**ТЕХНИЧЕСКОЕ ЗАДАНИЕ**

**на оказание услуг по развитию информационной системы управления**

**проектами (ИСУП)**

[Используемые сокращения, термины и определения 9](#__RefHeading___1)

[1. Общие сведения 13](#__RefHeading___2)

[1.1. Наименование Системы 14](#__RefHeading___3)

[1.2. Наименование предприятий разработчика и заказчика 14](#__RefHeading___4)

[1.3. Назначение и цели создания Системы 14](#__RefHeading___5)

[1.4. Требования к выполняемым работам 14](#__RefHeading___6)

[1.5. Общие требования к развитию системы 14](#__RefHeading___7)

[1.5.1 Требования к проведению тестирования 16](#__RefHeading___8)

[2. Требования к системе 20](#__RefHeading___9)

[2.1 Требования к технологическому стеку 20](#__RefHeading___10)

[2.2 Требования к журналированию действий пользователей 20](#__RefHeading___11)

[2.3 Требования к информационной безопасности 21](#__RefHeading___12)

[2.4 Защита информации в случаях сбоя 22](#__RefHeading___13)

[2.5 Требования к хранению и обработке персональных данных 22](#__RefHeading___14)

[2.6 Требования к эргономике и технической эстетике 23](#__RefHeading___15)

[2.7 Требования к патентной чистоте 23](#__RefHeading___16)

[2.8 Масштабирование системы 24](#__RefHeading___17)

[2.9 Требования по стандартизации и унификации  24](#__RefHeading___18)

[2.10 Требования Приказа ФСТЭК №21 24](#__RefHeading___19)

[УПД.17. Обеспечение доверенной загрузки средств вычислительной техники 24](#__RefHeading___20)

[УПД.16. Функциональные требования по предоставлению доступа к информационной системе только авторизированным пользователям 25](#__RefHeading___21)

[УПД.14. Регламентация и контроль использования в информационной системе технологий беспроводного доступа 27](#__RefHeading___22)

[УПД.12\_УПД.11. Разрешение (запрет) действий пользователей, разрешенных до идентификации и аутентификации 27](#__RefHeading___23)

[УПД.10. Блокирование сеанса доступа в информационную систему после установленного времени бездействия (неактивности) пользователя или по его запросу 28](#__RefHeading___24)

[УПД.9. Ограничение числа параллельных сеансов доступа для каждой учетной записи пользователя информационной системы 28](#__RefHeading___25)

[УПД.4. Разделение полномочий (ролей) пользователей, администраторов и лиц, обеспечивающих функционирование информационной системы 29](#__RefHeading___26)

[УПД.3. Управление информационными потоками является одной из важнейших задач в информационной системе 29](#__RefHeading___27)

[УПД.2\_УПД.5\_ЗСВ.2. Реализация методов управления доступами 32](#__RefHeading___28)

[УПД.1. Управление (заведение, активация, блокирование и уничтожение) учетными записями пользователей, в том числе внешних пользователей 38](#__RefHeading___29)

[УКФ.4. Документирование информации (данных) об изменениях в конфигурации информационной системы и системы защиты персональных данных. 43](#__RefHeading___30)

[УКФ.3. Анализ потенциального воздействия планируемых изменений в конфигурации информационной системы и системы защиты персональных данных на обеспечение защиты персональных данных и согласование изменений в конфигурации информационной системы с должностным лицом (работником), ответственным за обеспечение безопасности персональных данных 43](#__RefHeading___31)

[УКФ.2. Управление изменениями конфигурации информационной системы и системы защиты персональных данных 44](#__RefHeading___32)

[СОВ.1\_СОВ.2. Обнаружение вторжений 46](#__RefHeading___33)

[РСБ.7\_АВЗ.1\_АВЗ.2. Защита информации о событиях безопасности 47](#__RefHeading___34)

[РСБ.6. Генерирование временных меток и (или) синхронизация системного времени в информационной системе 47](#__RefHeading___35)

[РСБ.1\_РСБ.2\_РСБ.3\_РСБ.4\_РСБ.5\_ЗСВ.3. Техническое задание на подсистему учёта событий в информационной системе и процесс структурированного описания этих событий 48](#__RefHeading___36)

[ОЦЛ.6\_ОЦЛ.7\_ОЦЛ.8. В информационной системе должно осуществляться ограничение прав пользователей по вводу информации в информационную систему 49](#__RefHeading___37)

[ОЦЛ.4. Обнаружение и реагирование на поступление в информационную систему незапрашиваемых электронных сообщений (писем, документов) и иной информации, не относящихся к функционированию информационной системы (защита от спама) 50](#__RefHeading___38)

[ОЦЛ.3. Обеспечение возможности восстановления программного обеспечения, включая программное обеспечение средств защиты информации, при возникновении нештатных ситуаций 51](#__RefHeading___39)

[ОЦЛ.2. Контроль целостности персональных данных, содержащихся в базах данных информационной системы 52](#__RefHeading___40)

[ОЦЛ.1\_ЗСВ.8. Контроль целостности программного обеспечения, включая программное обеспечение средств защиты информации 53](#__RefHeading___41)

[ОПС.2. Управление установкой (инсталляцией) компонентов программного обеспечения, в том числе определение компонентов, подлежащих установке, настройка параметров установки компонентов, контроль за установкой компонентов программного обеспечения 54](#__RefHeading___42)

[ОПС.1. Управление запуском (обращениями) компонентов программного обеспечения, в том числе определение запускаемых компонентов, настройка параметров запуска компонентов, контроль за запуском компонентов программного обеспечения 55](#__RefHeading___43)

[ОДТ.4\_ОДТ.5. Периодическое резервное копирование персональных данных на резервные машинные носители персональных данных 56](#__RefHeading___44)

[ОДТ.1\_ОДТ.2\_ОДТ.3. Использование отказоустойчивых технических средств 57](#__RefHeading___45)

[ИНЦ.3 / ИНЦ.4 / ИНЦ.5 / ИНЦ.6. Своевременное информирование лиц, ответственных за выявление инцидентов и реагирование на них, о возникновении инцидентов в информационной системе пользователями и администраторами 58](#__RefHeading___46)

[ИНЦ.2. Обнаружение, идентификация и регистрация инцидентов 59](#__RefHeading___47)

[ИАФ.5 (скрытие пароля) 60](#__RefHeading___48)

[ИАФ.4\_УПД.6\_АНЗ.5 (парольная политика) 60](#__RefHeading___49)

[ИАФ.3. Управление идентификаторами, в том числе создание, присвоение, уничтожение идентификаторов 60](#__RefHeading___50)

[ИАФ.1\_ИАФ.2\_ИАФ.6\_ЗСВ.1. Идентификация и аутентификация пользователей, являющихся работниками оператора 61](#__RefHeading___51)

[ЗТС.4. Размещение устройств вывода (отображения) информации, исключающее ее несанкционированный просмотр 63](#__RefHeading___52)

[ЗТС.3. Контроль и управление физическим доступом к техническим средствам, средствам защиты информации, средствам обеспечения функционирования, а также в помещения и сооружения, в которых они установлены, исключающие несанкционированный физический доступ к средствам обработки информации, средствам защиты информации и средствам обеспечения функционирования информационной системы, в помещения и сооружения, в которых они установлены 63](#__RefHeading___53)

[ЗСВ.10. Разбиение виртуальной инфраструктуры на сегменты (сегментирование виртуальной инфраструктуры) для обработки персональных данных отдельным пользователем и (или) группой пользователей 64](#__RefHeading___54)

[ЗСВ.7. Контроль целостности виртуальной инфраструктуры и ее конфигураций 64](#__RefHeading___55)

[ЗСВ.6.Управление перемещением виртуальных машин (контейнеров) и обрабатываемых на них данных 65](#__RefHeading___56)

[ЗСВ.5. Доверенная загрузка серверов виртуализации, виртуальной машины (контейнера), серверов управления виртуализацией 66](#__RefHeading___57)

[ЗСВ.4. Управление (фильтрация, маршрутизация, контроль соединения, однонаправленная передача) потоками информации между компонентами виртуальной инфраструктуры, а также по периметру виртуальной инфраструктуры 67](#__RefHeading___58)

[ЗНИ.8. Уничтожение (стирание) или обезличивание персональных данных на машинных носителях при их передаче между пользователями, в сторонние организации для ремонта или утилизации, а также контроль уничтожения (стирания) или обезличивания 69](#__RefHeading___59)

[ЗНИ.2. Управление доступом к машинным носителям информации 70](#__RefHeading___60)

[ЗИС.20. Защита беспроводных соединений, применяемых в информационной системе 70](#__RefHeading___61)

[ЗИС.17. Разбиение информационной системы на сегменты (сегментирование информационной системы) и обеспечение защиты периметров сегментов информационной системы 71](#__RefHeading___62)

[ЗИС.16. Выявление, анализ и блокирование в информационной системе скрытых каналов передачи информации в обход реализованных мер или внутри разрешенных сетевых протоколов 71](#__RefHeading___63)

