**МИНИСТЕРСТВО НАУКИ
И ВЫСШЕГО ОБРАЗОВАНИЯ
РОССИЙСКОЙ ФЕДЕРАЦИИ**
(МИНОБРНАУКИ РОССИИ)

ЗАМЕСТИТЕЛЬ МИНИСТРА

Тверская ул., д. 11, стр. 1, 4, Москва, 125009
Тел.: (495) 547-13-16
e-mail: info@minobrnauki.gov.ru
http://www.minobrnauki.gov.ru

03.06.2020 № МН-11/424-АН

На № _____ от _____

О проведении отбора

Руководителям подведомственных научных организаций

Уважаемые коллеги!

Национальным проектом «Наука» предусмотрено достижение результата «S1.02.07 Введена в эксплуатацию единая цифровая платформа научного и научно-технического взаимодействия, организации и проведения совместных исследований в удаленном доступе, в том числе с участием зарубежных ученых (далее – ЦПСИ)». В рамках выполнения результата, разработанный проект технического задания на создание ЦПСИ был согласован общественно-деловым и экспертным советом по национальному проекту «Наука», а также Министерством цифрового развития, связи и массовых коммуникаций Российской Федерации.

В соответствии с решением, принятым на заочном заседании президиума Совета Минобрнауки России по цифровому развитию и информационным технологиям (протокол от 1 апреля 2020 года № 1), определение исполнителя на выполнение работ по созданию ЦПСИ будет осуществлено посредством проведения конкурсного отбора.

В случае заинтересованности участия в конкурсном отборе просим в срок до 14 июня 2020 года направить в адрес Минобрнауки России письмо с приложением заявки (предложения), включающей(-его), в том числе:

перечень документов, подтверждающий соответствие организации критериям, указанным в приложении;

финансово-экономическое обоснование стоимости работ;

детализированный план-график выполнения работ по созданию ЦПСИ.

Контактное лицо: Кочемиров Сергей Алексеевич, заместитель начальника отдела Департамента цифрового развития (e-mail: kochemirovsa@minobrnauki.gov.ru, тел.: 8-495-540-12-60 (доб. 2514).

Приложение № 1: критерии отбора на 1 л. в 1 экз.

Приложение № 2: регламент отбора на 2 л. в 1 экз.

Приложение № 3: техническое задание на 86 л. в 1 экз.

А.В Нарукавников

Руслан Вугарович Надтока
8-495-540-12-60 (доб. 2534)

Приложение № 1

Критерии отбора организаций на выполнение работ по созданию единой цифровой платформы научного и научно-технического взаимодействия, организации и проведения совместных исследований в удаленном доступе, в том числе с участием зарубежных ученых

1. Учредителем организации является Минобрнауки России;

2. Основным видом деятельности в соответствии с уставом организации является научная;

3. Уставом организации предусмотрена возможность создания информационных систем;

4. Наличие подтвержденного опыта участия в реализации национальных проектов;

5. Наличие опыта создания информационных систем стоимостью свыше 10 млн.;

6. Балансовая стоимость организации должна в 10 раз превышать стоимость создания платформ;

7. Квалификация кадрового состава организации должна обеспечивать возможность создания платформ.

Приложение № 2

Регламент проведения отбора организаций на выполнение работ по созданию единой цифровой платформы научного и научно-технического взаимодействия, организации и проведения совместных исследований в удаленном доступе, в том числе с участием зарубежных ученых

В целях достижения результата национального проекта «Наука» S1.02.07 «Введена в эксплуатацию единая цифровая платформа научного и научно-технического взаимодействия, организации и проведения совместных исследований в удаленном доступе, в том числе с участием зарубежных ученых (далее – ЦПСИ)» федерального проекта «Развитие научной и научно-производственной кооперации» Минобрнауки России проводит отбор на выполнение работ по созданию ЦПСИ.

Информация об отборе общедоступна и размещена на сайте Министерства науки и высшего образования Российской Федерации в информационно-телекоммуникационной сети «Интернет».

Срок проведения отбора: 4 июня 2020 г. – 22 июня 2020 г.

Участие в конкурсном отборе могут принять организации, учредителем которых является Минобрнауки России.

Отбор состоит из трех этапов:

1. Прием заявок от организаций.

   Срок: 4 июня 2020 г. – 14 июня 2020 г.

2. Оценка заявок на соответствие критериям.

   Срок: 15 июня 2020 г. – 18 июня 2020 г.

3. Презентация заявок на заседании президиума Совета Минобрнауки России по цифровому развитию и информационным технологиям (далее – президиум Совета).

Срок: 22 июня 2020 г.

На первом этапе организациями должны быть направлены официальные письма об участии в конкурсном отборе с приложениями заявки в адрес

Минобрнауки России. При формировании заявки организации должны ориентироваться на технические задания, согласованные общественно-деловым и экспертным советом по национальному проекту «Наука». Техническое задание не позднее 9.00 5 июня 2020 г. будет размещено на сайте Министерства науки и высшего образования Российской Федерации в информационно-телекоммуникационной сети «Интернет».

На втором этапе Минобрнауки России проводится оценка и отбор заявок на соответствие критериям отбора.

На третьем этапе на очередном заседании президиума Совета организации, соответствующие критериям отбора, презентуют заявки.

Протокольным решением президиума Совета будут выбраны организации-победители отбора на выполнение работ по созданию цифровых платформ в рамках национального проекта «Наука».

Приложение № 3

МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ

ЕДИНАЯ ЦИФРОВАЯ ПЛАТФОРМА НАУЧНОГО И НАУЧНО-ТЕХНИЧЕСКОГО ВЗАИМОДЕЙСТВИЯ, ОРГАНИЗАЦИИ И ПРОВЕДЕНИЯ СОВМЕСТНЫХ ИССЛЕДОВАНИЙ В УДАЛЕННОМ ДОСТУПЕ, В ТОМ ЧИСЛЕ С ЗАРУБЕЖНЫМИ УЧЕНЫМИ

ТЕХНИЧЕСКОЕ ЗАДАНИЕ

На 86 листах

2020

СОДЕРЖАНИЕ

Определения, обозначения и сокращения....4
1 Общие сведения....7
1.1 Полное наименование Системы и ее условное обозначение....7
1.2 Шифр темы или договора....7
1.3 Наименования организации Заказчика....7
1.4 Исполнитель работ....7
1.5 Перечень документов, на основании которых создается Система....7
1.6 Плановые сроки начала и окончания работы по созданию Системы....8
1.7 Сведения об источниках и порядке финансирования работ....8
1.8 Порядок оформления и предъявления Заказчику результатов работ по созданию Системы....8
2 Назначение и цели создания Системы....10
2.1 Назначение Системы....10
2.2 Цели создания Системы....11
3 Характеристика объекта автоматизации....12
4 Требования к Системе....14
4.1 Требования к системе в целом....14
4.1.1 Требования к структуре и функционированию Системы....14
4.1.2 Требования к численности и квалификации персонала Системы и режиму его работы....24
4.1.3 Показатели назначения....25
4.1.4 Требования к надежности....27
4.1.5 Требования безопасности....30
4.1.6 Требования к эргономике и технической эстетике....31
4.1.7 Требования к эксплуатации, техническому обслуживанию, ремонту и хранению компонентов Системы....32
4.1.8 Требования к защите информации от несанкционированного доступа....33
4.1.9 Требования по сохранности информации при авариях....42
4.1.10 Требования к защите от влияния внешних воздействий....43
4.1.11 Требования к патентной чистоте....43
4.1.12 Требования по стандартизации и унификации....43
4.2 Требования к функциям (задачам), выполняемым Системой....44
4.2.1 Обеспечивающие подсистемы....44
4.2.2 Интеграционная шина ЦПСИ....51

4.2.3 Подсистема интеграционного взаимодействия 51
4.2.4 Подсистема «Цифровой профиль исследователя» 52
4.2.5 Подсистема «Цифровой профиль организации» 54
4.2.6 Подсистема «Научная тема» 55
4.2.7 Подсистема «Гранты и конкурсы» 56
4.2.8 Открытый портал ЦПСИ 57
4.2.9 Подсистема обеспечения информационной безопасности (ПОИБ) 59
4.3 Требования к видам обеспечения 62
4.3.1 Требования к математическому обеспечению Системы 62
4.3.2 Требования к информационному обеспечению Системы 62
4.3.3 Требования к защите данных от разрушений при авариях и сбоях в электропитании системы 63
4.3.4 Требования к контролю, хранению, обновлению и восстановлению данных 63
4.3.5 Требования к лингвистическому обеспечению Системы 63
4.3.6 Требования к программному обеспечению Системы 64
4.3.7 Требования к техническому обеспечению Системы 65
4.3.8 Требования к метрологическому обеспечению 73
4.3.9 Требования к организационному обеспечению 73
4.3.10 Требования к методическому обеспечению 73
5 Состав и содержание работ по созданию Системы 74
6 Порядок контроля и приемки Системы 79
6.1 Виды, состав, объем и методы испытаний Системы и ее составных частей 80
6.2 Общие требования к приемке работ по стадиям, порядок согласования и утверждения приемочной документации 82
7 Требования к составу и содержанию работ по подготовке объекта автоматизации к вводу системы в действие 83
8 Требования к документированию 84
9 Источники разработки 85

ОПРЕДЕЛЕНИЯ, ОБОЗНАЧЕНИЯ И СОКРАЩЕНИЯ

Таблица 1 – Определения, обозначения и сокращения

Сокращение (обозначение)	Значение сокращения (обозначения)
CD	Оптический носитель информации, процесс записи и считывания информации с которого осуществляется при помощи лазера
DNS	Компьютерная распределённая система для получения информации о доменах
DOI	Уникальный идентификатор, присвоенный научной публикации
DVD	Оптический носитель информации, выполненный в форме диска, для хранения различной информации в цифровом виде
EMAIL	Адрес электронного почтового ящика
FIBRE CHANNEL	Семейство протоколов для высокоскоростной передачи данных
ISO	Международная организация, занимающаяся выпуском стандартов
JSON	Текстовый формат обмена данными, основанный на JavaScript
OLAP	Технология обработки данных, заключающаяся в подготовке суммарной информации на основе больших массивов данных, структурированных по многомерному принципу
PDF	Межплатформенный открытый формат электронных документов, изначально разработанный фирмой Adobe Systems
PDF/A	Стандартизированная по ISO версия PDF, предназначенная для долгосрочного архивного хранения электронных документов
REST	Архитектурный стиль взаимодействия компонентов распределённого приложения в сети
SAS	Последовательный компьютерный интерфейс, разработанный для подключения различных устройств хранения данных
SCOPUS	Библиографическая и реферативная база данных и инструмент для отслеживания цитируемости статей, опубликованных в научных изданиях
SINGLE SIGN-ON	Технология, при использовании которой пользователь переходит из одного раздела портала в другой без повторной аутентификации
SOAP	Протокол обмена структурированными сообщениями в распределённой вычислительной среде
SSD	Компьютерное энергонезависимое немеханическое запоминающее устройство на основе микросхем памяти
TCP	Один из основных протоколов передачи данных интернета, предназначенный для управления передачей данных
WEB OF SCIENCE	Поисковая интернет-платформа, объединяющая реферативные базы данных публикаций в научных журналах и патентов, в том числе базы, учитывающие взаимное цитирование публикаций
WHOIS	Сетевой протокол прикладного уровня, базирующийся на протоколе TCP. Предназначен для получения регистрационных

Сокращение (обозначение)	Значение сокращения (обозначения)
	данных о владельцах доменных имён, IP-адресов и автономных систем
XML	Расширяемый язык разметки
АИСУ ФЦП	Автоматизированная информационная система управления Федеральной целевой программы «Исследования и разработки по приоритетным направлениям развития научно-технологического комплекса России на 2014 — 2020 годы»
АПК	Аппаратно-программный комплекс
АС	Автоматизированная система
БД	База данных
ВАК	Высшая аттестационная комиссия
ГОСТ	Межгосударственный стандарт
Дедупликация	Специализированный метод сжатия массива данных, использующий в качестве алгоритма сжатия исключение дублирующих копий повторяющихся данных
ЕСИА	Единая система идентификации и аутентификации
ИАС РНФ	Информационно-аналитическая система Российского научного фонда
ИС	Информационная система
ИТ	Информационные технологии
ИСПДн	Информационная система персональных данных
ИС ФОИВ	Информационная система Федерального органа исполнительной власти Российской Федерации
КИАС РФФИ	Комплексная информационно-аналитическая система Российского фонда фундаментальных исследований
Минобрнауки России	Министерство науки и высшего образования Российской Федерации
НИР	Научно-исследовательская работа
НСД	Несанкционированный доступ
НОЦ	Научно-образовательный центр
НЦМУ	Научный центр мирового уровня
ОС	Операционная система
ПДн	Персональные данные
ПО	Программное обеспечение
ПОИБ	Подсистема обеспечения информационной безопасности
РАН	Российская академия наук
РИД	Результат интеллектуальной деятельности
РИНЦ	Российский индекс научного цитирования
РСУБД	Реляционная СУБД
РФ	Российская Федерация

Сокращение (обозначение)	Значение сокращения (обозначения)
СПО	Системное программное обеспечение
СрЗИ	Средство защиты информации
СУБД	Система управления базами данных
СХД	Система хранения данных
Таймлайн	Линия времени, где в хронологическом порядке представлены события, достижения или план действий
ТЗ	Техническое задание
ФИО	Фамилия, Имя, Отчество
ФСБ России	Федеральная служба безопасности Российской Федерации
ФСТЭК	Федеральная служба по техническому и экспортному контролю
ЦОД	Центр обработки данных
ЦПСИ, Система	Единая цифровая платформа научного и научно-технического взаимодействия, организации и проведения совместных исследований в удаленном доступе, в том числе с участием зарубежных ученых
ЧТЗ	Частное техническое задание
ЕСНСИ	Федеральная государственная информационная система «Единая система нормативной справочной информации» Минкомсвязи России

1 ОБЩИЕ СВЕДЕНИЯ

1.1 Полное наименование Системы и ее условное обозначение

Полное наименование системы: Единая цифровая платформа научного и научно-технического взаимодействия, организации и проведения совместных исследований в удаленном доступе, в том числе с участием зарубежных ученых.

Краткое наименование системы: ЦПСИ, Система.

1.2 Шифр темы или договора

ЦПСИ

1.3 Наименования организации Заказчика

Заказчик: Министерство науки и высшего образования Российской Федерации.

Юридический адрес: 125009, г Москва, ул. Тверская, 11 / Строение 1, 4.

1.4 Исполнитель работ

Разработчик Системы определяется по результатам конкурсных процедур в соответствии с требованиями федерального закона «О контрактной системе в сфере закупок товаров, работ, услуг для обеспечения государственных и муниципальных нужд» от 05.04.2013 № 44-ФЗ.

1.5 Перечень документов, на основании которых создается Система

Основанием для выполнения работ по созданию Системы являются следующие документы и нормативные акты:

- Указ Президента Российской Федерации от 07.05.2018 № 204 «О национальных целях и стратегических задачах развития Российской Федерации на период до 2024 года»;
- Указ Президента Российской Федерации от 21.01.2020 № 21 «О структуре федеральных органов исполнительной власти»;
- Указ Президента Российской Федерации от 31.12.2015 № 683 «О Стратегии национальной безопасности Российской Федерации»;
- Указ Президента Российской Федерации от 01.12.2016 № 642 «О Стратегии научно-технологического развития Российской Федерации»;

- Распоряжение Правительства Российской Федерации от 27.12.2012 № 2538-р «Об утверждении Программы фундаментальных научных исследований в Российской Федерации на долгосрочный период (2013-2020 годы)»;
- Федеральный закон от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации»;
- Федеральный закон от 23.08.1996 № 127-ФЗ «О науке и государственной научно-технической политике»;
- Постановление Правительства Российской Федерации от 29.03.2019 № 377 «Об утверждении Государственной программы Российской Федерации «Научно-технологическое развитие Российской Федерации»;
- «Паспорт национального проекта «Наука» (утв. президиумом Совета при Президенте Российской Федерации по стратегическому развитию и национальным проектам, протокол от 24.12.2018 № 16);
- «Паспорт национального проекта «Национальная программа «Цифровая экономика Российской Федерации» (утв. президиумом Совета при Президенте Российской Федерации по стратегическому развитию и национальным проектам, протокол от 04.06.2019 № 7).

1.6 Плановые сроки начала и окончания работы по созданию Системы

Сроки начала и окончания этапов работ определены в разделе 5 «Состав и содержание работ по созданию Системы» настоящего Технического задания.

Дата начала работ: с момента заключения Государственного контракта.

1.7 Сведения об источниках и порядке финансирования работ

Источником финансирования работ является федеральный бюджет Российской Федерации.

Порядок финансирования (оплаты выполненных Исполнителем работ) определяется в соответствии с нормативно-правовыми актами Российской Федерации, регулирующими вопросы финансирования расходов федерального бюджета, и Государственным контрактом.

1.8 Порядок оформления и предъявления Заказчику результатов работ по созданию Системы

Порядок оформления и предъявления Заказчику результатов работ по созданию Системы приведен в разделе 7 «Требования к составу и содержанию работ по подготовке объекта автоматизации к вводу системы в действие» настоящего Технического задания.

Результаты работ передаются Заказчику в порядке, определенном в соответствии с разделом 5 «Состав и содержание работ по созданию Системы» настоящего Технического задания в сроки, установленные Государственным контрактом.

Порядок предъявления Системы, ее испытаний и окончательной приемки определен в разделе **Ошибка! Источник ссылки не найден.** «Порядок контроля и приемки Системы» настоящего ТЗ.

