

**Государственная информационная система «Единая система
идентификации и аутентификации физических лиц с использованием
биометрических персональных данных»
(ГИС ЕБС)**

**Методические рекомендации
по использованию сервиса биометрической верификации
для руководителей проектов**

Версия 1.1
на 28 листах

Москва 2024

Содержание

1. Введение	9
2. Нормативные ссылки.....	10
3. Описание процесса биометрической верификации	13
4. Требования для инициации процедуры подключения к ЕБС	17
4.1. Активация сервиса биометрической верификации.....	17
4.2. Организация защищенного канала связи	19
5. Сценарии работы процесса биометрической верификации.....	21
5.1. Процесс подключение опции входа с помощью биометрии.	21
5.2. Возможный сценарий услуги с помощью биометрии.	22
6. Разработка раздела сайта, посвященного взаимодействию с ЕБС	25
6.1. Рекомендации по разработке раздела сайта	25
6.2. Порядок регистрации в ЕБС	25
7. Уведомление о запуске продукта представителей ЦБТ для размещения продукта в каталог услуг сайта ЕБС и МП «Госуслуги Биометрия»	27

Список терминов сокращений

Термин	Определение
Аутентификация	Совокупность мероприятий по проверке лица на принадлежность ему идентификаторов посредством сопоставления их со сведениями о лице, которыми располагает лицо, проводящее аутентификацию, и установлению правомерности владения лицом идентификаторами посредством использования аутентифицирующих признаков в рамках процедуры аутентификации, в результате чего лицо считается установленным
БД	База данных
Биометрическая верификация (аутентификация 1 к 1)	Процесс подтверждения биометрического заявления при сравнении
Биометрические данные (БДн)	Биометрический образец или совокупность биометрических образцов на любой стадии обработки, например, биометрический контрольный шаблон, биометрическая проба, биометрический признак или биометрическое свойство
Биометрическая проба	Биометрический образец или набор биометрических признаков, введённый в алгоритм для использования в качестве объекта сравнения с биометрическим контрольным шаблоном (биометрическими контрольными шаблонами)
Биометрическая система	Система, предназначенная для биометрического распознавания людей, основанного на их поведенческих и биологических характеристиках
Биометрический контрольный шаблон (БКШ)	Один или более хранимых биометрических шаблонов, относящихся к субъекту биометрических данных и используемых в качестве объекта сравнения
Биометрический образец (БО)	Аналоговое или цифровое представление биометрических характеристик, предшествующее извлечению биометрических признаков

Термин	Определение
Биометрический признак	Цифровое представление информации (числа или метки), извлечённое из биометрических образцов и используемое для сравнения
Биометрический шаблон	Набор хранимых биометрических признаков, сравниваемых непосредственно с биометрическими признаками биометрической пробы
ГИС ЕБС, ЕБС, или государственная информационная система Единая биометрическая система	Единая биометрическая система - Государственная информационная система «Единая система идентификации и аутентификации физических лиц с использованием биометрических персональных данных», которая содержит биометрические персональные данные физических лиц, векторы единой биометрической системы и иную предусмотренную в соответствии с частью 16 статьи 4 Федерального закона №572-ФЗ информацию, которая используется в целях осуществления идентификации, аутентификации с использованием биометрических персональных данных физических лиц, а также в иных правоотношениях в случаях, установленных законодательством Российской Федерации, и оператором которой является определенная Правительством Российской Федерации организация
ЕСИА	Федеральная государственная информационная система «Единая система идентификации и аутентификации в инфраструктуре, обеспечивающей информационно-технологическое взаимодействие информационных систем, используемых для предоставления государственных и муниципальных услуг в электронной форме», обеспечивающая санкционированный доступ к информации, содержащейся в информационных системах

Термин	Определение
«Живость» (Liveness)	Признаки жизни субъекта, выявленные анатомическими характеристиками, произвольными реакциями, физиологическими функциями, добровольными реакциями или поведением субъекта
ИС	Информационная система
ИС Поставщика БДн	Информационная система организации, зарегистрированная в ЕБС, и имеющая возможность осуществлять сбор и предоставление БДн для биометрической регистрации
ИС Потребителя БДн	Информационная система организации, зарегистрированная в ЕБС, и имеющая возможность осуществлять сбор и предоставление БДн для биометрической верификации
Коммерческая биометрическая система (КБС)	Система, получающая/деактивирующая БКШ от ЕБС в процессе выгрузки для использования в бизнес-процессе
Конечный пользователь, Пользователь ЕБС	Человек, взаимодействующий с биометрической системой с целью регистрации или идентификации его личности
ЛК	Личный кабинет
МП	Мобильное приложение
Мэтчинг (связывание)	Процедура в ЕБС по связыванию различных учетных записей ФЛ (УЗ различных IDP) между собой на основании данных для мэтчинга (Hash ПДн/OID ЕСИА/СНИЛС). Мэтчинг производится после регистрации УЗ и создания профиля в ЕБС
ПДн	Персональные данные
Поставщик БДн (ЕБС)	Участник биометрического взаимодействия, имеющий право и осуществляющий регистрацию Пользователей в ЕБС.

Термин	Определение
Потребитель БДн (ЕБС)	Участник биометрического взаимодействия, имеющий право и осуществляющий удаленную идентификацию Пользователей с использованием верификации биометрических данных в ЕБС.
Простая электронная подпись (ПЭП)	Электронная подпись, которая посредством использования кодов, паролей или иных средств подтверждает факт формирования электронной подписи определенным лицом, согласно статье 5 федерального закона от 06.04.2011 г. №63-ФЗ «Об электронной подписи».
Удаленная идентификация	Идентификация пользователей, в рамках требований Федерального закона от 07.08.2001 №115-ФЗ «О противодействии легализации (отмыванию) доходов, полученных преступным путём, и финансированию терроризма», осуществляемая по удалённым каналам связи, без визита пользователя в офис кредитной организации
Усиленная квалифицированная электронная подпись (УКЭП, КЭП)	Самый надежный вид электронной подписи, равносильный собственноручной подписи владельца (Федеральный закон от 06.04.2011 №63-ФЗ).
Усиленная неквалифицированная электронная подпись (УНЭП)	Аналог собственноручной подписи на бумажном документе, может применяться для любых типов документов, за исключением тех, которые оформляются только на бумажном носителе или с использованием УКЭП.
Участник БВ	Участник биометрического взаимодействия (юридическое лицо), владелец информационной системы, зарегистрированной в ЕБС и имеющей возможность использовать БДн из ЕБС, аккредитованная коммерческая биометрическая система или региональный сегмент ЕБС

Термин	Определение
Учетная запись (УЗ)	Совокупность данных о пользователе, необходимая для его опознавания (аутентификации) и предоставления доступа к его личным данным, настройкам и сервисам
ФГИС ЕСИА, ЕСИА	Федеральная государственная информационная система «Единая система идентификации и аутентификации в инфраструктуре, обеспечивающей информационно-технологическое взаимодействие информационных систем, используемых для предоставления государственных и муниципальных услуг в электронной форме», обеспечивающая санкционированный доступ к информации, содержащейся в информационных системах
ID	Уникальный идентификатор учётной записи в ИС
Web (Веб) приложение	Клиент-серверное приложение, в котором клиентом выступает интернет браузер, а сервером — интернет-сервер

1. Введение

ГИС ЕБС — это государственная цифровая платформа для удаленной идентификации и аутентификации, которая позволяет предоставлять новые цифровые услуги для граждан дистанционно в любое время и в любом месте. Одни из сервисов, который предоставляется ГИС ЕБС, является сервис биометрической верификации.

