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

Методические рекомендации по использованию сервиса проверки «живости» (Liveness) для руководителей проектов

Версия 1.0

на 27 листах

Москва 2024

Изменения документа

Версия	Дата	Автор	Изменение
1.0	02.07.2024	С. Гаврилов	Создание документа

Оглавление

Глоссарий 4

1 ВВЕДЕНИЕ 10

2 Нормативные ссылки 11

3 Описание сервиса для проверки «живости» (Liveness) 13

4 Порядок получения доступа ИС участника БВ к сервису проверки «живости» (Liveness) 16
4.1 Получение доступа к сервису проверки «живости» (Liveness) 16
4.2 Организация защищенного канала связи 18

5 Сценарии работы процесса проверки «живости» (Liveness) 21
5.1 Сценарий интеграции в терминалы и приложения кредитных организаций 21
5.2 Сценарий расширенного варианта прохождения теста CAPTCHA на сайтах в интернете 22

6 Разработка раздела сайта, посвященного взаимодействию с ГИС ЕБС 25
6.1 Рекомендации по разработке раздела сайта 25
6.2 Порядок регистрации в ГИС ЕБС 25

7 Уведомление о запуске продукта представителей АО «ЦБТ» для размещения продукта в каталоге услуг сайта ГИС ЕБС и МП «Госуслуги Биометрия» 25

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 персональные данные (БПДн), биометрические данные (БДн), биометрия	Сведения, которые характеризуют физиологические и биологические особенности человека (биометрический образец или совокупность биометрических образцов, биометрический признак или набор биометрических признаков), на основании которых можно установить его личность и которые в соответствии с частью 1 статьи 11 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» используются оператором для установления личности субъекта персональных данных.
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), вектор	Персональные данные, полученные в результате математического преобразования прошедших контроль качества биометрических персональных данных физического лица, содержащихся в ГИС ЕБС, которое произведено с использованием информационных технологий и технических средств, соответствующих требованиям 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» ФЗ и Приказа Министерства цифрового развития, связи и массовых коммуникаций Российской Федерации 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». Набор хранимых биометрических признаков, сравниваемых непосредственно с биометрическими признаками биометрической пробы
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
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
Дистанционная (удаленная) идентификация	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

Единая биометрическая система (ЕБС, ГИС ЕБС)	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
Единая система идентификации и аутентификации (ЕСИА, ФГИС 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»
«Живость» (Лайвнесс) / Liveness / витальность	Качество или признаки жизни субъекта, выявленные анатомическими характеристиками, непроизвольными реакциями, физиологическими функциями, добровольными реакциями или поведением субъекта
Импорт БО	Процедура регистрации пользователей через API с передачей персональных данных и биометрических образцов из ИС организации, осуществляющей импорт данных.
Информационная система контрагента (ИС КА)	Информационная система контрагента, осуществляющая сбор и отправку в ЕБС биометрических образцов физического лица (регистрация биометрических образцов)
Коммерческая биометрическая система (КБС)	Организация, осуществляющая аутентификацию на основе биометрических персональных данных физических лиц, владеющая информационными системами, обеспечивающими

	аутентификацию на основе биометрических персональных данных физических лиц, и (или) оказывающие услуги по аутентификации на основе биометрических персональных данных физических лиц, применяющая для этих целей векторы Единой биометрической системы и прошедшая аккредитацию в порядке, установленном в соответствии с Федеральным законом от 29.12.2022 №572-ФЗ
ЛК ЮЛ	Личный кабинет юридического лица на портале ГИС ЕБС https://ebs.ru/
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 ГИС 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.
СНИЛС	Страховой номер индивидуального лицевого счета, который присваивается каждому гражданину Социальным фондом России (СФР)
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 Единой биометрической системы.
Учетная запись (УЗ)	Совокупность данных о пользователе, необходимая для его опознавания (аутентификации) и предоставления доступа к его личным данным, настройкам и сервисам
ФЛ	Физическое лицо
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 информационная система, которая содержит БДПн ФЛ, векторы ГИС ЕБС и иную информацию, которая используется для осуществления идентификации и аутентификации с использованием БПДн ФЛ дистанционно в любое время и в любом месте. Одним из сервисов, который предоставляется ГИС ЕБС для использования биометрическими системами в процессах аутентификации (биометрической верификации и биометрической идентификации), является сервис проверки «живости» (Liveness).

