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

**Методические рекомендации**

**по использованию сервиса**

**биометрической идентификации**

Версия 1.13

Москва 2025

**Изменения документа**

| Версия | Дата | Автор | Изменение |
| --- | --- | --- | --- |
| 1.0 | 20.10.2023 | С. Гаврилов | Создание документа |
| 1.1 | 07.11.2023 | С. Гаврилов | Откорректирован п. 4.1: необязательность параметра matching, описание agree.date\_from |
| 1.2 | 04.12.2023 | С. Гаврилов | Дополнен п. 4.2 и откорректировано его название (уведомление IDP о деактивации) |
| 1.3 | 27.03.2024 | И. Липницкий | По всему тексту в документе были внесены изменения:* заменено доменное имя ebs-int.rtlabs.ru на int.ebs.ru
* заменено доменное имя ebs-dev.rtlabs.ru на dev.ebs.ru
 |
| 1.4 | 09.10.2024 | С. Гаврилов | В п. 4.3 откорректированы значения «MA», «MF» (мэтчинг) параметра stu |
| 1.5 | 21.10.2024 | С. Гаврилов | Добавлены п. 4.2.1, 4.2.2, 4.2.3 с версиями апи уведомления IDP о результатах регистрации УЗ/деактивации БШ v1, v2, v3. Откорректировано определение Хещ ПДн и добавлено Приложение 4 с описанием алгоритма хеширования. |
| 1.6 | 18.11.2024 | С. Гаврилов | Добавлено описание проверки возраста (18+) в п. 2.2, расширен алгоритм, добавлен п. 5.2.2.1 (запрос для получения данных по УЗ), добавлены мнемоники \_age, добавлены версии апи биометрической идентификации v2 в раздел 5 |
| 1.7 | 02.12.2024 | С. Гаврилов | Дополнено описание параметра aud в п. 4.4, 5.1.1, 5.1.2, 5.3.1 и 5.3.2 |
| 1.8 | 15.01.2025 | С. Гаврилов | В п. 4.1 дополнено описание параметра datetime\_tz |
| 1.9 | 27.01.2025 | С. Гаврилов | В Приложении 3 добавлены все имеющиеся мнемоники проверки возраста (\_age) |
| 1.10 | 25.04.2025 | С. Гаврилов | Скорректировано Приложение 3 (только поддерживаемые на сегодня мнемоники). Расширено описание Location в п. 5.1 |
| 1.11 | 04.06.2025 | С. Гаврилов | В п. 5.2.1 и 5.2.2 обновлены примеры успешного ответа на запрос (/upload) |
| 1.12 | 09.07.2025 | С. Гаврилов | Добавлен абзац в п. 3.1 (ПИН-код). В п. 5.2.1 добавлены коды ошибок. В п. 5.2.2 добавлено описание ответа с запросом на ввод ПИН-кода, добавлен пример, дополнительные коды ошибок. В п. 5.3.1 исправлен параметр identify\_status.transactionId, исправлены коды ошибок. В п. 5.3.2 исправлен параметр identify\_status.transactionId, исправлены коды ошибок.Обновлен Рисунок 3, добавлен Рисунок 4. Добавлен Раздел 6 (API PIN). Обновлено оглавление |
| 1.13 | 17.07.2025 | С. Гаврилов | Добавлен п. 3.3 с перечнем рекомендованных браузеров и их версий. |

Оглавление

[Глоссарий 4](#_Toc203668735)

[1 ВВЕДЕНИЕ 10](#_Toc203668736)

[2 Нормативные ссылки 11](#_Toc203668737)

[3 Описание процесса биометрической идентификации 15](#_Toc203668738)

[3.1 Предусловия для проведения биометрической идентификации 16](#_Toc203668739)

[3.2 Алгоритм взаимодействия в процессе биометрической идентификации 17](#_Toc203668740)

[3.3 Список поддерживаемых браузеров 20](#_Toc203668741)

[4 Интерфейсы работы с учетной записью Пользователя 22](#_Toc203668742)

[4.1 API регистрации УЗ Пользователя в ГИС ЕБС (регистрация без биометрических данных) 22](#_Toc203668743)

[4.2 API уведомления IDP о результатах регистрации УЗ или деактивации БШ 29](#_Toc203668744)

[4.2.1 API уведомления IDP об изменении статуса УЗ v1 (планируется к выводу из эксплуатации) 30](#_Toc203668745)

[4.2.2 API уведомления IDP об изменении статуса УЗ v2 (планируется к выводу из эксплуатации) 31](#_Toc203668746)

[4.2.3 API уведомления IDP об изменении статуса УЗ v3 33](#_Toc203668747)

[4.3 API уведомления IDP о результатах сопоставления УЗ 35](#_Toc203668748)

[4.4 API деактивации УЗ Пользователя 37](#_Toc203668749)

[5 API биометрической идентификации Пользователя 42](#_Toc203668750)

[5.1 API старта сессии биометрической идентификации 42](#_Toc203668751)

[5.1.1 API старта сессии биометрической идентификации v1 (планируется к выводу из эксплуатации) 42](#_Toc203668752)

[5.1.2 API старта сессии биометрической идентификации v2 48](#_Toc203668753)

[5.2 API приема БО для биометрической идентификации 54](#_Toc203668754)

[5.2.1 API приема БО для биометрической идентификации v1 (планируется к выводу из эксплуатации) 54](#_Toc203668755)

[5.2.2 API приема БО для биометрической идентификации v2 61](#_Toc203668756)

[5.3 API получения расширенного результата 69](#_Toc203668757)

[5.3.1 API получения расширенного результата v1 (планируется к выводу из эксплуатации) 69](#_Toc203668758)

[5.3.2 API получения расширенного результата v2 79](#_Toc203668759)

[6 API передачи PIN для сверки 90](#_Toc203668760)

[6.1 API передачи PIN-кода в ЕБС для проверки в рамках подтверждения биометрических операций 90](#_Toc203668761)

[ПРИЛОЖЕНИЕ №1. Дополнительные метаданные (meta) 93](#_Toc203668762)

[ПРИЛОЖЕНИЕ №2. Дополнительные данные о метриках системы (metrics) 96](#_Toc203668763)

[ПРИЛОЖЕНИЕ №3. Доступные мнемоники сбора БО в процессе биометрической идентификации 103](#_Toc203668764)

[ПРИЛОЖЕНИЕ №4. Описание алгоритма генерации хеш-функции 104](#_Toc203668765)

# Глоссарий

|  |  |
| --- | --- |
| **Термин** | **Описание** |
| **Аутентификация** | **Действия по проверке подлинности субъекта доступа в автоматизированной информационной системе** |
| Биометрические данные (БДн) | **Биометрический образец** или совокупность **биометрических образцов** на любой стадии обработки, например, **биометрический контрольный шаблон** или биометрический признак. |
| Библиотека контроля качества (БКК) | Библиотека, входящая в состав Единой биометрической системы и разработанная для определения качества биометрических образцов, передаваемых в Единую биометрическую систему в процессах биометрической регистрации, импорта биометрических образцов и самостоятельной регистрации (саморегистрации) |
| 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 |
| 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 |
| 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 |
| 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» |
| Живучесть (liveness) | 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 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 связывания в ЕБС УЗ ФЛ с мастер-УЗ 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 |
| Провайдер идентификации / Identity Provider (IDP) | **Информационная система, отвечающая за поддержку и управление информацией об идентификации пользователей и обеспечивающая аутентификацию пользователей для других информационных систем.**  |
| Региональный сегмент Единой биометрической системы | **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]](#footnote-2)**При подключении региональных сегментов к Единой биометрической системе следует руководствоваться теми же требованиями, которые применяются для подключения КБС.**  |
| 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](https://ru.wikipedia.org/wiki/%D0%94%D0%B0%D0%BD%D0%BD%D1%8B%D0%B5) о пользователе, необходимая для его опознавания ([аутентификации](https://ru.wikipedia.org/wiki/%D0%90%D1%83%D1%82%D0%B5%D0%BD%D1%82%D0%B8%D1%84%D0%B8%D0%BA%D0%B0%D1%86%D0%B8%D1%8F)) и [предоставления доступа](https://ru.wikipedia.org/wiki/%D0%9F%D1%80%D0%B0%D0%B2%D0%B0_%D0%B4%D0%BE%D1%81%D1%82%D1%83%D0%BF%D0%B0) к его личным данным, настройкам и сервисам |
| hash ПДн | Однонаправленное преобразование персональных данных пользователя в битовое значение установленной длины, выполняемое алгоритмом генерации хеш-функции последовательности двоичных символов по ГОСТ Р 34.11-2012 «Информационная технология. Криптографическая защита информации. Функция хэширования». |
| OID, Open ID | Идентификатор Пользователя в IDP ЕСИА, требуется для сопоставления (мэтчинга) УЗ Пользователя в ЕБС |

# ВВЕДЕНИЕ

Основные положения об осуществлении биометрической идентификации с использованием ЕБС содержатся в статье 10 (аутентификация с использованием ЕБС) и статье 11 (использование 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 сервиса 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» (см. п. 7.6, 9.1.6 и 9.2.6).

Взаимодействие с сервисом идентификации практически аналогично взаимодействию с сервисом биометрической верификации (используются аналогичные программные интерфейсы, мнемоники идентификации, так же создаются сессии и возвращается расширенный результат, используется web-форма ЕБС).

Электронная почта для связи по всем вопросам подключения и регламентных взаимодействий: support@ebs.ru

# Нормативные ссылки

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

1. Федеральный закон от 07 августа 2001 г. № 115-ФЗ «О противодействии легализации (отмыванию) доходов, полученных преступным путем, и финансированию терроризма» (далее - Федеральный закон от 07 августа 2001 г. № 115-ФЗ);
2. Федеральный закон от 07 июля 2003 г. № 126-ФЗ «О связи» (далее - Федеральный закон от 07 июля 2003 г. № 126-ФЗ);
3. Федеральный закон от 27 июля 2006 г. №152-ФЗ «О персональных данных» (далее - Федеральный закон от 27 июля 2006 г. №152-ФЗ);
4. Федеральный закон от 27 июля 2010 г. № 210-ФЗ «Об организации предоставления государственных и муниципальных услуг» (далее - Федеральный закон от 27 июля 2010 г. № 210-ФЗ);
5. Федеральный закон от 06 апреля 2011 г. № 63-ФЗ «Об электронной подписи» (далее - Федеральный закон от 06 апреля 2011 г. № 63-ФЗ);
6. Федеральный закон от 27 декабря 2019 г. № 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 декабря 2019 г. № 476-ФЗ);
7. Федеральный закон от 29 декабря 2020 г. № 479-ФЗ «О внесении изменений в отдельные законодательные акты Российской Федерации» (далее – Федеральный закон от 29 декабря 2020 г. № 479-ФЗ);
8. 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);
9. 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);
10. 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);
11. 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);
12. 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);
13. Постановление Правительства Российской Федерации от 15.10.2021 № 1754 «Об утверждении требований к проверке простой электронной подписи, которой в соответствии с частями 5 и 23 статьи 141 Федерального закона «Об информации, информационных технологиях и о защите информации» подписаны согласия на обработку персональных данных и биометрических персональных данных, при хранении указанных согласий» (далее – Постановление Правительства РФ от 15.10.2021 № 1754);
14. 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);
15. Постановление Правительства Российской Федерации от 16.12.2022 № 2326 «О возложении на акционерное общество «Центр Биометрических Технологий» функций оператора 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, а также о признании утратившими силу распоряжения Правительства Российской Федерации от 22 февраля 2018 г. № 293-р и пункта 4 изменений, которые вносятся в акты Правительства Российской Федерации, утвержденных постановлением Правительства Российской Федерации от 24 июня 2021 г. № 982» (далее – Постановление Правительства РФ от 16.12.2022 № 2326);
16. 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);
17. Приказ Минцифры России от 06.08.2021 № 816 «Об утверждении методик проверки соответствия предоставленных биометрических персональных данных физического лица его биометрическим персональным данным, содержащимся в информационных системах, обеспечивающих идентификацию и (или) аутентификацию с использованием биометрических персональных данных, а также об определении степени взаимного соответствия указанных биометрических персональных данных, достаточной для проведения идентификации, предусмотренной Федеральным законом от 27.07.2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации» (далее – Приказ Минцифры от 06.08.2021 № 816);
18. 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);
19. 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);
20. ГОСТ 34.201-89 «Информационная технология. Комплекс стандартов на автоматизированные системы. Виды, комплектность и обозначение документов при создании автоматизированных систем» (далее - ГОСТ 34.201-89).

# Описание процесса биометрической идентификации

Процесс биометрической идентификации представляет собой поиск пользователя по предоставленному БО среди биометрических данных пользователей, хранящихся в ЕБС (выполняется поиск по схеме «один ко многим»), с целью оказания услуг. ИС КА передает полученный БО в ГИС ЕБС[[2]](#footnote-3). Обработка биометрического образца в ИС КА осуществляется без их сохранения в ИС КА и средствах съема БО.

Для того, чтобы обеспечить взаимодействие ИС КА с ГИС ЕБС и возможность использования сервиса биометрической идентификации для пользователя в случаях, когда поиск «один ко многим» применяется в рамках аутентификации (ст. 10 Федерального закона №572-ФЗ), необходимо предварительно связать id этого пользователя в ИС КА с его учетной записью в ЕБС на основании данных для связывания/мэтчинга (Hash ПДн/OID ЕСИА/СНИЛС). Производится связывание (мэтчинг) ранее зарегистрированной в ЕБС учетной записи Пользователя, содержащей биометрические данные, и учетной записи Пользователя в ИС КА, которая будет использоваться в процессе биометрической идентификации.

Схема взаимодействия ИС КА с ГИС ЕБС в процессе регистрации УЗ (связывания) представлена на рисунке ниже (Рисунок 1).



Рисунок 1 – Схема взаимодействия ИС КА с ГИС ЕБС в процессе связывания учетных записей пользователя

## Предусловия для проведения биометрической идентификации

Для организации использования биометрической идентификации необходимо:

1. Зарегистрировать ИС КА в ГИС ЕБС[[3]](#footnote-4) в качестве:
	* Провайдера идентификации (IDP);
	* ИС Поставщика БДн (для отправки запросов на связывание УЗ и выгрузку шаблонов);
2. Активировать сервис биометрической идентификации[[4]](#footnote-5).
3. Зарегистрировать УЗ Пользователя в ГИС ЕБС под ранее заведенной IDP (например, IDP1) с идентификатором Пользователя в этой IDP и с передачей данных для сопоставления регистрируемой УЗ с УЗ ЕСИА, путем вызова API «Регистрация УЗ без БО» (см. раздел 4.1).
4. Получить от ГИС ЕБС уведомления об успешной регистрации учетной записи и успешном выполнении сопоставления учетных записей Пользователя на основе переданных при регистрации данных для сопоставления (OID и/или СНИЛС) (см. разделы 4.2, 4.3, 4.4).
5. При необходимости УЗ Пользователя может быть деактивирована с использованием API деактивации УЗ (см. раздел 4.4). Схема деактивации учетной записи представлена на ниже (Рисунок 2):



Рисунок 2 – Схема деактивации учетной записи

После этого организация, подключенная к сервису биометрической идентификации (ИС КА), подает запрос в ЕБС и вызывает сервис идентификации. ЕБС выдает результат идентификации.