2 НАЗНАЧЕНИЕ И ЦЕЛИ СОЗДАНИЯ СИСТЕМЫ

2.1 Назначение Системы

ЦПСИ предназначена для автоматизации процессов по организации взаимодействия исследователей, междисциплинарных научных групп, заказчиков исследований и иных заинтересованных сторон при выполнении научно-исследовательских, опытно-конструкторских и иных работ по созданию научной продукции, а также учета и анализа результатов данных работ.

ЦПСИ предназначена для решения следующих задач:

- обеспечение единой точки авторизации для различных информационных систем научной отрасли;
- накопление, хранение и предоставление информации о результатах научной деятельности в цифровом профиле исследователя;
- предоставление информации о публикациях научных статей, цитируемости в цифровом профиле исследователя;
- обеспечение научного и научно-технического взаимодействия участников исследовательских проектов, проводимых в НОЦ и НЦМУ;
- подбор грантов и конкурсов, исходя из интересов, опыта и знаний исследователя; информирование исследователя о возможностях поддержки его проекта институтами поддержки научных исследований;
- поиск специалистов по цифровому профилю исследователя; возможность отправлять приглашения на участие в проекте;
- обеспечение эффективного обмена научно-технической и наукометрической информацией между участниками проектов;
- формирование единого реестра грантов и конкурсов.

Участниками информационного взаимодействия, осуществляемого с помощью ЦПСИ являются:

- Министерство науки и высшего образования Российской Федерации;
- Российская академия наук;
- иные Федеральные органы исполнительной власти;
- научные организации, НОЦ, НЦМУ, вузы, фонды и институты развития, а также коммерческие, промышленные и общественные организации;
- физические лица, как являющиеся сотрудниками вышеперечисленных организаций, так и индивидуально, в том числе иностранные участники научного сообщества.

2.2 Цели создания Системы

Целями создания Системы являются:

- создание единого пространства научного и научно-технического взаимодействия, организации и проведения совместных исследований в удаленном доступе, в том числе с зарубежными учеными;
- снижение бюрократической и административной нагрузки на исследователя;
- повышение эффективности распределения бюджетных средств за счет увеличения объема данных об исследователях и результатах научных исследований, используемых при проведении анализа;
- повышение количества совместных научных исследований;
- повышение информированности исследователей к участию в конкурсных процедурах на предоставление научных грантов.

3 ХАРАКТЕРИСТИКА ОБЪЕКТА АВТОМАТИЗАЦИИ

Объектом автоматизации является комплекс задач, решение которых возложено на Министерство науки и высшего образования Российской Федерации, в частности:

- содействие развитию инновационной деятельности;
- формирование рынков научной, научно-технической, инновационной продукции (работ и услуг);
- информационное обеспечение научной и научно-технической деятельности.

Для решения указанных задач применяется комплекс информационных систем, реализованных фондами поддержки научной, научно-технической, инновационной деятельности и другими общественными организациями под руководством Министерства науки и высшего образования Российской Федерации.

Среди применяемых информационных систем можно выделить следующие системы и решаемые ими задачи:

- КИАС РФФИ, ИАС РНФ, АИСУ ФЦП – системы для автоматизации деятельности, связанной с выделением грантов и проведением конкурсов на выполнение исследований;
- реферативные базы данных и инструменты отслеживания цитируемости – информационные системы и веб-порталы, осуществляющие индексирование статей, публикуемых в научных изданиях и предоставляющие наукометрические данные (РИНЦ, Scopus, Web of Science и др.).

Наличие большого количества разнородных систем затрудняет работу исследовательских коллективов и контролирующих организаций по следующим причинам:

- необходимость ввода персональной информации исследователя в различных информационных системах научной отрасли;
- отсутствие источника верифицированной информации о достижениях исследователей;
- отсутствие инструментариев для мониторинга реализации проектов НОЦ и НЦМУ;
- отсутствие инструментов для прямого взаимодействия с членами научного сообщества;
- низкое количество коллабораций при проведении исследований.

Таким образом, функциональности существующих информационных систем недостаточно для реализации национального проекта «Наука», утвержденного

президиумом Совета при Президенте Российской Федерации по стратегическому развитию и национальным проектам (протокол от 24.12.2018 г. № 16).

Ключевыми целями национального проекта «Наука» являются:

- обеспечение присутствия Российской Федерации в числе пяти ведущих стран мира, осуществляющих научные исследования и разработки в областях, определяемых приоритетами научно-технологического развития;
- обеспечение привлекательности работы в Российской Федерации для ведущих российских и зарубежных ученых и молодых перспективных исследователей;
- опережающее увеличение внутренних затрат на научные исследования и разработки за счет всех источников по сравнению с ростом валового внутреннего продукта страны.

Для достижения поставленных целей в рамках настоящего ТЗ автоматизации подлежат следующие технологические задачи:

- обеспечение технологической поддержки создания новых знаний и перспективных технологий через предоставление исследователям и заинтересованным междисциплинарным научным группам доступа к цифровой среде для совместного выполнения научно-исследовательских и опытно-конструкторских работ;
- создание интегрированной системы управления выполнением научно-исследовательских, опытно-конструкторских и иных работ по созданию новых знаний, перспективных технологий и научной продукции, обеспечивающей достоверной и актуальной информацией о результатах данных работ, результатах интеллектуальной деятельности, публикационной активности подведомственных учреждений Заказчика;
- создание информационной базы по выполненным, выполняемым и планируемым научным исследованиям в электронном виде с доступом через единую точку для всех заинтересованных сторон.

С учетом вышеуказанных факторов должна быть создана ЦПСИ, обеспечивающая единое информационное пространство для эффективного взаимодействия научного сообщества, государства и бизнеса, формирования и деятельности виртуальных команд и виртуальной коллаборации при реализации комплексных научно-технических проектов, в том числе с участием зарубежных партнеров, поиска и привлечения к различным научным исследованиям и проектам необходимых ресурсов.

4 ТРЕБОВАНИЯ К СИСТЕМЕ

4.1 Требования к системе в целом

Работы по созданию Системы должны основываться на проектных документах, разработанных в ходе проведения работ по проектированию Системы.

Решения, применяемые при создании Системы, не должны дублировать функциональные возможности существующих информационных систем Министерства науки и высшего образования Российской Федерации.

Создание Системы должно производиться с учетом действующих нормативных правовых актов Российской Федерации.

Создание Системы должно включать в себя следующие работы:

- создание подсистем ЦПСИ;
- интеграция ЦПСИ с внешними информационными системами и сервисами;
- создание Подсистемы обеспечения информационной безопасности;
- проведение мероприятий по аттестации ЦПСИ.

4.1.1 Требования к структуре и функционированию Системы

Система должна состоять из набора внутренних подсистем и компонент, доступных только авторизованным при помощи Подсистема авторизации и управления доступом пользователям, и внешнего портала с открытым доступом.

Внутренние подсистемы должны включать в себя следующие подсистемы и их компоненты:

1) обеспечивающие подсистемы:
   - Подсистема авторизации и управления доступом;
   - Подсистема нормативно-справочной информации;
   - Подсистема журналирования;
   - Подсистема управления настройками;
   - Подсистема уведомлений;
   - Подсистема мониторинга;
   - Подсистема формирования оперативной и аналитической отчетности;
2) Интеграционная шина ЦПСИ;
3) Подсистема интеграционного взаимодействия;
4) Подсистема «Цифровой профиль исследователя»:
   - раздел «Персональная информация»;
   - раздел «Публикационная активность»;

- раздел «Проведенные НИР»;

5) Подсистема «Цифровой профиль организации»:

- раздел «Общие сведения об организации»;
- раздел «Участие в грантах и конкурсах»;
- раздел «Сотрудники организации»;

6) Подсистема «Научная тема»:

- раздел «Паспорт проекта»;
- раздел «Команда проекта»;

7) Подсистема «Гранты и конкурсы»:

- раздел «Единый реестр грантов и конкурсов»;
- раздел «Публикация грантов и конкурсов»;
- раздел «Заявки на участие в грантах и конкурсах»;

8) Подсистема обеспечения информационной безопасности.

9) Открытый портал должен включать следующие разделы:

- раздел «Научные проекты»;
- раздел «Аналитика».

Структурная схема ЦПСИ приведена в соответствии с рисунком 1.

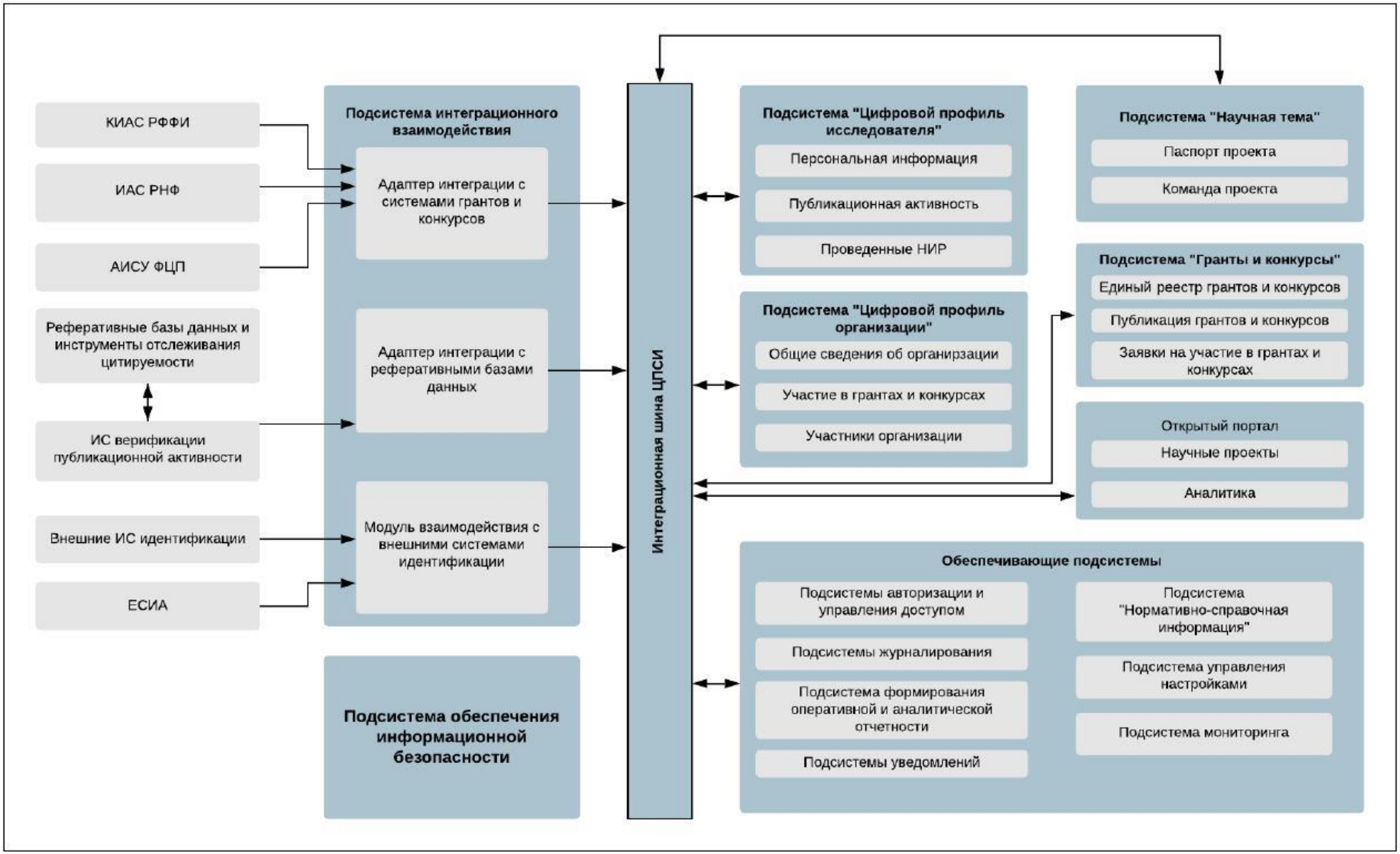

Рисунок 1 – Структурная схема ЦПСИ

4.1.1.1 Требования к личным кабинетам

Функциональность создаваемых подсистем и их компонентов должна быть доступна пользователям Системы через соответствующие личные кабинеты. Личный кабинет должен представлять собой автоматизированное рабочее место, позволяющее пользователю выполнять требуемый набор задач.

Вход в личный кабинет должен осуществляться с помощью подсистемы авторизации и управления доступом, в том числе с использованием ЕСИА. Детальное описание приведено в разделе 4.2.1.1.

Перечень личных кабинетов должен формироваться исходя из функциональных групп пользователей Системы и должен включать в себя следующие личные кабинеты:

- личный кабинет исследователя;
- личный кабинет научной организации;
- личный кабинет фонда или коммерческой организации;
- личный кабинет Минобрнауки России;
- личный кабинет администратора Системы.

Структурная схема, отображающая взаимосвязь личных кабинетов с подсистемами ЦПСИ и их компонентами, приведена в соответствии с рисунком Рисунок 2.

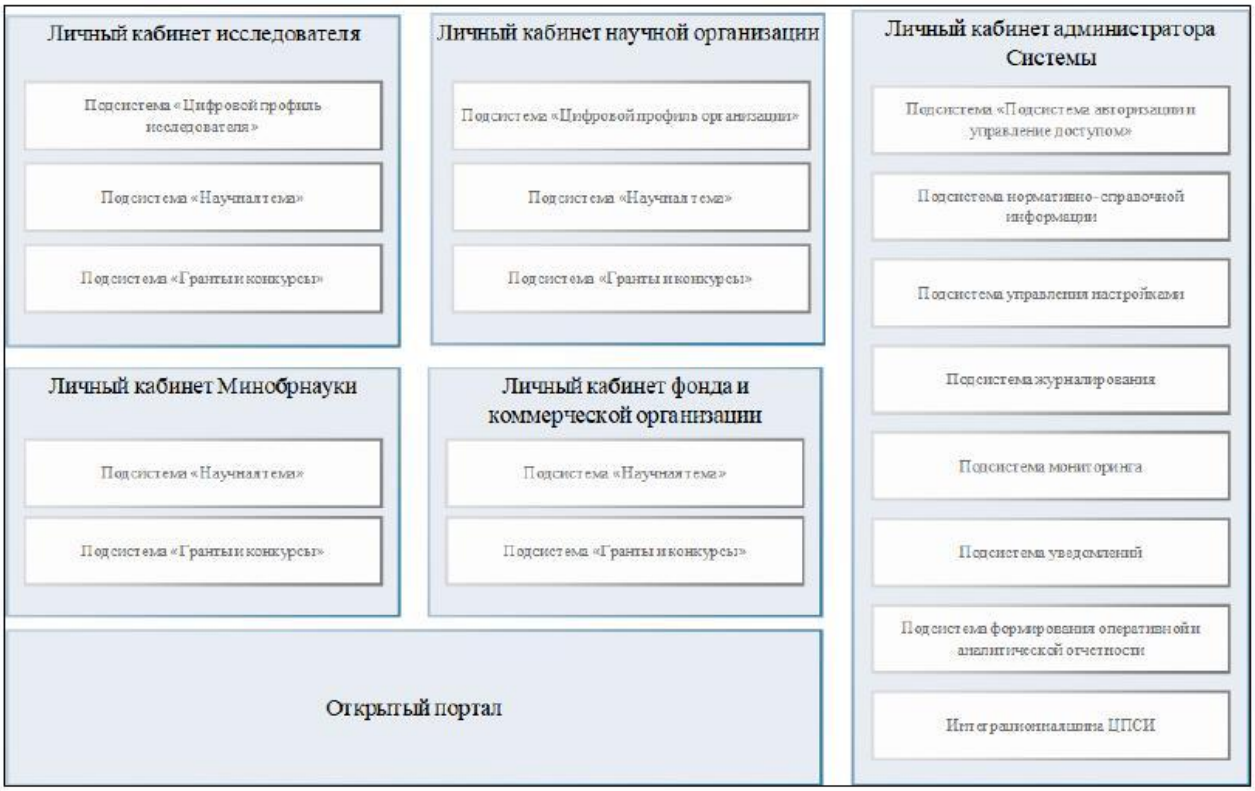

Рисунок 2 – Структурная схема личных кабинетов ЦПСИ

4.1.1.1.1 Личный кабинет исследователя

Личный кабинет исследователя должен обеспечивать доступ к Системе для исследователей и должен быть предназначен для исполнения процессов, связанных с выполнением исследовательской деятельности.

Личный кабинет исследователя должен обеспечивать выполнение следующих задач:

- регистрация исследователя в Системе;
- управление персональной информацией и учетными данными;
- управление сведениями о публикационной активности;
- управление сведениями о текущих, планируемых и проведенных проектах исследований , включая:
  - основные сведения о проекте;
  - формирование команды проекта с использованием цифровых профилей других исследователей и распределением функциональных ролей на проекте;
  - формирование единой базы артефактов проекта и проектной документации;
- управление приватностью сведений об исследователе, его проектах, и публикационной активности для других пользователей Системы и на открытом портале;
- поиск доступных грантов и конкурсов на проведение исследований;
- подача заявок на гранты и конкурсы с возможностью отслеживания этапов и результатов рассмотрения заявки.

4.1.1.1.2 Личный кабинет научной организации

Личный кабинет научной организации должен обеспечивать доступ к Системе для научных организаций, осуществляющих организацию научной деятельности.

Личный кабинет научной организации должен быть предназначен для учета проектов, выполняемых исследователями-сотрудниками научной организации, а также сопутствующих процессов, влияющих на количество и успешность научных исследований.

