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

**Методические рекомендации**

**по использованию сервиса**

**биометрической верификации**

**(в документе возможны изменения в связи с вступлением в силу 572-ФЗ и других подзаконных актов)**

Версия 1.20

Москва 2025

**Управление документом**

| Версия | Дата | Изменение |
| --- | --- | --- |
| 1.1 | 16.01.2023 | Создание документа |
| 1.2 | 20.02.2023 | Корректировка Рисунка 2, Рисунка 3 |
| 1.3 | 02.03.2023 | Исправление ошибок, дополнено Приложением №1, Приложением №2 |
| 1.4 | 17.03.2023 | Актуализация перечня нормативно-правовых документов (572-ФЗ и др.).Дополнение и изменение терминов и определений (ЕБС).Исправление ссылок на URL (ebs.ru).Исправление орфографических ошибок, опечаток и т.д. |
| 1.5 | 09.06.2023 | Исправление ошибки дублирующихся полей iss, sub в таблице 13 в п. 3.1. |
| 1.6 | 27.09.2023 | Обновлены описания API в п. 2.1 (СНИЛС ФЛ), 2.5, исключен п. 2.3 со сдвигом нумерации, откорректированы п. 3.1-3.4, отмечена обязательность date в metadata |
| 1.7 | 07.11.2023 | Откорректирован п. 2.1: необязательность параметра matching, дополнено описание agree.date\_from |
| 1.8 | 04.12.2023 | Дополнен п. 2.2 и откорректировано его название (уведомление IDP о деактивации) |
| 1.9 | 27.03.2024 | По всему тексту в документе были внесены изменения:- заменено доменное имя ebs-int.rtlabs.ru на int.ebs.ru |
| 1.10 | 09.10.2024 | В п. 2.3 откорректированы значения «MA», «MF» (мэтчинг) параметра stu |
| 1.11 | 18.10.2024 | Добавлены п. 2.2.1, 2.2.2, 2.2.3 с версиями апи уведомления IDP о результатах регистрации УЗ/деактивации БШ v1, v2, v3. Откорректировано определение Хещ ПДн и добавлено Приложение 3 с описанием алгоритма хеширования. |
| 1.12 | 20.11.2024 | Добавлено описание проверки возраста (18+) в п. 1.2, расширен алгоритм, добавлены мнемоники \_age, дополнен двумя параметрами п. 3.4 |
| 1.13 | 05.12.2024 | Дополнено описание параметра aud в п. 2.4, 3.1 и 3.4 |
| 1.14 | 15.01.2025 | В п. 2.1 дополнено описание параметра datetime\_tz |
| 1.15 | 27.01.2025 | В Таблице 1 добавлены все имеющиеся мнемоники проверки возраста (\_age)  |
| 1.16 | 25.04.2025 | Обновлен перечень доступных мнемоник по состоянию на апрель 2025 (все) |
| 1.17 | 03.06.2025 | В п. 3.3. обновлен пример успешного ответа на запрос (/upload) |
| 1.18 | 18.06.2025 | В раздел 3 добавлено описание ошибки EBS-00701 (Неизвестная ошибка ЕБС) |
| 1.19 | 17.07.2025 | Добавлен п. 1.3 с перечнем рекомендованных браузеров и их версий |
| 1.20 | 13.10.2025 | В п. 3.1 добавлен параметр pin\_check\_necessity, дополнен п. 1.1 (криптоконтроль целостности БО), дополнен алгоритм в п. 1.2 (проверка пин, криптографический контроль целостности БО). В п. 3.3 добавлено описание параметров заголовка hash-bio, обновлен пример, исключен параметр actions.duration, добавлен параметр actions.text. Обновлено описание алгоритма хэширования БО в API приема БО на верификацию п.3.3 |

**АННОТАЦИЯ**

Настоящий документ является инструкцией по организации использования биометрического сервиса верификации в качестве аутентификации Пользователя в информационной системе контрагента (далее – ИС КА).

Раздел 1 «Описание взаимодействия» описывает общую схему взаимодействия ИС КА и ГИС ЕБС в рамках предоставления биометрической верификации и импорта БО.

Разделы 2 и 3 содержат информацию о программных интерфейсах ГИС ЕБС.

Содержание

[ТЕРМИНЫ, ОПРЕДЕЛЕНИЯ И СОКРАЩЕНИЯ 5](#_Toc203668450)

[1. Описание взаимодействия 9](#_Toc203668451)

[1.1. Предусловия для проведения биометрической верификации 11](#_Toc203668452)

[1.2. Алгоритм взаимодействия в процессе биометрической верификации 13](#_Toc203668453)

[1.3. Список поддерживаемых браузеров 14](#_Toc203668454)

[2. Интерфейсы работы с учетной записью Пользователя 20](#_Toc203668455)

[2.1. API регистрации УЗ Пользователя в ГИС ЕБС (регистрация без биометрических данных) 20](#_Toc203668456)

[2.2. API уведомления IDP о результатах регистрации УЗ или деактивации БШ 28](#_Toc203668457)

[2.2.1. API уведомления IDP об изменении статуса УЗ v1 (планируется к выводу из эксплуатации) 29](#_Toc203668458)

[2.2.2. API уведомления IDP об изменении статуса УЗ v2 (планируется к выводу из эксплуатации) 31](#_Toc203668459)

[2.2.3. API уведомления IDP об изменении статуса УЗ v3 32](#_Toc203668460)

[2.3. API уведомления IDP о результатах сопоставления УЗ 34](#_Toc203668461)

[2.4. API деактивации УЗ Пользователя 36](#_Toc203668462)

[3. API биометрической верификации Пользователя с привязкой к IDP 40](#_Toc203668463)

[3.1. Старт процесса биометрической верификации 42](#_Toc203668464)

[3.2. Согласование инструкций Liveness 47](#_Toc203668465)

[3.3. Прием БО на верификацию 50](#_Toc203668466)

[3.4. Получение расширенного результата верификации 59](#_Toc203668467)

[ПРИЛОЖЕНИЕ №1. Дополнительные метаданные (meta) 65](#_Toc203668468)

[ПРИЛОЖЕНИЕ №2. Дополнительные данные о метриках системы  (metrics) 69](#_Toc203668469)

[ПРИЛОЖЕНИЕ №3. Описание алгоритма генерации хеш-функции 73](#_Toc203668470)

