МЕТОДИЧЕСКИЕ РЕКОМЕНДАЦИИ

по внедрению процесса регистрации биометрических данных

в банках

Оглавление

1 Введение

Единая биометрическая система — это цифровая платформа для удаленной идентификации, которая позволяет предоставлять новые цифровые услуги для граждан дистанционно в любое время и в любом месте.

Чтобы воспользоваться удаленной идентификацией, гражданину необходимо один раз лично прийти в уполномоченный банк для регистрации в единой биометрической системе (далее - ЕБС). При этом биометрические данные должны пройти процедуру проверки качества, после чего они могут использоваться для последующего дистанционного получения финансовых услуг - открытия счета (вклада), получения кредита или осуществления перевода.

Банки могут подключиться к Единой биометрической системе в роли:

- поставщика биометрических данных, т.е. организации, которая регистрирует биометрические данные граждан;
- потребителя сервиса удалённой идентификации, т.е. организации, которая получает результат удаленной идентификации - персональные данные клиентов с использованием единой системы идентификации и аутентификации (далее - ЕСИА) и ЕБС, а также банки могут предоставлять клиентам возможность подписать договор о банковском обслуживании дистанционно с использованием простой электронной подписи ЕСИА;
- организации, единовременного выполняющей роли поставщика биометрических данных и потребителя сервиса удалённой идентификации.

В документе вы найдете рекомендации по организации процесса регистрации биометрических данных (схема типового процесса представлена в Приложении 1).

1.1 Процесс биометрической регистрации в банке – поставщике биометрических данных

Для получения возможности прохождения удалённой идентификации через дистанционные каналы обслуживания гражданин должен лично обратиться в офис банка-поставщика, осуществляющего регистрацию в ЕСИА и ЕБС.

Общая схема биометрической регистрации гражданина представлена на рис. 1.

Рисунок 1 – Регистрация гражданина в ЕСИА и ЕБС

Описание процесса биометрической регистрации на стороне банка представлено на рисунке 2.

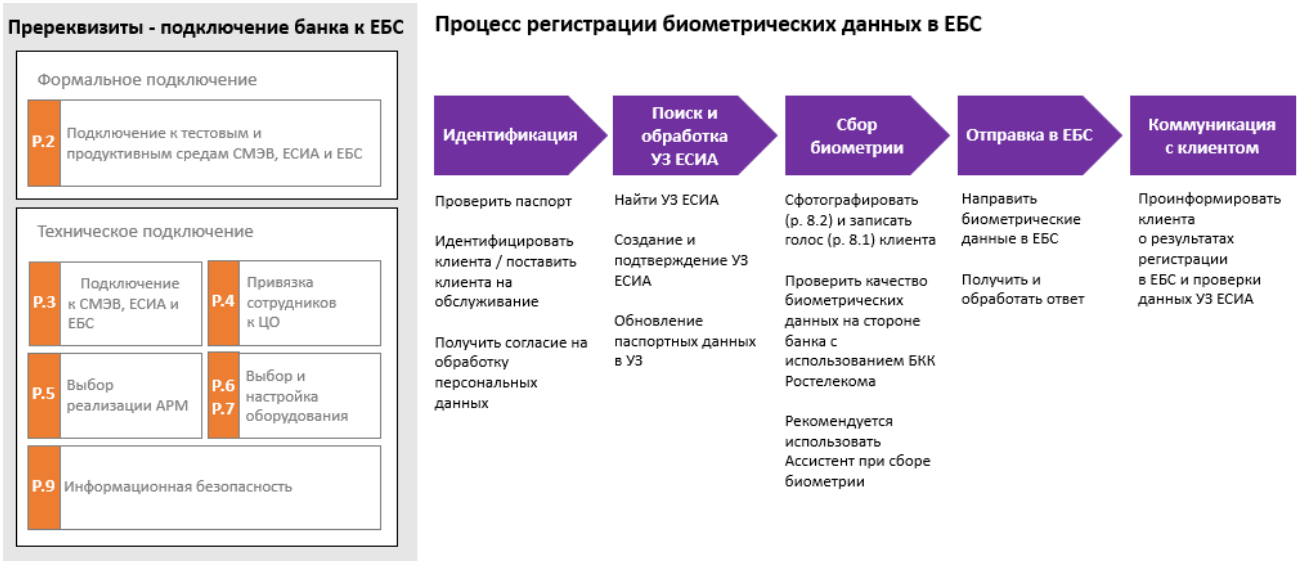


Рисунок 2 – Реализация процесса биометрической регистрации на стороне банка

Подключение банков к ЕБС, ЕСИА и СМЭВ

Для обеспечения процесса регистрации биометрических данных банку необходимо обеспечить взаимодействие следующих систем:

- информационные системы банка (ИС банка) – обеспечивают сбор и первичную проверку биометрических данных с использованием библиотеки контроля качества (БКК);

- система межведомственного электронного взаимодействия (СМЭВ) – транспортная система с гарантированной доставкой обеспечивает обмен данными между ИС банка, ЕБС и ЕСИА;
- единая система идентификации и аутентификации (ЕСИА) – обеспечивает ведение учетных записей пользователей и хранение персональных данных;
- единая биометрическая система (ЕБС) – предоставляет возможности хранения и сравнения биометрических данных, привязанных к учетным записям ЕСИА.

Для этого банку необходимо обеспечить:

- подключение банка к ЕБС (см. раздел 2) в соответствии с пошаговой инструкцией в личном кабинете (ЛК ЕБС);
- настройку сервисов для взаимодействия с ЕБС, СМЭВ и ЕСИА (см. раздел 3), используемых в процессе биометрической регистрации;
- закупку и настройку специализированного оборудования для сбора биометрических данных в отделениях (см. раздел 6 и 7).
- подготовку специализированных автоматизированных рабочих мест для биометрической регистрации (далее – АРМ) в отделениях банка (см. раздел 5).

Учётная запись ЕСИА сотрудника банка для проведения биометрической регистрации должна быть привязана к центру обслуживания (ЦО). Управление привязкой учётных записей сотрудников возможно вручную на техническом портале ЕСИА, либо автоматически с использованием специализированного REST-сервиса. Рекомендуется настройка сервисов прикрепления сотрудников к ЦО и последующего открепления с помощью REST-API ЕСИА (см. подробнее в разделе 4 настоящего документа).

Шаг 1. Идентификация гражданина

Гражданин пришел в отделение банка, воспользовался электронной очередью (при наличии) и был направлен к сотруднику, осуществляющему регистрацию в ЕСИА и ЕБС.

Гражданин предоставляет информацию о себе (паспорт), контактную информацию, а также (при наличии) СНИЛС.

Если он не является клиентом банка, ему предлагается стать клиентом. При этом банк проводит идентификацию клиента в соответствии со всеми требованиями ПОД/ФТ.

Шаг 2. Поиск и обработка учетной записи ЕСИА

Для регистрации в ЕСИА и ЕБС гражданин подписывает согласие на обработку его персональных данных по форме утверждённой распоряжением Правительства РФ от 30.06.2018 N 1322-р.

Сотрудником банка осуществляется поиск УЗ ЕСИА клиента. При настройке сервиса поиска УЗ рекомендуется установка параметров настройки сервиса[1] следующим образом:

- фамилия, имя и данные из паспорта (ДУЛ) заполняются обязательно;
- отчество заполняется обязательно, если присутствует в ДУЛ;
- адрес электронной почты, номер мобильного телефона и СНИЛС являются рекомендуемыми к заполнению, при этом должно быть заполнено минимум одно из этих полей.

Сотрудник банка на основании контактных и паспортных данных клиента с использованием сервиса поиска учетной записи ЕСИА проверяет статус учетной записи (УЗ) клиента в ЕСИА и при необходимости проводит процедуру обновления паспортных данных в УЗ, создания или подтверждения УЗ.[2]

В результате указанных действий банком должен быть получен идентификатор учетной записи в ЕСИА и её текущий статус.

Шаг 3. Сбор биометрических данных.

Сотрудник банка может приступить к процедуре регистрации биометрических данных, не дожидаясь ответа ЕСИА об обновлении/подтверждении УЗ ЕСИА. Используя интерфейс ИС Поставщика БДн для сбора биометрических данных, сотрудник делает аудиозапись голоса клиента и фотографию его лица (подробнее см. раздел 8). Полученные биометрические данные должны автоматически проверяться на соответствие требованиям качества с помощью БКК, предоставляемой ПАО «Ростелеком».

Шаг 4. Отправка биометрических данных в ЕБС

После того, как установлено, что качество полученных биометрических данных соответствует требованиям ЕБС с использованием БКК, биометрические данные и идентификатор УЗ ЕСИА передаются в ЕБС.

На основании предоставленных биометрических данных в ЕБС создается биометрический контрольный шаблон, который привязывается к идентификатору УЗ

[1] Подробнее о настройке сервисов см. в разделе 3
[2] Подробнее о настройке сервисов см. в разделе 3

ЕСИА. У созданной/обновленной учетной записи ЕСИА устанавливается дополнительный признак наличия биометрических данных, который отображается в личном кабинете на портале Госулуг.

Шаг 5. Коммуникации с клиентом

Если в процессе биометрической регистрации сотрудник банка получил статус подтверждения УЗ ЕСИА/обновления паспортных данных в УЗ ЕСИА, он должен проинформировать клиента о результатах и, в случае ошибки, о рекомендуемых дальнейших действиях.

