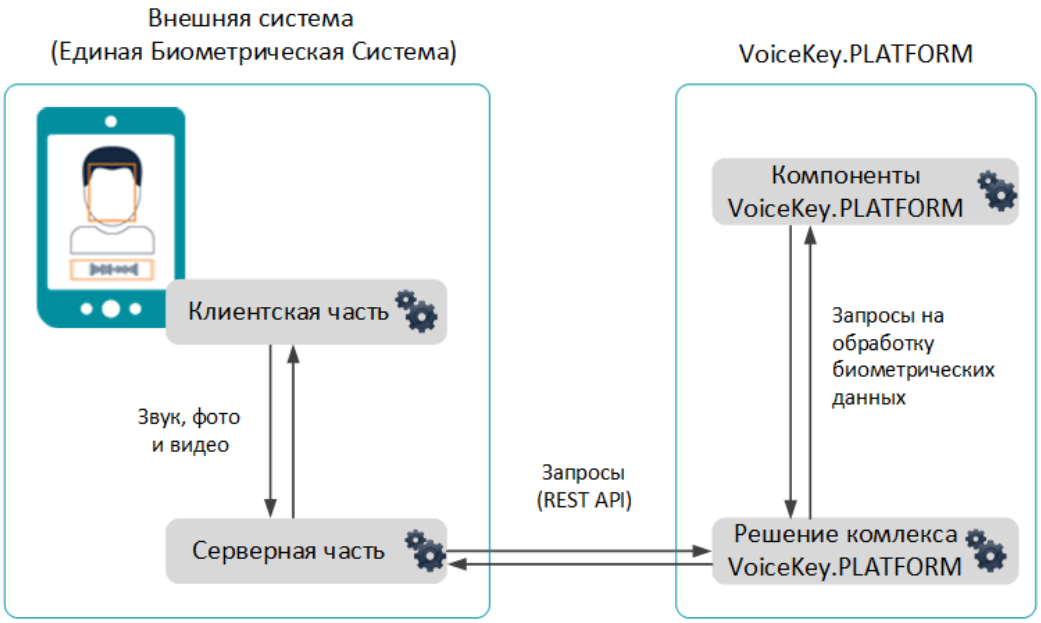
ТИПОВЫЕ СЦЕНАРИИ ИСПОЛЬЗОВАНИЯ

Реализация комплекса современных биометрических и речевых технологий позволяет с успехом использовать **VoiceKey.PLATFORM** во всех каналах дистанционного обслуживания:

- контактный центр;
- мобильное приложение;
- IVR или виртуальный ассистент системы самообслуживания;
- веб-приложение;
- виртуальный ассистент умного дома.

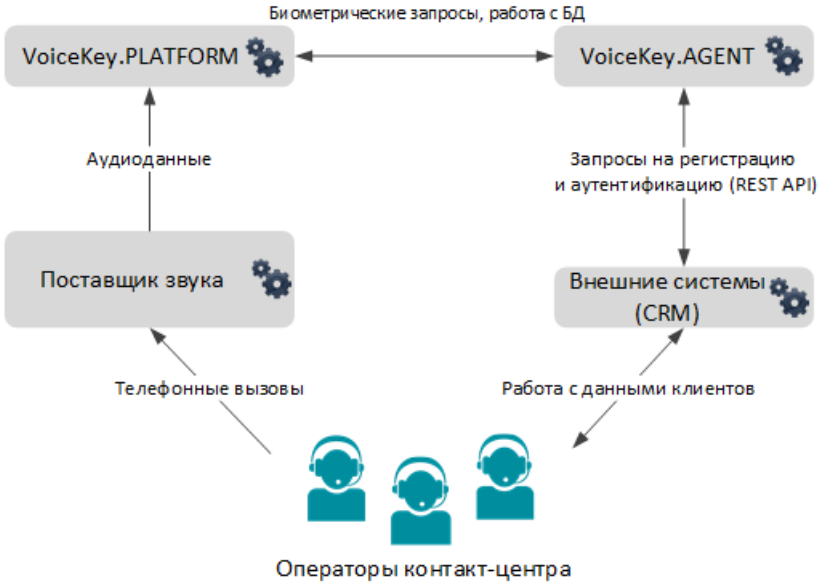
В соответствии с особенностями и требованиями каждой области применения возможно использование как одного, так и одновременно нескольких типов технологий.

Приоритетным направлением использования комплекса **VoiceKey.PLATFORM** является применение в Единых Биометрических Системах.



VoiceKey.AGENT

VoiceKey.AGENT предназначен для голосовой аутентификации клиента во время разговора с операторами контакт-центра или виртуальным ассистентом.



VoiceKey.AGENT формирует образец голоса клиента во время первого разговора с оператором контакт-центра или в мобильном приложении.

- Длительность речи для регистрации — от 30 секунд.