Личный кабинет научной организации должен обеспечивать выполнение следующих задач:

- регистрация научной организации, исследователей и учетных записей сотрудников, занятых организацией научной деятельности, в Системе;
- управление сведениями об организации, направлениях деятельности;

- управление сведениями о текущих, планируемых и проведенных проектах исследований , включая:
  - основные сведения о проекте;
  - формирование команды проекта с использованием цифровых профилей исследователей-сотрудников организации и распределением функциональных ролей на проекте;
  - формирование единой базы артефактов проекта и проектной документации;
  - мониторинг научного проекта и заполнение требуемой отчетности;
- сбор статистики с использованием отчетных форм и проведение аналитики на основе полученных показателей;
- поиск доступных грантов и конкурсов на проведение исследований;
- подача заявок на гранты и конкурсы с возможностью отслеживания этапов и результатов рассмотрения заявки.

4.1.1.1.3 Личный кабинет фонда или коммерческой организации

Личный кабинет фонда или коммерческой организации должен обеспечивать доступ к Системе для организаций, заинтересованных в получении услуг по выполнению научных исследований, и фондов, осуществляющих поддержку научно-исследовательских работ.

Личный кабинет фонда или коммерческой организации должен быть предназначен для исполнения процессов, связанных с финансированием научных исследований путем предоставления грантов и конкурсов, а также процессов по мониторингу научных проектов, на которые было выделено финансирование.

Личный кабинет фонда или коммерческой организации должен обеспечивать выполнение следующих задач:

- регистрация организации и учетных записей сотрудников в Системе;
- размещение грантов и конкурсов на проведение исследований и управление заявками, направленными кандидатами на получение грантов;
- выдвижение проектов на экспертизу (в т.ч. международную) и просмотр результатов экспертизы научных проектов, на которые выделено финансирование;
- сбор статистики с использованием отчетных форм и проведение аналитики на основе полученных показателей;
- поиск перспективных научных проектов, требующих финансирования со стороны коммерческих организаций или фондов поддержки исследовательской деятельности.

4.1.1.1.4 Личный кабинет Минобрнауки России

Личный кабинет Минобрнауки России должен обеспечивать доступ к Системе для сотрудников Министерства науки и высшего образования Российской Федерации, осуществляющих мониторинг и контроль деятельности научных организаций и исследователей.

Личный кабинет Минобрнауки России должен быть предназначен для исполнения процессов учета научных проектов, а также процессов финансирования научных исследований путем предоставления грантов и объявления конкурсов.

Личный кабинет Минобрнауки России должен обеспечивать выполнение следующих задач:

- регистрация сотрудника Минобрнауки России в Системе;
- поиск и просмотр сведений о научных проектах;
- размещение грантов и конкурсов на проведение исследований и управление заявками, направленными кандидатами на получение грантов;
- выдвижение проектов на экспертизу (в т.ч. международную) и просмотр результатов экспертизы научных проектов, на которые выделено финансирование;
- настройка отчетных форм;
- сбор статистики с использованием отчетных форм и проведение аналитики на основе полученных показателей.

4.1.1.1.5 Личный кабинет администратора Системы

Личный кабинет администратора Системы должен обеспечивать доступ к Системе для пользователей, выполняющих функции по администрированию, настройке и сервисному обслуживанию подсистем и их компонентов.

Личный кабинет администратора Системы должен обеспечивать выполнение следующих задач:

- настройка ролевой модели Системы;
- управление учетными записями пользователей Системы и аккаунтами организаций, включая модерацию и верификацию данных при регистрации;
- управление настройками Системы;
- мониторинг событий Системы, включая действия пользователей и возникающие ошибки;
- мониторинг ключевых параметров программно-аппаратного комплекса;

- настройка параметров отправки уведомлений, включая возможность ручной отправки уведомлений о плановых и регламентных работах;
- настройка форм для сбора регламентированной и произвольной отчетности, используемых в прикладных подсистемах;
- настройка источников данных и аналитических панелей для проведения аналитики и вывода статистических показателей;
- настройка параметров информационного взаимодействия с внешними информационными системами.

4.1.1.2 Требования к способам и средствам связи для информационного обмена между подсистемами

Информационный обмен между основными компонентами Системы должен осуществляться с использованием стандартизированных подходов к обмену информацией (REST, SOAP) с учетом требований обеспечения информационной безопасности, указанных в разделе 4.2.9. Разработка стандартов информационного обмена должна осуществляться Исполнителем на стадии техно-рабочего проектирования. В целях мониторинга информационного взаимодействия в рамках Системы должна быть реализована специализированная подсистема для работы с журналами, хранящими информацию обо всех осуществленных запросах между различными компонентами Системы и результатах их обработки.

4.1.1.3 Требования к характеристикам взаимосвязей Системы со смежными системами

Для обеспечения информационного сопряжения со смежными системами в Системе должны быть предусмотрены средства технической, программной, информационной, лингвистической совместимости.

Для обеспечения технической совместимости Системы со смежными системами на стадии техно-рабочего проектирования должны быть разработаны схемы технического сопряжения (взаимодействия). Нормативно-правовое и организационное обеспечение информационно-технического сопряжения (взаимодействия) Системы со смежными системами осуществляется Заказчиком.

Для обеспечения информационно-технического сопряжения Системы со смежными системами на этапе разработки технического проекта Системы должны быть разработаны проекты регламентов информационного взаимодействия с каждой смежной системой.

Согласование и введение в действие регламентов информационного взаимодействия осуществляется Заказчиком.

Подключение смежной системы должно включать этапы ввода в эксплуатацию (пуско-наладочные работы, предварительные испытания, опытная эксплуатация, приемочные испытания).

На этапе разработки технического проекта Системы должен быть определен перечень смежных систем, с которыми должно быть реализовано информационное сопряжение. Обеспечение работ по обследованию и определению перечня сопрягаемых систем осуществляется Заказчиком.

4.1.1.4 Требования к режимам функционирования Системы

Функционирование Системы должно быть обеспечено в следующих режимах:

- штатный режим (непрерывная работа в круглосуточном режиме с учетом технологических профилактических перерывов и перерывов на проведение регламентных работ);
- сервисный режим (для проведения обслуживания, реконфигурации, замены и пополнения новыми компонентами, а также при проведении резервного копирования информации);
- аварийный режим.

В штатном режиме функционирования Система должна обеспечивать следующий режим работы: доступность функций Системы в режиме – 24 часа в день, 7 дней в неделю (24х7). Круглосуточный режим работы Системы не требует организации круглосуточной работы пользователей и допускает работу пользователей в соответствии со штатным расписанием.

В сервисном режиме Система должна обеспечивать возможность проведения следующих работ:

- техническое обслуживание;
- модернизацию аппаратно-программного комплекса;
- устранение аварийных ситуаций;
- резервное копирование базы данных.

Система переходит в аварийный режим работы при возникновении нештатной ситуации и невозможности работы в штатном режиме. В случае перехода Системы в аварийный режим, обслуживающему персоналу необходимо перевести Систему в сервисный режим в соответствии с инструкциями, которые должны быть изложены в руководстве администратора Системы.

Регламентные работы должны производиться с учётом требований о доступности Системы. Регламентные работы, связанные с ограничением работы пользователей Системы, должны проводиться во внерабочее время. Время проведения таких регламентных работ и порядок уведомления о регламентных работах должны быть определены и согласованы между Заказчиком и Исполнителем, выполняющим работы по сопровождению Системы.

Функционирование Системы при отказах и сбоях серверного общесистемного и специального ПО и оборудования, в том числе структурных узлов Системы, не предусматривается.

4.1.1.5 Требования по диагностированию Системы

Диагностирование Системы должно производиться штатными средствами платформенного ПО.

Диагностирование Системы должно выполняться с целью своевременного предупреждения возникновения аварийных ситуаций и обеспечивать выявление неработоспособности Системы.

При диагностировании должна быть обеспечена возможность выполнения следующих работ:

- диагностирование физической целостности используемого программного обеспечения;
- диагностирование логической целостности используемого программного обеспечения.

В процессе диагностирования должна быть обеспечена:

- регистрация диагностических сообщений при работе специального программного обеспечения;
- генерация оповещений о возможности появления критичных событий в работе Системы.

Полный перечень параметров, подлежащих диагностике, определяется на стадии технического проектирования.

4.1.1.6 Требования к перспективам развития, модернизации Системы

При проектировании и разработке компонентов Системы должны быть заложены основы для их дальнейшего развития и масштабирования.

Должны быть предусмотрены следующие способы развития Системы:

- изменение программного кода Системы для добавления новых функций в существующих программных средствах;
- создание новых программных средств на основе уже имеющихся с целью удовлетворения потребностей пользователей Системы.

В Системе должна быть предусмотрена возможность увеличения ее производительности путем масштабирования без внесения изменений в исходные коды системы. Должна быть обеспечена возможность:

- расширения организационных рамок (увеличения числа пользователей, расширение количества подразделений, работающих в Системе);
- расширения функциональных рамок (возникновения новых либо изменения существующих процессов);
- роста объемов информации, обрабатываемой Системой.

4.1.2 Требования к численности и квалификации персонала Системы и режиму его работы

Численность персонала Системы должна быть установлена из расчета обеспечения работоспособности Системы в штатном режиме функционирования.

Режим работы персонала Системы должен обеспечить пользователям возможность работать в режиме 24/7/365 с учетом наличия технологических окон, необходимых для обеспечения работоспособности Системы.

Численность и квалификация персонала Системы должны определяться с учетом следующих требований:

- структура Системы должна предоставлять возможность управления всем доступным функционалом Системы как одному, так и нескольким администраторам;
- Система не должна требовать круглосуточного обслуживания и присутствия администраторов у консоли управления.

Для эксплуатации Системы должны быть определены следующие роли:

- «Системный администратор»;
- «Администратор»;
- «Пользователь».

Основные действия системного администратора:

- осуществление регламентных работ с Системой: резервное копирование данных, запуск регламентных процедур обмена информацией со смежными информационными системами;

- осуществление обновления конфигурации Системы при выходе обновлений и исправлений;
- осуществление прочих действий в соответствии с регламентом эксплуатации.

Основные действия администратора:

- осуществление ведения списка пользователей Системы (назначение прав доступа, изменение паролей доступа и др. административные функции);
- осуществление регистрации и диспетчеризации запросов пользователей, возникающих в ходе работы с Системой, а также консультация пользователей по вопросам работы с Системой;
- настройка и поддержание в актуальном состоянии справочников.

Основные действия пользователя:

- осуществление поиска, просмотра и ввода информации;
- формирование отчетов и других действий в соответствии с выполняемой ролью.

Система должна поддерживать возможность реализации неограниченного количества функциональных ролей пользователей с соответствующим разграничением доступа к функциональным возможностям, пользовательским интерфейсам Системы и хранимой в системе информации.

4.1.3 Показатели назначения

4.1.3.1 Требования к степени приспособляемости (к изменению условий эксплуатации), масштабируемости Системы

Система должна обладать свойствами приспособляемости и масштабируемости, заключающимися в возможности сохранения или повышения производительности при изменении условий эксплуатации, гибкости по отношению к изменениям, не связанным с коренным изменением нормативных документов, регулирующих деятельность пользователей Системы.

Требования к приспособляемости заключаются в обеспечении работоспособности в следующих случаях:

- при изменении количества потребителей информации;
- при изменении количества автоматизируемых функций;
- при изменении требований к безопасности;
- при изменении количества поставщиков информации.

4.1.3.2 Влияние изменения количества потребителей информации

Изменение количества потребителей информации изменяет нагрузку на серверы, что может вызвать необходимость повышения способности поддерживать увеличивающийся объем передаваемой информации без существенной потери производительности и отказов в обслуживании обращений (нагрузочной способности) серверов. Увеличение нагрузочной способности должно выполняться как за счет увеличения мощности серверов (увеличение количества процессоров, либо модернизация до более производительных процессоров, увеличение объема оперативной памяти и дискового пространства), так и за счет увеличения количества серверов. При этом должны соблюдаться следующие требования:

- Система должна адаптироваться к увеличению количества потребителей информации без необходимости изменения архитектуры;
- добавление новых серверов в состав группы серверов не должно приводить к полной остановке функционирования.

4.1.3.3 Влияние изменения количества автоматизируемых функций

Изменение количества функций, автоматизируемых с помощью Системы, влечет изменение в программных модулях Системы и их количестве, что влияет на нагрузку на серверы БД и веб-серверы (серверы приложений) Системы. Увеличение нагрузки на серверы БД и веб-серверы (серверы приложений) Системы потребует повышения нагрузочной способности серверов. Увеличение нагрузочной способности может выполняться как за счет увеличения мощности серверов БД и веб-серверов (серверов приложений), так и за счет увеличения их количества. Также в этом случае может применяться технология объединения серверов БД в кластеры (кластерная технология), при которой несколько серверов вместе обрабатывают одни и те же операции (транзакции), распределяя нагрузку между собой (между узлами кластера).

4.1.3.4 Влияние изменения требований к безопасности Системы

Изменение требований к безопасности Системы оказывает влияние на все ее составные части. Доработанные модули Системы должны адаптироваться в соответствии с изменяющимися требованиями с соблюдением следующих условий:

- в процессе адаптации защищенность не должна становиться хуже существующей на момент начала адаптации;
- процесс адаптации не должен прерывать доступ потребителей информации к информационным ресурсам;

- процесс адаптации не должен прерывать процесс подготовки и публикации документов;
- процесс адаптации не должен затрагивать тех пользователей, на которых не распространяются новые требования.

4.1.3.5 Влияние изменения количества поставщиков информации

Изменение количества поставщиков информации изменяет нагрузку на веб-серверы (серверы приложений) Системы и может повлечь расширение количества автоматизируемых функций, что повысит нагрузку на серверы БД. Повышение нагрузочной способности веб-серверов (серверов приложений) и серверов БД может выполняться различными методами и средствами. При этом также должны соблюдаться следующие условия:

- процедура публикации данных должна оставаться независимой от количества поставщиков информации;
- безопасность доработанных модулей Системы не должна ухудшаться при увеличении числа поставщиков информации;
- механизмы подготовки и публикации данных должны обеспечивать возможность обслуживания всех поставщиков информации без снижения производительности;
- желательна непрерывность процесса подготовки и публикации данных.

4.1.4 Требования к надежности

4.1.4.1 Показатели надежности Системы

При разработке Системы должно быть соблюдено требование по надежности, как свойству сохранять во времени в установленных пределах значения всех параметров, характеризующих способность Системы выполнять свои функции в заданных режимах и условиях эксплуатации.

Показатели надежности Системы тесно связаны с показателями надежности технических и программных средств, обеспечивающих функционирование Системы.

Система должна сохранять работоспособность и обеспечивать автоматическое восстановление своих функций при возникновении внештатных ситуаций, таких как:

- сбои в системе электроснабжения аппаратной части, приводящие к отключению или перезагрузке сервера, на котором размещена Система. Восстановление работоспособности Системы должно происходить автоматически после перезапуска серверов;

- ошибки в работе аппаратных средств (кроме носителей данных и программ). Восстановление функции Системы возлагается на службу администрирования, политику администрирования и регламент эксплуатации Системы;
- аварийные ситуации, вызванные неверными действиями пользователей, неверным форматом или недопустимыми значениями входных данных. В указанных случаях Система должна выдавать пользователю соответствующие сообщения, после чего возвращаться в рабочее состояние, предшествовавшее неверной (недопустимой) команде или некорректному вводу данных.

Резервное копирование Системы должно осуществляться с регулярностью не реже одного раза в неделю.

Восстановление системы после критического сбоя (отказа дисковой подсистемы) должно осуществляться администратором системы на основании регламента резервного копирования и восстановления данных. Время восстановления системы после критического сбоя не должно превышать 24 часов.

4.1.4.2 Аварийные ситуации

Система должна обеспечивать возможность формирования и хранения резервных копий данных Системы, а также возможность их восстановления. При возникновении сбоя в ПО в процессе выполнения пользовательских задач, должно быть обеспечено восстановление данных до состояния на момент окончания последней нормально завершенной перед сбоем операции (транзакции).

Время восстановления работоспособности при сбоях и отказах не должно превышать 3-х часов. В это время не входит разворачивание и настройка специального прикладного ПО на сервере(ах) приложений и сервере(ах) баз данных. В указанное время не входит решение проблем с техническим обеспечением и инсталляцией ОС указанных серверов.

4.1.4.3 Требования к надежности технических средств и программного обеспечения

При разработке Системы должно быть соблюдено требование по надежности, как свойству сохранять во времени в установленных пределах значения всех параметров, характеризующих способность Системы выполнять свои функции в заданных режимах и условиях эксплуатации.

Показатели надежности Системы должны определяться показателями надежности технических и программных средств, обеспечивающих функционирование Системы.

Система должна сохранять работоспособность и обеспечивать автоматическое восстановление своих функций при возникновении внештатных ситуаций, таких как:

- сбои в системе электроснабжения аппаратной части, приводящие к отключению или перезагрузке сервера, на котором размещена Система. Восстановление программы должно происходить автоматически после перезапуска сервера и запуска исполняемого файла Системы;
- ошибки в работе аппаратных средств (кроме носителей данных и программ). Восстановление функции Системы возлагается на службу администрирования, политику администрирования и регламент эксплуатации Системы;
- аварийные ситуации, вызванные неверными действиями пользователей, неверным форматом или недопустимыми значениями входных данных. В указанных случаях Система должна выдавать пользователю соответствующие сообщения, после чего возвращаться в рабочее состояние, предшествовавшее неверной (недопустимой) команде или некорректному вводу данных.

Резервное копирование Системы должно осуществляться с регулярностью, предусмотренной соответствующим регламентом, но не реже одного раза в неделю.

