Приложение №1
к Контракту№_____
от «___» _____ 20__ г.

УТВЕРЖДАЮ

Исполняющий обязанности директора государственного унитарного предприятия Донецкой Народной Республики «Республиканский центр информационных технологий»

_____ А.В. Сахов
«24» 08 2026 г.

ТЕХНИЧЕСКОЕ ЗАДАНИЕ

На оказание услуги по предоставлению прав использования программного обеспечения для создания информационно-аналитической системы Донецкой Народной Республики

на 54 листах

Донецк 2026

Описание объекта закупки

Предмет контракта: **оказание услуги по предоставлению прав использования программного обеспечения для создания информационно-аналитической системы Донецкой Народной Республики.**

Срок оказания услуг: с даты заключения Контракта в течение 120 календарных дней.

Место предоставления Лицензии – г. Донецк.

Территория использования Лицензии: Российская Федерация.

Исполнитель передает Заказчику документы, подтверждающие право Исполнителя на предоставление прав на использование программного обеспечения (далее – ПО). Исполнитель гарантирует, что ПО, право на использование которого предоставлено, правомерно введено в гражданский оборот на территории Российской Федерации, а также, что предоставленное право использования ПО не нарушает каких-либо авторских прав, неимущественных и/или имущественных прав любых третьих лиц.

Наименование объекта закупки, характеристики, количество:

Таблица № 1

Наименование ПО	Характеристики программного обеспечения КТРУ	Кол-во (шт.)
Программное обеспечение (Подсистема инструментальных средств)	**58.29.11.000-00000003** **Вид лицензии: простая (неисключительная)** **Класс программ для электронных вычислительных машин и баз данных: (10.01) Средства обработки Больших Данных (BigData)** **Способ предоставления: копия электронного экземпляра** *Дополнительные характеристики:* Лицензия на один продуктивный и один тестовый сервер (виртуальных машин); Количество поддерживаемых физических ядер процессора (CPU) – 16; Суммарное количество пользователей – 150. В том числе: Количество учетных записей пользователей - 95; Количество пользователи форм ввода – 50; Количество администраторов - 5	1 шт.

	Аутентификация (Singlesign-on)- LDAP, ADFS, OpenID; Объем обрабатываемого массива – 1Тб; Лицензионная поддержка – 1 год включена; Уровень лицензионной поддержки – Оптимальный; Территория использования: РФ; Срок использования: бессрочно Обоснование дополнительных характеристик: В связи с необходимостью полного и объективного описания объекта закупки с учетом положений статьи 33 ФЗ №44-ФЗ Заказчик применяет дополнительные характеристики для определения более детальной потребности Заказчика. Данный набор характеристик позволит максимально удовлетворить потребности Заказчика с учетом специфики его деятельности и обеспечить эффективное использование бюджетных средств.	
Программное обеспечение (Подсистема оркестрации ETL-процессов)	**58.29.11.000-00000003** **Вид лицензии: простая (неисключительная)** **Класс программ для электронных вычислительных машин и баз данных: (10.01) Средства обработки Больших Данных (BigData)** **Способ предоставления: копия электронного экземпляра** Лицензия на два физических сервера (виртуальных машины); Суммарное число одновременных ETL процессов – не менее 20 Срок использования: бессрочно; Лицензионная поддержка – 1 год включена. Обоснование дополнительных характеристик: В связи с необходимостью полного и объективного описания объекта закупки с учетом положений статьи 33 ФЗ №44-ФЗ Заказчик применяет дополнительные характеристики для определения более	1 шт.

	детальной потребности Заказчика. Данный набор характеристик позволит максимально удовлетворить потребности Заказчика с учетом специфики его деятельности и обеспечить эффективное использование бюджетных средств.	
Программное обеспечение (Подсистема прикладных аналитических модулей)	**58.29.11.000-00000003** **Вид лицензии: простая (неисключительная)** **Класс программ для электронных вычислительных машин и баз данных: (10.01) Средства обработки Больших Данных (BigData)** **Способ предоставления: копия электронного экземпляра** Лицензия на один продуктивный сервер и один сервер тестирования (виртуальных машины) Срок использования: бессрочно Лицензионная поддержка – 1 год включена Обоснование дополнительных характеристик: В связи с необходимостью полного и объективного описания объекта закупки с учетом положений статьи 33 ФЗ №44-ФЗ Заказчик применяет дополнительные характеристики для определения более детальной потребности Заказчика. Данный набор характеристик позволит максимально удовлетворить потребности Заказчика с учетом специфики его деятельности и обеспечить эффективное использование бюджетных средств	1 шт.
Программное обеспечение (Операционная система)	**58.29.11.000-00000003** **Вид лицензии: простая (неисключительная)** **Класс программ для электронных вычислительных машин и баз данных: 02.09 Операционные системы общего назначения** Бессрочная простая (неисключительная) лицензия на одну установку ОС.	3 шт

	Версия – по выбору Исполнителя из перечня поддерживаемых (п. 2.2.4.11). ОС должна быть сертифицирована ФСТЭК России в соответствии с требованиями для ГИС класса защищенности, определенного в п. 2.2.4.5.6. Обоснование дополнительных характеристик: В связи с необходимостью полного и объективного описания объекта закупки с учетом положений статьи 33 ФЗ №44-ФЗ Заказчик применяет дополнительные характеристики для определения более детальной потребности Заказчика. Данный набор характеристик позволит максимально удовлетворить потребности Заказчика с учетом специфики его деятельности и обеспечить эффективное использование бюджетных средств	
Услуги по настройке, внедрению и проектированию подсистемы защиты информации	**62.01.11.000** Услуги по настройке, внедрению и проектированию подсистемы защиты информации в соответствии с требованиями настоящего технического задания	1 шт

Условия предоставления прав (Лицензии):

Исполнитель обязуется уведомить Заказчика о дате и времени передачи Лицензии письменно по электронной почте inbox@rcit.gov-dpr.ru и по телефонам +7 (949) 386-80-00 или +7(856) 386-80-00 не позднее, чем за 2 (два) рабочих дня до предполагаемой даты передачи.

В Лицензии указывается:

- наименование Заказчика, в пользу которого выдана Лицензия;
- наименование ПО;
- номер, дата, срок действия Лицензии.

Тип Лицензии – простая (неисключительная). Исполнитель, обладая соответствующими правами и полномочиями, передает, а Заказчик получает неисключительное право на использование ПО.

Условия предоставления Лицензии: неисключительное право на ПО предоставляется Заказчику в виде Лицензии в бумажном виде. Заказчику передаются сканированные копии Лицензии в электронном виде на электронную почту: inbox@rcit.gov-dpr.ru.

Способы использования Лицензии: предоставляемое право включает в себя воспроизведение ПО, ограниченное правом инсталляции (установкой и размещением) и запуска ПО, а также использование ПО в соответствии с его функциональным назначением.

Исполнитель передает Заказчику комплект инструкций, дисков, поставляемых производителем программного обеспечения совместно с ПО.

1. Общие сведения

Назначение оказания Услуг:

реализация эффективной технологической поддержки информационного и экспертно-аналитического обеспечения процессов подготовки и принятия решений Главой Донецкой Республики и Правительством Донецкой Народной Республики, а также повышения эффективности информационного взаимодействия исполнительных органов и органов муниципального управления;

создание единого информационного ресурса для исполнения функций управления, реализации документов стратегического и территориального планирования, мониторинга показателей социально-экономического развития и обеспечения национальной (региональной) безопасности Донецкой Народной Республики, а также мониторинга эффективности деятельности участников стратегического планирования;

решение задач для всех уровней планирования: оперативного (региональный), тактического (муниципальный) и стратегического (федеральный) с необходимым для данного уровня управления детализацией;

осуществление взаимоувязки и взаимообусловленности задач для разных уровней планирования;

обеспечение межведомственного взаимодействия и интеграции различных средств, комплексов и систем автоматизации управления в едином информационном пространстве;

Задачи, решаемые в результате оказания Услуг:

поставка и развертывание программного обеспечения (инструментальных средств) для сбора, хранения, поиска, управления информацией и аналитической обработки с визуализацией данных;

настройка программных серверов приложений, в том числе прикладных разделов мониторинга и анализа;

обеспечение сбора и загрузки данных из различных источников;

формирование аналитической и регламентной отчетности;

проведение приемо-сдаточных испытаний информационно-аналитической системы.

В рамках настоящего Технического задания используются следующие сокращения, термины и определения:

Виджет – настраиваемый модуль, визуально отображающий характеристики данных в разном представлении (график, диаграмма и т.д.), с помощью которого осуществляется конструирование дашбордов;

ГАС «Управление» - государственная автоматизированная

информационная система «Управление», комплекс информационных систем и ресурсов, предназначенных для принятия управленческих решений в сфере государственного управления;

Группа показателей – объединение нескольких показателей одинакового уровня детализации;

Дашборд – информационная панель, которая состоит из одного или нескольких виджетов и элементов управления;

Измерение – набор доменов, по которым создается многомерное пространство;

ИАС, Система – информационно-аналитическая система Донецкой Народной Республики;

Идентификатор – представление (строка символов), однозначно идентифицирующее субъект и (или) объект доступа в Системе;

Куб – многомерный массив данных, как правило, разреженный и долговременно хранимый, используемый в OLAP;

НСИ – нормативно-справочная информация;

Объект доступа – единица информационного ресурса информационной системы (файл, техническое средство, узел сети, линия (канал) связи, мобильное устройство, программа, том, каталог, запись, поле записей и иные объекты), доступ к которой регламентируется правилами разграничения доступа и по отношению к которой субъекты доступа выполняют операции;

ОС – Операционная система;

Пользователь – лицо, которому разрешено выполнять некоторые действия (операции) по обработке информации в Системе или использующее результаты ее функционирования;

Показатель – данные, количественно характеризующие процесс, образующийся на пересечении измерений OLAP;

ПСИ – приемо-сдаточные испытания;

Событие безопасности (информационной) – идентифицированное возникновение состояния Системы (сегмента, компонента Системы), сервиса или сети, указывающее на возможное нарушение безопасности информации, или сбой средств защиты информации, или ранее неизвестную ситуацию, которая может быть значимой для безопасности информации;

Сторонние библиотеки – код или модуль программного обеспечения, необходимый для решения прикладных задач Системы;

СУБД – система управления базами данных;

Субъект доступа – пользователь, процесс, выполняющие операции (действия) над объектами доступа и действия которых регламентируются правилами разграничения доступа;

СЗИ – средство защиты информации;

СКЗИ – средство криптографической защиты информации;

Уязвимость – недостаток (слабость) Системы, который (которая) создает потенциальные или реально существующие условия для реализации или проявления угроз безопасности информации;

ФСБ России – Федеральная служба безопасности Российской Федерации;

ФСТЭК России – Федеральная служба по техническому и экспортному контролю;

API – Application programming interface (интерфейс прикладного программирования), набор готовых классов, процедур, функций, структур и констант, предоставляемых платформой для использования во внешних программных продуктах и позволяющий разработчикам использовать готовые блоки для построения приложения;

Drag-and-drop – способ оперирования элементами интерфейса в интерфейсах Пользователя (как графическим, так и текстовым) при помощи манипулятора «мышь» или сенсорного экрана;

Drill down – аналитический метод, который позволяет пользователю осуществлять навигацию среди различных уровней данных, от итоговых до детализированных, пути углубления могут быть определены иерархией вместе с размерностью, или другими связями;

ETL – Extract, Transform, Load (извлечение, преобразование, загрузка), процесс миграции данных из одного источника в другой;

FTP – File Transfer Protocol, протокол передачи файлов по сети;

JDBC – Java DataBase Connectivity, соединение с базами данных на Java, стандарт взаимодействия приложения с различными СУБД;

Kerberos – сетевой протокол аутентификации, который предлагает механизм взаимной аутентификации клиента и сервера перед установлением связи между ними;

LDAP – Lightweight Directory Access Protocol, облегчённый протокол прикладного уровня для доступа к службе каталогов X.500, позволяющий производить операции аутентификации, поиска и сравнения, а также операции добавления, изменения или удаления записей;

NTLM – NT LAN Manager, протокол сетевой аутентификации;

ODBC – Open DataBase Connectivity, соединение с базами данных на C или C++, стандарт взаимодействия приложения с различными СУБД;

OLAP – On-Line Analytical Processing, интерактивный анализ данных, технология обработки данных, заключающаяся в подготовке суммарной (агрегированной) информации на основе больших массивов данных, структурированных по многомерному принципу;

Single Sign-On – технология единого входа, при использовании которой Пользователь переходит из одного раздела Системы в другой, не связанный с предыдущим, без повторной аутентификации;

SQL – Structured Query Language, язык структурированных запросов, декларативный язык программирования, применяемый для создания, модификации и управления данными в реляционной базе данных, управляемой соответствующей системой управления базами данных;

TCP/IP – сетевая модель передачи данных, представленных в цифровом виде.

