Приложение №1 к Закупочной документации

ТЕХНИЧЕСКОЕ ЗАДАНИЕ

на выполнение работ по созданию системы
«Национальная биометрическая платформа»
(НБП)

На 59 листах

Москва 2017

Содержание

1 Общие положения

1.1 Полное наименование системы и ее условное обозначение

Полное наименование: Система «Национальная биометрическая платформа».

Условные обозначения: НБП, Система.

Далее по тексту будет использоваться как полное наименование, так и условные обозначения.

1.2 Номер договора (контракта)

1.3 Наименования Заказчика и Исполнителя работ

Заказчиком выполнения работ по созданию Системы «Национальная биометрическая платформа» (далее – работ) является Публичное акционерное общество международной и междугородней электрической связи «Ростелеком» (ПАО «Ростелеком»), далее Заказчик.

Исполнителем работ по созданию Системы является Акционерное общество «РТ К Софт Лабс» (ООО «РТК Софт Лабс»), далее Исполнитель.

1.4 Сроки начала и окончания работы по созданию системы

Начало работ – дата заключения договора на выполнение работ по созданию Системы, заключённому между Заказчиком и Исполнителем (далее Договор).

Окончание работ – не позднее 22 декабря 2017 года.

Сроки начала и окончания Этапов работ приведены в разделе 5 настоящего ТЗ.

1.5 Источники и порядок финансирования работ

Источник финансирования работ определяется Заказчиком.

Порядок финансирования работ определяется действующими нормативными правовыми актами Российской Федерации и Договором.

1.6 Порядок оформления и предъявления заказчику результатов работ по созданию Системы

Разработанная Система передаётся Заказчику в виде дистрибутива, исходных кодов прикладного программного обеспечения и комплекта документации на создание Системы. Требования к составу документации Системы определены в разделе «Требования к документированию» настоящего Технического задания.

Приёмка Системы осуществляется комиссией в составе уполномоченных представителей Заказчика с участием представителей Исполнителя.

Порядок предъявления Системы, её испытаний и окончательной приёмки определён в разделе «Порядок контроля и приемки системы» настоящего Технического задания.

1.7 Перечень нормативно-технических документов, методических материалов, использованных при разработке ТЗ

Выполняемая работа и оформление её результатов должны отвечать требованиям нормативно-правовых актов, а также соответствующих государственных стандартов из числа Комплекса стандартов на автоматизированные системы:

- ГОСТ 34.003-90 «Информационная технология. Комплекс стандартов на автоматизированные системы. Автоматизированные системы. Термины и определения»;
- ГОСТ 34.201-89 «Информационная технология. Комплекс стандартов на автоматизированные системы. Виды, комплектность и обозначение документов при создании автоматизированных систем»;
- ГОСТ 34.602-89 «Информационная технология. Комплекс стандартов на автоматизированные системы. Техническое задание на создание автоматизированной системы»;
- РД 50-34.698-90 «Автоматизированные системы. Требования к содержанию документов»;
- Федеральный закон РФ от 07.08.2001 № 115-ФЗ «О противодействии легализации (отмыванию) доходов, полученных преступным путем, и финансированию терроризма»;
- Федеральный закон РФ от 07.07.2003 № 126-ФЗ «О связи»;

– Положение Банка России от 15.10.2015 № 499-П «Об идентификации кредитными организациями клиентов, представителей клиента, выгодоприобретателей и бенефициарных владельцев в целях противодействия легализации (отмыванию) доходов, полученных преступным путем, и финансированию терроризма».

1.8 Термины и определения

Термин	Определение
Адаптация биометрического контрольного шаблона	Автоматическое инкрементное обновление биометрического контрольного шаблона
Аутентификация	Действия по проверке подлинности субъекта доступа в автоматизированной информационной системе
База данных биометрических контрольных шаблонов	База данных записей данных биометрических контрольных шаблонов
База данных биометрических регистраций	База данных записей данных биометрических регистраций
Биллинг	Комплекс процессов и решений, по сбору информации и тарификации услуг, операционному и финансовому абонентскому обслуживанию
Бимодальный режим	Режим работы биометрической системы, при котором процесс биометрического распознавания происходит одновременно по каким-либо двум биометрическим характеристикам
Биометрическая верификация	Процесс подтверждения биометрического заявления при сравнении
Биометрическая проба	Биометрический образец или набор

	биометрических признаков, введенный в алгоритм для использования в качестве объекта сравнения с биометрическим контрольным шаблоном (биометрическими контрольными шаблонами)
Биометрическая регистрация	Действия по созданию и сохранению записи данных биометрической регистрации в соответствии с правилами биометрической регистрации
Биометрическая регистрация в НБП	Действия по созданию и сохранению записи данных биометрической регистрации в соответствии с правилами биометрической регистрации в НБП
Биометрическая система	Система, предназначенная для биометрического распознавания индивидов, основанного на их поведенческих и биологических характеристиках
Биометрическая характеристика	Биологические и поведенческие характеристики индивида, которые могут быть зарегистрированы и использованы в качестве отличительных, повторяющихся биометрических признаков для автоматического распознавания индивидов.
Биометрические данные	Биометрический образец или совокупность биометрических образцов на любой стадии обработки, например, биометрический контрольный шаблон, биометрическая проба, биометрический признак или биометрическое свойство
Биометрический контрольный шаблон	Один или более хранимых биометрических образцов, биометрических шаблонов или биометрических моделей, относящихся к

	субъекту биометрических данных и используемых в качестве объекта сравнения
Биометрический образец	Аналоговое или цифровое представление биометрических характеристик, предшествующее извлечению биометрических признаков
Биометрический признак	Цифровое представление информации (числа или метки), извлеченное из биометрических образцов и используемое для сравнения
Биометрический шаблон	Набор хранимых биометрических признаков, сравниваемых непосредственно с биометрическими признаками биометрической пробы
Биометрическое заявление	Заявление, что субъект сбора биометрических данных является или не является собственно источником установленного или неустановленного биометрического контрольного шаблона
Биометрия (биометрическое распознавание)	Автоматическое распознавание человека, основанное на его поведенческих и биологических характеристиках.
Биометрический процессор	Обработчик запросов на выполнение биометрических операций.
Дистанционная идентификация	Идентификация пользователей, в рамках требований Федерального закона от 07.08.2001 №115-ФЗ, осуществляемая по удаленным каналам связи, без визита пользователя в офис кредитной организации
Запись данных биометрической	Запись данных, связанная с субъектом

регистрации	биометрических данных, содержащая не биометрические данные, и связанная с идентификатором (идентификаторами) биометрического контрольного шаблона
Идентификатор биометрического контрольного шаблона	Указатель на запись данных биометрического контрольного шаблона в базе данных биометрических контрольных шаблонов
Инфраструктура электронного правительства (ИЭП, e-Government)	Совокупность аппаратного и программного обеспечения для предоставления информации и оказания государственных услуг гражданам, бизнесу, другим ветвям государственной власти и государственным чиновникам, при котором личное взаимодействие между государством и заявителем минимизировано и максимально возможно используются информационные технологии.
Конечный пользователь, Пользователь НБП	Человек, взаимодействующий с биометрической системой с целью регистрации или идентификации его личности
Мультимодальная биометрическая система	Биометрическая система, работающая как минимум с двумя различными биометрическими характеристиками
Национальная биометрическая платформа (НБП)	Система, обеспечивающая сбор, хранение, обработку и передачу биометрических данных человека
Сбор биометрических данных	Получение и запись в воспроизводимой форме сигнала биометрической характеристики (биометрических характеристик) непосредственно от индивида, или от представления биометрической характеристики

	(биометрических характеристик)
Сравнение	Оценка, вычисление или измерение степени схожести и различия между биометрическим образцом и биометрическим контрольным шаблоном
Транзакция биометрической верификации	Одна или более попыток биометрической верификации, результатом которых является заключение о биометрическом заявлении
Транзакция сбора биометрических данных	Одна или более попыток сбора биометрических данных с целью получения всех биометрических данных от субъекта биометрических данных, необходимых для создания биометрического контрольного шаблона или биометрической пробы
Унимодальный режим	Режим работы биометрической системы, при котором процесс биометрического распознавания происходит по какой-либо одной биометрической характеристике (например, по записи голоса)

1.9 Обозначения и сокращения

Сокращение	Определение
ID	Уникальный идентификатор учетной записи в ИС
SMS (СМС)	Технология, позволяющая осуществлять приём и передачу коротких текстовых сообщений с помощью мобильного телефона подвижной радиосвязи.
Web (Веб) приложение	Клиент-серверное приложение, в котором клиентом выступает интернет браузер, а сервером — интернет-сервер

Сокращение	Определение
WSDL	Язык описания веб-сервисов и доступа к ним, основанный на языке XML
XML	Расширяемый язык разметки текстовых документов
БД	База данных
БДн	Биометрические данные
БИК	Банковский идентификационный код — уникальный идентификатор банка, используемый в платежных документах на территории РФ
ДКО	Дистанционные каналы обслуживания (WEB и мобильные приложения)
ИС	Информационная система
ИЭП	Инфраструктура электронного правительства
КО	Кредитные организации
КТС	Комплекс технических средств
КЭП	Квалифицированная электронная подпись
МВД	Министерство внутренних дел России
МКС	Министерство связи и массовых коммуникаций Российской Федерации
НБП, Система	Национальная биометрическая платформа
ОС	Операционная система
ПАК	Программно-аппаратный комплекс
ПДн	Персональные данные