На основе полученного образца создаётся контрольный голосовой шаблон клиента, который сохраняется в базе данных. При последующих диалогах **VoiceKey.AGENT** сравнивает голос клиента с контрольным шаблоном. Такой процесс сравнения называется верификацией.

VoiceKey.AGENT проверяет клиента по Чёрным спискам. В этом случае выполняется сравнение в реальном времени голоса абонента, позвонившего в контакт-центр, с голосами из одного или нескольких Чёрных списков — биометрических шаблонов выявленных ранее мошенников.

- Длительность речи для верификации — от 7 секунд.

При успешном прохождении верификации оператор предоставляет персональные данные клиенту (например, состояние личного счёта абонента). Если верификация не пройдена, оператор может перевести звонок на сотрудника службы безопасности или иное лицо, обозначенное в должностной инструкции.

Во время телефонного разговора также возможна верификация оператора контакт-центра и создание контрольного голосового шаблона оператора.

Для оптимального качества:

- регистрация и верификация должны происходить с одних и тех же устройств,
- записи должны быть не шумными,
- должна отсутствовать реверберация (эхо),
- микрофон должен быть расположен максимально близко к человеку.

Сценарии использования

Интеграция с **VoiceKey.AGENT** может строиться по двум сценариям:

- Сценарий «Обобщённая биометрическая транзакция» предполагает одну общую транзакцию, в рамках которой может проводиться и регистрация, и аутентификация в канале клиента. Даёт гибкость в реализации, но требует более тщательного выстраивания бизнес-процессов, чтобы не допустить снижения качества биометрии.
- Сценарий «Суфлёр» позволяет работать с биометрией, распознаванием речи и обработкой распознанной речи в двух каналах: оператора и клиента. При проведении биометрической транзакции происходит верификация и идентификация.

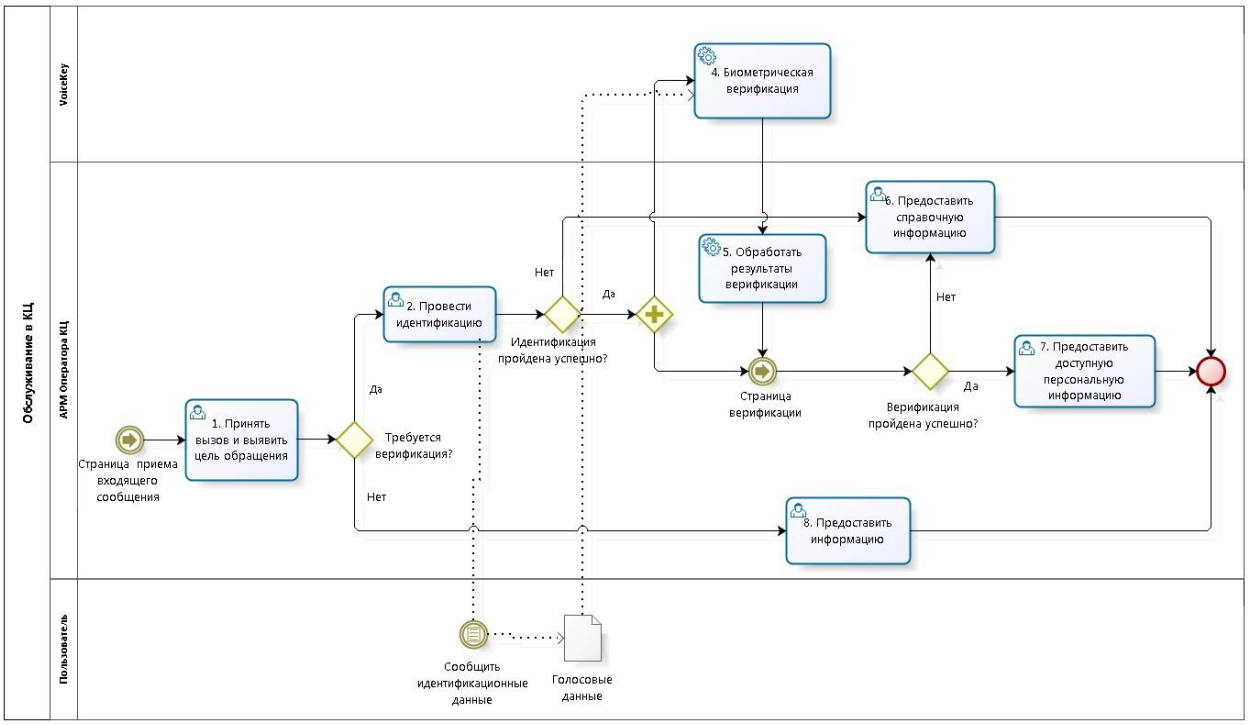
В таблице ниже приведено соответствие функциональности **VoiceKey.AGENT** сценариям использования.