Порядок выполнения, оформления и предъявления результатов оказания Услуг регламентирован следующим комплексом стандартов и руководящих документов:

Федеральный закон от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации»;

Федеральный закон от 27.07.2006 № 152-ФЗ «О персональных данных»;

Постановление Правительства Российской Федерации от 06.07.2015 № 676 «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»;

Постановление Правительства Российской Федерации от 01.11.2012 № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных»;

Приказ ФСТЭК России от 11.04.2025 № 117 «Об утверждении Требований о защите информации, содержащейся в государственных информационных системах, иных информационных системах государственных органов, государственных унитарных предприятий, государственных учреждений»;

Распоряжение Правительства Донецкой Народной Республики от 06.08.2026 № 75-Р29 «О реализации мероприятий по созданию, развитию и эксплуатации (сопровождению) региональной информационно-аналитической системы Донецкой Народной Республики»;

ГОСТ Р 59792-2021. Национальный стандарт Российской Федерации. Информационные технологии. Комплекс стандартов на автоматизированные системы. Виды испытаний автоматизированных систем;

ГОСТ Р 59793-2021. Национальный стандарт Российской Федерации. Информационные технологии. Комплекс стандартов на автоматизированные системы. Автоматизированные системы. Стадии создания;

ГОСТ Р 2.105-2019. Национальный стандарт Российской Федерации. Единая система конструкторской документации. Общие требования к текстовым документам;

ГОСТ Р ИСО/МЭК 14764-2002. Информационная технология. Сопровождение программных средств;

ГОСТ Р 51275-2006. Национальный стандарт Российской Федерации. Защита информации. Объект информатизации. Факторы, воздействующие на информацию. Общие положения»;

ГОСТ Р ИСО/МЭК 12207-2010. Национальный стандарт Российской Федерации. Информационная технология. Системная и программная инженерия. Процессы жизненного цикла программных средств;

ГОСТ Р 59356-2021. Национальный стандарт Российской Федерации. Системная инженерия. Защита информации в процессе сопровождения системы»;

методический документ «Состав и содержание мероприятий и мер по защите информации, содержащейся в информационных системах», утвержденный ФСТЭК России 12.04.2026.

Состав поставки программного обеспечения

В рамках оказания Услуг по настоящему Техническому заданию Исполнитель, помимо прав использования прикладного программного обеспечения, обязуется осуществить поставку лицензионных ОС для серверов, на которых будет развернута ИАС.

Исполнитель предоставляет Заказчику права использования (простые неисключительные лицензии) на ОС в количестве, необходимом для установки на все серверы, указанные в разделе 2.2.4.11 настоящего ТЗ, и обеспечивает их установку и базовую настройку в соответствии с требованиями раздела 2.2.4.11.

2. Требования к программному обеспечению

Исполнителем должны быть предоставлены права использования на условиях простой (неисключительной) лицензии (далее – Лицензия) в соответствии с приведенным ниже количеством и составом, а также функциями, соответствующими настоящему техническому заданию:

№ п/п	Наименование программного обеспечения, версия	Количество Лицензий	Характеристики	Срок действия Лицензии, мес.
1	Подсистема оркестрации ETL-процессов	1 лицензия на 2 сервера	Лицензия на 2 серверных установки: – 1 сервер для тестирования, – 1 сервер открытого продуктивного контура. Суммарное число	Бессрочно

№ п/п	Наименование программного обеспечения, версия	Количество Лицензий	Характеристики	Срок действия Лицензии, мес.
			одновременных ETL-процессов не менее 30	
2	Подсистема инструментальных средств	1 лицензия на 2 сервера	Лицензия на 2 серверных установки: – 1 сервер для тестирования, – 1 сервер открытого продуктивного контура, Суммарное число пользователей 150, в том числе: 50 операторов с правом ввода данных, 95 пользователей на просмотр, 5 администраторов. Объем обрабатываемых данных – 1 терабайт	Бессрочно
3	Подсистема прикладных аналитических модулей	1 лицензия на 2 сервера	Лицензия на 2 серверных установки: – 1 сервер для тестирования, – 1 сервер открытого продуктивного контура	Бессрочно
4	ОС для серверов ИАС	не менее количества серверов, требуемых для развертывания всех подсистем	Бессрочная простая (неисключительная) лицензия на одну установку ОС. Версия – по выбору Исполнителя из перечня поддерживаемых (п. 2.2.4.11). ОС должна быть сертифицирована ФСТЭК России в соответствии с требованиями для ГИС класса защищенности, определенного в п. 2.2.4.5.6.	Бессрочно

Программное обеспечение должно быть включено в реестр отечественного программного обеспечения.

2.2. Предоставляемое программное обеспечение должно отвечать следующим требованиям:

2.2.1. Требования к подсистеме оркестрации ETL-процессов.

Подсистема оркестрации ETL-процессов (далее – Подсистема ETL) должна обеспечивать загрузку данных из внешних информационных систем и файловых источников, а также поддерживать возможность интеграции

разъединенных детализированных данных из различных информационных систем и источников.

Подсистема ETL должна состоять из следующих функциональных разделов:

раздел ETL;

раздел оркестрации процессов;

раздел хранения метаданных ETL-интеграции;

раздел администрирования;

раздел плагинов расширения.

2.2.1.1. Требования к функциональным возможностям раздела ETL.

Раздел ETL должен обеспечивать извлечение, трансформацию и загрузку данных с разнородными источниками и обладать следующей функциональностью:

подключение, чтение и запись в базы данных: PostgreSQL, Postgres Pro, Greenplum, Arenadata DB, Arenadata Postgres, FireBird и других баз данных, поддерживающих протокол ODBC;

подключение, чтение и запись в любую базу данных через JDBC протокол, при реализации пользовательских скриптов;

подключение, чтение и запись файлов в файловые хранилища: FTP сервер, сетевое хранилище;

получение данных, метаданных и форматирования из структурированных файлов ODS, CSV, XML, HTML, TXT с помощью JSON-файлов метаданных;

создание и изменение структуры хранилища данных с помощью JSON-файлов метаданных;

построение ETL-процессов;

создание с помощью интерфейса объектов соединений к системам-источникам и системам-приемникам с шифрованием пароля;

создание с помощью интерфейса переменных параметров и использование их в ETL-интеграциях;

просмотр и редактирование кода ETL-процесса;

взаимодействие с модулями подсистемы аналитической обработки и визуализации информации через API;

получение и отправка данных в API любых сервисов, при реализации пользовательских скриптов;

использование e-mail-нотификаций для оповещения о статусах ETL-процессов;

использование режимов полной и инкрементальной загрузки данных;

логирование с указанием кода названия ошибки, места ошибки из SQL-скрипта, времени ошибки.

2.2.1.2. Требования к функциональным возможностям раздела оркестрации процессов.

Раздел оркестрации процессов должен обеспечивать функции планирования, мониторинга и запуска процессов Системы, синхронизации и ведения истории их выполнения и обладать следующей функциональностью:

запуск ETL-процессов в режимах: ручного запуска, ручного запуска процесса с конфигурационными переменными, запуска процесса по расписанию, заданному в cron-формате;

запуск ETL-процесса по событию появления файла в файловом хранилище;

визуальный анализ статуса выполнения ETL-процессов и их отдельных шагов;

графическое представление ETL-процесса, в том числе в режиме онлайн с цветовой индикацией статуса исполнения шагов процесса;

логирование процесса интеграции (шагов, процессов, ошибок с фиксацией кодов ошибок);

перезапуск ETL-процесса с любого выбранного шага;

создание ветвлений и условий переходов между шагами интеграции;

динамическое создание шагов интеграции в процессе ETL-интеграции;

выполнение произвольного скрипта на языке Python, SQL, Bash в качестве одного из шагов интеграции;

запуск дочерних ETL-интеграций из основного процесса интеграции;

использование метаданных интеграции в ETL-процессе.

2.2.1.3. Требования к функциональным возможностям раздела хранения метаданных ETL-интеграций.

Раздел должен обеспечивать хранение, наполнение и анализ выполнения интеграций и обладать следующей функциональностью:

запись и хранение статуса, времени старта и окончания каждой интеграции и шага интеграции;

запись и хранение информации о взаимодействии основного и дочернего процесса интеграции;

предоставление доступа статистике исполнения процессов интеграции.

2.2.2. Требования к подсистеме инструментальных средств

В состав подсистемы должны входить:

модуль обработки данных;

модуль визуализации информации;

модуль ручного ввода данных;

модуль администрирования.

2.2.2.1. Модуль обработки данных

Загрузка данных.

Загрузка данных должна осуществляться с помощью графического визуального интерфейса. Должны поддерживаться следующие технологии загрузки:

файлы CSV, XLSX, ODS;

подключение к СУБД PostgreSQL, MySQL, ClickHouse и загрузка данных с помощью выполнения SQL запросов. Должна быть возможность расширять список поддерживаемых СУБД;

подключение к источнику данных через JDBC-интерфейс, и загрузка данных с помощью выполнения SQL запросов. Должна быть возможность добавлять любой JDBC-драйвер.

Загрузка данных должна осуществляться во внутреннюю БД, оптимизированную под аналитические запросы.

Настройка модели данных.

Настройка модели данных должна производиться в пользовательском графическом интерфейсе. При этом:

настройка связей между таблицами должна производиться с помощью операции drag-and-drop;

настройка модели данных должна осуществляться на основе табличной модели данных без необходимости использования принципов многомерного моделирования.

Обновление данных.

Должна поддерживаться возможность обновления данных по требованию и по расписанию.

Обновление данных не должно блокировать работу пользователей, которые производят анализ данных в интерактивных отчетах.

Создание новых вычислений на языке DAX или аналоге.

Должна поддерживаться возможность создания новых вычислений на уровне модели данных, в том числе:

создание новых вычислений должно производиться на основе формульного функционального языка запросов DAX или аналога и возможностью переиспользования созданных вычислений во всех визуальных элементах;

должна быть возможность выполнения операций как на уровне строк, так и на уровне столбцов, а также возможность производить сброс фильтров для выбранных расчетов. Например, расчет доли от общего без доработок ХД.

Пользователю должны выводиться различные подсказки, упрощающие создание вычислений. В том числе должно поддерживаться автодополнение вводимых наименований функций и их параметров.

Перечень вычислений, которые должны осуществляться с использованием формульного функционального языка запросов DAX или аналога, должен включать:

статистические расчеты: проведение различных статистических расчетов, включая вычисление средних значений, медиан, стандартных отклонений и других статистических показателей;

математические и тригонометрические расчеты: выполнение арифметических операций, а также тригонометрических вычислений, необходимых для анализа данных;

фильтрация данных: применение различных методов фильтрации для управления контекстом данных и выделения необходимой информации;

работа с датами и временем: выполнение операций с временными значениями, включая преобразования, вычисления временных интервалов и манипуляции с датами;

проверка условий и логика ветвления: реализация логических операций для построения сложных условий и управления потоком выполнения на основе заданных критериев;

обработка строковых данных: выполнение операций над текстовыми данными, включая их форматирование, преобразование и манипуляции с содержимым строк.