В настоящем документе даны рекомендации по организации процесса биометрической верификации со ссылками на применимые положения нормативных актов.

Основные положения об осуществлении биометрической верификации с использованием ГИС ЕБС содержатся в статье 10 (осуществление аутентификации с использованием ГИС ЕБС) Федерального закона от 29.12.2022 №572-ФЗ «Об осуществлении идентификации и (или) аутентификации физических лиц с использованием биометрических персональных данных, о внесении изменений в отдельные законодательные акты Российской Федерации и признании утратившими силу отдельных положений законодательных актов Российской Федерации».

Подробная информация по подключению к сервису биометрической верификации представлена в Регламенте Государственной информационной системы «Единая система идентификации и аутентификации физических лиц с использованием биометрических персональных данных (ГИС ЕБС)», опубликованном по адресу <https://ebs.ru/documents> в разделе «Основные», и в разделе 4 настоящего документа.

Подробное описание программных интерфейсов, организации процесса биометрической верификации, взаимодействия между Участником БВ и сервисом биометрической верификации представлено в Методических рекомендациях по использованию сервиса биометрической верификации (для разработчиков), размещенных по адресу <https://ebs.ru/documents> в разделе «Основные».

2. Нормативные ссылки

При разработке настоящих Методических рекомендаций были использованы нормы и требования, содержащиеся в следующих нормативно-правовых актах:

1. Федеральный закон от 07.08.2001 № 115-ФЗ «О противодействии легализации (отмыванию) доходов, полученных преступным путем, и финансированию терроризма» (далее - Федеральный закон от 07.08.2001 № 115-ФЗ);

2. Федеральный закон от 27.07.2006 №152-ФЗ «О персональных данных» (далее - Федеральный закон от 27.07.2006 №152-ФЗ);

3. Федеральный закон от 27.07.2010 № 210-ФЗ «Об организации предоставления государственных и муниципальных услуг» (далее - Федеральный закон от 27.07.2010 № 210-ФЗ);

4. Федеральный закон от 06.04.2011 № 63-ФЗ «Об электронной подписи» (далее - Федеральный закон от 06.04.2011 № 63-ФЗ);

5. Федеральный закон от 27.12.2019 № 476-ФЗ «О внесении изменений в Федеральный закон «Об электронной подписи» и статью 1 Федерального закона «О защите прав юридических лиц и индивидуальных предпринимателей при осуществлении государственного контроля (надзора) и муниципального контроля» (далее - Федеральный закон от 27.12.2019 № 476-ФЗ);

6. Федеральный закон от 29.12.2020 № 479-ФЗ «О внесении изменений в отдельные законодательные акты Российской Федерации» (далее – Федеральный закон от 29.12.2020 № 479-ФЗ);

7. Федеральный закон от 29.12.2022 № 572-ФЗ «Об осуществлении идентификации и (или) аутентификации физических лиц с использованием биометрических персональных данных, о внесении изменений в отдельные законодательные акты Российской Федерации и признании утратившими силу отдельных положений законодательных актов Российской Федерации» (далее - Федеральный закон от 29.12.2022 № 572-ФЗ);

8. Постановление Правительства Российской Федерации от 28.11.2011 № 977 «О федеральной государственной информационной системе «Единая система идентификации и аутентификации в инфраструктуре, обеспечивающей информационно-технологическое взаимодействие информационных систем, используемых для предоставления государственных и муниципальных услуг в электронной форме» (далее – Постановление Правительства РФ от 28.11.2011 №977);

9. Постановление Правительства Российской Федерации от 10.07.2013 № 584 Об использовании федеральной государственной информационной системы «Единая система идентификации и аутентификации в инфраструктуре, обеспечивающей информационно-технологическое взаимодействие информационных систем, используемых для предоставления государственных и муниципальных услуг в электронной форме» (далее – Постановление Правительства РФ от 10.07.2013 №584);

10. Постановление Правительства Российской Федерации от 30.06.2018 г. № 772 «Об определении состава сведений, размещаемых в единой информационной системе персональных данных, обеспечивающей обработку, включая сбор и хранение, биометрических персональных данных, их проверку и передачу информации о степени их соответствия предоставленным биометрическим персональным данным физического лица, включая вид биометрических персональных данных, а также о внесении изменений в некоторые акты Правительства Российской Федерации» (далее – Постановление Правительства РФ от 30.06.2018 № 772);

11. Постановление Правительства Российской Федерации от 28.12.2018 № 1703 «Об утверждении Правил предоставления оператором единой информационной системы персональных данных, обеспечивающей обработку, включая сбор и хранение, биометрических персональных данных, их проверку и передачу информации о степени их соответствия предоставленным биометрическим персональным данным физического лица, в Министерство внутренних дел Российской Федерации и Федеральную службу безопасности Российской Федерации сведений, содержащихся в указанной системе» (далее – Постановление Правительства РФ от 28.12.2018 № 1703);

12. Постановление Правительства Российской Федерации от 15.06.2022 № 1066 «О размещении физическими лицами своих биометрических персональных данных в единой информационной системе персональных данных, обеспечивающей обработку, включая сбор и хранение, биометрических персональных данных, их проверку и передачу информации о степени их соответствия предоставленным биометрическим персональным данным физического лица» (далее – Постановление Правительства РФ от 15.06.2022 № 1066);

13. Постановление Правительства Российской Федерации от 06.04.2023 № 552 «Об утверждении Правил рассмотрения обращения высшего исполнительного органа субъекта Российской Федерации об образовании регионального сегмента в составе единой биометрической системы, а также предложений уполномоченного органа в сфере идентификации и аутентификации физических лиц на основе биометрических персональных данных об образовании регионального сегмента в составе единой биометрической системы и об исключении регионального сегмента из состава единой биометрической системы» (далее – Постановление Правительства РФ от 06.04.2023 № 552);