Функциональность	**Сценарий использования**	
	Обобщённая биометрическая транзакция	Суфлёр
Регистрация (канал оператора)		+
Регистрация (канал клиента)	+	+
Верификация (канал оператора)		+
Верификация (канал клиента)	+	+
Определение живого диктора (Антиспуфинг)	+	+
Идентификация (ЧС, БС) (канал оператора)		+

Идентификация (ЧС, БС) (канал клиента)	+	+
Распознавание речи (канал оператора)		+
Распознавание речи (канал клиента)		+

Верификация клиентов в голосовом канале контакт-центров

Верификация клиентов в голосовом канале при обращении в контакт-центр заключается в проверке соответствия голосового шаблона, построенного во время общения клиента с оператором контактного центра, с контрольным шаблоном клиента, хранящимся в базе данных системы. Результат проверки передаётся в систему Заказчика с целью проинформировать оператора для принятия им дальнейших действий.



Реализация сценария предполагает выполнение следующих работ:

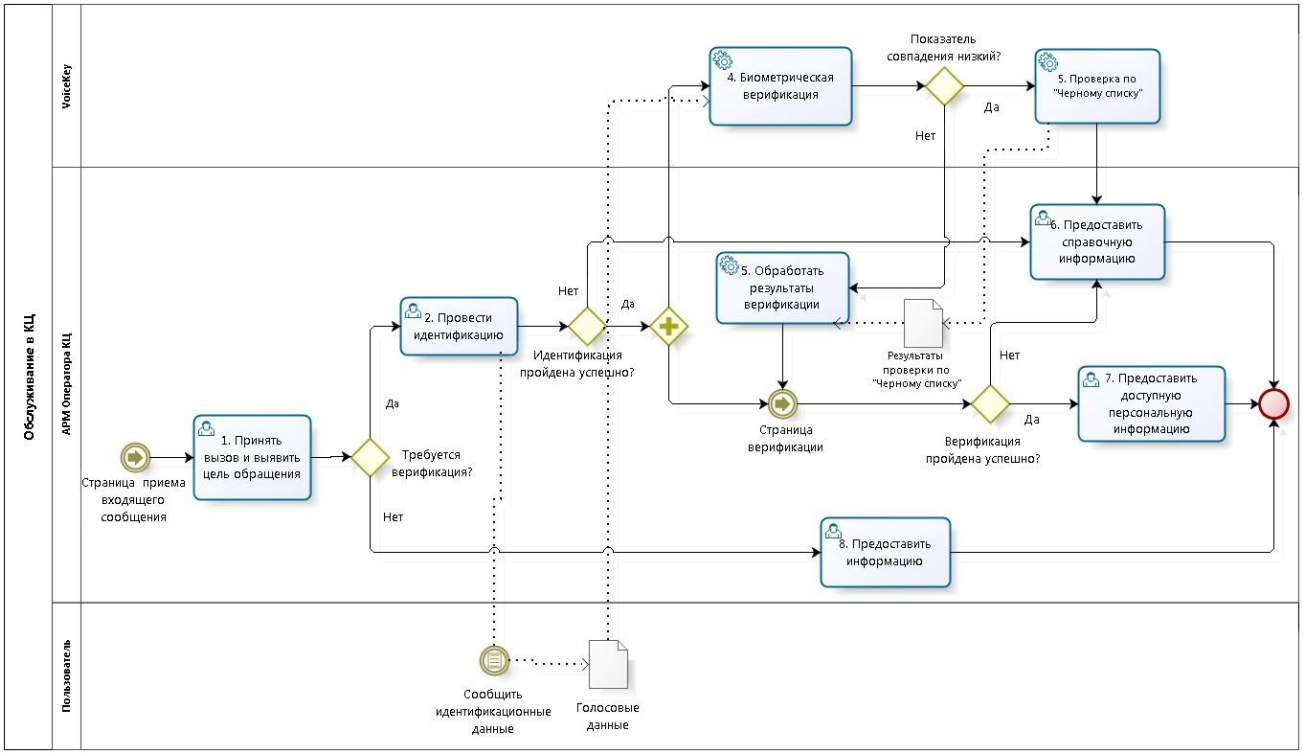
- Интеграция с CRM-системой контакт-центра в части инициации процесса регистрации и верификации клиента и вывода результата верификации. Выполняет интегратор или производитель CRM.
- Интеграция с телефонией в части съема звука из телефонного канала. Возможные варианты:
  - HTTP REST. Интегратор самостоятельно отправляет звукозапись по протоколу HTTP;

- WebSocket. Интегратор самостоятельно отправляет звукозапись по протоколу WebSocket;
- Интеграция с системой записи, используемой организацией-заказчиком. Потребуются работы со стороны интегратора и ЦРТ.

- Использование системы записи ЦРТ (сервер съёма звука).
  - Потребуются работы со стороны интегратора и ЦРТ.

