

**Единая система идентификации и аутентификации физических лиц с
использованием биометрических персональных данных**

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

Версия 1.0

на 28 листах

Москва 2024

Изменения документа

Версия	Дата	Автор	Изменение
1.0	19.01.2024	С. Гаврилов	Создание документа

Оглавление

Глоссарий	4
1 ВВЕДЕНИЕ	10
2 Нормативные ссылки	11
3 Описание процесса биометрической идентификации.....	14
4 Порядок получения доступа ИС участника БВ к сервису биометрической идентификации	18
4.1 Активация сервиса биометрической идентификации.....	18
4.2 Организация защищенного канала связи	19
5 Сценарии работы процесса биометрической идентификации	23
5.1 Сценарий оплаты в браузере	23
5.2 Сценарий оплаты в терминале самообслуживания	25
6 Разработка раздела сайта, посвященного взаимодействию с ГИС ЕБС	26
6.1 Рекомендации по разработке раздела сайта.....	26
6.2 Порядок регистрации в ГИС ЕБС.....	26
7 Уведомление о запуске продукта представителей АО «ЦБТ» для размещения продукта в каталоге услуг сайта ГИС ЕБС и МП «Госуслуги Биометрия».....	28

Глоссарий

Термин	Описание
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
Биометрические данные (БДн)	Биометрический образец или совокупность биометрических образцов на любой стадии обработки, например, биометрический контрольный шаблон или биометрический признак.
Биометрическая верификация	Процесс подтверждения биометрического заявления при сравнении (аутентификация «один к одному»), в рамках которого производится сопоставление БКШ пользователя с предъявляемым БО и определение степени соответствия, а результат может использоваться как фактор аутентификации в ИС Участника БВ. Биометрическая верификация в рамках требований Федерального закона от 07.08.2001 г. №115-ФЗ входит в процедуру удаленной идентификации. Биометрическая верификация вне Федерального закона от 07.08.2001 г. №115-ФЗ производится для подтверждения личности с использованием Провайдера идентификации, отличного от ЕСИА.
Биометрическая идентификация	Процесс сравнения представленного биометрического образца с контрольной выборкой шаблонов (схема «один ко многим») с целью определения соответствия образца какому-либо из контрольных шаблонов в данной контрольной выборке для установления соответствующей шаблону личности
Биометрическая модель	Хранимая функция, созданная из биометрических данных (по ГОСТ ISO/IEC 2382-37-2016)

Биометрическая проба	Биометрический образец или набор биометрических признаков, введенный в алгоритм для использования в качестве объекта сравнения с биометрическим контрольным шаблоном (биометрическими контрольными шаблонами)
Биометрическая регистрация	Действия по созданию и сохранению записи данных биометрической регистрации в соответствии с правилами биометрической регистрации
Биометрический образец (БО)	Аналоговое/дискретное (рисунок, напечатанная на принтере фотография, виниловая пластинка, аудио компакт-диск и др.) или цифровое представление биометрических характеристик, предшествующее извлечению биометрических признаков
Биометрический признак	Цифровое представление информации (числа или метки), извлеченное из биометрических образцов и используемое для сравнения
Биометрический процессор	Обработчик запросов на выполнение биометрических операций
Биометрический шаблон (БШ)	Один или более хранимых биометрических шаблонов, относящихся к субъекту биометрических данных и используемых в качестве объекта сравнения
Биометрический контрольный шаблон (БКШ)	Один или более хранимых биометрических образцов, биометрических шаблонов или биометрических моделей, относящихся к субъекту биометрических данных и используемых в качестве объекта сравнения
Биометрический шаблон (биометрический вектор, биометрический ключ)	Набор хранимых биометрических признаков, сравниваемых непосредственно с биометрическими признаками биометрической пробы
Биометрическое взаимодействие (БВ)	Информационное взаимодействие с целью использования БДн из ЕБС
Биометрическое заявление	Заявление, что субъект сбора биометрических данных является или не является собственно источником установленного или неустановленного биометрического контрольного шаблона
Выгрузка векторов	Процедура выгрузки БШ в ИС Участника БВ