ТЕРМИНЫ, ОПРЕДЕЛЕНИЯ И СОКРАЩЕНИЯ

| **Термин** | **Определение** |
| --- | --- |
| БДн | Биометрические данные |
| 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 биометрического взаимодействия. 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. |
| Биометрический контрольный шаблон (БКШ) | Один или более хранимых биометрических шаблонов, относящихся к субъекту биометрических данных и используемых в качестве объекта сравнения |
| Биометрический образец (БО) | Аналоговое или цифровое представление биометрических характеристик, предшествующее извлечению биометрических признаков |
| Биометрический шаблон (биометрический вектор, биометрический ключ) | Набор хранимых биометрических признаков, сравниваемых непосредственно с биометрическими признаками биометрической пробы |
| ГИС | Государственная информационная система |
| Единая биометрическая система, 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 |
| ИС КА | Информационная система контрагента |
| КБС (Коммерческая биометрическая система) | Система, получающая/деактивирующая БКШ от ГИС 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 производитсяпосле регистрации УЗ и создания профиля в ЕБС |
| ПДн, 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». |
| Пользователь, Клиент | Физическое лицо, взаимодействующее с ГИС ЕБС как с целью биометрической регистрации, биометрической верификации или биометрической идентификации |
| СИБ | Система идентификации болельщика |
| Технологический портал | Портал, входящий в состав ГИС ЕБС, предназначенный для автоматизации процесса подключения к ГИС ЕБС |
| УЗ | Учетная запись |
| Участник биометрического взаимодействия | Участник биометрического взаимодействия (юридическое лицо), владелец Информационной системы, зарегистрированной в Единой биометрической системе и имеющей возможность использовать биометрические данные из Единой биометрической системы, аккредитованная коммерческая биометрическая система или региональный сегмент Единой биометрической системы |
| ЮЛ | Юридическое лицо |
| ФЛ | Физическое лицо |
| API  | (Application programming interface, программный интерфейс приложения, интерфейс прикладного программирования).Набор готовых классов, процедур, функций, структур и констант, предоставляемых приложением (библиотекой, сервисом) или операционной системой для использования во внешних программных продуктах. |
| IDP | Провайдер идентификации, возможные значения: IDP ЕСИА, IDP КБС и др. |
| Liveness (Живучесть) | Качество или признаки жизни субъекта, выявленные анатомическими характеристиками, непроизвольными реакциями, физиологическими функциями, добровольными реакциями, или поведением субъекта |
| OID, Open ID | Идентификатор Пользователя в IDP ЕСИА, требуется для сопоставления (мэтчинга) УЗ Пользователя в ГИС ЕБС |

1. Описание взаимодействия

Для взаимодействия ИС КА и ГИС ЕБС в процессе биометрической верификации необходимо произвести связывание (мэтчинг) учетных записей Пользователя (ранее зарегистрированной в ЕБС учетной записи пользователя, содержащей биометрические данные, и учетной записи Пользователя в ИС КА, которая будет использоваться в процессе биометрической верификации).

Диаграмма 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

Диаграмма взаимодействия ИС КА с ГИС ЕБС в рамках биометрической верификации Пользователя в ИС КА без использования web-интерфейса ГИС ЕБС представлена на рисунке ниже (Рисунок 2).

Диаграмма взаимодействия ИС КА с ГИС ЕБС в рамках биометрического верификации Пользователя в ИС КА с использованием web-интерфейса ГИС ЕБС представлена на рисунке ниже (Рисунок 3).

 

Рисунок 2 – Схема взаимодействия ИС КА с ГИС ЕБС в процессе верификации без использования web-интерфейса ГИС ЕБС



Рисунок 3 – Схема взаимодействия ИС КА с ГИС ЕБС в процессе верификации с использованием web-интерфейса ГИС ЕБС

Предусловия для проведения биометрической верификации

Для организации использования биометрической верификации необходимо:

1. Зарегистрировать ИС КА в ГИС ЕБС в качестве:
	* ИС Поставщика БДн;
	* ИС Потребителя БДн;
	* Провайдера идентификации (IDP).
2. Зарегистрировать УЗ Пользователя в ГИС ЕБС под ранее заведенной IDP (например, SIB) с идентификатором Пользователя в этой IDP (OID) и с передачей данных для сопоставления УЗ (OID), путем вызова API «Регистрация УЗ без БО» (см. раздел 2.1).
3. 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 hash ПДн) (см. разделы 2.2, 2.3).
4. При необходимости УЗ Пользователя может быть деактивирована, используя API деактивации УЗ (см. раздел 2.4). Схема деактивации учетной записи представлена на рисунке ниже (Рисунок 3):



Рисунок 3 – Схема деактивации учетной записи

В процессе биометрической верификации реализованы:

1. **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,[[1]](#footnote-1) для чего:
* при старте биометрической верификации (см. п. 3.1) указывается признак запроса возраста (мнемоника с постфиксом \_age, см. Таблицу 1);
* при получении расширенного результата верификации передается в том числе информация о возрасте пользователя (см. п. 3.4).
1. **Криптографический контроль целостности БО**, который выполняется в соответствии с требованиями Приказа Минцифры от 05.05.2023 №445 в случаях, когда для съема БО используется конечное устройство организации (терминал, планшет и т.д.). В таких случаях организация **не может** использовать веб-форму ГИС ЕБС. В рамках криптографического контроля целостности должна осуществляться передача в ГИС ЕБС дополнительного заголовка, в котором передается JWT, содержащий следующую информацию:
* расчитанный хэш передаваемого (или передаваемых) БО;
* электронную подпись JWT.

Более подробная информация о передаваемом JWT представлена в п. 3.3.

Алгоритм взаимодействия в процессе биометрической верификации

1. ИС с ролью Потребителя БДн вызывает метод старта верификации (см. раздел 3.1) с указанием соответствующей мнемоники (согласно перечню доступных мнемоник сбора БО – Таблица 1). Подсистема Универсальный сервис идентификации 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. Таблицу 1).
	2. Для использования механизма проверки PIN-кода в запросе указывается дополнительное поле с параметром pin\_check\_necessity (см. п. 3.1).
2. По полученному в ответе от ГИС ЕБС URL (Передается в составе HTTP заголовка «Location») для снятия биометрических образцов в рамках прохождения биометрической верификации, в зависимости от мнемоники верификации (см п. 1.) Пользователь перенаправляется на:
	1. Web-форму сбора БО ГИС ЕБС, если передана мнемоника c постфиксом with\_webinterface/ with\_webinterface\_age,
	2. Web-форму ИС КА в остальных случаях.
3. В случае использования мнемоники верификации, требующей инструкции (см. Таблицу 1) ИС КА запрашивает инструкции у ГИС ЕБС (см. раздел 3.2).
	1. В случае если используются пользовательские конечные устройства, криптографический контроль целостности БО не выполняется (вне зависимости от того, применяется ли web-форма ГИС ЕБС или web-форма ИС КА).
	2. В случае если используются конечные устройства организации, web-форма ГИС ЕБС применяться не может, должна быть реализована собственная web-форма ИС КА (либо процесс должен осуществляться без web-формы съема БО), и дополнительно проводится криптографический контроль целостности БО.
4. Пользователь сдает биометрические образцы с использованием WEB-формы.
5. Снятые биометрические образцы Пользователя передаются в ГИС ЕБС для прохождения биометрической верификации (см. раздел 3.3).
	1. В случае если криптографический контроль целостности БО не проводится, должны применяться программные интерфейсы, описанные в разделе 3 (п. 3.3 без необязательного заголовка hash-bio).
	2. В случае если криптографический контроль целостности БО проводится, должны применяться программные интерфейсы, описанные в разделе 3 (п. 3.3 с необязательным заголовком hash-bio), и передаваться информация для проверки.
6. После успешного прохождения биометрической верификации:
	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 7.
	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 7.
7. ИС Потребителя направляет запрос в ГИС ЕБС для получения расширенного результата верификации (см. раздел 3.4).
8. ГИС ЕБС передает в ИС Потребителя расширенный результат верификации.
	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.

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.