[ЗИС.15. Защита архивных файлов, параметров настройки средств защиты информации и программного обеспечения и иных данных, не подлежащих изменению в процессе обработки персональных данных 73](#__RefHeading___64)

[ЗИС.11. Обеспечение подлинности сетевых соединений (сеансов взаимодействия), в том числе для защиты от подмены сетевых устройств и сервисов 73](#__RefHeading___65)

[ЗИС.10. Подтверждение происхождения источника информации, получаемой в процессе определения сетевых адресов по сетевым именам или определения сетевых имен по сетевым адресам 75](#__RefHeading___66)

[ЗИС.7. Контроль санкционированного и исключение несанкционированного использования технологий мобильного кода, в том числе регистрация событий, связанных с использованием технологий мобильного кода, их анализ и реагирование на нарушения, связанные с использованием технологий мобильного кода 75](#__RefHeading___67)

[ЗИС.6. Передача и контроль целостности атрибутов безопасности (меток безопасности), связанных с персональными данными, при обмене ими с иными информационными системами 76](#__RefHeading___68)

[ЗИС.4. Обеспечение доверенных канала, маршрута между администратором, пользователем и средствами защиты информации (функциями безопасности средств защиты информации) 77](#__RefHeading___69)

[ЗИС.3. Обеспечение защиты персональных данных от раскрытия, модификации и навязывания (ввода ложной информации) при ее передаче (подготовке к передаче) по каналам связи, имеющим выход за пределы контролируемой зоны, в том числе беспроводным каналам связи 77](#__RefHeading___70)

[ЗИС.1. Разделение в информационной системе функций по управлению (администрированию) информационной системой, управлению (администрированию) системой защиты персональных данных, функций по обработке персональных данных и иных функций информационной системы 78](#__RefHeading___71)

[3. Состав и содержание работ по развитию системы 93](#__RefHeading___72)

[4. Перечень работ 95](#__RefHeading___73)

[4.1 Доработка раздела «Список проектов» 95](#__RefHeading___74)

[4.1.1 Возможность вывода всех полей из заявки и паспорта проекта на странице списка проектов 95](#__RefHeading___75)

[4.2 Заявка проекта 96](#__RefHeading___76)

[4.2.1 Единая заявка 96](#__RefHeading___77)

[4.2.2 Создание заявки 98](#__RefHeading___78)

[4.2.3 Копирование заявки 98](#__RefHeading___79)

[4.2.4 Импорт заявок 99](#__RefHeading___80)

[4.3 Дорожная карта проекта 99](#__RefHeading___81)

[4.3.1 Содержание дорожной карты 101](#__RefHeading___82)

[4.3.2 Шаблоны дорожных карт 104](#__RefHeading___83)

[4.3.3 Типы задач 105](#__RefHeading___84)

[4.3.4 Просрочка задач 105](#__RefHeading___85)

[4.3.5 Экспорт дорожной карты и плана поддержки 105](#__RefHeading___86)

[4.4 Паспорт проекта 105](#__RefHeading___87)

[4.5 Оптимизация интеграции с Единым сервисом авторизации (SSO) и Leader-ID 106](#__RefHeading___88)

[4.6 Доработки уведомлений 109](#__RefHeading___89)

[4.7 Создание страницы авторизации 109](#__RefHeading___90)

[4.8 Задание критериев оценки проектов 110](#__RefHeading___91)

[4.9 Рейтинг проектов 110](#__RefHeading___92)

[4.10 Разработка раздела «Отчеты» 111](#__RefHeading___93)

[4.10.1 Отчет по статусам задач 111](#__RefHeading___94)

[4.10.2 Отчет по проектной деятельности 112](#__RefHeading___95)

[4.11 Управление коллегиальными органами 113](#__RefHeading___96)

[4.11.1 Раздел «Коллегиальные органы» 113](#__RefHeading___97)

[4.11.2 Функционал для проведения голосований 114](#__RefHeading___98)

[4.11.3 Печатные формы 114](#__RefHeading___99)

[4.12 Подписание согласия на передачу персональных данных и на поддержку проектов 115](#__RefHeading___100)

[4.13 Реализация требований информационной безопасности 116](#__RefHeading___101)

[4.13.1. Миграция с СУБД MySQL на СУБД PostgreSQL 116](#__RefHeading___102)

[4.13.2. Раздельное хранение и резервное копирование данных 116](#__RefHeading___103)

[4.13.3. Журналирование действий и изменений 116](#__RefHeading___104)

[4.14 Регистрация согласий субъектов об обработке персональных данных 116](#__RefHeading___105)

[4.15 Административная часть 118](#__RefHeading___106)

[4.15.1 Загрузка и настройка шаблонов писем, рассылка уведомлений (группе пользователей или одному) 118](#__RefHeading___107)

[4.15.2 Работа со справочниками 119](#__RefHeading___108)

[4.15.3 Настройка отборов 120](#__RefHeading___109)

[4.15.4 Настройка Шаблонов дорожных карт 121](#__RefHeading___110)

[4.15.5 Управление коллегиальными органами 121](#__RefHeading___111)

[4.15.6 Настройка логики бизнес-процессов системы 121](#__RefHeading___112)

[4.15.7 Функционал управления ролевой моделью 122](#__RefHeading___113)

[4.16 Доработка ролевой модели 122](#__RefHeading___114)

[4.16.1 Управление доступом к данным и полномочия пользователей 122](#__RefHeading___115)

[4.17 API для интеграции 124](#__RefHeading___116)

[4.18 История изменений 127](#__RefHeading___117)

[4.19 Адаптация системы под мобильную версию 128](#__RefHeading___118)

[4.20 Партнеры 129](#__RefHeading___119)

[4.20.1 Создание и редактирование карточки партнера 131](#__RefHeading___120)

[4.21 Личный кабинет пользователя 132](#__RefHeading___121)

[4.21.1 Общая информация 132](#__RefHeading___122)

[4.21.2 Логика работы личного кабинета 133](#__RefHeading___123)

[4.21.3 Содержание личного кабинета для сторонних пользователей ИС 133](#__RefHeading___124)

[4.21.4 Стартовая страница личного кабинета 134](#__RefHeading___125)

[4.21.5 Сохраненные шаблоны 137](#__RefHeading___126)

[4.22 Сертификаты для пользователей 137](#__RefHeading___127)

[4.23 Сквозной поиск 138](#__RefHeading___128)

[5. Порядок контроля и приёмки системы 139](#__RefHeading___129)

[5.1 Порядок оформления и предъявления заказчику результатов работ 139](#__RefHeading___130)

[5.2 Порядок приёмки результатов работ 139](#__RefHeading___131)

[6. Требования к документированию 142](#__RefHeading___132)

[Приложение №1. Требуемые методы защиты информации с указанием уровня ответственности Исполнителя и Заказчик 143](#__RefHeading___133)

[Приложение №2. Пример единой карточки проекта 146](#__RefHeading___134)

[Приложение №3. Вариант полной дорожной карты 151](#__RefHeading___135)

[Приложение №4. Вариант выгрузки части задач дорожной карты с типом задачи «Поддержка проекта» 153](#__RefHeading___136)

[Приложение №5. Вариант выгрузки части задач дорожной карты с типом задачи «Поддержка проекта» на этапе «сопровождение 155](#__RefHeading___137)

[Приложение №6. Пример выгрузки паспорта проекта в формате word 157](#__RefHeading___138)

[Приложение №7. Пример выгрузки паспорта проекта 160](#__RefHeading___139)

[Приложение №8. Пример отображения отчета 168](#__RefHeading___140)

[Приложение №9. Формы для предоставления на Комиссию по аудиту проектов (КАП) 169](#__RefHeading___141)

[Приложение №10. Формы для предоставления на Рабочую группу экспертного совета 171](#__RefHeading___142)

[Приложение №11. Формы отчетов по мониторингу отборов проектов 173](#__RefHeading___143)

[Приложение №12. Матрица ролей 174](#__RefHeading___144)

[Приложение №13. Пример карточки партнера 175](#__RefHeading___145)

[Приложение №14. Пример сертификата 178](#__RefHeading___146)

[Приложение № 15. Программа и методика испытания 179](#__RefHeading___147)