<p>Дистанционная (удаленная) идентификация</p>	<p>Идентификация физического лица в рамках требований Федерального закона от 7 августа 2001 г. №115-ФЗ «О противодействии легализации (отмыванию) доходов, полученных преступным путем, и финансированию терроризма», осуществляемая по удаленным каналам связи, без визита физического лица в офис кредитной организации</p>
<p>Единая биометрическая система (ЕБС, ГИС ЕБС)</p>	<p>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</p>
<p>Единая система идентификации и аутентификации (ЕСИА, ФГИС ЕСИА)</p>	<p>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»</p>
<p>«Живость» (Liveness)</p>	<p>Признаки жизни субъекта, выявленные анатомическими характеристиками, произвольными реакциями, физиологическими функциями, добровольными реакциями или поведением субъекта</p>
<p>Импорт БО</p>	<p>Процедура регистрации пользователей через API с передачей персональных данных и биометрических образцов из ИС организации, осуществляющей импорт данных.</p>

Информационная система контрагента (ИСКА)	Информационная система контрагента, осуществляющая сбор и отправку в ЕБС биометрических образцов клиента (регистрация биометрических образцов)
Коммерческая биометрическая система (КБС)	Система, получающая/деактивирующая БКШ от ЕБС в процессе выгрузки для использования в бизнес-процессе
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
Оператор Единой биометрической системы (Оператор ЕБС)	АО «ЦБТ», на основании Постановления Правительства Российской Федерации от 16.12.2022 № 2326.
Персональные данные (ПДн)	Персональные данные пользователя, обработка которых осуществляется в соответствии с требованиями Федерального закона от 27.07.2006 №152-ФЗ «О персональных данных»
Пользователь ГИС ЕБС, Пользователь	Человек, взаимодействующий с биометрической системой с целью биометрической регистрации и/или удаленной идентификации его личности в ГИС ЕБС
Поставщик БДн	Участник биометрического взаимодействия (юридическое лицо), владелец Информационной системы, зарегистрированной в ГИС ЕБС и имеющей возможность осуществлять сбор и предоставление БДн для биометрической регистрации
Потребитель БДн	Участник биометрического взаимодействия (юридическое лицо), владелец Информационной системы, зарегистрированной в ГИС ЕБС и имеющей возможность осуществлять использование БДн для предоставления услуг с использованием биометрии
Провайдер идентификации / Identity Provider (IDP)	Информационная система, отвечающая за поддержку и управление информацией об идентификации пользователей и обеспечивающая аутентификацию пользователей для других информационных систем.

<p>Региональный сегмент Единой биометрической системы</p>	<p>Элемент Единой биометрической системы, который содержит предусмотренную в соответствии с частью 16 статьи 4 и статьей 5 Федерального закона от 29.12.2022 №572-ФЗ информацию, оператором которого является орган исполнительной власти субъекта Российской Федерации или подведомственное ему государственное учреждение либо государственное унитарное предприятие, осуществляющие создание, развитие, модернизацию, эксплуатацию и иные полномочия оператора такого сегмента, который используется для осуществления аутентификации и в котором используются предназначенные для обработки биометрических персональных данных, векторов единой биометрической системы технические средства, в том числе программно-технические средства, и программы для электронных вычислительных машин.¹</p> <p>При подключении региональных сегментов к Единой биометрической системе следует руководствоваться теми же требованиями, которые применяются для подключения КБС.</p>
<p>СНИЛС</p>	<p>Страховой номер индивидуального лицевого счета, который присваивается каждому гражданину Социальным фондом России (СФР)</p>
<p>Участник БВ</p>	<p>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 Единой биометрической системы.</p>
<p>Учетная запись (УЗ)</p>	<p>Совокупность данных о пользователе, необходимая для его опознавания (аутентификации) и предоставления доступа к его личным данным, настройкам и сервисам</p>