После направления биометрических данных в ЕБС для их регистрации сотрудник банка должен проинформировать о результатах регистрации и, в случае возникновения ошибки, о рекомендуемых дальнейших действиях.

Если ошибка, не связана с техническими проблемами на стороне ЕСИА, ЕБС, СМЭВ или ИС банка, то клиенту необходимо предложить попробовать еще раз сдать биометрические данные.

Процессы, связанные с информированием клиента, отражены в схеме типового процесса регистрации в ЕСИА и ЕБС (см. Приложение 1).

Результат

Положительный. Клиент зарегистрирован в ЕБС. Внесение в УЗ ЕСИА статуса об успешной регистрации биометрических данных. Клиент и сотрудник банка проинформированы о результатах регистрации.

Отрицательный. Клиент проинформирован об ошибке при регистрации в ЕБС с предложением повторного прохождения биометрической регистрации после устранения ошибки. В случае, технической ошибки на стороне ЕБС, ЕСИА, СМЭВ или ИС банка, клиент проинформирован о невозможности сдать биометрические данные по техническим причинам.

В целях детального ознакомления с этим процессом рекомендуется ознакомиться с Методическими рекомендациями по работе с ЕБС [4] и подробной схемой типового процесса биометрической регистрации, представленной в Приложении 1.

2 Подключение к тестовым и продуктивным средам СМЭВ, ЕСИА и ЕБС

Для подключения информационной системы банка к ЕСИА и ЕБС, банку необходимо выполнить пошаговую инструкцию в личном кабинете (ЛК) на сайте https://bio.rt.ru/:

- получить ключ электронной подписи;
- подключить информационные системы банка к трем тестовым средам (ТСМЭВ, ТЕСИА, ТЕБС);
- протестировать информационную систему в тестовой среде ЕБС;
- подключить информационные системы банка к трем продуктивным средам (СМЭВ, ЕСИА, ЕБС);
- завершить все необходимые процедуры регистрации в личном кабинете.

Для подключения к продуктивной среде ЕБС необходимо подтвердить согласие с условиями договора оферты в личном кабинете на сайте https://bio.rt.ru/.

Подробное описание этапов подключения к ЕБС изложено в Приложении 2.

3 Рекомендации по настройке подключения банков к сервисам ЕСИА, ЕБС и СМЭВ

3.1 Использование СМЭВ

Подробная информация по использованию СМЭВ находится в документе «Методические рекомендации по работе с Единой системой межведомственного электронного взаимодействия» [2].

Для взаимодействия со СМЭВ можно использовать:

- решения сторонних производителей;
- собственные разработки с использованием типового клиента СМЭВ, производства Восход;
- полностью собственные разработки.

Сеть передачи данных СМЭВ использует СКЗИ класса КС3. Для подключения к СМЭВ устанавливаются криптографические маршрутизаторы.

Для взаимодействия со СМЭВ необходимо использование сертификатов КЭП для подписи всех исходящих запросов. Требования к классу СКЗИ для подписи запросов не предъявляются за исключением подписи запросов на регистрацию биометрических данных – КВ2.

Сервисы СМЭВ условно можно разделить на:

- транзакционные – сервисы, полное исполнение запросов к которым меняет состояние объектов;
- нетранзакционные – сервисы, исполнение которые не меняет состояние и несколько запросов с одинаковыми параметрами вернутся одинаковый результат.

Рекомендации по настройке сервисов

Рекомендация №1. Для нетранзакционных сервисов, скорость исполнения которых высока, (например, сервис поиска учетной записи в ЕСИА – FindAccount) возможно устанавливать короткий timeout (1-3 секунды), по истечении которого в случае отсутствия ответа повторять запрос с такими же параметрами.

Однако, рекомендация выполнима в случае оптимизированной работы с очередями СМЭВ, позволяющей достичь высокую скорость обработки ответных сообщений с результатами выполнения.

Оптимизация работы с очередями СМЭВ осуществляется по следующим ниже рекомендациям.

Рекомендация №2. Если очередь кредитной организации «пустует» и срабатывает timeout на вычитку сообщений из очереди – необходимо уменьшить timeout на вычитку сообщений из СМЭВ.

Рекомендация №3. Если в очереди ответных сообщений кредитной организации находится одновременно менее 1000 сообщений и их последовательная вычитка приводит к увеличенному времени обработки сообщений, то необходимо использовать отдельные модули вычитки сообщения для отдельных видов сведений и чтение очереди СМЭВ с фильтрацией по видам сведений[3].

[3] Подробнее в разделе Методических рекомендаций по работе со СМЭВ 5.3.2. Получение сообщения с фильтрацией по протоколу обмена [1]

В случае, если в очереди ответных сообщений банка находится свыше 1000 сообщений, то необходимо либо увеличивать количество модулей, вычитывающих из очереди СМЭВ, снижая тем самых количество одновременно находящихся сообщений до менее 1000 и следовать рекомендации 3.

Рекомендация №4. Если в очереди более 1000 сообщений, необходимо зарегистрировать отдельную информационную систему с собственной очередью ответных сообщений. Она будет посылать запросы в отдельные виды сведений от имени этой отдельной информационной системы и следовать рекомендации №2.

Конкретный метод оптимизации выбирается применительно к архитектуре информационной системы кредитной организации.

3.2 Взаимодействие с ЕСИА

Подробная информация по взаимодействию с ЕСИА содержится в Методических рекомендациях по работе с ЕСИА [3].

Для выстраивания работы с учетными записями и сервисами ЕСИА необходимо учитывать статусы учетных записей:

- упрощенная – учетная запись, полученная при самостоятельной регистрации и содержащая непроверенные ФИО и контактные данные;
- стандартная – в учетную запись занесены сведения из ДУЛ и СНИЛС, и они были проверены в сервисах МВД и ПФР;
- подтвержденная – данные учетной записи проверены (сведения из ДУЛ, и СНИЛС) в сервисах МВД и ПФР и личность владельца подтверждена при личной явке.

Регистрация биометрических данных включает использование следующих сервисов ЕСИА:

- поиск учетной записи в ЕСИА (FindAccount);
- регистрация подтвержденной учетной записи в ЕСИА с отправкой пароля для первого входа в систему на контактные данные (Register);
- подтверждение учетной записи в ЕСИА, созданной на основе существующей упрощенной (RegisterBySimplified);

- подтверждение личности гражданина РФ или иностранного гражданина в ЕСИА (Confirm);
- изменение паспортных данных пользователя в ЕСИА (update_passport_data).

В СМЭВ ЕСИА разработан сервис обновления паспортных данных, при помощи которого сотрудник банка может при необходимости вносить изменения в паспортные данные, которые уже были внесены в учетную запись ЕСИА клиента.

Сервисами восстановления и удаления учетной записи ЕСИА (Recover и Delete) можно пользоваться на усмотрение банка.

Руководства пользователя для настройки сервисов представлены на технологическом портале СМЭВ[4]. Предполагается выполнение сервисов в соответствии с типовым процессом биометрической регистрации (см. Приложение 1).

3.3 Взаимодействие с ЕБС

Подробная информация по взаимодействию с ЕБС содержится в методических рекомендациях по работе с ЕБС [4].

ЕБС хранит биометрические данные с привязкой к идентификатору учетной записи ЕСИА. При этом сохранение биометрических данных происходит вне зависимости от статуса учетной записи ЕСИА, однако сервис по удалённой идентификации доступен только клиентам с подтвержденной учетной записью.

В ЕБС функционирует контроль качества биометрических данных. Контроль осуществляется с использованием БКК, которая в том числе предоставляется в банки для минимизации количества ошибок при биометрической регистрации. БКК предоставляется в следующих видах:

- исходные коды на языке Си;
- собранные библиотеки под платформы Windows, Linux Ubuntu, Linux Centos;
- docker-образ для запуска библиотеки в контейнере.

В БКК реализованы интерфейсы для взаимодействия:

- программный интерфейс (экспортированы функции из библиотеки);
- REST API для вызова функций по сети.

[4] ссылка: https://smev3.gosuslugi.ru/portal/inquirytype.jsp?zone=fed&page=1

Рекомендуется реализация функций БКК на стороне банка при помощи специализированного ПО (подробнее в разделе 5).

4 Взаимодействие с центрами обслуживания

Для сокращения количества осуществляемых вручную операций, связанных с прикреплением и откреплением учетных записей ЕСИА сотрудников банка к центрам обслуживания (ЦО), рекомендуется настройка ряда новых сервисов ЕСИА при помощи REST-API:

- сервис управления ЦО;
- сервис безусловного добавления сотрудников в организацию;
- получение списка ЦО в организации;
- сервис прикрепления сотрудников к ЦО;
- блокировка сотрудников организации.

Подробное описание реализации сервисов для прикрепления сотрудников банка опубликовано на сайте bio.rt.ru. Перед настройкой сервисов ознакомьтесь с методическими рекомендациями по использованию ЕСИА (версия 2.54). Реализация открепления сотрудников от ЦО указана в пункте Б.7.3 Управление служебными данными присоединенных сотрудников, а также блокировка и удаление должностных лиц организации описано в Приложении Б к Рекомендациям.

Рекомендуется два варианта реализации указанных сервисов (в зависимости от возможности идентификации внутреннего структурного подразделения) при идентификации сотрудника в информационной системе банка:

1. *Есть возможность идентификации внутреннего структурного подразделения:* привязка и отвязка может осуществляться автоматически при идентификации сотрудника в информационной системе банка с АРМ. Это предпочтительный вариант.
2. *Нет возможности идентификации внутреннего структурного подразделения:* привязка и отвязка сотрудника к ЦО осуществляется единолично администратором, но подтверждения сотрудника в сравнении с привязкой через техпортал ЕСИА – не требуется.