Таблица 1 – Доступные мнемоники сбора БО по состоянию на апрель 2025

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| 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 верификации 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** |
| FZ\_115 | 1 | 1 | 1 | 0 | 0 | 1 | 0 | 0 | 1 | 1 | 1 | 1 | 1 |
| face\_only | 1 | 0 | 0 | 0 | 1 | 0 | 1 | 0 | 0 | 1 | 0 | 1 | 1 |
| voice\_only | 0 | 1 | 0 | 0 | 1 | 0 | 0 | 1 | 0 | 1 | 0 | 1 | 1 |
| face\_only\_with\_webinterface | 1 | 0 | 0 | 0 | 0 | 1 | 1 | 0 | 0 | 1 | 0 | 1 | 1 |
| voice\_only\_with\_webinterface | 0 | 1 | 0 | 0 | 0 | 1 | 0 | 1 | 0 | 1 | 0 | 1 | 1 |
| face\_with\_passive\_liveness | 1 | 0 | 0 | 1 | 1 | 0 | 1 | 0 | 0 | 1 | 0 | 1 | 1 |
| voice\_with\_passive\_liveness | 0 | 1 | 0 | 1 | 1 | 0 | 0 | 1 | 0 | 1 | 0 | 1 | 1 |
| face\_with\_passive\_liveness\_and\_webinterface | 1 | 0 | 0 | 1 | 0 | 1 | 1 | 0 | 0 | 1 | 0 | 1 | 1 |
| voice\_with\_passive\_liveness\_and\_webinterface | 0 | 1 | 0 | 1 | 0 | 1 | 0 | 1 | 0 | 1 | 0 | 1 | 1 |
| face\_with\_active\_liveness | 1 | 0 | 1 | 0 | 1 | 0 | 0 | 0 | 1 | 1 | 1 | 1 | 1 |
| voice\_with\_active\_liveness | 0 | 1 | 1 | 0 | 1 | 0 | 0 | 0 | 1 | 1 | 1 | 1 | 1 |
| face\_with\_active\_liveness\_and\_webinterface | 1 | 0 | 1 | 0 | 0 | 1 | 0 | 0 | 1 | 1 | 1 | 1 | 1 |
| voice\_with\_active\_liveness\_and\_webinterface | 0 | 1 | 1 | 0 | 0 | 1 | 0 | 0 | 1 | 1 | 1 | 1 | 1 |
| face\_with\_all\_liveness | 1 | 0 | 1 | 1 | 1 | 0 | 0 | 0 | 1 | 1 | 1 | 1 | 1 |
| voice\_with\_all\_liveness | 0 | 1 | 1 | 1 | 1 | 0 | 0 | 0 | 1 | 1 | 1 | 1 | 1 |
| face\_with\_all\_liveness\_and\_webinterface | 1 | 0 | 1 | 1 | 0 | 1 | 0 | 0 | 1 | 1 | 1 | 1 | 1 |
| voice\_with\_all\_liveness\_and\_webinterface | 0 | 1 | 1 | 1 | 0 | 1 | 0 | 0 | 1 | 1 | 1 | 1 | 1 |
| face\_and\_voice\_only | 1 | 1 | 0 | 0 | 1 | 0 | 1 | 1 | 0 | 1 | 0 | 1 | 1 |
| face\_and\_voice\_only\_with\_webinterface | 1 | 1 | 0 | 0 | 0 | 1 | 1 | 1 | 0 | 1 | 0 | 1 | 1 |
| face\_and\_voice\_with\_passive\_liveness | 1 | 1 | 0 | 1 | 1 | 0 | 1 | 1 | 0 | 1 | 0 | 1 | 1 |
| face\_and\_voice\_with\_passive\_liveness\_and\_webinterface | 1 | 1 | 0 | 1 | 0 | 1 | 1 | 1 | 0 | 1 | 0 | 1 | 1 |
| face\_and\_voice\_with\_active\_liveness | 1 | 1 | 1 | 0 | 1 | 0 | 0 | 0 | 1 | 1 | 1 | 1 | 1 |
| face\_and\_voice\_with\_active\_liveness\_and\_webinterface | 1 | 1 | 1 | 0 | 0 | 1 | 0 | 0 | 1 | 1 | 1 | 1 | 1 |
| face\_and\_voice\_with\_all\_liveness | 1 | 1 | 1 | 1 | 1 | 0 | 0 | 0 | 1 | 1 | 1 | 1 | 1 |
| face\_and\_voice\_with\_all\_liveness\_and\_webinterface | 1 | 1 | 1 | 1 | 0 | 1 | 0 | 0 | 1 | 1 | 1 | 1 | 1 |
| face\_only\_age | 1 | 0 | 0 | 0 | 1 | 0 | 1 | 0 | 0 | 1 | 0 | 1 | 1 |
| voice\_only\_age | 0 | 1 | 0 | 0 | 1 | 0 | 0 | 1 | 0 | 1 | 0 | 1 | 1 |
| face\_only\_with\_webinterface\_age | 1 | 0 | 0 | 0 | 0 | 1 | 1 | 0 | 0 | 1 | 0 | 1 | 1 |
| voice\_only\_with\_webinterface\_age | 0 | 1 | 0 | 0 | 0 | 1 | 0 | 1 | 0 | 1 | 0 | 1 | 1 |
| face\_with\_passive\_liveness\_age | 1 | 0 | 0 | 1 | 1 | 0 | 1 | 0 | 0 | 1 | 0 | 1 | 1 |
| voice\_with\_passive\_liveness\_age | 0 | 1 | 0 | 1 | 1 | 0 | 0 | 1 | 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 |
| voice\_with\_passive\_liveness\_and\_webinterface\_age | 0 | 1 | 0 | 1 | 0 | 1 | 0 | 1 | 0 | 1 | 0 | 1 | 1 |
| face\_with\_active\_liveness\_age | 0 | 1 | 1 | 0 | 1 | 0 | 0 | 0 | 1 | 1 | 1 | 1 | 1 |
| voice\_with\_active\_liveness\_age |  |  | 1 | 0 | 1 | 0 | 0 | 0 | 1 | 1 | 1 | 1 | 1 |
| face\_with\_active\_liveness\_and\_webinterface\_age | 1 | 0 | 1 | 0 | 0 | 1 | 0 | 0 | 1 | 1 | 1 | 1 | 1 |
| voice\_with\_active\_liveness\_and\_webinterface\_age | 0 | 1 | 1 | 0 | 0 | 1 | 0 | 1 | 0 | 1 | 1 | 1 | 1 |
| face\_with\_all\_liveness\_age | 1 | 0 | 1 | 1 | 1 | 0 | 0 | 0 | 1 | 1 | 1 | 1 | 1 |
| voice\_with\_all\_liveness\_age | 0 | 1 | 1 | 1 | 0 | 0 | 0 | 0 | 1 | 1 | 1 | 1 | 1 |
| face\_with\_all\_liveness\_and\_webinterface\_age | 1 | 0 | 1 | 1 | 0 | 1 | 0 | 0 | 1 | 1 | 1 | 1 | 1 |
| voice\_with\_all\_liveness\_and\_webinterface\_age | 0 | 1 | 1 | 1 | 0 | 1 | 1 | 0 | 1 | 1 | 1 | 1 | 1 |
| face\_and\_voice\_only\_age | 1 | 1 | 0 | 0 | 1 | 0 | 1 | 1 | 0 | 1 | 0 | 1 | 1 |
| face\_and\_voice\_only\_with\_webinterface\_age | 1 | 1 | 0 | 0 | 0 | 1 | 1 | 1 | 0 | 1 | 0 | 1 | 1 |
| face\_and\_voice\_with\_passive\_liveness\_age | 1 | 1 | 0 | 1 | 1 | 0 | 1 | 1 | 0 | 1 | 0 | 1 | 1 |
| face\_and\_voice\_with\_passive\_liveness\_and\_webinterface\_age | 1 | 1 | 0 | 1 | 0 | 1 | 1 | 1 | 0 | 1 | 0 | 1 | 1 |
| face\_and\_voice\_with\_active\_liveness\_age | 1 | 1 | 1 | 0 | 1 | 0 | 0 | 0 | 1 | 1 | 1 | 1 | 1 |
| face\_and\_voice\_with\_active\_liveness\_and\_webinterface\_age | 1 | 1 | 1 | 0 | 0 | 1 | 0 | 0 | 1 | 1 | 1 | 1 | 1 |
| face\_and\_voice\_with\_all\_liveness\_age | 1 | 1 | 1 | 1 | 1 | 0 | 0 | 0 | 1 | 1 | 1 | 1 | 1 |
| face\_and\_voice\_with\_all\_liveness\_and\_webinterface\_age | 1 | 1 | 1 | 1 | 0 | 1 | 0 | 0 | 1 | 1 | 1 | 1 | 1 |
| face\_only\_stream\_age | 1 | 0 | 0 | 0 | 1 | 0 | 0 | 0 | 1 | 1 | 0 | 1 | 1 |
| face\_only\_stream\_with\_webinterface\_age | 1 | 0 | 0 | 0 | 0 | 1 | 0 | 0 | 1 | 1 | 0 | 1 | 1 |
| face\_stream\_with\_passive\_liveness\_age | 1 | 0 | 0 | 1 | 1 | 0 | 0 | 0 | 1 | 1 | 0 | 1 | 1 |
| face\_stream\_with\_passive\_liveness\_and\_webinterface\_age | 1 | 0 | 0 | 1 | 0 | 1 | 0 | 0 | 1 | 1 | 0 | 1 | 1 |
| face\_stream\_with\_active\_liveness\_age | 1 | 0 | 1 | 0 | 1 | 0 | 0 | 0 | 1 | 1 | 1 | 1 | 1 |
| face\_stream\_with\_active\_liveness\_and\_webinterface\_age | 1 | 0 | 1 | 0 | 0 | 1 | 0 | 0 | 1 | 1 | 1 | 1 | 1 |
| face\_stream\_with\_all\_liveness\_age | 1 | 0 | 1 | 1 | 1 | 0 | 0 | 0 | 1 | 1 | 1 | 1 | 1 |
| face\_stream\_with\_all\_liveness\_and\_webinterface\_age | 1 | 0 | 1 | 1 | 0 | 1 | 0 | 0 | 1 | 1 | 1 | 1 | 1 |
| face\_and\_voice\_stream\_with\_active\_liveness\_age | 1 | 1 | 1 | 0 | 1 | 0 | 0 | 0 | 1 | 1 | 1 | 1 | 1 |
| face\_and\_voice\_stream\_with\_active\_liveness\_and\_webinterface\_age | 1 | 1 | 1 | 0 | 0 | 1 | 0 | 0 | 1 | 1 | 1 | 1 | 1 |
| face\_and\_voice\_stream\_with\_all\_liveness\_age | 1 | 1 | 1 | 1 | 1 | 0 | 0 | 0 | 1 | 1 | 1 | 1 | 1 |
| face\_and\_voice\_stream\_with\_all\_liveness\_and\_webinterface\_age | 1 | 1 | 1 | 1 | 0 | 1 | 0 | 0 | 1 | 1 | 1 | 1 | 1 |
| face\_only\_set\_age | 1 | 0 | 0 | 0 | 1 | 0 | 1 | 0 | 0 | 1 | 0 | 1 | 1 |
| face\_only\_set\_with\_webinterface\_age | 1 | 0 | 0 | 0 | 0 | 1 | 1 | 0 | 0 | 1 | 0 | 1 | 1 |
| face\_set\_with\_passive\_liveness\_age | 1 | 0 | 0 | 1 | 1 | 0 | 1 | 0 | 0 | 1 | 0 | 1 | 1 |
| face\_set\_with\_passive\_liveness\_and\_webinterface\_age | 1 | 0 | 0 | 1 | 0 | 1 | 1 | 0 | 0 | 1 | 0 | 1 | 1 |