14. Приказ Минцифры России от 17.04.2023 № 378 «Об утверждении методик проверки соответствия предоставленных биометрических персональных данных физического лица векторам единой биометрической системы и степени взаимного соответствия биометрических персональных данных и векторов единой биометрической системы, достаточной для проведения идентификации и (или) аутентификации» (далее – Приказ Минцифры от 17.04.2023 № 378);

15. Приказ Минцифры России от 12.05.2023 № 453 «О порядке обработки биометрических персональных данных и векторов единой биометрической системы в единой

биометрической системе и в информационных системах аккредитованных государственных органов, Центрального банка Российской Федерации в случае прохождения им аккредитации, организаций, осуществляющих аутентификацию на основе биометрических персональных данных физических лиц» (далее – Приказ Минцифры от 12.05.2023 № 453);

16. Приказ Минцифры России от 05.05.2023 № 445 «Об утверждении перечня угроз безопасности, актуальных при обработке биометрических персональных данных, векторов единой биометрической системы, проверке и передаче информации о степени соответствия векторов единой биометрической системы предоставленным биометрическим персональным данным физического лица в единой биометрической системе, а также актуальных при взаимодействии информационных систем государственных органов, органов местного самоуправления, Центрального банка Российской Федерации, организаций, за исключением организаций финансового рынка, индивидуальных предпринимателей, нотариусов с единой биометрической системой, с учетом оценки возможного вреда, проведенной в соответствии с законодательством Российской Федерации о персональных данных» (далее – приказ Минцифры от 05.05.2023 №445);

17. Приказ Минцифры России от 05.05.2023 № 446 «Об утверждении перечня угроз безопасности, актуальных при обработке биометрических персональных данных, векторов единой биометрической системы, проверке и передаче информации о степени соответствия векторов единой биометрической системы предоставленным биометрическим персональным данным физического лица в информационных системах организаций, осуществляющих аутентификацию на основе биометрических персональных данных физических лиц, за исключением организаций финансового рынка, и единой биометрической системы, а также актуальных при взаимодействии информационных систем государственных органов, органов местного самоуправления, Центрального банка Российской Федерации, организаций, за исключением организаций финансового рынка, индивидуальных предпринимателей, нотариусов с указанными информационными системами, с учетом оценки возможного вреда, проведенной в соответствии с законодательством Российской Федерации о персональных данных» (далее – Приказ Минцифры от 05.05.2023 №446);

18. Приказ ФСБ России от 10.07.2014 № 378 «Об утверждении состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных с использованием средств криптографической защиты информации, необходимых для выполнения установленных Правительством Российской Федерации требований к защите персональных данных для каждого из уровней защищенности» (далее – Приказ №378);

3. Описание процесса биометрической верификации

В процессе биометрической верификации в ГИС ЕБС по полученному идентификатору выполняется поиск вектора ГИС ЕБС (БШ) пользователя с последующим сопоставлением найденных в ГИС ЕБС БШ пользователя с предъявляемым БО и определение степени соответствия (выполнется поиск по схеме «один к одному»). Данный протокол предназначен для проведения биометрической верификации (аутентификации 1 к 1) пользователя. Обработка БО в информационной системе организации осуществляется без их сохранения в информационной системе организации и средствах съема БО.





Процедура использования сервиса биометрической верификации предполагает, что необходимо предварительно связать учетные записи пользователей в ИС организации (id) и ГИС ЕБС на основании данных для связывания/мэтчинга (Hash ПДн/OID ЕСИА/СНИЛС). Для связывания используется метод регистрации без БО посредством REST API (см. раздел 2 Методических рекомендаций по использованию сервиса биометрической верификации для разработчиков¹). Происходит мэтчинг (в рамках аутентификации по ст. 10 Федерального закона №572-ФЗ) ранее зарегистрированной в ГИС ЕБС учетной записи пользователя, содержащей биометрические данные, и учетной записи пользователя в ИС организации, которая будет использоваться в процессе биометрической верификации. После успешного выполнения процедуры связывания/мэтчинга учетных записей пользователей, организация сможет использовать сервис биометрической верификации.²

Сервис биометрической верификации поддерживает различные варианты использования:

- 1) Верификация по одной или двум модальностям (фотоизображение и/или аудиозапись голоса)
- 2) Верификация с использованием различных проверок на «живость» (Liveness) (активный и/или пассивный лайвнес)
- 3) Верификация с использованием различных веб-интерфейсов (веб-формы ГИС ЕБС или форма съема БО организации)

Схемы процессов мэтчинга и биометрической верификации показаны на Рисунках 1 и 2.

Условные обозначения:

 Клиент	Физическое лицо
 Биометрия	Web-форма съема биометрии/Мобильное приложение
 ИС КА	Организация, предоставляющая услуги с использованием биометрии
 ГИС ЕБС	Единая биометрическая система

¹ Опубликованы по адресу <https://ebs.ru/documents> в разделе «Основные»

² Более подробно об использовании сервиса биометрической верификации см. Раздел 3 Методических рекомендаций по использованию сервиса биометрической верификации (для разработчиков), размещенных на портале <https://ebs.ru/documents> в разделе «Основные».



Рисунок 1 – Схема процесса прохождения связывания/мэтчинга УЗ.

Шаги процесса прохождения связывания/мэтчинга УЗ:

1. Клиент авторизуется в МП или на web-сайте ИС КА (Организации) и выбирает получение услуги с помощью биометрии.
2. Запрос согласия пользователя на предоставления биометрических персональных данных.
3. Предоставление пользователем согласия.
4. ИС КА отправляет запрос на связывание/мэтчинг учетных записей пользователя в ИС КА и ГИС ЕБС на основании Hash ПДн/OID ЕСИА/СНИЛС.
5. ГИС ЕБС передает в ИС КА результат выполнения метода регистрации без БО.
6. ГИС ЕБС передает в ИС КА результат связывания ранее зарегистрированной в ГИС ЕБС УЗ пользователя, содержащей БДн, и УЗ пользователя в ИС КА, которая будет использоваться для биометрической верификации.
7. ИС КА уведомляет клиента об успешном выполнении связывания УЗ и возможности использования услуги.