В процессе биометрической идентификации реализована возможность проверки возраста пользователя, чтобы обеспечить возможность подтверждения возраста в транзакциях с ограничением возраста без предъявления пользователем паспорта, но используя биометрию и данные пользователя из ЕСИА в качестве альтернативы паспорта, для чего:

* при старте биометрической идентификации (см. п. 5.1) указывается признак запроса возраста (мнемоника с постфиксом \_age, см. Приложение №3);
* при получении расширенного результата передается в том числе информация о возрасте пользователя (п. 5.3).

В процессе биометрической идентификации реализована возможность использования дополнительного фактора идентифиции – ПИН-кода.

Использование пин-кода в качестве второго фактора идентификации позволит повысить безопасность операций в следующих случаях:

* угроза мошенничества;
* проведение операций с повышенными рисками;
* подтверждение личности Пользователя (при неоднозначной идентификации, например для близнецов).

Пользователь может установить пин-код в личном кабинете физического лица на портале ebs.ru.

Все программные интерфейсы биометрической идентификации должны быть версии v2 и выше.[[5]](#footnote-6)

## Алгоритм взаимодействия в процессе биометрической идентификации

Сценарий процесса биометрической идентификации состоит из следующих шагов:

* + 1. Организация, подключенная к сервису биометрической идентификации (ИС КА), вызывает метод старта идентификации (см. раздел 5.1). ГИС ЕБС осуществляет проверку переданной в запросе мнемоники.
			1. Для использования сервиса проверки возраста указывается мнемоника с возрастом (с постфиксом возраста \_age, более подробно о мнемониках см. Приложение №3).
			2. Для использования механизма проверки PIN-кода в запросе указывается дополнительное поле с параметром pin\_check\_necessity (см. п. 5.1.2).
		2. В зависимости от мнемоники, переданной в запросе на шаге 1, Пользователь перенаправляется на web-форму ГИС ЕБС для сбора БО в рамках прохождения биометрической идентификации по URL, полученному в ответе от ГИС ЕБС (передается в составе HTTP заголовка «Location», см. п. 5.1):
			1. если передана мнемоника c постфиксом with\_webinterface/ with\_webinterface\_age, Пользователь перенаправляется на web-форму ГИС ЕБС с интерфейсом для сбора БО;
			2. в остальных случаях ИС КА необходимо реализовать собственную web-форму либо осуществлять сбор БО без web-формы.
		3. Пользователь сдает биометрические образцы с использованием web-формы, следуя инструкциям на экране.
		4. Собранные биометрические образцы Пользователя передаются в ГИС ЕБС для прохождения биометрической идентификации (см. раздел 5.2).
		5. После успешного прохождения биометрической идентификации:
			1. В случае если не предполагалось использование пин-кода web-форма перенаправляет Пользователя по URL, который ИС КА передала в ГИС ЕБС на первом шаге настоящего алгоритма, а также передается verify\_token, необходимый для получения расширенного результата идентификации, далее шаг 6;
			2. В случае если предполагалось использование пин-кода web-форма перенаправляет Пользователя по URL для ввода пин-кода, после проверки которого, web-форма перенаправляет Пользователя по URI, который ИС КА передала в ГИС ЕБС на первом шаге настоящего алгоритма, а также передается verify\_token, необходимый для получения расширенного результата идентификации, далее шаг 6;
		6. ИС КА направляет запрос в ГИС ЕБС для получения расширенного результата идентификации (см. раздел 5.3).
		7. ГИС ЕБС передает в ИС КА расширенный результат идентификации.
			1. В случае если на шаге 1 передавалась мнемоника с постфиксом age (необходимость определить количество полных лет), то в составе расширенного результата ГИС ЕБС передает информацию о возрасте пользователя.

Участники: ГИС ЕБС, ИС КА.

В случае возникновения ошибок на каком-либо из шагов процесс прерывается и ИС КА необходимо осуществить повторную отправку запроса.

Процесс биометрической идентификации (без PIN-кода и с PIN-кодом) представлен на рисунках ниже (Рисунок 3 и Рисунок 4).



Рисунок 3 – Схема взаимодействия ИС КА с ГИС ЕБС в процессе биометрической идентификации (без PIN-кода)



Рисунок 4 – Схема взаимодействия ИС КА с ГИС ЕБС в процессе биометрической идентификации (с PIN-кодом)

## Список поддерживаемых браузеров

Рекомендовано использовать следующие браузеры с поддержкой криптографических алгоритмов ГОСТ TLS.

Для десктопных ОС Windows, macOS, Linux:

* Chromium GOST версии 138.0.7204.96 и выше;
* Яндекс Браузер версии 25.6.2.418 и выше.

Для мобильной ОС Android:

* Chromium GOST версии 138.0.7204.96 и выше;
* КриптоПро FOX версии Firefox 140.0.0 и выше, КриптоПро CSP 5.0.13456 и выше.

Для мобильной ОС iOS:

* в настоящее время не поддерживается.

Для мобильной ОС Аврора:

* Браузер Аврора версии 1.9.0 и выше.

# Интерфейсы работы с учетной записью Пользователя

## API регистрации УЗ Пользователя в ГИС ЕБС (регистрация без биометрических данных)

Интерфейс предоставляет возможность регистрации УЗ Пользователя без БДн для Провайдера идентификации, зарегистрированного в ГИС ЕБС, для последующего проведения биометрической идентификации с использованием этой УЗ и БДн этого же Пользователя, привязанных к ранее зарегистрированной в ГИС ЕБС УЗ.

**Вызов сервиса**

POST <host>:<port>/api/v1/registration

Заголовки:

* + Host: {ГИС ЕБС host}
	+ Content-Type: multipart/form-data; boundary={разделитель}
	+ Content-Length: {длина тела сообщения}
	+ X-EBS-TraceProcess: true (необязательный заголовок типа Boolean, флаг отправки сообщений по запросу в Технологический портал. Возможные значения true или false)

Заголовки вложенной сущности:

* + Content-Disposition: form-data; name=”params”
	+ Content-Type: application/octet-stream

Тело запроса: передается в виде JWT токена, формируемого и подписываемого информационной системой – инициатором запроса. JWT формируется в соответствии с RFC 7519 <https://datatracker.ietf.org/doc/html/rfc7519> без padding-ов.

Запрос должен быть подписан PKCS#7 (cert + Sig) или PLAIN. Без padding’ов

Алгоритмы, указываемые в JWT HEADER, перечислены в таблице ниже.

|  |  |
| --- | --- |
| **Алгоритм, указываемый в Header** | **Описание** |
| GS3410 | алгоритм GOST3411withECGOST3410 |
| GOST3410 | алгоритм GOST3411withGOST3410EL |
| GOST3410\_2012\_256 | алгоритм GOST3411\_2012\_256withGOST3410\_2012\_256 |
| GOST3410\_2012\_512 | алгоритм GOST3411\_2012\_512withGOST3410\_2012\_256 |

Пример JWT HEADER:

|  |
| --- |
| { "alg": "GOST3410\_2012\_256", "typ": "JWT"} |

Состав PAYLOAD в JWT:

|  |  |  |  |
| --- | --- | --- | --- |
| **Наименование параметра** | **Тип данных** | **Обязательность** | **Описание** |
| service\_type | string | да | Тип (мнемоника) услуги.reg-without-bio |
| datetime\_tz | number | да | Дата регистрации (Формат Unix time stamp в секундах).Пример: 1736932760. Значение данного параметра (10 цифр) проверяется в запросе. Если проверка не пройдена, ГИС ЕБС возвращает ошибку «400 EBS-010003 Неверный запрос. неверный параметр datetime\_tz» (см. также ошибки метода в таблице ниже). |
| infosystem | JSON-object | да | Содержит информацию о ИС Контрагента, отправившей запрос |
| infosystem.system\_id | string | да | Мнемоника ИС Контрагента |
| infosystem.contract\_id | string | да | Идентификатор контракта |
| infosystem.ra\_id | string | нет | Идентификатор центра обслуживания в реестре поставщика идентификации IDP |
| infosystem.employee\_id | string | нет | Сотрудник, осуществляющий регистрацию |
| infosystem.cert\_id | string | да | id сертификата, которым подписана JWT (сертификаты хранятся в реестре сертификатов в привязке к мнемонике ИС\_Поставщика БДн) |
| agree | JSON-object | нет | Содержит информацию о согласии |
| agree.agreement\_id | string | нет | Идентификатор записи данных согласия в ИС КА. Если согласие для ИС КА получает ГИС ЕБС, то заполняется идентификатор согласия в ГИС ЕБС |
| agree.date\_from | number | да | Дата, c которой действует согласие (Формат Unix time stamp в секундах). В случае заполнения параметра agree данный элемент подлежит обязательному указанию. |
| agree.date\_to | number | нет | Дата, до которой действует согласие (Формат Unix time stamp в секундах) |
| person | JSON-object | да | Содержит информацию о Пользователе |
| person.idp | string | да | Идентификатор (мнемоника) IDP |
| person.user\_id | string | да | ID УЗ Пользователя IDP |
| person.contact | JSON-object | нет | Контактные данные Пользователя |
| person.contact.phone | string | нет | Телефон Пользователя, указывается в формате +7XXXXXXXXXX, где X цифра от 0 до 9 |
| person.contact.email | string | нет | Электронная почта Пользователя |
| matching | array | нет | Содержит данные для мэтчинга |
| matching.key | string | да (в случае указания в запросе параметра matching) | Описание передаваемых данных для мэтчинга.Может принимать значения: 1. "hash" – данный ключ предполагает, что в поле value будет передан Хеш ПДн;[[6]](#footnote-7)2. "ESIA" – Мнемоника Провайдера идентификации ЕСИА;3. "SNILS" - СНИЛС ФЛ.Мэтчинг производится после регистрации УЗ и создания профиля в ЕБС. Мэтчинг производится по принципу первого найденного соответствия.  |
| matching.value | string | да (в случае указания в запросе параметра matching) | Значения данных для мэтчинга (Хеш ПДн[[7]](#footnote-8), OID или номер СНИЛС) |
| meta | JSON-object | нет | Дополнительные метаданные (согласно спецификации объекта metadata в Приложении №1). |
| metrics | JSON-object | нет | Дополнительные данные о метриках системы (согласно спецификации дополнительных данных о метриках системы в Приложении №2). |

Пример JWT.PAYLOAD:

|  |
| --- |
| { "service\_type": "registration\_without\_bio", "datetime\_tz": 1589277386, "infosystem": { "system\_id": "IDP\_TESTSYSTEM", "contract\_id": "51684869", "cert\_id": "4363463463223787878" }, "agree": { "agreement\_id": "12392737476-agreeID", "date\_from": 1589277386, "date\_to": 1683868229 }, "person": { "idp": "IDP\_TESTSYSTEM", "user\_id": "19615355324", "contact": { "email": "test-email@mail.ru" } }, "matching": [{ "key":"ESIA", "value": "1077118267" },{ "key":"SNILS", "value": "12345678901" }]} |

Пример запроса:

|  |
| --- |
| POST /api/v1/registrationHost: int.ebs.ruContent-Type: multipart/form-data; boundary=f3URHA\_Xnhk0D8gW1iCGLPQk9\_gjZr\_ywsHContent-Length: {длина тела сообщения} --f3URHA\_Xnhk0D8gW1iCGLPQk9\_gjZr\_ywsHContent-Disposition: form-data; name="params"Content-Type: application/octet-streameyJhbGciOiJHT1NUMzQxMF8yMDEyXzI1NiIsInR5cCI6IkpXVCJ9.eyJzZXJ2aWNlX3R5cGUiOiJyZWdpc3RyYXRpb25fd2l0aG91dF9iaW8iLCJkYXRldGltZV90eiI6MTU4OTI3NzM4NiwiaW5mb3N5c3RlbSI6eyJzeXN0ZW1faWQiOiJJRFBfVEVTVFNZU1RFTSIsImNvbnRyYWN0X2lkIjoiNTE2ODQ4NjkiLCJjZXJ0X2lkIjoiNDM2MzQ2MzQ2MzIyMzc4Nzg3OCJ9LCJhZ3JlZSI6eyJhZ3JlZW1lbnRfaWQiOiIxMjM5MjczNzQ3Ni1hZ3JlZUlEIiwiZGF0ZV9mcm9tIjoxNTg5Mjc3Mzg2LCJkYXRlX3RvIjoxNjgzODY4MjI5fSwicGVyc29uIjp7ImlkcCI6IklEUF9URVNUU1lTVEVNIiwidXNlcl9pZCI6IjE5NjE1MzU1MzI0IiwiY29udGFjdCI6eyJlbWFpbCI6InRlc3QtZW1haWxAbWFpbC5ydSJ9fSwibWF0Y2hpbmciOlt7ImtleSI6IkVTSUEiLCJ2YWx1ZSI6IjEwNzcxMTgyNjcifV19.FVFXHTyxLkvizyGbDGLaYXFCjTFObUGWMofeQueHJfPLLCeXGcSOJwtxGPtQQzztiubOzBoNJKunqMPHjQXRZgUItFVoLZogTS |

**Успешный ответ**

В случае успешного ответа, метод возвращает HTTP-код 202 Accepted, в HTTP BODY включен идентификатор запроса.

Пример успешного ответа:

|  |
| --- |
| HTTP/1.1 202 AcceptedContent-Type: application/json; charset=UTF-8{ "request\_id": "5234235235233"} |

**Ошибки метода**

В случае возникновения ошибки при обработке запроса ГИС ЕБС возвращает вызывающей стороне HTTP-код ошибки и описание в BODY, согласно таблице ниже:

|  |  |  |
| --- | --- | --- |
| **Код ответа HTTP** | **Значение параметра "code"** | **Описание (параметр "message")** |
| 400 | EBS-010003 | Неверный запрос. {описание ошибки} |
| 400 | EBS-010004 | Запрос не содержит обязательного параметра {название параметра} |
| 400 | EBS-02024 | Отсутствуют обязательные данные |
| 400 | EBS-010101 | Ошибка проверки маркера доступа |
| 401 | EBS-010102 | Ошибка проверки маркера доступа |
| 403 | EBS-02030 | Отказано в доступе. Указанный провайдер идентификации отсутствует в системе |
| 403 | EBS-02031 | Отказано в доступе. Указанный провайдер идентификации заблокирован в системе |
| 403 | EBS-02040 | Отказано в доступе. Указанная ИС отсутствует в системе |
| 403 | EBS-02041 | Отказано в доступе. Указанная ИС заблокирована в системе |
| 403 | EBS-02042 | Отказано в доступе. Указанная ИС не зарегистрирована в системе как поставщик БО |
| 403 | EBS-011101 | Ошибка проверки маркера доступа |
| 500 | EBS-010001 | Внутренняя ошибка API |
| 500 | EBS-010002 | Сервис в настоящее время не может выполнить запрос из-за большой нагрузки или технических работ на сервере |
| 503 | EBS-08001 | Сервис временно не доступен |

Пример ответа с ошибкой:

|  |
| --- |
| HTTP/1.1 400 Bad RequestContent-Type: application/json; charset=UTF-8{ "request\_id": "5234235235233", "code": "EBS-010003", "message": "Неверный запрос. Неверный параметр matching"} |

## API уведомления IDP о результатах регистрации УЗ или деактивации БШ

Уведомление провайдера идентификации о результатах регистрации УЗ осуществляется со стороны ГИС ЕБС в виде POST-запроса на URL Провайдера идентификации для отправки уведомлений, с использованием авторизационного токена. Токен постоянный, типа Bearer, генерируется на стороне ИС Провайдера идентификации и передается в ГИС ЕБС. В случае обновления новый токен должен быть также передан в ГИС ЕБС. Значения URL и авторизационного токена указываются при регистрации Провайдера идентификации в ГИС ЕБС. Провайдер идентификации на своей стороне должен реализовать REST API, обеспечивающий прием и корректную обработку соответствующего запроса от ГИС ЕБС.