¹ Применимо только для процессов выгрузки и импорта векторов.

hash ПДн	Однонаправленное преобразование персональных данных пользователя в битовое значение установленной длины, выполняемое определённым алгоритмом ЕСИА
OID, Open ID	Идентификатор Пользователя в IDP ЕСИА, требуется для сопоставления (мэтчинга) УЗ Пользователя в ЕБС

1 ВВЕДЕНИЕ

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

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

Основные положения об осуществлении биометрической идентификации с использованием ГИС ЕБС содержатся в статье 10 (осуществление аутентификации с использованием ГИС ЕБС) и статье 11 (использование ГИС ЕБС и ЕСИА при предъявлении документов, удостоверяющих личность ФЛ) 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 идентификации 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 идентификации, взаимодействия между Участником БВ и сервисом биометрической идентификации представлено в Методических рекомендациях по использованию сервиса биометрической идентификации (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 06.04.2011 № 63-ФЗ «Об электронной подписи» (далее - Федеральный закон от 06.04.2011 № 63-ФЗ);

4. 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);

5. 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);

6. 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);

7. 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);

8. 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);

9. 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);

10. Указание Банка России от 25.09.2023 № 6541-У «О перечне 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 финансового рынка, осуществляющих аутентификацию на основе биометрических персональных данных физических лиц, за исключением единой биометрической системы, а также актуальных при взаимодействии информационных систем организаций финансового рынка, иных организаций, индивидуальных предпринимателей....» (далее – Указание Банка России от 25.09.2023 №6541-У);

3 Описание процесса биометрической идентификации

Процесс биометрической идентификации представляет собой поиск пользователя по предоставленному БО среди биометрических данных пользователей, хранящихся в ГИС ЕБС (выполняется поиск по схеме «один ко многим»), с целью оказания услуг ИС КА. Обработка биометрических образцов в ИС КА осуществляется без их сохранения в ИС КА и средствах съема БО². Организация, подключенная к сервису биометрической идентификации, может идентифицировать своего клиента по БО и предоставить ему доступные услуги. Повышение скорости обслуживания достигается за счет того, что клиенту не нужно искать карты, пропуска или вводить пароль.

Процедура использования сервиса биометрической идентификации 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 4 Методических рекомендаций по использованию сервиса биометрической идентификации для разработчиков)³. 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 идентификации. После успешного выполнения процедуры связывания/мэтчинга учетных записей пользователей организация сможет использовать сервис биометрической идентификации.⁴

Результатом биометрической идентификации является:

- список кандидатов (идентификаторов пользователей в IDP ИС КА),
- степень схожести по каждому кандидату,
- результат проверки «живости» (Liveness) (при необходимости).

Схема процессов мэтчинга и биометрической идентификации представлены на Рисунках 1 и 2.

² В исполнение требований частей 7 и 9 статьи 14 Федерального закона №572-ФЗ, по истечении срока 10 суток Участник БВ (Поставщик БДн) обязан удалить хранимые им биометрические персональные данные с использованием метода многократного затирания файлов.

³ Опубликованы по адресу <https://ebs.ru/documents> в разделе «Основные»

⁴ Более подробно об использовании сервиса биометрической идентификации см. Раздел 5 Методических рекомендаций по использованию сервиса биометрической идентификации (для разработчиков), размещенных на портале <https://ebs.ru/documents> в разделе «Основные».

Условные обозначения:





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



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.

