

МИНОБРНАУКИ РОССИИ

Федеральное государственное бюджетное образовательное учреждение высшего образования **«МИРЭА – Российский технологический университет»  
РТУ МИРЭА**

**Институт кибербезопасности и цифровых технологий**

*(наименование института, филиала)*

**Кафедра КБ-2«Прикладные информационные технологии»**

*(наименование кафедры)*

**ОТЧЕТ**

по дисциплине: «Биометрические системы аутентификации»

Задание получил:

|  |  |
| --- | --- |
| III курс, группа БИСО-02-23 |  |
|  | *Подпись* |

|  |
| --- |
| Макаревич Сергей Витальевич |
| *ФИО* |

Проверил:

|  |  |
| --- | --- |
| «    » \_\_\_\_\_\_\_2025 г. |  |
| *Дата* | *Подпись* |

|  |  |
| --- | --- |
|  | Стародубов К. В. |
| *Отметка / результат* | *ФИО* |

Москва 2025 г.

Оглавление

[Техническое задание на проектирование и внедрение аккредитованной Единой биометрической системы 3](#_Toc209200060)

[1. Общие положения 3](#_Toc209200061)

[2. Определение и правовой статус 3](#_Toc209200062)

[3. Назначение, цели и функции системы 4](#_Toc209200063)

[3.1 Назначение 4](#_Toc209200064)

[3.2 Цели 4](#_Toc209200065)

[3.3 Функции 4](#_Toc209200066)

[4. Требования к организации-оператору для прохождения аккредитации 5](#_Toc209200067)

[5. Требования к оборудованию и функциональным возможностям 5](#_Toc209200068)

[6. Процесс проверки живости (Liveness) 6](#_Toc209200069)

[7. Общая архитектурная схема взаимодействия 7](#_Toc209200070)

Техническое задание на проектирование и внедрение аккредитованной Единой биометрической системы

1. Общие положения

Настоящее техническое задание разработано в целях проектирования, построения и ввода в эксплуатацию аккредитованной Единой биометрической системы (далее — ЕБС), функционирующей в соответствии с Федеральным законом от 29.12.2022 № 572-ФЗ «Об осуществлении идентификации и (или) аутентификации физических лиц с использованием биометрических персональных данных…», Постановлением Правительства Российской Федерации от 31.05.2023 № 883, а также приказами и методическими документами Минцифры России.

ЕБС является государственной информационной системой, предназначенной для сбора, обработки, хранения и использования биометрических персональных данных физических лиц в целях идентификации и (или) аутентификации, при оказании государственных, муниципальных и иных услуг, а также для обеспечения надёжной и безопасной работы цифровой экономики Российской Федерации.

2. Определение и правовой статус

Аккредитованная Единая биометрическая система — это государственная информационная система, прошедшая процедуру аккредитации в установленном порядке и обладающая правом на законное осуществление операций по приёму, обработке, хранению и сопоставлению биометрических персональных данных (изображений лица и голосовых записей), а также по формированию и применению векторов ЕБС.

Аккредитация представляет собой процедуру официального подтверждения соответствия организации или системы требованиям федерального законодательства, нормативных актов Минцифры России и стандартов информационной безопасности. По результатам аккредитации оператор ЕБС получает право функционировать в качестве доверенного элемента инфраструктуры идентификации и аутентификации Российской Федерации.

3. Назначение, цели и функции системы

3.1 Назначение

ЕБС предназначена для обеспечения единого и надёжного механизма подтверждения личности граждан Российской Федерации с использованием биометрических персональных данных.

3.2 Цели

Повышение уровня доверия к электронным сервисам и цифровой инфраструктуре;

Обеспечение упрощённого и безопасного доступа граждан к государственным и коммерческим услугам;

Снижение рисков подмены личности, мошенничества и неправомерного доступа;

Создание единого централизованного механизма обработки биометрических данных с гарантированным соблюдением требований законодательства о защите информации и персональных данных.