Оглавление

# Используемые сокращения, термины и определения

|  |  |
| --- | --- |
| Термины, сокращение | Название, определение |
| АСИ | Агентство стратегических инициатив по продвижению новых проектов |
| АРМ | Автоматизированное рабочее место |
| АСО | Автоматизированная система оповещения |
| БД | База данных |
| ДК | Дорожная карта |
| ЕГРЮЛ | Единый государственный реестр юридических лиц |
| ИБ | Информационная безопасность |
| ИНН | Идентификационный номер налогоплательщика |
| ИС | Информационная система |
| ИСУП | Информационная система управления проектами |
| ИТ | Информационные технологии |
| КАП | Комиссия по аудиту проектов |
| КО | Коллегиальные органы |
| КПП | Код причины постановки на учет |
| КПЭ | Ключевые показатели эффективности |
| ОГРН | Основной государственный регистрационный номер |
| ОКВЭД | Общероссийский классификатор видов экономической деятельности |
| ОС | Операционная система |
| ПДн | Персональные данные |
| ПМИ | Программа и Методика испытаний |
| ПО | Программное обеспечение |
| ПОИБ | Подсистема обеспечения информационной безопасности |
| ПСИ | Приемо-сдаточные испытания |
| РГЭС | Рабочая группа экспертного совета |
| РФ | Российская Федерация |
| СЗИ | Средства защиты информации |
| СПО | Свободное программное обеспечение |
| СУБД | Система управления базами данных |
| ТЗ | Техническое задание |
| ТОИС | Техническое описание информационной системы |
| ФЗ | Федеральный закон |
| ФИО | Фамилия, Имя, Отчество |
| ФОИВ | Федеральный орган исполнительной власти |
| ФСТЭК | Федеральная служба по техническому и экспортному контролю |
| Технический проект | Комплект проектной и конструкторской документации, специфицирующий детали реализации, отвечающий на вопросы «Как?», «Каким образом?», «С помощью чего?» в отношении Системы. |
| API | Application programming interface |
| CI | Continuous Integration – Непрерывная интеграция |
| CIS | Центр интернет-безопасности |
| DAST | Dynamic Application Security Testing |
| ID | Идентификационный номер |
| ISO | The International Organization for Standardization. Серия международных стандартов, включающая стандарты по информационной безопасности опубликованные совместно Международной Организацией по Стандартизации и Международной Электротехнической Комиссии. |
| LDAP | Lightweight Directory Access Protocol. Открытый протокол, используемый для хранения и получения данных из каталога с иерархической структурой |
| MVP | Minimum Viable Product |
| OWASP | The Open Worldwide Application Security Project. Это открытый проект обеспечения безопасности веб-приложений. |
| PCI DSS | Cтандарт безопасности данных платёжных карт, учреждённый международными платёжными системами Visa, MasterCard, American Express, JCB и Discover |
| SAST | Static Application Security Testing |
| SIEM | Объединение двух терминов, обозначающих область применения ПО: SIM - управление информацией о безопасности, и SEM - управление событиями безопасности. |
| SSO | Single sign-on – Технология единого входа пользователя. |
| UI | User Interface |
| UI-кит | User Interface Kit, или набор для пользовательского интерфейса. Это набор готовых элементов для дизайна интерфейса: шрифтов, иконок, форм и других элементов сайта или приложения. |

**Термины и определения**

| Термин | Определение |
| --- | --- |
| **Адаптивная верстка** | Это такой дизайн веб-страниц, который обеспечивает правильное отображение сайта на различных устройствах, подключённых к интернету, и динамически подстраивается под заданные размеры окна браузера. |
| **Администратор системы (роль)** | Пользователь системы, который имеет доступ к большему набору функций Системы |
| **Агентство** | Автономная некоммерческая организация «Агентство стратегических инициатив по продвижению новых проектов» |
| **Аккредетация** | Процедура официального подтверждения соответствия претендента на аккредитацию установленным критериям, показателям, требованиям. |
| **Акселерация** | Это программа по ускорению развития стартапов от различных фондов, корпораций и институтов развития. |
| **Архитектура продукта** | Принципиальная организация системы, воплощённая в её элементах, их взаимоотношениях друг с другом и со средой. |
| **Бэкенд (back-end)** | Программно-аппаратная часть |
| **Вебхук** | Это программный код, с помощью которого отслеживают изменения на одном сайте и передают данные об этом на другой. |
| **Верхнее меню** | Элемент интерфейса пользователя, позволяющий выбрать одну из нескольких перечисленных опций программы, расположенный в верхней части сайта в горизонтальном формате |
| **Вид проекта** | Категория лидерских проектов, которые отличаются по сферам реализации (технологии, качество жизни, экология, образование и кадры) |
| **Визуальный редактор** | Это компьютерное программное обеспечение для редактирования текстовых файлов с использованием текстового или графического пользовательского интерфейса, которое обычно отображает содержимое (текст) в соответствии со встроенным кодом разметки, например, HTML, Wikitext, а не отображает необработанный текст. |
| **Гиперссылка** | Это текст, фотография, иконка или другой элемент, по нажатию на который откроется другая веб-страница или другая часть веб-сайта. |
| **Десктоп** | Персональный компьютер |
| **Заказчик** | Юридическое лицо, заинтересованное в выполнении исполнителем работ |
| **Информационная безопасность** | Практика предотвращения несанкционированного доступа, использования, раскрытия, искажения, изменения, исследования, записи или уничтожения информации. Основная задача информационной безопасности — сбалансированная защита конфиденциальности, целостности и доступности данных. |
| **Исполнитель** | Юридическое лицо, выполняющее работу по заказу Заказчика согласно договору |
| **ИС/ Информационная система/ ИСУП / Система** | Информационная cистема управления проектами, доступная в сети интернет по адресу [https://isup.asi.ru](https://isup.asi.ru/), которая позволяет подавать проекты на отбор посредством оформления заявок, обрабатывать поданные заявки, сопровождать проекты, проводить оценку проектов и их экспертизу, генерировать аналитику и делать выгрузку данных по шаблонам/формам |
| **Контент** | Информационное содержание (тексты, графическая информация и прочее) |
| **Лидер проекта (роль)** | Пользователь системы, участник отбора (не сотрудник АСИ) |
| **Мобильная версия** | Версия сайта, предназначенная для мобильных устройств |
| **Оператор КО (роль)** | Пользователь системы, который отвечает за управление функционалом коллегиальных органов |
| **Операционная система** | Комплекс взаимосвязанных программ, предназначенных для управления ресурсами компьютера и организации взаимодействия с пользователем. |
| **Опытная эксплуатация** | Эксплуатация новой системы в ограниченном интервале времени, проводимая с целью выявления и устранения недостатков системы и определения её соответствия требованиям технической документации. |
| **Паспорт проекта** | Это модуль в ИСУП, который позволяет сотрудникам агентства автоматизировать работу с проектом: просматривать и редактировать данные по проекту, формировать выгрузки данных для представления на Рабочие группы и Бюро экспертного совета |
| **Пользовательский интерфейс** | Интерфейс, обеспечивающий передачу информации между пользователем-человеком и программно-аппаратными компонентами компьютерной системы |
| **Продуктивная среда** | Среда, в которой развернуто программное обеспечение, где продукт доступен пользователям. |
| **Проект** | Инициатива, поданная лидером проекта или инициатором |
| **Проектирование** | Процесс определения архитектуры, компонентов, интерфейсов и других характеристик системы или её части |
| **Радиобаттон** | Это элемент в визуальном оформлении веб-сайта, который можно отметить, чтобы выбрать один из предложенных вариантов. |
| **Регрессионное тестирование** | Это повторное выполнение функциональных и нефункциональных тестов для обеспечения того, чтобы ранее разработанное и протестированное программное обеспечение все еще работало после изменения. |
| **График выпуска релизов** | График подготовки выпусков (релизов) программного обеспечения, связанный с передачей разработанного функционала на следующий этап жизненного цикла модуля, подсистемы или системы в целом. |
| **Тема отбора** | Это тема, по которой лидеры подают свои заявки на поддержку проекта |
| **Техническая документация** | Набор документов, используемых при проектировании, создании и эксплуатации технических объектов. |
| **Техническое задание** | Документ, содержащий требования заказчика, в соответствии с которым осуществляются поставка товара, выполнение работ, оказание услуг и их приёмка. |
| **Тип проекта** | Категория проектов, которые реализуются Агентством (практики, лидерские проекты, сильные идеи, молодежные проекты и др.) |
| **Требование** | Утверждение, которое передаёт или выражает некоторую потребность и связанные с ней ограничения и условия. |
| **Трекер (роль)** | Сотрудник АСИ, сопровождающий проект в ИСУП |
| **Старший трекер (роль)** | Сотрудник АСИ, сопровождающий проект в ИСУП |
| **Фронтенд (front-end)** | Клиентская сторона пользовательского интерфейса к программно-аппаратной части сервиса |
| **Функциональное тестирование** | Это процесс обеспечения качества в рамках цикла разработки программного обеспечения, необходимый для проверки реализуемости функциональных требований, согласно спецификации тестируемого программного обеспечения |
| **Dev-среда (среда разработки)** | Это среда, в которой разрабатываются изменения программного обеспечения |
| **Keycloak** | Это решение для управления идентификацией и доступом с открытым исходным кодом, предназначенное для использования в ИС где могут использоваться паттерны микросервисной архитектуры |
| **Predprod-среда (превью среда)** | Это среда идентичная или максимально приближенная к продуктивной, которая используется, чтобы сделать финальную проверку ПО в условиях максимально приближенным к «боевым». |
| **Unit-тест** | Это программа, которая проверяет работу небольшой части кода. |

# Общие сведения

## Наименование Системы

Полное наименование: многофункциональная информационная система управления проектами, включающая программные модули, в функционал которых заложены типовые фазы преобразования информации: регистрация, хранение, обработка, передача и отображение данных (далее – ИСУП)

## Наименование предприятий разработчика и заказчика

Автономная некоммерческая организация «Агентство стратегических инициатив по продвижению новых проектов».