Верификация клиентов в голосовом канале контакт-центров с онлайн-проверкой по спискам («Чёрным» и «Белым»)

Верификация клиентов в голосовом канале с онлайн-проверкой по спискам при обращении в контакт-центр заключается в сопоставлении (проверке) голосового шаблона, построенного во время общения клиента с оператором, с контрольным шаблоном, хранящимся в базе данных системы и размещённом в соответствующих группах списков (ЧС, БС). Результат сопоставления передаётся в систему Заказчика с целью проинформировать оператора для принятия им дальнейших действий.

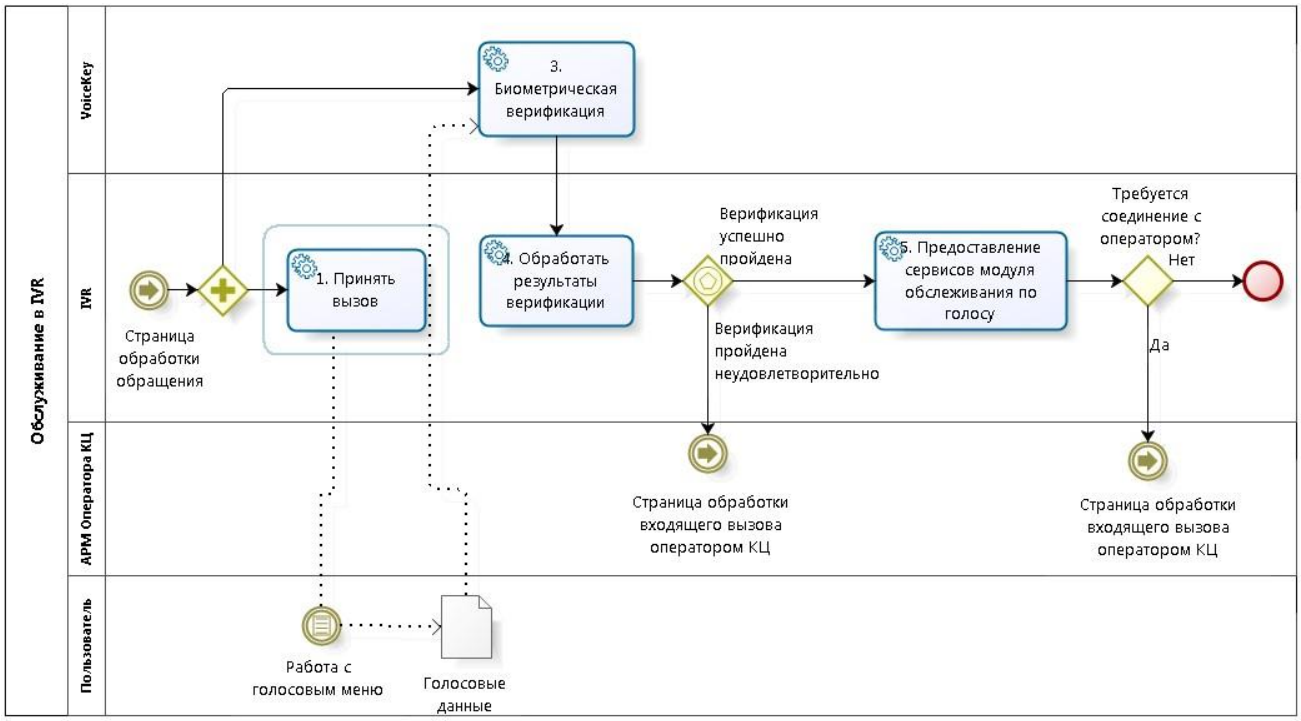


Реализация сценария предполагает выполнение тех же работ, что и верификация клиентов в голосовом канале при обращении в контакт-центр.

Верификация клиентов в голосовом меню IVR

Верификация клиентов в голосовом канале при обращении в контакт-центр с виртуальным голосовым ассистентом (голосовое самообслуживание) заключается в сопоставлении голосового шаблона,

построенного во время такого обращения, с контрольным шаблоном клиента, хранящимся в базе данных системы. Результат проверки передаётся в систему IVR Заказчика для принятия дальнейшего решения.



Реализация сценария предполагает выполнение следующих работ:

- Интеграция с IVR-приложением контакт-центра для осуществления процесса регистрации и верификации клиента. Выполняет интегратор или заказчик.

Суфлёр. Верификация в двух каналах: оператора и клиента, проведение распознавания речи и обработка распознанной речи

1. Верификация клиента в голосовом канале контакт-центра заключается в проверке соответствия голосового шаблона, построенного во время общения клиента с оператором контактного центра, с контрольным шаблоном клиента, хранящимся в базе данных системы.

Одновременно с верификацией возможно проведение распознавания речи клиента (speech-to-text). Результаты верификации клиента и распознавания его речи передаются во внешнюю систему Заказчика.