**Web-форма ГИС ЕБС (мнемоники с постфиксом \_webinterface) не может использоваться на конечных устройствах организации.**

1. Интерфейсы работы с учетной записью Пользователя

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

Интерфейс предоставляет возможность регистрации учетной записи пользователя без биометрических данных для провайдера идентификации, зарегистрированного в ГИС ЕБС (см. Регламент Государственной информационной системы «Единая система идентификации и аутентификации физических лиц с использованием биометрических персональных данных» (ГИС ЕБС), опубликованный на портале https://ebs.ru/documents/), для последующего проведения биометрической верификации с использованием этой учетной записи и биометрических данных этого же пользователя, привязанных к ранее зарегистрированной в ГИС ЕБС учетной записи.

**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 (Таблица 2).

Таблица 2 – Алгоритмы, указываемые в JWT HEADER

|  |  |
| --- | --- |
| **Алгоритм, указываемый в Header** | **Описание** |
| RS256 | алгоритм SHA256withRSA |
| RS512 | алгоритм SHA512withRSA |
| 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"} |

Доступные типы подписи указаны в таблице (Таблица 3).

Таблица 3 – Доступные типы подписи

|  |  |
| --- | --- |
| **Тип подписи** | **Описание** |
| PKCS7 attached signature | Подпись стандарта PKCS# 7. Содержит следующие атрибуты:Подпись (Attached);Набор обязательных подписываемых атрибутов (CONTENT\_TYPE (1.2.840.113549.1.9.3), SIGNING\_TIME (1.2.840.113549.1.9.5), MESSAGE\_DIGEST (1.2.840.113549.1.9.4));Дополнительные атрибуты (data (1.2.840.113549.1.7.1), идентификатор алгоритма хэширования и сертификаты подписантов). |
| PKCS7 detached signature | Подпись стандарта PKCS7 (RFC2315). Содержит следующие атрибуты:Подпись (Detached);Набор обязательных подписываемых атрибутов (CONTENT\_TYPE (1.2.840.113549.1.9.3), SIGNING\_TIME (1.2.840.113549.1.9.5), MESSAGE\_DIGEST (1.2.840.113549.1.9.4));Дополнительные атрибуты (идентификатор алгоритма хэширования, сертификаты подписантов (вместе с корневыми сертификатами) и открытый ключ (по идентификатору, соответствующему алгоритму подписания)). |

Состав PAYLOAD в JWT описан в таблице (Таблица 4).

Таблица 4 – Состав PAYLOAD в JWT

|  |  |  |  |
| --- | --- | --- | --- |
| **Наименование параметра** | **Тип данных** | **Обязательность** | **Описание** |
| service\_type | string | да | Тип (мнемоника) услуги.В данном поле должно быть указано следующее значение: 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 (указывается значение, как в заявке на подключение в роли Поставщика) |
| infosystem.contract\_id | string | да | Идентификатор контракта.Сущность, формирующаяся при заключении договора между ЮЛ и ЕБС. В контракт включается Пакет услуг. Для контракта настраиваются используемые Классы доверия биометрии, применимые в контракте. Содержит информацию о ЮЛ, провайдере (IDP), клиентском сервисе, сроках, статусе. |
| 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 (в случае указания в запросе параметра agree) | Дата, c которой действует согласие (Формат Unix time stamp в секундах) |
| 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.1. Может принимать значения: «hash» - Хеш ПДн;[[2]](#footnote-2)
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[[3]](#footnote-3), ID УЗ Пользователя IDP (OID) или номер СНИЛС) |
| meta | JSON-object | нет | Дополнительные метаданные (согласно спецификации, см. Приложение №1).  |
| metrics | JSON-object | нет | Дополнительные данные о метриках системы (согласно спецификации, см. Приложение №2).  |

Пример JWT.PAYLOAD:

|  |
| --- |
| { "service\_type": "reg-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" }]} |