## Назначение и цели создания Системы

Цель – создать инструмент автоматизации проектного менеджмента для реализации стратегии Агентства.

Цели создания системы:

* управление проектами на всём протяжении их жизненного цикла;
* централизованное хранение сведений обо всех проектах Агентства;
* формирование единой программной платформы для работы с проектами Агентства для разных категорий пользователей;
* анализ данных проектов;
* обмен данными проектов с другими внутренними и внешними сервисами и системами.

Исполнитель, выполняя работы по данному Техническому заданию, должен учитывать, что ИСУП предполагает дальнейшее развитие. Выполненные Исполнителем работы по данному Техническом заданию должны внедрять или применять архитектурные решения длительного срока использования в условиях развития моделей метаданных, обусловленных предметными областями. Кроме того, необходимо обеспечивать и контролировать качество и чистоту программного кода с помощью методов статического и динамического анализа.

## Требования к выполняемым работам

* Сверстанные страницы должны содержать все интерактивные элементы страниц (выпадающие списки, всплывающие окна, скрытие элементов при изменении размера экрана и т.п.).
* Графические элементы навигации должны быть снабжены альтернативной̆ подписью (поле ALT, TITLE).
* Страницы должны иметь мета-описание и атрибуты языка.

## Общие требования к развитию системы

При развитии системы архитектура должна измениться в соответствии с требованиями настоящего ТЗ, общими рекомендациями параграфа 1.3 «Назначение и цели создания Системы», а также требованиями надёжности и безопасности (в соответствии с требованиями Приказов ФСТЭК №№ 17 и 21 для второго класса защищенности, которые детально указаны в п.2.10).

Принципы работы пользователей с порталом, в том числе интерфейсные решения, должны улучшать пользовательский опыт как в существующих, так и в новых разделах и сервисах. Для существующего функционала Системы требуется согласование с Заказчиком отдельных изменений, если это необходимо для реализации требований данного технического задания.

В рамках разработки первого комплекта документов технического проекта по договору Исполнитель должен спроектировать и определить общие архитектурные и технические требования. Впоследствии перед началом разработки любого функционала, указанного в разделе 4 настоящего технического задания, Исполнитель должен поэтапно разрабатывать и предоставлять Заказчику на согласование технический проект или проектную документацию (в составе: прецедентная модель, архитектурная тетрадь, спецификация общесистемных требований и программа и методика испытаний[[1]](#footnote-1)), надлежащим образом заполненный. Данные требования должны быть использованы при разработке всего функционала в рамках настоящего технического задания.

Если разрабатываемый функционал требует создания новых интерфейсных форм, то до старта работ по доработке системы Исполнитель обязан разработать и предоставить Заказчику на согласование дизайн-макет интерфейса. При разработке дизайн-макетов Исполнитель должен использовать существующий UI-кит системы, при необходимости дополняя его необходимыми элементами.

Для новых элементов пользовательского интерфейса (разделы, страницы, окна) должна поддерживаться адаптивная верстка. Подробнее об адаптивной верстке в п.4.19.

Разработанные технические проекты подсистем ИСУП и его дизайн-макеты Исполнитель должен согласовать с Заказчиком и предоставлять ему в качестве одного из результатов выполнения настоящего ТЗ. Для каждой существующей подсистемы ИСУП, подлежащей изменению в рамках настоящего ТЗ, Исполнитель обязан внести изменения в существующую конструкторскую документацию.

Все задачи, указанные в разделе 4 настоящего технического задания, должны выполняться в следующем порядке:

1. Проектирование и разработка дизайн-макетов разрабатываемых интерфейсов, если это необходимо в рамках задачи
2. Согласование разработанных дизайн-макетов с Заказчиком.
3. Разработка и согласование технических проектов.
4. Реализация функционала на основании согласованных технических проектов.
5. Публикация разработанного функционала на опытной площадке «predprod» — rc.isup.asi.ru. При этом, он должен быть предварительно протестирован с помощью автоматических тестов (без отчёта о результатах тестирования публикация запрещена).
6. Квалификационное тестирование функционала проектной командой на основании ПМИ[[2]](#footnote-2) в соответствии с требованиями Раздела 5 настоящего Технического задания.
7. Исправление выявленных в ходе тестирования недостатков, выполнение статического и динамического анализа исходного кода Системы с составлением Исполнителем отчёта о выявленных недостатках и внесённых изменений.
8. Демонстрация Системы Заказчику и передача её в опытную эксплуатацию на площадке «predprod» с составлением соответствующего отчёта. В отношении выявленных дефектов: внести уточнения в ПМИ и устранить силами проектной команды.
9. Публикация разработанного функционала в продуктивной среде ответственными представителями Заказчика. При наличии выявленных недостатков в результатах работ Исполнителя публикация допускается только с письменного согласия уполномоченного(ых) представителей функциональных заказчиков, руководителей Службы информационных технологий и Службы информационной безопасности. В остальных случаях публикация запрещается.
10. Квалификационное тестирование разработанного функционала на продуктивной среде Заказчиком на основании ПМИ. Обнаруженные недостатки должны быть зафиксированы уполномоченными представителями Заказчика и переданы Исполнителю для устранения. Уполномоченные представители функционального(ых) заказчиков совместно с уполномоченными представителями Служб информационных технологий и информационной безопасности принимают решение о вводе в эксплуатацию или возврате Системы к исходному своему состоянию.

График выпуска релизов должен быть согласован Заказчиком на основании плана-графика проекта. В случае наличия сторонней команды, отвечающей за сборку релизов на продуктивную среду, Исполнитель должен передать доработки Системы и обеспечить устранение замечаний для сборки релиза в соответствии с описанным выше порядком.

### 1.5.1 Требования к проведению тестирования

Тестирование производится на основании Программы и Методики испытаний, разрабатываемой Исполнителем и утверждаемой Заказчиком. Подробно порядок контроля и приемки системы описан в разделе 5.

В ходе подготовки к приемке выполненных работ (оказанных услуг) должны быть выполнены:

* автоматическое модульное тестирование, интеграционное тестирование;
* функциональное и регрессионное тестирование;
* тестирование безопасности: а именно статический и динамический анализ исходного кода разработанных и интегрируемых подсистем, а также фаззинг тестирование[[3]](#footnote-3).

#### 1.5.1.1 Функциональное тестирование

Функциональное тестирование в рамках разработки нового функционала должно включать следующие этапы:

* Подготовка программы и методики испытаний в соответствии с требованиями, указанными в пункте 5.2 настоящего технического задания.
* Подготовка тестовых сценариев для проверки разрабатываемого функционала.
* Выполнение сценариев ручного тестирования.
* Подготовка отчета по результатам функционального тестирования.
* Составление графика внесения исправлений в исходный код Системы и его встраивание в график выпуска релизов.
* Актуализации тестовых сценариев после проведения итерации функционального тестирования.

#### 1.5.1.2 Регрессионное тестирование

После каждого релиза на pred-prod среду и продуктивную среду необходимо проводить регрессионное тестирование с целью выявления ухудшения существующего функционала система.

Исполнитель должен обеспечить как регулярное регрессионное тестирование (после каждого релиза), так и итоговое регрессионное тестирование (после выполнения всего объема функционала настоящего технического задания).

Регрессионное тестирование должно включать следующие этапы:

* Подготовка методики регрессионного тестирования
* Подготовка необходимых материалов для проведения регрессионного тестирования (тестовых сценариев, автоматизированных unit-тестов, чек-листов и т.д.)
* Выполнение тестирования на основании материалов, подготовленных на предыдущем шаге
* Подготовка отчета по результатам регрессионного тестирования
* Составление графика внесения исправлений в исходный код Системы и его встраивание в график выпуска релизов.
* Актуализации материалов после проведения итерации регрессионного тестирования.

#### 1.5.1.3 Тестирование безопасности

ИС должна обеспечивать выполнение следующих требований по защите информации:

* проверку защиты от несанкционированного доступа к информации:
  + проверку обеспечения защиты информации от неправомерного доступа, уничтожения, модифицирования, блокирования, копирования, предоставления, распространения, а также от иных неправомерных действий в отношении такой информации;
  + проверку предотвращения несанкционированного доступа к информации;
  + проверку своевременного обнаружения фактов несанкционированного доступа к информации.

Для реализации данных проверок выполняются:

* тестирование исходного кода на уязвимости: определение уязвимостей в исходных кодах ИС;
* тестирование приложения на уязвимости: определение уязвимостей в приложениях ИС;
* статический анализ кода: поиск кода, потенциально содержащего уязвимости;
* динамический анализ кода: поиск уязвимостей в исходном коде (в том числе ошибок неправильной работы с памятью, выход за границы выделенной памяти, использование освобождённой памяти, двойные или некорректные освобождения памяти);
* фаззинг тестирование.