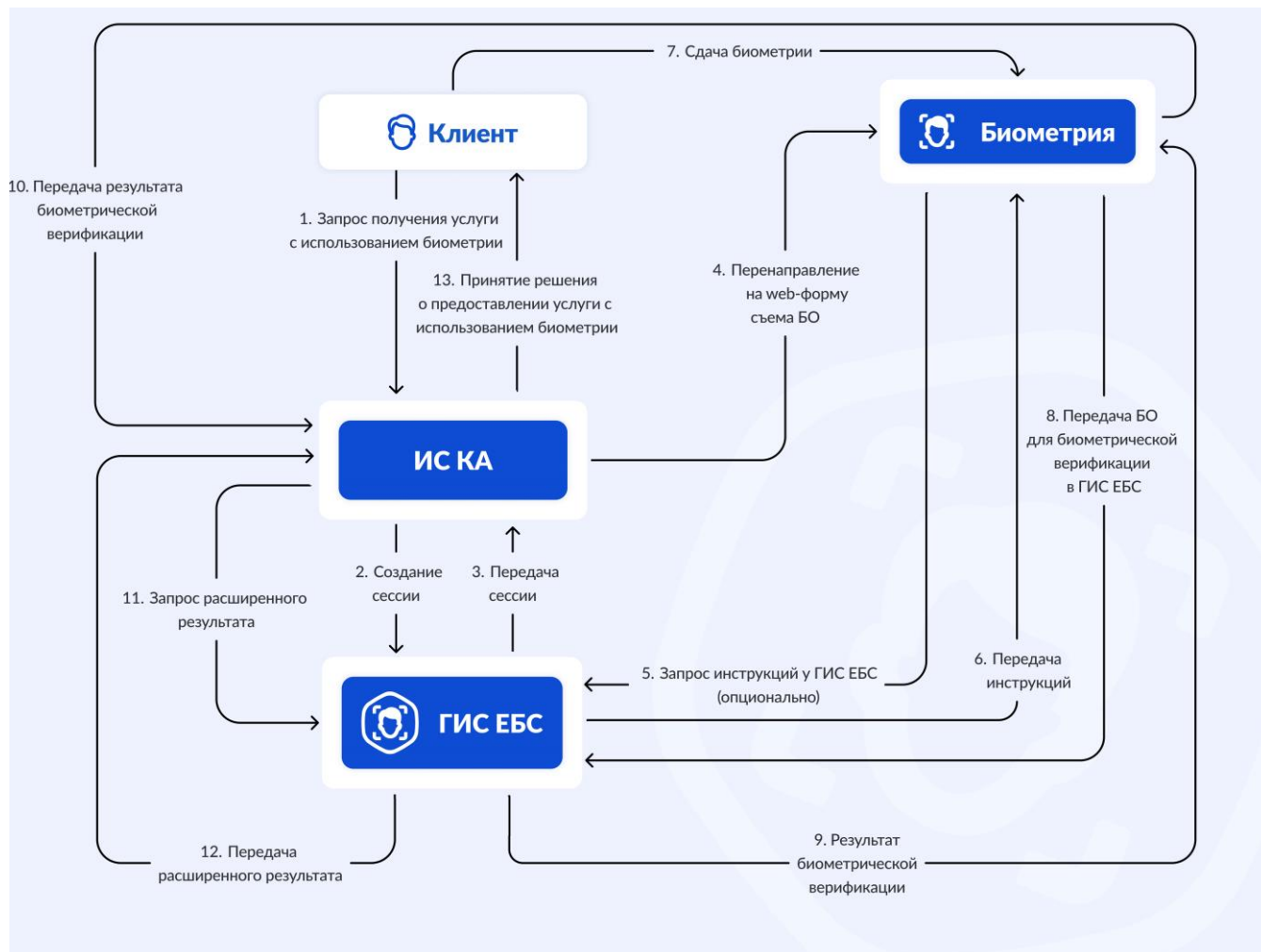


Рисунок 2 – Схема процесса прохождения биометрической верификации.

Шаги процесса прохождения биометрической верификации:

1. Клиент авторизуется в МП или на web-сайте ИС КА (Организации) и выбирает получение услуги с помощью биометрии.
2. ИС КА отправляет запрос на создание сессии в ГИС ЕБС.
3. ГИС ЕБС создаёт сессию и возвращает в ИС КА (и ссылку на web-форму ГИС ЕБС – опционально).
4. ИС КА перенаправляет клиента на страницу съема БО (web, webview или МП Госуслуги Биометрия).
5. В случае необходимости проверки на «живость», страница съема БО (или ИС КА запрашивает в ГИС ЕБС инструкции).
6. ГИС ЕБС передает инструкции.
7. Клиент сдаёт биометрию в соответствии с инструкциями на странице съема БО.
8. Страница съема БО передает данные в ГИС ЕБС для биометрической верификации.
9. ГИС ЕБС выполняет операцию биометрической верификации и возвращает результат (параметры `verify_token` – уникальный идентификатор, созданный ГИС ЕБС,

необходимый для получения расширенного результата верификации, и expired – время прекращения действия verify_token).

10. Страница съема БО передает результат биометрической верификации в ИС КА.
11. ИС КА запрашивает расширенный результат верификации в ГИС ЕБС (содержит степени схожести (общая и по каждой из модальностей)).
12. ГИС ЕБС возвращает расширенный результат верификации в ИС КА.
13. ИС КА принимает решение об оказании услуги клиенту.

Для каждой организации, подключающейся к сервису биометрической верификации, может быть настроен порог для отдачи результатов. В случае, если организация не намерена использовать уникальный порог, будет применяться значение по умолчанию, установленное в настройках ГИС ЕБС (степень схожести³ не ниже 99%). По вопросам настройки следует обращаться в службу Эксплуатации Оператора ГИС ЕБС по электронному адресу support@ebs.ru.

Более подробно реализация процесса биометрической верификации описана в Методических рекомендациях по использованию сервиса биометрической верификации, размещенных на сайте ГИС ЕБС <https://ebs.ru/documents/> в разделе «Основные».

³ Параметр степени схожести определяет, что помимо идентификаторов в результате будет присутствовать и степень схожести клиентов с переданным БО. Это количественный показатель, характеризующий схожесть извлеченных из образца признаков с шаблоном базы данных. Результаты, у которых схожесть ниже, не участвуют в выдаче.

4. Требования для инициации процедуры подключения к ГИС ЕБС

Порядок подключения сервиса биометрической верификации, в том числе требования по реализации мер защиты, информации, указаны в п. 4.1 и 4.2 настоящего документа, а также в п. 7.5, 9.1.1, 9.1.3, 9.2.1, 9.2.3, 12.1 Регламента информационного взаимодействия участников биометрических процессов с государственной информационной системой «Единая система идентификации и аутентификации физических лиц с использованием биометрических персональных данных» (ГИС ЕБС).⁴ Электронная почта для связи по всем вопросам подключения и регламентных взаимодействий: support@ebs.ru.

Организации также необходимо выполнить акцепт оферты «о заключении соглашения об оказании услуги по предоставлению информации о степени соответствия предоставленных клиентом - физическим лицом биометрических персональных данных векторам единой биометрической системы клиента – физического лица, содержащимся в Единой биометрической системе»⁵. Дополнительно могут применяться требования к соблюдению брендинга ГИС ЕБС, публикуемые по адресу <https://ebs.ru/documents> в разделе «Маркетинг».