Изменение параметров производится по заявке в соответствии с Регламентом Государственной информационной системы «Единая система идентификации и аутентификации физических лиц с использованием биометрических персональных данных» (ГИС ЕБС).

По этому же программному интерфейсу осуществляется уведомление провайдера идентификации о деактивации, производимой по запросу на деактивацию БШ на стороне Участника БВ (см. п. 4.7 Методических рекомендаций по использованию сервисов выгрузки векторов и импорта БО[[8]](#footnote-9)) администратором ГИС ЕБС или пользователем в личном кабинете ЕСИА. Статус результата операции в ЕБС (см. параметр stu ниже) в этом случае примет значение «D» – БШ деактивирован.

В случае направления со стороны провайдера идентификации в ГИС ЕБС запроса на деактивацию УЗ (см. п. 4.4), данное уведомление не отправляется в адрес провайдера идентификации, поскольку взаимодействие синхронное.

Используются три версии API метода: v1, v2 и v3. Версии API v1 и v2 метода планируются к выводу из эксплуатации.

### API уведомления IDP об изменении статуса УЗ v1 (планируется к выводу из эксплуатации)

Для обеспечения поддержки версионности данную версию принято считать версией v1. Используется {url IDP} из конфигурации (idp\_notify\_params.callback\_url) без указания версии в адресе запроса. API используется для извещения не только о результатах регистрации, но вообще об изменении статуса УЗ, в т.ч. деактивации, блокировки.

**Вызов сервиса**

POST https://{URL Провайдера идентификации для отправки уведомления о результатах регистрации},

где {URL Провайдера идентификации} – URL IDP, используемый для уведомления о результатах регистрации (idp\_notify\_params.callback\_url).

Заголовки запроса: Authorization: Bearer {заданный авторизационный токен}, Content-Type: application/json.

Состав тела запроса:

|  |  |  |  |
| --- | --- | --- | --- |
| **Поле** | **Тип** | **Обязательность** | **Описание** |
| user\_id | String | Да | Идентификатор учетной записи Пользователя в информационной системе провайдера идентификации |
| stu | String | Да | Статус результата операции в ГИС ЕБС.Принимает значения:**"A"** - Пользователь успешно зарегистрирован**"B"** - Пользователь заблокирован**"D"** – Пользователь/БШ деактивирован**"F"** - Неуспешная попытка регистрации Пользователя |

Пример запроса:

|  |
| --- |
| POST https://test.idp.ru/send/stu/here http/1.1Content-Type: application/json; charset=utf-8Authorization: Bearer bearer\_token{ "user\_id": "1000453364", "stu": "A"} |

**Успешный ответ**

200 OK без HTTP BODY

**Ошибки метода**

В случае ошибки метод должен вернуть HTTP-код + описание ошибки в BODY. Ошибки реализуются на стороне ИС Провайдера идентификации. Перечень и количество полей в JSON BODY не регламентируется и реализуется на усмотрение ИС Провайдера идентификации.

Пример запроса:

|  |
| --- |
| HTTP/1.1 400 Bad RequestContent-Type: application/json; charset=UTF-8{ "code": "ERR-00001", "message": "Неверный запрос. Неверный bearer"} |

### API уведомления IDP об изменении статуса УЗ v2 (планируется к выводу из эксплуатации)

Для обеспечения поддержки версионности данную версию принято считать версией v2. Используется {url IDP} из конфигурации (idp\_notify\_params.callback\_url) без указания версии в адресе запроса. API используется для извещения не только о результатах регистрации, но вообще об изменении статуса УЗ, в т.ч. деактивации, блокировки.

**Вызов сервиса**

POST https://{URL Провайдера идентификации для отправки уведомления о результатах регистрации},

где {URL Провайдера идентификации} – URL IDP, используемый для уведомления о результатах регистрации (idp\_notify\_params.callback\_url).

Заголовки запроса: Authorization: Bearer {заданный авторизационный токен}, Content-Type: application/json.

Состав тела запроса:

|  |  |  |  |
| --- | --- | --- | --- |
| **Поле** | **Тип** | **Обязательность** | **Описание** |
| user\_id | String | Да | Идентификатор учетной записи Пользователя в информационной системе провайдера идентификации |
| stu | String | Да | Статус результата операции в ГИС ЕБС.Принимает значения:**"A"** - Пользователь успешно зарегистрирован**"B"** - Пользователь заблокирован**"D"** – Пользователь/БШ деактивирован**"F"** - Неуспешная попытка регистрации Пользователя |
| bio\_class | String | Нет | Класс доверияExtractAndSaveResults.bio\_class |
| displayed\_bio\_type | String | Нет | Отображаемый тип биометрии |
| exp\_on | Long | Нет | Дата истечения срока жизни БДн в миллисекундах |

Пример запроса:

|  |
| --- |
| POST https://test.idp.ru/send/stu/here http/1.1Content-Type: application/json; charset=utf-8Authorization: Bearer bearer\_token{ "user\_id": "1000453364", "stu": "A", "bio\_class":"import\_high", "displayed\_bio\_type":"Подтвержденная", "exp\_on":179559879} |

**Успешный ответ**

200 OK без HTTP BODY

**Ошибки метода**

В случае ошибки метод должен вернуть HTTP-код + описание ошибки в BODY. Ошибки реализуются на стороне ИС Провайдера идентификации. Перечень и количество полей в JSON BODY не регламентируется и реализуется на усмотрение ИС Провайдера идентификации.

Пример запроса:

|  |
| --- |
| HTTP/1.1 400 Bad RequestContent-Type: application/json; charset=UTF-8{ "code": "ERR-00001", "message": "Неверный запрос. Неверный bearer"} |

### API уведомления IDP об изменении статуса УЗ v3

Для обеспечения поддержки версионности данную версию принято считать версией v3. Используется {url IDP} из конфигурации (idp\_notify\_params.callback\_url) без указания версии в адресе запроса. API используется для извещения не только о результатах регистрации, но вообще об изменении статуса УЗ, в т.ч. деактивации, блокировки.

**Вызов сервиса**

POST https://{URL Провайдера идентификации для отправки уведомления о результатах регистрации},

где {URL Провайдера идентификации} – URL IDP, используемый для уведомления о результатах регистрации (idp\_notify\_params.callback\_url).

Заголовки запроса: Authorization: Bearer {заданный авторизационный токен}, Content-Type: application/json.

Состав тела запроса:

|  |  |  |  |
| --- | --- | --- | --- |
| **Поле** | **Тип** | **Обязательность** | **Описание** |
| user\_id | String | Да | Идентификатор учетной записи Пользователя в информационной системе провайдера идентификации |
| stu | String | Да | Статус результата операции в ГИС ЕБС.Принимает значения:**"A"** - Пользователь успешно зарегистрирован**"B"** - Пользователь заблокирован**"D"** – Пользователь/БШ деактивирован**"F"** - Неуспешная попытка регистрации Пользователя |
| bio\_class | String | Нет | Класс доверияExtractAndSaveResults.bio\_class |
| displayed\_bio\_type | String | Нет | Отображаемый тип биометрии |
| exp\_on | Long | Нет | Дата истечения срока жизни БДн в миллисекундах |
| event\_time | Long | да | Дата и время создания события в формате unix timestamp + microseconds (точность до микросекунд). Параметр берется из сообщения очереди, инициировавшего отправку запроса. |

Пример запроса:

|  |
| --- |
| POST https://test.idp.ru/send/stu/here http/1.1Content-Type: application/json; charset=utf-8Authorization: Bearer bearer\_token{ "user\_id": "1000453364", "stu": "A", "bio\_class":"import\_high", "displayed\_bio\_type":"Подтвержденная", "exp\_on":179559879**,**"**event\_time**"**: 1675066824123456**} |

**Успешный ответ**

200 OK без HTTP BODY

**Ошибки метода**

В случае ошибки метод должен вернуть HTTP-код + описание ошибки в BODY. Ошибки реализуются на стороне ИС Провайдера идентификации. Перечень и количество полей в JSON BODY не регламентируется и реализуется на усмотрение ИС Провайдера идентификации.

Пример запроса:

|  |
| --- |
| HTTP/1.1 400 Bad RequestContent-Type: application/json; charset=UTF-8{ "code": "ERR-00001", "message": "Неверный запрос. Неверный bearer"} |

## API уведомления IDP о результатах сопоставления УЗ

Уведомление Провайдера идентификации о завершении мэтчинга УЗ осуществляется со стороны ГИС ЕБС в виде POST-запроса на URL Провайдера идентификации для отправки уведомлений о результатах мэтчинга, с использованием авторизационного токена. Токен постоянный, типа Bearer, генерируется на стороне ИС Провайдера идентификации и передается в ГИС ЕБС. В случае обновления, новый токен должен быть также передан в ГИС ЕБС. Значения URL и авторизационного токена указываются при регистрации Провайдера идентификации в ГИС ЕБС. Провайдер идентификации на своей стороне должен реализовать REST API, обеспечивающий прием и корректную обработку соответствующего запроса от ГИС ЕБС.

**Вызов сервиса**

POST {URL Провайдера идентификации для отправки уведомления о завершении мэтчинга}

Заголовок: Authorization: Bearer {заданный авторизационный токен}, Content-Type: application/json.

Описание тела запроса:

|  |  |  |  |
| --- | --- | --- | --- |
| **Поле** | **Тип** | **Обязательность** | **Описание** |
| description | String | Нет | Текст ошибки |
| request\_id | String | Да | Идентификатор запроса |
| stu | String | Да | Статус результата регистрации Пользователя в ГИС ЕБС.Принимает значение:**«MA»** - успешный мэтчинг (связывание УЗ пользователя);**«MF»** - неуспешная попытка мэтчинга (связывания УЗ пользователя) |
| user\_id | string | Да | Идентификатор учетной записи Пользователя в информационной системе провайдера идентификации |

Пример запроса при успешном мэтчинге:

|  |
| --- |
| { "request\_id": "dd003e53-2700-4cf5-85af-42d5584a5c05", "user\_id": "1000453364", "stu": "MA"} |

Пример запроса при неуспешном мэтчинге:

|  |
| --- |
| { "request\_id": "dd003e53-2700-4cf5-85af-42d5584a5c05", "user\_id": "1000453364", "stu": "MF", "description": "Неверный запрос. Неверный параметр matching"} |

**Успешный ответ**

200 OK без HTTP BODY

**Ошибки метода**

HTTP-код + описание ошибки в BODY. Ошибки реализуются на стороне ИС Провайдера идентификации. Перечень и количество полей в JSON BODY не регламентируется и реализуется на усмотрение ИС Провайдера идентификации.

Пример ответа с ошибкой:

|  |
| --- |
| HTTP/1.1 400 Bad RequestContent-Type: application/json; charset=UTF-8{ "code": "ERR-00001", "message": "Неверный запрос. Неверный bearer"} |

## API деактивации УЗ Пользователя

В случае получения уведомления о деактивации УЗ Пользователя, все привязанные к ней БКШ получают отметку о деактивации.

Деактивация УЗ производится:

* + администратором ГИС ЕБС в ручном режиме, с использованием интерфейса модуля администрирования и управления доступом;
	+ администратором или Пользователем в личном кабинете Провайдера идентификации.

**Вызов сервиса**

DELETE /api/v3/users/deactivate-acc

Заголовки:

* + Authorization: Bearer {JWT, формируется в соответствии с RFC 7519 <https://datatracker.ietf.org/doc/html/rfc7519>} без padding-ов.
	+ Content-Type: application/json
	+ Cache-Control: no-cache
	+ Host: {ГИС ЕБС host}

Тело запроса: опциональный JSON, содержащий перечень дополнительных данных

Состав PAYLOAD в JWT описан ниже.

JWT формируется в соответствии с RFC 7519 <https://datatracker.ietf.org/doc/html/rfc7519> без padding-ов.

Состав PAYLOAD в JWT:

|  |  |  |  |
| --- | --- | --- | --- |
| **Наименование параметра** | **Тип данных** | **Обязательность** | **Описание** |
| iss | String | да | Полученный от IDP идентификатор (чувствительная к регистру строка или URI, которая является уникальным идентификатором стороны, генерирующей токен) Например: http(s)://example.ru |
| sub | String | да | Идентификатор УЗ Пользователя IDP (чувствительная к регистру строка или URI, которая является уникальным идентификатором стороны, о которой содержится информация в данном токене) |
| aud | String или Array of Strings | нет | Чувствительная к регистру строка или URI, либо массив чувствительных к регистру строк или URI, являющийся списком получателей данного токена. Когда принимающая сторона получает JWT с данным ключом, она должна проверить наличие себя в получателях — иначе проигнорировать токен (audience) |
| exp | Number | да | Время в формате Unix Time, определяющее момент, когда токен станет не валидным (expiration) |
| nbf | Number | нет | Время в формате Unix Time, ранее которого нельзя использовать токен |
| iat | Number | да | Время в формате Unix Time, определяющее момент, когда токен был создан |
| cert\_id | string | да | id сертификата, которым подписана JWT. В процессе подключения к ГИС ЕБС, ИС контрагента передает public key, который сохраняется в ГИС ЕБС, где ему присваивается идентификатор и передается обратно в ИС КА. Этот идентификатор и является cert\_id. |

Пример запроса:

|  |
| --- |
| DELETE /api/v3/users/deactivate-acc HTTP/1.1Host: example.comContent-Type: application/jsonAuthorization: Bearer eyJhbGciOiJHT1NUMzQxMF8yMDEyXzI1NiIsInR5cCI6IkpXVCJ9.eyJpc3MiOiJleHRJRDEiLCJzdWIiOiJjb2ZmZWViZWFuIiwiYXVkIjoxNjQzODcyMjA2LCJleHAiOjE2NDQzMzM5MDUsIm5iZiI6MTY0NDIwMzkwNSwiaWF0IjoxNjQ0MjAzOTA1LCJ0cnVzdF9jaXJjbGUiOiJ0ZXN0IiwiY2VydF9pZCI6NDA1NDExMjE5MzYxfQ.hmKMNkS7jYqDZxxszjigkaIuHWNwNltIhyaUCCxDPZfUBnOqkkzQjWqpPvFQPPAeTiwQTnFTwFLCRZaWGnUkqURoNvRMVimmUlfTJzCIhQEreiWqnSIsfmFT\_DPKBVD5xxtk5-TMM87CLC0vVjIO9ssGwdyhgZ9szMjeCache-Control: no-cache |

Успешный ответ

В случае успешного выполнения запроса ГИС ЕБС возвращает HTTP-код 200 OK без HTTP BODY.