Указанные выше проверки должны быть реализованы при помощи автоматизированных средств:

* автоматические тесты:
  + Selenium: для пользовательского интерфейса;
  + Выполнить покрытие всех архитектурных решений с помощью типовых средств, характерных для используемых программных каркасов: для модульного и интеграционного тестирования в прикладном и серверном слоях системы.
* статический анализ: с помощью SonarLint для выбранного технологического стека (общие требования представлены ниже);
* динамический анализ: с помощью Valgrind или его аналогов для выбранного технологического стека. Аналог должен быть согласован с Заказчиком;
* фаззинг тест: с помощью AFL++[[4]](#footnote-4) или его аналогами для выбранного технологического стека. Аналог должен быть согласован с Заказчиком

Общий порядок выполнения услуг по тестированию безопасности:

* подготовка кода к тестированию;
* подготовка плана тестирования;
* настройка автоматизированных средств тестирования;
* проведение тестирования (в том числе статического и динамического согласно ГОСТ Р 56939-2016) при помощи автоматизированного средства;
* анализ отчета, сформированного средством тестирования;
* внесение корректировок в код для устранения замечаний;
* подготовка итогового отчета по выявленным уязвимостям.

Общие требования проведения статического анализа кода:

1. Статический анализ обязателен к проведению для каждого запроса на слияния в ветки master, [номерных|кандидатов] релизов и production (master - основной ствол разработки, production - ветка публикации в продуктивную среду в терминологии техпроцесса GitLab Flow), совместно именуемые «рабочие ветки». Наличие ошибок, выявленных в результате анализа, является основанием для отклонения запроса на слияние с целью устранения выявленных дефектов.
2. Разработчик Исполнителя самостоятельно осуществляет статический анализ кода перед предложением слияний и выполняет данные в его рамках рекомендации, если это требуется.
3. Ответственный представитель Заказчика осуществляет архитектурный надзор и контроль качества кода на основании статического анализа запросов на слияния в ветки [номерных|кандидатов] релизов и production. При необходимости он уполномочен выполнять указанные процедуры для исходных кодов всех рабочих веток. При обнаружении дефектов, он имеет право:
   * мотивированно отказать в принятии запроса на слияние, в рамках которого были обнаружены дефекты;
   * зарегистрировать заявку на устранение выявленных дефектов с последующим уведомлением ответственных сотрудников Заказчика.
4. Классификация дефектов, определяемых в рамках статического анализа, принадлежащих категориям «блокирующие» (blocker), «критические» (critical) и «важные» (major) (в терминологии базы знаний SonarSource [https://rules.sonarsource.com/]), подлежащих обязательному устранению:
   * ошибки (bugs);
   * уязвимости (vulnerabilities);
   * потенциальные уязвимости (security hotspot);
   * признаки рефакторинга (code smells); допускается дублирование кода на уровне не более 5% в контексте кодовой базы всего проекта.
5. В случаях выявления дефектов, исправление которых связано с исправлением программного кода, созданного вне рамок действующих договоров и не являющегося их предметом, Стороны взаимосогласованно регистрируют заявку на устранение выявленных дефектов.
6. Для осуществления статического анализа Стороны согласились использовать следующие программные средства:
   * SonarQuebe 10: SonarQube Community Edition для выполнения автоматического статического анализа над исходным кодом, публикуемого в репозитории <указать ссылку>;
   * SonarLint 8.4.0: установленного в качестве плагина к распространённым интегрированным разработческим средам (IDE).

Возможна дополнительная детализация и изменения общих требований в частных случаях проведения статического анализа с письменного согласия Исполнителя и Заказчика.

# Требования к системе

## Требования к технологическому стеку

Таблица 1

|  |  |  |
| --- | --- | --- |
| **№** | **Компонент системы** | **Технологический стек** |
| 1 | Frontend | ReactJS  MobX  TypeScript  NextJS  Sass  Методология BEM |
| 2 | Backend | TypeScript  NodeJS  NestJS  RabbitMQ |
| 3 | Инфраструктура | Gitlab CI/CD  Kubernetes  Helm  Docker  Nginx  Prometheus/Grafana  RabbitMQ |
| 4 | Базы данных | PostgreSQL  MySQL  Redis |

## Требования к журналированию действий пользователей

В системе должен быть предусмотрен механизм, позволяющий регистрировать следующие действия пользователей:

* авторизация в системе;
* события логики работы системы, приводящие к вводу(изменению) или выводу[[5]](#footnote-5) данных;
* события внешних API системы;
* события регистрации юридически значимых действий в отношении оферт, в том числе данных пользователями согласий в соответствии с требованиями 4.18 «Регистрация согласий субъектов об обработке персональных данных».

При авторизации пользователя в журнале должны регистрировать следующие сведения:

* Идентификатор пользователя;
* отметка времени действия (дата/время вызова метода);
* идентификатор сессии;
* авторизация пользователя: список ролей, групп, мандатов, которые действие разрешили или запретили;
* провайдер доступа (LDAP или Leader-ID).

При изменении данных пользователем в журнале должны фиксироваться следующие сведения:

* Идентификатор пользователя;
* отметка времени действия (дата/время вызова метода);
* идентификатор сессий;
* авторизация пользователя: список ролей, групп, мандатов, которые действие разрешили или запретили;
* название вызванного метода (для режима отладки);
* входные и выходные параметры вызванного метода (для режима отладки);

В процессе работы системы информация об указанных действиях должна передаваться в сервис журналирования, а при отсутствии возможности передачи в сервис журналирования сохраняться в файловом журнале и передаваться в журнал системы. Доступ приложения к сервису журналирования должен осуществляться от имени технической учетной записи. Сервис журналирования предоставляется Заказчиком.

Перечень работ по реализации требований к журналированию указан в п. 4.17 настоящего ТЗ.

## Требования к информационной безопасности

В создаваемой системе должны быть реализованы меры по обеспечению безопасности обрабатываемых данных (в т. ч. персональных данных), соответствующие требованиям Федерального законодательства, нормативных актов и документов регуляторов, а также, стандартов и методик Заказчика.

Защита информации обеспечивается встроенными механизмами, наложенными средствами защиты информации и также организационными мерами.

Защита информации должна быть организована в соответствии требованием обеспечения 2-го уровня защищённости персональных данных на основании:

* Федеральный закон РФ № 152-ФЗ «О персональных данных»;
* Постановление Правительства РФ от 01.11.2012 N 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных» (Пункт 10, подпункты г) и д));
* Приказ ФСТЭК РФ № 21 «Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных».

Дополнительно, средства обеспечения защиты Системы должны разрабатываться в соответствии с (верховенство конфликтных требований за Федеральным законодательством, Постановлениями Правительства РФ и Приказами ФСТЭК):

* Нормативная документация по информационной безопасности Заказчика;
* Международные методические рекомендации и стандарты разработки в области защиты информации ISO 2700x, OWASP, CIS при необходимости PCI DSS.

Для обеспечения безопасности и защиты информации в системе должна быть реализована подсистема обеспечения информационной безопасности (далее ПОИБ), включающая в себя следующие подсистемы:

* подсистема контроля и управления доступом;
* подсистема регистрации и учёта событий;
* подсистему обеспечения защиты от вредоносного кода/ПО (в контексте исходного кода решения и связанных с ним зависимостей);
* подсистема контроля защищенности;
* подсистема обновления активов ПО;
* подсистему резервного копирования и восстановления.

В Приложении 1 указана таблица с разделами требуемых методов защиты с указанием уровня ответственности Исполнителя и Заказчика.

Детальные требования указаны в п.4.13.

## Защита информации в случаях сбоя

В системе должно быть предусмотрено резервное копирование конфигурации Системы, программного кода и исполняемых двоичных файлов (или их эквивалентов), а также данных, находящихся на хранении в системе.

Система должна предусматривать следующие режимы восстановления данных:

– при загрузке отдельными реестрами данных (без больших объектов) в течение 4-6 часов;

– реестры данных и массивы двоичных данных, хранящиеся в отдельном S3-хранилища, восстанавливаются до 8 часов.

Исполнитель работ должен разработать планы резервного копирования, использующие режим работы СУБД PostgreSQL «непрерывное архивирование и восстановление на момент времени (Point-in-Time Recovery)», предусматривающий накопление журналов перезаписи, установки меток восстановления и указания конкретного момента времени для восстановления. Автоматические сценарии должны предусматривать контроль доступности дискового пространства и передавать записи своего журнала в системный журнал.

Резервное копирование и восстановление данных должно осуществляться раздельно для персональных данных (которые должны находиться в отдельных табличных пространствах, сгруппированных по целям обработки) и прочих типов данных. Для резервного копирования и восстановления данных должны использоваться штатные средства, используемых систем хранения данных. Подробные требования указаны в Приложении 1.

Система должна сохранять работоспособность и частичную функциональность при отключении базы данных с персональными данными.