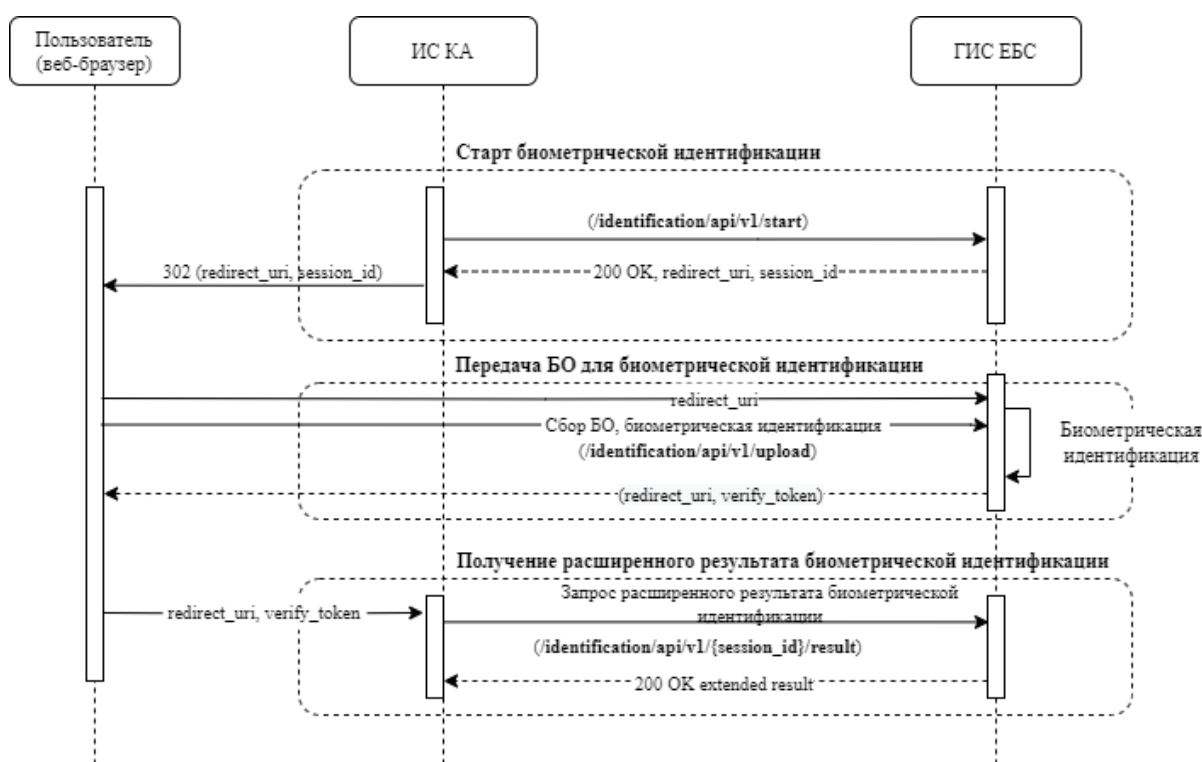


Рисунок 2 – Схема процесса биометрической идентификации

В состав сервиса биометрической идентификации входят следующие методы:

- Старт идентификации в ГИС ЕБС - для создания сессии биометрической идентификации Пользователя, зарегистрированного в ГИС ЕБС.
- Прием БО на биометрическую идентификацию - для получения БО на идентификацию и возврата результата биометрической идентификации.
- Получение расширенного результата биометрической идентификации - для предоставления ИС Поставщика БДн расширенного результата в случае успешной идентификации, включающего в себя значения степеней схожести по отдельным модальностям. Для этого ИС

Поставщика БДн формирует запрос к ГИС ЕБС с передачей информации о Пользователе.

Более подробно реализация процесса и программные интерфейсы сервиса биометрической идентификации описаны в Методических рекомендациях по использованию сервиса биометрической идентификации (для разработчиков), размещенных на портале <https://ebs.ru/documents> в разделе «Основные».

4 Порядок получения доступа ИС участника БВ к сервису биометрической идентификации

Порядок подключения сервиса биометрической идентификации, в том числе требования по реализации мер защиты информации, указаны в п. 4.1 и 4.2 настоящего документа, а также в п. 7.6, 9.1.1, 9.1.2, 9.2.1, 9.2.2, 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)⁵. 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»⁶. Дополнительно могут применяться требования к соблюдению брендинга ГИС ЕБС, публикуемые по адресу <https://ebs.ru/documents> в разделе «Маркетинг».