5 Рекомендации по реализации АРМ для биометрической регистрации

Рекомендуемый процесс биометрической регистрации на стороне банка включает действия по идентификации клиента, работе с учетной записью клиента в ЕСИА, получению и регистрации биометрических данных (см. рис. 3). Все шаги осуществляются в присутствии клиента с использованием автоматизированного рабочего места.

Рисунок 3 – Процесс биометрической регистрации на стороне КО

Предполагается, что разрабатываемый процесс должен включать описание процедуры биометрической регистрации гражданина от выбора услуги клиентом в электронной очереди до его информирования о результатах регистрации в Единой биометрической системе. Рекомендуется взять за основу детализированную схему процесса регистрации клиента в ЕСИА и ЕБС из Приложения 1.

Важно! При реализации процесса также следует учитывать взаимодействие информационной системы банка с центром обслуживания ЕСИА в части привязки и отвязки учётных записей ЕСИА сотрудников банка (см. подробнее в разделе 4).

При выборе решения для реализации автоматизированного рабочего места в соответствии с рекомендуемым процессом регистрации[5] следует учитывать порядок осуществления процесса регистрации биометрических данных, а также соответствующие требования к информационным технологиям и техническим средствам установленный в Приказе Минкомсвязи России от 25.06.2018 № 321[5].

Рекомендуется обеспечить максимальный уровень автоматизации процесса регистрации, включая, но не исключая прочее, привязку учетной записи ЕСИА сотрудника

[5] Подробнее см. описание в разделе 1.1

к центру обслуживания ЕСИА, контроль или мониторинг условий получения биометрических данных для каждой используемой модальности (лицо и голос), использование ассистентов (специализированного программного обеспечения) показывающих рекомендации в режиме реального времени для сотрудника и клиента, и осуществление контроля качества полученных биометрических данных. Выбор оптимального решения для автоматизированного рабочего места позволит минимизировать временные затраты на выполнение биометрической регистрации. Комплексные решения для автоматизированного рабочего места могут разрабатываться банком самостоятельно или предоставляться сторонними производителями.

Для снижения вероятности отказов регистрации по результатам проверки качества биометрических данных со стороны ЕБС в АРМ, или на сервере, который осуществляет контроль данных, требуется установка БКК, предоставляемой ПАО «Ростелеком», которая обеспечит минимизацию расхождения в методах измерения ключевых характеристик биометрических данных. БКК ПАО «Ростелеком» публикуется на портале bio.rt.ru[6].

В качестве ПО, помогающего сотруднику банка производить сбор биометрических данных, рекомендуется использование ассистента, предоставляемого ПАО «Ростелеком».

При помощи Ассистента предполагается реализация:

- функций контроля качества биометрических данных в режиме реального времени;
- информирования сотрудника банка и клиента о рекомендуемых действиях для получения качественных биометрических данных;
- получения набора биометрических данных и предварительного выбора в нем максимально подходящих для регистрации изображений лица;
- осуществление кадрирования путем фиксирования изображения без посторонних деталей, таких как второе лицо, фотографии, портреты на заднем фоне и др.

Необходимые для установки ассистента ПАО «Ростелеком» материалы публикуются на портале bio.rt.ru[7].

При реализации автоматизированного рабочего места также рекомендуется:

[6] https://bio.rt.ru/documents/software/
[7] https://bio.rt.ru/documents/software/

- настроить предварительное заполнение согласия клиента на обработку персональных данных для снижения времени обслуживания и удобства клиента;
- настроить обработку ответа о возникновении ошибки при проверке привязки учётной записи ЕСИА сотрудника к ЦО и корректное информирование сотрудника об этом до обслуживания клиента;
- настроить параллельное осуществление поиска/регистрации /подтверждения УЗ и сбора биометрических данных для снижения среднего времени обслуживания одного клиента при процессе регистрации.

6 Рекомендации по выбору оборудования

Для подготовки внутренних структурных подразделений банка к сбору биометрических персональных данных клиентов необходимо соответствующее оборудование: камеры и микрофоны. При закупке оборудования банки могут руководствоваться следующими нормативными документами и информационными материалами:

- приказ Минкомсвязи России № 321 «Об утверждении порядка обработки, включая сбор и хранение, параметров биометрических персональных данных в целях идентификации, порядка размещения и обновления биометрических персональных данных в единой биометрической системе, а также требований к информационным технологиям и техническим средствам, предназначенным для обработки биометрических персональных данных в целях проведения идентификации» [5], содержащий требования к оборудованию внутренних структурных подразделений банка;
- перечень информационных технологий и технических средств, прошедших подтверждение соответствия требованиям к информационным технологиям и техническим средствам, предназначенным для обработки биометрических персональных данных. Он включает оборудование, которое уже прошло сертификацию на соответствие требованиям Приказа № 321, но при этом не являющееся обязательным для закупки. Банки вправе закупать любое оборудование, которое соответствует требованиям Приказа № 321;
- иные вспомогательные материалы на сайте https://bio.rt.ru/business/.

Оборудование для сбора биометрии должно получить положительное заключение комиссии Минкомсвязи о соответствии требованиям Приказа. Характеристики

оборудования рекомендуется брать либо с сайта производителя, либо из инструкции к закупленному оборудованию. Если какая-то характеристика отсутствует, следует направить официальный запрос производителю или его представителю для получения официального ответа.

6.1 Рекомендации по выбору микрофона

Микрофон должен удовлетворять характеристикам пункта 3 приложения 3 Приказа [5].

Микрофон не должен иметь функции шумоподавления и автоматической регулировки усиления звука: эти функции запрещены в Приказе.

Одной из главных характеристик микрофона является чувствительность. Чувствительность показывает, сколько микрофон производит выходного напряжения при определенном уровне звукового давления. Высокочувствительный микрофон выдает выходной сигнал большего напряжения, в отличии от низкочувствительного, когда оба находятся в одинаковых условиях под одной и той же звуковой нагрузкой. Низкочувствительный микрофон нуждается в большем усилении звукового сигнала с микшера, чем высокочувствительный. Большее усиление обычно приводит к усилению внутреннего шума электронных компонентов микрофона и звуковой карты. Рекомендуется использовать микрофоны с большей чувствительностью. Окно по настройке чувствительности и усиления микрофона в ОС Windows 10 представлено на рисунке 6.

Важно и как микрофон «слышит» звук с разных направлений - одинаково или более точно реагирует на звук, приходящий по оси микрофона, или с боков и сзади микрофона. Отклик микрофона на звук, приходящий со всех направлений называют его диаграммой направленности. Существует несколько типов диаграммы направленности (см. рисунок 4).

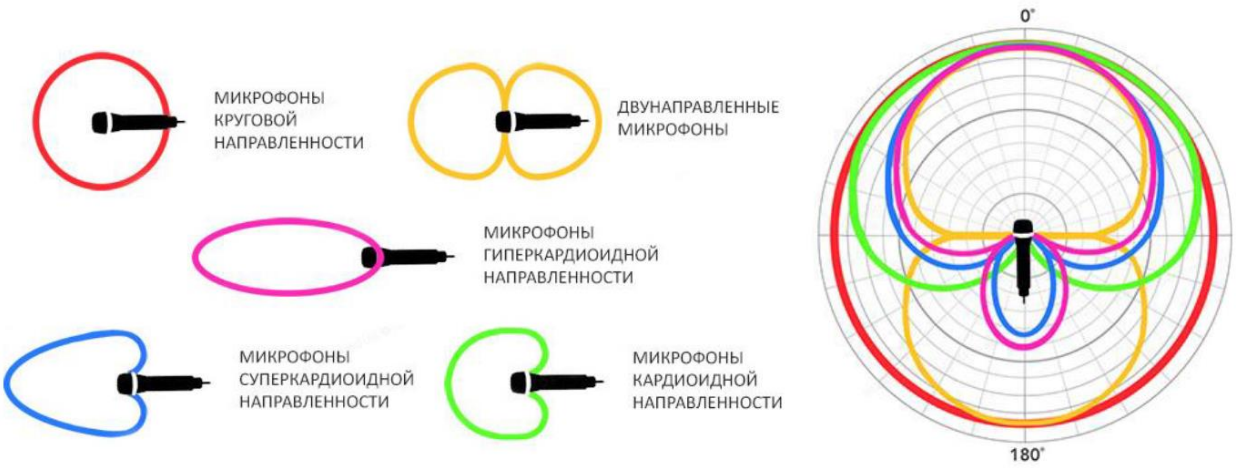


Рисунок 4 – Диаграмма направленности микрофонов

Микрофоны с круговой (всенаправленной) диаграммой одинаково снимают звук с различных направлений, ввиду чего не получается изолировать источник полезного

сигнала. Направленная диаграмма имеет более узкую зону захвата звука, что позволяет регистрировать полезный сигнал с большим отношением сигнал/шум, в отличии от микрофонов с круговой диаграммой направленности.

Для сбора биометрических данных в условиях банковского офиса рекомендуется использовать микрофоны с узкой диаграммой направленности (кардиоида, суперкардиоида и гиперкардиоида).

6.2 Рекомендации по выбору камеры

Камера должна удовлетворять характеристикам пункта 2 приложения 3 Приказа [5].