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.eyJzZXJ2aWNlX3R5cGUiOiJyZWctd2l0aG91dC1iaW8iLCJkYXRldGltZV90eiI6MTU4OTI3NzM4NiwiaW5mb3N5c3RlbSI6eyJzeXN0ZW1faWQiOiJJRFBfVEVTVFNZU1RFTSIsImNvbnRyYWN0X2lkIjoiNTE2ODQ4NjkiLCJjZXJ0X2lkIjoiNDM2MzQ2MzQ2MzIyMzc4Nzg3OCJ9LCJhZ3JlZSI6eyJhZ3JlZW1lbnRfaWQiOiIxMjM5MjczNzQ3Ni1hZ3JlZUlEIiwiZGF0ZV9mcm9tIjoxNTg5Mjc3Mzg2LCJkYXRlX3RvIjoxNjgzODY4MjI5fSwicGVyc29uIjp7ImlkcCI6IklEUF9URVNUU1lTVEVNIiwidXNlcl9pZCI6IjE5NjE1MzU1MzI0IiwiY29udGFjdCI6eyJlbWFpbCI6InRlc3QtZW1haWxAbWFpbC5ydSJ9fSwibWF0Y2hpbmciOlt7ImtleSI6IkVTSUEiLCJ2YWx1ZSI6IjEwNzcxMTgyNjcifV19.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:

Таблица 5 – Коды ошибок метода

|  |  |  |
| --- | --- | --- |
| **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 ГИС ЕБС (см. Регламент Государственной информационной системы «Единая система идентификации и аутентификации физических лиц с использованием биометрических персональных данных» (ГИС ЕБС), опубликованный на портале <https://ebs.ru/documents/>).

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[[4]](#footnote-4)) 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.

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

В случае направления со стороны провайдера идентификации в ГИС ЕБС запроса на деактивацию УЗ (см. п. 2.4), данное уведомление не отправляется в адрес провайдера идентификации, поскольку взаимодействие синхронное.

* + 1. 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.

Тело запроса описано в таблице (Таблица 6).

Таблица 6 – 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"} |

* + 1. 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.

Тело запроса описано в таблице (Таблица 7).

Таблица 7 – 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"} |

* + 1. 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.

Тело запроса описано в таблице (Таблица 8).

Таблица 8 – 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.

Тело запроса описано в таблице (Таблица 9).

Таблица 9 – Описание тела запроса

|  |  |  |  |
| --- | --- | --- | --- |
| **Поле** | **Тип** | **Обязательность** | **Описание** |
| 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"} |

**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 клиента, 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 в таблице (Таблица 10).

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

Таблица 10 – Состав PAYLOAD в JWT

|  |  |  |  |
| --- | --- | --- | --- |
| **Наименование параметра** | **Тип данных** | **Обязательность** | **Описание** |
| iss | String | да | URL ([URI](https://ru.wikipedia.org/wiki/URI), сопоставляемый с Мнемоникой IDP, являющийся уникальным идентификатором стороны, генерирующей токен) |
| 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 (сертификаты хранятся в реестре сертификатов в привязке к мнемонике IDP). 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 контрагента. Этот идентификатор и является cert\_id. |
| JSON Object, передаваемый в теле запроса: |
| metadata | JSON Object | нет | Содержит перечень дополнительных данных (согласно спецификации, см. Приложение №1). |

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, согласно таблице (Таблица 11).

Таблица 11 – Возвращаемые ошибки метода

|  |  |  |  |
| --- | --- | --- | --- |
| 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"} |

1. API биометрической верификации Пользователя с привязкой к IDP

В процессе биометрической верификации по полученному идентификатору Пользователя выполняется поиск его БКШ. Затем из БО, переданного на биометрическую верификацию (см. раздел 3.3), создается биометрический шаблон, который сравнивается с БКШ Пользователя, хранящимся в ГИС ЕБС.

Таблица 12 – Коды ошибок биометрической верификации

|  |  |  |
| --- | --- | --- |
| Код HTTP ответа | Значение параметра «code» | Описание (параметр «message») |
| 500 | EBS-00701 | Неизвестная ошибка ЕБС (любая ошибка из ЕБС, которая не перенаправляется клиенту) |
| 500 | EBS-010001 | Внутренняя ошибка API |
| 400 | EBS-010003 | Неверный запрос |
| 400 | EBS-010004 | Запрос не содержит обязательного параметра %s |
| 400 | EBS-010005 | Отсутствует тело запроса |
| 401 | EBS-010101 | Ошибка проверки маркера доступа |
| 401 | EBS-010102 | Ошибка проверки ЭП ЕСИА |
| 400 | EBS-010103 | Маркер доступа не содержит обязательного параметра |
| 401 | EBS-010104 | Маркер доступа просрочен |
| 400 | EBS-010105 | Биометрический образец отсутствует |
| 400 | EBS-010106 | Присутствует более одного образца |
| 400 | EBS-010107 | Не удалось извлечь биометрические признаки |
| 400 | EBS-010108 | Ошибка верификации (биометрическая верификация не пройдена) |
| 403 | EBS-010109 | Провайдеру идентификации (IDP) запрещен доступ к ЕБС |
| 403 | EBS-010110 | Пользователю запрещен доступ к ЕБС |
| 403 | EBS-010111 | Неверный формат действий (описание действий не совпадает с отправленными) |
| 400 | EBS-010112 | Неверный порядок вызова API ЕБС |
| 400 | EBS-010113 | Тип или версия клиента не могут быть изменены в рамках одной сессии |
| 400 | EBS-010114 | Неверный формат инструкций |
| 400 | EBS-010115 | Неверный формат метаданных |
| 400 | EBS-010118 | Ошибка верификации (биометрическая верификация и проверка liveness не пройдены) |
| 400 | EBS-010128 | Ошибка верификации (проверка liveness не пройдена) |
| 400 | EBS-010201 | Параметр redirect не установлен |
| 400 | EBS-010202 | Параметр redirect содержит неправильно сформированный URL |
| 403 | EBS-010203 | Системе-клиенту (ИС Потребителя БДн) запрещен доступ к ЕБС |
| 400 | EBS-010301 | Пользователь не найден |
| 400 | EBS-010302 | Идентификатор сессии не найден |
| 400 | EBS-010303 | Время жизни сессии истекло |
| 400 | EBS-010304 | Превышено количество попыток верификации в рамках одной сессии |
| 400 | EBS-02024 | Отсутствуют обязательные данные |
| 503 | EBS-08001 | Сервис временно не доступен |

Старт процесса биометрической верификации

Для старта процесса биометрической верификации внешняя информационная система производит отправку соответствующего запроса в ГИС ЕБС с передачей ссылки на страницу ИС Потребителя БДн, на которую Пользователь будет перенаправлен после успешной верификации.

**Вызов сервиса**

POST /api/v3/verifications?redirect={redirect\_uri}

Заголовки:

* + Host: {host ГИС ЕБС}
	+ Content-Type: application/json
	+ X-EBS-TraceProcess: true (необязательный заголовок, необходимый для проверки взаимодействия с использованием Технологического портала)
	+ Authorization: Bearer {JWT от провайдера идентификации, сформированный в соответствии с RFC 7519 https://datatracker.ietf.org/doc/html/rfc7519}
	+ Cache-Control: no-cache

Каждая из частей токена доступа, полученного от провайдера идентификации (IDP) представляет из себя Base64url Encoding значение.

JWT.HEADER – описание свойств токена, в том числе 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).

Параметры запроса описаны в таблице (Таблица 13).