4.1 Активация сервиса биометрической идентификации

Для получения доступа к сервису биометрической идентификации ИС Участника БВ необходимо выполнить следующие шаги согласно п. 7.6 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 ГИС ЕБС);
2. Подать заявку на подключение ИС к тестовому контуру ГИС ЕБС в роли Поставщика БДн (в соответствии с п. 9.1.3 Регламента Государственной

⁵ Опубликован по адресу <https://ebs.ru/documents> в разделе «Основные»

⁶ Доступна организациям в ЛК ЮЛ в разделе «Оферты», а также опубликована на портале ГИС ЕБС (<https://ebs.ru/documents>)

информационной системы «Единая система идентификации и аутентификации физических лиц с использованием биометрических персональных данных (ГИС ЕБС)» и методическими рекомендациями ГИС ЕБС);

3. Заключить соглашение с Оператором ГИС ЕБС⁷, предоставив информацию и документы, подтверждающие соответствие Участника БВ требованиям статьи 10 Закона № 572-ФЗ;

4. 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)»;

5. 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 работе с ЕБС⁸);

6. 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.

4.2 Организация защищенного канала связи

При работе с персональными данными должны выполняться требования к защите информации, установленные Указанием Банка России от 25.09.2023 №6541-У, Федеральным законом от 29.12.2022 №572-ФЗ, Федеральным законом от 27.07.2006 №152-ФЗ и действующими нормативными (правовыми) актами ФСБ России, ФСТЭК России и Банка России.

⁷ 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 (<https://ebs.ru>).

⁸ Опубликованы на <https://ebs.ru/documents>

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 КС3 (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 КС3 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 25.09.2023 № 6541-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 НСМ 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.

⁹ Информация о типовом решении по информационной безопасности доступна на сайте 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»).

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)».

5 Сценарии работы процесса биометрической идентификации

Для получения возможности оказания услуг 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.

5.1 Сценарий оплаты в браузере

Одним из способов применения биометрической идентификации является оказание услуг с оплатой по лицу. Возможный сценарий оказания услуги с оплатой в браузере с помощью биометрии изображен на Рисунке 3.