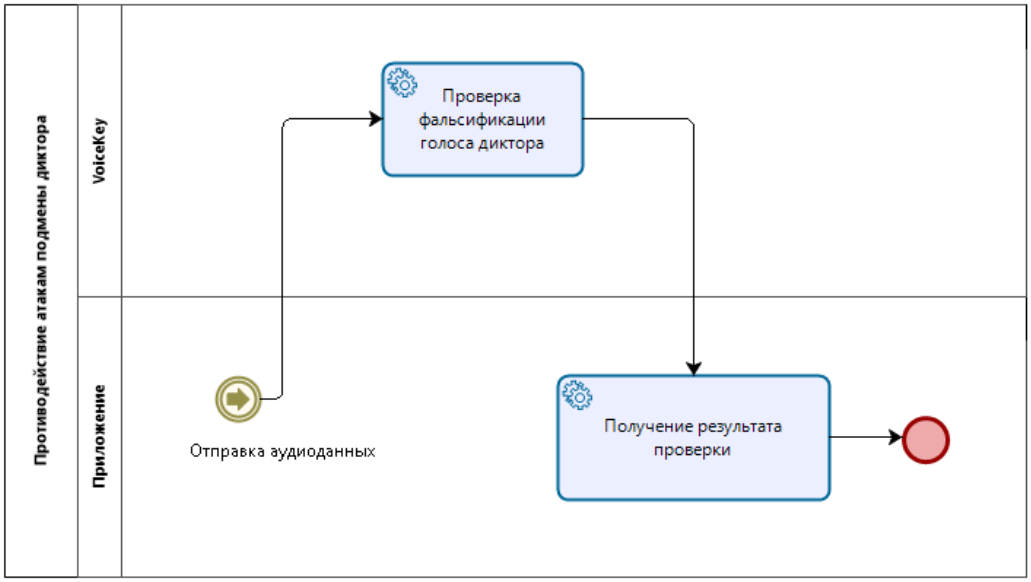
2. Верификация оператора в голосовом канале контакт-центра заключается в проверке соответствия голосового шаблона, построенного во время общения с клиентом, с контрольным шаблоном оператора, хранящимся в базе данных системы.

Одновременно с верификацией возможно проведение распознавания речи оператора (speech-to-text). Результаты верификации оператора и распознавания его речи передаются во внешнюю систему Заказчика.

Антиспуфинг. Противодействие атакам подмены диктора на систему голосовой аутентификации

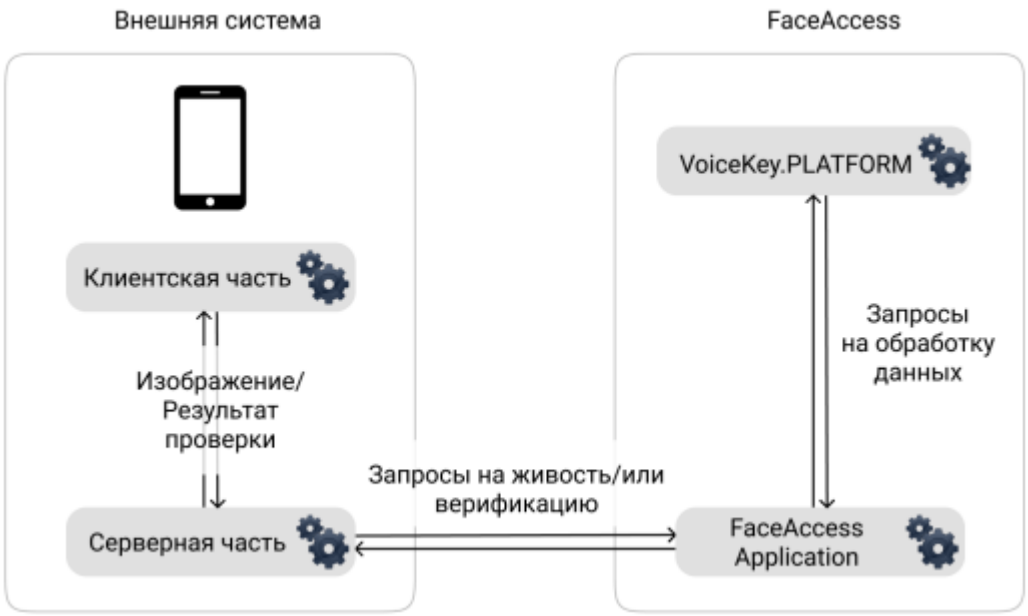
Сценарий позволяет анализировать звуковые данные, получаемые из внешней системы, определяя наличие признаков цифровой обработки сигнала и атак повторного воспроизведения (подстановка аудиозаписи). Результат проверки передаётся во внешнюю систему.

Реализация сценария предполагает выполнение тех же работ, что и верификация клиентов в голосовом канале при обращении в контактный центр, IVR.



VoiceKey.FaceAccess

Решение **VoiceKey.FaceAccess** предназначено для встраивания возможностей аутентификации и проверки на живость в программное обеспечение, онлайн-сервисы, мобильные приложения и другие продукты.



Решение **VoiceKey.FaceAccess** позволяет провести:

- регистрацию клиента (создание биометрического контрольного шаблона на основе фото/видео);
- проверку liveness;
- верификацию клиента.