Сокращение	Определение
ПО	Программное обеспечение
ПОД/ФТ	Противодействие легализации (Отмыванию) Доходов, полученных преступным путем, и Финансированию Терроризма
ПОИБ	Подсистема обеспечения информационной безопасности
ППО	Прикладное программное обеспечение
СУБД	Система управления базами данных
ТП	Техническое проектирование
УЗ	Учетная запись
ФГИС ЕСИА, ЕСИА	Федеральная государственная информационная система «Единая система идентификации и аутентификации в инфраструктуре, обеспечивающей информационно-технологическое взаимодействие информационных систем, используемых для предоставления государственных и муниципальных услуг в электронной форме»
ФГИС СМЭВ, СМЭВ	Федеральная государственная информационная Система Межведомственного Электронного Взаимодействия
ФЛ	Физическое лицо
ФОИВ	Федеральный орган исполнительной власти
ФСБ	Федеральная служба безопасности России
ЦБ РФ	Центральный Банк Российской Федерации
ЧТЗ	Частное техническое задание

2 Назначение и цели создания системы

Национальная биометрическая платформа (НБП) предназначена для обеспечения удаленной биометрической верификации (подтверждения) личности по биометрическим параметрам при получении доступа к персональным данным при выполнении банковских операций.

2.1 Цели и задачи создания Системы

Целью создания Системы является обеспечение возможности проведения удаленной электронной биометрической верификации пользователей по биометрическим характеристикам для исполнения требований, установленных федеральными законами от 07.08.2001 № 115-ФЗ «О противодействии легализации (отмыванию) доходов, полученных преступным путем, и финансированию терроризма» (далее – Федеральный закон № 115-ФЗ) и от 07.07.2003 № 126-ФЗ «О связи» (далее – Федеральный закон № 126-ФЗ).

Система должна позволять обеспечивать идентификацию физических лиц кредитными организациями (КО), с дальнейшим оказанием им банковских услуг.

Система должна обеспечить возможность решения следующих задач:

1. Процесса сбора биометрических данных как в офисах КО, так и удаленно;
2. Процесса передачи биометрических образцов от КО в НБП;
3. Процесса хранения биометрических образцов в НБП;
4. Процесса формирования из биометрических образцов биометрических шаблонов с приданием им статуса биометрических контрольных шаблонов;
5. Хранение в Системе биометрических контрольных шаблонов;
6. Получение биометрических образцов от пользователей через ДКО КО;
7. Сравнение биометрических образцов с биометрическими контрольными шаблонами для проведения процедуры биометрической верификации в НБП;
8. Процесса взаимодействия НБП с ДКО КО;
9. Процесса взаимодействия НБП с ЕСИА и СМЭВ;
10. Процесс тарификации использования биометрических данных.

Система должна обеспечивать мультимодальный режим работы. Список биометрических характеристик (модальностей), используемых для осуществления процесса верификации, будет определен на этапе технического проектирования.

3 Характеристика объекта автоматизации

3.1 Список процессов автоматизации

Объектом автоматизации является деятельность по организации и проведению удаленной идентификации пользователей в КО и/или инфраструктуре электронного правительства посредством сличения биометрических данных.

Объектом автоматизации являются следующие процессы:

- Процесс биометрической регистрации (создания биометрического контрольного шаблона пользователя);
- Процесс биометрической верификации;
- Процесс адаптации биометрического контрольного шаблона;
- Процесс деактивации биометрического контрольного шаблона.

3.2 Описание процессов

3.2.1 Биометрическая регистрация

Для получения возможности прохождения удаленной идентификации через ДКО в различных КО, физическое лицо, должно лично обратиться в КО, имеющую право проводить биометрическую регистрацию, с целью прохождения процедуры биометрической регистрации. Список КО, имеющих право проводить полную биометрическую регистрацию устанавливается Банком России.

В соответствии с требованиями Федерального закона № 115-ФЗ, процесс биометрической регистрации физического лица в НБП должен сопровождаться идентификацией физического лица в ЕСИА, и не может быть осуществлен частично.

Снятые биометрические образцы идентифицированного клиента проверяются с помощью, поставляемой НБП библиотеки контроля качества на соответствие требованиям, после чего данные биометрические образцы с дополнительной информацией передаются в НБП.

Передача биометрических образцов из КО в НБП должна осуществляться с использованием Единой системы межведомственного информационного взаимодействия (СМЭВ) в соответствии с действующими методическими рекомендациями СМЭВ.

На этапе создания биометрического шаблона из биометрического образца создается модель – биометрический признак, содержащий информацию об уникальных биометрических характеристиках физического лица. Созданные унимодальные или бимодальные биометрические признаки пользователя после успешной регистрации в системе называются биометрическим шаблоном. Биометрический шаблон, сохраненный в хранилище биометрических данных пользователей вместе с биометрическими образцами называется биометрическим контрольным шаблоном. Дополнительная не биометрическая информация, хранимая в Подсистеме хранения данных НБП, связанная с идентификатором УЗ пользователя в ЕСИА и биометрическим контрольным шаблоном называется записью данных биометрической регистрации.

Дополнительная информация, хранимая в записи данных биометрической регистрации должна включать в себя:

- дату, время и место проведения биометрической регистрации;
- идентификатор КО, проводившей биометрическую регистрацию;
- дата и время последней адаптации биометрического контрольного шаблона, включая идентификаторы КО;
- Иные транзакционные параметры, необходимые для повышения мер, направленных на совершенствование мер контроля режима ПОД/ФТ и совершенствования мер противодействия мошенническим операциям (должны быть уточнены на этапе технического проектирования).

По окончанию создания биометрического контрольного шаблона в НБП, установке в УЗ ЕСИА признака наличия биометрии и соответствию статуса УЗ ЕСИА «Подтвержденная», ЕСИА информирует клиента и КО об изменении статуса его УЗ, а также, что данный клиент может проходить процедуру удаленной идентификации в ДКО.

3.2.2 Биометрическая верификация

Процедура удаленной идентификации включает последовательное прохождение аутентификации в ЕСИА по логину/паролю и в НБП по степени схожести биометрического образца.

Для обеспечения процедуры удаленной идентификации используются средства, реализованные посредством универсального механизма для снятия биометрических

данных в ДКО, с помощью которого, производится снятие и проверка качества биометрических образцов и осуществляется передача биометрических данных в НБП.

На этапе биометрической верификации в НБП создается биометрическая проба, состоящая из предоставленных биометрических образцов и созданных из биометрических образцов моделей – биометрических признаков. Биометрическая проба сравнивается с биометрическим контрольным шаблоном, находящимся в хранилище биометрических данных пользователей. Результатом верификации является:

- расчет значения степени схожести биометрической пробы и соответствующего биометрического контрольного шаблона;
- передача результатов сравнения во внешнюю систему.

НБП возвращает положительный результат, если степень схожести превышает установленный правительством РФ по согласованию с ЦБ минимальный порог. В ином случае возвращается отказ.

3.2.3 Адаптация биометрического контрольного шаблона

Адаптация биометрического контрольного шаблона происходит после того, как пользователь успешно прошел биометрическую верификацию с высокой степенью схожести. Созданные на этапе верификации биометрические образцы и признаки объединяются с биометрическим контрольным шаблоном, содержащимся в хранилище биометрических данных пользователей.

Процесс адаптации биометрических контрольных шаблонов идентичен процессу их создания.

3.2.4 Деактивация биометрического контрольного шаблона

В случае получения от ФЛ уведомления об остановке действия согласия на обработку относящихся к нему персональных данных, все относящиеся к нему биометрические шаблоны, находящиеся в НБП, получают отметку о деактивации. С такими шаблонами в дальнейшем не производится никаких действий, в том числе адаптации и аутентификации с их применением. Такие шаблоны не передаются какой-либо второй стороне, за исключением случаев, предусмотренных законодательством РФ.

4 Требования к системе

4.1 Требования к системе в целом

4.1.1 Требования к структуре и функционированию системы

4.1.1.1 Перечень подсистем, их назначение и основные характеристики

Система должна представлять собой многокомпонентное ПО, позволяющее осуществлять:

- сбор, хранение, обработку и управление биометрическими данными пользователей;
- верификацию пользователя по его биометрическим данным:
  - в унимодальном режиме;
  - в бимодальном режиме.
- адаптацию биометрического контрольного шаблона;
- деактивацию биометрического контрольного шаблона.