7 Рекомендации по настройке оборудования

Указанные ниже рекомендации не должны рассматриваться отдельно от рекомендаций по выбору оборудования, так как могут оказаться недостаточными для успешной реализации процедуры регистрации, если оборудование не подходит для конкретных условий ВСП. В связи с этим необходимо тестировать оборудование и выполнять его настройку индивидуально в каждом ВСП до момента начала обслуживания клиентов банка.

7.1 Рекомендации по настройке микрофона

Эта рекомендация предназначается для сотрудника, ответственного за настройку оборудования.

Рекомендуем выполнить следующие шаги:

1. проверить настройки эффектов микрофона: все эффекты (в том числе шумоподавление, устранение акустического эха и др.) должны быть отключены как при настройке микрофона, так и в процессе сбора биометрических данных (см. Рисунок 5);

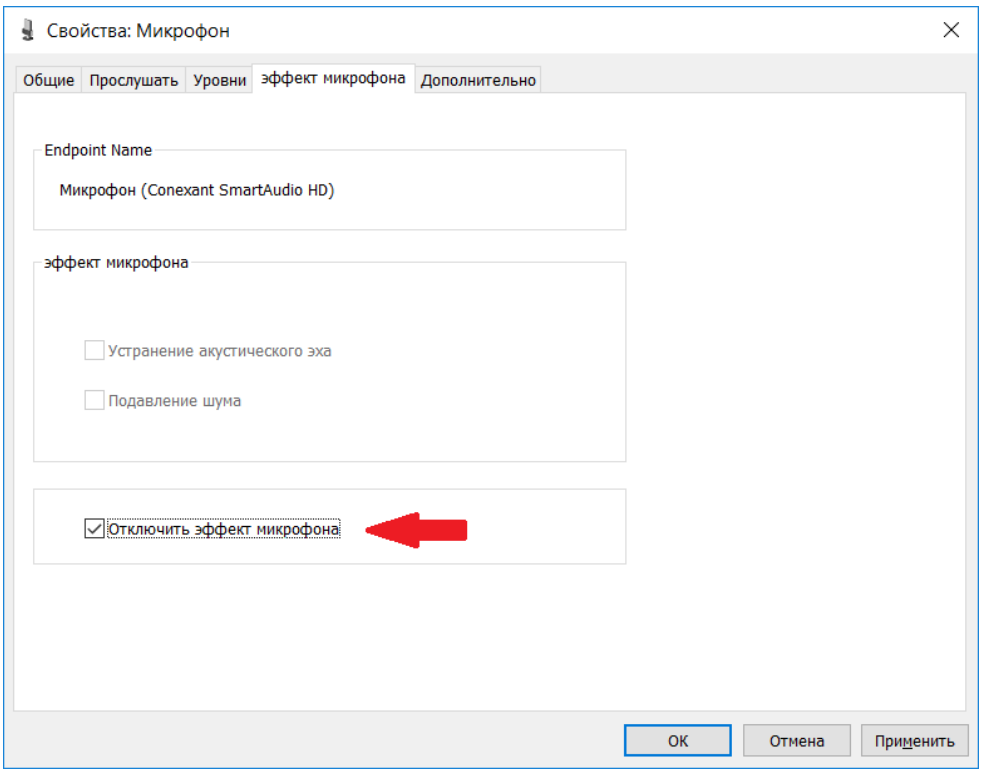


Рисунок 5 – Окно настройки микрофона с отключенными эффектами микрофона в ОС Windows 10

2. сделать подряд несколько записей голоса испытуемого человека с корректировкой уровня микрофона (см. Рисунок 6), чтобы выставить максимальный уровень громкости записываемого голоса в диапазоне от -9 до -6 dBFs. Испытуемый должен находится на дистанции от микрофона, соответствующей предполагаемым условиям биометрической регистрации клиента. Голос испытуемого должен соответствовать разговорной речи без эмоциональной окраски. Измерения рекомендуется проводить при помощи специализированного программного обеспечения с визуализацией уровня громкости записи (например Audacity).

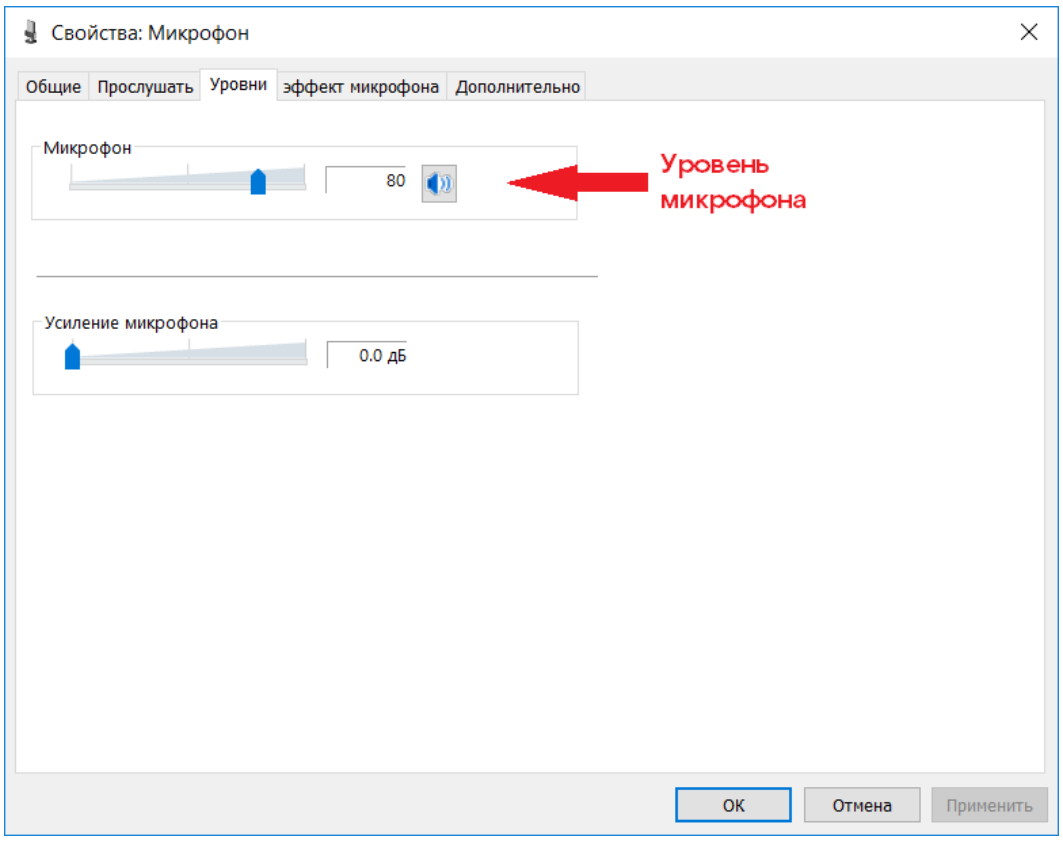


Рисунок 6 – Окно настройки микрофона с включенным уровнем микрофона и выключенным усилением в ОС Windows 10

В отличии от усиления микрофона, регулировку уровня микрофона можно производить до максимально допустимого значения;

3. отправить запись на проверку в БКК. Данный шаг рекомендуется сделать для нескольких тестовых записей (минимум 3), и проверить все их на наличия следующих ошибок:
    a. в случае наличия кода ошибки – Перегрузка микрофона, уменьшить уровень микрофона. Провести 3 тестовые записи, после выполнения данной регулировки, для проверки корректности настройки;
    b. в случае наличия кода ошибки – Недостаточно голосовых данных, увеличить уровень микрофона. Провести 3 тестовые записи, после выполнения данной регулировки, для проверки корректности настройки;
    c. в случае наличия кода ошибки – Недостаточно голосовых данных, и максимально выставленного уровня микрофона, следует провести настройку усиления микрофона. Рекомендуется данную настройку делать минимально возможной. Максимально допустимое значение усиления микрофона: + 24 дБ (см. Рисунок 7);

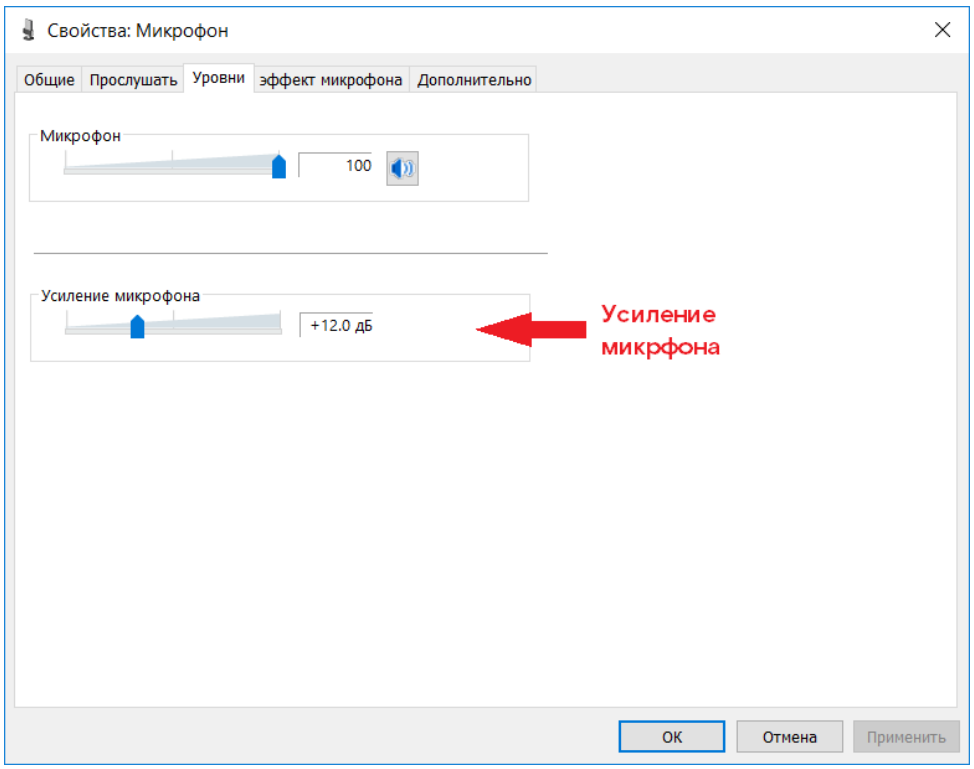


Рисунок 7 – Окно настройки микрофона с настроенным уровнем и усилением микрофона в ОС Windows 10

Провести 3 тестовые записи, после выполнения данной регулировки, для проверки корректности настройки;

- сохранить итоговые настройки оборудования.