Регистрация с проверкой liveness

Перед регистрацией пользователя необходимо произвести проверку его изображения на живость. В случае успешного прохождения проверки доступна регистрация персоны.

Проверка liveness

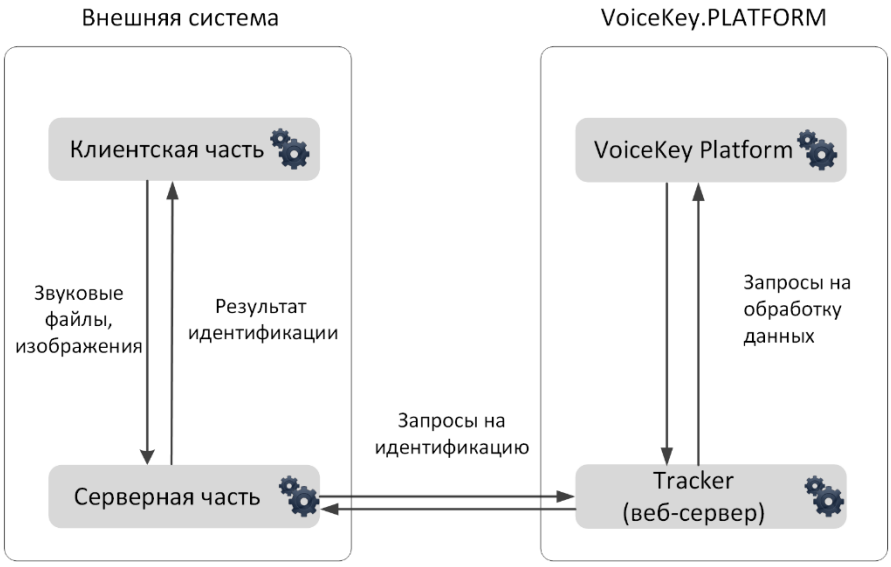
Проверка пользователя на живость заключается в отправке FaceAccess Application запроса, в теле которого передаётся фотография или видео (в процессе обработки видеозапись делится на кадры, выбираются изображения лица, по которым и происходит проверка). В ответе возвращается качественный результат проверки (прошёл ли пользователь проверку или нет) и количественный результат (числовое значение).

Верификация с проверкой liveness

Верификация зарегистрированного пользователя проводится после проверки его изображения на живость.

VoiceKey.TRACKER

Решение **VoiceKey.TRACKER** предназначено для идентификации по лицу и по голосу по большим массивам фотографий и аудиозаписей.

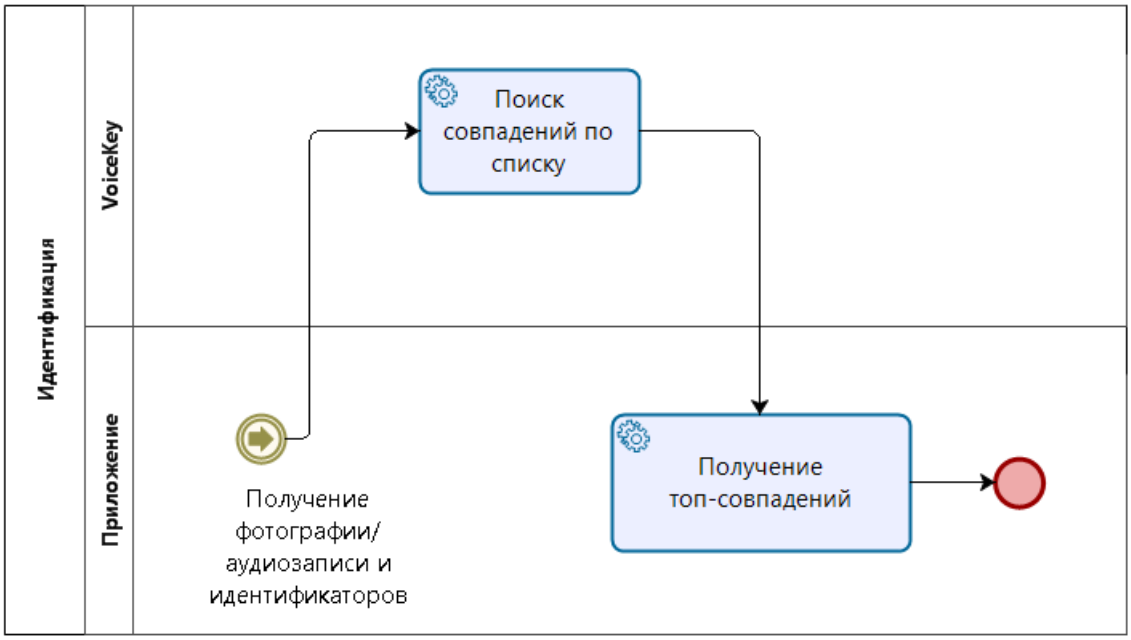


VoiceKey.TRACKER также используется для массового построения биометрических шаблонов лица и голоса. В процессе создания БКШ создаётся и профиль персоны, содержащий идентификатор, голосовой и/или лицевой шаблон.