Сервис проверки «живости» (Liveness) предназначен для использования в информационных системах различных организаций, подключенных к ГИС ЕБС, в целях повышения безопасности проведения аутентификации в КБС.

В настоящем документе даны рекомендации по организации подключения и использования сервиса проверки живости (Liveness), со ссылками на применимые положения нормативных актов.

Общие законодательные положения, применимые к процессам аутентификации (в том числе в которых используется сервис проверки живости (Liveness)), содержатся в статье 10 (осуществление аутентификации с использованием ГИС ЕБС) и статье 15 (обработка биометрических персональных данных вне 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».

Подробное описание программных интерфейсов, организации использования сервиса для проверки живости (Liveness), взаимодействия между Участником БВ и сервисом для проверки живости (Liveness) представлено в Методических рекомендациях по использованию сервиса для проверки живости (Liveness) (для разработчиков), размещенных по адресу https://ebs.ru/documents в разделе «Технические документы».

2 Нормативные ссылки

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

1. Федеральный закон от 27.07.2006 №152-ФЗ «О персональных данных» (далее - Федеральный закон от 27.07.2006 №152-ФЗ);
2. Федеральный закон от 06.04.2011 № 63-ФЗ «Об электронной подписи» (далее - Федеральный закон от 06.04.2011 № 63-ФЗ);
3. 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);
4. 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);
5. 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);

6. 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);

7. 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);

8. 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 сервиса для проверки «живости» (Liveness)

Сервис предназначен для использования результатов проверки «живости» в предоставляемых ИС КА сервисах при осуществлении аутентификации ФЛ.

Сервис выполняет по запросам ИС КА – Потребителей БДн проверку «живости» (Liveness) ФЛ по его БПДн, с последующим использованием результатов в клиентских путях и предоставляемых сервисах ИС КА. Это позволяет ИС КА – Потребителям БДн реализовывать различные клиентские пути, в рамках которых можно получать информацию по «живости» в любой требуемый для принятия решения (по предоставлению своих сервисов) момент.

Обработка биометрических образцов в ИС КА, осуществляющих аутентификацию на основе БПДн ФЛ с использованием сервиса проверки «живости» (Liveness), осуществляется без их сохранения в ИС КА и средствах съема БО.

Схема процесса проверки «живости» (Liveness) представлена на Рисунке 1.