Восстановление системы после критического сбоя (отказа дисковой подсистемы) должно осуществляться администратором Системы на основании регламента резервного копирования и восстановления данных. Время восстановления Системы после критического сбоя не должно превышать 24 часов.

В целом надежность Системы должна обеспечивать выполнение функций со временем однократного простоя не более 6-ти часов и суммарным временем простоя не более 48 часов в год, если иное не согласовано с Заказчиком.

Показатели надежности Системы, за исключением среднего срока сохраняемости, устанавливаются для нормальных климатических условий эксплуатации в соответствии с ГОСТ 21552-84.

Средняя наработка на отказ аппаратных средств хранения данных Системы должна быть, в соответствии с требованиями ГОСТ 21552-84 и ГОСТ 27201-87, не менее 10 000 часов.

Действия по восстановлению работоспособности при отказе или выходе из строя Системы должны регламентироваться условиями гарантии и Соглашением о Технической Поддержке, представляемыми производителями программного обеспечения и технических средств защиты.

Система должна удовлетворять следующим требованиям по надежности программного обеспечения:

- средняя наработка программных средств на отказ – не менее 500 часов;
- среднее время восстановления программных средств серверов – не более 8 часов;
- среднее время восстановления программных средств Системы пользователя – не более 6 часов;
- среднее время на восстановление работоспособности путем перехода на резервные программно-аппаратные средства – не более 1 часа.

Программно-аппаратная архитектура, удовлетворяющая приведенным выше требованиям, должна быть спроектирована Исполнителем и согласована с Заказчиком на этапе подготовки технического проекта.

4.1.5 Требования безопасности

Система должна обеспечивать безопасность обслуживающего персонала при эксплуатации, техническом обслуживании и ремонте с учетом требований:

- ГОСТ 21552-84 «Средства вычислительной техники. Общие технические требования, приемка, методы испытаний, маркировка, упаковка, транспортирование и хранение»;
- ГОСТ 25861-83 «Машины вычислительные и системы обработки данных. Требования по электрической и механической безопасности и методы испытаний».

Электробезопасность должна соответствовать требованиям:

- ГОСТ 12.1.030-81 «Система стандартов безопасности труда. Электробезопасность. Защитное заземление. Зануление»;
- ГОСТ 12.2.003-91 «Система стандартов безопасности труда. Оборудование производственное. Общие требования безопасности»;
- ГОСТ 12.2.007.0-75 «Система стандартов безопасности труда. Изделия электротехнические. Общие требования безопасности».

Помимо соответствия действующей системе государственных стандартов безопасности труда, технические средства Системы должны иметь сертификаты по электробезопасности и электромагнитной безопасности.

Основой для пожарной безопасности должны служить следующие нормативные документы:

- НПБ 110-03 «Перечень зданий, сооружений, помещений и оборудования, подлежащих защите автоматическими установками пожаротушения и автоматической пожарной сигнализацией»;
- СНиП 21-01-97 «Пожарная безопасность зданий и сооружений»;

– НПБ 105-03 «Определение категорий помещений, зданий и наружных установок по взрывопожарной и пожарной опасности».

4.1.6 Требования к эргономике и технической эстетике

При выполнении работ следует руководствоваться стандартом ГОСТ Р ИСО 9241-210-2016 «Эргономика взаимодействия человек-система. Часть 210. Человеко-ориентированное проектирование интерактивных систем», который утвержден и введен в действие Приказом Федерального агентства по техническому регулированию и метрологии от 2 ноября 2016 г. № 1581-ст., а также интерфейсными стандартами производителей или операционных систем, в рамках которых будет использоваться Система.

Взаимодействие пользователей с Системой должно осуществляться посредством визуального графического интерфейса.

Интерфейс Системы должен быть понятным и удобным, не должен быть перегружен графическими элементами.

Ввод-вывод данных Системы, прием управляющих команд и отображение результатов их исполнения должны выполняться в интерактивном режиме. Интерфейс должен соответствовать современным эргономическим требованиям и обеспечивать удобный доступ к основным функциям и операциям Системы.

Все надписи экранных форм, а также сообщения об ошибках пользователей должны выводиться на экран монитора на русском и английском языках. В случаях, когда сообщение формируется на уровне общесистемного ПО, сообщение может выводиться только на английском языке.

Пользователь должен получать информацию, как об успешном завершении операций, так и о возникновении сбоев в ходе их выполнения или невозможности выполнения.

Система должна обеспечивать корректную обработку аварийных ситуаций, вызванных неверными действиями пользователей, неверным форматом или недопустимыми значениями входных данных. В указанных случаях Система должна выдавать пользователю сообщения, отражающие проблему и содержащие рекомендации по ее устранению, после чего возвращаться в рабочее состояние, предшествовавшее неверной (недопустимой) команде или некорректному вводу данных.

Каждая веб-страница Системы должна обладать кратким заголовком.

4.1.7 Требования к эксплуатации, техническому обслуживанию, ремонту и хранению компонентов Системы

Условия эксплуатации, а также виды и периодичность обслуживания технических средств должны соответствовать требованиям по эксплуатации, техническому обслуживанию, ремонту и хранению, изложенным в документации завода-изготовителя на них.

Технические средства Системы должны размещаться в помещениях, которые по климатическим условиям соответствуют ГОСТ 15150-69 «Машины, приборы и другие технические изделия. Исполнения для различных климатических районов. Категории, условия эксплуатации, хранения и транспортирования в части воздействия климатических факторов внешней среды» (температура окружающего воздуха от 5 до 40 °С, относительная влажность от 40 до 80 % при t = 25 °С, атмосферное давление от 630 до 800 мм ртутного столба). Размещение технических средств и организация автоматизированных рабочих мест должны быть выполнены в соответствии с требованиями ГОСТ 21958-76 «Система «Человек-машина». Зал и кабины операторов. Взаимное расположение рабочих мест. Общие эргономические требования».

Техническое обслуживание Системы должно осуществляться эксплуатирующим персоналом. Численность, квалификация, режим работы и функции эксплуатирующего персонала, а также регламент технического обслуживания определяются на стадии технорабочего проектирования.

Система должна быть рассчитана на эксплуатацию в составе программно-технического комплекса Заказчика. Техническая и физическая защита аппаратных компонентов Системы, носителей данных, бесперебойное энергоснабжение, резервирование ресурсов, текущее обслуживание реализуется техническими и организационными средствами Заказчика.

Все пользователи Системы должны соблюдать правила эксплуатации электронной вычислительной техники.

Система не должна требовать регулярного администрирования. Штатные средства Системы должны позволять проводить удаленное администрирование базы данных и настройку Системы (при наличии технической возможности доступа к серверам Системы).

Техническое обслуживание Системы должно проводиться специалистом, прошедшим обучение по обслуживанию (администрированию) Системы.

Ремонт и восстановление Системы после сбоев и отказов должны проводиться квалифицированными специалистами.

4.1.8 Требования к защите информации от несанкционированного доступа

В Системе должна быть реализована технология единого входа, при которой пользователь, регистрируясь в Системе, проходит аутентификацию один раз в начале работы. После первичной аутентификации для доступа к другим функциям Системы в рамках своих полномочий (должностных обязанностей) повторная аутентификация не требуется.

Требования к защите информации от несанкционированного доступа должны быть реализованы в рамках создания подсистем:

- Подсистемы обеспечения информационной безопасности (ПОИБ);
- Подсистемы авторизации и управления доступом.

Создание Подсистемы обеспечения информационной безопасности осуществляется поэтапно. Описание Подсистемы авторизации и управления доступом приведено в разделе 4.2.1.1.

4.1.8.1 Формирование требований к ПОИБ

В рамках данного этапа требуется выполнить следующие работы:

- сбор информации о порядке, способах обработки информации, структуре и составе Системы:
  1) определение перечня сведений, подлежащих защите;
  2) сбор информации о процессах, в рамках которых осуществляется обработка информация ограниченного доступа, определение целей обработки;
  3) сбор информации о конфигурации и топологии Системы в целом и ее отдельных компонентов, ее характеристиках, используемых информационных технологиях и технологических процессах обработки данных;
  4) определение состава и количества автоматизированных рабочих мест и серверов Системы, активного сетевого оборудования, участвующего (либо планируемого) в процессе обработки информации;
  5) определение состава системного и прикладного программного обеспечения Системы, мест и форм обработки информации;
  6) определение взаимодействия Системы с другими информационными системами, включая взаимодействие с системами других организаций (в том числе по сети Интернет);
- классификация Системы по требованиям защиты информации (далее – классификация информационной системы) в соответствии с действующими

требованиями Законодательства РФ, в том числе определения уровня защищенности ПДн;

- определение актуальных угроз безопасности информации с учетом Банка данных угроз ФСТЭК России (http://bdu.fstec.ru/) и разработку на их основе модели угроз безопасности информации;
- определение базового набора мер защиты информации для установленного класса защищенности информационной системы;
- адаптация базового набора мер по обеспечению безопасности информации с учетом структурно-функциональных характеристик информационной системы, информационных технологий, особенностей функционирования информационной системы (в том числе исключение из базового набора мер, непосредственно связанных с информационными технологиями, не используемыми в информационной системе, или структурно-функциональными характеристиками, не свойственными информационной системе);
- уточнение адаптированного базового набора мер защиты информации с учетом не выбранных ранее мер защиты информации, в результате чего определяются меры защиты информации, обеспечивающие блокирование (нейтрализацию) всех актуальных угроз безопасности информации, включенных в модель угроз безопасности информации;
- дополнение уточненного адаптированного базового набора мер защиты информации мерами, обеспечивающими выполнение требований о защите информации, установленными иными нормативными правовыми актами в области защиты информации, в том числе в области защиты персональных данных;
- разработка технического задания на создание ПОИБ, с учетом ГОСТ 34.602, ГОСТ Р 51583 и ГОСТ Р 51624, и содержащего:
    1) цель и задачи обеспечения защиты информации в информационной системе;
    2) класс защищенности информационной системы (уровень защищенности ПДн);
    3) перечень нормативных правовых актов, методических документов и национальных стандартов, которым должна соответствовать информационная система;
    4) перечень объектов защиты информационной системы;
    5) требования к мерам и средствам защиты информации, применяемым в информационной системе;

6) требования к защите информации при информационном взаимодействии с иными информационными системами и информационно-телекоммуникационными сетями, в том числе с информационными системами уполномоченного лица, а также при применении вычислительных ресурсов (мощностей), предоставляемых уполномоченным лицом для обработки информации.

Результаты работ данного этапа должны быть зафиксированы в документах:

- Проект акта классификации;
- Модель угроз;
- Модель нарушителя;
- Частное техническое задание на создание ПОИБ.

4.1.8.2 Разработка внутренних нормативных и организационно-распорядительных документов по порядку обработки информации в Системе

В ходе данного этапа требуется разработка проектов внутренних нормативных и организационно-распорядительных документов Заказчика (или предложений по доработке существующих документов), необходимых при организации процесса обработки и обеспечения безопасности информации в соответствии с действующим Законодательством РФ, а также определяющих правила и процедуры, полностью или частично необходимые для реализации выбранных мер по обеспечению безопасности информации:

- Приказ о вводе в эксплуатацию автоматизированной системы;
- Приказ об определении ответственности должностных лиц и проведении мероприятий по защите информации;
- Акт классификации информационной системы;
- Акт определения уровня защищенности ПДн, обрабатываемых в ИСПДн;
- Перечень организационно-технических мероприятий по защите информации;
- Должностная инструкция администратора безопасности информации автоматизированной системы;
- Должностная инструкция пользователя автоматизированной системы по обеспечению безопасности информации;
- Инструкция по проведению антивирусного контроля в автоматизированной системе;
- Инструкция по организации парольной защиты в автоматизированной системе;
- Инструкция по внесению изменений в списки пользователей и наделению их полномочиями доступа к защищаемым ресурсам;

- Инструкция по установке, модификации и техническому обслуживанию программного обеспечения и аппаратных средств;
- Инструкция по выявлению и реагированию на инциденты информационной безопасности;
- Технический паспорт на автоматизированную систему;
- Описание технологического процесса обработки информации в автоматизированной системе;
- Перечень защищаемых информационных ресурсов автоматизированной системы;
- Журнал учета носителей конфиденциальной информации;
- Матрица доступа к разделяемым информационным ресурсам автоматизированной системы;
- Положение о порядке организации и проведения работ по защите информации ограниченного доступа (включая персональные данные), не содержащей сведений, составляющих государственную тайну;
- Положение о пропускном и внутриобъектовом режиме;
- Положения о разрешительной системе допуска исполнителей к документам и сведениям в организации;
- Перечень сведений конфиденциального характера;
- Перечень лиц, доступ которых к АС необходим для выполнения служебных (трудовых) обязанностей.

Указанные документы разрабатываются с учетом специфики деятельности Заказчика на основе действующих в РФ требований Законодательства и нормативных правовых актов по защите информации.

Перечень документов данного этапа должен быть уточнен по итогам работ первого этапа.

4.1.8.3 Техническое проектирование решений ПОИБ

В ходе технического проектирования требуется определение и документирование технических решений и состава необходимых программно-технических средств защиты, предполагаемых к использованию в составе ПОИБ в соответствии с предъявленными в ЧТЗ требованиями, а также необходимых для их функционирования общесистемных и прикладных программных средств и оборудования.

При проектировании технических решений в составе ПОИБ требуется:

- определить технические решения по реализации указанных в ЧТЗ требований с учетом уже реализованных у Заказчика технических мер;

- выбрать средства защиты информации с учетом их совместимости с ИТ и техническими средствами, функций безопасности этих средств и особенностей их реализации, а также требуемых мер защиты информации с учетом класса защищенности Системы;
- разработать структуру технических решений ПОИБ (состав и назначение составных частей ПОИБ) и описание применения ПОИБ, включая определение мест размещения компонентов средств и систем защиты, способов взаимодействия между ними, способов управления и мониторинга;
- разработать требования по реализации необходимых функций и механизмов безопасности в прикладном ПО Системы (в случае необходимости);
- разработать спецификацию поставляемого оборудования и ПО ПОИБ, необходимых для создания/модернизации ПОИБ;
- определить необходимые условия для ввода ПОИБ в действие, включая назначение лиц, ответственных за обеспечение безопасности информации и эксплуатацию ПОИБ, требования к системной и сетевой инфраструктуре объектов внедрения для внедрения ПОИБ.

Результаты проектирования ПОИБ отражаются в проектной документации, разрабатываемой с учетом ГОСТ 34.201-89 «Информационная технология. Комплекс стандартов на автоматизированные системы. Виды, комплектность и обозначение документов при создании автоматизированных систем» (далее – ГОСТ 34.201-89).

В проектной документации на ПОИБ:

- определяются типы субъектов доступа (пользователи, процессы и иные субъекты доступа) и объектов доступа, являющихся объектами защиты (устройства, объекты файловой системы, запускаемые и исполняемые модули, объекты системы управления базами данных, объекты, создаваемые прикладным программным обеспечением, иные объекты доступа);
- определяются методы управления доступом (дискреционный, мандатный, ролевой или иные методы), типы доступа (чтение, запись, выполнение или иные типы доступа) и правила разграничения доступа субъектов доступа к объектам доступа (на основе списков, меток безопасности, ролей и иных правил), подлежащие реализации в информационной системе;
- выбираются меры защиты информации, подлежащие реализации в системе защиты информации информационной системы;
- определяются виды и типы средств защиты информации, обеспечивающие реализацию технических мер защиты информации;

- определяется структура ПОИБ информационной системы, включая состав (количество) и места размещения ее элементов;
- осуществляется выбор средств защиты информации, сертифицированных на соответствие требованиям по безопасности информации, с учетом их стоимости, совместимости с информационными технологиями и техническими средствами, функций безопасности этих средств и особенностей их реализации, а также класса защищенности информационной системы;
- определяются параметры настройки программного обеспечения, включая программное обеспечение средств защиты информации, обеспечивающие реализацию мер защиты информации, а также устранение возможных уязвимостей информационной системы, приводящих к возникновению актуальных угроз безопасности информации;
- определяются меры защиты информации при информационном взаимодействии с иными информационными системами и информационно-телекоммуникационными сетями, в том числе с информационными системами уполномоченного лица, а также при применении вычислительных ресурсов (мощностей), предоставляемых уполномоченным лицом для обработки информации;
- определяются необходимые условия для ввода ПОИБ в действие, включая назначение лиц, ответственных за обеспечение безопасности информации и эксплуатацию ПОИБ, требования к системной и сетевой инфраструктуре объектов внедрения для внедрения ПОИБ.

Результаты работ данного этапа должны быть зафиксированы в документах:

- Пояснительная записка к техническому проекту ПОИБ;
- Спецификация оборудования и программного обеспечения ПОИБ.

При проектировании ПОИБ должны использоваться СрЗИ, прошедшие сертификацию ФСТЭК России в части некриптографических методов защиты информации и ФСБ России в части криптографических методов защиты информации.

При отсутствии необходимых средств защиты информации, сертифицированных на соответствие требованиям по безопасности информации, организуется разработка (доработка) средств защиты информации и их сертификация в соответствии с законодательством Российской Федерации.

4.1.8.4 Разработка рабочей документации

На данном этапе требуется разработка рабочей документации, содержащей необходимую информацию для проведения пусконаладочных работ по внедрению ПОИБ на объектах защиты и их приемки в эксплуатацию.

Разработка рабочей документации на систему защиты информации информационной системы должна осуществляться в соответствии с техническим заданием на создание ПОИБ.