Решение позволяет произвести идентификацию по лицу/голосу, сравнивая одно или несколько изображений/аудиозаписей с одним или несколькими изображениями/аудиозаписями.

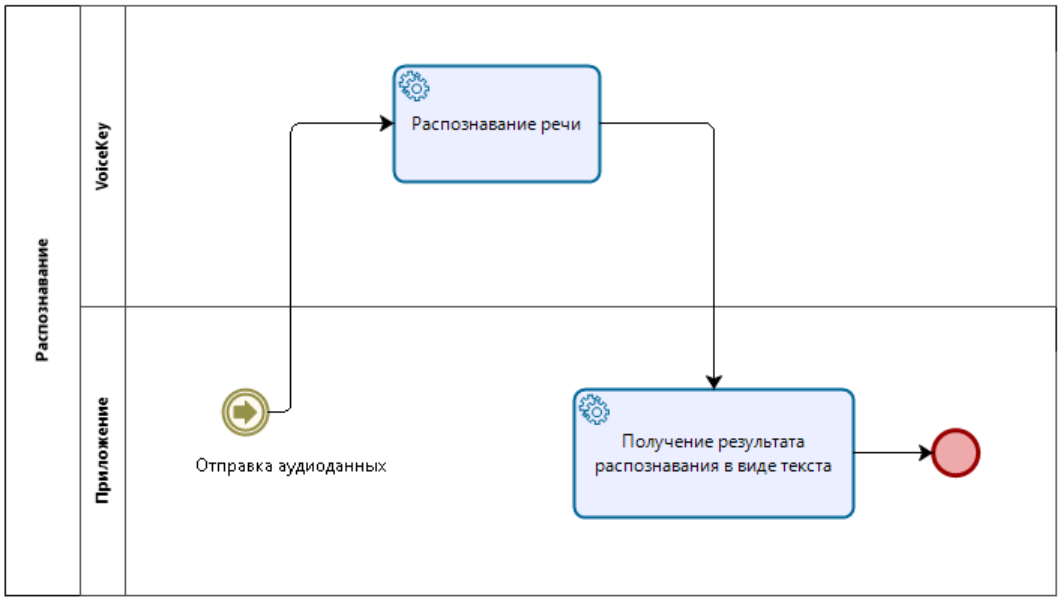
Идентификация клиентов по лицу и голосу

Идентификация клиентов по лицу голосу заключается в проверке соответствия голосового или лицевого шаблона с биометрическими шаблонами, содержащимися в хранилище биометрических данных. В результате проверки программный компонент **VoiceKey.TRACKER** возвращает список совпадений и показатель сходства для каждого изображения/аудиозаписи.


Идентификация
VoiceKey
Приложение
Поиск совпадений по списку
Получение фотографии/ аудиозаписи и идентификаторов
Получение топ-совпадений

VoiceKey.ASR / Распознавание речи (Speech-to-Text)

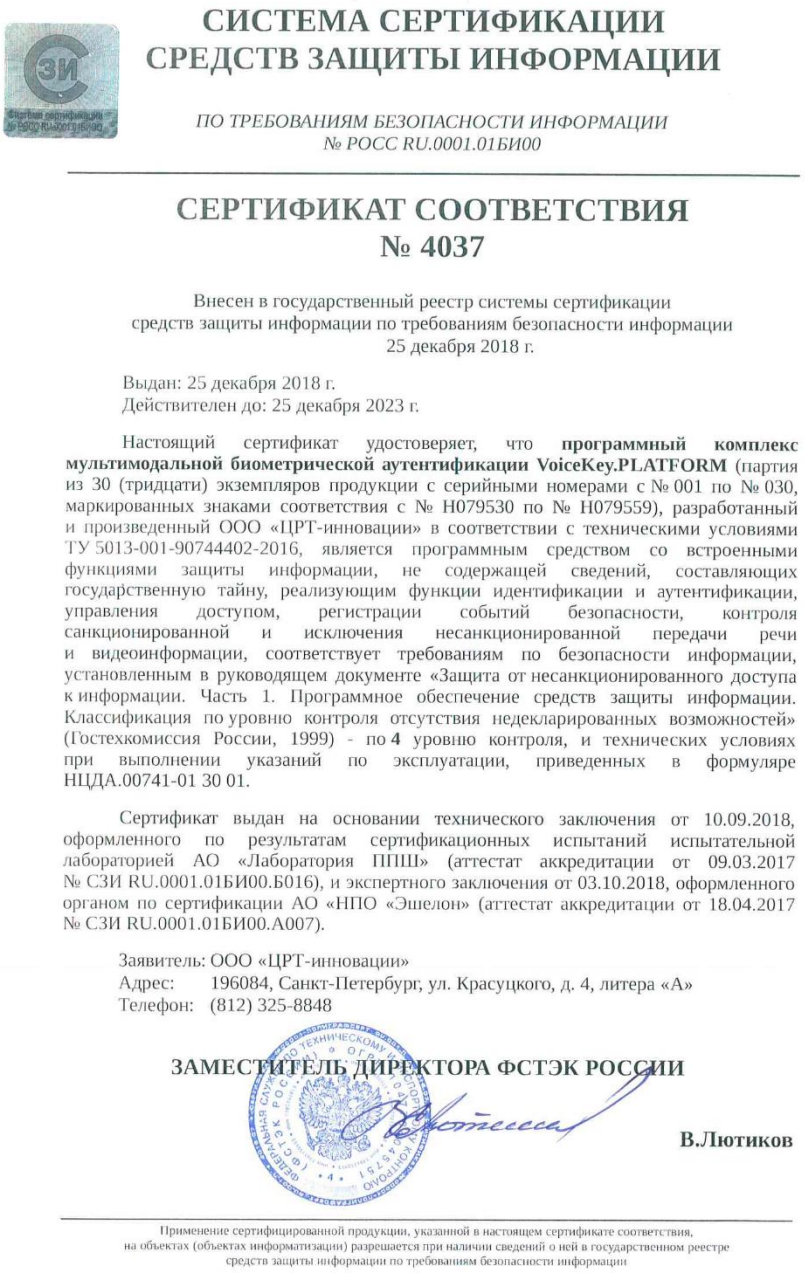
Компонент **VoiceKey.ASR** преобразует звуковые данные, получаемые через внешнюю систему, в текст. Результат преобразования передается во внешнюю систему.