Преобразование и подготовка данных.

Модуль обработки данных должен содержать решение для самостоятельного преобразования и подготовки данных конечными пользователями без привлечения ИТ специалистов.

Модуль обработки данных должен обладать следующей функциональностью:

доступ через веб-браузер без необходимости установки дополнительных компонентов на локальный компьютер пользователя;

создание запросов в простом, интуитивно понятном графическом интерфейсе;

извлечение данных из различных источников, включая базы данных;

фильтрация данных в запросе;

добавление и удаление столбцов в запросе;

замена значений в запросе;

объединение запросов;

форматирование значений в запросе;

удаление дубликатов;

добавление результирующей таблицы в модель данных.

2.2.2.2. Модуль визуализации информации.

2.2.2.2.1. Создание интерактивных отчетов.

Должна поддерживаться возможность создания интерактивных отчетов на основе подготовленной модели данных.

Настройка состава данных у визуальных элементов должна производиться с помощью операции drag-and-drop.

В интерактивных отчетах должна быть возможность использования следующих стандартных визуальных элементов:

линейный график;

столбчатая диаграмма;

диаграмма с областями;

комбинированная диаграмма;

круговая диаграмма;

сводная таблица;

плоская таблица;

фильтр;

календарный фильтр по диапазону дат;

изображение;

текст;

диаграмма дерева;

спидометр.

Все визуальные элементы должны обладать следующей функциональностью:

настройка и изменение заголовка и подписей визуального элемента;

возможность изменения форматирования текста в подписях на основе формул условного форматирования.

Визуальные элементы, представляющие собой фильтры, должны поддерживать:

возможность работы во включающем или исключающем режиме;

полнотекстовый поиск, а также поиск по подстроке.

Визуальные элементы, представляющие собой графики и диаграммы, должны обладать следующей функциональностью:

гибкая настройка легенды, в том числе местоположения;

гибкая настройка оси, в том числе возможность использования дополнительной оси;

гибкая настройка серий, в том числе возможность задавать цвет.

Визуальные элементы, представляющие собой таблицы, должны обладать следующей функциональностью:

гибкая настройка заголовков столбцов и строк;

возможность изменения форматирования текста, цвета текста и цвета фона

на основе формул условного форматирования.

В диаграммах и сводной таблице должна быть возможность перейти на более низкий уровень данных (Drill-Down). Глубина перехода и измерения для перехода должны настраиваться в процессе создания отчета и не требовать перенастройки данных и метаданных.

У всех визуальных элементов должна быть возможность настройки собственного среза данных по определенным значениям измерений. При этом должна поддерживаться работа во включающем или исключающем режиме.

2.2.2.2.2. Расширение возможностей визуальных элементов.

– Функциональность всех визуальных элементов должна быть расширяема с помощью редактирования JavaScript-кода существующего визуального элемента. При этом настройка других визуальных элементов, в которых не требуется расширение функциональности, должна быть доступна без редактирования кода. Редактирование JavaScript-кода элемента должно осуществляться во встроенном редакторе кода с подсветкой синтаксиса. Должна быть предусмотрена возможность подключения внешних JavaScript-библиотек.

Должна быть возможность создавать новые визуальные элементы на языке JavaScript и подключать их к стандартным источникам данных. Созданные элементы должны быть опционально подключаемыми и переносимыми на другие экземпляры ПО.

Повторное использование нового визуального элемента, созданного с использованием программирования, должно происходить без редактирования JavaScript-кода. Для этого у разработчика визуального элемента должна быть возможность создавать свойства элемента, которые при повторном использовании виджета можно редактировать в визуальном интерфейсе без написания кода.

2.2.2.2.3. Публикация наработок.

Должна поддерживаться возможность делиться интерактивными отчетами, а именно:

публиковать интерактивный отчет по ссылке;

встраивать интерактивный отчет в сторонний портал;

публиковать интерактивный отчет на аналитическом портале.

создать публичную ссылку на отчет без ограничения доступа, доступную всем неавторизованным пользователям.

Должна поддерживаться возможность делиться набором данных, а именно: предоставлять доступ на создание интерактивных отчетов на основе набора данных, при этом не предоставляя прав на редактирование этого набора данных. В то же время, пользователи должны понимать, что это наборы данных, которые им специально предоставили другие пользователи.

2.2.2.2.4. Аналитический портал

Аналитический портал предназначается для просмотра агрегированной и подготовленной информации в виде интерактивных отчетов.

Аналитический портал должен обладать следующей функциональностью:

Доступ через веб-браузер, без необходимости установки дополнительных компонентов на локальный компьютер пользователя;

Предоставление пользователю навигации по порталу;

Предоставление доступа к интерактивным отчетам в соответствии с установленными правами пользователей;

Возможность опубликовать созданный аналитический отчет. Только после этого отчет должен быть виден пользователям на портале;

Возможность просматривать разные интерактивные отчеты на стартовой странице в зависимости от роли пользователя;

Адаптивное масштабирование интерактивных отчетов и отдельных листов отчетов в зависимости от установленных параметров масштабирования листа;

Поиск отчета по названию;

Формирование изображений для предпросмотра интерактивного отчета;

Возможность перехода с портала в режим редактирования дашборда для внесения изменений и настроек;

Экспорт интерактивных отчетов в форматы: *.pptx, *.png, *.pdf;

Настраиваемая структура разделов портала.

Модуль ручного ввода данных.

Модуль ручного ввода данных предназначен для ввода данных в формы ввода и управления справочниками через веб-интерфейс. Модуль ручного ввода данных должен быть тесно интегрирован с модулями обработки данных и визуализации информации. Настройка форм должна производиться в соответствии с принципами многомерного хранения данных и технологии OLAP. Настройка форм должна производиться через веб-интерфейс.

Настройка модели данных модуля ручного ввода данных.

В части настройки модели данных модуль должен обладать следующей функциональностью:

Создание, редактирование и удаление многомерных сущностей: измерений, атрибутов измерений, мер, кубов;

Возможность собрать куб из пересечения любых измерений, мер и календаря;

Создание, редактирование, удаление единиц измерения;

Встроенный календарь с возможностью работы с датами, месяцами, днями недели;

Поддержка разной календарной гранулярности ввода, от года до дня;

Возможность указать для меры единицы измерения, точность знака после запятой;

Просмотр истории изменения кубов, измерений, атрибутов измерений, значений измерений.

Формы ввода.

Модуль ручного ввода данных должен предоставлять возможность создавать и предварительно настраивать формы для работы с данными. В режиме предварительной настройки модуль должен обладать следующей функциональностью:

Ввод наименования формы;

Внешний вид формы;

Распределение измерений и мер по строкам и столбцам;

Установка фильтров на измерения;

Настройка собственных стилей формы;

Возможность массового создания форм по элементам или атрибутам одного, или нескольких измерений, с учетом заданной последовательности этих элементов;

Сокращение отображаемых экземпляров форм при массовом создании, с помощью определения даты начала и даты окончания повторений; количества повторений; даты окончания действия календаря;

Предпросмотр внешнего вида экземпляров форм;

Поддержка типов данных: строка, дата, число, логический тип, ссылка на значение элемента другого измерения;

Настройка отображения элементов на форме в зависимости от элемента другого измерения, чтобы скрыть пустые и не значимые ячейки на форме ввода на основе зависимостей между измерениями.

Для вводящего данные пользователя модуль должен предоставлять удобный веб интерфейс с формой ввода и обладать следующей функциональностью:

Фильтрация списка форм по измерениям, кубам, статусам бизнес-процессов, дате;

Поиск формы по наименованию;

Возможность навигации между созданными формами и их экземплярами;

Возможность открытия форм и экземпляров по прямой ссылке;

Возможность редактирования данных на пересечении всех заданных измерений;

Типы данных редактируемых значений должны включать: числовые значения, текстовые значения, логические значения (выбор из двух вариантов), выбор из фиксированного списка значений другого измерения;

Возможность фильтрации по атрибутам;

Визуальные пользовательские настройки отображения формы;

Просмотр истории изменения по любой ячейке или по группе ячеек;

Создание и редактирование комментариев для любой ячейки в таблице.

Управление нормативно-справочной информацией.

Модуль ручного ввода данных должен позволять управлять составом и содержанием НСИ. Модуль должен предоставлять возможность создания, редактирования и удаления измерений, атрибутов измерений, структуры измерений.

В режиме настройки НСИ модуль должен обладать следующей функциональностью:

Настройка размещения элементов по каталогам;

Настройка иерархии каталогов;

Настройка порядка отображения атрибутов и распределение атрибутов по нескольким листам на карточке редактирования элемента измерения;

Возможность импорта и экспорта структуры и элементов;

Возможность создания атрибута, который является ссылкой на элемент другого измерения;

Возможность указать список атрибутов, которые составляют уникальный ключ и не могут быть повторно введены;

Настройка обязательности заполнения атрибута;

Опциональный запрет на ввод одинаковых значений атрибута;

Поддержка типов данных: строка, текст, дата, целое число, вещественное число, ссылка на значение элемента другого измерения;

Возможность написания сценариев для автоматического заполнения части данных НСИ в зависимости от значений других атрибутов;

Возможность написания сценариев доступности атрибутов и их значений для заполнения в зависимости от значений других атрибутов.

Для вводящего данные пользователя модуль должен предоставлять удобный веб интерфейс с формой ввода НСИ и обладать следующей функциональностью:

Создание, редактирование и удаление элементов измерений;

Редактирование атрибутов измерений. Типы данных редактируемых значений должны включать: текстовые значения, числовые значения, дата, выбор из фиксированного списка значений другого измерения;

Возможность фильтрации по атрибутам;

Управление видимостью атрибутов на форме.

Бизнес-процессы.

Модуль ручного ввода данных должен позволять управлять бизнес-

процессом ввода данных, задавать последовательность статусов, правила их перехода, а также назначать ответственных на каждом этапе. Данные, проходящие по бизнес-процессу, получают дополнительные свойства, в зависимости от статуса, такие как:

Дополнительные ограничения прав доступа на чтение и редактирование данных;

Контроль целостности данных.

Оператор ввода должен иметь возможность перевода статуса формы ввода в соответствии с настроенным бизнес-процессом. При редактировании НСИ перевод статуса должен быть доступен для каждого значения измерения. При переводе статуса должна быть возможность ввести комментарий с использованием редактора текста с поддержкой продвинутого форматирования, такого как выделение цветом, управление жирностью, размером шрифта, добавление изображений и т.д.

Должна быть возможность включить и отключить обязательное требование комментария при переводе статуса.

Должна быть возможность просмотра истории перехода статусов.

Форматно-логический контроль.

Модуль ручного ввода данных должен обладать функциональностью форматно-логического контроля при вводе данных. Форматно-логический контроль должен настраиваться с помощью формул на этапе подготовки форм.

Синтаксис формул должен позволять:

Использовать базовые математические операции;

Использовать логические операторы;

Использовать операторы сравнения;

Обращаться к атрибутам и значениям измерений.

Должна быть возможность настроить текст оповещения пользователя и цвет подсветки ячейки в случае, если его ввод не соответствует правилу форматно-логического контроля. Должно быть предусмотрено два типа оповещения:

предупреждение (можно продолжить и сохранить данные);

ошибка (нельзя продолжить и сохранить данные).

Проверка формул логического контроля должна происходить в момент сохранения данных формы пользователем. Если ввод пользователя не соответствует одному или нескольким правилам, пользователь должен быть уведомлен об этом. Подмножество ячеек каждого правила, не прошедшего проверку, должно изменить цвет фона в соответствии с настройками. Возможность пропустить уведомление и продолжить сохранение определяется настройками.

Бизнес-правила.