3.3 Функции

приём и преобразование биометрических персональных данных в цифровые шаблоны (векторы);

централизованное хранение данных и векторов в защищённой среде;

идентификация и аутентификация физических лиц по запросам уполномоченных организаций;

обеспечение юридически значимого подтверждения личности;

поддержка процесса проверки живости (liveness detection);

интеграция с государственной системой ЕСИА и иными информационными ресурсами;

ведение журналов событий, аудит и контроль за использованием биометрических данных.

4. Требования к организации-оператору для прохождения аккредитации

Организация, претендующая на аккредитацию в качестве оператора ЕБС, обязана:

* быть юридическим лицом, зарегистрированным на территории Российской Федерации;
* иметь лицензии ФСТЭК и ФСБ России, позволяющие осуществлять деятельность по обработке и защите информации;
* эксплуатировать средства защиты информации, соответствующие требованиям Федерального закона № 152-ФЗ «О персональных данных» и ГОСТ Р 57580.1-2017;
* обеспечить размещение всей технической инфраструктуры (серверов, хранилищ, сетевых компонентов) исключительно на территории Российской Федерации;
* внедрить комплекс организационных мер, включающих внутренние регламенты, назначение ответственных лиц, подготовку персонала и проведение регулярных аудитов;
* обеспечить возможность прохождения оценки соответствия, независимого аудита и взаимодействия с органами государственного контроля.

5. Требования к оборудованию и функциональным возможностям

Для выполнения возложенных функций оператор ЕБС обязан использовать современное и сертифицированное оборудование, включающее:

* камеры высокого разрешения (в том числе 3D и инфракрасные), обеспечивающие качественный захват изображения лица при различных условиях освещённости;
* микрофоны с функцией подавления шумов, предназначенные для записи голосовых данных с высоким уровнем достоверности;
* серверное оборудование с модулем аппаратного ускорения (GPU/TPU) для обработки биометрических данных и работы нейронных сетей;
* средства криптографической защиты информации, сертифицированные в установленном порядке, для обеспечения конфиденциальности и целостности данных.

Функционал должен включать:

* формирование и хранение биометрических шаблонов (векторов);
* применение нейросетевых моделей для распознавания лица и анализа голоса;
* реализацию обязательных процедур проверки живости (liveness detection);
* защиту данных от подделки, утечки и несанкционированного доступа;
* интеграцию с государственными и коммерческими системами исключительно по защищённым каналам связи.

6. Процесс проверки живости (Liveness)

Liveness detection является обязательным элементом процедуры идентификации и направлен на исключение попыток обмана системы посредством использования фотографий, видеозаписей, масок, синтезированного или записанного голоса.

Процесс включает:

* предъявление пользователю случайных инструкций (например, повернуть голову, моргнуть, произнести определённую фразу);
* фиксацию реакции с помощью камер и микрофонов в реальном времени;
* анализ глубины изображения, текстуры кожи, естественности движений и речи;
* применение специализированных алгоритмов и нейросетей для выявления признаков подделки;
* вынесение решения о подлинности данных и фиксацию результата в системе.

Данный процесс регламентирован требованиями приказов Минцифры России, а также ГОСТами в области биометрической аутентификации и защиты информации.

7. Общая архитектурная схема взаимодействия

В архитектуре ЕБС выделяются следующие участники:

* Субъект персональных данных (гражданин): предоставляет свои биометрические данные.
* Оператор сбора биометрии: осуществляет сбор данных, проведение liveness и передачу результатов в ЕБС.
* Аккредитованная ЕБС: выполняет преобразование, хранение и сопоставление биометрических данных, а также обеспечивает выдачу результатов идентификации и аутентификации.
* Государственные и коммерческие информационные системы: используют результат аутентификации для оказания услуг.
* Регулирующие органы: осуществляют контроль и надзор за соблюдением требований законодательства.

Информационные потоки организуются по принципу защищённых каналов связи с обязательным применением сертифицированных средств криптографической защиты. Передаются исключительно цифровые шаблоны (векторы) и результаты аутентификации; исходные биометрические данные не раскрываются.