ПРИЛОЖЕНИЯ

Сертификация комплекса

VoiceKey.PLATFORM является сертифицированным средством защиты информации.



СИСТЕМА СЕРТИФИКАЦИИ
СРЕДСТВ ЗАЩИТЫ ИНФОРМАЦИИ

ПО ТРЕБОВАНИЯМ БЕЗОПАСНОСТИ ИНФОРМАЦИИ
№ РОСС RU.0001.01БИ00

СЕРТИФИКАТ СООТВЕТСТВИЯ
№ 4037

Внесен в государственный реестр системы сертификации
средств защиты информации по требованиям безопасности информации
25 декабря 2018 г.

Выдан: 25 декабря 2018 г.
Действителен до: 25 декабря 2023 г.

Настоящий сертификат удостоверяет, что **программный комплекс мультимодальной биометрической аутентификации VoiceKey.PLATFORM** (партия из 30 (тридцати) экземпляров продукции с серийными номерами с № 001 по № 030, маркированных знаками соответствия с № Н079530 по № Н079559), разработанный и произведенный ООО «ЦРТ-инновации» в соответствии с техническими условиями ТУ 5013-001-90744402-2016, является программным средством со встроенными функциями защиты информации, не содержащей сведений, составляющих государственную тайну, реализующим функции идентификации и аутентификации, управления доступом, регистрации событий безопасности, контроля санкционированной и исключения несанкционированной передачи речи и видеоинформации, соответствует требованиям по безопасности информации, установленным в руководящем документе «Защита от несанкционированного доступа к информации. Часть 1. Программное обеспечение средств защиты информации. Классификация по уровню контроля отсутствия недекларированных возможностей» (Гостехкомиссия России, 1999) - по **4** уровню контроля, и технических условиях при выполнении указаний по эксплуатации, приведенных в формуляре НЦДА.00741-01 30 01.

Сертификат выдан на основании технического заключения от 10.09.2018, оформленного по результатам сертификационных испытаний испытательной лабораторией АО «Лаборатория ППШ» (аттестат аккредитации от 09.03.2017 № СЗИ RU.0001.01БИ00.Б016), и экспертного заключения от 03.10.2018, оформленного органом по сертификации АО «НПО «Эшелон» (аттестат аккредитации от 18.04.2017 № СЗИ RU.0001.01БИ00.А007).

Заявитель: ООО «ЦРТ-инновации»
Адрес: 196084, Санкт-Петербург, ул. Красуцкого, д. 4, литера «А»
Телефон: (812) 325-8848

ЗАМЕСТИТЕЛЬ ДИРЕКТОРА ФСТЭК РОССИИ

В.Лютиков

Применение сертифицированной продукции, указанной в настоящем сертификате соответствия, на объектах (объектах информатизации) разрешается при наличии сведений о ней в государственном реестре средств защиты информации по требованиям безопасности информации

Сертификат удостоверяет, что **VoiceKey.PLATFORM** является программным средством со встроенными функциями защиты информации; не содержит сведений, составляющих государственную тайну; реализует функции идентификации и аутентификации, управления доступом, регистрации событий

безопасности, контроля санкционированной и исключения несанкционированной передачи речи и видеоинформации, а также соответствует требованиям по безопасности информации.