4.1. Активация сервиса биометрической верификации

Для получения доступа к сервису биометрической верификации ИС Участника БВ необходимо выполнить следующие шаги согласно п. 7.5 Регламента Государственной информационной системы «Единая система идентификации и аутентификации физических лиц с использованием биометрических персональных данных (ГИС ЕБС)»:

1. Подать заявку на подключение IDP Участника БВ к тестовому контуру ГИС ЕБС (в соответствии с п. 9.1.1 Регламента Государственной информационной системы «Единая система идентификации и аутентификации физических лиц с использованием биометрических персональных данных (ГИС ЕБС)» и методическими рекомендациями по использованию сервиса биометрической верификации);

2. Подать заявку на подключение ИС к тестовому контуру ГИС ЕБС в роли Поставщика БДн (в соответствии с п. 9.1.2 Регламента Государственной информационной системы «Единая система идентификации и аутентификации физических лиц с использованием биометрических персональных данных (ГИС ЕБС)» и методическими рекомендациями по использованию сервиса биометрической верификации);

3. Подать заявку на подключение ИС к тестовому контуру ГИС ЕБС в роли Потребителя БДн (в соответствии с п. 9.1.3 Регламента Государственной информационной

⁴ Опубликован по адресу <https://ebs.ru/documents> в разделе «Основные»

⁵ Доступна организациям в ЛК ЮЛ в разделе «Оферты», а также опубликована на портале ГИС ЕБС (<https://ebs.ru/documents>)

системы «Единая система идентификации и аутентификации физических лиц с использованием биометрических персональных данных (ГИС ЕБС)» и методическими рекомендациями по использованию сервиса биометрической верификации);

4. Заключить соглашение с Оператором ГИС ЕБС⁶, предоставив информацию и документы, подтверждающие соответствие Участника БВ требованиям части 7 статьи 10 Федерального закона от 29.12.2022 г. № 572-ФЗ;

5. Организовать защищенный канал в соответствии с разделом 12.1.1 Регламента Государственной информационной системы «Единая система идентификации и аутентификации физических лиц с использованием биометрических персональных данных (ГИС ЕБС)»;

6. Подать заявку на подключение IDP Участника БВ к продуктивному контуру ГИС ЕБС (в соответствии с п. 9.2.1 Регламента Государственной информационной системы «Единая система идентификации и аутентификации физических лиц с использованием биометрических персональных данных (ГИС ЕБС)» и методическими рекомендациями по использованию сервиса биометрической верификации⁷);

7. Подать заявку на подключение ИС к продуктивному контуру ГИС ЕБС в роли Поставщика БДн (в соответствии с п. 9.2.3 и п. 12 Регламента Государственной информационной системы «Единая система идентификации и аутентификации физических лиц с использованием биометрических персональных данных (ГИС ЕБС)»). Для корректной работы в продуктивных контурах ЕСИА, СМЭВ, ГИС ЕБС, необходимо выполнить организацию защищенного канала.

8. Подать заявку на подключение ИС к продуктивному контуру ГИС ЕБС в роли Потребителя БДн (в соответствии с п. 9.2.3 и п. 12 Регламента Государственной информационной системы «Единая система идентификации и аутентификации физических лиц с использованием биометрических персональных данных (ГИС ЕБС)»).⁸

В рамках сервиса биометрической верификации не происходит регистрации БО. Однако для связывания учетных записей пользователей используется программный интерфейс регистрации пользователя без предоставления БО, для которого необходимо подключение в роли Поставщика БДн.

⁶ Необходимо провести акцепт оферты «о заключении соглашения об оказании услуги по предоставлению информации о степени соответствия предоставленных клиентом - физическим лицом биометрических персональных данных векторам единой биометрической системы, содержащимся в Единой биометрической системе», опубликованной на портале ГИС ЕБС (<http://ebs.ru>).

⁷ Опубликованы на <https://ebs.ru/documents>

⁸ Для корректной работы в продуктивных контурах ЕСИА, СМЭВ, ГИС ЕБС, необходимо выполнить организацию защищенного канала.

4.2. Организация защищенного канала связи

При работе с персональными данными должны выполняться требования к защите информации, установленные Федеральным законом от 29.12.2022 №572-ФЗ, Федеральным законом от 27.07.2006 №152-ФЗ и действующими подзаконными нормативно-правовыми актами.

Информационное взаимодействие ИС Участников БВ с ГИС ЕБС должно осуществляться по защищенному каналу связи с применением средств криптографической защиты информации, сертифицированных ФСБ России.

В процессе обработки БДн, их проверки и передачи сведений/информации о степени их соответствия предоставленным БДн физического лица между ИС Участников БВ и ГИС ЕБС должны быть обеспечены целостность и достоверность такой информации с применением средств ЭП соответствующего класса (определенных в соответствии с Приказом Минцифры от 05.05.2023 №445 и другими действующими Приказами Минцифры России), совместимых с ПАКМ «КриптоПро HSM». Реализация в ИС Участников БВ мер защиты информации осуществляется Участниками БВ самостоятельно или с привлечением организаций-лицензиатов по соответствующим видам работ. Для обеспечения целостности передаваемых биометрических персональных данных организациям необходимо получить квалифицированный сертификат ключа проверки электронной подписи класса КСЗ (в соответствии с Моделью угроз и нарушителя безопасности информации ГИС ЕБС 2023 года и Приказом ФСБ России от 10.07.2014 №378).

Для обеспечения конфиденциальности передаваемой информации при взаимодействии с клиентом рекомендуется применять СКЗИ класса не ниже КС1 на стороне клиента и не ниже КСЗ на стороне организации (в соответствии с Приказами Минцифры от 05.05.2023 №446, от 05.05.2023 №445, и соответствующими мерами защиты, определенными в приложении к приказу ФСБ России № 378). Взаимодействие с целью передачи биометрических персональных данных осуществляется по защищенной сети передачи данных со СМЭВ/ЕСИА/ГИС ЕБС, с применением безопасного протокола SSL/TLS для доступа в сеть «Интернет», виртуальных частных сетей (VPN), криптографических алгоритмов (шифрование) для каналов связи, с использованием СКЗИ, сертифицированных ФСБ, и других способов организации защищенных соединений.

Особое внимание стоит обратить на возможные пути реализации организациями требований по электронной цифровой подписи:

- Самостоятельное проектирование и внедрение HSM и системного программного обеспечения (СПО) для подписи организациями. Этот вариант предполагает, что организация самостоятельно разработает необходимое решение в соответствии с требованиями ФСБ России (или на основании Указания Банка России от 16.12.2021 № 6017-У – для банков, а также в соответствии с применимыми Приказами Минцифры, в том числе Приказом от 05.05.2023 №445), обеспечит его встраивание и самостоятельную сертификацию.