Система должна состоять из следующих подсистем см. Таблица **1.**

Таблица 1. Подсистемы АС "Национальная биометрическая платформа"

№	Название модуля	Требование
1.	Подсистема внешней интеграции	создание
2.	Подсистема балансировки и обработки запросов	создание
3.	Подсистема интеграционная шина	создание
4.	Подсистема управления конфигурацией	создание
5.	Подсистема администрирования и управления доступом	создание
6.	Подсистема хранилища биометрических данных	создание
7.	Подсистема журналирования и аудита	создание
8.	Подсистема отчётности	создание
9.	Подсистема детектирования подделок	создание
10.	Подсистема мониторинга	создание
11.	Подсистема тарификации	создание

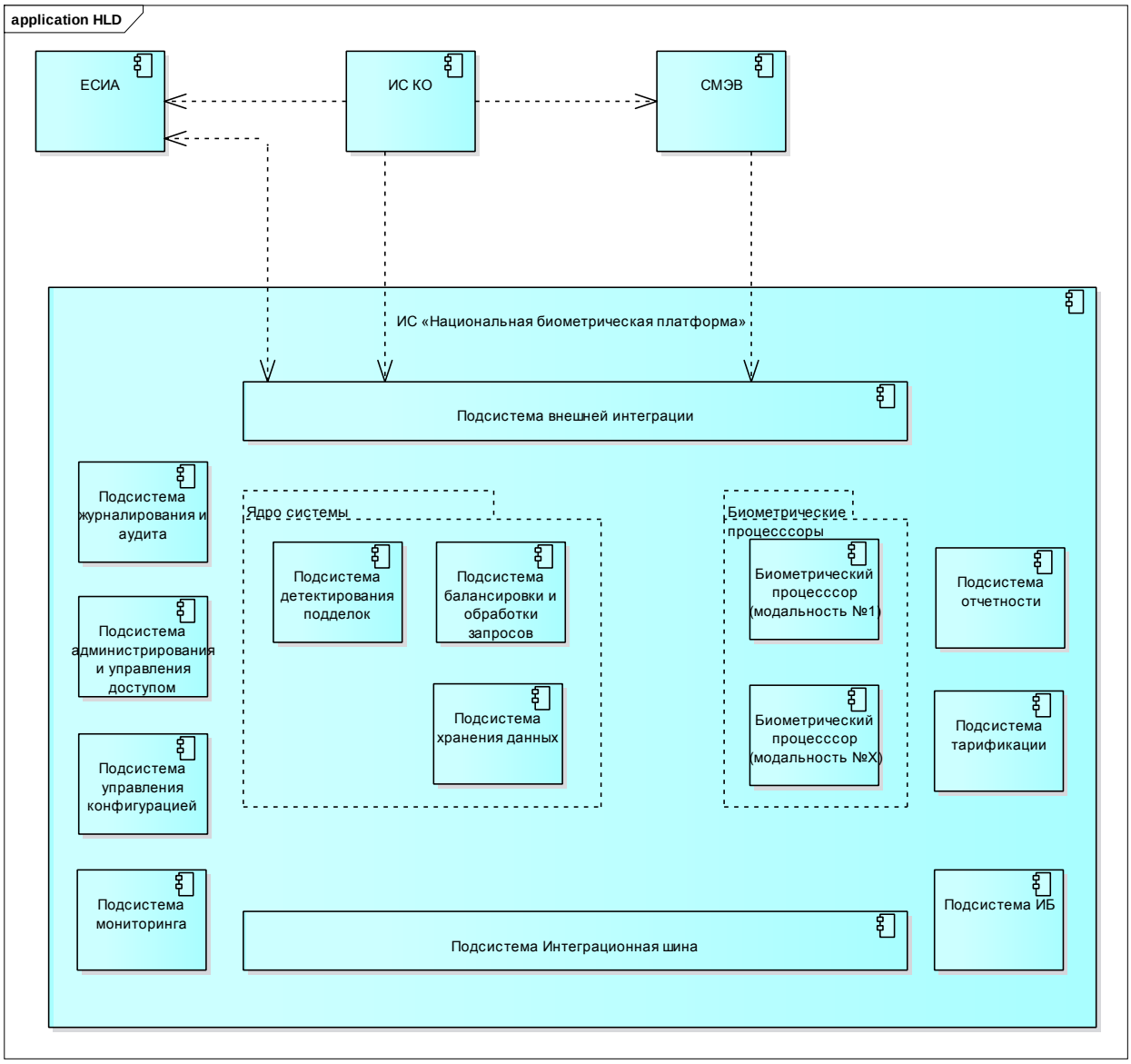

Рисунок 1 Эскиз архитектурной схемы Системы

Система должна иметь модульную структуру и состоять из следующих логических блоков, взаимодействующих между собой:

- управляющих программных компонентов, обеспечивающих корректное бесперебойное функционирование Системы;
- ядра Системы - программных компонентов обработки запросов и хранения биометрических данных;
- биометрических процессоров обработки биометрических данных;
- интеграционной шины, используемой для взаимодействия компонентов системы;
- программных компонентов отчетности и тарификации;

- программных интерфейсов взаимодействия с существующей инфраструктурой и бизнес-приложениями.

Каждый компонент НБП должен представлять собой независимую подсистему, предназначенную для выполнения ряда функции.

Система должна поддерживать мультивендорность используемых биометрических технологий, позволяющую как смену вендора, так и одновременную работу нескольких вендоров, без внесения доработок в архитектуру Системы. Мультивендорность должна достигаться в первую очередь стандартизацией сбора, обработки и хранения биометрических образцов. Обеспечение мультивендорности, в частности алгоритм и реализация, должны быть согласованы с Заказчиком в ЧТЗ.

4.1.1.1.1 Подсистема внешней интеграции

Подсистема внешней интеграции предназначена для обеспечения взаимодействия с внешними информационными системами и существующей ИЭП. В число смежных систем, с которыми предполагается взаимодействие, входят:

- ЕСИА;
- СМЭВ;
- ИС КО.

4.1.1.1.2 Подсистема балансировки и обработки запросов

Подсистема балансировки и обработки запросов предназначена для распределения запросов на биометрическую регистрацию, верификацию и адаптацию биометрических контрольных шаблонов, направляемых в биометрические процессоры с учетом типа биометрии и правил выбора соответствующего биометрического процессора.

4.1.1.1.2.1 Функция биометрической регистрации

Биометрическая регистрация заключается в создании биометрического контрольного шаблона и представляет собой два последовательных шага:

1. создании в биометрическом процессоре биометрических шаблонов физического лица по предоставленным биометрическим образцам;
2. сохранении в хранилище биометрических данных соответствующих наборов или комбинаций предоставленных биометрических образцов и шаблонов

одного конечного пользователя с привязкой к ID учетной записи данного пользователя в ЕСИА.

4.1.1.1.2.2 Функция биометрической верификации

Биометрическая верификация осуществляется в биометрическом процессоре и представляет собой два последовательных шага:

1. создание биометрической пробы пользователя;
2. сравнение данной биометрической пробы с биометрическим контрольным шаблоном пользователя, содержащимся в хранилище биометрических данных пользователей.

4.1.1.1.2.3 Функция адаптации биометрического контрольного шаблона

Адаптация биометрического контрольного шаблона заключается в адаптации содержащихся в нем биометрических шаблонов к:

- естественным изменениям биометрических характеристик человека;
- временным изменениям биометрических характеристик, обусловленных использованием различных каналов связи.

4.1.1.1.3 Подсистема интеграционная шина

Интеграционная шина данных предназначена для асинхронной передачи данных между компонентами Системы с гарантированной доставкой.

4.1.1.1.4 Подсистема управления конфигурацией

Подсистема управления конфигурацией предназначена для:

- централизованного хранения конфигурации компонентов (модулей и подсистем) Системы;
- управления компонентами Системы (запуск, остановка, перезапуск);
- проверки состояния компонентов Системы (запущен, остановлен) в ручном режиме.

4.1.1.1.5 Подсистема администрирования и управления доступом

Подсистема администрирования и управления доступом предназначена для:

- управления доступом пользователей к Системе;

- управления доступом смежных систем к сервисам Системы.

4.1.1.1.6 Подсистема хранения данных

Подсистема хранения данных предназначена для:

- записи, чтения и хранения, биометрических контрольных шаблонов;
- записи, чтения и хранения, биометрических образцов;
- записи, чтения и хранения, дополнительной информации.

4.1.1.1.7 Подсистема журналирования и аудита

Подсистема журналирования и аудита предназначена для:

- фиксации изменений бизнес объектов, журналирования всех интеграционных процессов;
- аудита административных действий, выполняемых в Подсистеме администрирования и управления доступом.

4.1.1.1.8 Подсистема отчетности

Подсистема отчетности предназначена для формирования и представления пользовательских отчетов по данным, полученным от Подсистемы хранения данных и Подсистемы журналирования и аудита.

4.1.1.1.9 Подсистема детектирования подделок

Подсистема детектирования подделок предназначена для обеспечения защиты биометрических верификаций от попыток компрометации путем предоставления фальсифицированных биометрических образцов.

4.1.1.1.10 Подсистема мониторинга

Подсистема мониторинга предназначена для:

- контроля состояния компонентов Системы;
- оповещения сотрудников эксплуатации системы об отказах компонентов Системы;
- отслеживание динамики показателей (тенденций) потребления ресурсов, обеспечивающих предоставление сервисов Системы.

4.1.1.1.11 Подсистема тарификации

Подсистема тарификации предназначена для дифференцированной тарификации использования Кредитными организациями биометрических данных с целью дистанционной идентификации физических лиц с использованием биометрии.

Тарификация использования биометрических данных для целей дистанционной верификации физических лиц с использованием биометрии осуществляется на основании тарифов, установленных Оператором НБП по согласованию с Министерством связи и массовых коммуникаций и Банком России.