Максимальный уровень громкости рекомендуется контролировать при каждой записи голоса в рамках процесса регистрации биометрического шаблона. Рекомендуется визуализировать текущий и максимальный уровень громкости в момент записи голоса.

Рекомендуется запрещать приложениям использовать устройство в монопольном режиме (см. Рисунок 8), если это не автоматический процесс калибровки микрофона, разработанный в целях настройки оборудования для выполнения дальнейшего сбора биометрических данных.

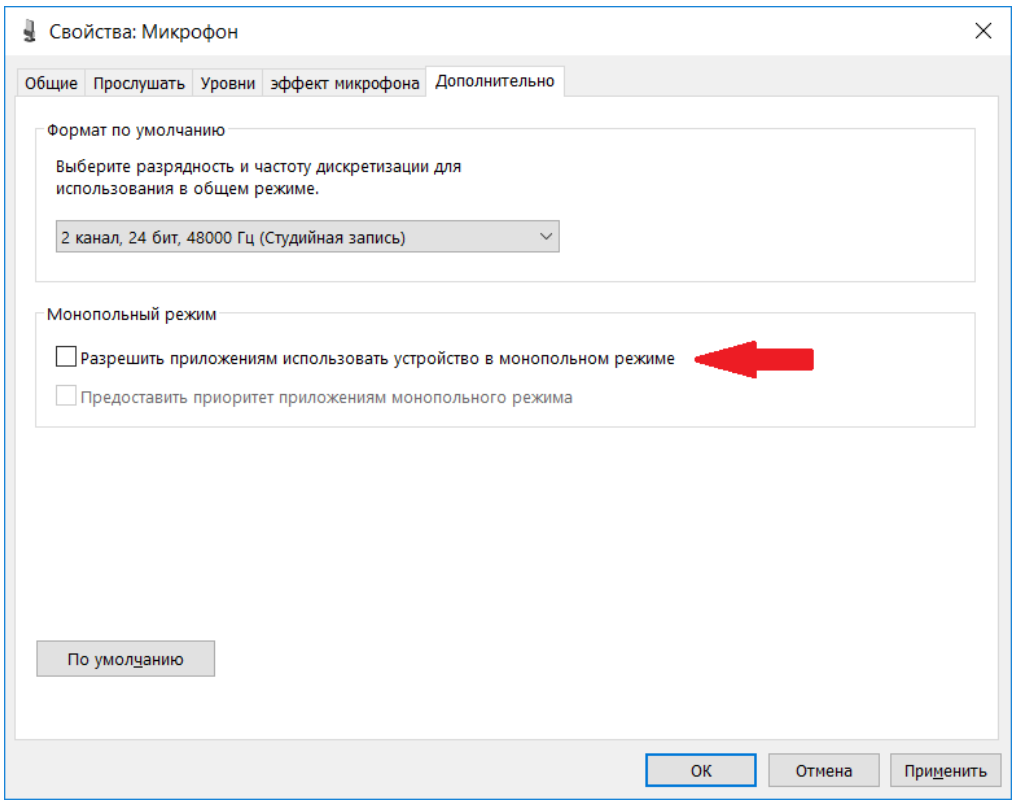


Рисунок 8 – Окно настройки микрофона с выключенным монопольным режимом в ОС Windows 10

7.2 Рекомендации по настройке камеры и освещенности помещения

Камера должна обладать следующими характеристиками:

- разрешение получаемого изображения: не менее 1280x720 пикселей;
- снятие изображения лица должно проводиться при использовании режима автоматической корректировки баланса белого цвета;
- снятие изображения лица должно проводиться при использовании режима автофокусировки.

Для обеспечения естественной цветопередачи кожи рекомендуется, чтобы цветовая температура осветителей составляла от 4800 до 6500 К. Требуемая цветовая температура обеспечивается люминесцентными или светодиодными источниками освещения. Используемые источники освещения должны создавать в области лица освещенность:

− для камер без автоматической коррекции освещенности не менее 300 лк;

− для камер с автоматической коррекцией освещенности не менее 100 лк.

При исполнении рекомендаций по получению лицевых биометрических данных (раздел 8.2 методических рекомендаций) дополнительных настроек камеры не требуется.

8 Рекомендации по получению биометрических данных

8.1 Рекомендации по получению голосовых биометрических данных

Перед получением голосовых биометрических данных необходимо настроить уровень микрофона (и, в случае необходимости, усиление микрофона) так, чтобы при записи голоса не происходила перегрузка микрофона. Перегрузка часто не слышна на слух, однако хорошо заметна на осциллограмме аудиозаписи (информация по настройке оборудования представлена в разделе 7.1).

При получении голосовых биометрических данных рекомендуется выполнить следующие шаги:

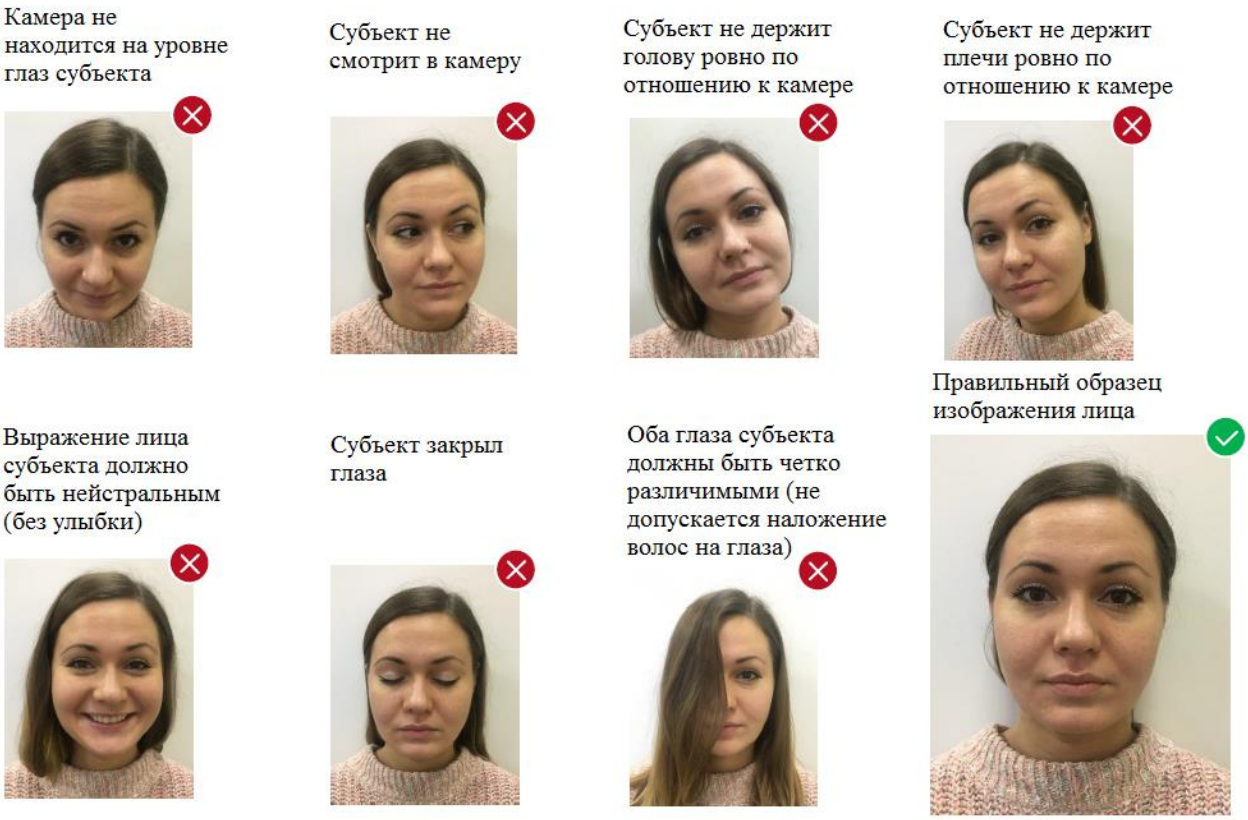
- проверить работоспособность батарейки в микрофоне (в случае её наличия);
- контролировать правильность произношения последовательности значений клиентом;
- в случае возникновения ошибки – «Недостаточно голосовых данных» попросить клиента подвинуться к микрофону или приблизить микрофон к клиенту;
- в случае возникновения ошибки «Перегрузка микрофона» следует отодвинуть микрофон от клиента. Если ошибка повторяется часто, следует повторить все шаги настройки из раздела 7.1.