Пример успешного ответа:

|  |
| --- |
| HTTP/1.1 200 OK |

**Ошибки метода**

В случае возникновения ошибки при обработке запроса, ГИС ЕБС возвращает вызывающей стороне HTTP-код ошибки и описания в BODY:

|  |  |  |  |
| --- | --- | --- | --- |
| Код ответа HTTP | Значение параметра "code" | Описание (параметр "message") | Описание возникновения ошибки |
| 400 | EBS-010003 | Неверный запрос | Неверно составлен запрос |
| 400 | EBS-010103 | Маркер доступа не содержит обязательного параметра | При отсутствии iss в payload, отсутствие необходимых полей для pipeline |
| 400 | EBS-010116 | БКШ не найден | Биометрические данные пользователя не найдены |
| 400 | EBS-010117 | БКШ не активен | Биометрические данные пользователя не активны |
| 400 | EBS-010118 | Пользователь уже деактивирован |  |
| 400 | EBS-010301 | Пользователь не найден |  |
| 401 | EBS-010101 | Ошибка проверки маркера доступа | При проверке JWT, в случае: в запросе более или менее 3(трёх) частей: header, payload, signature; ошибка десериализации header, payload, signature из base64 → json; отсутствия alg в header; |
| 401 | EBS-010102 | Ошибка проверки ЭП Провайдера идентификации | При проверке JWT, в случае: не получения списка ключей (для сервиса подписания); не прохождения проверки подписи в сервисе подписания; |
| 401 | EBS-010104 | Маркер доступа просрочен | При проверке JWT, в случае: exp меньше или равно системного времени; iat больше системного времени; nbf больше текущего времени; |
| 403 | EBS-02030 | Отказано в доступе. Указанный Провайдер идентификации отсутствует в системе | Через ISS определено IDP, но нет в реестре; |
| 403 | EBS-010109 | Провайдеру идентификации (IDP) запрещен доступ к ЕБС |  |
| 403 | EBS-02031 | Отказано в доступе. Указанный Провайдер идентификации заблокирован в системе | Через ISS определено IDP, она найдена в реестре, её статус неактивен; |
| 500 | EBS-010001 | Внутренняя ошибка API | Ошибка на стороне ГИС ЕБС |
| 500 | EBS-010002 | Сервис в настоящее время не может выполнить запрос из-за большой нагрузки или технических работ на сервере | Ошибка на стороне ГИС ЕБС |
| 503 | EBS-08001 | Сервис временно не доступен | Ошибка на стороне ГИС ЕБС |

Пример ответа с ошибкой:

|  |
| --- |
| HTTP/1.1 401 UnauthorizedContent-Type: application/json; charset=UTF-8{ "code": "EBS-010101", "message": "Ошибка проверки маркера доступа"} |

# API биометрической идентификации Пользователя

## API старта сессии биометрической идентификации

### API старта сессии биометрической идентификации v1 (планируется к выводу из эксплуатации)

**Метод «Старт идентификации в ЕБС» предназначен для создания сессии биометрической идентификации Пользователя, зарегистрированного в ГИС ЕБС**.

**Вызов сервиса**

POST <host>:<port>identification/api/v1/start

Заголовки запроса:

* + Host: {host ГИС ЕБС}.
	+ Content-Type:application/json.
	+ X-EBS-TraceProcess: true (необязательный заголовок, необходимый для проверки взаимодействия с использованием Технологического портала, возможные значения true или false, предназначен для отслеживания тестовых запросов с использованием технологического портала ГИС ЕБС).
	+ Authorization: Bearer {JWT от провайдера идентификации, сформированный в соответствии с RFC 7519}.
	+ Cache-Control: no-cache.

**Описание запроса**

JWT.HEADER – описание свойств токена, в т.ч. описание используемого алгоритма для подписи.

JWT.PAYLOAD – содержимое токена (см. ниже в параметрах запроса).

JWT.SIGNATURE – подпись запроса. Запрос должен быть подписан Cades-T или PLAIN, закодированный в формате Base64url.

**Входные параметры запроса**

Передаются в формате JWT-токена.

Payload JWT указан ниже.

|  |  |  |  |
| --- | --- | --- | --- |
| Наименование параметра | Тип данных | Обязательность | Описание |
| redirect | string | нет | Передается в виде query-параметра в строке запроса. Полный URL ИС Поставщика БДн, на который ЕБС осуществит перенаправление пользователя после удачной идентификации. В качестве зарегистрированного имени хоста данного URL допускается: FQDN хоста (не ниже домена второго уровня), или localhost (только для тестовых сред), или IPv4-адрес (только для тестовых сред). Используется только когда есть указание на использование интерфейса ГИС ЕБС:* WEB-интерфейс текущий (115-ФЗ),
* WEB-интерфейс новый (фото),
* WEB-интерфейс новый (аудио).

Для остальных случаев параметр redirect не нужен. По той же логике строится обязательность поля Location в ответах 1-го и 3-го запроса. |
| metadata | JSON-объект | да | Передается в теле запроса. Содержит перечень дополнительных данных согласно спецификации объекта metadata (см. Приложение №1). |
| bio\_collecting\_type | string | да | Требуемая мнемоника согласованной схемы сбора БО. Возможные значения и соответствующие им параметры описаны в Перечне возможных мнемоник (см. Приложение №3): на данный момент следует передавать только мнемонику: face\_with\_passive\_liveness\_and\_webinterface.Не поддерживает мнемонику с постфиксом \_age |
| external\_transaction\_id | string | да | Идентификатор транзакции на стороне ИС |

Описание параметров PAYLOAD:

|  |  |  |  |
| --- | --- | --- | --- |
| Наименование параметра | Тип данных | Обязательность | Описание |
| iss | string  | да | Полученный от IDP идентификатор (чувствительная к регистру строка или URI, которая является уникальным идентификатором стороны, генерирующей токен), например: «https://testidp.ru» |
| sub  | string | да | Идентификатор устройства сбора (или идентификатор конкретного магазина). |
| aud | string или array of strings | нет | Чувствительная к регистру строка или URI, либо массив чувствительных к регистру строк или URI, являющийся списком получателей данного токена. Когда принимающая сторона получает JWT с данным ключом, она должна проверить наличие себя в получателях — иначе проигнорировать токен (audience). |
| exp | number | да | Время в формате Unix Time, определяющее момент, когда токен станет не валидным (expiration) |
| nbf | number | нет | Время в формате Unix Time, ранее которого нельзя использовать токен. |
| iat | number | да | Время в формате Unix Time, определяющее момент, когда токен был создан. |
| client\_id | string | да | Мнемоника Поставщика БДн. |

Пример JWT.payload:

|  |
| --- |
| { "iss":"http(s):test.idp.ru/urn", "sub":"X5/654189126" "iat":1551940551, "exp":1551941153, "client\_id":"TEST\_SYSTEM"} |

Пример запроса:

|  |
| --- |
| POST /identification/api/v1/start?redirect=https%3A%2F%2Ftest.client.local%2F HTTP/1.1Host: int.ebs.ruContent-Type: application/jsonX-EBS-TraceProcess: trueAuthorization: Bearer {JWT от IDP}Cache-Control: no-cache{ "metadata":{ "date":"1520467814933", "time\_zone":"2018-03-30T17:30:09.453+0500" }, "bio\_collecting\_type":" face\_with\_passive\_liveness\_and\_webinterface ", "external\_transaction\_id": "3d744bf8-c51b-4a41-bdd1-e59c2c041f55"} |

**Успешный ответ**

В случае успешного ответа метод возвращает HTTP-код 200 со следующими заголовками.

* Location - заголовок содержит URL web-формы ГИС ЕБС, на который Поставщик БДн осуществит перенаправление пользователя для снятия биометрических образцов. В составе URL присутствует в виде параметра адрес redirect, полученный в запросе. Если мнемоника верификации подразумевает использование видеопотока, то URL веб-формы дополнительно содержит WebSocket для управления. Дополнительно в составе Location передаются следующие query-параметры:

|  |  |  |  |
| --- | --- | --- | --- |
| **Наименование параметра** | **Тип данных** | **Обязательность** | **Описание** |
| redirect | String | да | URL-адрес страницы ИС КА, переданный в параметрах запроса, на которую пользователь будет перенаправлен в случае ошибки. Передается в составе HTTP заголовка «Location» |
| bs\_type | Int | да | Тип сбора биометрии, формируется исходя из полученного bio\_collection\_type в запросе |
| session\_id | String | да | Идентификатор сессии идентификации в ГИС ЕБС (например, 668E49B9CAF645F786601F2432A952B3) |
| video\_control | String | нет | URL модуля управления видеопотоком (в случае использования WEB интерфейса ЕБС) |

* Session-Id – идентификатор сессии идентификации в ГИС ЕБС (см. выше параметр session\_id в составе Location, передается в дополнительном HTTP заголовке «Session-Id»).

Пример успешного ответа:

|  |
| --- |
| HTTP/1.1 200 OKLocation:https://int.ebs.ru/vrf?session\_id=668E49B9CAF645F786601F2432A952B3&redirect=https%3A%2F%2bank.example.com%2Fiss%2Fcode%2Fverify&bs\_type=0Session-Id: 668E49B9CAF645F786601F2432A952B3 |

**Ошибки метода**

В случае возникновения ошибки при обработке запроса ЕБС возвращает вызывающей стороне коды ответов HTTP и описания ошибок в HTTP BODY, согласно таблице ниже.

Коды ошибок:

|  |  |  |
| --- | --- | --- |
| Код ответа HTTP | Значение параметра «code» | Описание (параметр «message») |
| 403 | EBS-010203 | Системе-клиенту (ИС Поставщика БДн) запрещен доступ к ЕБС |
| 400 | EBS-010003 | Неверный запрос. {Описание ошибки} |
| 400 | EBS-010004 | Запрос не содержит обязательного параметра {название параметра} |
| 400 | EBS-02024 | Отсутствуют обязательные данные/Некорректно сформированный запрос |
| 401 | EBS-010101 | Ошибка проверки маркера доступа |
| 500 | EBS-010001 | Внутренняя ошибка API |
| 400 | EBS-010303 | Время жизни сессии истекло |
| 501 | EBS-08001 | Сервис временно не доступен |

Пример ответа с ошибкой:

|  |
| --- |
| HTTP/1.1 400 Bad RequestContent-Type: application/json; charset=UTF-8   {  "code": "EBS-010303",  "message": " Время жизни сессии истекло"} |

### API старта сессии биометрической идентификации v2

**Метод «Старт идентификации в ЕБС» предназначен для создания сессии биометрической идентификации Пользователя, зарегистрированного в ГИС ЕБС**.

**Вызов сервиса**

POST <host>:<port>identification/api/v2/start

Заголовки запроса:

* + Host: {host ГИС ЕБС}.
	+ Content-Type:application/json.
	+ X-EBS-TraceProcess: true (необязательный заголовок, необходимый для проверки взаимодействия с использованием Технологического портала, возможные значения true или false, предназначен для отслеживания тестовых запросов с использованием технологического портала ГИС ЕБС).
	+ Authorization: Bearer {JWT от провайдера идентификации, сформированный в соответствии с RFC 7519}.
	+ Cache-Control: no-cache.

**Описание запроса**

JWT.HEADER – описание свойств токена, в т.ч. описание используемого алгоритма для подписи.

JWT.PAYLOAD – содержимое токена (см. ниже в параметрах запроса).

JWT.SIGNATURE – подпись запроса. Запрос должен быть подписан Cades-T или PLAIN, закодированный в формате Base64url.

**Входные параметры запроса**

Передаются в формате JWT-токена.

Payload JWT указан ниже.

|  |  |  |  |
| --- | --- | --- | --- |
| Наименование параметра | Тип данных | Обязательность | Описание |
| redirect | string | нет | Передается в виде query-параметра в строке запроса. Полный URL ИС Поставщика БДн, на который ЕБС осуществит перенаправление пользователя после удачной идентификации. В качестве зарегистрированного имени хоста данного URL допускается: FQDN хоста (не ниже домена второго уровня), или localhost (только для тестовых сред), или IPv4-адрес (только для тестовых сред). Используется только когда есть указание на использование интерфейса ГИС ЕБС:* WEB-интерфейс текущий (115-ФЗ),
* WEB-интерфейс новый (фото),
* WEB-интерфейс новый (аудио).

Для остальных случаев параметр redirect не нужен. По той же логике строится обязательность поля Location в ответах 1-го и 3-го запроса. |
| metadata | JSON-объект | да | Передается в теле запроса. Содержит перечень дополнительных данных согласно спецификации объекта metadata (см. Приложение №1). |
| bio\_collecting\_type | string | да | Требуемая мнемоника согласованной схемы сбора БО. Возможные значения и соответствующие им параметры описаны в Перечне возможных мнемоник (см. Приложение №3. Для использования проверки возраста следует выбирать мнемонику с постфиксом \_age. |
| external\_transaction\_id | string | да | Идентификатор транзакции на стороне ИС |

Описание параметров PAYLOAD:

|  |  |  |  |
| --- | --- | --- | --- |
| Наименование параметра | Тип данных | Обязательность | Описание |
| iss | string  | да | Полученный от IDP идентификатор (чувствительная к регистру строка или URI, которая является уникальным идентификатором стороны, генерирующей токен), например: «https://testidp.ru» |
| sub  | string | да | Идентификатор устройства сбора (или идентификатор конкретного магазина). |
| aud | string или array of strings | нет | Чувствительная к регистру строка или URI, либо массив чувствительных к регистру строк или URI, являющийся списком получателей данного токена. Когда принимающая сторона получает JWT с данным ключом, она должна проверить наличие себя в получателях — иначе проигнорировать токен (audience). |
| exp | number | да | Время в формате Unix Time, определяющее момент, когда токен станет не валидным (expiration) |
| nbf | number | нет | Время в формате Unix Time, ранее которого нельзя использовать токен. |
| iat | number | да | Время в формате Unix Time, определяющее момент, когда токен был создан. |
| client\_id | string | да | Мнемоника Поставщика БДн. |
| pin\_check\_necessity | string | нет | Необходимость вызова формы PIN-кода. Может принимать значения:* pin\_require (запросить ПИН);
* without\_pin (не запрашивать ПИН);
* ebs\_resolve (ГИС ЕБС решит сама).

В случае если параметр пришел с пустым значением или если отсутствует, принимается значение "without\_pin" (не запрашивать ПИН). |

Пример JWT.payload:

|  |
| --- |
| { "iss":"http(s):test.idp.ru/urn", "sub":"X5/654189126" "iat":1551940551, "exp":1551941153, "client\_id":"TEST\_SYSTEM", "pin-check-necessity":"pin\_require"} |

Пример запроса:

|  |
| --- |
| POST /identification/api/v1/start?redirect=https%3A%2F%2Ftest.client.local%2F HTTP/1.1Host: int.ebs.ruContent-Type: application/jsonX-EBS-TraceProcess: trueAuthorization: Bearer {JWT от IDP}Cache-Control: no-cache{ "metadata":{ "date":"1520467814933", "time\_zone":"2024-10-30T17:30:09.453+0500" }, "bio\_collecting\_type":" face\_with\_passive\_liveness\_and\_webinterface\_age", "external\_transaction\_id": "3d744bf8-c51b-4a41-bdd1-e59c2c041f55"} |

**Успешный ответ**

В случае успешного ответа метод возвращает HTTP-код 200 со следующими заголовками.

* Location - заголовок содержит URL web-формы ГИС ЕБС, на который Поставщик БДн осуществит перенаправление пользователя для снятия биометрических образцов. В составе URL присутствует в виде параметра адрес redirect, полученный в запросе. Если мнемоника верификации подразумевает использование видеопотока, то URL веб-формы дополнительно содержит WebSocket для управления. Дополнительно в составе Location передаются следующие query-параметры:

|  |  |  |  |
| --- | --- | --- | --- |
| **Наименование параметра** | **Тип данных** | **Обязательность** | **Описание** |
| redirect | String | да | URL-адрес страницы ИС КА, переданный в параметрах запроса, на которую пользователь будет перенаправлен в случае ошибки. Передается в составе HTTP заголовка «Location» |
| bs\_type | Int | да | Тип сбора биометрии, формируется исходя из полученного bio\_collection\_type в запросе |
| session\_id | String | да | Идентификатор сессии идентификации в ГИС ЕБС (например, 668E49B9CAF645F786601F2432A952B3) |
| video\_control | String | нет | URL модуля управления видеопотоком (в случае использования WEB интерфейса ЕБС) |

* Session-Id – идентификатор сессии идентификации в ГИС ЕБС (см. выше параметр session\_id в составе Location, передается в дополнительном HTTP заголовке «Session-Id»).