4.1.1.2 Требования к характеристикам взаимосвязей создаваемой системы со смежными системами

Подсистема внешней интеграции должна обеспечивать возможность взаимодействия Системы со следующими внешними ИС (см. Таблица 2)

Таблица 2 Взаимосвязи с внешними ИС

№	Название информационной системы	Описание взаимодействия
1.	ЕСИА	Передача информации об успешном окончании процесса биометрической регистрации
2.	СМЭВ	Обеспечение транспорта данных между КО и НБП в целях обеспечения процесса биометрической регистрации
3.	ИС КО	Получение биометрических и не биометрических данных для обеспечения процессов биометрической регистрации и биометрической верификации

4.1.1.3 Требования к режимам функционирования системы

Система должна функционировать в следующих режимах:

- штатный режим;
- режим технического обслуживания.

Штатный режим должен являться основным режимом функционирования, обеспечивающим выполнение задач Системы.

Режим технического обслуживания должен являться технологическим режимом и использоваться для сопровождения Системы, в том числе – изменения конфигурации, параметров работы, настроек, выполнения регламентного обслуживания программно-технических средств. В режиме технического обслуживания осуществляются профилактические работы по обслуживанию системы, а также обновление ПО. Обслуживание проводится эксплуатационным персоналом в условиях минимальной нагрузки на КТС Системы (например, в ночные часы) и включает в себя следующие работы:

- контроль технического состояния оборудования;
- замена оборудования (в случае необходимости);
- обслуживание оборудования в соответствии с требованиями инструкций по эксплуатации этого оборудования фирм-производителей;
- обновление ПО;
- резервное копирование.

Проведение технического обслуживания компонентов Системы должно проводится только после проведения резервного копирования и включения дублирующих экземпляров обслуживаемых компонентов.

Так же в режиме технического обслуживания эксплуатационным персоналом осуществляется восстановление работоспособности системы после следующих отказов/сбоев:

- программного обеспечения;
- отказ серверного оборудования и серверного программного обеспечения;
- отказ активного сетевого оборудования;
- отказ внутренних линий связи между компонентами системы.

При восстановлении после сбоев могут выполняться работы:

- по текущему ремонту оборудования;
- по настройке (установке/переустановке) ПО;

– работы по восстановлению данных из резервных копий.

Во время восстановления после сбоев доступ пользователей к системе невозможен.

4.1.1.4 Требования по диагностированию системы

Программная реализация Системы должна включать в себя программные средства самодиагностики.

Для диагностирования состояния Системы должны использоваться собственные средства контроля доступности и режимов функционирования специального программного обеспечения Системы.

Каждая из подсистем должна иметь возможность работать в режиме диагностики, в котором компоненты системы формируют информацию об ошибках выполнения программного кода в одном или нескольких из возможных видов:

– текстовый лог-файл;

– вывод информации в консоль.

4.1.1.5 Перспективы развития, модернизации системы

Система должна предусматривать возможность масштабирования по производительности и объёму обрабатываемой информации без модификации её программного обеспечения путём модернизации используемого комплекса технических средств.

Система должна быть спроектирована и введена в действие с учётом возможности дальнейшего расширения сферы ее использования, а также возможности расширения списка используемых для автоматического распознавания биометрических характеристик.

Необходимо предусмотреть возможность расширения хранилища биометрических данных до объема полной базы граждан РФ.

4.1.2 Требования к численности и квалификации персонала

Штатный состав персонала, эксплуатирующего Систему, должен формироваться на основании нормативных документов Российской Федерации и Трудового кодекса Российской Федерации.

4.1.3 Показатели назначения

Система должна соответствовать требованиям, в части показателей назначения, приведенным в Таблице 3.

Таблица 3 Требования к показателям назначения

№	Параметр	2017 г
1	Количество уникальных биометрических контрольных шаблонов (шт.)	1 300 000
2	Ожидаемый прирост количества пользователей Системы в год (%)	30%
3	График работы системы	24*7*365 (8760 час/год)
4	Срок хранения биометрических контрольных шаблонов	бессрочно
5	Производительность	15 транзакций/сек
6	Количество одновременных биометрических верификаций	60

4.1.4 Требования к надежности системы

Система должна относиться к обслуживаемым восстанавливаемым изделиям общего назначения многократного циклического применения согласно ГОСТ 27.003-90 «Состав и общие правила задания требований по надежности». Надежность Системы определяется уровнем безотказности в работе и способностью к восстановлению работоспособности после отказов.

Система должна быть устойчива по отношению к программно-аппаратным ошибкам, отказам технических и программных средств, с возможностью восстановления его работоспособности и целостности информационного содержимого при возникновении ошибок и отказов.

Должно быть обеспечено восстановление программного обеспечения серверов в случае сбоя работы оборудования.

Надежность Системы должна обеспечиваться следующими показателями:

- надежностью системы электропитания;
- организацией дисковых массивов серверов технологии RAID;

- дублированием узлов пониженной надежности в серверном оборудовании (вентиляторы, блоки питания);
- наличием и использованием узлов с возможностью «горячей» замены на критичных серверах (вентиляторы, блоки питания, накопители на жестких дисках);
- выполнением резервирования виртуальных вычислительных мощностей и кластеризацией применяемого общего и специального ПО.

Для создаваемой Системы устанавливаются следующие количественные значения показателей надёжности:

- режим работы в целом – 7 дней в неделю, 24 часа в сутки, 365 дней в году;
- доступность Системы не менее 98,7%, включая проведение сервисных и регламентных работ при строгом соблюдении регламентных процедур;
- время восстановления системы (RTO) в штатном режиме после сбоя, не более 35 минут;
- максимальная потеря данных (RPO), не более 2 минут.

4.1.5 Требования к информационной безопасности

На основании п.1 ст.19 Федерального закона от 27.07.2006 №152-ФЗ «О персональных данных», оператор при обработке персональных данных обязан принимать необходимые правовые, организационные и технические меры или обеспечивать их принятие для защиты персональных данных от неправомерного или случайного доступа к ним, уничтожения, изменения, блокирования, копирования, предоставления, распространения персональных данных, а также от иных неправомерных действий в отношении персональных данных.

Защита информации должна быть обеспечена в соответствии с требованиями Законодательства Российской Федерации и нормативно-технической документацией, в частности:

- Федеральный закон от 27.07.2006 № 152-ФЗ «О персональных данных»;
- Постановление Правительства РФ от 06.07.2008 № 512 «Об утверждении требований к материальным носителям биометрических персональных

данных и технологиям хранения таких данных вне информационных систем персональных данных»;

- Постановление Правительства РФ от 01.11.2012 № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных»;
- Постановление Правительства РФ от 03.02.2012 № 79 «О лицензировании деятельности по технической защите конфиденциальной информации»;
- Приказ ФСБ России от 10.07.2014 № 378 «Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных с использованием средств криптографической защиты информации, необходимых для выполнения установленных Правительством Российской Федерации требований к защите персональных данных для каждого из уровней защищенности»;
- Приказ ФСТЭК России от 18.02.2013 № 21 «Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных»;
- Методический документ ФСТЭК России от 11.02.2014 «Меры защиты информации в Государственных информационных системах»;
- Методический документ ФСТЭК России от 15.02.2008 «Базовая модель угроз безопасности персональных данных при их обработке в информационных системах персональных данных»;
- Методический документ ФСТЭК России от 14.02.2008 «Методика определения актуальных угроз безопасности персональных данных при их обработке в информационных системах персональных данных»;
- Методический документ ФСБ России от 21.02.2008 №149/54-144 «Методические рекомендации по обеспечению с помощью криптосредств безопасности персональных данных при их обработке в информационных системах персональных данных с использованием средств автоматизации»;

- ГОСТ Р ИСО/МЭК 24713-1-2013 «Информационные технологии. Биометрические профили для взаимодействия и обмена данными. Часть 1. Общая архитектура биометрической системы и биометрические профили»;
- ГОСТ Р ИСО/МЭК 19784-1-2007 «Автоматическая идентификация. Идентификация биометрическая. Биометрический программный интерфейс. Часть 1. Спецификация биометрического программного интерфейса»;
- ГОСТ Р ИСО/МЭК 19785-1-2008 «Автоматическая идентификация. Идентификация биометрическая. Единая структура форматов обмена биометрическими данными. Часть 1. Спецификация элементов данных»;
- ГОСТ Р ИСО/МЭК 19785-4-2012 «Информационные технологии. Биометрия. Единая структура форматов обмена биометрическими данными. Часть 4. Спецификация формата блока защиты информации»;
- ГОСТ Р 52633.0-2006 «Защита информации. Техника защиты информации. Требования к средствам высоконадежной биометрической аутентификации»;
- ГОСТ Р 52633.1-2009 «Защита информации. Техника защиты информации. Требования к формированию баз естественных биометрических образов, предназначенных для тестирования средств высоконадежной биометрической аутентификации»;
- ГОСТ Р 52633.2-2010 «Защита информации. Техника защиты информации. Требования к формированию синтетических биометрических образов, предназначенных для тестирования средств высоконадежной биометрической аутентификации»;
- ГОСТ Р 52633.3-2011 «Защита информации. Техника защиты информации. Тестирование стойкости средств высоконадежной биометрической защиты к атакам подбора».

Набор требований к составу мер безопасности и основным механизмам защиты информации определяется на основе модели угроз и модели нарушителя, разрабатываемых в рамках данной работы. Меры безопасности и механизмы защиты информации должны быть реализованы в рамках инфраструктуры развертывания системы либо встроенными функциями прикладного программного обеспечения.