Таблица 13 – Параметры запроса

|  |  |  |  |
| --- | --- | --- | --- |
| **Наименование параметра** | **Тип данных** | **Обязательность** | **Описание** |
| redirect | string | нет | Передается в виде query-параметра в строке запросаПолный URL ИС Потребителя БДн, на который ГИС ЕБС осуществит перенаправление Пользователя после удачной верификации.В ГИС ЕБС должна быть зарегистрирована часть данного URL: имя хоста.В качестве зарегистрированного имени хоста данного URL допускается: FQDN имя хоста (не ниже домена второго уровня), или localhost (только для тестовых сред), или IPv4-адрес (только для тестовых сред).Используется только когда требуется использование WEB-интерфейса ЕБС.В случае использования WEB-интерфейса ИС КА, параметр redirect не требуется. По той же логике строится обязательность поля Location в ответах 1 и 3 запроса (п. 3.1 и п. 3.3). |
| metadata | JSON Object | да | Передается в теле запроса. Содержит перечень дополнительных данных (см. Приложение №1) |
| bio\_collecting\_type | String | да | Требуемая мнемоника согласованной схемы сбора БО (см. Таблицу 1 из п. 1.2). Для использования проверки возраста следует выбирать мнемонику с постфиксом \_age. |
| Параметры JWT.PAYLOAD |
| iss | String | да | чувствительная к регистру строка или [URI](https://ru.wikipedia.org/wiki/URI), которая является уникальным идентификатором стороны, генерирующей токен (например https://test.idp.ru/urn) |
| sub | String | да | Идентификатор УЗ Пользователя в IDP  |
| 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 Потребителя 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).
 |

Пример JWT.PAYLOAD:

|  |
| --- |
| { "iss":"http(s):test.idp.ru/urn", "sub":"11111111", "iat":1551940551, "exp":1551941153, "client\_id":"TEST\_SYSTEM", "pin-check-necessity":"pin\_require"} |

Пример запроса:

|  |
| --- |
| POST /api/v3/verifications?redirect=https%3A%2F%2Ftest.client.local%2F HTTP/1.1Host: int.ebs.ruContent-Type: application/jsonX-EBS-TraceProcess: trueAuthorization: Bearer {JWT от провайдера идентификации}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 "} |

**Успешный ответ**

В случае успешного ответа метод возвращает НТТР-код 200 OK со следующими заголовками:

* + Location – содержит URL веб-формы ГИС ЕБС, на который Потребитель БДн осуществит перенаправление Пользователя для снятия биометрических образцов (в составе URL присутствует в виде параметра адрес redirect, полученный в запросе);
	+ Session-Id – идентификатор сессии верификации в ГИС ЕБС.

Пример успешного ответа:

|  |
| --- |
| HTTP/1.1 200 OKLocation: https://int.ebs.ru /ui/verification?redirect=https%3A%2F%2Ftest.client.local%2FSession-Id: D530D7AF1EFA47489653FC4CEA5AC625 |

В случае успешного прохождения биометрической верификации по БО, отправленным в ГИС ЕБС со страницы съема БО, в браузер Пользователя возвращается сообщение НТТР OK (код состояния 200).

В HTTP заголовке «Location» содержится URL ИС Потребителя БДн, для перенаправления Пользователя после удачной верификации. ГИС ЕБС использует значение URL ИС Потребителя БДн, переданное в параметре «redirect» при вызове метода «Старт верификации в ГИС ЕБС». В случае возникновения ошибки метод вернет в ответе код и описание ошибки и не перенаправит Пользователя по адресу, указанному в redirect.

В составе дополнительных заголовков передаются параметры, приведенные в таблице (Таблица 14).

Таблица 14 – Параметры ответа при успешной верификации

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

Пример ответа от формы съема БО в случае успешной верификации:

|  |
| --- |
| HTTP/1.1 200 OK Location: http(s)://test.client.local/return\_uri Verification-Token:0BCAF243SE9CF4F607E3CEB7EE416D031 Session-Expires:1499443407648 |

**Ошибки метода**

В случае возникновения ошибки при обработке запроса система возвращает вызывающей стороне коды ответов HTTP и описания ошибок в HTTP BODY, согласно [таблице 12](#Таблица12) выше.

Пример ответа с ошибкой:

|  |
| --- |
| HTTP/1.1 400 Bad RequestContent-Type: application/json; charset=UTF-8{ "code": "EBS-010301", "message": "Пользователь не найден"} |

Согласование инструкций Liveness

**Описание:** Получение необходимых для прохождения биометрической верификации и проверки liveness инструкций, с описанием действий по формированию БО.

Метод является опциональным. Данный метод реализуется на стороне ИС КА в случае использования web-интерфейса сбора БО не ЕБС, а также необходимости проверки liveness.

**Авторизация:** По session\_id

**Тип контента HTTP-запроса:** «application/json»

**Client-Type:** В заголовке Client-Type необходимо передавать тип клиента и его версию

**Вызов:**

POST /api/**v3**/verifications/*{session\_id}*/**negotiate**,

где *{session\_id} -*идентификатор сессии верификации в ЕБС, полученный в ответе метода «Старт верификации в ЕБС»

**Описание запроса:**

Входные параметры:

|  |  |  |  |
| --- | --- | --- | --- |
| Наименование параметра | Тип данных | Обязательность | Описание |
| metadata | JSON Object | да | Содержит перечень дополнительных данных (согласно спецификации, см. Приложение №1) |

Пример запроса:

|  |
| --- |
| POST /api/v3/verifications/D530D7AF1EFA47489653FC4CEA5AC625/negotiate HTTP/1.1Host: int.ebs.ruUser-Agent: Mozilla/5.0 (X11; Linux x86\_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/51.0.2704.103 Safari/537.3Client-Type: application/vnd.ebs.v1.mobile.android+jsonAccept: application/jsonContent-Type: application/jsonCache-Control: no-cache { "metadata":{ "camera\_id":"2", "screen":"1200;1920", "device\_number":"0819da27", "date":"1520467814933" }} |

**Успешный ответ метода:**

В случае успешного ответа, метод возвращает сообщение, содержащее следующие параметры:

|  |  |  |  |
| --- | --- | --- | --- |
| Наименование параметра | Тип данных | Обязательность | Описание |
| liveness\_action | JSON Object | да | Содержит мнемонику согласованной схемы проверки Liveness и объект – описание необходимых действий метода на стороне клиентского приложения |
| liveness\_action.mnemonic | String | да | Мнемоника согласованной схемы проверки Liveness |
| liveness\_action.index | String | да | 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 |
| actions.type | String | да | Описание исполняемого Пользователем действия |
| actions.index | String | да | Указание очередности в запросе исполняемого Пользователем действия |
| actions.duration | String | да | Время отображения действия Пользователю (в миллисекундах) |
| actions.message | String | да | Инструкция, описывающая действие, предлагаемое к совершению Пользователем |
| actions.text | String | нет | Содержит кодовую последовательность (в данном случае для действия «numbers-digits»: неповторяющиеся цифры от 0 до 9) в текстовой форме, предлагаемую к прочтению Пользователем |

Пример ответа:

|  |
| --- |
| HTTP/1.1 200 OKContent-Type: application/json; charset=UTF-8 { "liveness \_action": [{ "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" }] }]} |

**Ошибки метода:**

В случае возникновения ошибки при обработке запроса, ЕБС возвращает вызывающей стороне коды ответов HTTP и описания ошибок в HTTP BODY, согласно [таблице 12](#Таблица12) выше.

Прием БО на верификацию

Для проведения процесса биометрической верификации зарегистрированного в ГИС ЕБС Пользователя необходимо осуществить прием БО на верификацию. Для этого внешняя информационная система производит отправку соответствующего запроса в ГИС ЕБС с передачей данных БО для дальнейшего проведения процесса верификации.

Сервис используется для получения биометрических образцов на верификацию и возврата результата биометрической верификации.