Пример успешного ответа:

|  |
| --- |
| HTTP/1.1 200 OKLocation: https://int.ebs.ru/vrf?session\_id=668E49B9CAF645F786601F2432A952B3&redirect=https%3A%2F%2bank.example.com%2Fiss%2Fcode%2Fverify&bs\_type=1Session-Id: 668E49B9CAF645F786601F2432A952B3 |

**Ошибки метода**

В случае возникновения ошибки при обработке запроса ЕБС возвращает вызывающей стороне коды ответов HTTP и описания ошибок в HTTP BODY, согласно таблице ниже.

Коды ошибок:

|  |  |  |
| --- | --- | --- |
| Код ответа HTTP | Значение параметра «code» | Описание (параметр «message») |
| 403 | EBS-010203 | Системе-клиенту (ИС Поставщика БДн) запрещен доступ к ЕБС |
| 400 | EBS-010003 | Неверный запрос. {Описание ошибки} |
| 400 | EBS-010004 | Запрос не содержит обязательного параметра {название параметра} |
| 400 | EBS-02024 | Отсутствуют обязательные данные/Некорректно сформированный запрос |
| 401 | EBS-010101 | Ошибка проверки маркера доступа |
| 500 | EBS-010001 | Внутренняя ошибка API |
| 400 | EBS-010303 | Время жизни сессии истекло |
| 501 | EBS-08001 | Сервис временно не доступен |

Пример ответа с ошибкой:

|  |
| --- |
| HTTP/1.1 400 Bad RequestContent-Type: application/json; charset=UTF-8   {  "code": "EBS-010003",  "message": "Неверный запрос. {описание ошибки}"} |

## API приема БО для биометрической идентификации

### API приема БО для биометрической идентификации v1 (планируется к выводу из эксплуатации)

**Метод предназначен для приема БО на биометрическую идентификацию с целью прохождения биометрической идентификации Пользователя, зарегистрированного в ГИС ЕБС, с отправкой ИС КА запроса и передачей БО для проведения процесса идентификации. Используется для получения БО на идентификацию и возврата результата биометрической идентификации.**

**Вызов сервиса**

POST <host>:<port>identification/api/v1/*{session\_id}*/upload

**где** *{session\_id} –* **идентификатор сессии идентификации в ЕБС, полученный в ответе метода «Старт идентификации в ЕБС».**

**Заголовки запроса:**

* + Host: {host ГИС ЕБС}
	+ Content-Type: multipart/form-data; boundary={разделитель}
	+ User-Agent: {тип и характеристики ПО}
	+ X-EBS-TraceProcess: true (необязательный заголовок, необходимый для проверки взаимодействия с использованием Технологического портала)
	+ Client-Type: {тип клиента}
	+ Accept: application/json
	+ Cache-Control: no-cache

Заголовки вложенных сущностей:

* + Content-Disposition: form-data; name={название содержимого}
	+ Content-Type: {тип содержимого по MIME}

**Параметры запроса**

|  |  |  |  |
| --- | --- | --- | --- |
| Наименование параметра | Тип данных | Обязательность | Описание |
| **Часть multipart для передачи биометрических данных:** |
| bs\_<мнемоника> | Части multipart | да | Содержит биометрические образцы для извлечения БШ.Заголовочные поля:* Content-Disposition: form-data
* Content-Type:
	+ video/mp4;
	+ video/mov;
	+ image/jpeg;
	+ image/png;
	+ audio/wav;
* name="bs\_photo", "bs\_audio", "bs\_video" (в соответствии с заданной мнемоникой идентификации);
* filename="xxx.jpg"
 |
| **Часть multipart для передачи инструкций:** |
| liveness\_action | Часть multipart | нет | Часть multipart для передачи описания примененного метода обнаружения живучести.Заголовочные поля:* Content-Disposition: form-data;
* Content-Type: application/json;
* name="liveness\_action"
 |
| liveness\_action.mnemonic | string | да | Содержит мнемоники согласованных схем проверки Liveness |
| liveness\_action.index | string | да | Содержит указание очередности в запросе согласованной схемы проверки Liveness |
| liveness\_action.actions | JSON-object | да | Содержит перечень необходимых действий метода проверки Liveness на стороне клиентского приложения, исполненных Пользователем |
| actions.type | string | да | Мнемоника исполняемого Пользователем действия |
| actions.index | string | да | Содержит указание очередности в запросе исполняемого Пользователем действия |
| actions.duration | string | да | Содержит время отображения действия Пользователю (в миллисекундах) |
| actions.client\_duration | string | да | Содержит фактическое время исполнения действия Пользователем (в миллисекундах) |
| actions.message | string | да | Содержит инструкцию, описывающую действие, предлагаемое к совершению Пользователем |
| **Часть multipart для передачи дополнительных данных:** |
| Наименование параметра | Тип данных | Обязательность | Описание |
| metadata | Часть multipart | да | Содержит дополнительные данные согласно [Спецификации параметров metadata](https://confluence.ebsbio.tech/pages/viewpage.action?pageId=109412356#API%D0%BF%D1%80%D0%B8%D0%B5%D0%BC%D0%B0%D0%91%D0%9E%D0%B4%D0%BB%D1%8F%D0%B8%D0%B4%D0%B5%D0%BD%D1%82%D0%B8%D1%84%D0%B8%D0%BA%D0%B0%D1%86%D0%B8%D0%B8-metadata) (см. Приложение №1).Заголовочные поля:* Content-Disposition: form-data;
* Content-Type: application/json;
* name="metadata"
 |

Пример запроса:

|  |
| --- |
| POST /identification/api/v1/D530D7AF1EFA47489653FC4CEA5AC625/upload HTTP/1.1Host: int.ebs.ruContent-Type: multipart/form-data; boundary=----WebKitFormBoundary7MA4YWxkTrZu0gWUser-Agent: Mozilla/5.0 (X11; Linux x86\_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/51.0.2704.103 Safari/537.3X-EBS-TraceProcess: trueClient-Type: application/vnd.ebs.v1.mobile.android+jsonAccept: application/jsonCache-Control: no-cache  ------WebKitFormBoundary7MA4YWxkTrZu0gWContent-Disposition: form-data; name="bs\_photo"Content-Type: image/jpeg   {Поток байт Биометрического образца}  ------WebKitFormBoundary7MA4YWxkTrZu0gWContent-Disposition: form-data; name="metadata"Content-Type: application/json   {        "camera\_id":"2",        "screen":"1200;1920",        "device\_number":"0819da27",        "date":"1520467814933"   }------WebKitFormBoundary7MA4YWxkTrZu0gW-- |

**Успешный ответ метода:**

В случае успешного ответа метод возвращает НТТР-код 200 OK. В HTTP заголовке «Location» содержится URL ИС Поставщика БДн, для перенаправления пользователя после успешной идентификации. ГИС ЕБС использует значение URL ИС Поставщика БДн, переданное в параметре «redirect» при вызове метода «Старт идентификации в ЕБС».

Дополнительно в виде заголовков передаются следующие параметры:

|  |  |  |  |
| --- | --- | --- | --- |
| Наименование параметра | Тип данных | Обязательность | Описание |
| **verify\_token** Передается в составе HTTP заголовка "**verification-Token**" | string | да | Контрольное значение (уникальный идентификатор, созданный ГИС ЕБС), необходимое для получения расширенного результата идентификации после успешной идентификации. |
| expiredПередается в дополнительном HTTP заголовке "Session-Expires" | Number | да | Время прекращения действия результата биометрической идентификации пользователя в ЕБС, в миллисекундах с 1 января 1970 г. 00:00:00 GMT.После указанного в параметре момента времени получение расширенного результата идентификации в ЕБС будет невозможно.Может быть уникальным для IDP. По умолчанию принимается равным 15 минутам. |

**Пример ответа:**

|  |
| --- |
| HTTP/1.1 200 OKLocation: http:/test.example.ru?verify\_token=1000188d-2fe2-479b-b8b9-919d0968a33b&expired=1748948741479Session-Expires:1748948741479 Verification-Token: 1000188d-2fe2-479b-b8b9-919d0968a33b |

**Ошибки метода**

В случае возникновения ошибки при обработке запроса перенаправления на указанную при старте идентификации страницу внешней ИС не произойдет. ГИС ЕБС вернет вызывающей стороне код ответа HTTP и описание ошибки в HTTP BODY согласно таблице ниже:

|  |  |  |
| --- | --- | --- |
| Код ответа HTTP | Значение параметра «code» | Описание (параметр «message») |
| 400 | EBS\_010003 | Неверный запрос. Ошибка очередности вызова API |
| 400 | EBS-010004 | Запрос не содержит обязательного параметра {название параметра} |
| 400 | EBS-010105 |

|  |
| --- |
| Биометрический образец отсутствует |

 |
| 400 | EBS-010107 | Не удалось извлечь биометрические признаки |
| 400 | EBS-010119 | Ошибка идентификации (биометрическая идентификация не пройдена) |
| 400 | EBS-010120 | Ошибка прохождения liveness. [Описание ошибки] |
| 400 | EBS-010121 | Превышен лимит попыток идентификации |
| 400 | EBS-010115 | Неверный формат метаданных. Данная ошибка отдается также в случае, если в запросе получен mime-type невалидного формата или mime-type не соответствует модальности передаваемого БО, например: в запросе bs\_audio, а content-type: video/mp4 |
| 400 | EBS-010302 | Идентификатор сессии не найден |
| 400 | EBS-010303 | Время жизни сессии истекло |
| 403 | EBS-010111 | Неверный формат действий (описание действий не совпадают с отправленными) |
| 500 | EBS-010001 | Внутренняя ошибка API |

Пример ответа с ошибкой:

|  |
| --- |
| HTTP/1.1 400 Bad RequestContent-Type: application/json; charset=UTF-8    {  "code": "EBS-010108",  "message": "Ошибка идентификации"} |

### API приема БО для биометрической идентификации v2

**Метод предназначен для приема БО на биометрическую идентификацию с целью прохождения биометрической идентификации Пользователя, зарегистрированного в ГИС ЕБС, с отправкой ИС КА запроса и передачей БО для проведения процесса идентификации. Используется для получения БО на идентификацию и возврата результата биометрической идентификации.**

**Вызов сервиса**

POST <host>:<port>identification/api/v2/*{session\_id}*/upload

**где** *{session\_id} –* **идентификатор сессии идентификации в ЕБС, полученный в ответе метода «Старт идентификации в ЕБС».**

**Заголовки запроса:**

* + Host: {host ГИС ЕБС}
	+ Content-Type: multipart/form-data; boundary={разделитель}
	+ User-Agent: {тип и характеристики ПО}
	+ X-EBS-TraceProcess: true (необязательный заголовок, необходимый для проверки взаимодействия с использованием Технологического портала)
	+ Client-Type: {тип клиента}
	+ Accept: application/json
	+ Cache-Control: no-cache

Заголовки вложенных сущностей:

* + Content-Disposition: form-data; name={название содержимого}
	+ Content-Type: {тип содержимого по MIME}

**Параметры запроса**

|  |  |  |  |
| --- | --- | --- | --- |
| Наименование параметра | Тип данных | Обязательность | Описание |
| **Часть multipart для передачи биометрических данных:** |
| bs\_<мнемоника> | Части multipart | да | Содержит биометрические образцы для извлечения БШ.Заголовочные поля:* Content-Disposition: form-data
* Content-Type:
	+ video/mp4;
	+ video/mov;
	+ image/jpeg;
	+ image/png;
	+ audio/wav;
* name="bs\_photo", "bs\_audio", "bs\_video" (в соответствии с заданной мнемоникой идентификации);
* filename="xxx.jpg"
 |
| **Часть multipart для передачи инструкций:** |
| liveness\_action | Часть multipart | нет | Часть multipart для передачи описания примененного метода обнаружения живучести.Заголовочные поля:* Content-Disposition: form-data;
* Content-Type: application/json;
* name="liveness\_action"
 |
| liveness\_action.mnemonic | string | да | Содержит мнемоники согласованных схем проверки Liveness |
| liveness\_action.index | string | да | Содержит указание очередности в запросе согласованной схемы проверки Liveness |
| liveness\_action.actions | JSON-object | да | Содержит перечень необходимых действий метода проверки Liveness на стороне клиентского приложения, исполненных Пользователем |
| actions.type | string | да | Мнемоника исполняемого Пользователем действия |
| actions.index | string | да | Содержит указание очередности в запросе исполняемого Пользователем действия |
| actions.duration | string | да | Содержит время отображения действия Пользователю (в миллисекундах) |
| actions.client\_duration | string | да | Содержит фактическое время исполнения действия Пользователем (в миллисекундах) |
| actions.message | string | да | Содержит инструкцию, описывающую действие, предлагаемое к совершению Пользователем |
| **Часть multipart для передачи дополнительных данных:** |
| Наименование параметра | Тип данных | Обязательность | Описание |
| metadata | Часть multipart | да | Содержит дополнительные данные согласно [Спецификации параметров metadata](https://confluence.ebsbio.tech/pages/viewpage.action?pageId=109412356#API%D0%BF%D1%80%D0%B8%D0%B5%D0%BC%D0%B0%D0%91%D0%9E%D0%B4%D0%BB%D1%8F%D0%B8%D0%B4%D0%B5%D0%BD%D1%82%D0%B8%D1%84%D0%B8%D0%BA%D0%B0%D1%86%D0%B8%D0%B8-metadata) (см. Приложение №1).Заголовочные поля:* Content-Disposition: form-data;
* Content-Type: application/json;
* name="metadata"
 |

Пример запроса:

|  |
| --- |
| POST  /identification/api/v2/D530D7AF1EFA47489653FC4CEA5AC625/upload HTTP/1.1Host: int.ebs.ruContent-Type: multipart/form-data; boundary=----WebKitFormBoundary7MA4YWxkTrZu0gWUser-Agent: Mozilla/5.0 (X11; Linux x86\_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/51.0.2704.103 Safari/537.3X-EBS-TraceProcess: trueClient-Type: application/vnd.ebs.v1.mobile.android+jsonAccept: application/jsonCache-Control: no-cache  ------WebKitFormBoundary7MA4YWxkTrZu0gWContent-Disposition: form-data; name="bs\_photo", filename="xxx.jpg"Content-Type: image/jpeg   {Поток байт Биометрического образца}  ------WebKitFormBoundary7MA4YWxkTrZu0gWContent-Disposition: form-data; name="bs\_audio", filename="xxx.wav"Content-Type: audio/wav {Поток байт биометрического образца}  ------WebKitFormBoundary7MA4YWxkTrZu0gWContent-Disposition: form-data; name="liveness\_action"Content-Type: application/json [   {      "mnemonic": "move-instructions",      "index": 0,      "actions": [         {            "type": "BLINK",            "index": 0,            "duration": 7000,            "message": "Пожалуйста, моргните"         },         {            "type": "SMILE",            "index": 1,            "duration": 7000,            "message": "Пожалуйста, улыбнитесь"         }      ]   },   {      "mnemonic": "text-instructions",      "index": 1,      "actions": [         {            "type": "numbers-digits",            "index": 0,            "duration": 7000,            "message": "Произнесите цифры:",            "text": "один два три четыре пять"         }      ]   }] ------WebKitFormBoundary7MA4YWxkTrZu0gWContent-Disposition: form-data; name="metadata"Content-Type: application/json   {        "camera\_id":"2",        "screen":"1200;1920",        "device\_number":"0819da27",        "date":"1520467814933"   }------WebKitFormBoundary7MA4YWxkTrZu0gW-- |

**Успешный ответ метода:**

В случае успешного прохождения биометрической идентификации **без запроса на ввод ПИН-кода** метод возвращает НТТР-код 200 OK. В HTTP заголовке «Location» содержится URL ИС Поставщика БДн, для перенаправления пользователя после успешной идентификации. ГИС ЕБС использует значение URL ИС Поставщика БДн, переданное в параметре «redirect» при вызове метода «Старт идентификации в ЕБС».