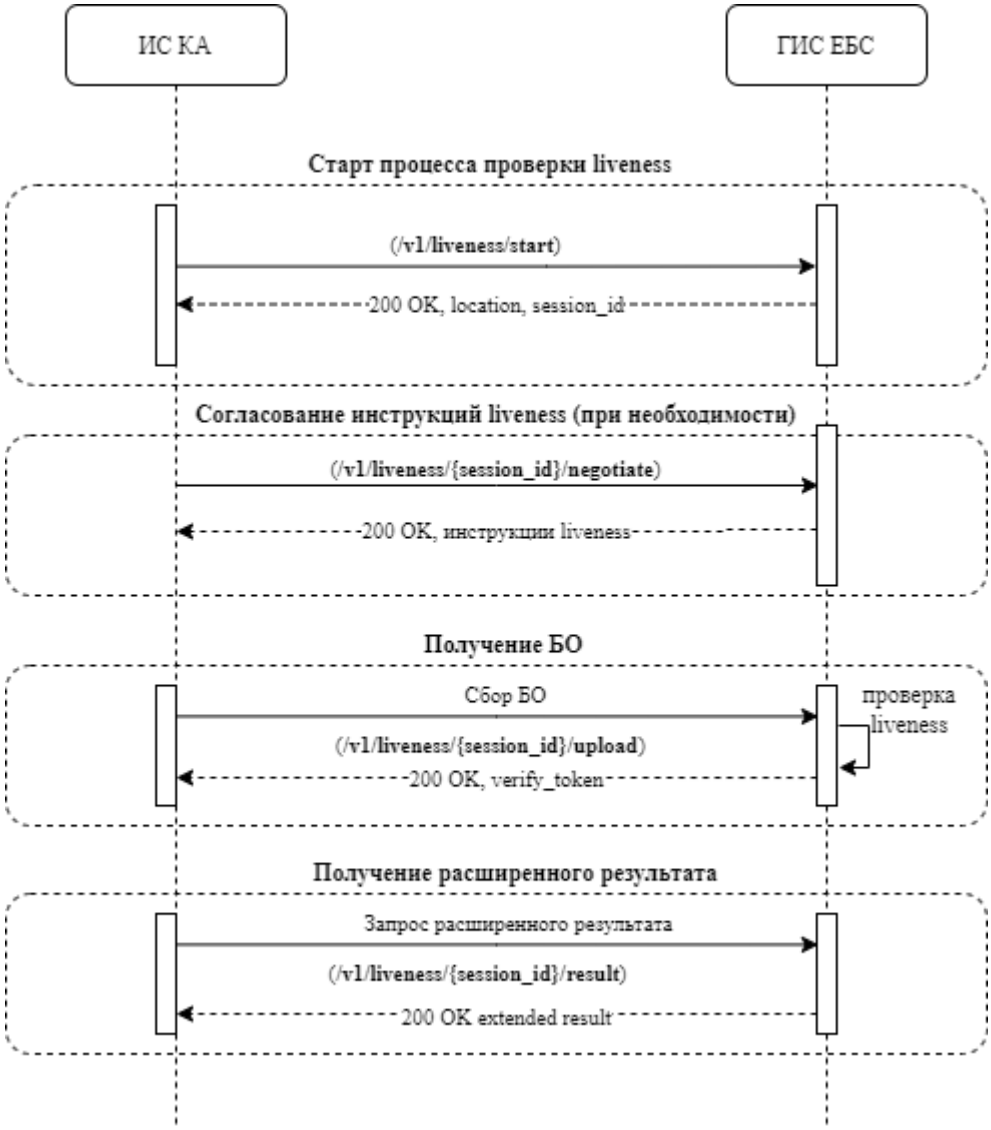


Рисунок 1 – Схема процесса проверки «живости»

В состав сервиса проверки «живости» входят следующие методы:

- Старт процесса проверки «живости» (Liveness) – для создания сессии проверки «живости» Пользователя, зарегистрированного в ГИС ЕБС.
- Согласование инструкций «живости» (Liveness) – для получения уникального набора инструкций, необходимых для работы сервиса в случае необходимости активного Liveness. В случае если активный Liveness не требуется, данный метод не вызывается со стороны ИС КА.
- Прием БО для проверки «живости» - для получения БО на проверку «живости» и возврата результата операции проверки «живости».
- Получение расширенного результата - для предоставления ИС Поставщика БДн расширенного результата в случае успешной

биометрической операции проверки «живости». Для этого ИС Поставщика БДн формирует запрос к ГИС ЕБС с передачей информации о Пользователе.

Более подробно реализация процесса и программные интерфейсы сервиса проверки «живости» (Liveness) описаны в Методических рекомендациях по использованию сервиса проверки «живости» (Liveness) (для разработчиков), размещенных на портале https://ebs.ru/documents в разделе «Технические документы».

4 Порядок получения доступа ИС участника БВ к сервису проверки «живости» (Liveness)

Порядок подключения сервиса «проверки живости» (Liveness), 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, 9.1.2, 9.1.3, 9.2.1, 9.2.2, 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)[1]. Электронная почта для связи по всем вопросам подключения и регламентных взаимодействий: support@ebs.ru.

Организации также необходимо выполнить в ЛК ЮЛ в разделе «Оферты» 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».[2]

4.1 Получение доступа к сервису проверки «живости» (Liveness)

Для получения доступа ИС Участника БВ к сервису проверки «живости» (Liveness) следует выполнить шаги подключения к сервису биометрической верификации согласно п. 7.5 «**Ошибка! Источник ссылки не найден.** и к сервису проверки «живости» (Liveness)»[3] 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)»).