**В случае использования конечного устройства организации должен осуществляться криптографический контроль целостности БО: в запросе должен передаваться дополнительный заголовок hash-bio для проверки подписи и хэш-суммы БО, присылаемого в запросе.**

**Вызов сервиса**

POST /api/v3/verifications/{session\_id}/upload,

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

**Заголовки запроса:**

* X-EBS-TraceProcess: true (Необязательный. Возможные значения true или false)
* Авторизация: по session\_id
* Тип контента HTTP-запроса: «multipart/form-data»
* Client-Type: В заголовке Client-Type необходимо передавать тип клиента и его версию
* **hash-bio: {JWT} - необязательный заголовок, параметр с указанием хэш-суммы БО.**

**Параметры hash-bio: {JWT}**

|  |  |  |  |
| --- | --- | --- | --- |
| Наименование параметра | Тип данных | Обязательность | Описание |
| JWT состоит из трёх частей, разделённых точкой, и имеет следующий вид: HEADER.PAYLOAD.SIGNATUREКаждая из частей токена представляет из себя Base64url Encoding значение.JWT.HEADER - описание свойств токена, в том числе 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).  |
| **Параметры JWT.PAYLOAD:** |
| iss | String | да | Полученный от IDP идентификатор (чувствительная к регистру строка или URI, которая является уникальным идентификатором стороны, генерирующей токен)Например: "https://example.ru" |
| 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 (*expiration*) |
| 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 |
| **Дополнительные параметры PAYLOAD:** |
| hash\_bio | array | да | Список хэш-сумм БО |
| hash\_bio.filename | String | да | Уникальное название файла БО |
| hash\_bio.hash | String | да | Хэш-сумма БО (алг. GOST3411-2012-256) |

Пример заголовка hash-bio запроса:

|  |
| --- |
| **POST /api/v3/verifications/D530D7AF1EFA47489653FC4CEA5AC625/upload** **hash-bio: eyJpc3MiOiJodHRwKHMpOnRlc3QuaWRwLnJ1L3VybiIsImV4cCI6MTU1MTk0MTE1MywiaWF0IjoxNTUxOTQwNTUxfQ.eyJoYXNoX2JpbyI6W3siZmlsZW5hbWUiOiJmaWxlLndhdiIsImhhc2giOiJlNzZhMTczMzVhM2FmNzAxNzJkNjJmNzY2ZDZlNDA3YjRiNTdiYTkyNjMxMzdmMGQ0NmU1NzA5MmU0Zjc0YTQwIn0seyJmaWxlbmFtZSI6ImZpbGUuanBnIiwiaGFzaCI6IjcxYzQ4MGRmYjI1NzllOGI2NzRmNWQ3ODU0NzQwODAyODQ1Mjc5ODkwNTBjOWExMDgyYzg5ZjY5ODAwODQ3NzEifV19** |

Пример Payload JWT (hash-bio):

|  |
| --- |
| { "iss": "https://example.ru", "exp": 1758702898, "iat": 1758702598, "hash\_bio": [ { "filename": "file.wav", "hash": "e76a17335a3af70172d62f766d6e407b4b57ba9263137f0d46e57092e4f74a40" }, { "filename": "file.jpg", "hash":"71c480dfb2579e8b674f5d785474080284527989050c9a1082c89f6980084771" } ]} |

Входные параметры запроса описаны в таблице ниже (Таблица 15):

Таблица 15 – 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<мнемоника> 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"

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.client\_duration | String | Да | Содержит фактическое время исполнения действия Пользователем (в миллисекундах) |
| actions.message | String | Да | Содержит инструкцию, описывающую действие, предлагаемое к совершению Пользователем |
| actions.text | String | Нет | Содержит текст для прочтения Пользователем |
| **Часть multipart для передачи дополнительных данных** |
| metadata | Часть multipart | Да | Содержит дополнительные данные (согласно Спецификации параметров metadata в Приложении №1).Заголовочные поля:* Content-Disposition: form-data;
* Content-Type: application/json;
* name="metadata"
 |

**Пример запроса:**

|  |
| --- |
| POST /api/v3/verifications/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/537.3Client-Type: application/vnd.ebs.v1.mobile.android+jsonAccept: application/jsonCache-Control: no-cachehash-bio: eyJpc3MiOiJodHRwKHMpOnRlc3QuaWRwLnJ1L3VybiIsImV4cCI6MTU1MTk0MTE1MywiaWF0IjoxNTUxOTQwNTUxfQ.eyJoYXNoX2JpbyI6W3siZmlsZW5hbWUiOiJmaWxlLndhdiIsImhhc2giOiJlNzZhMTczMzVhM2FmNzAxNzJkNjJmNzY2ZDZlNDA3YjRiNTdiYTkyNjMxMzdmMGQ0NmU1NzA5MmU0Zjc0YTQwIn0seyJmaWxlbmFtZSI6ImZpbGUuanBnIiwiaGFzaCI6IjcxYzQ4MGRmYjI1NzllOGI2NzRmNWQ3ODU0NzQwODAyODQ1Mjc5ODkwNTBjOWExMDgyYzg5ZjY5ODAwODQ3NzEifV19 ------WebKitFormBoundary7MA4YWxkTrZu0gWContent-Disposition: form-data; name="bs\_photo"Content-Type: image/jpeg  {Поток байт Биометрического образца} ------WebKitFormBoundary7MA4YWxkTrZu0gWContent-Disposition: form-data; name="bs\_audio"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",                    "clientDuration":2000,                    "duration":1,                    "index":0,                    "message":"Пожалуйста моргните"                },                {                    "type":"smile",                    "clientDuration":2000,                    "duration":1,                    "index":1,                    "message":"Пожалуйста улыбнитесь"                }            ]        },        {            "mnemonic":"text-instructions",            "index":1,            "actions":[                {                    "type":"digits",                    "clientDuration":2000,                    "duration":1,                    "index":0,                    "message":"Пожалуйста произнесите цифры"                }            ]        }    ]------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 сообщение НТТР OK (код состояния 200). В HTTP заголовке «Location» содержится URL ИС Потребителя БДн, для перенаправления пользователя после удачной верификации. ЕБС использует значение URL ИС Потребителя БДн, переданное в параметре «redirect» при вызове метода «Старт верификации в ЕБС». В случае возникновения ошибки метод вернет в ответе код и описание ошибки и не перенаправит пользователя по адресу, указанному в redirect.

В составе дополнительных заголовков передаются параметры, приведенные в таблице ниже.

Таблица 16 – Выходные параметры

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

**Пример ответа:**

|  |
| --- |
| HTTP/1.1 200 OKLocation: https:/bank.example.com/iss/code/verify?bank\_session=12345&expired=1499443407648&verify\_token=0BCAF243SE9CF4F607E3CEB7EE416D031Verification-Token:0BCAF243SE9CF4F607E3CEB7EE416D031Session-Expires:1499443407648 |

**Ошибки метода:** В случае возникновения ошибки при обработке запроса, ЕБС возвращает вызывающей стороне коды ответов HTTP и описания ошибок в HTTP BODY, согласно [таблице 12](#Таблица12) выше.

Получение расширенного результата верификации

Завершающим этапом проведения биометрической верификации зарегистрированного в ГИС ЕБС Пользователя является предоставление внешней информационной системе расширенного результата успешной верификации, включающего в себя значения степеней схожести по отдельным модальностям. Для этого внешняя информационная система формирует соответствующий запрос к ГИС ЕБС с передачей информации о Пользователе, а также токена получения расширенного результата верификации, полученного от ГИС ЕБС на этапе отправки биометрических образцов (переадресации с формы съема БО).