Дополнительно в виде заголовков передаются следующие параметры:

|  |  |  |  |
| --- | --- | --- | --- |
| Наименование параметра | Тип данных | Обязательность | Описание |
| **verify\_token** Передается в составе HTTP заголовка "**verification-Token**" | string | да | Контрольное значение (уникальный идентификатор, созданный ГИС ЕБС), необходимое для получения расширенного результата идентификации после успешной идентификации. |
| expiredПередается в дополнительном HTTP заголовке "Session-Expires" | Number | да | Время прекращения действия результата биометрической идентификации пользователя в ЕБС, в миллисекундах с 1 января 1970 г. 00:00:00 GMT.После указанного в параметре момента времени получение расширенного результата идентификации в ЕБС будет невозможно.Может быть уникальным для IDP. По умолчанию принимается равным 15 минутам. |

**Пример ответа:**

|  |
| --- |
| HTTP/1.1 200 OKLocation: http:/test.example.ru?verify\_token=1000188d-2fe2-479b-b8b9-919d0968a33b&expired=1748948741479Session-Expires:1748948741479 Verification-Token: 1000188d-2fe2-479b-b8b9-919d0968a33b |

В **случае** успешного прохождения биометрической **идентификации с запросом на ввод ПИН-кода** метод возвращает НТТР-код 200 OK. В HTTP-заголовке «Location» содержится URL ИС Поставщика БДн, для перенаправления пользователя после успешной идентификации. ГИС ЕБС использует значение URL ИС Поставщика БДн, переданное в параметре «redirect» при вызове метода «Старт идентификации в ЕБС».

**В качестве вложенных query\_params передается параметр enter\_pin, в котором хранится ссылка на форму ввода ПИН-кода:**

|  |  |  |  |
| --- | --- | --- | --- |
| Наименование параметра | Тип данных | Обязательность | Описание |
| enter\_pin | String | Нет | URL формы ввода PIN-кода |

**Пример ответа:**

|  |
| --- |
| HTTP/1.1 200 OKLocation: https://client.example.ru/return\_uri?enter\_pin="**URL\_формы\_ввода\_ПИН\_кода**" |

**Ошибки метода**

В случае возникновения ошибки при обработке запроса перенаправления на указанную при старте идентификации страницу внешней ИС не произойдет. ГИС ЕБС вернет вызывающей стороне код ответа HTTP и описание ошибки в HTTP BODY согласно таблице ниже:

|  |  |  |
| --- | --- | --- |
| Код ответа HTTP | Значение параметра «code» | Описание (параметр «message») |
| 400 | EBS\_010003 | Неверный запрос. {Описание ошибки}. Пример: «Неверный запрос. Ошибка очередности вызова API» |
| 400 | EBS-010004 | Запрос не содержит обязательного параметра {название параметра} |
| 400 | EBS-010105 |

|  |
| --- |
| Биометрический образец отсутствует |

 |
| 400 | EBS-010107 | Не удалось извлечь биометрические признаки |
| 400 | EBS-010117 | Ошибка при вызове API |
| 400 | EBS-010119 | Ошибка идентификации (биометрическая идентификация не пройдена) |
| 400 | EBS-010120 | Ошибка прохождения liveness. [Описание ошибки] |
| 400 | EBS-010121 | Превышен лимит попыток идентификации |
| 400 | EBS-010115 | Неверный формат метаданных. Данная ошибка отдается также в случае, если в запросе получен mime-type невалидного формата или mime-type не соответствует модальности передаваемого БО, например: в запросе bs\_audio, а content-type: video/mp4 |
| 400 | EBS-010302 | Идентификатор сессии не найден |
| 400 | EBS-010303 | Время жизни сессии истекло |
| 403 | EBS-010111 | Неверный формат действий (описание действий не совпадают с отправленными) |
| 500 | EBS-010033 | Ошибка при получении данных |
| 500 | EBS-010001 | Внутренняя ошибка API |

Пример ответа с ошибкой:

|  |
| --- |
| HTTP/1.1 400 Bad RequestContent-Type: application/json; charset=UTF-8    {  "code": "EBS-010119",  "message": "Ошибка идентификации (биометрическая идентификация не пройдена)"} |

## API получения расширенного результата

### API получения расширенного результата v1 (планируется к выводу из эксплуатации)

Метод предназначен для предоставления ИС Поставщика БДн расширенного результата 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, а также токена получения расширенного результата идентификации, полученного от ГИС ЕБС на этапе отправки БО.

**Авторизация**

ИС Поставщика БДн в HTTP-заголовке «Authorization» должна:

* указать схему аутентификации «Bearer»;
* передать JWT-токен, сформированный на стороне ИС Поставщика БДн.

**Вызов сервиса**

GET <host>:<port>identification/api/v1/*{session\_id}*/result

**где** *{session\_id} –* **идентификатор сессии идентификации в ЕБС, полученный в ответе метода «Старт идентификации в ЕБС».**

**Заголовки запроса:**

* + Host: {host ГИС ЕБС}.
	+ Content-Type: application/json.
	+ X-EBS-TraceProcess: true (необязательный заголовок, необходимый для проверки взаимодействия с использованием Технологического портала, возможные значения true или false).
	+ Authorization: Bearer {JWT от провайдера идентификации, сформированный в соответствии с RFC 7519}.
	+ Cache-Control: no-cache.

**Описание запроса**

JWT состоит из трёх частей, разделённых точкой, и имеет следующий вид: HEADER.PAYLOAD.SIGNATURE. Каждая из частей токена представляет из себя Base64url Encoding значение.

JWT.HEADER – описание свойств токена, в т.ч. описание используемого алгоритма для подписи.

JWT.PAYLOAD – содержимое токена (см. ниже в параметрах запроса).

JWT.SIGNATURE – подпись запроса. Запрос должен быть подписан Cades-T или PLAIN, закодированный в формате Base64url.

**Входные параметры запроса**

**Описание параметров PAYLOAD:**

|  |  |  |  |
| --- | --- | --- | --- |
| Наименование параметра | Тип данных | Обязательность | Описание |
| iss | string  | да | Мнемоника IDP (чувствительная к регистру строка или [URI](https://ru.wikipedia.org/wiki/URI), которая является уникальным идентификатором стороны, генерирующей токен) |
| sub  | string | да | Идентификатор устройства сбора (или идентификатор конкретного магазина). Чувствительная к регистру строка или URI, которая является уникальным идентификатором стороны, о которой содержится информация в данном токене |
| aud | string или array of strings | нет | Чувствительная к регистру строка или URI, либо массив чувствительных к регистру строк или URI, являющийся списком получателей данного токена. Когда принимающая сторона получает JWT с данным ключом, она должна проверить наличие себя в получателях — иначе проигнорировать токен (audience). |
| exp | number | да | Время в формате Unix Time, определяющее момент, когда токен станет не валидным (expiration) |
| nbf | number | да  | Время в формате Unix Time, ранее которого нельзя использовать токен. |
| iat | number | да | Время в формате Unix Time, определяющее момент, когда токен был создан. |

**Дополнительные параметры PAYLOAD:**

|  |  |  |  |
| --- | --- | --- | --- |
| Наименование параметра | Тип данных | Обязательность | Описание |
| client\_id | string | да | Мнемоника Поставщика БДн. |
| verify\_token | string | да | Контрольное значение (уникальный идентификатор, созданный ЕБС), необходимое для получения расширенного результата после успешной идентификации. |

Пример запроса:

|  |
| --- |
| GET /identification/api/v1/D530D7AF1EFA47489653FC4CEA5AC625/result HTTP/1.1Host: int.ebs.ruAuthorization: eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJpc3MiOiJURVNUX0lEUCIsImF1ZCI6IkVCUyIsImV4cCI6MTYyMTAwMDU2NCwibmJmIjoxNjIwOTk5NjY0LCJpYXQiOjE2MjA5OTk2MDQsImNsaWVudF9pZCI6IlRFU1RfQ0xJRU5UIn0.tM1FwEe9REnoRjqAUdjyDkOnJ77Y1YnjhsWAaGZj1jcCache-Control: no-cache |

Пример JWT.payload:

|  |
| --- |
| { "iss":"http(s):test.idp.ru/urn", "sub":"X5/3587618", "iat":1551940551, "exp":1551941153, "nbf":1584652769, "client\_id":"TEST\_SYSTEM", "verify\_token":"0BCAF243SE9CF4F607E3CEB7EE416D031"} |

**Успешный ответ метода**

В случае успешного ответа, метод возвращает НТТР-код 200 OK, а также тело ответа следующего состава:

|  |  |  |  |
| --- | --- | --- | --- |
| Наименование параметра | Тип данных | Обязательность | Описание |
| extended\_result | string | да | Расширенный результат идентификации, содержащий степени схожести (общая и по каждой из модальностей).Параметр передается в формате JWT токена |
| JWT состоит из трёх частей, разделённых точкой, и имеет следующий вид: HEADER.PAYLOAD.SIGNATURE. Каждая из частей токена представляет из себя Base64urlEncoding значение.JWT.HEADER – описание свойств токена, в том числе описание используемого алгоритма для подписи.JWT.PAYLOAD – непосредственно данные (см. описание параметров PAYLOAD ниже);JWT.SIGNATURE – подпись запроса (запрос должен быть подписан CAdES-T, закодированный в формате Base64url). |
| **Описание параметров PAYLOAD** (JWT.PAYLOAD): |
| Наименование параметра | Тип данных | Обязательность | Описание |
| iss | string | да | Идентификатор организации, выпустившей токен, например для ЕБС: «http:[int-ebs.ru](http://ebs-fr.rtlabs.ru/)» |
| sub | string | да | Идентификатор УЗ пользователя в IDP |
| aud | string | да | Мнемоника ИС Поставщика БДн |
| nbf | number | да | Время в формате [Unix Time](https://ru.wikipedia.org/wiki/UNIX-%D0%B2%D1%80%D0%B5%D0%BC%D1%8F), ранее которого нельзя использовать токен |
| iat | number | да | Время в формате [Unix Time](https://ru.wikipedia.org/wiki/UNIX-%D0%B2%D1%80%D0%B5%D0%BC%D1%8F), определяющее момент, когда токен был создан |
| exp | number | да | Время в формате [Unix Time](https://ru.wikipedia.org/wiki/UNIX-%D0%B2%D1%80%D0%B5%D0%BC%D1%8F), определяющее момент, когда токен станет невалидным |
| result | string | да | Результат биометрической идентификации |
| Extra-Data | string | да | Дополнительные данные из первого запроса |
| **Данные о результатах идентификации identify\_status (JSON) (блок заполняется всегда, с разным набором данных для успешного и не успешного прохождения идентификации):** |
| identify\_status | JSON | да | Данные о результатах идентификации |
| identify\_status.allCount | number | да | Количество сравнений с порогом совпадения выше заданного |
| identify\_status.result | string | да | Статус результата идентификации:* success;
* failed
 |
| identify\_status.transactionId | string | да | Идентификатор транзакции, полученный от подсистемы идентификации (модуль Identify) |
| identify\_status.persons | array | да в случае success | Содержит данные с порогом совпадения выше заданного |
| identify\_status.persons[].id | string | да | ID User от IDP |
| identify\_status.persons[].modalities | array | да | JSON, не именуется |
| identify\_status.persons[].modalities[].modality | string | да | Модальность (photo, sound) |
| identify\_status.persons[].modalities[].score | number | да | Значение схожести [0:1] |
| identify\_status.error | JSON | да в случае failed |  |
| identify\_status.error.code | string | да | Код ошибки |
| identify\_status.error.message | string | да | Сообщение расшифровки ошибки |
| **Данные о результатах прохождения лайвнесс (liveness\_status) (заполняется только при использовании мнемоник, подразумевающих прохождение лайвнесс):** |
| liveness\_status | JSON | да | Данные о прохождении лайвнесс» |
| liveness\_status.status | string | да | Результат прохождения лайвнесс. Может иметь значения:* success;
* failed
 |

**Пример ответа:**

|  |
| --- |
| HTTP/1.1 200 OKContent-Type: application/json; charset=utf-8{"extended\_result":"{Base64url JWT Token с расширенным результатом идентификации}"} |

**Пример JWT.PAYLOAD extended\_result:**

|  |
| --- |
| { "iss": "http(s):test.idp.ru/urn", "sub": "11111111", "aud": "TEST\_SYSTEM", "iat": 1551940551, "exp": 1551941153, "nbf": 1584652769, "result": "success", "Extra-Data": "Some usefull data", "identify\_status": { "transactionId": "5fc03087-d265-11e7-b8c6-83e29cd24f4c", "result": "success", "allCount": 1, "persons": [ { "id": "240409821", "modalities": [ { "modality": "photo", "score": 0.8023058772087097 } ] } ] }, "liveness\_status": { "status": "success" }} |

**Ошибки метода**

В случае возникновения ошибки при обработке запроса, ЕБС возвращает вызывающей стороне коды ответов HTTP и описания ошибок в HTTP BODY, согласно таблице ниже:

|  |  |  |
| --- | --- | --- |
| Код ответа HTTP | Значение параметра «code» | Описание (параметр «message») |
| 400 | EBS-010302 | Идентификатор сессии не найден |
| 400 | EBS-010303 | Время жизни сессии истекло |
| 400 | IDE-1000 | Невалидный формат присланной multipart/form-data |
| 400 | IDE-1001 | Невалидный формат присланных метаданных |
| 400 | IDE-1002 | Передан образец неверной модальности |
| 400 | IDE-1003 | В переданных метаданных представлена невалидная информация о модальностях |
| 400 | IDE-1004 | Передан невалидный идентификатор транзакции в cookie |
| 400 | IDE-1005 | Запрос не содержит обязательного параметра {название параметра} |
| 400 | IDE-1006 | Недопустимое значение параметра {название параметра} |
| 400 | IDE-1007 | Недостаточное количество успешно ответивших вендоров (количество обязательно используемых вендоров, указанное в конфигурациях, не достигнуто) |
| 400 | IDE-1008 | Ошибка запроса в обязательный вендор (вендор, указанный в конфигурациях обязательным, ответил с ошибкой) |
| 400 | EBS-010003 | Неверный запрос. {Описание ошибки} |
| 400 | EBS-010004 | Запрос не содержит обязательного параметра {название параметра} |
| 400 | EBS-02024 | Отсутствуют обязательные данные/Некорректно сформированный запрос |
| 400 | EBS-010303 | Время жизни сессии истекло |
| 401 | EBS-010101 | Ошибка проверки маркера доступа |
| 403 | EBS-010203 | Системе-клиенту (ИС Поставщика БДн) запрещен доступ к ЕБС |
| 500 | EBS-010001 | Внутренняя ошибка API |
| 500 | IDE-0003 | Внутренняя ошибка |
| 500 | IDE-0005 | Внутренняя ошибка |
| 503 | IDE-0004 | Сервис временно недоступен |
| 501 | EBS-08001 | Сервис временно не доступен |

Пример ответа с ошибкой:

|  |
| --- |
| HTTP/1.1 400 Bad RequestContent-Type: application/json; charset=UTF-8    {  "code": "EBS-010302",  "message": "Идентификатор сессии не найден"} |

### API получения расширенного результата v2

Метод предназначен для предоставления ИС Поставщика БДн расширенного результата 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, а также токена получения расширенного результата идентификации, полученного от ГИС ЕБС на этапе отправки БО.