[1] Опубликован по адресу https://ebs.ru/documents в разделе «Технические документы»
[2] Также опубликована по адресу http://ebs.ru/documents в разделе «Тарифы, оферты, соглашения»
[3] Для получения доступа к сервису проверки «живости» (Liveness) достаточно подключиться к ГИС ЕБС в роли IDP и Потребителя БДн, организовать защищенный канал с ГИС ЕБС и принять оферту. Подачи заявки на активацию сервиса проверки «живости» (Liveness) по форме Приложения А к Регламенту Государственной информационной системы «Единая система идентификации и аутентификации физических лиц с использованием биометрических персональных данных (ГИС ЕБС) не требуется.

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)»).

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 системы «Единая система идентификации и аутентификации физических лиц с использованием биометрических персональных данных (ГИС ЕБС)»).

4. Произвести акцепт оферты о «заключении соглашения об оказании услуг по предоставлению информации о степени соответствия предоставленных клиентом - физическим лицом биометрических персональных данных векторам единой биометрической системы, содержащимся в Единой биометрической системе», опубликованной по адресу http://ebs.ru/documents в разделе «Основные» и в ЛК ЮЛ в разделе «Оферты».

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)»).

7. Подать заявку на подключение ИС к продуктивному контуру ГИС ЕБС в роли Поставщика БДн (в соответствии с п. 9.2.2 Регламента Государственной информационной системы «Единая система идентификации и аутентификации физических лиц с использованием биометрических персональных данных (ГИС ЕБС)»).

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)»).[4]

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

4.2 Организация защищенного канала связи

При работе с ПДн 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.

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 БПДн 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 БПДн осуществляется по защищенной сети передачи данных со СМЭВ/ЕСИА/ГИС ЕБС, с применением безопасного протокола SSL/TLS для доступа в сеть «Интернет», 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 безопасности[5]. 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 КС3, принадлежащих Участнику БВ на праве собственности или на ином законном основании, или использовать СКЗИ класса КС3, 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»[6] (в целях обеспечения совместимости средств СКЗИ, применяемых Участниками БВ, могут использоваться только совместимые с используемыми в ГИС ЕБС, сертифицированные СКЗИ класса КС3, 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

[5] Информация о типовом решении по информационной безопасности доступна на сайте ЕБС по адресу https://ebs.ru/security/.
[6] 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»).

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)».

5 Сценарии работы процесса проверки «живости» (Liveness)

Для получения возможности оказания услуг с использованием биометрии организации необходимо:

- Получить согласие пользователя на обработку ПДн: 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. Организация по собственному усмотрению определяет какой способ или способы получения согласия будут у нее реализованы.
- Узнать идентификатор пользователя в ЕСИА (oid) и передать его в ГИС ЕБС вместе с идентификатором пользователя в своей системе.

5.1 Сценарий интеграции в терминалы и приложения кредитных организаций

Одним из способов применения сервиса проверки «живости» (Liveness) является интеграция в процессы оказания услуг с использованием аутентификации в терминалах и приложениях банков, с целью повышения безопасности предоставляемых услуг. Сервис позволит удостовериться, что аутентификацию проходит настоящий человек. Возможный сценарий изображен на Рисунке 2