8.2 Рекомендации по получению лицевых биометрических данных

При получении лицевых биометрических данных необходимо выполнить следующие условия:

- камера должна находиться на уровне глаз клиента;
- клиент должен смотреть прямо в камеру, держать голову прямо и плечи ровно по отношению к камере;
- лицо должно быть равномерно освещено, чтобы на изображении отсутствовали тени, блики, области пересвета;
- на изображении должно присутствовать только одно лицо;
- выражение лица должно быть нейтральным (без улыбки), оба глаза нормально открыты (т.е. не широко) и четко различимыми (волосы не должны падать на глаза, рот должен быть закрыт;
- отсутствие яркого контрового, бокового света и теней;
- расстояние между зрачками на изображении должно составлять не менее 120 пикселей.

Примеры качественных и некачественных лицевых биометрических данных указаны на рисунке 9.



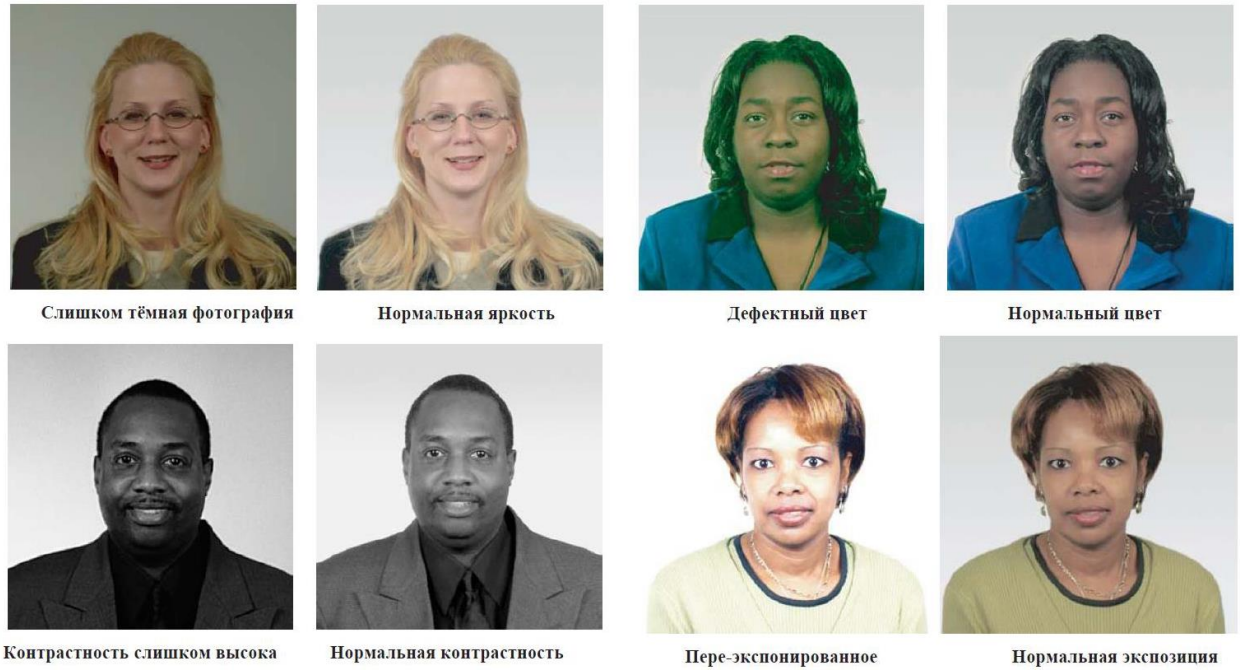


Рисунок 9 – Примеры качественных и некачественных лицевых биометрических данных

9 Информационная безопасность

Требования, к защите информации при работе с персональными данными установлены Указанием Банка России и ПАО «Ростелеком» от 09.07.2018 № 4859-У/01/01/782-18 «О перечне угроз безопасности, актуальных при обработке, включая сбор и хранение, биометрических персональных данных, их проверке и передаче информации о степени их соответствия предоставленным биометрическим персональным данным гражданина Российской Федерации в государственных органах, банках и иных организациях, указанных в абзаце первом части 1 статьи 14.1 Федерального закона от 27 июля 2006 года № 149-ФЗ «Об информации, информационных технологиях и о защите информации», в единой биометрической системе», Федеральным законом №152-ФЗ от 27 июля 2006 года «О персональных данных» и действующими нормативными (правовыми) актами ФСБ России и ФСТЭК России.

Особое внимание стоит обратить на возможные пути реализации банками требований к защите информации по классу КВ2:

- Самостоятельное проектирование и внедрение HSM и системного программного обеспечения (СПО) для подписи банками. Этот вариант предполагает, что банк самостоятельно разработает необходимое решение на основании Указания Банка России и ПАО «Ростелеком» от 09.07.2018 № 4859-У/01/01/782-18, обеспечит его встраивание и самостоятельную сертификацию.

- Использование типового решения по информационной безопасности. Данный вариант предполагает внедрение типового программно-аппаратного комплекса по обеспечению информационной безопасности, в состав которого входят необходимые компоненты, включая СПО и HSM с проведенными тематическими исследованиями и положительным заключением ФСБ России о корректности встраивания СКЗИ.

Для обеспечения целостности передаваемых биометрических персональных данных банкам необходимо получить квалифицированный сертификат ключа проверки электронной подписи класса КВ2 в ФГБУ НИИ «Восход».

10 Нормативные и полезные ссылки

При разработке настоящего документа были использованы нормы, требования и рекомендации, приведенные в следующих законодательных, нормативных правовых и иных актах и документах:

[1] - Регламент использования Единой биометрической системы (последняя версия размещается по адресу https://bio.rt.ru/upload/iblock/525/Reglament-ispolzovaniya-Edinoy-biometricheskoy-sistemy-_Versiya-1.7-ot-13.08.2018_.pdf);

[2] - Методические рекомендации по работе с СМЭВ 3.x (размещаются по адресу https://smev3.gosuslugi.ru/portal/ в разделе «Технологические стандарты и рекомендации»);

[3] - Методические рекомендации по работе с ЕСИА (актуальная версия размещается по адресу http://minsvyaz.ru/ru/documents/6186/);

[4] - Методические рекомендации по работе с ЕБС (актуальная версия документа размещается по адресу https://bio.rt.ru/documents/basic/);

[5] - Приказ Минкомсвязи России от 25.06.2018 № 321 «Об утверждении порядка обработки, включая сбор и хранение, параметров биометрических персональных данных в целях идентификации, порядка размещения и обновления биометрических персональных данных в единой биометрической системе, а также требований к информационным технологиям и техническим средствам, предназначенным для обработки биометрических персональных данных в целях проведения идентификации» (размещается по адресу: https://digital.gov.ru/ru/documents/6214/);

Приложение 1. To be: Процесс регистрации клиента в ЕСИА и ЕБС

Предусловия и целевое время

1. Протестировано и готово к работе: оборудование банка для сбора биометрических данных, сетевое взаимодействие с ЕБС.
2. Сотрудник банка прошел инструктаж по регистрации клиентов в ЕСИА и ЕБС, а также получил практические навыки работы с оборудованием для сбора биометрических данных в ЕБС.
3. Сотрудник банка имеет необходимые роли в ЕСИА, «привязан» к центру регистрации в ЕСИА.
4. В отделении банка распечатаны необходимые справочные материалы о порядке регистрации в ЕБС и памятка по удаленной идентификации

1. Идентификация и/или поиск клиента – 60 сек.
2. Регистрация нового клиента (при необходимости) – 300 сек.
3. Подписание согласия на сбор биометрических данных клиентом – 60 сек.

4.Фотографирование и запись голоса – 120 сек.
5. Поиск учетной записи в ЕСИА (от момента направления банков сведений до получения ответа) – 10 сек. (сейчас 20-30 сек)
6. Регистрация биометрических данных (от момента направления банков сведений до получения ответа) – 15 сек. (сейчас 30-40 сек)

Клиент (ФЛ)

1. ФЛ в терминале электронной очереди выбрал услугу – «Биометрия -> Единая биометрическая система» и получил талон
3. Клиент предоставляет информацию о себе (паспорт)
8. Клиент предоставляет контактную информацию информацию о себе, в том числе подписывает согласие на обработку ПДН в банке
11. Клиент подписывает документы
14. Клиент подписывает согласие на обработку ПДН в банке, получает памятку
16. Клиент предоставляет контактную информацию о себе (номер телефона/e-Mail, при необходимости) и СНИЛС при наличии
31. Клиент, уведомлён, что без СНИЛС регистрация невозможна
32. Клиент уведомлён о необходимости обновить данные телефона и/или email в ЕСИА для получения уведомлений
45. Клиент, уведомлён, регистрация биометрических данных невозможна из-за неработоспособности оборудования
46. Информирование клиента о подтверждении записи в ЕСИА
47. Клиенту, направлен пароль для первого входа в ЕСИА
48. Клиент, уведомлён, что подтверждение учетной записи не возможно. Необходимо самостоятельно в ЕСИА обновить контакт на актуальный
56. Информирование клиента об ошибке при проверки его данных в МВД или ПФР
57. Информирование об успешной регистрации в ЕБС
58. Информирование об ошибке при регистрации в ЕБС