Разработка мероприятий и технических решений по обеспечению информационной безопасности должны проводиться по требованиям Частного Технического задания на подсистему информационной безопасности и составлять неотъемлемую часть работ по созданию Системы НБП.

Необходимо провести подготовку документации к аттестации Системы НБП, включая следующие работы:

- разработка частного технического задания на создание ПОИБ;
- разработка пояснительной записки на создание ПОИБ;
- описание технологического процесса обработки информации;
- разработка инструкции администратора системы защиты конфиденциальной информации в автоматизированной системе;
- разработка проекта акта определения уровня защищенности ПДн;
- разработка проекта приказа об организации работ по обработке конфиденциальной информации;
- разработка проекта детализированной модели угроз;
- разработка проекта дифференцированной модели возможностей вероятного нарушителя.

4.1.6 Требования к эксплуатации и техническому обслуживанию

Периодическое техническое обслуживание используемых технических средств должно проводиться в соответствии с требованиями технической документации изготовителей, но не реже одного раза в год.

Периодическое техническое обслуживание и тестирование технических средств должны включать в себя обслуживание и тестирование всех используемых средств, включая рабочие станции, серверы, кабельные системы и сетевое оборудование, устройства бесперебойного питания.

На основании результатов тестирования технических средств должны проводиться анализ причин возникновения обнаруженных дефектов и приниматься меры по их ликвидации.

Восстановление работоспособности технических средств должно проводиться в соответствии с инструкциями разработчика и поставщика технических средств, а также

документами по восстановлению работоспособности технических средств, и завершаться проведением их тестирования.

Срок гарантийного обслуживания, включающий исправление возникающих ошибок, должен составлять не менее одного года с момента ввода Системы в эксплуатацию.

4.1.7 Требования по сохранности информации при авариях

В Системе должна быть обеспечена сохранность пользовательских данных:

- при авариях и сбоях в системе электропитания, отказах в работе серверного и сетевого оборудования;
- при пожарах, затоплениях, землетрясениях и других стихийных бедствиях: организационными и защитными мерами, опирающимися на подготовленность помещений и персонала, обеспечивающими сохранность хранимых копий информации на магнитных носителях;
- при разрушениях данных при механических и электронных сбоях и отказах в работе компьютеров: на основе программных процедур восстановления информации с использованием хранимых копий баз данных, программных файлов Системы, а также загружаемых файлов;
- при сбое в электропитании: организационными и защитными мерами, опирающимися на подготовленность резервного питания для поддержания нормального функционирования системы в течение времени, необходимого для устранения сбоя в электропитании или для корректного завершения работы Системы;
- при сбое из-за ошибок в работе персонала: организационными и защитными мерами, опирающимися на подготовленность персонала.

Для обеспечения сохранности информации в Системе должны быть включены следующие функции:

- резервное копирование операционных систем, баз данных, программных и загружаемых файлов;
- восстановление данных в непротиворечивое состояние при программно-аппаратных сбоях (отключение электрического питания, сбоях

операционной системы и других) вычислительно-операционной среды функционирования;

- восстановление данных в непротиворечивое состояние при сбоях в работе сетевого программного и аппаратного обеспечения.

4.2 Требования к функциям (задачам), выполняемым системой

4.2.1 Требования к подсистеме внешней интеграции

На стадии технического проектирования необходимо разработать программный модуль (далее – Модуль) для обеспечения возможности интеграции в ИС КО. Модуль должен обеспечивать проверку качества снимаемых биометрических образцов в процессе биометрической регистрации. Модуль должен передаваться в виде исходного кода.

Необходимо произвести разработку универсального механизма подключения Системы к СМЭВ в соответствии с действующими методическими рекомендациями по подключению ИС к СМЭВ.

Необходимо произвести разработку универсального механизма подключения Системы к ЕСИА в соответствии с действующими методическими рекомендациями по подключению ИС к ЕСИА.

Необходимо разработать универсальный механизм (API- внешней интеграции) для обеспечения возможности подключения ИС КО к НБП.

Детальные требования к подсистеме должны быть определены на этапе разработки технического проекта.

4.2.2 Требования к подсистеме балансировки и обработки запросов

Подсистема балансировки и обработки запросов должна обеспечить реализацию следующих функций:

- обработка входящих запросов для передачи в биометрические процессоры;
- балансировка нагрузки на подключенные биометрические процессоры в соответствии с типом биометрической информации и количества загруженных биометрических объектов.

Детальные требования к подсистеме должны быть определены на этапе разработки технического проекта.

4.2.2.1 Требования к процессу биометрической регистрации

В процессе создания биометрических шаблонов должна быть предусмотрена возможность создания отдельных шаблонов на каждую модальность.

Деактивация биометрического контрольного шаблона должна производиться с использованием интерфейса подсистемы администрирования и управления доступом.

Процесс деактивации биометрического контрольного шаблона, а также схема данного бизнес-процесса должны быть согласованы с Заказчиком на стадии технического проекта.

На стадии технического проекта необходимо разработать функционал автоматического контроля времени жизни биометрического контрольного шаблона.

Функционал автоматического контроля времени жизни биометрического контрольного шаблона, должен иметь возможность настройки с использованием интерфейса Подсистемы администрирования и управления доступом.

Детальные требования к процессу биометрической регистрации должны быть определены на этапе разработки технического проекта.

4.2.2.2 Требования к процессу биометрической верификации

Точность биометрической верификации при выполнении сравнения «1 к 1» должна соответствовать требованию: ошибка пропуска «чужого» должна быть менее 0,1% (вероятность ложного совпадения) при ошибке отказа в приеме «своего» не более 3% (вероятность ложного несовпадения).

Должна формироваться и передаваться в ИС КО на основании проведенной верификации следующая информация:

- результат операции аутентификации физического лица;
- степень схожести по каждой биометрической модальности;
- суммарную степень схожести.

Детальные требования к процессу биометрической верификации должны быть определены на этапе разработки технического проекта.

4.2.2.3 Требование к процессу адаптации биометрического контрольного шаблона

Адаптация биометрического контрольного шаблона должна происходить при каждой удачной биометрической верификации с высокой степенью схожести с биометрическим контрольным шаблоном (значение будет установлена на этапе технического проектирования).

При адаптациии биометрического контрольного шаблона должно происходить объединение полученных биометрических образцов и признаков с сохраненными данными и обновлении биометрических шаблонов, находящихся в хранилище биометрических данных.

Если у пользователя по тем и или иным причинам возникают проблемы с биометрической верификацией, он должен иметь возможность обновить свои биометрические данные в Системе, обратившись в установленную Банком России КО.

Детальные требования к процессу адаптации биометрического контрольного шаблона должны быть определены на этапе разработки технического проекта.

4.2.3 Требования к подсистеме интеграционная шина

Интеграционная шина данных должна обеспечить реализацию следующих требований:

- возможность организации асинхронной передачи потоков сообщений между Подсистемами;
- возможность подписки на получение сообщений;
- возможность гарантированной доставки сообщений от отправителя получателю;
- унификация правил взаимодействия Подсистем, гибкая реализация логики взаимодействия.

Детальные требования к подсистеме должны быть определены на этапе разработки технического проекта.

4.2.4 Требования к подсистеме управления конфигурацией

Настройки компонентов Системы должны храниться в конфигурационных файлах подсистемы управления конфигурацией.

На этапе технического проектирования необходимо разработать описание схем конфигурации каждой компоненты Системы.

Детальные требования к подсистеме должны быть определены на этапе разработки технического проекта.

4.2.5 Требования к подсистеме администрирования и управления доступом

Подсистема должна предоставлять следующие интерфейсы:

- Режим администрирования;
- Режим оператора.

Основным ресурсом подсистемы администрирования и управления доступом является ролевая модель.

Подсистема должна обеспечивать возможность на основании ролевой модели предоставлять доступ к режимам администрирования.

Ролевая модель должна быть разработана на стадии технического проектирования.

Подсистема должна осуществлять регистрацию событий авторизации пользователей и фиксировать события в подсистеме журналирования и аудита.

Подсистема должна регистрировать и журналировать безусловно все действия совершенные в режимах администрирования и оператора.

Регистрация событий должна позволять установить пользователя, осуществившего операцию, дату операции и тип операции.

Требования к подсистеме в плане идентификации и аутентификации должны быть разработаны на стадии технического проектирования и уточнены на стадии технического проектирования ПОИБ с учетом следующих требований:

- невозможность администрирования для непривилегированного пользователя;
- возможность разграничения доступа по группам пользователей, местоположению, времени;
- необходимость аутентификации перед сменой пароля;
- отслеживание неудачных попыток входа в систему, задержка после ввода неверного пароля перед следующей попыткой, оперативное оповещение

администратора безопасности при нескольких последовательных неудачных попытках входа в систему;

- системная защита данных, использующихся для аутентификации, и регистрационных данных пользователей;
- проверка требований к паролям (по длине, допустимым символам и т.п.); ограничение на доступ к системной базе паролей и на отображение паролей на экране;
- защита данных, используемых при аутентификации, хранение паролей только в зашифрованном виде;
- обязательная периодическая смена паролей, новые пароли обязательно должны отличаться от старых;
- обязательная аутентификация пользователей при доступе к базе данных; смена стандартных паролей, используемых при установке;
- выдача при входе пользователя в Систему времени последнего входа/выхода, использовавшихся сервисах, числе неудачных попыток входа с данным именем после последнего сеанса;
- настройка параметров времени ожидания (ограничение бездействующего сеанса) и повторной аутентификации пользователя после истечения этого времени.