## Требования к хранению и обработке персональных данных

В системе будут храниться и обрабатываться общедоступные персональные данные (ФИО, номер телефона, адрес электронной почты, идентификатор Leader-ID) и иные персональные данные (должность, место работы, сведения о проектах, сведения об образовании, профиль компетенций и другие). Должна существовать возможность указать системе вид персональных данных при добавлении новых свойств объектов данных и/или табличных полей.

Хранение и обработка персональных данных должны осуществляться в соответствии с законодательством Российской Федерации:

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

Приказ ФСТЭК России от 18.02.2013 г. № 21

Постановление Правительства Российской Федерации от 01.11.2012 г. № 1119

Хранение персональных данных должно осуществляться в отдельном удалённом табличном пространстве, Система должна поддерживать ограничение доступа к нему при необходимости.

Система должна обеспечивать информирование субъектов персональных данных о политике их обработки в каждом разделе (на каждой странице), где осуществляется такая обработка.

## Требования к эргономике и технической эстетике

Дизайн интерфейса пользователя должен соответствовать современным требованиям и рекомендациям.

При разработке графического интерфейса должны быть соблюдены следующие общие принципы:

единство базовых текстовых, цветовых и графических обозначений;

однотипный интерфейс навигации по экранным формам системы;

простота и наглядность, не требующая от пользователя специальных знаний, выходящих за рамки стандартных способов навигации.

## Требования к патентной чистоте

Используемые при проектировании, разработке, развертывании и тестировании инструменты разработки ПО должны быть лицензированными на территории Российской Федерации для работы в используемых режимах.

Исполнитель должен гарантировать отсутствие нарушения исключительных прав других лиц при передаче Заказчику полученных в ходе выполнения результатов выполненных работ. При необходимости использования исключительных прав третьих лиц на результаты интеллектуальной деятельности в ходе выполнения работ, Исполнитель должен направить Заказчику об этом уведомление, в том числе – условия приобретения прав на использование объектов интеллектуальной собственности.

Созданные и использованные при исполнении договора объекты интеллектуальной собственности подлежат отражению в отчетных документах Исполнителя о результатах выполнения работ по договору и передаются Заказчику на условиях, предусмотренных в договоре. Программные средства должны быть обеспечены гарантийным обслуживанием организации-разработчика. Соответствующие обязательства должны быть переданы Заказчику.

Программные средства должны быть обеспечены гарантийным обслуживанием организации-разработчика таких программных средства. Соответствующие обязательства должны быть переданы Заказчику не позднее сдачи результатов выполненных работ.

## Масштабирование системы

Вычислительные узлы, на которых расположены сервисы системы, должны поддерживать кластеризацию. Добавление новых узлов может осуществляться как автоматически, так и вручную. Система должна поддерживать режимы самодиагностики нагрузки основных сервисов. Транзакции должны изолироваться в рамках узлов, в которых они возникли.

Система должна поддерживать журналирование технического состояния и выводить на информационную панель администратора сводную информацию по учитываемым метрикам: в разворотах на момент времени и в динамике, в разрезах узлов и сервисов.

Первоначальная нагрузочная способность системы не должна быть ниже двух тысяч одновременных пользовательских сессий (с перспективой роста до 20 000), а время отклика не должно превышать двух секунд.

Среднее время отклика сервера – до 700 мс

Скорость поиска – 150 мс.

Исполнитель должен разработать план масштабирования системы в случае увеличения нагрузки и подключения дополнительных компонентов сторонних систем.

## Требования по стандартизации и унификации

Дополнительные требования не предъявляются, за исключением требований к соблюдению стандартов и нормативных актов, явно указанных в тексте тех или иных разделов данного ТЗ.

## Требования Приказа ФСТЭК №21

УПД.17. Обеспечение доверенной загрузки средств вычислительной техники

Требования:

Блокирование попыток несанкционированной загрузки нештатной операционной системы (среды) или недоступность информационных ресурсов для чтения или модификации в случае загрузки нештатной операционной системы:

Все компьютерные системы должны иметь функцию “доверенной загрузки”, которая обеспечивает запуск только авторизованных операционных систем на системе:

1.1 «Доверенная загрузка» блокирует любые попытки загрузки и запуска нестандартных операционных систем или сред;

1.2 Если обнаружена нестандартная операционная система, “доверенная загрузка” предотвращает несанкционированный доступ к информационным ресурсам, включая файлы и данные, на системе;

1.3 “Доверенная загрузка” также должна предотвращать любые изменения системы или данных неавторизованными пользователями;

1.4 Все компьютерные системы должны регулярно обновляться, чтобы гарантировать, что функция “доверенной загрузки” актуальна и эффективна.

Контроль доступа пользователей к процессу загрузки операционной системы:

2.1 Регулирования Доверенной Загрузки должны обеспечивать полный контроль доступа пользователя к процессу загрузки операционной системы. Это включает в себя установление политик доступа, аутентификацию пользователей и авторизацию доступа к компьютерной системе.

Контроль целостности программного обеспечения и аппаратных компонентов средств вычислительной техники:

3.1 Мониторинг процесса загрузки, чтобы гарантировать, что на систему загружается только авторизованное программное обеспечение и микропрограммы;

3.2 Проверка целостности операционной системы и других компонентов программного обеспечения перед их выполнением;

3.3 Проверка системной микропрограммы и аппаратного обеспечения на наличие несанкционированных модификаций или вмешательства;

3.4 Регистрация всей активности загрузки для обнаружения и расследования любой подозрительной или несанкционированной активности;

В информационной системе должна осуществляться доверенная загрузка уровня базовой системы ввода-вывода или уровня платы расширения:

4.1 Все информационные системы должны иметь возможность доверенной загрузки на уровне базового ввода-вывода системы или на уровне платы расширения.

### 

### УПД.16. Функциональные требования по предоставлению доступа к информационной системе только авторизированным пользователям

Доступ к информационной системе должен быть предоставлен только авторизованным пользователям. Для этого должны быть выполнены следующие функциональные требования:

1. **Аутентификация пользователей:** Система должна запрашивать у пользователя логин и пароль для аутентификации при попытке входа в систему. Данные о пользователях и паролях должны храниться в защищенной базе данных.
2. **Установка прав доступа:** После успешной аутентификации пользователю должны быть предоставлены только те права доступа, которые ему необходимы для выполнения своих задач. Администратор системы должен иметь возможность устанавливать права доступа для каждого пользователя, а также изменять их в любой момент времени.
3. **Защита от неавторизованного доступа:** Система должна обеспечивать защиту от неавторизованного доступа, блокируя попытки входа в систему с неправильными учетными данными и ограничивая количество неудачных попыток входа.
4. **Регистрация действий пользователей:** Система должна вести журнал действий пользователей, чтобы можно было отслеживать и контролировать их действия. Журнал должен содержать информацию о датах и времени входа в систему, действиях пользователя и изменениях, внесенных в систему.
5. **Разграничение доступа:** Система должна обеспечивать разграничение доступа к информации, хранящейся в системе, в зависимости от роли пользователя. Таким образом, каждый пользователь должен иметь доступ только к той информации, которая ему необходима для выполнения своих задач.

Система должна обеспечивать предоставление доступа только к тем типам прикладного программного обеспечения, к которым у пользователя есть права доступа. Для этого необходимо реализовать следующие требования:

1. **Установка прав доступа:** Администратор системы должен иметь возможность устанавливать права доступа к каждому типу прикладного программного обеспечения для каждого пользователя. Пользователь должен иметь доступ только к тем типам, которые ему необходимы для выполнения своих задач.
2. **Защита от неавторизованного доступа:** Система должна обеспечивать защиту от неавторизованного доступа к тем типам прикладного программного обеспечения, к которым у пользователя нет прав доступа.
3. **Регистрация действий пользователей:** Система должна вести журнал действий пользователей для каждого типа прикладного программного обеспечения, чтобы можно было отслеживать и контролировать их действия. Журнал должен содержать информацию о датах и времени входа в систему, действиях пользователя и изменениях, внесенных в систему для каждого типа прикладного программного обеспечения.
4. **Разграничение доступа:** Система должна обеспечивать разграничение доступа к каждому типу прикладного программного обеспечения в зависимости от роли пользователя. Таким образом, каждый пользователь должен иметь доступ только к тому типу прикладного программного обеспечения, который ему необходим для выполнения своих задач.

### УПД.14. ****Регламентация и контроль использования в информационной системе технологий беспроводного доступа****

**Требования:**

1. Ограничения использования устройств: Следует установить ограничения на типы устройств, которые могут получить доступ к информационной системе, а также на типы действий, которые могут выполняться на этих устройствах;
2. Контроль доступа к сети (NAC): Решения NAC могут использоваться для идентификации устройств и принудительного выполнения политик, основанных на их уровне доверия. Решения NAC могут использоваться для обеспечения того, что только авторизованные устройства имеют доступ к корпоративной Wi-Fi-сети.
3. Сертификаты устройств: Сертификаты устройств могут использоваться для аутентификации устройств до того, как им разрешен доступ к корпоративной Wi-Fi-сети. Сертификаты могут быть выданы устройствам, которым доверяют и которым разрешен доступ к сети.
4. Фильтрация MAC-адресов: Фильтрация MAC-адресов может использоваться для разрешения или запрета доступа к корпоративной Wi-Fi-сети на основе MAC-адреса устройства. Только устройства с авторизованными MAC-адресами будут иметь доступ к сети.
5. Гостевая сеть: Корпоративные Wi-Fi-сети должны иметь отдельную гостевую сеть, которая изолирована от основной сети. Гостям должно быть требовано аутентифицироваться перед предоставлением доступа к гостевой сети.