Рабочая документация на систему защиты информации информационной системы должна разрабатываться с учетом ГОСТ 34.601-90, ГОСТ 34.201-89, ГОСТ Р 51624 и должна в том числе содержать описание:

- структуры ПОИБ;
- состава, мест установки, параметров и порядка настройки средств защиты информации, программного обеспечения и технических средств;
- порядка испытаний ПОИБ.

Результаты работ данного этапа должны быть зафиксированы в документах:

- Программа и методика испытаний ПОИБ;
- Схема соединений и подключений ПОИБ;
- Чертеж установки технических средств ПОИБ.

4.1.8.5 Внедрение ПОИБ

В ходе данного этапа Исполнитель должен произвести монтаж, установку СрЗИ в соответствии с утвержденными проектными решениями, их настройку, опытную эксплуатацию и приемку.

Работы данного этапа входят:

- установка и настройка СрЗИ, входящих в систему защиты информации в соответствии с проектной документацией;
- сопровождение и консультации по реализации организационных мер защиты информации;
- проведение предварительных испытаний;
- проведение опытной эксплуатации;
- проведение анализа уязвимостей информационной системы и принятие мер защиты информации по их устранению;
- проведение приемочных испытаний.

Результатом работ данного этапа является реализованная ПОИБ, которая обеспечивает блокирование (нейтрализацию) угроз безопасности информации в Системе в соответствии с необходимым классом защищенности и соответствует требованиям ЧТЗ, решениям проектной и эксплуатационной документации.

4.1.8.6 Инструментальный анализ защищённости Системы

В ходе данного этапа производится инструментальный анализ защищённости компонент Системы с целью выявления уязвимостей.

Инструментальный анализ защищенности Системы включает в себя:

- из сети Интернет путем выполнения теста на проникновение, при проведении которого осуществляется:
  - сбор и анализ общедоступной информации об организации и ее информационных системах с помощью поисковых систем, через регистрационные базы данных (DNS, WHOIS) и другие публичные источники информации;
  - проведение инвентаризационного сканирования открытых портов и активных сервисов на внешнем сетевом периметре;
  - проведение сбора информации и формирование списка целей для атак;
  - выявление уязвимостей ресурсов внешнего сетевого периметра (включая веб-приложения), эксплуатация которых может привести к компрометации ресурса и/или использована для получения неавторизованного доступа к критичной информации;
  - разработка векторов и методов проникновения в Систему с учетом анализа полученных данных;
  - выполнение попытки получения доступа к внутренним информационным ресурсам Системы и местам хранения/обработки критичной информации.
- изнутри Системы:
  - идентификация доступных в пределах помещения организации точек беспроводного доступа и анализ возможности проникновения через них в Систему;
  - сбор информации о сетевых сервисах, доступных из сегмента пользователей Системы и определение мест возможного хранения/обработки критичной информации;

- сбор информации об операционных системах, доступных из сегмента пользователей Системы и определение мест возможного хранения/обработки критичной информации;
- сбор информации о приложениях, доступных из сегмента пользователей Системы и определение мест возможного хранения/обработки критичной информации;
- сбор информации о других информационных ресурсах, доступных из сегмента пользователей Системы и определение мест возможного хранения/обработки критичной информации;
- реализация попытки получения учетных записей и другой критичной информации путём перехвата сетевого трафика;
- выявление уязвимостей ресурсов, способных привести к возможности осуществления несанкционированных воздействий на них;
- разработка векторов и методов получения несанкционированного доступа к ключевым ресурсам Системы с учетом анализа полученных данных;
- выполнение попытки получения несанкционированного доступа к серверам с использованием уязвимостей программного обеспечения, сетевого оборудования, некорректных настроек и найденных учетных записей;
- выполнение попытки получения несанкционированного доступа к базам данных, с использованием уязвимостей программного обеспечения, сетевого оборудования, некорректных настроек и найденных учетных записей;
- выполнение попытки получения несанкционированного доступа к компьютерам пользователей с использованием уязвимостей программного обеспечения, сетевого оборудования, некорректных настроек и найденных учетных записей;
- выполнение попытки получения несанкционированного доступа к другим информационным ресурсам с использованием уязвимостей программного обеспечения, сетевого оборудования, некорректных настроек и найденных учетных записей.

По результатам инструментального анализа защищенности разрабатывается отчет об инструментальном анализе защищенности Системы.

4.1.8.7 Подготовка и проведение аттестации Системы

В ходе данного этапа Исполнитель должен произвести следующие работы в соответствии с национальными стандартами ГОСТ РО 0043-003-2012 и ГОСТ РО 0043-004-2013:

- разработку технического паспорта информационной системы;
- разработку программы и методик аттестационных испытаний;
- определение порядка, содержания, условий и методов испытаний;
- проведение оценки защищенности от несанкционированного доступа;
- проверку соответствия исходных данных реальным условиям эксплуатации;
- оценку эффективности организационных мер защиты информации;
- проведение аттестационных испытаний, включая испытания инженерного оборудования объекта информатизации, отдельных технических и программных средств, средств защиты информации;
- оформление Протокола по результатам аттестационных испытаний от несанкционированного доступа;
- оформление Заключения по результатам аттестационных испытаний;
- оформление Аттестата соответствия требованиям по безопасности (при положительном заключении по результатам аттестационных испытаний), который подтверждает соответствие Системы (объекта информатизации) требованиям безопасности информации в соответствии установленным классом защищенности / уровнем защищенности ПДн.

Результатом работ данного этапа является:

- Технический паспорт;
- Программа и методики проведения аттестационных испытаний;
- Протокол по результатам аттестационных испытаний;
- Заключение по результатам аттестационных испытаний;
- Аттестат соответствия.

4.1.9 Требования по сохранности информации при авариях

Программное обеспечение компонентов Системы, разрабатываемых и дорабатываемых в рамках настоящего ТЗ, должны автоматически восстанавливать свое функционирование при корректном перезапуске аппаратных средств.

Должна быть предусмотрена возможность организации автоматического или ручного резервного копирования данных с использованием стандартных программных и аппаратных средств.

Серверы, на которых функционирует Системы, должны быть обеспечены средствами бесперебойного электроснабжения на время не менее 30 минут для сворачивания операционной системы и приложений при прекращении первичного электроснабжения.

В случае сбоев программных средств Системы необходимо обеспечить информирование пользователей о ее временной недоступности.

Резервные копии базы данных Системы должны храниться вне информационных ресурсов Системы. Серверные мощности для хранения резервных копий предоставляются Заказчиком.

4.1.10 Требования к защите от влияния внешних воздействий

Требования к защите от влияния внешних воздействий не предъявляются.

4.1.11 Требования к патентной чистоте

Используемые при проектировании, разработке, развертывании и тестировании компонентов Системы, разрабатываемых в рамках настоящего ТЗ, инструменты разработки ПО должны быть лицензионными и не нарушать права третьих лиц.

В случае использования собственных разработок должно быть предоставлено наличие документальных свидетельств на владение интеллектуальной собственностью и авторскими правами.

Предлагаемые проектные решения в части программного обеспечения должны удовлетворять требованиям патентной чистоты, предъявляемым к программам для электронных вычислительных машин на территории Российской Федерации.

4.1.12 Требования по стандартизации и унификации

Создание Системы должно осуществляться с использованием стандартных методологий функционального и информационного моделирования.

При модернизации Системы должно использоваться общесистемное ПО известных производителей, имеющее поддержку на территории Российской Федерации, включая ОС, СУБД, серверы приложений.

При вводе однотипных данных в Системе должны использоваться единые (в рамках Системы) справочники и классификаторы для различных видов алфавитно-цифровой и текстовой информации.

Этапы создания Системы должны соответствовать требованиям Постановления Правительства Российской Федерации № 676 от 06 июля 2015 г. «О требованиях к порядку создания, развития, ввода в эксплуатацию, эксплуатации и вывода из эксплуатации государственных информационных систем и дальнейшего хранения содержащейся в их базах данных информации».

4.2 Требования к функциям (задачам), выполняемым Системой

4.2.1 Обеспечивающие подсистемы

Обеспечивающие подсистемы должны обеспечивать работу ядра Системы и включать в себя следующие подсистемы:

- Подсистема авторизации и управления доступом;
- Подсистема нормативно-справочной информации;
- Подсистема управления настройками;
- Подсистема журналирования;
- Подсистема мониторинга;
- Подсистема уведомлений;
- Подсистема формирования оперативной и аналитической отчетности.

4.2.1.1 Подсистема авторизации и управления доступом

Подсистема авторизации и управления доступом должна представлять собой единую точку авторизации для различных информационных систем научной отрасли и централизованного управления правами доступа пользователей Системы.

Подсистема авторизации и управления доступом должна обеспечивать выполнение следующих функций:

- обеспечение идентификации и аутентификации пользователей по специальным идентификаторам – именам учетных записей пользователей, обеспечение аутентификации пользователей с использованием паролей;
- обеспечение аутентификации пользователей с использованием ЕСИА;
- обеспечение интеграции с внешними системам идентификации (в том числе зарубежными);
- функции управления аутентификационной информацией пользователей:

- генерация и выдача начальной аутентификационной информации;
- защита аутентификационной информации от неправомерного доступа к ней и модифицирования;
- защита аутентификационной информации в процессе ее ввода для аутентификации от возможного использования лицами, не имеющими на это полномочий. Защита осуществляется путем исключения отображения для пользователя действительного значения аутентификационной информации. Вводимые символы пароля должны отображаться условными знаками «*»;

- управление учетными записями пользователей:
  - регистрация пользователей;
  - редактирование атрибутов карточки пользователя;
  - активация пользователей;
  - блокирование пользователей;
  - назначение пользователям ролей в подсистемах;
  - просмотр списка пользователей;
  - фильтрация списка пользователей по заданным атрибутам;
  - поиск пользователей;
- реализация ролевого метода управления доступом субъектов доступа (пользователей) к объектам доступа на основе ролей субъектов доступа:
  - регистрация ролей подсистем ЦПСИ;
  - редактирование атрибутов ролей подсистем ЦПСИ;
  - удаление ролей подсистем ЦПСИ;
  - просмотр списка ролей;
  - фильтрация списка ролей по заданным атрибутам;
  - поиск ролей;
- управление списком подсистем ЦПСИ:
  - регистрация подсистем ЦПСИ;
  - редактирование атрибутов подсистем ЦПСИ;
  - просмотр списка подсистем ЦПСИ;
  - фильтрация списка подсистем ЦПСИ по заданным атрибутам;
  - поиск подсистем ЦПСИ.

4.2.1.2 Подсистема нормативно-справочной информации

Подсистема нормативно-справочной информации (далее – Подсистема НСИ) должна быть предназначена для ведения внутренних справочников Системы.

Подсистема НСИ должна обеспечивать выполнение следующих функций:

- хранение справочников с учетом их версионности;
- просмотр списка справочников;
- поиск справочников;
- просмотр списка версий справочника;
- просмотр содержимого справочника;
- поиск по содержимому справочника;
- выгрузка содержимого справочника;
- создание версии справочника:
  - загрузка содержимого версии справочника;
  - редактирование черновика версии справочника;
- публикация версии справочника.

Подсистема должна предусматривать возможность интеграции с внешними общегосударственными сервисами такими как ЕСНСИ.

4.2.1.3 Подсистема управления настройками

Подсистема управления настройками должна быть предназначена для хранения и предоставления настроек окружения Системы и других системных настроек.

Подсистема управления настройками должна быть предназначена для настройки Системы и должна обеспечивать функцию управления настройками в соответствии с правами доступа.

Подсистема управления настройками должна обеспечивать следующие функциональные возможности:

- просмотр списка настроек;
- поиск настроек;
- создание настройки;
- переопределение общесистемных настроек на подсистему;
- редактирование настройки;
- удаление настройки;
- группировка настроек.

4.2.1.4 Подсистема журналирования

Подсистема журналирования должна быть предназначена для хранения и отображения сведений о событиях Системы.

Подсистема журналирования должна выполнять следующие функции:

- аудит действий пользователя:
  - регистрация действий пользователя;
  - просмотр журнала действий пользователей;
  - поиск событий по различным параметрам;
  - просмотр информации о событии с указанием времени, пользователя и сущности;
- аудит работы интеграционных сервисов;
  - просмотр журнала интеграционных сервисов;
  - поиск событий по различным параметрам;
  - просмотр информации о событии с указанием времени, сервиса, системы-отправителя, системы-получателя и результата обработки запроса;
- отображение журнала авторизации и сессий, а также неудачных попыток доступа;
- отображение журнала действий над объектами при изменении сущностей системы с указанием времени, пользователя и сущности.

4.2.1.5 Подсистема мониторинга

Подсистема мониторинга должна быть предназначена для поддержки бесперебойной работы системы и выполнять функцию предоставления администратору Системы возможности мониторинга ключевых параметров программно-аппаратного комплекса Системы.

Подсистема мониторинга должна позволять контролировать следующие ключевые показатели:

- аппаратная часть (состояние память, дисковых массивов):
  - объем свободной оперативной памяти;
  - активность дисковых массивов;
  - объем свободной физической памяти;
- мониторинг приложений и сервисов:
  - получение данных о времени выполнения процессов Системой;
  - получение данных о доступности Системы;
- мониторинг производительности СУБД:

- выявление проблемы транзакций;
- контроль за функциональными показателями путем выполнения прямых запросов.

4.2.1.6 Подсистема уведомлений

Подсистема уведомлений должна предоставлять следующие функциональные возможности:

- информирование пользователей о каких-либо действиях над объектами внутри Системы и/или с помощью электронного сообщения на адрес электронной почты пользователя;
- появление нового сообщения, отправленного через внутреннюю Систему уведомлений, должно сопровождаться цветовой индикацией (счетчиком непрочитанных сообщений);
- редактирование шаблонов текста уведомлений, автоматически создаваемых в подсистемах, а также включения и отключения варианта уведомления (уведомление в системе / с помощью электронного сообщения на адрес электронной почты).

Уведомления Системы должны характеризоваться следующими параметрами:

1) по компонентам Системы (настраивается для каждой подсистемы. Указывается, если надо явно выделить к какой части, объекту, сущности Системы относится уведомление. Поле несет информативный характер);
2) по уровню важности:
   - важный;
   - информация;
   - ошибка;
   - предупреждение;
3) по способу информирования:
   - центр уведомления;
   - email – уведомления отправляются на адреса электронной почты пользователей, указанные в их учетных записях;
4) по способу формирования:
   - автоматические (или системные уведомления, формируются в ходе выполнения операций в прикладных модулях);
   - ручные (через пользовательский интерфейс администратора Системы);
5) по типу получателей:

- пользователь;
- всем пользователям.

4.2.1.7 Подсистема формирования оперативной и аналитической отчетности

Подсистема формирования оперативной и аналитической отчетности должна быть предназначена для консолидации значений основных статистических и качественных показателей, касающихся автоматизируемой Системой деятельности, их обработки и представления, позволяющих руководству Заказчика оперативно принимать управленческие решения.

Подсистема формирования оперативной и аналитической отчетности должна включать в себя следующие блоки:

- модуль оперативного анализа данных;
- модуль отчетности;
- модуль «Аналитические панели»;
- модуль «Хранилище данных».

4.2.1.7.1 Модуль оперативного анализа данных

Модуль оперативного анализа данных должен позволять конструировать интерактивные аналитические таблицы в терминах многомерной базы и предметной области (меры, размерностей, атрибуты, иерархии) – OLAP-представления. OLAP-представление должно представлять собой инструмент анализа данных, предназначенный для определения, агрегации, фильтрации значений числовых показателей (мер) на пересечениях различных аналитических срезов (размерностей).

Модуль должен позволять пользователю самостоятельно в веб-интерфейсе подсистемы выбирать источник данных для OLAP-представления. OLAP-представление на основании структуры источника данных должно отображать все имеющиеся в нем размерности и меры. Должна быть реализована возможность произвольно в качестве строк или столбцов располагать интересующие для анализа размерности, а также выбирать необходимые меры. В отношении таблицы OLAP-представления должна быть доступна фильтрация по произвольному набору использованных в ней мер и размерностей, сортировка по возрастанию и убыванию.

Помимо табличного вида, должен быть предусмотрен графический вид OLAP-представления: графики, диаграммы, гистограммы. Должна быть реализована возможность изменять визуальный стиль выводимой информации (цвет, форматирование

текста/чисел и пр.). Возможности по изменению визуального стиля должны зависеть от способа представления информации (таблица, график, диаграмма).

Подсистема должна позволять сохранять настроенные OLAP-представления с заданием имени. Должен быть реализован реестр OLAP-представлений с возможностью поиска, создания, изменения и удаления OLAP-представлений.

4.2.1.7.2 Модуль отчетности

Модуль отчетности должен быть предназначен для формирования отчетности, возникающей в процессе исследований, и систематизации сбора информации с участников научного сообщества и организаций, использующих Систему.

Модуль отчетности должен обеспечивать выполнение следующих функций:

- заполнение и формирование форм проектной отчетности;
- настройка интерактивных веб-форм для сбора показателей в виде опросов пользователей Системы (включая организации);
- заполнение интерактивных веб-форм пользователями Системы (включая организации).

Перечень заполняемых и формируемых в модуле отчетных форм должен быть определен и согласован с Заказчиком на этапе технического проектирования.

4.2.1.7.3 Модуль «Аналитические панели»

Модуль «Аналитические панели» должен быть предназначен для работы с аналитическими панелями. Аналитическая панель должна представлять собой набор виджетов (OLAP-представлений) с различными способами визуализации (таблицы, графики, диаграммы), размещенными на экране в определенном порядке.