Необходимо реализовать возможность ведения реестра ИС КО, который будет содержать информацию о подключенных ИС КО. Должен быть разработан механизм и веб-интерфейс для регистрации ИС КО в подсистеме. Должна быть разработана возможность приостановки доступа для ИС КО к НБП.

Необходимо реализовать возможность поиска и деактивации биометрических контрольных шаблонов с использованием административного интерфейса подсистемы.

Необходимо разработать возможность управления следующими параметрами:

- минимальный порог схожести для положительной верификации по каждой модальности;
- минимальный порог схожести для автоматической адаптации по каждой модальности.

– лимит неудачных попыток верификации.

Детальные требования к административному интерфейсу будут уточнены на этапе разработки ЧТЗ.

Детальные требования к подсистеме должны быть определены на этапе разработки технического проекта.

4.2.6 Требования к подсистеме хранения данных

Хранилище биометрических данных должно представлять собой набор БД.

В хранилище биометрических данных должны размещаться биометрические контрольные шаблоны пользователей с привязкой к ID этих пользователей в ЕСИА, включающие в себя следующие данные:

1. Дата, время и место проведения биометрической регистрации;
2. Идентификаторы КО, проводившей биометрическую регистрацию (включая КЭП КО и идентификаторы сотрудника или представителя КО);
3. Дату и время последней адаптации биометрического контрольного шаблона физического лица, включая идентификаторы КО и иные транзакционные параметры, необходимые для совершенствования мер контроля режима ПОД/ФТ;
4. Биометрические образцы (в т.ч. предыдущие версии), в составе:
   – биометрических образцов, прошедших проверку качества (полученные данные должны быть связаны с соответствующими идентификаторами дескрипторов и ID пользователя);
   – биометрических образцов, не прошедших проверку качества (такие данные должны храниться в целях анализа и отладки, однако иметь определённые ограничения на время хранения, чтобы избежать роста хранилища).
5. ID учетной записи пользователя в ЕСИА.

Объем хранилища биометрических данных должен вычисляться исходя из объема биометрического контрольного шаблона на одного пользователя.

Детальные требования к подсистеме должны быть определены на этапе разработки технического проекта.

4.2.7 Требования к подсистеме журналирования и аудита

В целях мониторинга и осуществления аудита подсистема должна обеспечить журналирование всех событий, связанных с работой Системы.

Подсистема журналирования и аудита должна обеспечить реализацию следующих функций:

- фиксация изменений объектов инфраструктуры Системы, журналирование всех интеграционных процессов;
- аудит административных действий, выполняемых в модуле администрирования и управления доступом.

При просмотре зарегистрированных событий должна быть реализована возможность их фильтрации.

Подсистема журналирования и аудита должна иметь возможность, используя внешний почтовый шлюз, направлять администратору Системы по электронной почте уведомления о критических событиях аудита, в том числе n-попыток ошибочной авторизации в подсистеме администрирования и управления правами и других критических событиях.

Подсистема должна позволять настраивать по каким событиям аудита направлять уведомления по электронной почте.

Подсистема должна представлять собой адаптер (протокол) для взаимодействия, в том числе и в автоматическом режиме, с Email и SMS-шлюзами, предоставленными Заказчиком.

Подсистема должна быть реализована с учетом следующих требований:

- необходимо обеспечивать ведение протоколирования (логирование) при обращении и доступу к данным Подсистемы хранения данных;
- необходимо обеспечить возможность настройки событий, которые записываются в журнал событий;
- необходимо обеспечить возможность выбора применения настроек как для отдельных пользователей, так и для групп пользователей и отдельных объектом СУБД;

- необходимо вести протоколирование и журналирование действий всех пользователей Системы;
- средства протоколирования/аудита должны иметь возможность отслеживать события следующих классов:
  - использование механизмов идентификации и аутентификации;
  - создание, модификация, удаление объектов;
  - действия пользователей;
  - передача данных во внешние ИС;
  - сеансов работы пользователей Системы;
  - изменение прав доступа пользователям, группам пользователей в соответствии с ролевой моделью, которая будет разработана на стадии технического проекта;
  - активация и деактивация ИС КО;
  - деактивация биометрических данных.

Детальные требования к подсистеме должны быть определены на этапе разработки технического проекта.

4.2.8 Требования к подсистеме отчетности

Подсистема должна предоставлять возможность формирования отчётов на основании информации о событиях, получаемых от Подсистемы хранения данных и Подсистемы журналирования и аудита.

Отчёты, сформированные модулем, должны иметь возможность сохранения в форматах PDF/XLS и представлять собой документ, состав и представление данных в котором настраиваются пользователем в соответствии с имеющимися шаблонами.

На этапе технического проектирования должны быть разработаны и согласованы с Заказчиком не более 5 (пяти) типовых форм отчетов.

Детальные требования к подсистеме должны быть определены на этапе разработки технического проекта.

4.2.9 Требование к подсистеме детектирования подделок

Подсистема должна обеспечивать защиту от предъявления при верификации не подлинных (фальсифицированных) биометрических образцов для считывания системой.

Подсистема должна принимать только динамические биометрические данные, снятые с человека непосредственно в момент верификации.

Необходимо реализовать обеспечение защиты от подбора не подлинных биометрических образцов в объеме не менее 10^4 попыток на каждый образец.

Подсистема должна иметь возможность получения дополнительных данных о месте проведения удаленной верификации (геоданные).

Детальные требования к подсистеме должны быть определены на этапе разработки технического проекта.

4.2.10 Требования к подсистеме мониторинга

Подсистема должна предоставлять возможность интеграции с программными комплексами мониторинга ИЭП.

Объектами мониторинга должны являться:

- управляющие программные компоненты, обеспечивающие корректное бесперебойное функционирование НБП;
- программные компоненты обработки биометрических запросов;
- хранилище биометрических данных;
- интеграционная шина данных, используемая для взаимодействия компонентов системы;
- программные интерфейсы интеграции и взаимодействия с ИЭП.

Модуль мониторинга состояния компонентов Системы должен обеспечить реализацию следующих функций:

- сбор, регистрацию и анализ контролируемых параметров;
- хранение информации о событии до 6 месяцев;
- контроль состояния оборудования, общего и специального ПО на серверах, виртуальных машинах Системы;

- мониторинг работы подключённых биометрических процессоров в части их работоспособности и загрузки;
- сбор метрик доступности, производительности и утилизации основных компонентов для объектов мониторинга;
- контроль работоспособности составных блоков технического обеспечения;
- возможность удалённого опроса объектов, возможность использования агентов;
- возможность выбора метрик мониторинга и установки пороговых значений;
- возможность реализации заранее не заложенных в систему метрик мониторинга при помощи скриптов;
- возможность фильтрации событий мониторинга пользователем по статусу, критичности и дате создания;
- возможность настройки уведомлений о событиях.

Пороги контролируемых параметров должны быть определены на этапе технического проектирования, исходя из рекомендаций производителя соответствующего оборудования и ПО, а также опыта эксплуатации. Контролируемые параметры должны обеспечивать объем и глубину мониторинга (доступность, производительность, утилизация), достаточную для исполнения обязательств по задачам сопровождения информационных систем в контуре мониторинга и соответствовать требованиям данного документа. Пороги контролируемых параметров должны быть объединены в модели здоровья (МЗ) и согласованы с заказчиком.

Взаимодействие с внешними системами отправки уведомлений на электронный почтовый ящик и текстовых сообщений на мобильный телефон осуществляется с использованием унифицированных программных интерфейсов в автоматическом режиме. Данные внешних систем отправки уведомлений предоставляются Заказчиком.

Детальные требования к подсистеме должны быть определены на этапе разработки технического проекта.

4.2.11 Требования к подсистеме тарификации

С использованием подсистемы тарификации должны быть обеспечены следующие функции:

- учет договорных отношений со всеми КО, включая даты заключения и даты завершения договора, схемы взаиморасчетов (авансовая/кредитная), тарифы;
- обеспечение возможности учитывать остаток средств КО при авансовой схеме расчетов, а также предоставлять возможность его корректировки;
- оповещение служб Заказчика и КО о потенциальной блокировке (по финансовым причинам или сроку завершения договора), а также возможность осуществлять временную блокировку КО при наступлении соответствующих событий;
- учет лицензионных отношений с каждым вендором используемых биометрических технологий, включая дату завершения лицензий и/или количество разрешенных лицензией транзакций за период;
- оповещение служб Заказчика о потенциальной блокировке лицензий, а также возможность осуществлять их временную блокировку при наступлении соответствующих событий;
- учет уведомлений, отправляемых Системой, в разрезе каналов отправки (почта, СМС и т.п.);
- обеспечение передачи информации в бухгалтерские системы заказчика с помощью выгрузки данных в формате, который должен быть установлен в ЧТЗ.

Детальные требования к подсистеме должны быть определены на этапе разработки технического проекта.