### УПД.12\_УПД.11. ****Разрешение (запрет) действий пользователей, разрешенных до идентификации и аутентификации****

Функциональные требования на запрет действий пользователей до идентификации и аутентификации могут быть более подробно описаны следующим образом:

1. Система должна запрещать любые действия незарегистрированных и неподтвержденных пользователей, включая работу с API и загрузку файлов. Пользователь должен быть аутентифицирован в системе, чтобы использовать любые функции, которые могут повлиять на работу приложения или на других пользователей.
2. Должна быть реализована защита от попыток обхода ограничений путем изменения URL или других параметров запроса. Система должна проверять запросы на наличие необходимых параметров и проверять их на соответствие правилам доступа. Если запрос не удовлетворяет этим условиям, пользователю должно выводиться соответствующее сообщение об ошибке.
3. Система должна иметь возможность установки различных уровней доступа для зарегистрированных пользователей, чтобы управлять доступом к функциональности приложения. Например, некоторые пользователи могут иметь доступ только к определенным разделам сайта или функциям, в то время как другие пользователи могут иметь полный доступ к приложению.
4. Система должна иметь возможность проводить аудит действий пользователей, которые не прошли аутентификацию, чтобы обнаруживать и предотвращать любые попытки нарушения безопасности.

### УПД.10. Блокирование сеанса доступа в информационную систему после установленного времени бездействия (неактивности) пользователя или по его запросу

**Требования:**

1.1 Система должна автоматически завершать неактивные сессии, если пользователь не проявляет активность в течение 15 минут;

1.2 Пользователь может получать предупреждение о скором завершении сеанса доступа в систему, за 1 минуту до завершения неактивной сессии;

1.3 После завершения неактивной сессии, пользователь должен перенаправляться на страницу авторизации для повторного входа в систему;

1.4 Настройки системы могут предоставлять возможность администраторам системы просматривать историю неактивных сессий пользователей, включая время и причину завершения сессии;

1.5 При возобновлении сеанса после завершения неактивной сессии, система должна перенаправлять пользователя на страницу, которую он просматривал перед завершением сессии, если эта страница доступна для пользователя.

### УПД.9. ****Ограничение числа параллельных сеансов доступа для каждой учетной записи пользователя информационной системы****

**Описание задачи:**

Система должна ограничивать количество параллельных (одновременных) сессий для каждого пользователя не более двух активных сессий на разных устройствах одновременно.

**Функциональные требования:**

1.1 Система должна контролировать количество активных сессий для каждого пользователя;

1.2 Если пользователь пытается начать новую сессию, когда уже имеется две активные сессии, то система должна выдавать сообщение об ошибке и отправлять оповещение администратору;

1.3 Пользователь может завершить любую из своих активных сессий в любое время;

1.4 Если пользователь завершает одну из своих активных сессий, то система должна позволять ему начать новую сессию;

1.5 Система должна обеспечивать безопасность и надежность при ограничении количества параллельных сессий;

1.6 Система должна предоставлять возможность настройки количества параллельных сессий для каждого пользователя в зависимости от его роли или группы;

1.7 Система должна предоставлять администратору системы доступ к количеству активных сессий для каждой учётной записи.

### УПД.4. ****Разделение полномочий (ролей) пользователей, администраторов и лиц, обеспечивающих функционирование информационной системы****

**Требования:**

1. Правила разделения полномочий должны обеспечивать управление доступом субъектов при входе в информационную систему;
2. Правила разделения полномочий должны определять, какой уровень доступа должен быть предоставлен каждому субъекту при входе в систему;
3. Правила разделения полномочий определяют, какие действия могут быть выполнены каждым субъектом при входе в систему;
4. Правила разделения полномочий определяют, какие ресурсы могут быть доступны каждому субъекту при входе в систему;
5. Правила разделения полномочий обеспечивают защиту конфиденциальной информации от несанкционированного доступа каждого субъекта при входе в систему;
6. Правила разграничения доступа должны соответствовать законодательству и стандартам безопасности информации;

### УПД.3. Управление информационными потоками является одной из важнейших задач в информационной системе

Важным шагом в управлении информационными потоками является анализ существующей информационной системы. Необходимо определить потоки информации, которые проходят через систему, а также выявить возможные узкие места в процессе передачи информации.

**Требования:**

Обеспечивать возможность передачи информации только по установленному маршруту. Для обеспечения передачи информации только по установленному маршруту необходимо внедрить механизмы контроля доступа в информационной системе. Это может быть достигнуто путем установки правил маршрутизации на шлюзах и маршрутизаторах, а также путем использования шифрования и аутентификации при передаче данных. Это обеспечит более высокий уровень безопасности и надежности при передаче информации в информационной системе.

Обеспечивать надежность и безопасность передачи информации. Для обеспечения надежности и безопасности передачи информации необходимо использовать механизмы шифрования и аутентификации при передаче данных. Шифрование позволяет защитить данные от несанкционированного доступа и предотвратить их изменение в процессе передачи. Аутентификация позволяет проверить подлинность пользователя, который отправляет или получает данные, и предотвратить несанкционированный доступ к системе. Кроме того, важно контролировать доступ к информации на основе прав доступа пользователей, чтобы каждый пользователь имел доступ только к той информации, которая ему необходима для выполнения своих задач.

Предоставлять возможность контроля доступа к информации.

Установление маршрута передачи информации.

Маршрут должен быть уникальным и защищён от перенаправления для каждой передаваемой информации. Перенаправлять маршрут допускается только в случаях, установленных администратором.

Контроль передачи информации только по установленному маршруту.

Аутентификация пользователей.

Система должна проверять подлинность пользователей, чтобы предотвратить несанкционированный доступ к системе.

Система должна контролировать доступ к информации на основе прав доступа пользователей.

Пользователи должны иметь доступ только к той информации, которая им необходима для выполнения своих задач.

Технический регламент по управлению информационными потоками в информационной системе должен включать следующие меры:

1. Установление маршрута передачи информации. Каждый информационный пакет должен иметь уникальный маршрут, который определяется на основе правил маршрутизации в информационной системе. Маршрут должен быть защищен от перенаправления, и перенаправление должно быть допускается только в случаях, установленных администратором.
2. Контроль передачи информации только по установленному маршруту. Для обеспечения контроля передачи информации только по установленному маршруту необходимо использовать механизмы контроля доступа в информационной системе. Это может быть достигнуто путем установки правил маршрутизации на шлюзах и маршрутизаторах, а также путем использования шифрования и аутентификации при передаче данных. Это обеспечит более высокий уровень безопасности и надежности при передаче информации в информационной системе.
3. Аутентификация пользователей. Система должна проверять подлинность пользователей, чтобы предотвратить несанкционированный доступ к системе. Это может быть достигнуто путем использования паролей, биометрических данных или других методов идентификации пользователя.
4. Предоставление возможности контроля доступа к информации. Для предоставления возможности контроля доступа к информации необходимо установить права доступа для каждого пользователя в информационной системе. Каждый пользователь должен иметь определенный уровень доступа к информации в системе, который определяется его должностными обязанностями и ролью в организации.
5. Маршруты передачи информации должны быть защищены от перенаправления. Для обеспечения защиты маршрутов передачи информации необходимо использовать механизмы шифрования и аутентификации при передаче данных. Шифрование позволяет защитить данные от несанкционированного доступа и предотвратить их изменение в процессе передачи. Аутентификация позволяет проверить подлинность пользователя, который отправляет или получает данные, и предотвратить несанкционированный доступ к системе.
6. Контроль доступа к информации на основе прав доступа пользователей. Для обеспечения контроля доступа к информации необходимо использовать механизмы аутентификации и авторизации. Авторизация позволяет определить, какие права доступа имеет пользователь после того, как он был аутентифицирован. Это обеспечивает контроль доступа к информации на основе прав доступа пользователя и предотвращает несанкционированный доступ к конфиденциальной информации.
7. Установление прав доступа для каждого пользователя в информационной системе. Каждый пользователь должен иметь определенный уровень доступа к информации в системе, который определяется его должностными обязанностями и ролью в агентстве.
8. Механизмы управления доступом на уровне файловой системы. Для обеспечения контроля доступа к информации на более детальном уровне и предотвращения несанкционированного доступа к конфиденциальной информации можно использовать механизмы управления доступом на уровне файловой системы.
9. Контроль доступа на основе ролей пользователей. Для обеспечения более гибкого контроля доступа к информации можно использовать механизмы контроля доступа на основе ролей пользователей. Это позволяет определять доступ пользователей к информации на основе их роли в организации и задач, которые они выполняют.
10. Контроль доступа к сетевым ресурсам. Для обеспечения контроля доступа к сетевым ресурсам необходимо использовать механизмы авторизации и аутентификации. Это позволяет определить, какие сетевые ресурсы могут быть доступны для каждого пользователя в системе и предотвратить несанкционированный доступ к сетевым ресурсам.
11. Ограничение доступа к информации на основе времени. Для обеспечения контроля доступа к информации на основе времени можно использовать механизмы ограничения доступа к информации в определенное время. Это позволяет установить ограничения на доступ к информации в нерабочее время или в определенные дни недели.
12. Контроль доступа к информации на основе местоположения пользователя. Для обеспечения контроля доступа к информации на основе местоположения пользователя можно использовать механизмы определения местоположения пользователя и установления ограничений на доступ к информации в зависимости от его местоположения.
13. Ограничение доступа к информации на основе типа устройства. Для обеспечения контроля доступа к информации на основе типа устройства можно использовать механизмы определения типа устройства и установления ограничений на доступ к информации в зависимости от типа устройства.
14. Механизмы мониторинга и аудита. Для обеспечения контроля доступа к информации необходимо использовать механизмы мониторинга и аудита. Мониторинг позволяет отслеживать активность пользователей в системе и выявлять несанкционированные попытки доступа к информации. Аудит позволяет отслеживать изменения в системе и выявлять возможные нарушения безопасности.