Обслуживание завершено
Обслуживание завершено
ЕСИА, Портал Госуслуг, СМС, EMAIL
СМС, EMAIL
ЕСИА, Портал Госуслуг, СМС, EMAIL
ЕСИА, Портал Госуслуг, СМС, EMAIL, моб. приложение Госуслуг, ЛК на Bio.rt.ru
ЕСИА, Портал Госуслуг, СМС, EMAIL, моб. приложение Госуслуг, ЛК на Bio.rt.ru

Сотрудник банка

2. Запрос паспорта ФЛ
4. Поиск клиента
Клиент найден?
Нет
Согласен стать Клиентом?
нет
да
Да
5. Проверить данные клиента, при необходимости обновить. (В том числе согласие на обработку данных в банке)
7. Ввод информации о Клиенте
10. Подписать документы о банковском обслуживании
13. Сбор согласия на обработку ПДн для банка, ЕСИА и ЕБС (в бумажном), передать памятку
15. Поиск учетной записи в ЕСИА (по ФИО, серии/номеру паспорта, номеру телефона + email (если имеется) + СНИЛС (если имеется)
15.1. Поиск учетной записи в ЕСИА (по ФИО, серии/номеру паспорта, СНИЛС)
Да
Есть у клиента СНИЛС?
нет
17. Фотографирование лица
19. Запись голоса
нет (многократно)
нет
да
Успешно?
Подтверждение невозможно
Информирование Клиента об ошибке проверки в ПФР
Информирование клиента об ошибке, предложите прийти позже после устранения ошибки
Информирование клиента о статусе выполнения операции
9. Проверить согласно внутренним инструкциям и зарегистрировать клиента
нет
да
Прошла Проверка?
6. Обновить данные (при необходимости)
12. Клиент зарегистрирован
нет (многократно)
18. Проверка ВКК банка полученного фотоизображения
Успешно?
нет
да
20. Проверка ВКК полученной записи голоса
Совпали ФИО, паспорт, телефон/email?
да
нет
25. Совпали только ФИО и паспорт
26. Совпали только ФИО и телефон/email
44. Сохранить OID
50. Направить биометрические данные с OID в ЕБС
Информирование о статусе выполнения операции
Информирование статусе выполнения операции
Нет, (многократно) повторите сбор
Нет
Успешно?
да
55. Получен ответ от ЕБС
21. Поиск учетной записи в ЕСИА (УЗ), данные подгружаются из ИС банка
Найдена подтверждённая запись?
нет
да
Совпали ФИО, паспорт, телефон/email?
да
нет
Найдена стандартная запись?
да
Нет (поиск без СНИЛС)
Нет (при поиске со СНИЛС)
27. Совпали только ФИО и паспорт
28. Совпали только ФИО и телефон/email
Информирование о статусе выполнения операции
Информирование о статусе выполнения операции
51. Подписание данных с использование м HSM
Найдена упрощенная запись?
да
нет

Информационная система Банка

СМЭВ

22. Запрос на поиск УЗ (и признак согласия)
24. Получен ответ от ЕСИА
29. Запрос на обновление паспорта и подтверждение записи
31. Запрос на подтверждение стандартной записи
33. Получен ответ от ЕСИА
34. Запрос на регистрацию учетной записи
38. Дополнение данных и подтверждение упрощенной записи
42. Получен ответ от ЕСИА
43. Информирование об ошибке
52. Запрос на регистрацию/обновление биометрических данных
54. Получен ответ от ЕБС

ЕСИА

23. Обработка запроса на поиск УЗ и направление ответа
30. Обновление данных в ЕСИА
32. Подтверждение стандартной записи в ЕСИА
35. Получение запроса на создание УЗ
37. Получение запроса на подтверждение упрощенной УЗ
39. Создание УЗ
Создание УЗ
36. Проверка в ПФР (выполняется через СМЭВ)
Проверка пройдена?
да
нет
Подтверждение УЗ
41. Изменение статуса УЗ на подтвержденную
да
Нет
40. Проверка в МВД*
Проверка пройдена?
Внесение статуса об успешной регистрации биометрических данных

ЕБС

нет
53. Проверка ВКК полученных Биометрических данных
Успешно?
да

** Возможна длительная проверка данных в МВД России (до 5 дней)*

Приложение 2. Этапы подключения кредитной организации к ЕБС

Основные этапы, в независимости от типа подключения, остаются неизменными, но есть и различия, которые будут выделены отдельно в этом разделе.

Для подключения к Единой Биометрической Системе (далее – ЕБС) кредитной организации необходимо выполнить следующие **12 этапов**:

Этап 1. Заключение оферты на удаленную идентификацию и на регистрацию в продуктивном контуре ЕБС

Для подключения к ЕБС необходимо ознакомиться с Регламентом Единой биометрической системы, который можно скачать на портале ЕБС, особое внимание следует уделить пунктам:

- 8.1 «Регистрация Участника биометрического взаимодействия и его ИС в роли Поставщика БДн/Потребителя БДн в тестовом контуре ЕБС»
- 6.1 «Общие положения»

В личном кабинете необходимо акцептовать оферты. В зависимости от роли организации, необходимо акцептовать одну или обе оферты:

- Для **Потребителя (Верификация)**

Публичная оферта «о заключении соглашения об оказании услуги по предоставлению информации о степени соответствия предоставленных клиентом — физическим лицом биометрических персональных данных биометрическим персональным данным клиента — физического лица, содержащимся в Единой биометрической системе»

- Для **Поставщика (Регистрация)**

Публичная оферта «о заключении соглашения об оказании услуги по сбору биометрических данных и их передаче в Единую биометрическую систему»

Этап 2. Получение тестового сертификата ключа электронной подписи информационной системы.

Для получения тестового сертификата ключа электронной подписи информационной системы, который потребуется для регистрации в системах заполните заявление на получение электронной подписи и направьте его в электронном виде на адрес Минкомсвязи РФ sd@sc.minsvyaz.ru.

Заполненное заявление можно скачать на портале ЕБС по ссылке ниже: http://bio.rt.ru/documents/basic/?SECTION_ID=193#

Этап 3. Регистрация Участника и/или ИС в ТСМЭВ 3.

Для регистрации Участника и/или информационной системы в ТСМЭВ 3, ответственным от кредитной организации необходимо изучить Приложение 3. Правила и процедуры работы в СМЭВ по Методическим рекомендациям версии 3.x п. 10.6.2 «Регистрация Участника и/или информационной системы в тестовой среде СМЭВ» [1]

Затем нужно заполнить и отправить в электронном виде на адрес Минкомсвязи sd@sc.minsvyaz.ru следующие заявки:

- Заполненная форма заявки на регистрацию Участника и/или информационной системы в СМЭВ 3.0;
- Подписанная Заявка на присоединение к Регламенту обеспечения предоставления государственных услуг и исполнения государственных функций в электронном виде.
- После получения одобрения Минкомсвязи, Вы будете подключены к тестовой СМЭВ.

Этап 4. Подключение к ТЕСИА и получение доступа к ВС ЕБС в ТСМЭВ.

Для подключения к ТЕСИА и получению доступа к ВС ЕБС в ТСМЭВ, кредитной организации необходимо выполнить следующие шаги:

а) Регистрация организации в промышленной ЕСИА и регистрация информационной системы в промышленной ЕСИА

Для регистрации организации в промышленной ЕСИА следует учесть, что Заявитель должен иметь средство квалифицированной подписи, выданное на его имя (**сертификат КЭП** содержит сведения о Заявителе и сведения о регистрируемом органе/организации). КЭП выдается в аккредитованном УЦ.

Регистрация организации выполняется самостоятельно на сайте ЕСИА (https://esia.gosuslugi.ru).

В качестве инструкции необходимо использовать Руководство пользователя ЕСИА, пункт 3.2 [2].

Регистрация информационной системы в промышленной ЕСИА выполняется самостоятельно на сайте ЕСИА (https://esia.gosuslugi.ru/console/tec).

В качестве инструкции необходимо использовать Руководство пользователя технологического портала ЕСИА, п. 3.1 [3].

b) Получение доступа к сервисам аутентификации ТЕСИА

Для получения доступа следует ознакомиться с Регламентом информационного взаимодействия Участников с Оператором ЕСИА, пунктом 9 [4].

После ознакомления, необходимо заполнить и отправить в электронном виде на адрес Минкомсвязи sd@sc.minsvyaz.ru следующие документы:

- Заполненная форма заявки на подключение, в соответствии с Приложением Е Регламента. Включая перечень скоупов, на которые запрашивается доступ: bio, ext_auth_result, openid.

Дополнительно требуется указать скоупы для получения необходимых персональных данных.

- Сертификат ИС, который был получен на этапе 1.

c) Получение доступа к ВС ТЕСИА (ЕСИА) на стороне ЕСИА

Для получения доступа следует ознакомиться с Регламентом информационного взаимодействия Участников с Оператором ЕСИА. После ознакомления нужно заполнить и отправить в электронном виде на адрес Минкомсвязи sd@sc.minsvyaz.ru заявку на подключение в соответствии с Приложением З Регламента.

Этап 5. Регистрация информационной системы в тестовом контуре ЕБС.

Для подключения к тестовому контуру ЕБС (ТЕБС), кредитной организации необходимо ознакомиться с Регламентом использования Единой биометрической системы, пунктом 8.1 [5].

После того, как вы ознакомитесь с информацией, нужно будет заполнить и отправить в электронном виде на техподдержку ЕБС support@bio.rt.ru следующие документы:

- Заполненная форма заявки на подключение в соответствии с Приложением А Регламента использования Единой биометрической системы.
- Сертификат ИС, который был получен на этапе 1.