4.2.12 Требования к инфраструктуре Системы

Для размещения КТС Системы на этапе ТП должны быть разработаны и согласованы с Заказчиком следующие документы:

- план размещения комплекса технических средств;
- схему взаимодействия компонентов системы, в том числе и сетевое взаимодействие включая номера портов;
- описание возможности масштабирования/кластеризации компонентов системы в виде таблицы с составом полей:
  - компонент, ПО;

- кластер да/нет;
- комментарий.

- описание требования к размещению (сервера или виртуальные машины);
- схему интеграции с другими системами, которая должна включать в себя подробное описание с какими системами и каким образом осуществляется интеграция.

Ресурсы, используемые в плане, должны соответствовать требованиям обеспечения отказоустойчивости, масштабируемости и обеспечивать производительность серверного оборудования. Минимальные системные требования для программно-аппаратного комплекса (далее – ПАК), должны быть определены на этапе технического проектирования, и добавлены в Пояснительную записку ТП в виде таблицы минимальных системных требований к ПАК

4.3 Требования к видам обеспечения

4.3.1 Требования к техническому обеспечению

Техническое обеспечение Системы (на всех этапах реализации) осуществляется Заказчиком путём предоставления оборудования в соответствии с разработанными и утверждёнными спецификациями.

Техническое обеспечение Системы должно удовлетворять следующим базовым требованиям:

- обеспечивать работу с заданным количеством пользователей;
- обеспечить возможность наращивания вычислительных мощностей Системы путём масштабирования вычислительных мощностей, увеличением числа процессоров, оперативной памяти, дисковых подсистем;
- обеспечивать восстановление данных без потери информации;
- обеспечивать выполнение требований по надёжности Системы в целом.

4.3.2 Требования к программному обеспечению Системы

В состав программного обеспечения Системы должно входить программное обеспечение следующих видов:

- общее программное обеспечение (ОПО);

- специальное программное обеспечение (СПО).

В рамках создания Системы должно использоваться следующее общее программное обеспечение:

- система управления базами данных, обеспечивающая взаимодействие с сервером приложений;
- программный веб-сервер, обеспечивающий представление веб-интерфейса в браузере пользователя Системы;
- многозадачные многопользовательские операционные системы 32- битной или 64-битной архитектуры, обеспечивающие сетевое взаимодействие с использованием стека протоколов TCP/IP (для серверов);
- многозадачные операционные системы 32-битной или 64-битной архитектуры, обеспечивающие сетевое взаимодействие с использованием стека протоколов TCP/IP (для рабочих станций);
- по согласованию с Заказчиком на этапе технического проектирования – программное обеспечение виртуализации со встроенными возможностями восстановления работоспособности виртуальных машин и систем хранения данных.

Общее программное обеспечение для Системы предоставляется Заказчиком.

Графический интерфейс Системы должен быть реализован как веб-приложение, используемое с помощью веб-браузеров Google Chrome, Mozilla Firefox, Opera, Apple Safari, Internet Explorer.

При условии соответствия функциональным и техническим требованиям по согласованию с Заказчиком может использоваться программное обеспечение с открытым программным кодом.

Система должна предусматривать возможность установки на ОС с открытым исходным кодом.

Требования к клиентским устройствам для проведения бимодальной верификации:

- Мобильные устройства:
  - iOS 8 и выше, Android 4.4 и выше;
  - камера, поддерживающая съемку в разрешении не ниже 640x480.

- Настольные устройства (ПК):
  - интернет-браузеры Internet Explorer, Chrome, Firefox, Opera, Safari, Edge;
  - камера, поддерживающая съемку в разрешении не ниже 640x480;
  - направленный микрофон, не зависимый от встроенного в камеру или ПК.

Детальные требования к версионности используемых веб-браузеров и ОС должны быть определены на этапе разработки технического проекта.

4.3.2.1 Требования к порядку предъявления исходного кода

Программное обеспечение Системы должно быть передано в виде исходных кодов СПО, поделенных на компоненты/каталоги/проекты в соответствии с тем, как они будут собираться (без конфигурационных файлов и файлов БД).

Важно: при сборке не должно быть никаких ссылок и обращений к сторонним ресурсам, сборка должна происходить локально. Недопустима передача исходных кодов в незафиксированном состоянии, то есть версия не должна находиться в состоянии разработки (не должен использоваться мгновенный снимок).

4.3.2.2 Требования к дистрибутиву

Дистрибутив СПО должен содержать следующий набор артефактов:

- Исходный код СПО.
- Конфигурационные файлы, включая изменяемые файлы СПО.
- Схема БД с описанием пошаговых действий по его восстановлению в СУБД (если требуется).
- Сторонние библиотеки, используемые при сборке программного обеспечения из исходных кодов с указанием ссылок на открытые источники для загрузки библиотек и их исходных кодов.
- Исходные коды сторонних библиотек, если нет возможности их скачать через открытые источники.

4.3.3 Требования к информационному обеспечению системы

Состав, структура и способы организации данных в Системе должны быть определены на этапе проектирования.

Для обеспечения целостности данных должны использоваться встроенные механизмы СУБД.

Система должна обеспечивать возможность работы в отказоустойчивом режиме, а также обеспечивать возможность резервного копирования данных и их восстановления.

Информационное обеспечение Системы должно обеспечивать информационную совместимость с ИЭП по содержанию (единство понятий, терминов, определений), по системам классификации и кодирования, по форматам данных, по способам и формам представления данных общего пользования, по методам агрегирования (организации) информации.

Структура базы данных должна быть организована рациональным способом, исключающим единовременную полную выгрузку информации, содержащейся в базе данных Системы.

4.3.4 Требования к лингвистическому обеспечению системы

Лингвистическое обеспечение Системы должно содержать совокупность средств и правил для формализации естественного языка, используемых при общении пользователей Системы с программно-техническими комплексами при функционировании системы.

В случаях обоснованной необходимости применения и использования языков программирования для создания Системы и её компонентов должны применяться языки программирования высокого уровня, имеющие промышленные масштабы развития и сопровождения.

Для описания протоколов, параметров и внешних интерфейсов SOAP сервисов должны применяться XML и WSDL. Для описания сообщений (команд) должен использоваться XML.

В системных диалогах с пользователями в текстах сообщений должен применяться русский язык за возможным исключением для системных сообщений, которые могут не подлежать переводу на русский язык.

5 Состав и содержание работ по созданию системы

Этапы проведения работ по созданию системы НБП приведены в таблице 4.

Таблица 4 Календарный план на выполнение работ по разработке системы «Национальная биометрическая платформа»

Этап	Состав работ	Наименование документа	Разработан согласно	Сроки выполнения
1.	**Создание Системы**	Частное техническое задание на реализацию Национальной биометрической платформы	ГОСТ 34.602-89	60 календарных дней с даты подписания Договора, но не позднее 01.12.2017
1.1	Разработка Технического проекта	Ведомость технического проекта	РД 50-34.698-90	01.12.2017
		Пояснительная записка к техническому проекту	РД 50-34.698-90	
		Паспорт информационной системы	РД 50-34.698-90	

Этап	Состав работ	Наименование документа	Разработан согласно	Сроки выполнения
1.2	Разработка Опытного образца Системы	Дистрибутив и исходные коды программного обеспечения Опытного образца Системы на оптическом носителе		01.12.2017
1.3	Разработка Программы и методики испытаний	Программа и методика испытаний Национальной биометрической платформы	РД 50-34.698-90	01.12.2017
1.4	Разработка рабочей документации	Ведомость эксплуатационных документов	РД 50-34.698-90	01.12.2017
		Руководство администратора НБП	РД 50-34.698-90	
		Руководство пользователя НБП	РД 50-34.698-90	
15	Проведение	Протокол предварительных испытаний Опытного образца	РД 50-34.698-90	01.12.2017

Этап	Состав работ	Наименование документа	Разработан согласно	Сроки выполнения
	предварительных испытаний	Протокол согласования замечаний (составляется, если в ходе испытаний были выявлены замечания)	РД 50-34.698-90	
		Акт сдачи-приемки этапа работ	РД 50-34.698-90	
2	**Опытная эксплуатация**			22.12.2017
2.1	Проведение опытной эксплуатации	Проведение опытной эксплуатации		22.12.2017
2.2	Доработка рабочей документации	Эксплуатационная документация, разработанная в соответствии с РД 50-34.698-90, в составе доработанной по результатам опытной эксплуатации эксплуатационной документации Этапа 2.		22.12.2017
2.3	Доработка программ и методик	Программы и методики испытаний, разработанные в соответствии с РД 50-34.698-90, в составе доработанных по результатам опытной эксплуатации программ и методик испытаний Этапа 2.		22.12.2017

Этап	Состав работ	Наименование документа	Разработан согласно	Сроки выполнения
	испытаний			
2.4	Предоставление прикладного программного обеспечения	Дистрибутив и исходные коды прикладного программного обеспечения, предоставляемые на CD или DVD в составе:		22.12.2017
		Исполняемые коды (дистрибутивы)		
		Исходные тексты		
2.5	Документация для аттестации информационной системы	Проект документации для аттестации информационной системы по требованиям Приказа №21 ФСТЭК от 18 февраля 2013г.		22.12.2017
2.6	Разработка Технического	Акт определения уровня и класса защищенности Системы, проект	-	22.12.2017
		Частное техническое задание на создание ПОИБ	-	

Этап	Состав работ	Наименование документа	Разработан согласно	Сроки выполнения
	проекта ПОИБ	Пояснительная записка технического проекта на создание ПОИБ	-	
		Описание технологического процесса обработки информации	-	
		Детализированная модель угроз, проект	-	
		Дифференцированная модель возможностей вероятного нарушителя, проект	-	
		Приказ об организации работ по обработке конфиденциальной информации, проект	-	
		Инструкция администратора системы защиты конфиденциальной информации в автоматизированной системе	-	
2.7	Приемочные испытания	Программа опытной эксплуатации	ГОСТ 34.603-92	22.12.2017

Этап	Состав работ	Наименование документа	Разработан согласно	Сроки выполнения
		Журнал опытной эксплуатации	ГОСТ 34.603-92	
		Протокол приёмочных испытаний	РД 50-34.698-90	
		Протокол согласования замечаний (составляется, если в ходе испытаний были выявлены замечания)	РД 50-34.698-90	
		Акт сдачи-приемки этапа работ	РД 50-34.698-90	

6 Порядок контроля и приемки системы

6.1 Виды, состав, объем и методы испытаний системы

Испытания должны быть организованы и проведены в соответствии с требованиями ГОСТ 34.603 «Информационная технология. Виды испытаний автоматизированных систем».