Модуль ручного ввода данных должен содержать возможность написания формул бизнес-правил, которые должны позволять:

Совершать базовые математические операции;

Производить действия по консолидации;

Производить действия по переносу данных в разные кубы;

Рассчитывать итоги с использованием функций агрегаций SUM, AVG, COUNT;

Производить массовые операции на пересечении измерений, значений иерархии каталогов измерений, значений элементов измерений над подмножеством ячеек.

Ячейки данных, в которых происходит запись через формулы бизнес-правил должны быть недоступны для ручного ввода.

Для сложных манипуляций с данными должна быть предусмотрена возможность использования Python скриптов в качестве бизнес-правила.

Расчет формул бизнес-правил осуществляется с пользовательского интерфейса, в момент сохранения формы ввода. В этом случае рассчитываются только бизнес-правила, связанные с данной формой, а также, опционально, все зависимые бизнес-правила. Должна быть предусмотрена возможность вызова перерасчета всех бизнес-правил.

Интеграция с модулями обработки данных и визуализации информации

Все данные и НСИ, введенные в модуле ручного ввода данных, должны быть доступны в модуле обработки данных с последующим выводом модулем визуализации информации в качестве аналитического отчета. Периодичность синхронизации данных должна настраиваться по расписанию или выполняться вручную.

Кроме непосредственно введенных в формы данных, в модуле обработки данных должна передаваться информация об актуальных статусах бизнес-процессов и обеспечиваться возможность построения отчетов на основе этой информации.

Модуль администрирования.

Управление пользователями.

Модуль администрирования должен позволять администратору управлять пользователями и производить следующие действия:

создавать, редактировать, удалять пользователей;

изменять пароль пользователя;

создавать, редактировать, удалять группы пользователей;

назначать права доступа пользователю через присвоение определенной роли или нескольких ролей;

использовать LDAP-совместимые службы каталогов, в том числе Active Directory, в качестве источника списка зарегистрированных пользователей;

проводить удаленную проверку пароля по протоколу LDAP;

поддерживать LDAPS (LDAP over SSL);

использовать внешние провайдеры аутентификации, осуществляющих работу по протоколу OpenID Connect;

работать в режиме Single Sign-On (SSO) по протоколу Kerberos и OpenID Connect, что позволяет не вводить пароль для доступа к системе, если пользователь уже был аутентифицирован в домене.

Управление правами доступа.

Модуль администрирования должен предоставлять администратору системы средства для управления правами доступа на основе ролевой модели доступа и должна обладать следующей функциональностью:

создание, редактирование, удаление ролей;

назначение ролей пользователям;

при использовании LDAP, возможность автоматического назначения ролей в зависимости от группы пользователя в AD;

при использовании внешних провайдеров аутентификации, осуществляющих работу по протоколу OpenID Connect, возможность автоматического назначения ролей в системе на основе роли пользователя во внешнем провайдере аутентификации.

Функциональное разграничение доступа.

Только пользователи, созданные в системе, должны иметь доступ к работе в данной системе.

С точки зрения доступа к функциональности, в системе должны быть предусмотрены следующие функциональные роли:

администратор (полный доступ);

разработчик интерактивного отчета (доступ к загрузке данных из базы данных, созданию и редактированию модели данных, доступ к созданию и редактированию интерактивных отчетов);

авторизованный пользователь (доступ к просмотру и взаимодействию с интерактивными отчетами).

Должна быть возможность для разных структурных подразделений Заказчика настраивать независимую работу с наборами данных, с настройкой аналитических отчетов. При этом должна быть возможность давать доступ некоторым пользователям из одного структурного подразделения к наборам данных и аналитическим отчетам другого структурного подразделения.

Разграничение доступа к данным.

Доступ к просмотру данных должен настраиваться в разрезах значений

атрибутов измерений (строк в таблицах). Разграничение в разрезе значений атрибутов измерений должно позволять разным пользователям видеть на одном и том же отчете разные данные, в соответствии с настроенными правами доступа.

В случае использования внешних провайдеров аутентификации, осуществляющих работу по протоколу OpenID Connect, должна быть возможность ограничить доступ к данным на основе значения атрибута пользователя, отправленного внешним провайдером аутентификации.

Резервное копирование и восстановление.

Модуль администрирования должен предоставлять инструменты для резервного копирования и восстановления аналитических отчетов и системы.

Диагностирование.

Модуль администрирования должен предоставлять средства для диагностики системы. Данные инструменты должны обладать функциональностью мониторинга производительности сервера и свободных ресурсов в разрезе компонентов, в том числе: состояние жестких дисков, состояние оперативной памяти, загрузка сетевых интерфейсов, загрузка процессоров.

Доступ к формам ввода.

Должна быть возможность ограничить доступ к данным и справочникам НСИ в модуле ручного ввода данных в разрезе измерений, атрибутов измерений и значений измерений по уровням доступа:

доступ запрещен;

только просмотр (чтение);

просмотр и редактирование.

Пользователям должны быть доступны формы ввода в соответствии с доступными данными. Создание новых форм ввода возможно только на тех данных, к которым у разработчика форм ввода есть доступ на чтение или редактирование.

Должна быть возможность настроить динамическое изменение прав доступа в зависимости от текущего статуса бизнес-процесса на форме ввода и текущего статуса элемента измерения.

Должна быть возможность настроить правила формирования прав по умолчанию.

2.2.3. Требования к подсистеме прикладных аналитических модулей.

В рамках решения задач мониторинга и анализа Исполнителем должны быть поставлены следующие аналитические разделы:

2.2.3.3. Модуль мониторинга индикаторов, определенных Указом Президента Российской Федерации от 28 ноября 2024 г. № 1014 должен обеспечивать:

– ввод данных (на основе файловой выгрузки из ГАС «Управление»), в ежеквартальной периодичности в разрезе субъектов Российской Федерации о плановых и фактических значениях показателей для оценки эффективности высших должностных лиц;

– ввод данных, детализирующих индикаторы первого уровня;

– отображение % достижения целевых значений индикаторов в табличном и графическом виде;

– отображение места ДНР среди субъектов Российской Федерации по значению выбранного целевого показателя за предыдущий отчетный период.

Состав показателей может быть уточнен по согласованию с Заказчиком в ходе оказания услуг.

2.2.3.4. Модуль мониторинга социально-экономического развития.

Модуль предназначен для мониторинга и анализа показателей социально-экономического развития на основе данных Федеральной службы государственной статистики, а также ведомственных и муниципальных данных, в том числе показателей для формирования паспорта ДНР (Перечень показателей должен быть согласован в ходе оказания услуг).

Загрузка данных Федеральной службы государственной статистики (источник данных ЕМИСС) должна происходить автоматически по согласованному в ходе оказания услуг перечню показателей.

Ввод данных Территориального органа Федеральной службы Государственной статистики, а также данных органов исполнительной власти и органов местного самоуправления должен осуществляться с помощью форм ввода, настраиваемых Исполнителем.

Модуль должен обеспечивать отображение показателей в табличном, графическом (динамика) и картографическом виде (карта субъектов Российской Федерации для показателей загружаемых в разрезе субъектов Российской Федерации, карта муниципальных образований Донецкой Народной Республики для показателей вносимых в разрезе муниципальных районов и городских округов республики). Форма представления данных для показателей должна быть предложена Исполнителем и согласована Заказчиком. В части показателей, относящихся к паспорту субъекта помимо аналитического отчета должен быть реализован регламентный отчет, позволяющий получить форму для печати.

2.2.3.5 Модуль мониторинга государственных закупок

Модуль должен отражать информацию о фактическом выполнении плана государственных и муниципальных закупок в разрезе главных распределителей бюджетных средств, государственных учреждений и в целом по муниципальным образованиям. Данные на странице должны быть представлены в виде таблиц и диаграмм.

Состав информации модуля может быть уточнен Исполнителем и согласован с Заказчиком.

Подраздел «Информация о выполнении плана государственных закупок Донецкой Народной Республики»

Подраздел должен отражать информацию о фактическом выполнении плана государственных закупок в разрезе главных распределителей бюджетных средств, государственных учреждений и в целом по муниципальным образованиям. Данные на странице должны быть представлены в виде диаграмм.

Подраздел «Структура расходов на государственные закупки Донецкой Народной Республики

Подраздел должен обеспечивать представление структуры бюджетных средств, расходуемых на государственные закупки в Донецкой Народной Республики. Данные должны быть представлены в виде диаграмм.

Подраздел «Оценка эффективности размещения заказов для государственных нужд Донецкой Народной Республики»

Подраздел должен отражать информацию об отклонениях от начальной суммы стоимости контрактов в разрезе источников финансирования. Данные на странице должны быть представлены в виде таблицы и диаграммы.

Общая сумма заключенных контрактов и объявленных закупок, а также фактический объем размещенных заказов в разрезе главных распорядителей бюджетных средств должны формироваться на основе выгрузки из единой информационной системы в сфере закупок (ЕИС) по уровню заказчика «Субъект РФ» для Донецкой Народной Республики.

«Мониторинг закупок в разрезе региональных проектов и объектов» (паспорт закупки, связи с объектами) осуществляется в модуле 2.2.3.8. Настоящий модуль обеспечивает сводный мониторинг исполнения плана государственных закупок

2.2.3.6. Модуль мониторинга общественно-политической ситуации

Подраздел «Мониторинг обращений граждан на основе информации Платформы обратной связи»

Подраздел должен обеспечивать рейтингование числа сообщений в разрезе тематик за выбранный период, а также картографическое отображение числа сообщений по выбранной тематике. Состав информации раздела может быть уточнен Исполнителем и согласован с Заказчиком после получения уточненного набора данных.

Подраздел «Мониторинг обращений граждан, полученных через систему «Инцидент-менеджмент»

Подраздел должен обеспечивать отображение в табличном и графическом виде количества созданных инцидентов и инцидентов с ответами в разрезе

ответственных органов власти и атрибутов:

- группа тем;
- тема;
- дата поступления;
- территория;
- текущий шаг инцидента.

Подраздел должен обеспечивать возможность экспорта табличной формы в xlsx.

Источником данных для наполнения раздела должен быть файл экспорта системы «Инцидент менеджмент», формируемый специалистами Заказчика. В случае невозможности получения файла Исполнителем должна быть разработана форма ввода.

Подраздел анализа обращений граждан, поступивших по итогам проведения прямой линии с Президентом РФ

Источником данных для наполнения раздела должен быть файл экспорта формируемый специалистами Заказчика.

Подраздел должен обеспечивать мониторинг статусов обращений, зафиксированных по результатам прямой линии с Президентом Российской Федерации.

2.2.3.7. Модуль мониторинга исполнительской дисциплины

Модуль контроля исполнения поручений должен базироваться на выгрузках из системы СЭД «Дело».

Модуль должен обеспечивать визуализацию состояния (в т.ч. в динамике) исполнительской дисциплины по следующим показателям:

количество резолюций (поручений) от имени текущего пользователя;

количество резолюций (поручений), исполнителем которых является текущий пользователь;

количество резолюций (поручений) на исполнении подразделения/группы подразделений (от имени всех или указанных пользователей; исполнителями являются сотрудники выбранного подразделения (подразделений)).

Модуль должен позволять управлять отображением данных за выбранный пользователем период.

Пользователь должен иметь возможность выбрать:

период (диапазон дат);

конкретные значения: день, месяц, год.

Модуль должен обеспечивать возможность отображения данных за выбранный пользователем период в сравнении с предыдущими периодами (за указанный в настоящем и аналогичные периоды в прошлом году или предыдущие аналогичные периоды текущего года).

Модуль должен обеспечивать возможность отображения данных в следующих разрезах:

состояние исполнение резолюции (поручения):

исполненная;

неисполненная;

тип поручения:

контрольное (в контрольном поручении должна быть установлена плановая дата исполнения поручения);

не контрольное (в не контрольном поручении плановая дата исполнения поручения не установлена);

подразделения;

исполнительская дисциплина (исполнено\на исполнении):

с нарушением срока\срок истек;

без нарушения срока\срок не наступил;

не контрольная;

исполнитель и автор поручения.