- Использование типового решения по информационной безопасности⁹. 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 и о соответствии системному проекту.

Для организации защищенного канала связи между ИС Участников БВ и ГИС ЕБС необходимо:

1. Обеспечить защиту канала связи с использованием СКЗИ производителей АО «Инфотекс» и (или) ООО «Код безопасности» класса не ниже КСЗ, принадлежащих Участнику БВ на праве собственности или на ином законном основании, или использовать СКЗИ класса КСЗ, применяемое оператором ИС Участников БВ для информационного взаимодействия со СМЭВ и (или) ЕСИА в соответствии с документом «Требования к сети передачи данных участников информационного взаимодействия»¹⁰ (в целях обеспечения совместимости средств СКЗИ, применяемых Участниками БВ, могут использоваться только совместимые с используемыми в ГИС ЕБС, сертифицированные СКЗИ класса КСЗ, предназначенные для защиты информации при передаче по каналам связи, производства компаний «Код Безопасности» (АПКШ «Континент») или «ИнфоТеКС» («ViPNet Coordinator»)).

2. Заключить договор с ПАО «Ростелеком» об организации защищенного канала связи со СМЭВ/ЕСИА/ЕБС, для чего обратиться в Ситуационный центр электронного правительства по адресу <https://sc.digital.gov.ru/> (не требуется при наличии на момент подключения ИС Участников БВ к ГИС ЕБС защищенного канала связи со СМЭВ и (или) ЕСИА).

3. Направить запрос на организацию защищенного канала связи с ГИС ЕБС по адресу kriptokanal@rt.ru.

Подробное описание шагов по организации защищенного канала связи и требования к классам применяемых СКЗИ ГИС ЕБС приведены в п. 12.1.1 Регламента Государственной информационной системы «Единая система идентификации и аутентификации физических лиц с использованием биометрических персональных данных (ГИС ЕБС)».

⁹ Информация о типовом решении по информационной безопасности доступна на сайте ГИС ЕБС по адресу <https://ebs.ru/security/>.

¹⁰ Актуальный документ «Требования к сети передачи данных участников информационного обмена» доступен на портале Единой системы контекстных справок (ЕСКС) <https://info.gosuslugi.ru/> (раздел «Документация, СМЭВ 3»).

5. Сценарии работы процесса биометрической верификации

5.1. Процесс подключение опции входа с помощью биометрии

Для предоставления возможности получения сервисов и/или услуг клиентом с использованием биометрии организации необходимо:

- Получить согласие пользователя на обработку персональных данных: клиент может дать согласие посредством УКЭП, УНЭП Госключ, ПЭП ЕСИА, подписью на бумажном документе, а также другими способами, не противоречащими статьям 3-4 Федерального закона №572-ФЗ, включая подтверждение согласия на экране терминала или другого пользовательского устройства. Организация по собственному усмотрению определяет какой способ или способы получения согласия будут у нее реализованы.
- Узнать идентификатор пользователя в ЕСИА (oid) и передать его или СНИЛС в ГИС ЕБС вместе с идентификатором пользователя в своей системе.

Возможный сценарий подключения опции входа с помощью биометрии (в случае подписания согласия ПЭП ЕСИА) изображен на Рисунке 2.

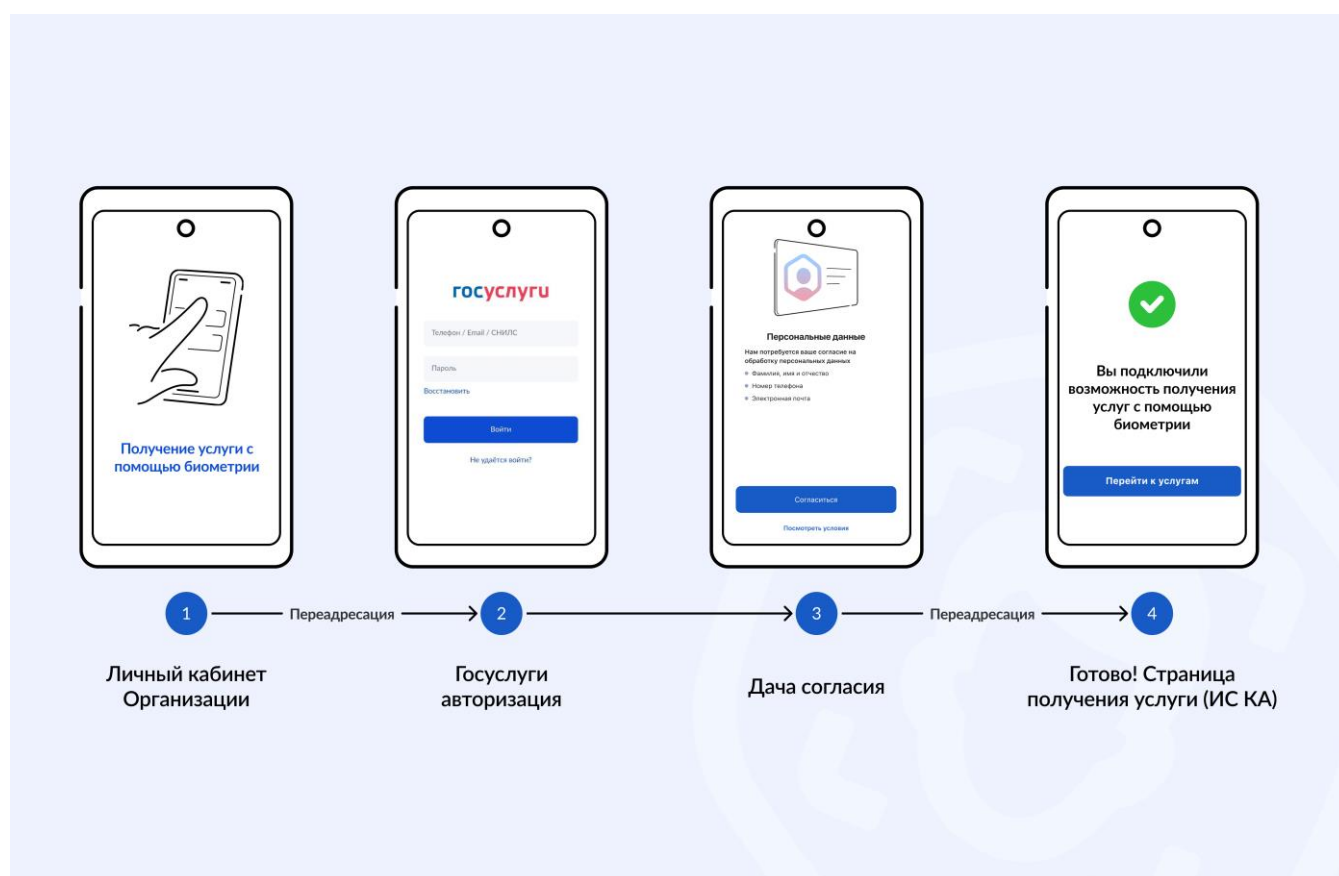


Рисунок 3 – Возможный сценарий подключение опции входа с помощью биометрии (в случае подписания согласия ПЭП ЕСИА)

Один из возможных сценариев:

Предварительные условия: У пользователя есть аккаунт на Госуслугах и сдана биометрия в ГИС ЕБС.