Модуль «Аналитические панели» должен обеспечивать выполнение следующих функций:

- просмотр списка информационных панелей, доступных пользователю;
- создание аналитических панелей, включающих одно или более OLAP-представление;
- настройка расположения OLAP-представлений на аналитической панели, в том числе:
  - распределение OLAP-представлений на аналитической панели;
  - настройка высоты и ширины окна визуального представления;
  - вставка вкладок, заголовков и разделителей.

4.2.1.7.4 Модуль «Хранилище данных»

Модуль «Хранилище данных» должен быть предназначен для хранения информации, используемой для оперативного анализа, собираемых показателей, а также метаописаний OLAP-представлений и аналитических панелей.

Модуль «Хранилище данных» должен обеспечивать выполнение следующих функций:

- управление списком подключений к базам данных, предоставляющим информацию для оперативного анализа;
- управление списком источников данных (кубов или витрин данных) для OLAP-представлений, включая создание, изменение, удаление источников данных;
- настройка источников данных, включая список возможных мер и размерностей источника данных;
- хранение информации, загружаемой из внешних баз данных, и используемой в Модуле оперативного анализа данных.

4.2.2 Интеграционная шина ЦПСИ

Интеграционная шина ЦПСИ должна быть предназначена для организации централизованного и унифицированного событийно-ориентированного обмена сообщениями между подсистемами ЦПСИ, построенное на основе сервисно-ориентированной архитектуры.

Интеграционная шина должна обеспечивать следующие функциональные возможности:

- синхронный и асинхронный режимы обмена сообщениями с использованием протокола REST;
- управление настройками информационного взаимодействия с использованием интерфейса пользователя:
  - настройка адресов;
  - настройка параметров;
- гарантированная доставка сообщений.

4.2.3 Подсистема интеграционного взаимодействия

Подсистема интеграционного взаимодействия должна быть предназначена для организации централизованного и унифицированного событийно-ориентированного обмена сообщениями с внешними информационными системами, при наличии сервисов интеграционного взаимодействия со стороны внешних информационных систем.

Подсистема интеграционного взаимодействия должна обеспечивать обмен данными через единые центры, в которых обеспечивается маршрутизация и сохранность данных.

Подсистема интеграционного взаимодействия должна включать в себя адаптеры, автоматизирующие процессы получения, сбора, обработки и отправки сообщений между ЦПСИ и внешними информационными системами:

- адаптер интеграции с внешними источниками данных:
  - ЕСНСИ
- адаптер интеграции с реферативными базами данных:
  - ИС верификации публикационной активности.

Итоговый перечень интеграций должен быть определен и согласован с Заказчиком на этапе технического проектирования.

4.2.4 Подсистема «Цифровой профиль исследователя»

Подсистема «Цифровой профиль исследователя» должна быть предназначена для формирования досье исследователя, обеспечивающего учет наукометрической информации и достижений, с целю упрощения процедур подачи конкурсных заявок и коллаборации с научно-исследовательскими командами.

В Подсистеме «Цифровой профиль исследователя» должна быть реализована возможность формирования персональной страницы исследователя, содержащей следующие разделы:

- раздел «Персональная информация»;
- раздел «Публикационная активность»;
- раздел «Проведенные НИР».

4.2.4.1 Раздел «Персональная информация»

Раздел «Персональная информация» должен позволять заполнять следующие регистрационные сведения об исследователе:

- фамилия;
- имя;
- отчество;
- фамилия на английском;
- имя на английском;
- дата рождения;
- пол;
- личная фотография;

- страна проживания;
- регион проживания;
- адрес электронной почты;
- телефон;
- образование;
- места работы, включая сведения о занимаемых должностях;
- научные степени;
- области знаний;
- идентификаторы в реферативных базах и патентных системах.

Итоговый перечень сведений должен быть определен и согласован с Заказчиком на этапе технического проектирования.

4.2.4.2 Раздел «Публикационная активность»

Раздел «Публикационная активность» должен позволять отображать данные о статьях, автором которых является исследователь:

- название статьи;
- авторы;
- идентификатор научной публикации (DOI);
- издание (Журнал).

Раздел должен формироваться автоматически, на основании данных, полученных из ИС «Верификации публикационной активности». Данные, поступившие из ИС «Верификации публикационной активности», не должны быть доступны для редактирования пользователем.

В разделе должна быть реализована возможность добавления пользователем сведений о научных статьях, автором которых он является. Статьи, внесенные пользователем, должны быть помечены как не подтвержденные автоматически.

Раздел должен обеспечивать раздельный учет статей, введенных пользователем вручную, и статей, сведения о которых получены посредством информационного сопряжения с ИС «Верификации публикационной активности».

4.2.4.3 Раздел «Проведенные НИР»

Раздел «Проведенные НИР» должен быть предназначен для учета сведений о проведенных НИР.

В разделе должно быть организовано отображение:

- сведений о научных работах, внесенных в подсистеме «Научная тема».

В разделе должна быть реализована возможность ручного указания исследователем сведений о завершенных ранее НИР для научных тем, финансирование которых осуществлялось не в рамках государственного финансирования.

4.2.5 Подсистема «Цифровой профиль организации»

Подсистема «Цифровой профиль организации» должна быть предназначена для формирования досье организации, ведущей научную деятельность. В подсистеме должна быть реализована возможность формирования страницы организации, содержащей следующие разделы:

- раздел «Общие сведения об организации»;
- раздел «Участие в грантах и конкурсах»;
- раздел «Сотрудники организации».

4.2.5.1 Раздел «Общие сведения об организации»

Раздел «Общие сведения об организации» должен содержать сведения об организации:

- полное наименование организации;
- краткое наименование организации;
- руководитель организации;
- адрес организации;
- телефон организации.

4.2.5.2 Раздел «Участие в грантах и конкурсах»

Раздел «Участие в грантах и конкурсах» должен содержать сведения об участии организации и/или сотрудников организации в грантах и конкурсах. Перечень сведений должен формироваться на основании сведений, заполненных подсистеме «Гранты и конкурсы».

4.2.5.3 Раздел «Сотрудники организации»

Раздел «Сотрудники организации» должен содержать список сотрудников, работающих в организации. Перечень сведений о проекте должен формироваться на основании сведений, заполненных в Подсистеме «Цифровой профиль исследователя».

4.2.6 Подсистема «Научная тема»

Подсистема «Научная тема» должна быть предназначена для комплексного учета сведений о реализуемом научно-исследовательском проекте. В подсистеме должна быть реализована возможность формирования страницы проекта, содержащей следующие разделы:

- раздел «Паспорт проекта»;
- раздел «Команда проекта».

4.2.6.1 Раздел «Паспорт проекта»

В разделе «Паспорт проекта» должна быть реализована возможность заполнения основной информации по проекту:

- научное направление в соответствии с паспортом специальностей ВАК;
- организация, на базе которой проходит исследование;
- финансирование по годам;
- привлеченные гранты;
- вид исследования (фундаментальное, прикладное, инновационное предпринимательство);
- публикации в рамках исследования, путем выбора из списка публикаций членов команды научной темы;
- доклады на конференциях;
- ссылка на официальный сайт;
- партнеры и источники финансирования;
- фотографии или графические материалы.

4.2.6.2 Раздел «Команда проекта»

Раздел «Команда проекта» должен быть предназначен для указания сведений о сотрудниках, задействованных на различных этапах жизненного цикла проекта. В разделе должны быть предусмотрены функции:

- указания сведений об участниках проекта путем добавления цифровых профилей исследователей;
- присвоения участнику проекта роли руководителя проекта.

4.2.7 Подсистема «Гранты и конкурсы»

Подсистема «Гранты и конкурсы» должна быть предназначена для получения информации о всех проводимых грантах и конкурсах с возможностью подачи заявки на участие.

Подсистема «Гранты и конкурсы» должна состоять из следующих разделов:

- раздел «Единый реестр грантов и конкурсов»;
- раздел «Публикация грантов и конкурсов»;
- раздел «Заявки на участие в грантах и конкурсах».

4.2.7.1 Раздел «Единый реестр грантов и конкурсов»

Раздел «Единый реестр грантов и конкурсов» должен быть предназначен для формирования единого реестра актуальных грантов и конкурсов для ученых и предпринимателей.

Формирование единого реестра должно быть основано на сведениях, предоставляемые системами:

- КИАС РФФИ;
- ИАС РНФ;
- АИСУ ФЦП.

Модуль «Единый реестр грантов и конкурсов» должен содержать следующие сведения:

- название;
- сумма (при наличии);
- возможные участники;
- сроки;
- файлы с документацией (при наличии).

Итоговый перечень интеграций и сведений должен быть определен и согласован с Заказчиком на этапе технического проектирования.

4.2.7.2 Раздел «Публикация грантов и конкурсов»

Раздел «Публикация грантов и конкурсов» предназначен для создания и публикации грантов и конкурсов через ЦПСИ. Раздел должен обеспечивать следующие функциональные возможности:

- просмотр списка грантов и конкурсов по своей организации;
- ввод сведений о гранте или конкурсе;

- публикация гранта или конкурса;
- редактирование гранта или конкурса;
- отмена гранта или конкурса;
- экспертиза научного проекта, на который был выделен грант.

4.2.7.3 Раздел «Заявки на участие в грантах и конкурсах»

Раздел «Заявки на участие в грантах и конкурсах» должен быть предназначен для работы с заявками на гранты и конкурсы в ЦПСИ. Раздел должен обеспечивать следующие функциональные возможности:

1) подача заявок на гранты и конкурсы исследователями или организациями, включая:
   - подачу индивидуальной заявки на участие в гранте или конкурсе;
   - подачу совместной заявки от нескольких исследователей или организаций;
   - отображение списка поданных заявок;
   - отслеживание поданной заявки;
   - отображение результата;
2) анализ откликов на участие в грантах и конкурсах, включая:
   - отображение списка откликов;
   - выбор победителей гранта или конкурса;
   - завершение конкурса с возможностью прикрепления подтверждающих документов (протокола, выписки из протокола конкурсной комиссии или другое).

4.2.8 Открытый портал ЦПСИ

Открытый портал ЦПСИ должен быть предназначен для публикации открытых данных об осуществляемой научно-исследовательской работе, научных организациях и коллективах, аналитической информации.

Портал должен быть организован в виде тематических разделов, обеспечивающих навигацию по порталу и возможность перехода между разделами. Портал должен предоставлять возможность поиска информации внутри раздела с использованием текстовых запросов и тематических фильтров.

Открытый портал должен включать в себя следующие разделы:

- раздел «Научные проекты»;
- раздел «Аналитика».

4.2.8.1 Раздел «Научные проекты»

Раздел «Научные проекты» должен быть предназначен для предоставления информации о планируемых, реализуемых и завершенных научно-исследовательских проектах. Список научных проектов должен формироваться на основе сведений, заполненных в Подсистеме «Научная тема».

Раздел должен обеспечивать возможность поиска научного проекта по запросам:

- исследовательская организация;
- научное направление;
- вид исследования;
- участники проекта;
- период реализации проекта;
- партнеры и источники финансирования.

Полный перечень отображаемых в разделе сведений и фильтров должен быть определен Исполнителем и согласован с Заказчиком на этапе разработки технического проекта.

4.2.8.2 Раздел «Аналитика»

Раздел «Аналитика» должен быть предназначен для просмотра открытых данных о количественных показателях научной деятельности на основе сведений, размещаемых в Системе.

Раздел должен поддерживать вывод показателей с помощью различных способов представления: таблицы графики, диаграммы, карта мира и субъектов РФ.

В разделе должны быть представлены данные о следующих показателях научной деятельности:

- сведения о количестве грантов, конкурсов и объемах финансирования научных проектов в разрезе источников финансирования и организаций;
- сведения о количестве научных и коммерческих организаций, проектов в разрезе направлений деятельности, территориальной принадлежности;
- сведения о результатах научной деятельности (количество научных публикаций, зарегистрированных РИД) по различным направлениям;
- сведения о количестве исследователей, задействованных на научных проектах, и потребности в специалистах на основе данных об открытых вакансиях.

4.2.9 Подсистема обеспечения информационной безопасности (ПОИБ)

ПОИБ должна обеспечивать защиту информации от неправомерного или случайного доступа к ней, уничтожения, изменения, блокирования, копирования, предоставления, распространения, а также от иных неправомерных действий в отношении защищаемой информации.

В состав ПОИБ должны входить организационные и технические меры, обеспечивающие:

- защиту машинных носителей информации;
- регистрацию событий безопасности;
- антивирусную защиту;
- обнаружение вторжений;
- контроль (анализ) защищенности информации;
- целостность информационной системы;
- защиту среды виртуализации;
- защиту технических средств;
- защиту передачи данных.

4.2.9.1 Требования по защите машинных носителей информации

Применяемые для построения ПОИБ организационные и технические меры должны обеспечивать:

- уничтожение (стирание) или обезличивание информации на машинных носителях при их передаче между пользователями, в сторонние организации для ремонта или утилизации, а также контроль уничтожения (стирания) или обезличивания.

4.2.9.2 Требования по регистрации событий безопасности

Применяемые для построения ПОИБ организационные и технические меры должны обеспечивать:

- определение событий безопасности, подлежащих регистрации, и сроков их хранения;
- определение состава и содержания информации о событиях безопасности, подлежащих регистрации;
- сбор, запись и хранение информации о событиях безопасности в течение установленного времени хранения;
- защиту информации о событиях безопасности.

4.2.9.3 Требования по антивирусной защите

Применяемые для построения ПОИБ организационные и технические меры должны обеспечивать:

- реализацию антивирусной защиты;
- обновление базы данных признаков вредоносных компьютерных программ (вирусов).

4.2.9.4 Требования по обнаружению вторжений

Применяемые для построения ПОИБ организационные и технические меры должны обеспечивать:

- обнаружение вторжений;
- обновление базы решающих правил и сигнатур атак.

4.2.9.5 Требования по контролю (анализу) защищенности

Применяемые для построения ПОИБ организационные и технические меры должны обеспечивать:

- выявление, анализ уязвимостей информационной системы и оперативное устранение вновь выявленных уязвимостей;
- контроль установки обновлений программного обеспечения, включая обновление программного обеспечения средств защиты информации;
- контроль работоспособности, параметров настройки и правильности функционирования программного обеспечения и средств защиты информации;
- контроль состава технических средств, программного обеспечения и средств защиты информации.

4.2.9.6 Требования по обеспечению целостности

Применяемые для построения ПОИБ организационные и технические меры должны обеспечивать:

- возможность восстановления программного обеспечения, включая программное обеспечение средств защиты информации, при возникновении нештатных ситуаций.

4.2.9.7 Требования по защите среды виртуализации

Применяемые для построения ПОИБ организационные и технические меры должны обеспечивать:

- идентификацию и аутентификацию субъектов доступа и объектов доступа в виртуальной инфраструктуре, в том числе администраторов управления средствами виртуализации;
- управление доступом субъектов доступа к объектам доступа в виртуальной инфраструктуре, в том числе внутри виртуальных машин;
- регистрацию событий безопасности в виртуальной инфраструктуре;
- реализацию и управление антивирусной защитой в виртуальной инфраструктуре;
- разбиение виртуальной инфраструктуры на сегменты (сегментирование виртуальной инфраструктуры) для обработки информации отдельным пользователем и (или) группой пользователей.

4.2.9.8 Требования по защите технических средств

Применяемые для построения ПОИБ организационные и технические меры должны обеспечивать:

- контроль и управление физическим доступом к техническим средствам, средствам защиты информации, средствам обеспечения функционирования, а также в помещения и сооружения, в которых они установлены, исключающие несанкционированный физический доступ к средствам обработки информации, средствам защиты информации и средствам обеспечения функционирования информационной системы, в помещения и сооружения, в которых они установлены;
- размещение устройств вывода (отображения) информации, исключающее ее несанкционированный просмотр.

4.2.9.9 Требования по защите передачи данных

Применяемые для построения ПОИБ организационные и технические меры должны обеспечивать:

- защиту информации от раскрытия, модификации и навязывания (ввода ложной информации) при ее передаче (подготовке к передаче) по каналам связи, имеющим выход за пределы контролируемой зоны.

4.3 Требования к видам обеспечения

4.3.1 Требования к математическому обеспечению Системы

Математические методы и алгоритмы, используемые для обработки информации, должны обеспечивать актуальность и достоверность предоставляемых пользователю результатов и предоставляются Исполнителю Заказчиком на этапе технического проектирования.

Математические методы и алгоритмы, используемые для шифрования/ дешифрования данных, а также программное обеспечение, реализующее их, должны быть сертифицированы уполномоченными организациями для использования в государственных органах Российской Федерации.

4.3.2 Требования к информационному обеспечению Системы

4.3.2.1 Требования к составу, структуре и способам организации данных в Системе

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

4.3.2.2 Требования по применению систем управления базами данных

Хранение структурированных данных в Системе должно быть обеспечено функциями реляционной СУБД (далее – РСУБД), относящихся к СПО или включенных в Реестр отечественного ПО. Для обеспечения целостности данных должны использоваться встроенные механизмы РСУБД.

Хранение бинарных данных (документы, графические материалы и т.п.) должно обеспечиваться файловым хранилищем.

В рамках технического проектирования Исполнителем должно быть выработано техническое решение о способах взаимодействия между РСУБД и файловым хранилищем.

Средства РСУБД, а также средства используемых операционных систем должны обеспечивать протоколирование обрабатываемой в Системе информации.

Структура базы данных должна поддерживать хранение и обработку информации в соответствии с классификаторами (там, где они применимы).

Система должна позволять обеспечивать резервное копирование и восстановление данных.

4.3.2.3 Требования к структуре процесса сбора, передачи и представления доступа к данным в Системе

Доступ к данным должен учитывать ролевую модель Системы: часть данных доступна пользователям без авторизации, авторизованным пользователям предоставляется доступ к более широкому набору данных с учетом категории запрашиваемой информации.