Этап 6. Регистрация тестовой учетной записи (далее – УЗ) в ТЕСИА.

Тестовая учетная запись обязательна для дальнейшего тестирования кредитной организацией интеграции с ТЕБС.

Регистрацию учетной записи кредитной организации необходимо выполнить самостоятельно через ВС ТЕСИА в ТСМЭВ (код маршрутизации TESIA).

Этап 7. Тестирование ИС в ТЕБС

На полученную на этапе 6 тестовую учетную запись необходимо произвести:

- ***Для поставщика биометрии*** — успешную биометрическую регистрацию, используя созданные кредитной организацией информационные системы поставщика биометрии..
- ***Для потребителя биометрии*** — успешную биометрическую верификацию, используя созданные банком информационные системы потребителя .
- ***Поставщика и Потребителя биометрии*** — успешную биометрическую регистрацию и верификацию, используя созданные кредитной организацией информационные системы поставщика и потребителя биометрии.

Этап 8. Тестирование ВС ЕБС и ЕСИА в тестовом контуре СМЭВ 3 с эмулятором

Для продолжения регистрации в ЕБС, ознакомьтесь с Приложением 3 Правила и процедуры работы в СМЭВ по Методическим рекомендациям версии 3.x п. 10.9.1 «Тестирование ВС в роли Потребителя в тестовой среде СМЭВ» и выполнить тестирование ВС.

В регламенте ознакомьтесь со следующими процедурами:

- Универсальный вид сведений для приема заявлений на биометрическую регистрацию.
- Регистрация подтвержденной учетной записи в ЕСИА с отправкой пароля для первого входа в систему на контактные данные.
- Подтверждение личности гражданина РФ или иностранного гражданина в ЕСИА.
- Подтверждение учетной записи в ЕСИА, созданной на основе существующей упрощенной.
- Поиск учетной записи в ЕСИА.
- Удаление учетной записи в ЕСИА **(не обязательно).**

Кредитная организация проводит тестирование самостоятельно с эмулятором ТСМЭВ.

Для каждого вида сведений необходимо отправить эталонный запрос методом **SendRequest** в тестовой среде СМЭВ 3, добавив в него элемент **//TestMessage** в блок данных запроса (в элемент **//SenderProvidedRequestData**).

Получить ответ методом **GetResponse** и подтвердить получение ответа методом **Ack**.

Если у ВС зарегистрировано несколько тестовых сценариев, то необходимо провести тестирование всех тестовых сценариев данного ВС.

Бизнес-данные должны соответствовать формату, заданному в РП.

Необходимо сформировать сообщение на основании эталонных сообщений (ничего в них не менять и не вносить иных данных) и провести тестирование.

Результаты и дату тестирования необходимо сохранить.

Этап 9. Получение сертификата ключа электронной подписи информационной системы.

Для получения сертификата ключа электронной подписи, заполните заявление на получение электронной подписи и направьте его в электронном виде на адрес Минкомсвязи sd@sc.minsvyaz.ru.

Важно! Вы должны использовать сертификаты ключей подписей, изготовленные любым аккредитованным Минкомсвязью России удостоверяющим центром (http://e-trust.gosuslugi.ru/CA). Структура сертификата ключа ЭП-ОВ должна соответствовать Требованиям к единой структуре сертификата ключа проверки электронной подписи, утверждаемым ФСБ России в соответствии с Федеральным законом от 6 апреля 2011 года № 63-ФЗ «Об электронной подписи».

Этап 10. Регистрация Участника и/или ИС в продуктивной среде СМЭВ 3

Для регистрации Участника и/или информационной системы в ТСМЭВ 3, ответственным от кредитной организации необходимо изучить Приложение 3. Правила и процедуры работы в СМЭВ по Методическим рекомендациям версии 3.x п. 10.6.3 «Регистрация Участника и/или информационной системы в тестовой среде СМЭВ».

После ознакомления, необходимо заполнить и отправить в электронном виде на адрес Минкомсвязи sd@sc.minsvyaz.ru следующие заявки:

- Форма заявки на регистрацию Участника и/или информационной системы в СМЭВ 3.0;
- Сертификат ключа электронной подписи информационной системы в формате BASE 64, полученный на этапе 9.

Этап 11. Подключение к ЕСИА и получение доступа к ВС ЕБС в СМЭВ

Для подключения к ЕСИА и получению доступа к ВС ЕБС в СМЭВ, выполните следующие шаги:

а) Получите доступ к ВС ЕБС в продуктивной среде СМЭВ 3

Для получения доступа к ВС ЕБС,ознакомьтесь с Приложением 3 Правила и процедуры работы в СМЭВ по Методическим рекомендациям версии 3.x п. 10.8.3 «Получение доступа к Виду сведений в продуктивной среде СМЭВ в качестве Потребителя или к Виду сведений с типом «Рассылка».

Затем заполните форму заявки на предоставление доступа к ВС в СМЭВ 3 (в качестве потребителя ВС)» и отправьте в электронном виде на адрес Минкомсвязи sd@sc.minsvyaz.ru, каждая заявка подается отдельно для следующих ВС:

- Универсальный вид сведений для приема заявлений на биометрическую регистрацию
- Регистрация подтвержденной учетной записи в ЕСИА с отправкой пароля для первого входа в систему на контактные данные (https://smev3.gosuslugi.ru/portal/inquirytype_one.jsp?id=87015&zone=fed&page=1)
- Подтверждение личности гражданина РФ или иностранного гражданина в ЕСИА (https://smev3.gosuslugi.ru/portal/inquirytype_one.jsp?id=87011&zone=fed&page=1)
- Подтверждение учетной записи в ЕСИА, созданной на основе существующей упрощенной(https://smev3.gosuslugi.ru/portal/inquirytype_one.jsp?id=87033&zone=fed&page=1)
- Восстановление доступа к подтвержденной учетной записи в ЕСИА с выдачей пароля для входа
- (https://smev3.gosuslugi.ru/portal/inquirytype_one.jsp?id=87030&zone=fed&page=1)
- Поиск учетной записи в ЕСИА
- (https://smev3.gosuslugi.ru/portal/inquirytype_one.jsp?id=87013&zone=fed&page=1)

- Удаление учетной записи в ЕСИА (https://smev3.gosuslugi.ru/portal/inquirytype_one.jsp?id=87000&zone=fed&page=1)
- Обновление паспортных данных (https://smev3.gosuslugi.ru/portal/inquirytype_one.jsp?id=131864&zone=fed&page=1&dTest=true)

b) Получите доступ к сервисам аутентификации ЕСИА

Для получения доступа следует ознакомиться с Регламентом информационного взаимодействия Участников с Оператором ЕСИА п. 10.

После ознакомления заполните и отправьте в электронном виде на адрес Минсвязи sd@sc.minsvyaz.ru следующие документы:

- Форма заявки на подключение в соответствии с Приложением М Регламента. Включая перечень скоупов, на которые запрашивается доступ: **bio, ext_auth_result, openid.** Дополнительно требуется указать скоупы для получения необходимых персональных данных.
- Сертификат ИС, полученный на этапе 9.

c) Регистрация Центров обслуживания в ЕСИА

Для получения доступа ознакомьтесь с Регламентом информационного взаимодействия Участников с Оператором ЕСИА п. 14.

Регистрация ЦО выполняется организацией самостоятельно через веб-интерфейс ЕСИА (https://esia.gosuslugi.ru/console/tech).

Важно помнить, что в ВС ЕСИА введен обязательный контроль соответствия идентификатора ЦО и СНИЛС Оператора ЦО:

- В соответствии с методическими рекомендациями и Регламентом СМЭВ 3 запросы ВС подписываются только КЭП Организации - владельца ЦО, а не КЭП должностного лица. И для идентификации оператора в состав запросов ВС введен обязательный параметр - СНИЛС Оператора, по которому ЕСИА определяет принадлежность Оператора к ЦО;
- Контроль осуществляется на основании Постановления Правительства Российской Федерации от 25 января 2013 г. № 33 «Об использовании простой электронной подписи при оказании государственных и муниципальных услуг»

и Постановления Правительства Российской Федерации от 9 февраля 2012 г. № 111.

Проверка принадлежности Оператора ЦО к конкретному ЦО делается в соответствии с указанными НПА и не противоречит им.

Таким образом оператор ЦО должен осуществить привязку к ЦО, от имени которого будет выполняться отправка запросов к ВС ЕСИА, в технологическом портале ЕСИА в соответствии с РП http://minsvyaz.ru/ru/documents/4545/.

Этап 12. Регистрация в продуктивной среде ЕБС

Для подключения к ЕБС кредитной организации необходимо ознакомиться с Регламентом Единой биометрической системы, который можно скачать на портале ЕБС, особое внимание следует уделить пунктам:

- **8.1** «Регистрация Участника биометрического взаимодействия и его ИС в роли Поставщика БДн/Потребителя БДн в тестовом контуре ЕБС»
- **8.2** «Регистрация Участника биометрического взаимодействия и его ИС в роли Поставщика БДн/Потребителя БДн в продуктивном контуре ЕБС»

После ознакомления, необходимо заполнить и отправить в электронном виде на техподдержку ЕБС support@bio.rt.ru следующие документы:

- Номера оферт (если выбрана одна роль и подписана одна оферта, то один номер)
- Заполненная форма заявки на подключение в соответствии с Приложением Б Регламента использования Единой биометрической системы.
- Сертификат ИС, который был получен на этапе 9.