Протокольные поручения в рамках реализации региональных проектов формируются и ведутся в Системе в модуле 2.2.3.8. Настоящий модуль обеспечивает мониторинг исполнительской дисциплины по данным СЭД «Дело».

2.2.3.8. Модуль управления реализацией региональных проектов

Модуль предназначен для ведения проектной деятельности, мониторинга и анализа реализации региональных проектов, реализуемых в рамках национальных проектов на территории Донецкой Народной Республики.

Для всех ведущихся в Модуле сущностей (проекты, объекты, контрольные точки, закупки, поручения, риски) должны обеспечиваться регистрация и ведение электронной карточки, просмотр и изменение её атрибутов, форматно-логический контроль (далее – ФЛК) вводимых данных, управление файлами документов и разграничение прав доступа.

2.2.3.8.1. Паспорта проектов и объектов.

Модуль должен обеспечивать ведение и хранение электронного паспорта (карточки) проекта, содержащего следующие сведения:

основные положения;

показатели регионального проекта;

помесячный план достижения показателей в текущем году;

мероприятия (результаты);

финансовое обеспечение реализации;

помесячный план исполнения бюджета в части бюджетных ассигнований на текущий год;

план реализации;

дополнительные и обосновывающие материалы.

Модуль должен обеспечивать создание и хранение электронного паспорта (карточки) объектов, реализуемых в рамках проектной деятельности, содержащего:

адрес объекта;

сроки реализации;

сведения о подрядчике и заказчике;

перечень ответственных лиц;

связь с проектом.

2.2.3.8.2. Планы-графики работ по объектам.

Модуль должен обеспечивать формирование и отслеживание плана ключевых событий в рамках объектов: формирование календарного плана, определение связей между контрольными точками (далее – КТ), указание исполнителей, ведение версий план-графика.

Модуль должен обеспечивать выполнение следующих функций:

регистрация карточки КТ с указанием необходимых атрибутов и изменение её атрибутов;

поиск, фильтрация и сортировка КТ по атрибутам;

формирование и выгрузка шаблона план-графика объекта (типового или на основе существующей версии);

загрузка новой версии план-графика из шаблона;

указание предшественника для визуализации связи между контрольными событиями;

визуализация календарного плана объекта в виде диаграммы Ганта.

2.2.3.8.3. Показатели проектов.

Модуль должен обеспечивать формирование показателей (индикаторов) проекта и выполнение следующих функций:

создание показателя и его привязка к проекту;

учет целевых (плановых) значений показателей, в том числе по периодам;

сбор или ввод фактических значений показателей, в том числе по периодам.

2.2.3.8.4. Закупки в рамках проектов.

Модуль должен обеспечивать мониторинг закупочной деятельности в разрезе проектов и объектов, а также формирование электронного паспорта закупки, содержащего:

способ закупки;

планируемую и фактическую даты закупки;

статус прохождения конкурсной процедуры;

сроки выполнения работ по контракту;

начальную (максимальную) цену контракта (далее – НМЦК);

сумму контракта;

сведения о подрядчике и заказчике;

идентификатор закупки;

перечень ответственных лиц;

связь с объектами.

Модуль должен обеспечивать формирование связей «одна закупка – несколько объектов» (с выделением процента суммы закупки, направленной на каждый объект) и «один объект – несколько закупок».

2.2.3.8.5. Финансовые показатели проектов.

Модуль должен обеспечивать формирование и контроль исполнения бюджета проектов, включая формирование планового бюджета проекта на трехлетний период и оперативный контроль освоения выделенных средств.

Модуль должен обеспечивать выполнение следующих функций:

ввод и согласование планового бюджета проектов на трехлетний период;

ввод помесячного плана кассового исполнения;

оперативный сбор данных о фактическом исполнении.

Формирование и контроль исполнения бюджета проекта (объекта) должны осуществляться в разрезе федерального, республиканского (регионального), муниципального бюджета, а также внебюджетных источников.

2.2.3.8.6. Протокольные поручения.

Модуль должен обеспечивать формирование протокольных поручений в рамках реализации региональных проектов.

Протокольное поручение должно содержать реквизиты поручения, перечень исполнителей и лиц, осуществляющих контроль исполнения, перечень связанных проектов и объектов.

Модуль должен обеспечивать выполнение следующих функций:

создание поручений, в том числе периодически повторяющихся;

предоставление отчетов об исполнении поручения каждым исполнителем;

согласование отчетов об исполнении;

формирование сводной отчетности по исполнению поручений.

2.2.3.8.7. Риски объектов.

Модуль должен обеспечивать ведение реестра рисков реализации каждого объекта.

Карточка риска должна содержать:

тип риска;

описание риска;

влияние риска на результаты работ по объекту;

вероятность наступления риска;

дату выявления и плановую дату снятия риска;

перечень негативных последствий.

Для каждого риска должна обеспечиваться возможность ведения перечня мер реагирования.

2.2.3.8.8. Анализ информационного сопровождения и брендирования.

Модуль должен обеспечивать загрузку, обработку, хранение и визуализацию данных об информационном сопровождении региональных проектов, реализуемых в рамках национальных проектов, и данных о размещении носителей с имиджевым брендированием и QR-кодом в разрезе объектов.

Основным источником данных являются файлы формата XLSX, загружаемые по правилам п. 2.2.3.8.9, в том числе:

сводная информация об утвержденных материалах (отчетах) в разрезе каналов коммуникаций, федеральных информационных кампаний и организаций;

сводная информация об утвержденных инфоповодах в разрезе организаций с указанием начисленных баллов рейтинга;

сводная информация об утвержденных материалах (отчетах) в разрезе организаций с указанием начисленных баллов рейтинга;

сводная информация о наличии носителей с имиджевым брендированием и с QR-кодом в разрезе объектов и исполнительных органов Донецкой Народной Республики.

Модуль должен обеспечивать формирование следующей сводной отчетности:

сводный отчет по количеству утвержденных материалов (отчетов) в разрезе каналов коммуникаций (с расчетом итоговых баллов и просмотром в динамике за несколько отчетных периодов);

рейтинг исполнительных органов по информационному освещению национальных проектов (расчет сводного рейтинга и его прироста к предыдущему месяцу, анализ динамики количества реализуемых проектов, инфоповодов, баллов за инфоповоды, утвержденных материалов и баллов за них);

сводный отчет по брендированию и носителям QR;

сводные дашборды с возможностью выгрузки в формат презентации.

2.2.3.8.9. Общие правила загрузки данных из XLSX.

Настоящие правила применяются при загрузке данных, предусмотренной п. 2.2.3.8.8. Модуль должен обеспечивать выполнение следующих функций:

загрузка XLSX-файлов: предоставление интерфейса загрузки файла через

стандартный диалог выбора файла;

выбор отчетной даты, на которую производится загрузка;

для данных о брендировании и QR – дополнительно выбор типа загрузки (автоматически создавать новые объекты либо пропускать отсутствующие);

валидация структуры файла: проверка наличия обязательных столбцов с точными наименованиями полей (для данных о брендировании и QR – Global ID, федеральный проект, тип объекта, тип работ, населенный пункт, статус объекта, Имиджевое/QR, исполнительный орган Донецкой Народной Республики);

при несоответствии структуры – блокировка обработки файла и вывод сообщения с указанием отсутствующих столбцов;

валидация данных: проверка отсутствия пустых значений в ключевых полях и наличия элементов в связанных справочниках; при обнаружении ошибок – формирование списка ошибок без прерывания обработки корректных строк;

импорт данных: загрузка данных в базу данных после успешной валидации с сохранением сведений о пользователе, дате и времени загрузки;

при импорте данных о брендировании и QR – обновление реестра объектов (сопоставление по Global ID, актуализация статуса брендирования и наличия QR) с выводом сведений о добавленных и пропущенных объектах.

2.2.3.8.10. Интеграция с budget.gov.ru

Модуль должен обеспечивать загрузку структуры паспортов региональных проектов на основе API-интерфейса 7710168360-RPASSPORT, содержащего сведения об основных параметрах реализации региональных проектов, обеспечивающих достижение целей, показателей и результатов федеральных проектов в части полномочий субъекта Российской Федерации и вопросов местного значения муниципальных образований.

Модуль должен обеспечивать автоматическое обновление разделов паспортов проектов в составе, определенном в п. 2.2.3.8.1, а также вести логи изменений паспортов, произведенных в ходе актуализации данных посредством указанного API-интерфейса.

2.2.3.8.11. Картографическое представление объектов.

Модуль должен обеспечивать отображение на карте объектов, реализуемых в рамках проектов, и выполнение следующих функций:

задание географических координат каждого объекта с возможностью предварительного просмотра введенного местоположения (для отображения должна использоваться публичная картографическая подложка, подписка предоставляется Заказчиком);

настройка карточки объекта для отображения на карте;

формирование картографического представления объектов с возможностью фильтрации отображаемых объектов.

2.2.3.8.12. Аналитическая отчетность по исполнению проектов.

Модуль должен обеспечивать формирование аналитической и регламентной отчетности по проектам на основе данных остальных разделов Модуля.

В Модуле должно быть настроено разграничение прав доступа к информации в соответствии с ролью пользователя.

Должны быть настроены следующие отчетные представления:

сводные дашборды по исполнению региональных проектов, включающие: бюджет проекта (план, факт), процент кассового исполнения, количество реализуемых объектов, статус исполнения контрольных точек, статус исполнения показателей проекта. На дашбордах должна быть настроена цветовая индикация степени достижения плановых значений (по срокам, бюджету, индикаторам) и переходы к детализированной информации по проекту и его структурным элементам (карточки проектов, объектов, контрактов, показателей и контрольных точек);

тематические представления, требования к которым описаны в соответствующих разделах Модуля: визуализация план-графиков в виде диаграммы Ганта (п.2.2.3.8.2); сводная отчетность и дашборды по информационному сопровождению и брендированию (п.2.2.3.8.8); картографическое представление объектов (п.2.2.3.8.11);

формы регламентной отчетности:

информация об объемах бюджетных средств (ФБ и РБ);

финансирование проектов в разрезе исполнителей;

свод по достижению показателей проектов;

анализ план-графиков работ по объектам с возможностью сравнения версий;

отчетность для ИФНС (с аналитикой по контрактам со снижением НМЦК выше 25 % и выборкой подрядчиков, участвующих более чем в 3 закупках);

сводная информация по исполнению поручений;

сводная информация по исполнению планов-графиков объектов в разрезе исполнителей;

информация об исполнении плана реализации регионального проекта (мероприятий, контрольных точек).

Состав показателей, отчетных форм и справочников Модуля уточняется Исполнителем и согласуется с Заказчиком в ходе оказания услуг.

2.2.4. Общие требования.

2.2.4.1. Требования к способам и средствам связи для информационного обмена.

Информационный обмен между компонентами Системы должен

обеспечиваться с помощью современных протоколов и форматов передачи данных, между серверной частью Системы и клиентскими приложениями должен осуществляться по протоколу HTTP, на транспортном уровне для взаимодействия компонентов Системы должен использоваться стек протоколов TCP/IP.

Информационный обмен между клиентскими местами и серверами должен осуществляться с использованием Интернет-технологий, средств СУБД, реализующих клиент-серверную технологию.

Информационное взаимодействие между физическими серверами Системы (при использовании многосерверной конфигурации) должно обеспечиваться посредством локальной сети типа Ethernet 100/1000, обеспечивающей передачу данных по протоколу TCP/IP.

Компоненты подсистемы ИАС должны обеспечивать возможность взаимодействия с ведомственными информационными системами за счет использования API загрузки данных.

2.2.4.2. Показатели назначения.

Система должна быть реализована по принципу открытой архитектуры, обеспечивающей возможность встраивания и взаимодействия с другими информационными системами.