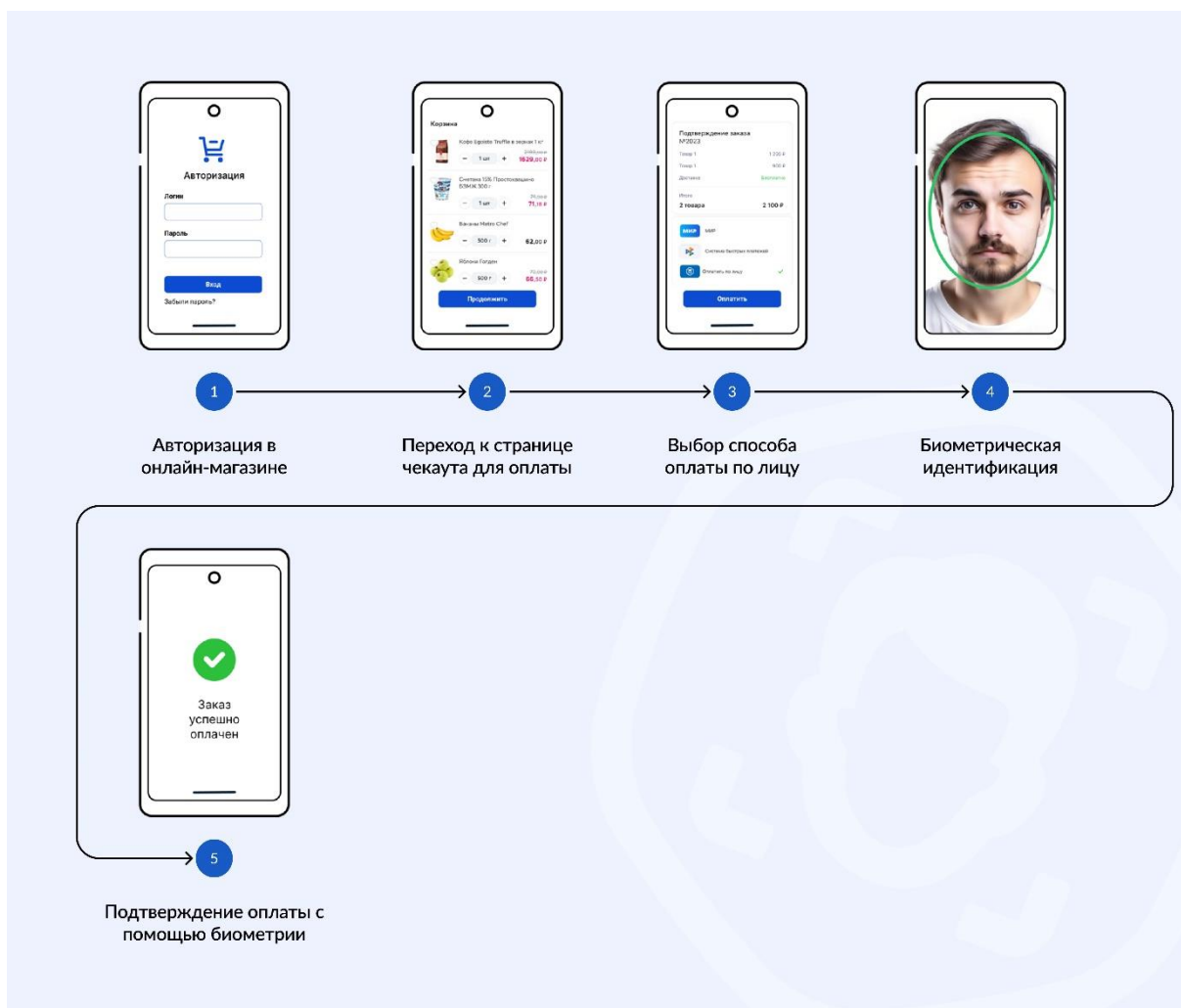


Рисунок 3 –Сценарий оказания услуги с оплатой в браузере с помощью биометрии

Предварительные условия: у Пользователя сдана биометрия (по модальности «лицо») в ГИС ЕБС.

Шаг 1. Пользователь авторизуется в онлайн-магазине через МП.

Шаг 2. Пользователь выбирает товары/услуги в корзину и переходит к странице чекаута для оплаты.

Шаг 3. Пользователь подтверждает оплату и выбирает способ оплаты по лицу.

Шаг 4. Производится сбор биометрии через web view, осуществляется биометрическая идентификация Пользователя.

Шаг 5. В браузере отображается успешное подтверждение оплаты с помощью биометрии.

5.2 Сценарий оплаты в терминале самообслуживания

Возможный сценарий оказания услуги с оплатой в терминале самообслуживания изображен на Рисунке 4.