Сведения для реализации разделения доступа должны быть предоставлены Заказчиком Исполнителю до начала этапа разработки технического проекта.

4.3.3 Требования к защите данных от разрушений при авариях и сбоях в электропитании системы

Для обеспечения сохранности информации при аварийных ситуациях в Системе должны быть предусмотрены средства обеспечения бесперебойного питания, дублирования информации.

Средства бесперебойного питания должны обеспечивать работоспособность АПК при импульсных помехах и перерывах в электропитании длительностью до 30 минут.

4.3.4 Требования к контролю, хранению, обновлению и восстановлению данных

Система должна контролировать корректность вводимой информации, а также проверять логическую целостность информации в БД при выполнении операций с БД.

В Системе должно быть предусмотрено резервное копирование (архивирование) информации из БД.

Система должна протоколировать все события, связанные с изменением своего информационного наполнения.

4.3.5 Требования к лингвистическому обеспечению Системы

Система должна разрабатываться с учётом необходимости выполнения следующих общих требований:

- создание Системы должно выполняться с использованием современных методов проектирования и средств разработки приложений;
- взаимодействие всех пользователей с Системой должно осуществляться на языке, выбранном пользователем. В Системе, создающейся на основании настоящего Технического задания, должен быть предусмотрен выбор между русским и английским языком. Исключения могут составлять только системные сообщения, не подлежащие переводу с английского языка;

- для разработки Системы должны использоваться компилируемые языки программирования высокого уровня;
- для информационного обмена с внешними и смежными системами могут использоваться универсальный язык разметки документов – XML или текстовый формат обмена данными JSON.

4.3.6 Требования к программному обеспечению Системы

Программное обеспечение Системы представляет собой совокупность общесистемного и специального программного обеспечения. Программное обеспечение системы должно обладать открытой, модульной архитектурой, обеспечивающей возможность эволюционного развития Системы.

Общесистемное программное обеспечение Системы должно представлять собой совокупность программных средств со стандартными интерфейсами, предназначенных для организации и реализации информационно-вычислительных процессов в Системе. Состав общесистемного программного обеспечения формируется на этапе разработки технического проекта.

Общесистемное программное обеспечение Системы должно быть сертифицировано (в том числе по требованиям безопасности информации) или иметь соответствующие сертификаты для использования на территории Российской Федерации. Вопросы его использования и тиражирования должны регулироваться соответствующими соглашениями или сублицензионными договорами, а также положениями Постановления Правительства Российской Федерации от 16 ноября 2015 года № 1236 «Об установлении запрета на допуск программного обеспечения, происходящего из иностранных государств, для целей осуществления закупок для обеспечения государственных и муниципальных нужд» (вместе с «Правилами формирования и ведения единого реестра российских программ для электронных вычислительных машин и баз данных», «Порядком подготовки обоснования невозможности соблюдения запрета на допуск программного обеспечения, происходящего из иностранных государств, для целей осуществления закупок для обеспечения государственных и муниципальных нужд»).

Специальное программное обеспечение Системы должно соответствовать требованиям к общесистемным компонентам, а также должно учитывать следующие основные принципы:

- должно быть реализовано на базе отечественных программных разработок;
- возможность использования облачных технологий для хранения и обработки данных;

- минимальная номенклатура используемых программных средств;
- масштабируемость и высокая производительность;
- совместимость;
- наличие встроенной системы безопасности;
- надежность и отказоустойчивость;
- использование свободно распространяемых компонентов.

Разработанное специальное обеспечение Системы должно обеспечивать:

- функциональную полноту – реализацию всех подлежащих автоматизации функций объекта автоматизации;
- возможность адаптации и настройки программных средств с учетом специфики объекта автоматизации;
- эргономичность – обеспечение удобства и унификации пользовательского интерфейса;
- защиту от ошибочных действий оператора (пользователя);
- контроль и защиту от некорректных исходных данных.

4.3.7 Требования к техническому обеспечению Системы

Техническое обеспечение Системы должно обеспечивать работу в соответствии с показателями назначения и создаваться на базе современных вычислительных средств и совместимого с ними периферийного оборудования.

Требования к техническому обеспечению Системы должны быть определены на этапе разработки технического проекта, который должен содержать требования к организации следующих подсистем:

- кабельная подсистема;
- вычислительная подсистема (серверная подсистема);
- сетевая подсистема;
- подсистема хранения данных;
- подсистема резервного копирования;
- подсистема управления;
- подсистема виртуализации;
- подсистема информационной безопасности;
- подсистема авторизации и аутентификации;
- подсистема обновления программного обеспечения;
- подсистема мониторинга;

- подсистема времени;
- подсистема пользователей;
- инженерная подсистема.

4.3.7.1 Требования к кабельной подсистеме

Кабельная подсистема ядра сети должна обеспечивать передачу трафика приложений на скоростях не ниже 10 Гбит/с и соответствовать международным, и российским сетевым стандартам с учетом обеспечения требуемой скорости передачи данных и задержек не более чем 1 мс при нагрузке не более 80% и обеспечивать передачу трафика сети хранения данных стандарта Fibre Channel на скоростях не ниже 16 Гбит/с и соответствовать международным и российским сетевым стандартам с учетом обеспечения требуемой скорости и стандарта передачи данных.

В случае, если в ходе проектирования и расчетов необходимой производительности системы будет выявлена необходимость увеличения каких-либо параметров, Исполнитель вправе, по согласованию с Заказчиком, использовать более высокие требования.

Кабельная подсистема должна обеспечивать резервирование всех каналов передачи данных.

4.3.7.2 Требования к вычислительной подсистеме (серверной подсистеме)

Серверная подсистема предназначена для предоставления вычислительных мощностей компонентам Системы для решения функциональных задач и должна включать в свой состав следующие компоненты:

- виртуализируемые вычислительные узлы;
- выделенные вычислительные узлы.

Проектные решения по виртуализируемым вычислительным узлам должны формировать общий пул ресурсов для подсистемы виртуализации. Выделенные вычислительные узлы должны предоставлять вычислительные мощности для систем/ подсистем, виртуализация которых невозможна.

Проектные решения по серверной подсистеме должны обеспечивать необходимую производительность Системы с учетом выполняемых функций, обрабатываемой информации, перечня интегрируемых смежных систем.

В рамках проектирования Исполнителем должен быть представлен расчет производительности и состава серверной подсистемы.

4.3.7.3 Требования к сетевой подсистеме

Проектные решения по составу сетевой подсистемы должны включать средства межсетевого экранирования с функциями маршрутизации, коммутационное оборудование для передачи трафика приложений, коммутационное оборудование сети хранения данных.

В сетевой подсистеме планируется иметь модульную иерархическую архитектуру, предусматривающую дальнейшее масштабирование по производительности и портовой ёмкости.

Проектные решения по иерархии сетевой подсистемы должны обеспечиваться наличием следующих уровней:

- уровень ядра сети;
- уровень доступа.

Исполнитель должен спроектировать сегментирование сети передачи данных в зависимости от обрабатываемых данных, предназначения, приоритизации и требований информационной безопасности. По меньшей мере в отдельные сегменты должны быть выделены:

- сегмент трафика приложений;
- сегмент управления;
- сегмент демилитаризованной зоны;
- сегмент пользователей;
- сегмент серверного оборудования;
- сегмент подсистемы хранения данных.

Проектные решения по сетевой подсистеме должны включать в себя активное сетевое оборудование уровня ядра и доступа. Уровень ядра сегмента передачи данных транспортной подсистемы должен обеспечивать маршрутизацию трафика сети передачи данных и взаимодействие с сетевым оборудованием смежных систем. Уровень ядра сегмента передачи данных транспортной подсистемы должен обеспечивать подключение оборудования подсистемы вычислительных комплексов и подсистемы хранения данных.

Сетевая подсистема на уровне ядра должна обеспечивать резервирование каналов передачи данных и сетевого оборудования с автоматическим переключением между ними. Скорость сети передачи данных уровня ядра между всеми участниками должна составлять не менее 10 Гбит/с.

Проектные решения по передаче данных между всеми серверами (физическими и виртуальными) и подсистемами (за исключением подключения пользователей) должны осуществляться на уровне ядра сети.

Сетевая подсистема трафика приложений должна обеспечивать передачу трафика на скоростях не менее 10 Гбит/с и временем задержек не более 1 мс при загрузке оборудования не более чем на 80%.

Доступ пользователей к системе должен осуществляться на скорости не менее 1 Гбит/с и временем задержек не более 1 мс при загрузке оборудования не более чем на 80%.

Скорость взаимодействия с каждой из сторонних систем должна рассчитываться Исполнителем исходя из параметров взаимодействия.

Сетевая подсистема хранения данных должна быть спроектирована с использованием технологии Fibre Channel и скорости передачи данных не ниже 16 Гбит/с.

В качестве коммутационного и маршрутизирующего оборудования трафика должно быть спроектировано оборудование с возможностью расширения.

4.3.7.4 Требования к подсистеме хранения данных

Подсистема хранения данных должна включать следующие компоненты:

- устройства хранения (дисковые массивы, системы хранения данных);
- сеть хранения данных.

Устройства хранения должны обеспечивать необходимый объем хранения и предоставлять функциональным и обеспечивающим подсистемам данные в минимальных временных интервалах и обеспечивать надежное хранение данных за счет использования отказоустойчивых технологий.

В ходе проектных работ Исполнитель должен выполнить расчет необходимого объема дискового пространства подсистемы хранения данных и ее производительности для размещения данных Системы. Объем системы хранения данных должен обеспечить хранение данных Системы в течение 5 лет без необходимости модернизации.

В проектных решениях по подключению устройств хранения к серверному оборудования должны быть предусмотрены по технологии Fibre Channel на скорости каждого канала не менее 16 Гбит/с.

В рамках проектирования следует учесть, что сеть хранения данных должна обеспечивать скорость передачи данных не менее 16 Гбит/с.

Проектные решения по подключению к дисковым полкам должны основываться на использовании интерфейса SAS со скоростью не менее 12 Гбит/с.

В рамках проектирования должно быть учтено, что устройства хранения должны иметь в составе не менее двух контроллеров управления. В каждом контроллере должно быть не менее 32 Гбайт кэш-памяти.

Для обеспечения сбалансированности показателей производительности и объема хранения в системе хранения должны быть спроектированы диски 3 типов: SSD, SAS со скорость вращения 15000 об/с и SAS со скоростью вращения 7200 об/с. Функциональные возможности подсистемы хранения данных должны обеспечивать возможность автоматического перемещения данных между дисками в зависимости от частоты обращения к ним.

Проектные решения по применяемой системе хранения данных должны быть не ниже, чем корпоративного класса и отвечать последним технологическим решениям.

В рамках проектирования Исполнителем должен быть представлен обоснованный расчет подсистемы хранения и ее состава.

4.3.7.5 Требования к подсистеме резервного копирования

Проектные решения по подсистеме резервного копирования и восстановления данных должны обеспечивать выполнение следующих функций:

- периодическое архивирование различных массивов данных;
- дублирование критически важных элементов Системы, выход из строя которых может привести к отказу работоспособности Системы;
- извлечение данных из архива и запись их в соответствующий массив;
- хранение и учет копий данных.

Подсистема резервного копирования должна состоять из:

- системы хранения резервных копий;
- программно-аппаратного комплекса резервного копирования.

Проектные решения должны обеспечивать резервное копирование информации без создания дополнительной нагрузки на сетевую подсистему трафика приложений при резервном копировании виртуальных серверов. Процесс резервного копирования должен быть спроектирован без необходимости остановки работы подсистем Системы, физических и/или виртуальных серверов.

Проектные решения по подключению системы хранения резервных копий должны осуществляться с использованием сетевых интерфейсов со скоростью не менее 10 Гбит/с.

Проектные решения по подсистеме резервного копирования должны обеспечивать выборочное восстановление информации, в том числе отдельных файлов и объектов.

Проектные решения по хранению резервных копий должны обеспечивать автоматическое сжатие информации, хранящейся на ней, а также ее дедупликацию.

В ходе проектных работ Исполнитель должен рассчитать количественные и технические параметры подсистемы резервного копирования, в том числе объем системы хранения резервных копий, производительность программно-аппаратного комплекса.

Проектные решения по подсистеме резервного копирования должны быть рассчитаны на хранение информации в течение сроков, предусмотренных законодательством Российской Федерации.

4.3.7.6 Требование к подсистеме управления

Подсистема управления предназначена для управления и информационного обеспечения Системы.

Проектные решения по подсистеме управления должны быть вынесены в отдельный сетевой сегмент и отделены от иных подсистем средствами межсетевого экранирования, должны позволять осуществлять управление всеми подсистемами Системы. Управление должно осуществляться централизованно.

4.3.7.7 Требования к подсистеме виртуализации

Подсистема виртуализации предназначена для повышения надежности и оптимизации вычислительных ресурсов Системы.

Проектные решения по подсистеме виртуализации должны включать в свой состав следующие компоненты:

- гипервизоры;
- виртуальные машины (серверы);
- управляющий модуль.

Конфигурация и требования к подсистеме виртуализации уточняются на этапе проектирования.

Подсистема виртуализации должна проектироваться с применением технологий обеспечения высокой доступности виртуальных машин.

В рамках проектирования подсистема виртуализации должна быть спроектирована не ниже, чем для корпоративного класса.

Проектные решения по подсистеме виртуализации должны иметь сертификат соответствия ФСТЭК России от НСД или для нее должны быть спланированы специальные средства защиты от НСД.

4.3.7.8 Требования к подсистеме информационной безопасности

В ходе проектирования Системы и определения требований к системе защиты

информации Исполнитель должен предусмотреть все необходимые ресурсы для размещения системы защиты информации.

4.3.7.9 Требования к подсистеме авторизации и аутентификации

В Системе должна быть спроектирована централизованная система авторизации и аутентификации пользователей и серверов, централизованное управление правами и ролями пользователей, доступом к серверам.

4.3.7.10 Требования к подсистеме обновления программного обеспечения

В Системе должна быть спроектирована подсистема обновления программного обеспечения, позволяющая обновлять версии прошивок серверного, коммутационного оборудования и системы хранения данных, а также система обновления системного и прикладного программного обеспечения.

4.3.7.11 Требования к подсистеме мониторинга

Проектные решения по подсистеме мониторинга должны обеспечивать круглосуточный мониторинг всего серверного и коммутационного оборудования, системы хранения данных, системного и прикладного ПО и иметь возможность незамедлительного информирования администраторов о сбое, должны иметь сенсоры для мониторинга системного и прикладного ПО, с учетом их функциональных возможностей.

4.3.7.12 Требования к подсистеме времени

Проектные решения по оборудованию, системному и прикладному программному обеспечению должны использовать централизованную локальную систему времени, которая в свою очередь синхронизируется с глобальными (мировыми) системами (серверами) времени.

4.3.7.13 Требования к инженерной подсистеме

Исполнитель, с учетом места расположения и технических особенностей помещений, где планируется разметить Систему, должен разработать проектное решение по инженерной подсистеме.

Проектные решения по инженерной подсистеме должны включать в себя средства электропитания, резервные средства электропитания, источники бесперебойного питания, средства кондиционирования воздуха, заземления, средства приточной вентиляции, серверные стойки, фальшпол и потолок, освещение, резервное освещение, пожарная и

охранная сигнализация, средства пожаротушения, систему контроля доступа, систему видеонаблюдения и т.д.

Инженерная подсистема должна соответствовать российским и международным стандартам к серверным помещениям и/или центрам обработки данных с учетом требований по отказоустойчивости.

Проектные решения по инженерной подсистеме должны позволять обеспечить возможность работы Системы в соответствии с требованиями безопасности информации, рекомендациями производителей оборудования, международных и российских стандартов, ГОСТов и рекомендаций.

Количество и технические параметры серверного, коммутационного оборудования (в том числе средств межсетевого экранирования), систем хранения данных, системы резервного копирования должно быть определены в ходе проектирования и обоснованы расчетным методом, экономическими показателями, а также методом сравнительного анализа с оборудованием иных производителей.

В проектной документации должен быть обозначен подробный перечень оборудования, комплектующих и программного обеспечения Системы с указанием их количества и моделей.

В Системе должно быть спроектировано применение серверного, коммутационного оборудования и СХД корпоративного класса.

Проектное решение по инженерной подсистеме должно обеспечить ее работоспособность 24 часа, 7 дней в неделю, 365 дней в году.

4.3.7.14 Требования к резервированию

В ходе проектирования Системы все ее подсистемы должны быть зарезервированы. В Системе не должно быть единой точки отказа.

Все проектируемые технические решения должны быть согласованы с Заказчиком и по указанию Заказчика с иными заинтересованными ведомствами.

4.3.7.15 Требования к размещению технических средств

При проведении работ по проектированию требуется предусмотреть размещение технических средств Системы на площади зданий (ЦОД), находящихся в собственности Заказчика. Проектная документация должна иметь копии согласований с владельцами площадей, планируемых для размещения технических средств Системы.

Необходимость разработки проектных решений по организации инженерных систем, требования к степени интеграции, по каждой из вышеперечисленных систем, определяются и согласовываются с Заказчиком на стадии технического проектирования.

4.3.8 Требования к метрологическому обеспечению

Требования к метрологическому обеспечению не предъявляются.