Система должна обеспечить централизованный учет, хранение, обработку и представление информации в соответствии с правами доступа Пользователей.

Система должна иметь открытые интерфейсы для развития и интеграции, обеспечивать своевременное и корректное представление информации всем зарегистрированным Пользователям.

Система должна обеспечить возможность поэтапного наращивания своих возможностей, как по производительности, так и по функциональности. Возможности масштабирования должны обеспечиваться средствами используемого системного и прикладного программного обеспечения.

Система должна быть адаптирована к изменяющемуся количеству Пользователей. Подключение новых Пользователей не должно влиять на изменение архитектуры ИАС.

Система должна быть устойчивой по отношению к ошибкам эксплуатационного, технического персонала и Пользователей, отказам технических и программных средств.

Система должна обеспечивать возможность одновременного просмотра Пользователями одного информационного объекта.

Должна быть обеспечена возможность конфигурирования ИАС собственными силами Заказчика посредством параметризации и настройки подсистем.

2.2.4.3. Требования к надежности.

Количественные значения показателей надежности для Системы:

- среднее время восстановления работоспособности программно-технических средств ИАС должно составлять не более 3 часов, без учета времени решения организационных вопросов;

- среднее время восстановления работоспособности Системы после отказов технических средств должно составлять не более 3 часов, без учета времени решения организационных вопросов;

- среднее время восстановления работоспособности Системы после отказа системного или прикладного программного обеспечения должно составлять не более 3 часов без учета времени решения организационных вопросов;

- среднее время восстановления работоспособности Системы в случае сбоя или отказа из-за ошибок прикладного программного обеспечения должно составлять до 3 часов;

- максимальное время простоя ИАС должно составлять не более 3 часов, без учета времени решения организационных вопросов;

- общее максимальное время простоя ИАС в течение года должно составлять не более 100 часов.

Количественные значения показателей надежности должны уточняться по результатам опытной эксплуатации Системы.

2.2.4.4. Требования к режимам функционирования Системы.

РИС должна функционировать в следующих режимах:

– штатный режим, при котором должно обеспечиваться выполнение задач Пользователей в объеме функций, предусмотренных настоящим Техническим заданием в режиме 24 часа 7 дней в неделю;

– режим системного администрирования (профилактический), необходимый для проведения технического обслуживания, реконфигурации и пополнения технических и программных средств ИАС новыми компонентами;

– аварийный режим, при котором Система недоступна для функционирования.

2.2.4.5. Требования к информационной безопасности.

В Системе должно быть реализовано разделение полномочий и ролей Пользователей.

В Системе должны быть реализованы следующие механизмы безопасности прикладного уровня:

– управление правами доступа;

– аутентификация и идентификация.

До начала оказания услуг Заказчик и Исполнитель должны заключить дополнительное соглашение «о конфиденциальности и безопасности

персональных данных».

По окончании оказания Услуг Заказчиком совместно с Исполнителем должно быть проведено тестирование корректного функционирования Системы с установленными и настроенными в соответствии с политиками Заказчика СЗИ.

Система должна быть совместима с сертифицированными ФСТЭК России СЗИ. В случае выявления конфликта совместимости СЗИ и компонентов Системы, Исполнитель должен доработать (донастроить) Систему для разрешения конфликта с СЗИ.

2.2.4.5.1. Требования к защите информации от несанкционированного доступа.

Система должна обеспечивать меры защиты информации от несанкционированного доступа:

– доступ к Системе посредством web-интерфейса;

– средства идентификации пользователей (вход в пользовательскую часть возможен только при указании имени пользователя и пароля);

– разграничение доступа Пользователей к функциям Системы на основе ролевой модели;

– разграничение доступа к данным на уровне отдельных информационных сущностей (справочников, групп показателей, реестров, форм, отчетов, дашбордов).

2.2.4.5.2. Требования к управлению правами доступа.

Реализация механизма управления правами доступа в Системе должна удовлетворять требованиям:

– механизм распределения прав доступа к функциям Системы должен позволять предоставление Пользователям прав, минимально необходимых для выполнения их функциональных обязанностей;

– архитектура и построение базы данных должны быть таковы, чтобы права Пользователей в базе данных не превышали прав Пользователей в прикладной Системе;

– механизм распределения прав доступа должен охватывать все операции Пользователей над объектами (данные, хранимые или обрабатываемые в Системе), а все объекты и операции над ними должны охватываться механизмом распределения прав доступа;

– механизм разграничения прав доступа должен быть реализован на основе ролей;

– роли должны быть на основе функциональной позиции Пользователя с учетом принципа минимальных полномочий и иерархии Пользователя в организационной структуре;

– ролевая модель должна охватывать и определять доступ к данным, хранимым и обрабатываемым в Системе;

– создание отчетов должно осуществляться с учетом ролевой модели и разграничения доступа к данным;

– должно осуществляться блокирование анонимного доступа к базе данных, подключения должны производиться только для авторизованных Пользователей.

2.2.4.5.3. Требования к механизмам аутентификации.

Пользователи Системы должны однозначно идентифицироваться и аутентифицироваться для всех видов доступа, кроме тех видов доступа, которые определяются, как действия по ознакомлению с общедоступной информацией, опубликованной в Системе для доступа неограниченного числа Пользователей в сети Интернет.

После успешного прохождения Пользователем процедур аутентификации:

– Пользователю предоставляются закрепленные за ним права доступа к информации и функциям Системы;

– действия Пользователя регистрируются средствами подсистемы аудита.

Реализация механизмов аутентификации должна удовлетворять требованиям:

– доступ к информации и функциям Системы должен предоставляться Пользователю только после предъявления уникального персонифицированного идентификатора (имени) Пользователя и проведения процедуры аутентификации на основе вводимой Пользователем информации (пароль);

– должна быть обеспечена возможность определения авторства операции и отсутствие неавторизованных операций на основе уникальных персонифицированных идентификаторов каждого Пользователя, процедуры аутентификации и протоколирования действий Пользователей в журналах аудита.

Доступ в Систему должен осуществляться с обязательным вводом пароля.

В Системе должна присутствовать возможность установить минимальные характеристики пароля:

– длина пароля не менее шести символов;

– максимальное количество неуспешных попыток аутентификации (ввода неправильного пароля) до блокировки — 5 попыток;

– блокировка программно-технического средства или учетной записи Пользователя в случае достижения установленного максимального количества неуспешных попыток аутентификации от 10 до 30 минут;

– смена паролей не более чем через 120 дней.

Механизмами Системы должно быть реализовано блокирование учетной записи Пользователя через период времени неиспользования не более 90 дней.

Вводимые символы пароля должны отображаться условными знаками (например, «*», «•») или не отображаться вовсе.

Механизмами Системы должна быть реализована возможность смены пароля учетной записи администратором Системы.

Механизмами Системы должна быть реализована защита аутентификационной информации от неправомерного доступа к ней и модифицирования. В частности, не допускается размещение пароля для доступа к базе данных в тексте кода веб-приложения. Пароли должны храниться в Системы не в открытом, а в преобразованном виде (например, с использованием хеш-функций). При этом не допускается использовать слабые алгоритмы преобразования (например, md5, sha-1). Пароли должны передаваться в преобразованном виде.

При вводе неверного логина или пароля сообщения об ошибке не должны различаться.

2.2.4.5.4. Требования к журналированию событий.

Должно осуществляться журналирование действий Пользователей Системы с регистрацией событий:

– вход (выход), попытки входа;

– изменение прав доступа Пользователей, создание новых Пользователей;

– выполнение задачи резервного копирования данных и настроек Системы.

При регистрации событий должна быть зафиксирована информация:

– дата и время действия;

– результат действия (успех/неудача).

Только Администратор Системы должен иметь доступ к журналу событий. Администратор Системы и Пользователи не должны иметь возможности редактировать журнал событий.

2.2.4.5.5. Требования к веб-интерфейсу.

Доступ к административному разделу веб-приложения Системы должен быть возможен только из инфраструктуры Заказчика.

Должна быть обеспечена фильтрация загружаемых Пользователями Системы файлов.

Сообщения об ошибках должны фиксироваться в специальных журналах, доступ к которым ограничен для посторонних лиц.

Механизмы Системы должны обеспечивать блокирование сеанса доступа

Пользователя после 15 минут бездействия (неактивности) Пользователя. В пользовательском интерфейсе Системы после блокировки сеанса не должна отображаться информация сеанса Пользователя.

Доступ Пользователей к веб-интерфейсу Системы должен осуществляться по протоколу HTTPS. Для реализации HTTPS должен использоваться протокол TLS версии 1.2 и выше. При обращении пользователя по протоколу HTTP к веб-интерфейсу Системы он должен быть перенаправлен на соединение по HTTPS.

2.2.4.5.6 Требования к классификации Системы и определения уровня защищенности персональных данных

Для Системы должны быть определены уровень защищенности персональных данных и класс защищенности.

Определение уровня защищенности персональных данных Системы должно производиться в соответствии с требованиями Постановления Правительства Российской Федерации от 1 ноября 2012 г. № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных».

Результаты определения уровня защищенности персональных данных должны быть зафиксированы в документе «Проект акта определения уровня защищенности персональных данных».

Определение класса защищенности Системы должно производится в соответствии с требованиями Приказа ФСТЭК России от 11 апреля 2025 года № 117 «Об утверждении требований о защите информации, содержащейся в государственных информационных системах, иных информационных системах государственных органов, государственных унитарных предприятий, государственных учреждений», с учетом установленного уровня защищенности персональных данных.

Результаты классификации должны быть зафиксированы в документе «Проект акта классификации информационной системы».

2.2.4.5.7 Требования к разработке Модели угроз безопасности

Исполнителем должна быть разработана Модель угроз безопасности в соответствии с Методическим документом, утвержденным ФСТЭК России 05 февраля 2021 г. «Методика оценки угроз безопасности информации», а также с методическими и руководящими документами ФСБ России.

Модель угроз безопасности должна содержать описание Системы и ее структурно-функциональных характеристик, а также описание угроз безопасности информации, включающее описание возможностей нарушителей (модель нарушителя), возможных уязвимостей, способов реализации угроз безопасности информации и последствий от нарушения свойств безопасности информации.

Модель угроз безопасности информации Системы должна включать:

1. Общие положения.

2. Описание Системы (сегментов Системы) и особенностей ее функционирования:

– Цели и задачи, решаемые Системой (сегментом Системы).

– Класс защищенности, категория значимости систем и сетей, уровень защищенности персональных данных.

– Номенклатура защищаемых данных, обрабатываемых в Системе (подсистеме) и функциональных задач, для решения которых они используются.

– Назначение и структура объектов информатизации (сегментов) Системы.

– Описание структурно-функциональных характеристик информационной системы (состав технических и программных средств Системы, сетевая инфраструктура).

– Описание взаимосвязей с другими информационными системами (подсистемами) и телекоммуникационными сетями.

– Описание групп внешних и внутренних пользователей систем и сетей, уровней их полномочий и типов доступа.

– Описание процессов обеспечения информационной безопасности.

– Описание технологии обработки информации.

– Информация о функционировании систем и сетей на базе информационно-телекоммуникационной инфраструктуры центра обработки данных.

3. Возможные негативные последствия от реализации (возникновения) угроз безопасности информации:

– Описание рисков (ущербов) от нарушения или прекращения основных процессов.

– Описание негативных последствий, приводящих к возникновению рисков (ущерба).

4. Источники угроз безопасности информации (модель нарушителя):

– Характеристика нарушителей и возможные цели реализации ими угроз безопасности информации.

– Категории актуальных нарушителей.

– Описание возможностей нарушителей по реализации ими угроз безопасности применительно к назначению, составу и архитектуре систем и сетей.

5. Способы реализации (возникновения) угроз безопасности информации:

– Описание способов реализации (возникновения) угроз безопасности информации.

– Описание интерфейсов объектов воздействия.