Шаг 1. Пользователь авторизуется в ЛК Организации и выбирает получение услуги с помощью биометрии.

Шаг 2. МП Организации (или web) перенаправляет Пользователя на старницу аутентификации Госуслуг.

Шаг 3. Пользователь авторизуется в Госуслугах и даёт согласие на обработку биометрических персональных данных посредством ПЭП ЕСИА.

Шаг 4. У Пользователя отображается страница с информацией о том, что он подключил возможность получения услуг с помощью биометрии.

5.2. Возможный сценарий услуги с помощью биометрии

Одним из возможных сервисов является использование биометрии в качестве второго фактора (как на портале Госуслуги, пример представлен на Рисунке 3) или авторизация в ЛК с помощью биометрии (пример на Рисунке 4).

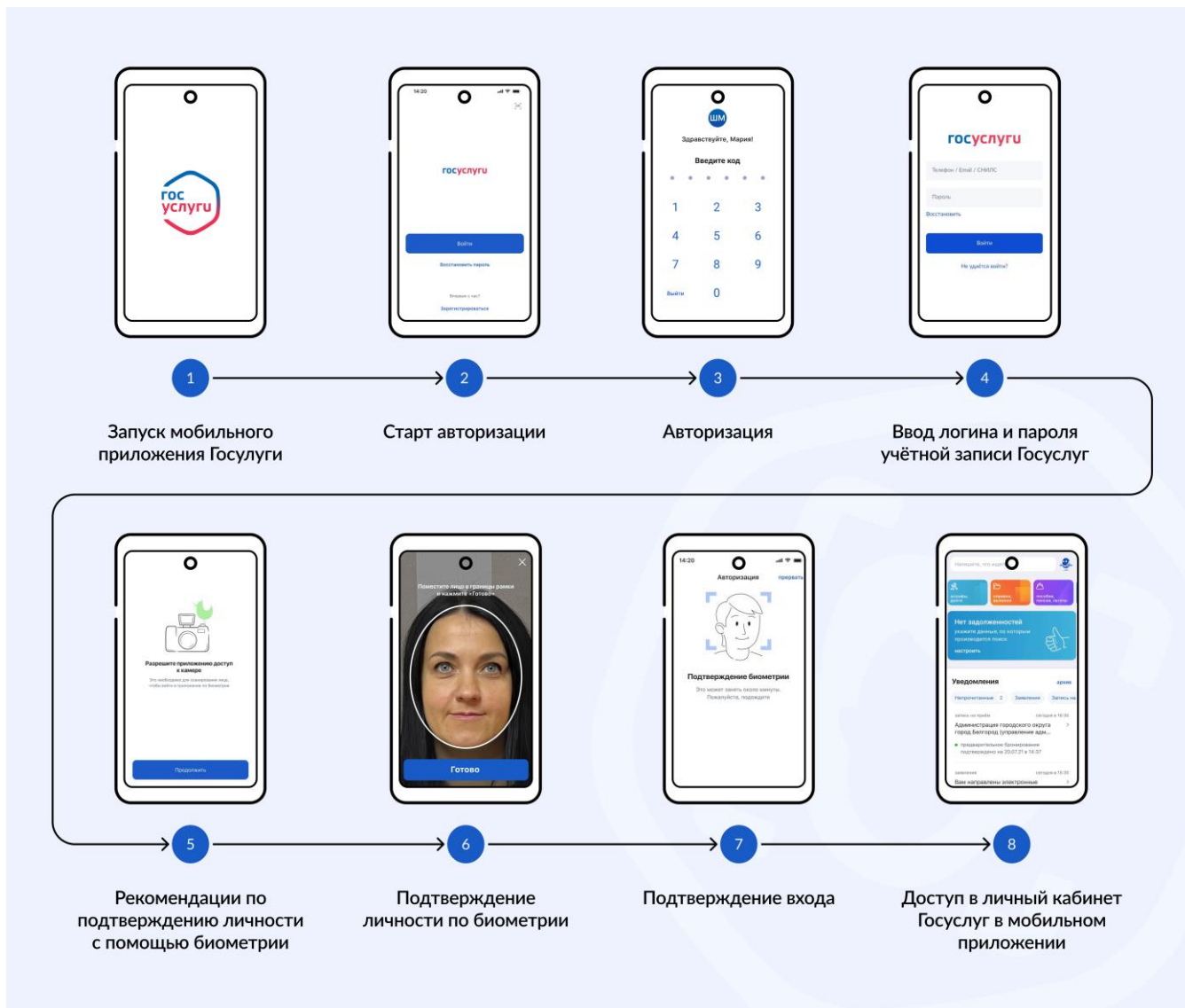


Рисунок 4 – Сценарий использования биометрии для авторизации в качестве второго фактора

Один из возможных сценариев авторизации с помощью биометрии:

Предварительные условия: У пользователя есть подтвержденная учетная запись на Госуслугах, зарегистрирована биометрия в ГИС ЕБС и подключен вход по биометрии в Организации.

Шаг 1. Пользователь хочет авторизоваться в ЛК Организации с помощью биометрии.

Шаг 2. МП Организации (или web) отображает Пользователю страницу съема биометрии.

Шаг 3. Пользователь сдает биометрию.

Шаг 4. МП Организации (или web) пускает Пользователя в личный кабинет.