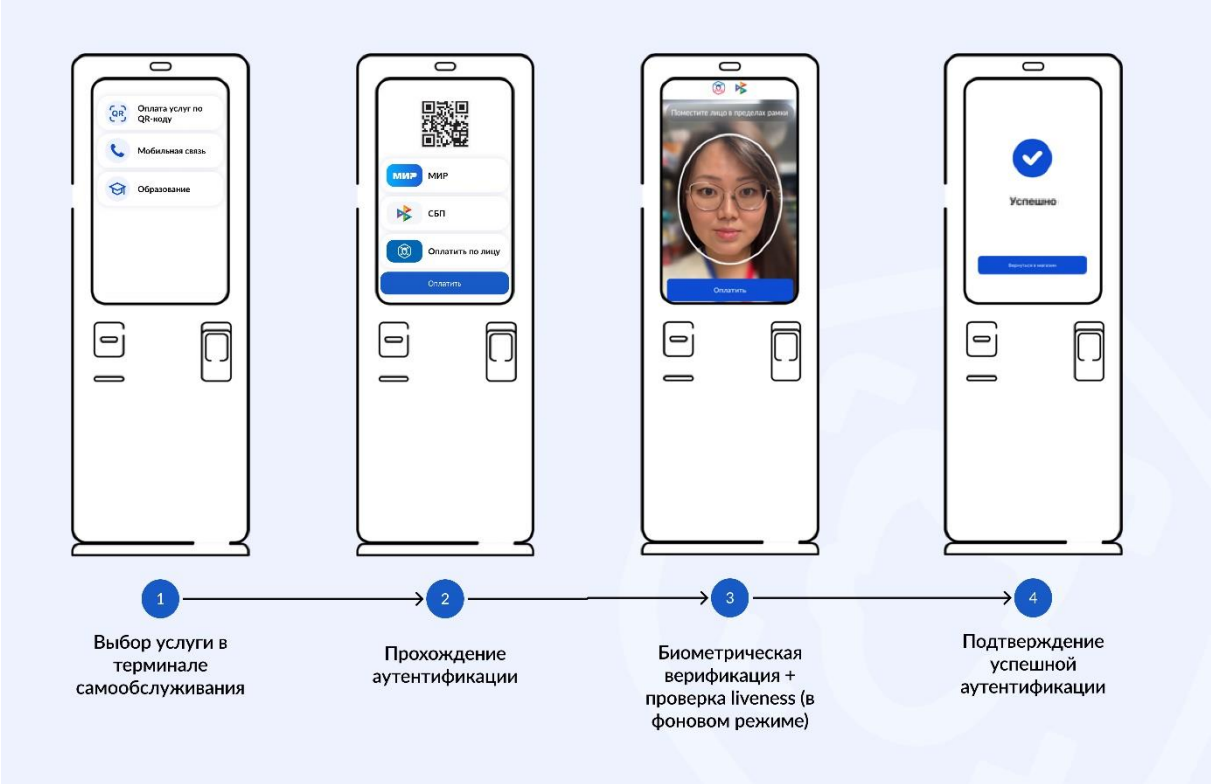


Рисунок 2 –Сценарий оказания услуги с использованием проверки «живости»

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

Шаг 1. Пользователь в терминале организации выбирает получение услуги с помощью биометрии.

Шаг 2. Пользователь авторизуется и даёт согласие на обработку БПДн.

Шаг 3. Производится сбор биометрии, осуществляется биометрическая верификация Пользователя (аутентификация «один к одному»). В фоновом режиме производится проверка «живости» Пользователя.

Шаг 4. В браузере отображается подтверждение успешной аутентификации.

5.2 Сценарий расширенного варианта прохождения теста CAPTCHA на сайтах в интернете

Компьютерный тест CAPTCHA (Completely Automated Public Turing test to tell Computers and Humans Apart – полностью автоматизированный публичный тест Тьюринга для различения компьютеров и людей) используется в виде проверочного кода как одна из разновидностей мер безопасности. Проверка «живости» при прохождении теста CAPTCHA дополнительно повысит безопасность биометрической операции аутентификации.

Возможный сценарий расширенного варианта теста CAPTCHA изображен на Рисунке 3.