6. Актуальные угрозы безопасности информации, включая:

– Перечень возможных (вероятных) угроз безопасности информации для соответствующих способов их реализации и уровней возможностей нарушителей.

– Описание возможных сценариев реализации угроз безопасности информации.

7. Выводы об актуальности угроз безопасности информации.

8. Перечень актуальных угроз информационной безопасности.

9. Выводы о необходимом к применению (или его отсутствии) классе СКЗИ.

При идентификации возможных угроз безопасности информации должен использоваться Банк данных угроз безопасности информации, сформированный ФСТЭК России (http://bdu.fstec.ru/), учитывая структурно-функциональные особенности Системы, возможные источники угроз.

В соответствии с требованиями пункта 3 Требований к порядку создания, развития, ввода в эксплуатацию, эксплуатации и вывода из эксплуатации государственных информационных систем и дальнейшего хранения содержащейся в их базах данных информации, утвержденных Постановлением Правительства РФ от 06.07.2015 № 676 «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», модель угроз безопасности информации согласуется с федеральным органом исполнительной власти в области обеспечения безопасности и федеральным органом исполнительной власти, уполномоченным в области противодействия техническим разведкам и технической защиты информации, в пределах их полномочий в части, касающейся выполнения установленных требований о защите информации. Согласование Модели угроз безопасности проводится силами Заказчика.

2.2.4.5.8 Требования к разработке Частного технического задания на создание системы защиты информации

На основе перечня актуальных угроз и возможностей нарушителя безопасности информации, Исполнителем должны быть определены требования по защите информации, подлежащие реализации в составе системы защиты информации Системы. Частное техническое задание на создание системы защиты информации в том числе должно содержать:

1. Цель и задачи обеспечения защиты информации.

2. Класс защищенности Системы.

3. Перечень нормативных правовых актов, методических документов и национальных стандартов, которым должна соответствовать Система.

4. Перечень объектов защиты Системы.

5. Требования к мерам и средствам защиты информации, применяемым в Системе.

6. Стадии (этапы работ) создания системы защиты Системы.

7. Требования к используемым техническим средствам, программному обеспечению, средствам защиты информации.

8. Функции заказчика и оператора по обеспечению защиты информации на Систему.

9. Требования к защите средств и систем, обеспечивающих функционирование Системы (обеспечивающей инфраструктуре).

10. Требования к защите информации при информационном взаимодействии с иными информационными системами и информационно-телекоммуникационными сетями.

Согласование Частного технического задания на создание системы защиты информации с регуляторами проводится силами Заказчика.

2.2.2.5.9 Требования к разработке технического проекта на создание системы защиты информации

Исполнителем должен быть разработан технический проект на создание системы защиты информации, включающий в себя:

- пояснительная записка к техническому проекту;
- ведомость технического проекта;
- спецификация системы защиты информации.

Проектные решения по построению системы защиты информации должны быть выполнены с учетом ГОСТ Р 59795-2021 «Информационные технологии. Комплекс стандартов на автоматизированные системы. Автоматизированные системы. Требования к содержанию документов» и должны отражать следующие предложения:

1. 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).

2. 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 Системе.

3. Меры защиты информации, подлежащие реализации в системе защиты информации.

4. Виды и типы средств защиты информации, обеспечивающие реализацию технических мер защиты информации.

5. Структура системы защиты информации Системы, включая состав (количество) и места размещения ее элементов.

6. 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 Системы.

7. Меры защиты информации при информационном взаимодействии с иными информационными системами и информационно-телекоммуникационными сетями.

Комплекс организационных и технических мер, направленных на нейтрализацию актуальных угроз безопасности, определенных с учетом специфики Системы и условий ее функционирования, должны предусматривать меры защиты информации, указанные в методическом: документе «Состав и содержание мероприятий и мер по защите информации, содержащейся в информационных системах», утвержденный ФСТЭК России 12.04.2026.

Меры защиты информации должны выбираться в системе защиты информации с учетом угроз безопасности информации применительно ко всем объектам и субъектам доступа Системы на аппаратном, системном, прикладном и сетевом уровнях, в том числе в среде виртуализации и облачных вычислений.

2.2.4.5.10 Требования к разработке эксплуатационной и организационно-распорядительной документации

В рамках проектирования системы защиты информации Исполнителем должны быть разработаны эксплуатационной и организационно-распорядительной документы в соответствии с методическим: документом «Состав и содержание мероприятий и мер по защите информации, содержащейся в информационных системах», утвержденный ФСТЭК России 12.04.2026 и приказом ФСТЭК России от 11.04.2025 № 117 «Об утверждении Требований о защите информации, содержащейся в государственных информационных системах, иных информационных системах государственных органов, государственных унитарных предприятий, государственных учреждений».

Эксплуатационная и организационно-распорядительная документация должна включать в себя в том числе:

– руководство администратора безопасности Системы;

– руководство пользователя системы защиты информации Системы;
– инструкция по эксплуатации системы защиты информации.

Состав разрабатываемых документов должен быть уточнен на этапе технического проектирования системы защиты информации Системы.

Работы по поставке, установке и настройке средств защиты информации, необходимых для реализации системы защиты информации Системы осуществляются силами Заказчика.

2.2.4.6. Требования по сохранности информации.

При эксплуатации ИАС должны приниматься меры по регулярному резервному копированию, хранению снимков состояния, и, при необходимости, восстановлению данных. Резервное копирование метаданных (настроек показателей и измерений) должно осуществляется средствами ИАС. Резервное копирование основных данных, загружаемых в Систему, должно осуществиться средствами СУБД и общесистемного программного обеспечения.

Отказоустойчивость ИАС должна соответствовать уровню современных информационных Систем класса «клиент-сервер».

Отказ клиентской рабочей станции не должен приводить к нарушениям работы других клиентских станций и ИАС в целом, к разрушению целостности базы данных.

Отказ сервера, на котором функционирует СУБД, не должен приводить к потере данных за срок, превышающий период до последнего архивирования базы данных.

Для обеспечения защиты данных от разрушений при авариях и сбоях в процессе выполнения пользовательских задач при повреждении журналов регистрации СУБД должно быть обеспечено создание резервных копий баз данных.

Резервное копирование баз данных должно осуществляться в соответствии с регламентом их ведения, но не реже чем один раз в неделю. В соответствии с регламентом ведения данных должно быть обеспечено регулярное создание резервных копий изменений баз данных и резервное копирование виртуального сервера, и периодическое создание полных копий резервируемых баз данных, и резервное копирование виртуального сервера. Копирование и архивирование данных ИАС должно осуществляться без прерывания функционирования сервисов ИАС.

2.2.4.7. Требования к эргономике и технической эстетике.

Взаимодействие пользователей с ИАС должно осуществляться посредством визуального графического интерфейса.

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

отображение экранных форм.

Навигационные элементы должны быть выполнены в удобной для пользователя форме.

Средства редактирования информации должны удовлетворять принятым соглашениям в части использования функциональных клавиш, режимов работы, поиска, использования оконной системы.

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.

Интерфейс должен быть рассчитан на преимущественное использование манипулятора типа «мышь», то есть управление ИАС должно осуществляться с помощью набора экранных меню, кнопок, значков и т. п. элементов. Клавиатурный режим ввода должен использоваться главным образом при заполнении и/или редактировании текстовых и числовых полей экранных форм.

Все надписи экранных форм, а также сообщения, выдаваемые пользователю (кроме системных сообщений), должны быть на русском языке.

Система должна обеспечивать корректную обработку аварийных ситуаций, вызванных неверными действиями Пользователей, неверным форматом или недопустимыми значениями входных данных. В указанных случаях ИАС должна выдавать Пользователю соответствующие сообщения, после чего возвращаться в рабочее состояние, предшествовавшее неверной (недопустимой) команде или некорректному вводу данных.

Экранные формы должны проектироваться с учетом требований унификации:

– все экранные формы пользовательского интерфейса должны быть выполнены в едином графическом дизайне, с одинаковым расположением основных элементов управления и навигации;

– для обозначения одних и тех же операций должны использоваться одинаковые графические значки, кнопки и другие управляющие (навигационные) элементы, должны быть унифицированы термины, используемые для описания идентичных понятий, операций и действий Пользователя;

– реакция ИАС на действия оператора (наведение указателя «мыши», переключение фокуса, нажатие кнопки) должна быть типовой для каждого действия над одними и теми же графическими элементами, независимо от их расположения на экране.

2.2.4.8. Требования к патентной чистоте.

Исполнитель должен использовать только объекты интеллектуальной

собственности, права на которые приобретены (получены) и используются без нарушений прав на интеллектуальную собственность третьих лиц. Это требование должно обеспечивать соблюдение авторских, смежных, патентных и иных прав разработчиков используемых сторонних компонент.

2.2.4.9. Требования по стандартизации и унификации.

Системная архитектура ИАС должна быть построена на основе унифицированных технических решений.

Прикладное программное обеспечение ИАС должно быть построено с использованием стандартных и унифицированных методов разработки программных систем.

В составе ИАС по возможности должны применяться типовые (унифицированные) классификаторы и справочники, действие которых на территории Российской Федерации определено соответствующими нормативными актами и стандартами. В ИАС должна быть предусмотрена возможность наращивания классификаторов и справочников.

2.2.4.10. Требования к информационному обеспечению.

Информационное обеспечение ИАС должно включать в свой состав совокупность всех необходимых для функционирования Системы данных и систем обеспечения. В состав информационного обеспечения требуется включить нормативно-справочную информацию, информационные объекты, входные и выходные данные, структуру управления базами данных.

Состав данных должен быть достаточным для выполнения всех функций Системы и отвечать требованиям полноты, достоверности, однозначной идентификации, непротиворечивости и необходимой точности представления.

ИАС должна соответствовать требованию однократного ввода данных вне зависимости от того, в каких информационных массивах или базах данных они будут храниться и какими функциональными подсистемами использоваться.

ИАС должна обеспечивать первичный контроль вводимых данных на соответствие формальным правилам: проверка типов, размерности, допустимости значений.

2.2.4.11. Требования к программному и техническому обеспечению.

Программное обеспечение ИАС должно обеспечивать решение функций и задач ИАС.

Системное и прикладное программное обеспечение должно поддерживать формат кириллицы и иметь эксплуатационную документацию на русском языке.

Для функционирования ИАС должно использоваться унифицированное системное и прикладное программное обеспечение.

Системное программное обеспечение должно обеспечить, поддержку технологий мониторинга и управления локальных вычислительных сетей, и

управления регламентами.

Прикладное программное обеспечение должно включать вновь разрабатываемое программное обеспечение ИАС, обеспечивающее непосредственную реализацию ее функций.

Программное обеспечение ИАС должно функционировать на базе ОС, указанных в таблице ниже. Исполнитель обязан поставить, установить и настроить лицензионные копии ОС для всех серверов, задействованных в проекте. Заказчик предоставляет аппаратное обеспечение (серверы, СХД, сетевое оборудование) и базовую инфраструктуру виртуализации.

Исполнитель вправе выбрать любую ОС из списка поддерживаемых при условии, что она обеспечивает полную совместимость с поставляемым прикладным ПО и соответствует требованиям по защите информации для государственных информационных систем с классом защищенности, определённым в п. 2.2.4.5.6.

Все поставляемые ОС должны иметь действующий сертификат ФСТЭК России о соответствии требованиям безопасности информации.

Допускается использование аналогов указанных ОС при условии их включения в единый реестр отечественного ПО и наличия сертификата ФСТЭК.