4.3.9 Требования к организационному обеспечению

В ходе разработки Системы должно быть обеспечено постоянное взаимодействие между Заказчиком и Исполнителем, для чего ими будут сформированы рабочие группы по проекту, включающие представителей Заказчика и Исполнителя, уровень компетенции которых достаточен для:

- решения административных вопросов (организация встреч, предоставление допусков, рассмотрение и согласование проектной документации и т.п.);
- решения инженерно-технических вопросов (согласование технических аспектов реализации и администрирования Системы, определение и размещения технических средств, коммуникаций и т.п.);
- нормативно-методического и информационного обеспечения проектных работ, включая необходимое консультирование, организацию интервьюирования экспертных групп с целью уточнения функциональных характеристик подсистем и т. п.;
- согласования позиций и принятия (организации принятия) оперативных решений по вопросам разработки Системы.

Рабочие группы должны быть созданы не позднее 20 календарных дней с даты заключения контракта.

4.3.10 Требования к методическому обеспечению

При разработке компонентов Системы и создании документации на них должны руководствоваться следующими нормативными документами:

- ГОСТ 34.601-90 «Информационная технология. Комплекс стандартов на автоматизированные системы. Автоматизированные системы. Стадии создания»;
- ГОСТ 34.201-89 «Информационная технология. Комплекс стандартов на автоматизированные системы. Виды, комплектность и обозначение документов при создании автоматизированных систем».

5 СОСТАВ И СОДЕРЖАНИЕ РАБОТ ПО СОЗДАНИЮ СИСТЕМЫ

Выполнение работ по созданию Системы должно предусматривать выполнение этапов работ, приведенных в соответствии с таблицей 2.

Таблица 2 – Этапы работ по созданию Системы

№	Наименование работ	Содержание работ	Результат работ, отчетные материалы и документация	Сроки выполнения этапа работ (начало – окончание)
I.	Работы по созданию подсистем ЦПСИ			
1.	Этап 1. Техническое проектирование	Разработка и согласование Частного технического задания	– Частное техническое задание	Не позднее 80 календарных дней с даты подписания контракта
2.		Актуализация технических требований к инфраструктуре	– Технические требования к инфраструктуре	
3.		Проведение проектных работ	– Пояснительная записка к техническому проекту	
4.	Этап 2. Разработка подсистем ЦПСИ	Проведение разработки	– Комплект исходных кодов; – Инструкция по сборке исходного кода	Не позднее 160 календарных дней с даты окончания работ по этапу 1
5.		Разработка Рабочей документации на систему и ее части	– Руководство пользователя; – Руководство администратора; – Общее описание Системы; – Описание организации информационной базы	
6.	Этап 3. Проведение испытаний	Развертывание ЦПСИ на вычислительных мощностях Министерства науки и высшего образования Российской Федерации	– Отчет о развертывании	Не позднее «18» декабря 2020 г.

№	Наименование работ	Содержание работ	Результат работ, отчетные материалы и документация	Сроки выполнения этапа работ (начало – окончание)
7.		Проведение предварительных испытаний ИС	– Программа и методика предварительных испытаний; – Протокол проведения предварительных испытаний; – Акт о вводе ЦПСИ в опытную эксплуатацию	
8.		Проведение опытной эксплуатации	– Программа и методика опытной эксплуатации; – Журнал опытной эксплуатации; – Акт о завершении опытной эксплуатации и допуске Системы к приемочным испытаниям	
9.		Проведение приемочных испытаний	– Программа и методика приемочных испытаний; – Протокол проведения приемочных испытаний; – Акт о приемке Системы в постоянную эксплуатацию	
II.	Работы по проектированию ПОИБ			
10.	Этап 1. Техническое проектирование	Формирование требований	– Проект акта классификации; – Модель угроз; – Модель нарушителя; – Частное техническое задание на создание ПОИБ	Не позднее 120 календарных дней с даты подписания контракта
11.		Разработка внутренних нормативных и организационно-	– Приказ о вводе в эксплуатацию автоматизированной системы;	

№	Наименование работ	Содержание работ	Результат работ, отчетные материалы и документация	Сроки выполнения этапа работ (начало – окончание)
		распорядительных документов по порядку обработки информации в Системе	– Приказ об определении ответственности должностных лиц и проведении мероприятий по защите информации; – Акт классификации информационной системы; – Акт определения уровня защищенности ПДн, обрабатываемых в ИСПДн; – Перечень организационно-технических мероприятий по защите информации; – Должностная инструкция администратора безопасности информации автоматизированной системы; – Должностная инструкция пользователя автоматизированной системы по обеспечению безопасности информации; – Инструкция по проведению антивирусного контроля в автоматизированной системе; – Инструкция по организации парольной защиты в автоматизированной системе; – Инструкция по внесению изменений в списки пользователей и наделению их полномочиями доступа к защищаемым ресурсам; – Инструкция по установке, модификации и техническому обслуживанию	

№	Наименование работ	Содержание работ	Результат работ, отчетные материалы и документация	Сроки выполнения этапа работ (начало – окончание)
			программного обеспечения и аппаратных средств; – Инструкция по выявлению и реагированию на инциденты информационной безопасности; – Технический паспорт на автоматизированную систему; – Описания технологического процесса обработки информации в автоматизированной системе; – Перечень защищаемых информационных ресурсов автоматизированной системы; – Журнал учета носителей конфиденциальной информации; – Матрица доступа к разделяемым информационным ресурсам автоматизированной системы; – Положение о порядке организации и проведения работ по защите информации ограниченного доступа (включая персональные данные), не содержащей сведений, составляющих государственную тайну; – Положение о пропускном и внутриобъектовом режиме;	

№	Наименование работ	Содержание работ	Результат работ, отчетные материалы и документация	Сроки выполнения этапа работ (начало – окончание)
			– Положения о разрешительной системе допуска исполнителей к документам и сведениям в организации; – Перечень сведений конфиденциального характера; – Перечень лиц, доступ которых к АС необходим для выполнения служебных (трудовых) обязанностей	
12.		Техническое проектирование решений	– Пояснительная записка к техническому проекту ПОИБ; – Спецификация оборудования и программного обеспечения ПОИБ	
13.	Этап 2. Внедрение ПОИБ	Разработка рабочей документации	– Программа и методика испытаний ПОИБ; – Схема соединений и подключений ПОИБ; – Чертеж установки технических средств ПОИБ	Не позднее 160 календарных дней с даты окончания работ по этапу 1 работ по созданию ПОИБ

6 ПОРЯДОК КОНТРОЛЯ И ПРИЕМКИ СИСТЕМЫ

Приемка результата работ осуществляется приемочной комиссией Заказчика с участием представителей Исполнителя.

Испытаниям должно предшествовать проведение Исполнителем пусконаладочных работ на вычислительных мощностях Заказчика, выделенных в соответствии с Техническими требованиями к инфраструктуре ЦПСИ, разработанных на этапе технического проектирования. Пусконаладочные работы должны включать в себя автономную наладку технических средств и программного обеспечения Системы, комплексную наладку технических средств и программного обеспечения Системы, создание на технических средствах Исполнителя инфраструктуры, необходимой для проверки Системы, включая установку и настройку программного обеспечения на сервере (серверах), рабочих станциях, а также другие необходимые мероприятия.

Перед началом испытаний Исполнитель должен совместно с Заказчиком определить количество и перечень пользователей, участвующих в предварительных испытаниях, опытной эксплуатации и приемочных испытаниях Системы. Исполнитель должен предоставить доступ к средствам Системы для обозначенных пользователей и настроить для них соответствующий уровень доступа.

Перед началом предварительных испытаний, опытной эксплуатации и приемочных испытаний должны быть настроены и подключены все функциональные возможности Системы.

Испытания компонентов Системы проводятся в соответствии с Программой и методикой испытаний посредством выполнения сценариев проверок совместно с приемочной комиссией Заказчика.

Проверка выполнения функциональных требований к Системе, указанных в настоящем ТЗ, должна осуществляться на заданном наборе данных, подготовленных Исполнителем.

Общая продолжительность испытаний должна составлять не менее 10 и не более 25 рабочих дней, сроки проведения испытаний определяются Исполнителем по согласованию с Заказчиком.

6.1 Виды, состав, объем и методы испытаний Системы и ее составных частей

Этап проведения предварительных испытаний включает:

- разработку программы и методики предварительных испытаний», в соответствии с которыми осуществляется проверка Системы на работоспособность и соответствия выполненных работ техническому заданию;
- проверку работоспособности Системы и соответствия выполненных работ и разработанной технической документации техническому заданию;
- устранение выявленных при проведении предварительных испытаний неисправностей и внесение изменений в техническую и рабочую документацию на Систему;
- оформление протокола предварительных испытаний и акта приемки Системы в опытную эксплуатацию.

По результатам предварительных испытаний Исполнителем в течение 3 рабочих дней с даты завершения предварительных испытаний должны быть подготовлены и представлены на согласование Заказчику протокол предварительных испытаний и акт приемки Системы в опытную эксплуатацию.

До начала проведения опытной эксплуатации Исполнитель разрабатывает и согласовывает с Заказчиком программу и методику опытной эксплуатации. Программа и методика опытной эксплуатации должны предусматривать настройку Системы и проверку ее функциональности.

Опытная эксплуатация Системы проводится согласно разработанным программе и методике на территории Заказчика с участием его представителей.

Срок опытной эксплуатации составляет не более 15 рабочих дней. Опытная эксплуатация проводится в штатном режиме функционирования Системы в соответствии с требованиями ГОСТ 34.603-92 «Информационная технология. Виды испытаний автоматизированных систем».

Во время проведения опытной эксплуатации Исполнитель должен вести рабочий журнал опытной эксплуатации, в который заносятся сведения о продолжительности функционирования Системы, отказах, сбоях, аварийных ситуациях, изменениях параметров объекта автоматизации, проводимых корректировках документации и программных средств, наладке технических средств, а также предложений представителей Заказчика по совершенствованию Системы. В журнале фиксируются:

- дата и московское время обращения;
- контактные данные обратившегося лица (ФИО, телефон и/или email);

- содержание обращения;
- способ поступления обращения (телефон, email и т.д.);
- дата и московское время полной отработки обращения;
- содержание принятых по обращению мер.

В ходе опытной эксплуатации в случае обнаружения недостатков Исполнитель осуществляет необходимые доработки программного обеспечения Системы и дополнительную настройку технических средств.

По результатам опытной эксплуатации Исполнителем в течение 3 рабочих дней с даты завершения опытной эксплуатации должен быть подготовлен акт о завершении опытной эксплуатации и допуске Системы к приемочным испытаниям.

Приемочные испытания Системы проводятся после устранения Исполнителем недостатков, выявленных на этапе опытной эксплуатации, согласно разработанным программе и методике приемочных испытаний. Приемочные испытания Системы проводятся на территории Заказчика с участием его представителей.

Срок приемочных испытаний составляет не более 5 рабочих дней. Приемочные испытания проводятся в штатном режиме функционирования Системы в соответствии с требованиями ГОСТ 34.603-92.

Приемочные испытания должны включать:

- проверку реализации требований по созданию Системы, указанных в настоящем ТЗ;
- проверку работоспособности функционала Системы, разработанного в рамках настоящего ТЗ, а также сохранения работоспособности функционала, не подвергавшегося изменениям в рамках работ по развитию Системы;
- проверку комплектности и качества представленной Исполнителем документации;
- проверку устранения Исполнителем выявленных на этапе опытной эксплуатации замечаний.

По результатам проведения приемочных испытаний Исполнитель в течение 3 рабочих дней должен подготовить и передать на согласование Заказчику протокол проведения приемочных испытаний и акт приемки Системы в постоянную эксплуатацию.

Процедура приемочных испытаний должна проводиться до подписания Заказчиком и Исполнителем протокола проведения приемочных испытаний с положительным заключением.

6.2 Общие требования к приемке работ по стадиям, порядок согласования и утверждения приемочной документации

Сдача-приемка выполненных работ осуществляется по предъявлении Исполнителем комплектов соответствующих документов и завершается оформлением акта сдачи-приемки выполненных работ, подписанного Исполнителем и Заказчиком.

Передача Заказчику комплекта документации и дистрибутивов разработанного ПО осуществляется одновременно с актом сдачи-приемки выполненных работ с сопроводительным письмом.

В процессе приемки результатов работ должна быть осуществлена проверка Системы на соответствие требованиям настоящего ТЗ.

Испытания Системы должны проводиться в соответствии с ГОСТ 34.603-92 «Виды испытаний автоматизированных систем» и подразделом **Ошибка! Источник ссылки не найден.** данного документа.

Акт сдачи-приемки выполненных работ передается Исполнителем Заказчику по окончании приемо-сдаточных испытаний по всем работам, проводимым в рамках Государственного контракта.

Гарантийные обязательства должны действовать в течение 12 месяцев после подписания акта сдачи-приемки выполненных работ.

7 ТРЕБОВАНИЯ К СОСТАВУ И СОДЕРЖАНИЮ РАБОТ ПО ПОДГОТОВКЕ ОБЪЕКТА АВТОМАТИЗАЦИИ К ВВОДУ СИСТЕМЫ В ДЕЙСТВИЕ

Для создания условий функционирования объектов автоматизации Системы, при которых гарантируется соответствие разработанной Системы требованиям, содержащимся в настоящем ТЗ, должны быть проведены следующие мероприятия:

- настройка аппаратно-программного комплекса Системы;
- проведение испытаний Системы в соответствии с разделом **Ошибка! Источник ссылки не найден.** настоящего технического задания;
- передача Исполнителем Заказчику реквизитов доступа к компонентам Системы.

8 ТРЕБОВАНИЯ К ДОКУМЕНТИРОВАНИЮ

Отчетные материалы должны разрабатываться в соответствии с ГОСТ 34.201-89 «Информационная технология. Комплекс стандартов на автоматизированные системы. Виды, комплектность и обозначение документов при создании автоматизированных систем».

Комплект документов на Систему должен включать документы, указанные в разделе 5 «Состав и содержание работ по созданию Системы».

Документация представляется в двух экземплярах на бумажном носителе и в одном экземпляре на электронном носителе (на CD/DVD-дисках или иных электронных носителях). Текстовые документы, передаваемые на электронном носителе, должны быть представлены в форматах PDF/A, с обеспечением навигации по оглавлению и возможности полнотекстового поиска.

Дистрибутив программного обеспечения и исходный код в текстовом формате, соответствующем используемому языку программирования, должны быть представлены в электронном виде (на CD/DVD-дисках или иных электронных носителях) в одном экземпляре.

9 ИСТОЧНИКИ РАЗРАБОТКИ

1) ГОСТ 34.601-90 «Информационная технология. Комплекс стандартов на автоматизированные системы. Автоматизированные системы. Стадии создания»;
2) ГОСТ 34.602-89 «Информационная технология. Комплекс стандартов на автоматизированные системы. Техническое задание на создание автоматизированной системы»;
3) ГОСТ 34.603-92 «Информационная технология. Виды испытаний автоматизированных систем»;
4) ГОСТ 34.201-89 «Информационная технология. Комплекс стандартов на автоматизированные системы. Виды, комплектность и обозначения документов при создании автоматизированных систем»;
5) ГОСТ Р ИСО 9241-210-2016 «Эргономика взаимодействия человек-система. Часть 210. Человеко-ориентированное проектирование интерактивных систем»;
6) ГОСТ Р 51583-2014 «Защита информации. Порядок создания автоматизированных систем в защищенном исполнении. Общие положения»;
7) ГОСТ Р 51624 «Защита информации. автоматизированные системы в защищенном исполнении. Общие требования»;
8) ГОСТ Р 56103-2014 «Защита информации. Автоматизированные системы в защищенном исполнении. Организация и содержание работ по защите от преднамеренных силовых электромагнитных воздействий. Общие положения»;
9) ГОСТ РО 0043-003-2012 «Аттестация объектов информатизации. Общие положения»;
10) ГОСТ РО 0043-004-2013 «Программа и методики аттестационных испытаний»;
11) ГОСТ 15150-69 «Машины, приборы и другие технические изделия. Исполнения для различных климатических районов. Категории, условия эксплуатации, хранения и транспортирования в части воздействия климатических факторов внешней среды»;
12) ГОСТ 21958-76 «Система «Человек-машина»;
13) ГОСТ 21552-84 «Средства вычислительной техники. Общие технические требования, приемка, методы испытаний, маркировка, упаковка, транспортирование и хранение»;
14) ГОСТ 27201-87 «Машины вычислительные электронные персональные. Типы, основные параметры, общие технические требования»;

15) ГОСТ 25861-83 «Машины вычислительные и системы обработки данных. Требования по электрической и механической безопасности и методы испытаний»;

16) ГОСТ 12.1.030-81 «Система стандартов безопасности труда. Электробезопасность. Защитное заземление, зануление»;

17) ГОСТ 12.2.003-91 «Система стандартов безопасности труда. Оборудование производственное. Общие требования безопасности»;

18) ГОСТ 12.2.007.0-75 «Система стандартов безопасности труда. Изделия электротехнические. Общие требования безопасности»;

19) НПБ 110-03 «Перечень зданий, сооружений, помещений и оборудования, подлежащих защите автоматическими установками пожаротушения и автоматической пожарной сигнализацией»;

20) СНиП 21-01-97 «Пожарная безопасность зданий и сооружений»;

21) НПБ 105-03 «Определение категорий помещений, зданий и наружных установок по взрывопожарной и пожарной опасности»;

22) Постановление Правительства Российской Федерации № 676 от 06 июля 2015 г. «О требованиях к порядку создания, развития, ввода в эксплуатацию, эксплуатации и вывода из эксплуатации государственных информационных систем и дальнейшего хранения содержащейся в их базах данных информации»;

23) Постановление Правительства Российской Федерации от 16 ноября 2015 года № 1236 «Об установлении запрета на допуск программного обеспечения, происходящего из иностранных государств, для целей осуществления закупок для обеспечения государственных и муниципальных нужд».