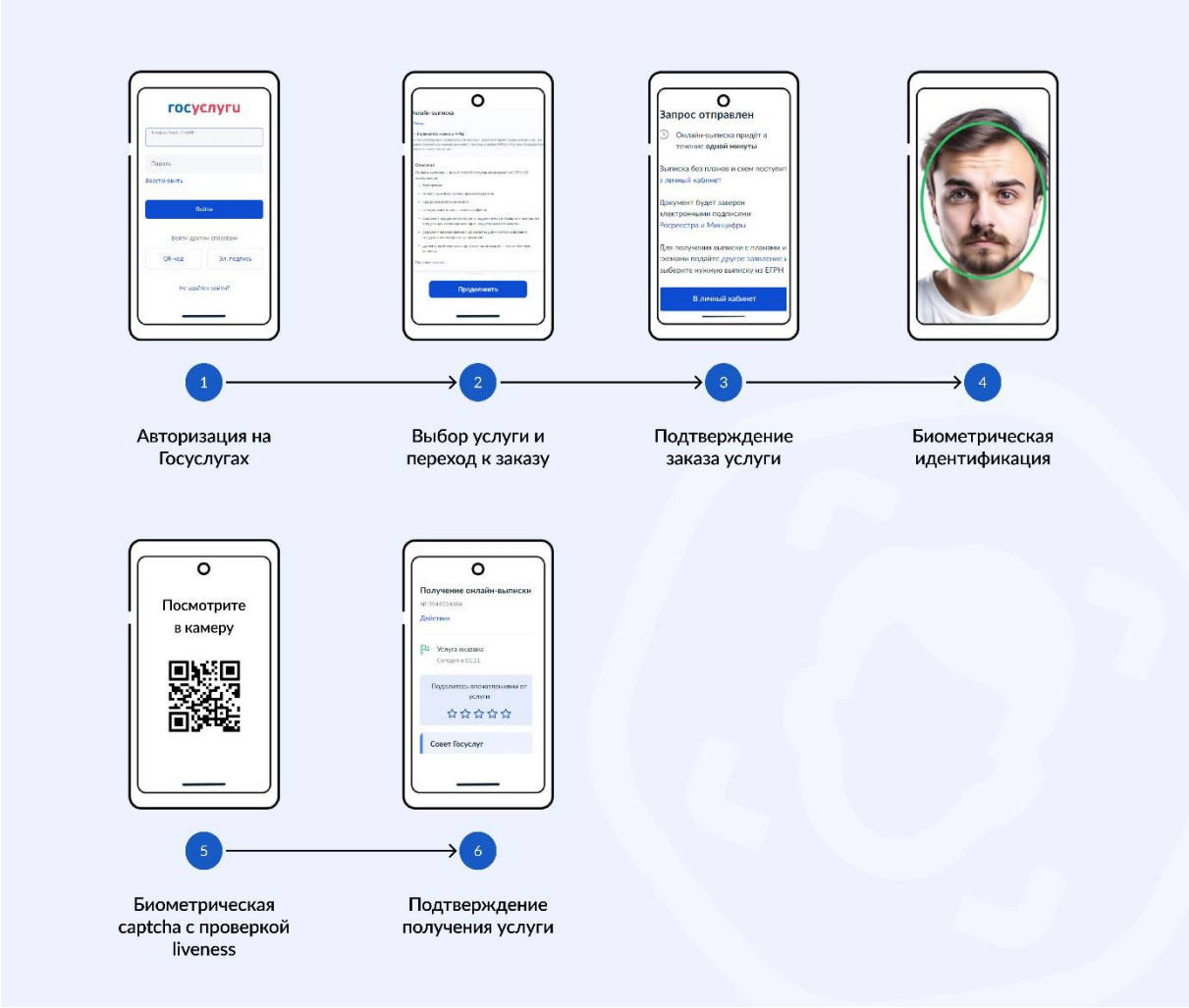


Рисунок 3 –Сценарий расширенного варианта теста CAPTCHA

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

Шаг 1. Пользователь авторизуется на портале Госуслуг в веб-приложении или МП Госуслуг.

Шаг 2. Пользователь выбирает услугу и переходит к странице заказа услуги.

Шаг 3. Пользователь подтверждает заказ услуги, при необходимости, если услуга платная, выбирает способ оплаты по лицу.

Шаг 4. Производится сбор биометрии, осуществляется биометрическая идентификация Пользователя.

Шаг 5. В браузере отображается captcha с предложением посмотреть в камеру для проверки «живости» Пользователя (биометрическая captcha).

Шаг 6. В браузере отображается успешное подтверждение оказания услуги.

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. Оформление футера/баннера/страницы допустимо менять, адаптируя под стиль ИС КА, при условии информационного взаимодействия и согласования с департаментом маркетинга Оператора ГИС ЕБС. Для согласования необходимо обратиться по адресу электронной почты marketing@ebs.ru

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 следует явиться 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.