**Авторизация**

ИС Поставщика БДн в HTTP-заголовке «Authorization» должна:

* указать схему аутентификации «Bearer»;
* передать JWT-токен, сформированный на стороне ИС Поставщика БДн.

**Вызов сервиса**

GET <host>:<port>identification/api/v2/*{session\_id}*/result

**где** *{session\_id} –* **идентификатор сессии идентификации в ЕБС, полученный в ответе метода «Старт идентификации в ЕБС».**

**Заголовки запроса:**

* + Host: {host ГИС ЕБС}.
	+ Content-Type: application/json.
	+ X-EBS-TraceProcess: true (необязательный заголовок, необходимый для проверки взаимодействия с использованием Технологического портала, возможные значения true или false).
	+ Authorization: Bearer {JWT от провайдера идентификации, сформированный в соответствии с RFC 7519}.
	+ Cache-Control: no-cache.

**Описание запроса**

JWT состоит из трёх частей, разделённых точкой, и имеет следующий вид: HEADER.PAYLOAD.SIGNATURE. Каждая из частей токена представляет из себя Base64url Encoding значение.

JWT.HEADER – описание свойств токена, в т.ч. описание используемого алгоритма для подписи.

JWT.PAYLOAD – содержимое токена (см. ниже в параметрах запроса).

JWT.SIGNATURE – подпись запроса. Запрос должен быть подписан Cades-T или PLAIN, закодированный в формате Base64url.

**Входные параметры запроса**

|  |  |  |  |
| --- | --- | --- | --- |
| Наименование параметра | Тип данных | Обязательность | Описание |
| session\_id | String | Да | Идентификатор сессии идентификации в ЕБС, полученный в ответе метода «Старт идентификации в ЕБС» |
| **Описание параметров PAYLOAD:** |
| iss | string  | да | Мнемоника IDP (чувствительная к регистру строка или [URI](https://ru.wikipedia.org/wiki/URI), которая является уникальным идентификатором стороны, генерирующей токен) |
| sub  | string | да | Идентификатор устройства сбора (или идентификатор конкретного магазина). Чувствительная к регистру строка или URI, которая является уникальным идентификатором стороны, о которой содержится информация в данном токене |
| aud | string или array of strings | нет | Чувствительная к регистру строка или URI, либо массив чувствительных к регистру строк или URI, являющийся списком получателей данного токена. Когда принимающая сторона получает JWT с данным ключом, она должна проверить наличие себя в получателях — иначе проигнорировать токен (audience). |
| exp | number | да | Время в формате Unix Time, определяющее момент, когда токен станет не валидным (expiration) |
| nbf | number | да  | Время в формате Unix Time, ранее которого нельзя использовать токен. |
| iat | number | да | Время в формате Unix Time, определяющее момент, когда токен был создан. |

**Дополнительные параметры PAYLOAD:**

|  |  |  |  |
| --- | --- | --- | --- |
| Наименование параметра | Тип данных | Обязательность | Описание |
| client\_id | string | да | Мнемоника Поставщика БДн. |
| verify\_token | string | да | Контрольное значение (уникальный идентификатор, созданный ЕБС), необходимое для получения расширенного результата после успешной идентификации. |

Пример запроса:

|  |
| --- |
| GET /identification/api/v2/D530D7AF1EFA47489653FC4CEA5AC625/result HTTP/1.1Host: ebs-int.rtlabs.ruAuthorization: eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJpc3MiOiJodHRwKHMpOnRlc3QuaWRwLnJ1L3VybiIsInN1YiI6Ilg1LzM1ODc2MTgiLCJpYXQiOjE1NTE5NDA1NTEsImV4cCI6MTU1MTk0MTE1MywibmJmIjoxNTg0NjUyNzY5LCJjbGllbnRfaWQiOiJURVNUX1NZU1RFTSIsInZlcmlmeV90b2tlbiI6IjBCQ0FGMjQzU0U5Q0Y0RjYwN0UzQ0VCN0VFNDE2RDAzMSJ9.tM1FwEe9REnoRjqAUdjyDkOnJ77Y1YnjhsWAaGZj1jcCache-Control: no-cache |

Пример JWT.payload:

|  |
| --- |
| { "iss":"http(s):test.idp.ru/urn", "sub":"X5/3587618", "iat":1551940551, "exp":1551941153, "nbf":1584652769, "client\_id":"TEST\_SYSTEM", "verify\_token":"0BCAF243SE9CF4F607E3CEB7EE416D031"} |

**Успешный ответ метода**

В случае успешного ответа метод возвращает НТТР-код 200 OK, а также тело ответа следующего состава:

|  |  |  |  |
| --- | --- | --- | --- |
| Наименование параметра | Тип данных | Обязательность | Описание |
| extended\_result | string | да | Расширенный результат идентификации, содержащий степени схожести (общая и по каждой из модальностей).Параметр передается в формате JWT токена |
| JWT состоит из трёх частей, разделённых точкой, и имеет следующий вид: HEADER.PAYLOAD.SIGNATURE. Каждая из частей токена представляет из себя Base64urlEncoding значение.JWT.HEADER – описание свойств токена, в том числе описание используемого алгоритма для подписи.JWT.PAYLOAD – непосредственно данные (см. описание параметров PAYLOAD ниже);JWT.SIGNATURE – подпись запроса (запрос должен быть подписан CAdES-T, закодированный в формате Base64url). |
| **Описание параметров PAYLOAD** (JWT.PAYLOAD): |
| Наименование параметра | Тип данных | Обязательность | Описание |
| iss | string | да | Идентификатор организации, выпустившей токен, например для ЕБС: «http:[ebs-fr.rtlabs.ru](http://ebs-fr.rtlabs.ru/)» |
| sub | string | да | Идентификатор УЗ пользователя в IDP |
| aud | string | да | Мнемоника ИС Поставщика БДн |
| nbf | number | да | Время в формате [Unix Time](https://ru.wikipedia.org/wiki/UNIX-%D0%B2%D1%80%D0%B5%D0%BC%D1%8F), ранее которого нельзя использовать токен |
| iat | number | да | Время в формате [Unix Time](https://ru.wikipedia.org/wiki/UNIX-%D0%B2%D1%80%D0%B5%D0%BC%D1%8F), определяющее момент, когда токен был создан |
| exp | number | да | Время в формате [Unix Time](https://ru.wikipedia.org/wiki/UNIX-%D0%B2%D1%80%D0%B5%D0%BC%D1%8F), определяющее момент, когда токен станет не валидным |
| result | string | да | Результат биометрической идентификации |
| Extra-Data | string | да | Дополнительные данные из первого запроса |
| **Данные о результатах идентификации identify\_status (JSON) (блок заполняется всегда, с разным набором данных для успешного и не успешного прохождения идентификации):** |
| identify\_status | JSON | да | Данные о результатах идентификации |
| identify\_status.allCount | number | да | Количество сравнений с порогом совпадения выше заданного |
| identify\_status.result | string | да | Статус результата идентификации:* success;
* failed
 |
| identify\_status.transactionId | string | да | Сквозной идентификатор транзакции, полученный от подсистемы идентификации (модуль Identify) |
| identify\_status.persons | array | да в случае success | Содержит данные с порогом совпадения выше заданного |
| identify\_status.persons[].id | string | да | ID User от IDP |
| identify\_status.persons[].idp | String | Да | IDP пользователя |
| identify\_status.persons[].age | Number | Нет | Полный возраст идентифицируемого.Параметр передается только для мнемоник подразумевающих возврат возраста |
| identify\_status.persons[].age\_determined | Boolean | Нет | Флаг успеха при расчете возраста пользователя |
| identify\_status.persons[].modalities | array | да | JSON, не именуется |
| identify\_status.persons[].modalities[].modality | string | да | Модальность (photo, sound) |
| identify\_status.persons[].modalities[].score | number | да | Значение схожести [0:1] |
| identify\_status.error | JSON | да в случае failed |  |
| identify\_status.error.code | string | да | Код ошибки |
| identify\_status.error.message | string | да | Сообщение расшифровки ошибки |
| **Данные о результатах прохождения лайвнесс (liveness\_status) (заполняется только при использовании мнемоник, подразумевающих прохождение лайвнесс):** |
| liveness\_status | JSON | да | Данные о прохождении лайвнесс» |
| liveness\_status.status | string | да | Результат прохождения лайвнесс. Может иметь значения:* success;
* failed
 |

**Пример ответа:**

|  |
| --- |
| HTTP/1.1 200 OKContent-Type: application/json; charset=utf-8{"extended\_result":"{Base64url JWT Token с расширенным результатом идентификации}"} |

**Пример JWT.PAYLOAD extended\_result:**

|  |
| --- |
| {    "iss": "http(s):test.idp.ru/urn",    "sub": "11111111",    "aud": "TEST\_SYSTEM",    "iat": 1551940551,    "exp": 1551941153,    "nbf": 1584652769,    "result": "success",    "Extra-Data": "Some usefull data",    "identify\_status": {        "transactionId": "5fc03087-d265-11e7-b8c6-83e29cd24f4c",        "result": "success",        "allCount": 1,        "persons": [            {                "id": "240409821",                "idp": "sber",                "age": 21,                "age\_determined": "TRUE",                "modalities": [                    {                        "modality": "photo",                        "score": 0.7042558772085213                    }                ]            },            {                "id": "657409833",                "idp": "esia",                "age": 21,                "age\_determined": "TRUE",                "modalities": [                    {                        "modality": "photo",                        "score": 0.8023058772087097                    }                ]            }        ]    },    "liveness\_status": {        "status": "success"    }} |

**Ошибки метода**

В случае возникновения ошибки при обработке запроса, ЕБС возвращает вызывающей стороне коды ответов HTTP и описания ошибок в HTTP BODY, согласно таблице ниже:

|  |  |  |
| --- | --- | --- |
| Код ответа HTTP | Значение параметра «code» | Описание (параметр «message») |
| 400 | EBS-010302 | Идентификатор сессии не найден |
| 400 | EBS-010303 | Время жизни сессии истекло |
| 400 | IDE-1000 | Невалидный формат присланной multipart/form-data |
| 400 | IDE-1001 | Невалидный формат присланных метаданных |
| 400 | IDE-1002 | Передан образец неверной модальности |
| 400 | IDE-1003 | В переданных метаданных представлена невалидная информация о модальностях |
| 400 | IDE-1004 | Передан невалидный идентификатор транзакции в cookie |
| 400 | IDE-1005 | Запрос не содержит обязательного параметра {название параметра} |
| 400 | IDE-1006 | Недопустимое значение параметра {название параметра} |
| 400 | IDE-1007 | Недостаточное количество успешно ответивших вендоров (количество обязательно используемых вендоров, указанное в конфигурациях, не достигнуто) |
| 400 | IDE-1008 | Ошибка запроса в обязательный вендор (вендор, указанный в конфигурациях обязательным, ответил с ошибкой) |
| 400 | EBS-010003 | Неверный запрос. {Описание ошибки} |
| 400 | EBS-010004 | Запрос не содержит обязательного параметра {название параметра} |
| 400 | EBS-02024 | Отсутствуют обязательные данные/Некорректно сформированный запрос |
| 400 | EBS-010303 | Время жизни сессии истекло |
| 401 | EBS-010101 | Ошибка проверки маркера доступа |
| 403 | EBS-010203 | Системе-клиенту (ИС Поставщика БДн) запрещен доступ к ЕБС |
| 500 | EBS-010001 | Внутренняя ошибка API |
| 500 | IDE-0003 | Внутренняя ошибка |
| 500 | IDE-0005 | Внутренняя ошибка |
| 501 | EBS-08001 | Сервис временно не доступен |
| 503 | IDE-0004 | Сервис временно недоступен |

Пример ответа с ошибкой:

|  |
| --- |
| HTTP/1.1 400 Bad RequestContent-Type: application/json; charset=UTF-8    {  "code": "EBS-010302",  "message": "Идентификатор сессии не найден"} |

# API передачи PIN для сверки

## API передачи PIN-кода в ЕБС для проверки в рамках подтверждения биометрических операций

Метод вызывается из Web-формы для передачи в ГИС ЕБС запроса с PIN-кодом для проверки в рамках подтверждения биометрических операций.

Взаимодействие с ГИС ЕБС должно осуществляться по ГОСТ TLS (КС1).

**Вызов**

POST /v1/pin-check

**Описание параметров PAYLOAD**

| **Наименование параметра** | **Тип данных** | **Обязательность** | **Описание** |
| --- | --- | --- | --- |
| session\_id | STRING | да | Идентификатор сессии.Пример: eb128356-deea-42a0-8d73-b2219aefa03d |
| pin | STRING | да | Пин-код.Пример: 1234 |

**Пример запроса:**

|  |
| --- |
| POST /v1/pin-check**Content-Type: application/json; charset=utf-8****{** **"**session\_id**": "**eb128356-deea-42a0-8d73-b2219aefa03d**",** **"**pin"**: "**1234**"****}** |

**Ответ:**

**Media type: application/json.**

В случае успешного ответа, метод возвращает HTTP-ответ 200 OK.

Дополнительно в виде заголовков передаются следующие параметры:

|  |  |  |  |
| --- | --- | --- | --- |
| Наименование параметра | Тип данных | Обязательность | Описание |
| location | String | Нет | Location состоит из 3-х частей:* URL ИС Потребителя БДн для перенаправления пользователя
* verify\_token – токен идентификации
* expired – время жизни токена

verify\_token и expired передаются в качестве query-params. |
| **verify\_token** Передается в составе HTTP заголовка "**verification-Token**" | string | да | Контрольное значение (уникальный идентификатор, созданный ГИС ЕБС), необходимое для получения расширенного результата идентификации после успешной идентификации. |
| expiredПередается в дополнительном HTTP заголовке "Session-Expires" | Number | да | Время прекращения действия результата биометрической идентификации пользователя в ЕБС, в миллисекундах с 1 января 1970 г. 00:00:00 GMT.После указанного в параметре момента времени получение расширенного результата идентификации в ЕБС будет невозможно.Может быть уникальным для IDP. По умолчанию принимается равным 15 минутам. |

Пример:

|  |
| --- |
| { "location": "https://bank.example.com/iss/code/identify?expired=1591702694&verify\_token=ec15d0c6-ab31-4f8a-813e-624dfa00e99b", "verify\_token": "0BCAF243SE9CF4F607E3CEB7EE416D031", "expired": "1499443407648"} |

**Ошибки метода**

В случае возникновения ошибки при обработке запроса возвращаются соответствующие коды ответов HTTP и описания ошибок в HTTP BODY:

|  |  |  |
| --- | --- | --- |
| **Код ответа HTTP** | **Значение параметра «code»** | **Описание (параметр «message»)** |
| 400 | PCS-0001 | Неверный запрос |
| 500 | PCS-0002 | Внутренняя ошибка API |

# ПРИЛОЖЕНИЕ №1. Дополнительные метаданные **(meta)**

Все параметры metadata, перечисленные в таблице ниже, являются обязательными для проверки в запросе.