**Вызов сервиса**

GET /api/v3/verifications/{session\_id}/result

где: {session\_id} – идентификатор сессии верификации в ГИС ЕБС, полученный в ответе метода «Старт верификации в ГИС ЕБС».

Заголовки:

* + Host: {host ГИС ЕБС}
	+ X-EBS-TraceProcess: true (необязательный заголовок, необходимый для проверки взаимодействия с использованием Технологического портала)
	+ Authorization: Bearer {JWT токен от провайдера идентификации, сформированный в соответствии с RFC 7519 https://datatracker.ietf.org/doc/html/rfc7519}
	+ Cache-Control: no-cache

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 том числе описание используемого алгоритма для подписи;

JWT.PAYLOAD – непосредственно данные (состав в таблице ниже);

JWT.SIGNATURE – подпись запроса (запрос должен быть подписан CAdES-T или PLAIN, закодированный в формате Base64url).

Состав JWT.PAYLOAD описан в таблице (Таблица 17).

Таблица 17 – Состав JWT.PAYLOAD

|  |  |  |  |
| --- | --- | --- | --- |
| **Наименование параметра** | **Тип данных** | **Обязательность** | **Описание** |
| iss | String | да | Чувствительная к регистру строка или [URI](https://ru.wikipedia.org/wiki/URI), которая является уникальным идентификатором стороны, генерирующей токен (например http://test.idp.ru/urn |
| sub | String | да | Идентификатор УЗ Пользователя IDP  |
| aud | String или Array 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 |
| client\_id | String | да | Мнемоника Потребителя БДн |
| verify\_token | String | да | Контрольное значение (уникальный идентификатор, созданный ГИС ЕБС на этапе отправки БО для верификации), необходимое для получения расширенного результата верификации после успешной верификации. |

Пример JWT.PAYLOAD:

|  |
| --- |
| { "iss":"http(s)://test.idp.ru/urn", "sub":"11111111", "iat":1551940551, "exp":1551941153, "nbf":1584652769, "client\_id":"TEST\_SYSTEM", "verify\_token":"0BCAF243SE9CF4F607E3CEB7EE416D031"} |

Пример запроса:

|  |
| --- |
| { GET /api/v3/verifications/D530D7AF1EFA47489653FC4CEA5AC625/result HTTP/1.1 Host: int.ebs.ru X-EBS-TraceProcess: true Authorization: Bearer {JWT токен} Cache-Control: no-cache} |

**Успешный ответ**

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

Таблица 18 – Состав успешного ответа

|  |  |  |  |
| --- | --- | --- | --- |
| **Наименование параметра** | **Тип данных** | **Обязательность** | **Описание** |
| extended\_result | String | да | Расширенный результат верификации, 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 Base64url Encoding значение.

JWT.HEADER – описание свойств токена, в том числе описание используемого алгоритма для подписи;

JWT.PAYLOAD – непосредственно данные (состав в таблице ниже);

JWT.SIGNATURE – подпись запроса (запрос должен быть подписан CAdES-T, закодированный в формате Base64url).

Состав JWT.PAYLOAD описан в таблице (Таблица 20).

Таблица 19 - Состав JWT.PAYLOAD

|  |  |  |  |
| --- | --- | --- | --- |
| **Наименование параметра** | **Тип данных** | **Обязательность** | **Описание** |
| iss | String | да | Идентификатор организации, выпустившей токен. В данном случае ГИС ЕБС: http(s)://ebs-fr.rtlabs.ru |
| sub | String | да | Идентификатор УЗ Пользователя в IDP |
| aud | String | да | Мнемоника ИС Потребителя БДн |
| 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 |
| exp | Number | да | Время в формате Unix Time, определяющее момент, когда токен станет не валидным |
| result | String | да | Результат биометрической верификации |
| age\_determined | Boolean | нет | Признак успешного определения возраста. Заполняется только при использовании схем сбора с определением возраста |
| age | Int | нет | Возраст субъекта верификации. Заполняется только при использовании схем сбора с определением возраста, если удалось определить возраст |
| match | JSON Object | да | Содержит степени схожести (общая и по каждой из модальностей) |
| match.overall | Number | да | Суммарная степень схожести.Вычисляется как разность единицы и произведения вероятностей ложного совпадения по каждой из модальностей |
| match.{модальность} | Number | да | Степень схожести по отдельным модальностям.Вычисляется как разность единицы и вероятности ложного совпадения по отдельной модальности. |

Пример ответного JWT.PAYLOAD:

|  |
| --- |
| { "iss":"http://ebs-fr.rtlabs.ru", "sub":11111111, "aud":"TEST\_SYSTEM", "nbf":1551940552, "iat":1551940551, "exp":1551941153, "result":true, "age\_determined": true, "age": 32, "match":{ "voice": 0.70903534, "face": 0.999999022, "overall":0.9999997154365625 }} |

Пример успешного ответа:

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

**Ошибки метода**

В случае возникновения ошибки при обработке запроса, ГИС ЕБС возвращает вызывающей стороне HTTP-код ошибки и описание ошибки в BODY, согласно [таблице 12](#Таблица12) выше.

ПРИЛОЖЕНИЕ №1. Дополнительные метаданные (meta)

Все параметры metadata, перечисленные в таблице ниже, имеют тип String.

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

Помимо целевого значения, все параметры (в случае указания), 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.

| **Наименование параметра** | **Описание** | **Формат** | **Пример** |
| --- | --- | --- | --- |
| date | Дата и время начала операции (формирования запроса клиентом) | timestamp | 1520467814933 |
| time\_zone | 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 | Координаты (Геолокация): широта и долгота | latitude;longitude | 51.7556415;55.1028652 |
| rooted | Наличие jailbreak или root-доступа в операционной системе | true/false | true |
| operating\_system | Операционная система устройства:−      название;−      версия | name version | Android 6.0.1 |
| isp | Провайдер | name | MegaFon |
| advertising\_id | Идентификатор рекламы устройства (AdID в Android и IDFA в iOS) | value | 38400000-8cf0-11bd-b23e-10b96e40000d |
| screen | Разрешение экрана | width;height | 1200;1920 |
| dpi | Плотность экрана устройства - значение, единицы измерения плотности пикселей | value | 320 Dpi |
| camera\_id | Идентификатор камеры | name | 2 |
| locale | 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 | Серийный номер мобильного устройства. | deviceNumber | 0819da27 |
| imei | IMEI - международный идентификатор мобильного оборудования | value | 357719051789508 |
| device\_id | Уникальный идентификатор Android-устройства | value | d1b23eв2f3b480сb |
| device\_manufacturer | Производитель устройства | name | asus |
| device\_model | Модель устройства | name | Nexus 7 |
| device\_cpu | Информация о процессоре устройства | value | ARMv7 Processor rev 0 (v7l) |
| sim | 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 получения значения.

|  |  |  |  |
| --- | --- | --- | --- |
| **Мнемоника** | **Тип данных** | **Обязательность** | **Описание** |
| 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 (акципт, 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. |
| 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. |
| 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. |
| 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. |
| name\_equipment\_camera | string | необязательное | **В случае доступности такой информации.**Наименование оборудования (камера)если информация не доступна указывается |
| name\_equipment\_microphone | string | необязательное |  Наименование оборудования (микрофон) |

ПРИЛОЖЕНИЕ №3. 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. 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-1)
2. Описание алгоритма хеширования данных представлено в Приложении №3. [↑](#footnote-ref-2)
3. Описание алгоритма хеширования данных представлено в Приложении №3. [↑](#footnote-ref-3)
4. Доступны по адресу <https://ebs.ru/documents> в разделе «Основные» [↑](#footnote-ref-4)