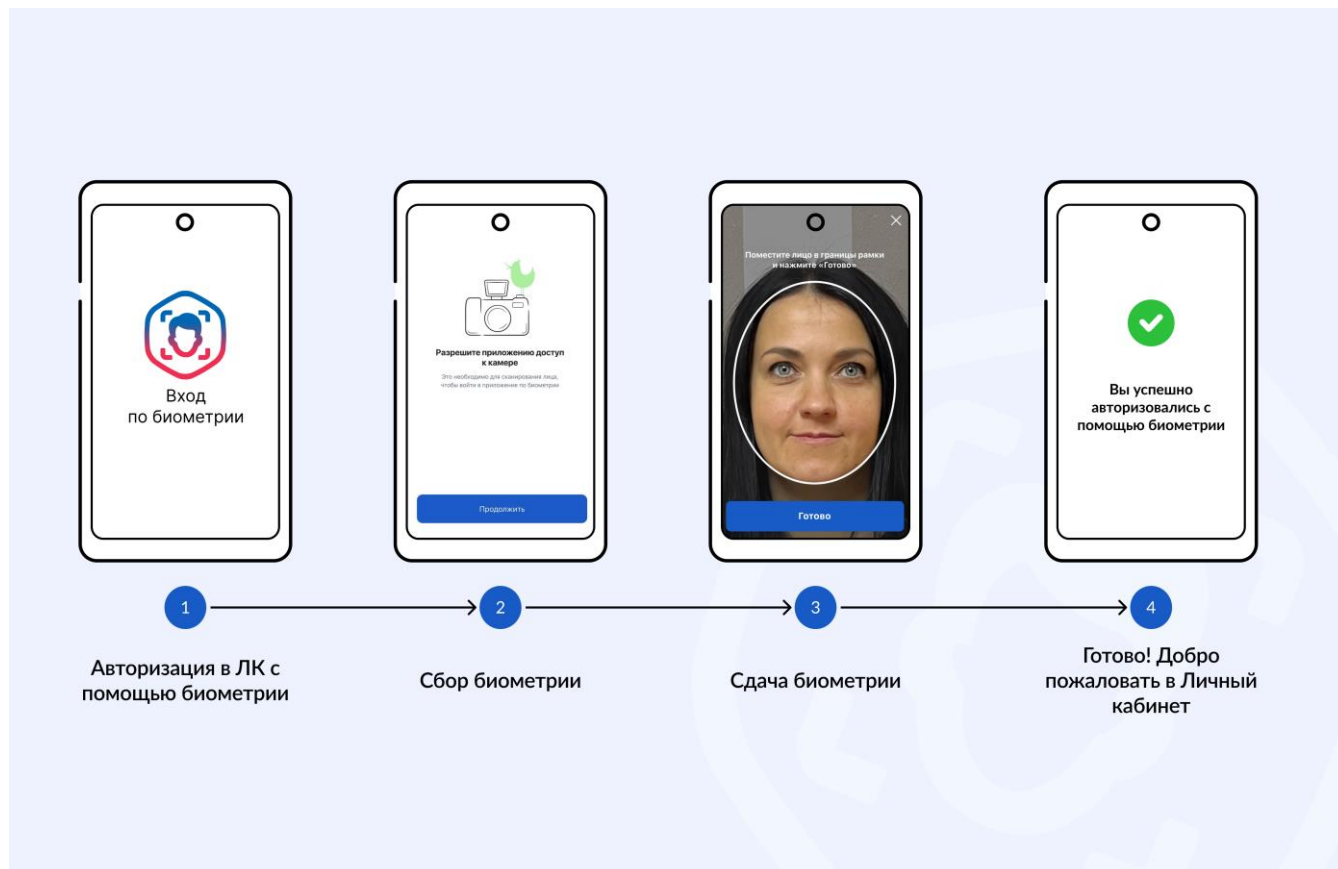


Рисунок 5 – Сценарий входа с помощью биометрии

6. Разработка раздела сайта, посвященного взаимодействию с ГИС ЕБС

На сайте организации должен быть разработан раздел, посвященный взаимодействию с ГИС ЕБС. Страница о ГИС ЕБС в выпадающем главном меню должна быть размещена не дальше второго уровня.

6.1. Рекомендации по разработке раздела сайта

В разделе взаимодействия с ГИС ЕБС должно быть отражено:

- Назначение и преимущества использования ГИС ЕБС (<https://ebs.ru/citizens/>);
- Услуги ГИС ЕБС (<https://ebs.ru/services/>);
- Порядок регистрации и саморегистрации в ГИС ЕБС со ссылками на портал (https://ebs.ru/citizens#how_register*) и карту отделений банка, регистрирующих биометрию.

Текстовое наполнение раздела должно быть согласовано с Департаментом внешних коммуникаций АО «ЦБТ» по электронной почте pr@ebs.ru.

На сайт может быть установлен футер/баннер с логотипом ГИС ЕБС в соответствии с гайдлайном по дизайну (доступен по адресу <https://ebs.ru/documents/> в разделе «Маркетинг»). Футер/баннер должен вести на раздел сайта, посвященный взаимодействию с ГИС ЕБС.

6.2. Порядок регистрации в ГИС ЕБС

На сайте организации в разделе, посвященном взаимодействию с ГИС ЕБС, должна быть информация для клиента об использовании биометрии, в том числе:

1. Информация о преимуществах использования биометрии:
 - Клиент с помощью биометрии может получить лучшие предложения;
 - Клиент может получить услуги в любом месте;
 - Клиент может получить услуги в любое время;
 - Клиент получает услуги без оформления бумажных документов.
2. Информация о процессе регистрации:
 - Клиенту нужно прийти в отделение банка или воспользоваться мобильным приложением «Госуслуги Биометрия» для регистрации в ГИС ЕБС;
 - Карта отделений, где клиент может пройти регистрацию;
 - Список документов, которые необходимо иметь при себе для регистрации в ГИС ЕБС (паспорт гражданина РФ и СНИЛС);
 - Клиент может проверить статус своей учетной записи в ЛК участника взаимодействия на сайте Госуслуг (<https://lkuv.gosuslugi.ru/>), в МП Госуслуги, на сайте ГИС ЕБС, в МП «Госуслуги Биометрия».
3. Информация о получении услуг организации дистанционно:

- Услуги, доступные с использованием биометрии;
- Инструкция по оформлению услуги с помощью компьютера;
- Инструкция по оформлению услуги с помощью телефона;
- Ссылка на МП организации;
- Ссылка на МП «Госуслуги Биометрия».

7. Уведомление о запуске продукта представителей ЦБТ для размещения продукта в каталог услуг сайта ГИС ЕБС и МП «Госуслуги Биометрия»

После запуска продукта организации необходимо уведомить представителей ЦБТ по почте marketing@ebs.ru о готовности и представить свой клиентский путь. Представители ЦБТ должны в течение двух рабочих дней ответить на запрос.

Уведомление должно содержать информацию:

- Название организации и продукта;
- Ссылка на продукт, доступный через использование биометрии на сайте организации или в МП с возможность протестировать работу сервиса;
- Основные условия предоставления услуги, которые могут быть выведены в каталог услуг на портале ebs.ru и в МП «Госуслуги Биометрия»;
- Категория услуги (например, «Счет» или «Кредитная карта»);
- Краткие условия предоставления услуги – кратко в формате каталога <https://ebs.ru/services/>;
- Подробные условия предоставления услуги, в случае, когда того требует Федеральный закон от 03.03.2006 №38-ФЗ «О рекламе»;
- Логотип организации в формате *.svg.

После проверки продукт организации будет добавлен в каталог услуг на портале ebs.ru и в МП «Госуслуги Биометрия» на соответствующих приложениях платформ.