Помимо целевого значения, все параметры, за исключением **date**, могут принимать следующие значения:

* unknown – значение неизвестно;
* empty – значение пустое;
* error – возникла ошибка при получении значения;
* not\_perm – нет разрешений на получения значения.

Набор приведенных обязательных параметров является исчерпывающим. Набор необязательных параметров (не проверяются в запросе) является неограниченным.

Для сервиса биометрической идентификации обязательным для указания во всех запросах параметром является только параметр date, остальные можно не указывать.

| **№** | **Наименование параметра** | **Обязательность** | **Описание** | **Формат** | **Пример** |
| --- | --- | --- | --- | --- | --- |
|  | date | Обязательное | Дата и время начала операции (формирования запроса клиентом) | timestamp | 1520467814933 |
|  | time\_zone | Обязательное | Временная зона:−      Год;−      Месяц;−      День;−      Часы;−      Минуты;−      Секунды;−      временная зона | yyyy-MM-dd'T'HH:mm:ss.SSSZ | 2018-03-30T17:30:09.453+0500 |
|  | geolocation | Обязательное | Координаты (Геолокация): широта и долгота | latitude;longitude | 51.7556415;55.1028652 |
|  | rooted | Обязательное | Наличие jailbreak или root-доступа в операционной системе | true/false | true |
|  | operating\_system | Обязательное | Операционная система устройства:−      название;−      версия | name version | Android 6.0.1 |
|  | isp | Обязательное | Провайдер | name | MegaFon |
|  | advertising\_id | Обязательное | Идентификатор рекламы устройства (AdID в Android и IDFA в iOS) | value | 38400000-8cf0-11bd-b23e-10b96e40000d |
|  | screen | Обязательное | Разрешение экрана | width;height | 1200;1920 |
|  | dpi | Обязательное | Плотность экрана устройства - значение, единицы измерения плотности пикселей | value | 320 Dpi |
|  | camera\_id | Обязательное | Идентификатор камеры | name | 2 |
|  | locale | Обязательное | Региональные настройки (локаль): страна, язык, название временной зоны.Данный параметр зависит от устройства и выбранных пользователем настроек. | country;language;timezonename | RU;ru;Москва, стандартное время |
|  | device\_serial | Обязательное | Серийный номер мобильного устройства. | deviceNumber | 0819da27 |
|  | imei | Обязательное | IMEI - международный идентификатор мобильного оборудования | value | 357719051789508 |
|  | device\_id | Обязательное | Уникальный идентификатор Android-устройства | value | d1b23eв2f3b480сb |
|  | device\_manufacturer | Обязательное | Производитель устройства | name | asus |
|  | device\_model | Обязательное | Модель устройства | name | Nexus 7 |
|  | device\_cpu | Обязательное | Информация о процессоре устройства | value | ARMv7 Processor rev 0 (v7l) |
|  | sim | Обязательное | Информация о SIM-карте:−      оператор;−      название оператора;−      страна;−      номер сим карты.Можно отдавать раздельно. | simOperator;simOperatorName;simCountryIso;simSerialNumber | 25002;MegaFon;ru;897210285241754519 |

# ПРИЛОЖЕНИЕ №2. Дополнительные данные о метриках системы **(metrics)**

Формат данных:

* дата и время события в формате YYYY-MM-DD HH:MM:SS.MsMsMs;
* string – строка, не пустая;

Помимо целевого значения, все параметры в зависимости от процесса регистрации могут принимать следующие значения:

* unknown – значение неизвестно;
* empty – значение пустое;
* error – возникла ошибка при получении значения;
* not\_perm – нет разрешений на получение значения.

Набор обязательных параметров (проверяются в запросе) является исчерпывающим. Набор необязательных параметров (не проверяются в запросе) является неограниченным.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **№** | **Мнемоника** | **Тип данных** | **Обязательность** | **Описание** |
|  | total\_reg\_time\_end  | timestamp | Обязательное  | Время завершения процесса подготовки пакета и готовности направить пакет в ЕБС  |
|  | new\_client\_time\_start  | timestamp  | Необязательное  | Событие при входе в бизнес-процесс создания нового Клиента в системе поставщика БО или регистрирующего партнера, в случае если Клиент не был найден и его создание необходимо для старта процесса сбора |
|  | new\_client\_time\_end  | timestamp  | Необязательное  | Событие перехода к процессу регистрации на стороне поставщика БО или регистрирующего партнера после создания нового Клиента в системе постащика БО или регистрирующего партнера. |
|  | consent\_time\_start | timestamp | Необязательное | Событие процесса регистрации, которое инициализует сбор согласия на передачу БПДн (вывод экранной формы, запрос такого вывода с Бэк приложения, печать согласия и иное) |
|  | consent\_time\_end | timestamp | Необязательное | Событие процесса регистрации, при котором клиентом было выражено согласие на передачу БПДн (акцепт, переход на экранную форму, отметка оператора и иное)При отсутствии возможности определения timestamp события, передавать <Value>2000-01-01 00:00:00.000</Value> |
|  | photo\_time\_start\_<part> | timestamp | Обязательное | Дата и время, когда инициировано на стороне сервера или прикладного ПО начало съемки лица клиента. Для каждой попытки, последовательно. |
|  | photo\_time\_end\_<part> | timestamp | Обязательное | Дата и время завершения сбора БО изображения лица (получение изображения сервером). Для каждой попытки, последовательно |
|  | front\_bqc\_estimators\_photo\_<part>  | string  | Обязательное  | Строка, передаваемая в библиотекой контроля качества, используемой поставщиком БО, со значениями результатов проверки качества БО изображения лица. Для каждой попытки, последовательно. |
|  | sound\_direct\_time\_start\_<part> | timestamp | Обязательное (при съеме БО) / необязательное (если не снимается БО) | Дата и время, когда инициировано на стороне сервера или прикладного ПО начало сбора первого БО записи голоса. Для каждой попытки, последовательно. |
|  | sound\_direct\_time\_end\_<part> | timestamp | Обязательное (при съеме БО) / необязательное (если не снимается БО) | Дата и время завершения сбора первого БО записи голоса (получение записи сервером). Для каждой попытки, последовательно. |
|  | front\_bqc\_estimators\_sound\_direct\_<part>  | string  | Обязательное (при съеме БО) / необязательное (если не снимается БО  | Строка, передаваемая библиотекой контроля качества, используемой поставщиком БО, со значениями результатов проверки качества первого БО записи голоса. Для каждой попытки, последовательно  |
|  | sound\_reverse\_time\_start\_<part> | timestamp | Обязательное (при съеме БО) / необязательное (если не снимается БО) | Дата и время, когда инициировано на стороне сервера или прикладного ПО начало сбора второго БО записи голоса. Для каждой попытки, последовательно. |
|  | sound\_reverse\_time\_end\_<part> | timestamp | Обязательное (при съеме БО) / необязательное (если не снимается БО) | Дата и время завершения сбора второго БО записи голоса (получение записи сервером). Для каждой попытки, последовательно. |
|  | front\_bqc\_estimators\_sound\_reverse\_<part>  | string  | Обязательное (при съеме БО) / необязательное (если не снимается БО  | Строка, передаваемая библиотекой контроля качества, используемой поставщиком БО, со значениями результатов проверки качества второго БО записи голоса. Для каждой попытки, последовательно  |
|  | sound\_random\_time\_start\_<part> | timestamp | Обязательное (при съеме БО) / необязательное (если не снимается БО) | Дата и время, когда инициировано на стороне сервера или прикладного ПО начало сбора третьего БО записи голоса. Для каждой попытки, последовательно. |
|  | sound\_random\_time\_end\_<part> | timestamp | Обязательное (при съеме БО) / необязательное (если не снимается БО) | Дата и время завершения сбора третьего БО записи голоса (получение записи сервером). Для каждой попытки, последовательно. |
|  | front\_bqc\_estimators\_sound\_random\_<part>  | string  | Обязательное (при съеме БО) / необязательное (если не снимается БО  | Строка, передаваемая библиотекой контроля качества, используемой поставщиком БО, со значениями результатов проверки качества третьего БО записи голоса. Для каждой попытки, последовательно  |
|  | sound\_all\_time\_end\_<part>  | timestamp | Обязательное (при съеме БО) / необязательное (если не снимается БО  | Дата и время завершения проверки записи, склеенной в одну запись, на соответствие требованиям с использованием ПО или сервиса контроля качества. Для каждой попытки, последовательно  |
|  | front\_bqc\_estimators\_sound\_all\_<part>  | string  | Обязательное (при съеме БО) / необязательное (если не снимается БО  | Строка, передаваемая библиотекой контроля качества, используемой поставщиком БО, со значениями результатов проверки качества записи, склееной в одну запись. Для каждой попытки, последовательно  |
|  | bank\_find\_profile\_time\_start\_<part>  | timestamp | Обязательное (для АРМ) / необязательное | **Только для АРМ или сбора оператором**. Дата и время, когда уполномоченный сотрудник поставщика БО или или регистрирующего партнера инициировал отправку запроса по поиску учётной записи клиента в ЕСИА. Для каждой попытки |
|  | bank\_find\_profile\_time\_end\_<part>  | timestamp | Обязательное (для АРМ) / необязательное | **Только для АРМ или сбора оператором**. Дата и время, когда ИС поставщика БО или регистрирующего партнера подтвердила приём сообщения от СМЭВ, содержащего ответ на запрос по поиску учётной записи в ЕСИА. Для каждой попытки |
|  | esia\_find\_account\_msg\_id  | string  | Обязательное (для АРМ) / необязательное | **Только для АРМ или сбора оператором**. Идентификатор запроса на поиск УЗ в ЕСИА |
|  | esia\_confirm\_msg\_id  | string | Обязательное (для АРМ) / необязательное | **Только для АРМ или сбора оператором**. Идентификатор запроса, направленного на подтверждение личности клиента, УЗ которого находится в одном из статусов: * упрощенная, готовая к подтверждению;
* стандартная;
* подтвержденная через ФГУП «Почта России»
 |
|  | esia\_register\_by\_simplified\_msg\_id  | string | Обязательное (для АРМ) / необязательное | **Только для АРМ или сбора оператором**. Идентификатор запроса, направленного на подтверждение УЗ клиента КО в ЕСИА, имеющей статус «Упрощенная» |
|  | esia\_recover\_msg\_id  | string  | Обязательное (для АРМ) / необязательное | **Только для АРМ или сбора оператором**. Идентификатор запроса обновления УЗ клиента в ЕСИА  |
|  | name\_equipment\_camera | string | необязательное | **В случае доступности такой информации.**Наименование оборудования (камера),если информация не доступна, не указывается |
|  | name\_equipment\_microphone | string | необязательное | Наименование оборудования (микрофон) |

# ПРИЛОЖЕНИЕ №3. Доступные мнемоники сбора БО в процессе биометрической идентификации

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| Мнемоника схемы сбора БО | Модальность | Необходимость инструкций проверки liveness(Active) | Необходимость проверки liveness(Passive) | Тип (URL) сбора на WEB интерфейсе | Content-Type(bio\_sample) | Методы, используемые в процессе биометрической идентификации в зависимости от мнемоники схемы сбора БО |
|  | **Face** | **Voice** | WEB интерфейс**не ЕБС** | WEB интерфейс **ЕБС** | **image/jpeg****image/png****multipart name=****bs\_photo** | **audio/wav****multipart name=****bs\_audio** | **video/mp4****video/mov****multipart name=****bs\_video** | **start** | **negotiate** | **upload** | **result** |
| face\_only | 1 | 0 | 0 | 0 | 1 | 0 | 1 | 0 | 0 | 1 | 0 | 1 | 1 |
| face\_only\_with\_webinterface | 1 | 0 | 0 | 0 | 0 | 1 | 1 | 0 | 0 | 1 | 0 | 1 | 1 |
| face\_with\_passive\_liveness | 1 | 0 | 0 | 1 | 1 | 0 | 1 | 0 | 0 | 1 | 0 | 1 | 1 |
| face\_with\_passive\_liveness\_and\_webinterface | 1 | 0 | 0 | 1 | 0 | 1 | 1 | 0 | 0 | 1 | 0 | 1 | 1 |
| face\_only\_age | 1 | 0 | 0 | 0 | 1 | 0 | 1 | 0 | 0 | 1 | 0 | 1 | 1 |
| face\_only\_with\_webinterface\_age | 1 | 0 | 0 | 0 | 0 | 1 | 1 | 0 | 0 | 1 | 0 | 1 | 1 |
| face\_with\_passive\_liveness\_age | 1 | 0 | 0 | 1 | 1 | 0 | 1 | 0 | 0 | 1 | 0 | 1 | 1 |
| face\_with\_passive\_liveness\_and\_webinterface\_age | 1 | 0 | 0 | 1 | 0 | 1 | 1 | 0 | 0 | 1 | 0 | 1 | 1 |

# ПРИЛОЖЕНИЕ №4. Описание алгоритма генерации хеш-функции

Хеширование данных Хеш ПДн производится с использованием метода шифрования по стандарту ГОСТ Р 34.11.2012 «Информационная технология. Криптографическая защита информации. Функция хэширования», размер хеша 512 бит.

| **Осуществляется хеширование следующих данных ФЛ:** |
| --- |
|  | ФИО; |
|  | Серия и номер паспорта. |
| **Формат хеширования данных:**  |
| SSSSNNNNNNSURNAMEPATRONYMICNAME, где |
| SSSS | серия паспорта |
| NNNNNN | номер паспорта |
| SURNAME | ФАМИЛИЯ (верхний регистр все буквы обязательно!) |
| PATRONYMIC | ОТЧЕСТВО (верхний регистр все буквы обязательно!) |
| NAME | ИМЯ (верхний регистр, все буквы обязательно!). |

1. Применимо только для процессов выгрузки и импорта векторов. [↑](#footnote-ref-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. [↑](#footnote-ref-3)
3. В соответствии с требованиями п. 7.6, 9.1.1, 9.1.2, 9.2.1, 9.2.2 Регламента Государственной информационной системы «Единая система идентификации и аутентификации физических лиц с использованием биометрических персональных данных». [↑](#footnote-ref-4)
4. В соответствии с требованиями п. 9.1.6, 9.2.6 Регламента Государственной информационной системы «Единая система идентификации и аутентификации физических лиц с использованием биометрических персональных данных» [↑](#footnote-ref-5)
5. Размер платы по транзакциям по запросам с проверкой возраста при подключении организаций к сервисам биометрической идентификации/верификации с использованием мнемоник возраста устанавливается по отдельным тарифам, указываемым на веб-странице <https://ebs.ru/documents/> в разделе «Тарифы, оферты, соглашения». [↑](#footnote-ref-6)
6. Описание алгоритма хеширования данных представлено в Приложении №4. [↑](#footnote-ref-7)
7. Описание алгоритма хеширования данных представлено в Приложении №4. [↑](#footnote-ref-8)
8. Доступны по адресу <https://ebs.ru/documents> в разделе «Основные» [↑](#footnote-ref-9)