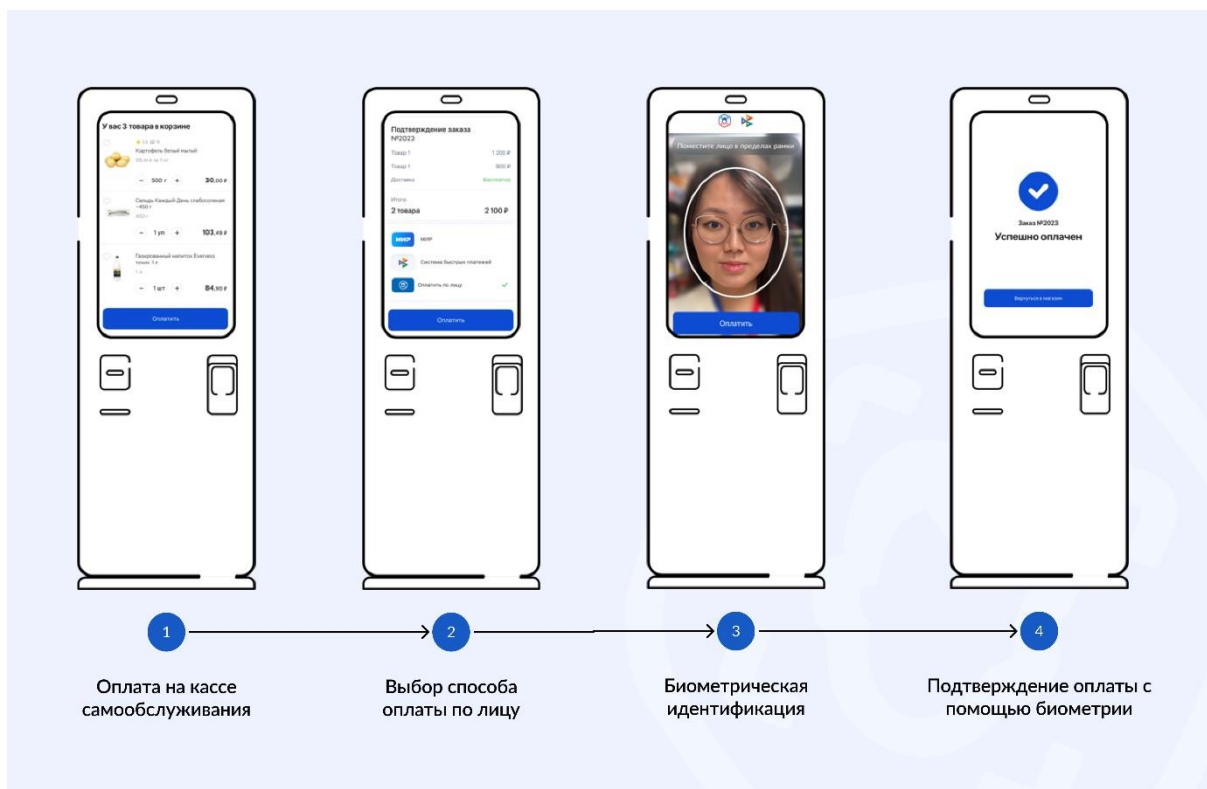


Рисунок 4 –Сценарий оказания услуги с оплатой в терминале самообслуживания

Предварительные условия: у Пользователя сдана биометрия (по модальности «фото») в ГИС ЕБС.

Шаг 1. Пользователь отсканировал товары в магазине на кассе самообслуживания и переходит к оплате покупок.

Шаг 2. Пользователь выбирает способ оплаты по лицу.

Шаг 3. Производится сбор биометрии через web view, осуществляется биометрическая идентификация Пользователя.

Шаг 4. В браузере отображается успешное подтверждение оплаты 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 содержаться информация для клиента об использовании биометрии, в том числе:

1. Информация о преимуществах использования биометрии:
 - Пользователь с помощью биометрии может получить лучшие предложения;
 - Пользователь может получить услуги в любом месте;
 - Пользователь может получить услуги в любое время;
 - Пользователь может получить услуги без оформления бумажных документов.
2. Информация о процессе регистрации:

- Пользователю нужно прийти в отделение банка или воспользоваться мобильным приложением «Госуслуги Биометрия» для регистрации в ГИС ЕБС;
- Карта отделений, где Пользователь может пройти регистрацию;
- Список документов, которые необходимо иметь при себе для регистрации в ГИС ЕБС (паспорт гражданина РФ и СНИЛС);
- Пользователь 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 АО «ЦБТ» для размещения продукта в каталоге услуг сайта ГИС ЕБС и МП «Госуслуги Биометрия»

После запуска продукта организации необходимо уведомить представителей АО «ЦБТ» по почте marketing@ebs.ru о готовности и представить свой клиентский путь. Представители АО «ЦБТ» должны в течение 2х 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 Госуслуги «Биометрия» с возможностью 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 приложению платформах.