Тип сервера/рабочей станции	ОС	СУБД	Дополнительные программы
Рабочая станция	ОС семейства Linux, сертифицированные ФСТЭК России	–	Веб-браузер: Яндекс.Браузер 22 и выше, Cromium 120 и выше
Сервер Подсистемы ETL	Astra Linux SE 1.6 (Смоленск) или эквивалент с сертификатом ФСТЭК	PostgresPRO	–
Продуктивный сервер Подсистемы аналитической обработки и визуализации информации	– Astra Linux SE 1.7.5 x64 – Astra Linux SE 1.8 x64 – Альт Сервер 10.0 x64 – Роса Хром Сервер 12.4 – RED OS 7.3 – RED OS 8 или эквивалент с сертификатом ФСТЭК	–	–

Тип сервера/рабочей станции	ОС	СУБД	Дополнительные программы
Сервер для тестирования и разработки Подсистемы аналитической обработки и визуализации информации	– Astra Linux SE 1.7.5 x64 – Astra Linux SE 1.8 x64 – Альт Сервер 10.0 x64 – Роса Хром Сервер 12.4 – RED OS 7.3 – RED OS 8 или эквивалент с сертификатом ФСТЭК	—	—

В соответствии с постановлением Правительства Российской Федерации от 16.11.2015 № 1236 «Об установлении запрета на допуск программного обеспечения, происходящего из иностранных государств, для целей осуществления закупок для обеспечения государственных и муниципальных нужд» устанавливается запрет на допуск программ для электронных вычислительных машин и баз данных, реализуемых независимо от вида договора на материальном носителе и (или) в электронном виде по каналам связи, происходящих из иностранных государств (за исключением программного обеспечения, включенного в единый реестр программ для электронных вычислительных машин и баз данных из государств-членов Евразийского экономического союза, за исключением Российской Федерации (далее – реестр евразийского программного обеспечения), а также исключительных прав на такое программное обеспечение и прав использования такого программного обеспечения, для целей осуществления закупки.

Ссылка на официальный сайт реестра российского программного обеспечения:

https://reestr.digital.gov.ru/

Ссылка на официальный сайт реестра евразийского программного обеспечения:

https://eac-reestr.digital.gov.ru/

В соответствии с Приказом Министерства цифрового развития, связи и массовых коммуникаций Российской Федерации от 22.09.2020 № 486 «Об утверждении классификатора программ для электронных вычислительных машин и баз данных» закупаемое программное обеспечение относится к разделу «Средства анализа данных», классам:

«Инструменты извлечения и трансформации данных (ETL)», код (числовое обозначение) раздела и класса программ для ЭВМ и баз данных 11.01,

«Средства аналитической обработки в реальном времени (OLAP)», код (числовое обозначение) раздела и класса программ для ЭВМ и баз данных 11.03,

«Средства интеллектуальной обработки информации и интеллектуального анализа бизнес-процессов», код (числовое обозначение) раздела и класса программ для ЭВМ и баз данных 05.13

3. Порядок и условия предоставления Услуг

Ключ активации Лицензии на предоставляемое программное обеспечение должен включать в себя:

- полное наименование предоставляемого программного обеспечения;
- полное наименование Заказчика;
- количество пользователей.

Права использования программного обеспечения передаются для использования на территории Российской Федерации.

Действие прав использования программного обеспечения распространяется на обновления, дополнения, добавляемые компоненты, службы поддержки продукта, которые относятся к программному обеспечению, в течение срока действия гарантийного обслуживания.

Исполнителем должна быть предоставлена инструкция по доступу к сайту производителя (правообладателя) программного обеспечения для получения дистрибутива программного обеспечения.

Исполнитель обеспечивает настройку подсистемы прикладных задач под условия Донецкой Народной Республики. В частности, вносит перечень муниципальных образований, настраивает картосхему и права доступа.

Исполнитель обязан в течение 5 (пяти) рабочих дней с даты заключения Контракта разработать и согласовать с Заказчиком график оказания услуг по внедрению программного обеспечения (далее – График).

4. Порядок сдачи и приемки оказанных Услуг

4.1. Исполнитель в день окончания срока оказания Услуг, наряду с документом о приемке, предоставляет Заказчику следующие отчетные документы на бумажном носителе:

– подписанный со своей Стороны Акт приема-передачи прав использования программы для ЭВМ (программное обеспечение подсистемы оркестрации ETL-процессов, программное обеспечение инструментальных средств, программное обеспечение подсистемы прикладных аналитических модулей) в двух экземплярах, по одному для каждой из Сторон;

– лицензионное свидетельство с указанием наименования Лицензиата

(или сертификат, или иной документ, установленный правообладателем, Лицензиаром);

- установочные файлы программного обеспечения;
- установочные файлы (дистрибутивы) ОС, переданных в составе лицензий;
- копии сертификатов ФСТЭК России на поставленные версии ОС;
- руководство пользователя;
- руководство администратора;
- акт приемочных испытаний.

Допускается передача документации на лицензионное программное обеспечение в виде ссылок на онлайн документацию производителя.

4.2. Требования к составу и содержанию работ по подготовке к вводу в действие.

Для создания условий функционирования объектов автоматизации, при которых гарантируется соответствие создаваемой Системы требованиям, содержащимся в настоящем документе, и возможность эффективного использования Системы, Заказчиком обеспечивается проведение следующих мероприятий:

обеспечение необходимой инфраструктуры для функционирования Системы, включая защищенные каналы связи;

обеспечение необходимых организационных мероприятий по назначению специалистов Заказчика, отвечающих за эксплуатацию Системы, а также для взаимодействия Исполнителя с Заказчиком по возникающим вопросам, связанных с оказанием Услуг.

Исполнителю необходимо выполнить условия:

обеспечить совместимость программного обеспечения с последней версией операционной системы на момент подписания контракта и последних стабильных версий прикладного программного обеспечения в рамках данной версии операционной системы (согласно требованиям настоящего Технического задания);

4.3. Требования к документированию.

4.3.1. Состав технической документации:

описание комплекса технических средств;

описание программного обеспечения;

матрица доступа Пользователей к ресурсам (в Системе для описания матрицы доступа должна использоваться ролевая модель контроля доступа (RBAC) с поддержкой ограничений и иерархии (модель RBAC3) в соответствии со стандартом ANSI INCITS 359 2012 «Ролевой метод контроля доступа»);

описание базы данных программного обеспечения и файлового хранилища

Системы.

Содержание документации должно быть достаточным для обеспечения эксплуатации программного обеспечения Системы.

4.3.2. Состав эксплуатационной документации:

– инструкция и регламент технического обслуживания Системы, включающие в себя:

– описание способов контроля администратором работоспособности Системы;

– информацию о логах, которые необходимо отслеживать, описание ошибок, которые могут возникнуть и действия, которые в этих случаях необходимо предпринимать;

– инструкция и регламент резервного копирования Системы, включающие в себя:

– список данных, подлежащих резервированию, в том числе данные, хранящиеся в базах данных (для каждого типа данных из списка должно быть составлено подробное руководство по созданию резервной копии);

– инструкция по разворачиванию Системы, соответствующая требованиям:

– инструкция должна подробно описывать установку Системы, начиная с момента, когда у администратора имеется только дистрибутивы Программного обеспечения Системы, а также необходимое для разворачивания оборудование и программное обеспечение, и заканчивая, когда Система развернута и полностью работоспособна в соответствии с тем функционалом, который она обеспечивает по документации;

– инструкция не должна создавать ситуации, в которых администратору приходится действовать на свое усмотрение (за исключением случаев, когда это явно указано);

– если при установке программного обеспечения сторонних разработчиков требуется выполнить действия, указанные в инструкциях к этому программному обеспечению, то это необходимо отразить в виде ссылок на разделы официальных инструкций данного программного обеспечения;

– инструкция по восстановлению базы данных Системы, включающая в себя:

– список данных, подлежащих восстановлению в случае сбоя (для каждого типа данных из списка должно быть составлено подробное руководство по восстановлению из резервной копии);

– список портов, которые должны быть открыты на каждом из серверов для корректной работоспособности Системы;

– список процессов, которые должны быть в работе на каждом из серверов для корректной работоспособности Системы;

– действия администратора перед отключением каждого из серверов Системы;

– действия администратора при включении каждого из серверов Системы;

– список возможных проблем, ошибок и методов их решения.

4.3.3. Техническая и эксплуатационная документация на Систему должна удовлетворять требованиям комплекса стандартов и руководящих документов на автоматизированные системы.

Документация должна предоставляться Заказчику в одном экземпляре в электронном виде (DVD, CD, USB-флеш-накопитель) в запароленном zip-архиве, подписанном для удостоверения и подтверждения подлинности открепленной электронной подписью в порядке, установленном законодательством Российской Федерации. Документация, предоставленная в электронном виде, должна быть в виде файлов с расширением *.PDF.

Документация должна быть выполнена на русском языке, за исключением официальных наименований используемого программного и технического обеспечения, а также кодов программ.

4.4. Результатом оказания предусмотренных в Техническом задании Услуг должны являться:

установленное на технических средствах Заказчика и настроенное ПО (программное обеспечение подсистемы оркестрации ETL-процессов, программное обеспечение подсистемы аналитической обработки и визуализации информации, программное обеспечение подсистемы прикладных задач) в соответствии с требованиями раздела п. 2.1 Технического задания, включая тестовый и промышленный контуры;

получение Заказчиком Лицензий и дистрибутивов программного обеспечения, удовлетворяющего требованиям Технического задания;

подписанный акт приемочных испытаний;

протокол инструктажа пользователей по работе с программным обеспечением.

Исполнитель разрабатывает и передает на утверждение Заказчику программу и методику приемочных испытаний.

4.6. Обязанности Исполнителя:

4.6.1. Исполнитель должен иметь возможность оказывать Услуги по гарантийному обслуживанию Системы по защищенному каналу связи между Исполнителем и Заказчиком.

Для организации защищенного канала связи с шифрованием

передаваемого трафика необходимо использовать сертифицированные ФСБ России средства криптографической защиты информации, совместимые с продуктовой линейкой защищенной ViPNet-сети исполнительных органов Донецкой Народной Республики, предоставляемые Заказчиком (1 лицензия) Исполнителю на время выполнения всех обязательств по Контракту.

4.6.2. Исполнитель должен иметь возможность обеспечить присутствие специалистов на технологической площадке Заказчика в случае возникновения сбоев в работе Системы, устранение которых по защищенному каналу связи невозможно.

4.6.3. Исполнитель должен предоставить контактные телефоны, по которым представитель Заказчика может информировать персонал Исполнителя о работе программного обеспечения, предоставленного в рамках Технического задания.

5. Гарантийное сопровождение (обслуживание)

Срок гарантийного сопровождения исчисляется с даты размещения Заказчиком в единой информационной системе документа о приемке результатов оказанных услуг и должен составлять 12 (двенадцать) месяцев.

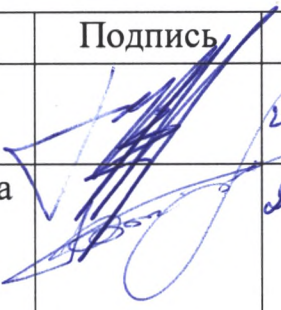
Гарантийное обслуживание должно включать в себя:

– обеспечение поддержки со стороны производителя (правообладателя) программного обеспечения в рамках консультационной помощи в режиме «горячей линии» по телефону, электронной почте с 09.00 до 18.00 в рабочее время Заказчика;

– исправление ошибок и устранение обнаруженных уязвимостей в ПО Системы, приводящих к неправильной или нестабильной работе Системы, либо препятствующих надлежащему обеспечению информационной безопасности и защиты информации в Системе от несанкционированного доступа, не выявленных Заказчиком при приемке оказанных Услуг.

5.3. Ошибки в реализации Системы, а также обнаруженные уязвимости Системы, выявленные в период гарантийного обслуживания, устраняются Исполнителем в рамках очередного обновления Системы или в рамках внеочередного экстренного обновления в случае, если обнаруженные ошибки препятствуют или ограничивают эксплуатацию Системы в штатном режиме.

СОСТАВИЛИ

ФИО	Должность исполнителя	Подпись	Дата
Романов Андрей Николаевич	Заместитель директора		24.08.2026
Балицкий Андрей Владимирович	Руководитель департамента системного администрирования инженерных систем, разработки и эксплуатации центров обработки данных		24.08.2026