Должны быть проведены следующие виды испытаний:

- предварительные испытания;
- опытная эксплуатация;
- приемочные испытания.

Отдельные виды испытаний проводятся поэтапно в сроки, установленные календарным планом выполнения работ по договору.

Объем и методы предварительных и приемочных испытаний определяются документом «Программа и методика испытаний», разрабатываемым Исполнителем по согласованию с Заказчиком.

«Программа и методика испытаний» для проведения приемочных испытаний дорабатывается с учетом результатов опытной эксплуатации, при этом проверки системы НБП в части не устраненных высококритичных дефектов реализации НБП, выявленных в процессе опытной эксплуатации, выносятся в специальный раздел.

Испытания должны проводиться комиссией, состоящей из уполномоченных представителей Заказчика, при участии представителей Исполнителя.

Испытания должны проводиться на технологической площадке, предоставленной Заказчиком.

6.2 Общие требования к приемке работ по стадиям

Приемка результатов работ осуществляется поэтапно, в соответствии с Календарным планом выполнения работ по Договору.

Испытания системы НБП должны проводиться в соответствии с требованиями ГОСТ 34.603-92 и на основании документа «Программа и методика испытаний», разработанного с учетом требований РД 50-34.698-90.

В процессе приемки работ должна быть осуществлена проверка системы на соответствие требованиям Частного технического задания на систему НБП.

Результаты проведения испытаний должны быть зафиксированы в соответствующих Протоколах испытаний. К недостаткам реализации могут быть отнесены исключительно выявленные отклонения от требований Частного технического задания на систему НБП.

Прочие требования и дефекты системы НБП, выявленные на испытаниях и не относящиеся к требованиям, приведенным в Техническом задании и Частном техническом задании на систему НБП, могут документироваться как желательные доработки. Наличие желательных доработок не влияет на приемку работ и процесс передачи системы НБП в эксплуатацию.

По завершении предварительных и приемочных испытаний оформляются соответствующие Протоколы испытаний, содержащие вывод о соответствии системы НБП предъявляемым требованиям, а также критичность и сроки устранения дефектов, выявленных комиссией в ходе испытаний.

Результаты опытной эксплуатации отражаются в документе «Журнал опытной эксплуатации» и рассматриваются в ходе приемочных испытаний.

Приемка результатов выполнения работ по каждому этапу проводятся следующие виды испытаний:

- предварительные испытания и ввод в опытную эксплуатацию;
- опытная эксплуатация;
- приемочные испытания.

Результаты предварительных испытаний системы НБП на втором этапе работ оформляются документом «Акт ввода системы НБП в опытную эксплуатацию» с приложением к нему прокола предварительных испытаний.

Результаты опытной эксплуатации системы НБП на третьем этапе работ оформляются документом «Акт о проведении опытной эксплуатации системы НБП».

Вывод Системы в эксплуатацию производится по окончании опытной эксплуатации Системы, по согласованию с Министерством связи и массовых коммуникаций Российской Федерации и Центральным Банком Российской Федерации.

Все создаваемые в рамках настоящих работ программные продукты (за исключением покупных) передаются Заказчику, как в виде готовых модулей, так и в виде исходных кодов, представляемых в электронной форме на стандартном машинном носителе (например, на компакт-диске).

Допускается проведение предварительных испытаний на специальных испытательных стендах. В ходе предварительных испытаний определяется готовность системы к запуску в опытную эксплуатацию.

6.3 Статус приемочной комиссии

Состав приемочной комиссии определяется Заказчиком до проведения испытаний. От каждой Стороны для участия в испытаниях должен быть выделен как минимум один представитель.

7 Требования к составу и содержанию работ по подготовке объекта автоматизации к вводу системы в действие

В ходе выполнения проекта на объекте автоматизации требуется выполнить работы по подготовке к вводу системы в действие. При подготовке к вводу в эксплуатацию системы НБП Заказчик должен обеспечить выполнение следующих работ:

- Определить подразделение и ответственных должностных лиц, ответственных за внедрение и проведение опытной эксплуатации НБП;
- Обеспечить присутствие пользователей на обучении работе с системой, проводимом Исполнителем;
- Обеспечить соответствие помещений и рабочих мест пользователей системы в соответствии с требованиями, изложенными в настоящем ТЗ;
- Обеспечить выполнение требований, предъявляемых к программно-техническим средствам, на которых должно быть развернуто программное обеспечение НБП;
- Совместно с Исполнителем подготовить план развертывания системы на технических средствах Заказчика;
- Провести опытную эксплуатацию НБП.

Требования к составу и содержанию работ по подготовке объекта автоматизации к вводу системы в действие, включая перечень основных мероприятий и их исполнителей должны быть уточнены на стадии подготовки рабочей документации и по результатам опытной эксплуатации.

8 Требования к документированию

В рамках проведения работ должна быть разработана следующая документация:

- частное техническое задание;
- комплект документации технического проекта;
- комплект рабочей документации.

Комплект документации технического проекта должен включать в себя следующие документы:

- ведомость технического проекта;
- пояснительная записка к техническому проекту;

Комплект рабочей документации должен включать в себя следующие документы:

- ведомость эксплуатационных документов;
- руководство пользователя;
- руководство системного администратора, содержащее как минимум следующую информацию:
  - схема развёртывания программного обеспечения;
  - описание процедуры развёртывания и настройки Системы;
  - порядок запуска, остановки и перезапуска компонентов Системы;
  - описание способов проверки доступности и работоспособности компонентов Системы;
- паспорт;
- программа и методика испытаний.

Отчётная документация должна передаваться Заказчику в бумажном и электронном виде (на оптическом CD или DVD носителе) на русском языке. Вспомогательная документация (не указанная в качестве непосредственного результата работ) передаётся только в электронном виде.

Техническая и эксплуатационная документация на Систему (далее - документы на Систему) должна быть разработана в составе, указанном в разделе 5, и должна удовлетворять требованиям комплекса стандартов и руководящих документов на автоматизированные системы:

- ГОСТ 34.003-90 - в части терминологии;
- ГОСТ 34.201-89 - в части наименования и обозначения документов;
- ГОСТ 34.602-89 - в части состава, содержания и правил оформления документов «Техническое задание», «Частное техническое задание»;
- РД 50-34.698-90 - в части структуры и содержания документов.

Документам на Систему должны в обязательном порядке присваиваться уникальные децимальные номера в соответствии с порядком, установленном в ГОСТ 34.201-89.

Для разрабатываемой Системы должны быть представлены в электронном виде (на оптическом CD или DVD носителе):

- исходные тексты прикладного программного обеспечения, включая контрольные суммы для каждого файла по алгоритму MD5;
- инструкция по сборке из исходных текстов рабочего прикладного программного обеспечения;
- исполняемые файлы (где применимо), включая контрольные суммы для каждого файла по алгоритму MD5.

Комплект документации на подсистему обеспечения информационной безопасности (ПОИБ) Системы должен включать в себя следующие документы:

- частное техническое задание на создание ПОИБ;
- пояснительная записка на создание ПОИБ;
- описание технологического процесса обработки информации;
- инструкция администратора системы защиты конфиденциальной информации в автоматизированной системе;
- проект акта определения уровня и класса защищенности Системы;
- проект приказа об организации работ по обработке конфиденциальной информации;
- проект детализированной модель угроз;
- проекта дифференцированной модели возможностей вероятного нарушителя.

9 Требования к предоставлению гарантии качества работ

Исполнитель принимает на себя обязательства по гарантии качества результатов, полученных при выполнении работ. Срок (период) на который предоставляютсяения гарантии качества Работ - 12 (Двенадцать) месяцев с даты приемки результатов работ Заказчиком (дата подписания Заказчиком Акта сдачи-приемки Работ).

Исполнитель несет ответственность за дефекты и недостатки, обнаруженные в период гарантийного срока. В случае выявления дефектов и недостатков в гарантийный период Исполнитель безвозмездно выполняет работы по их устранению, в том числе, в случае если в процессе эксплуатации будет выявлено несоответствие Системы показателям назначения, заявленным в ее Частном техническом задании и/или Техническом проекте. Срок устранения дефектов и недостатков устанавливается по согласованию между Заказчиком и Исполнителем, но не должен превышать одного месяца.