### УПД.2\_УПД.5\_ЗСВ.2. Реализация методов управления доступами

Для обеспечения безопасности информации в информационных системах используются различные методы управления доступами. Рассмотрим три наиболее распространенных метода: дискреционный, ролевой и мандатный.

**1. Дискреционный метод**

Дискреционный метод управления доступами предполагает, что владелец информации самостоятельно определяет, кто и как может получить доступ к его ресурсам. Контроль за доступом осуществляется на основе списка контроля доступа (СКД), который содержит список пользователей и групп пользователей, имеющих доступ к объекту, а также уровень доступа (чтение, запись, исполнение и т.д.).

Реализация дискреционного метода управления доступами может быть осуществлена на уровне операционной системы или на уровне приложений.

**Требования:**

1.1 Реализация дискреционного метода управления доступами должна осуществляться на уровне операционной системы или на уровне приложений.

1.2 Должен быть разработан список контроля доступа (СКД), который содержит список пользователей и групп пользователей, имеющих доступ к объекту, а также уровень доступа (чтение, запись, исполнение и т.д.).

1.3 Владелец информации должен иметь возможность самостоятельно определять, кто и как может получить доступ к его ресурсам.

1.4 Должна быть предусмотрена возможность изменения списка контроля доступа владельцем информации.

**2. Ролевой метод**

Ролевой метод управления доступами предполагает, что доступ к ресурсам определяется на основе роли, которую играет пользователь в организации. Роли определяются в соответствии с функциями и задачами, которые выполняет пользователь. Реализация ролевого метода управления доступами может быть осуществлена на уровне приложений или на уровне баз данных.

**Требования:**

2.1 Реализация ролевого метода доступа должна осуществляться на уровне приложений или на уровне баз данных.

2.2 Должны быть разработаны роли пользователей, которые будут определять доступ к ресурсам информационной системы;

2.3 Должна быть предусмотрена возможность изменения ролей пользователей владельцем информации;

2.4 Роли пользователей должны быть определены на основе функций и задач, которые выполняет пользователь в организации;

2.5 Реализация ролевого метода доступа должна быть осуществлена с учетом требований к производительности и масштабируемости системы;

2.6 Для обеспечения безопасности информации необходимо предусмотреть возможность аудита доступа, который будет регистрировать все действия пользователей, связанные с доступом к ресурсам информационной системы.

**3. Мандатный метод**

Мандатный метод управления доступами предполагает, что доступ к ресурсам определяется на основе уровня доступа, который назначается для каждого объекта системы. Уровень доступа определяется в соответствии с категорией секретности информации, к которой относится ресурс. При использовании мандатного метода управления доступом субъект (пользователь системы) не можем управлять доступом к объектам системы, которые создаёт.

Реализация мандатного метода управления доступами может быть осуществлена на уровне операционной системы или на уровне приложений.

**Требования:**

3.1 Реализация мандатного метода управления доступами должна осуществляться на уровне операционной системы или на уровне приложений;

3.2 Должны быть разработаны уровни доступа, которые определяются в соответствии с уровнем конфиденциальности информации, к которой относится ресурс;

3.3 Должна быть предусмотрена возможность изменения уровней доступа владельцем информации.

3.4 Для реализации уровней доступа необходимо использовать базу данных, которая будет содержать информацию о пользователях, группах пользователей и уровнях доступа.

3.5 Для обеспечения безопасности информации необходимо предусмотреть возможность аудита доступа, который будет регистрировать все действия пользователей, связанные с доступом к ресурсам информационной системы.

**4. Реализация разграничения правил доступа в информационной системе**

**Требования:**

4.1 Реализация разграничения правил доступа должна осуществляться на уровне операционной системы или на уровне приложений;

4.2 Должны быть разработаны правила доступа, которые определяют, кто и как может получить доступ к ресурсам информационной системы;

4.3 Пользователю должно быть предоставлено только тот минимальный доступ, который необходим для выполнения его задач;

4.4 Должна быть предусмотрена возможность изменения правил доступа владельцем информации;

4.5 Для реализации правил доступа необходимо использовать базу данных, которая будет содержать информацию о пользователях, группах пользователей и уровнях доступа;

4.6 Для обеспечения безопасности информации необходимо предусмотреть возможность аудита доступа, который будет регистрировать все действия пользователей, связанные с доступом к ресурсам информационной системы.

4.7 Правила доступа должны быть определены на основе ролей пользователей, а также на основе уровня допуска к информации, к которой относится ресурс.

4.8 Реализация разграничения правил доступа должна быть осуществлена с учетом требований к производительности и масштабируемости системы.

**Границы применения методов управления доступом**

Необходимо комбинировать методы управления доступом, т. к. ни один из методов, при использовании его в чистом виде, не отвечает требованиям, предъявляемым к системе. Примеры использования методов:

* Для предоставления пользователем прав доступа к компонентам и функциям системы - использовать ролевой метод.
* Для предоставления доступа к файлам, которые пользователи загружают в систему и используют для совместной работы с другими пользователями - использовать дискреционный метод.
* Для работы с данными, расположенными в СУБД (в том числе и с персональными данными) использовать ролевой метод.
* Для работы с файлами, расположенными во внешних системах (в том числе и с персональными данными) использовать мандатный метод.

**5. Управление доступом к техническим средствам, устройствам и внешним устройствам**

Управление доступом к техническим средствам, устройствам и внешним устройствам предполагает контроль доступа к оборудованию, которое используется для обработки, хранения и передачи информации. Это включает в себя компьютеры, серверы, мобильные устройства, сетевое оборудование и другие устройства.

**Требования:**

5.1 Должны быть определены пользователи и группы пользователей, которые имеют право на доступ к техническим средствам, устройствам и внешним устройствам;

5.2. Должен быть разработан список контроля доступа (СКД), который содержит список пользователей и групп пользователей, имеющих доступ к техническим средствам, устройствам и внешним устройствам, а также уровень доступа (чтение, запись, исполнение и т.д.).

5.3 Должна быть предусмотрена возможность изменения списка контроля доступа владельцем информации.

5.4 Для реализации управления доступом к техническим средствам, устройствам и внешним устройствам необходимо использовать базу данных, которая будет содержать информацию о пользователях, группах пользователей и уровнях доступа.

5.5 Должны быть определены правила и процедуры для управления доступом к техническим средствам, устройствам и внешним устройствам.

5.6 Должна быть предусмотрена возможность аудита доступа, который будет регистрировать все действия пользователей, связанные с доступом к техническим средствам, устройствам и внешним устройствам.

5.7 Управление доступом к техническим средствам, устройствам и внешним устройствам должно быть осуществлено с учетом требований к производительности и масштабируемости системы.

5.8 Должны быть определены процедуры и правила безопасности для использования технических средств, устройств и внешних устройств.

5.9 Должны быть определены правила и процедуры для управления доступом к сетевым ресурсам и сервисам.

5.10 Должна быть предусмотрена возможность ограничения доступа к техническим средствам, устройствам и внешним устройствам для пользователей и групп пользователей, которые не имеют необходимого уровня доступа.

5.11 Должны быть реализованы механизмы защиты от вредоносного кода и злоумышленников при использовании технических средств, устройств и внешних устройств.

5.12 Должны быть реализованы механизмы защиты от утечки конфиденциальной информации при использовании технических средств, устройств и внешних устройств.

5.13 Должна быть обеспечена возможность удаленного управления техническими средствами, устройствами и внешними устройствами с целью обеспечения безопасности информации.

**6. Управление доступом субъектов к объектам, создаваемым общесистемным (общим) программным обеспечением**

**Требования:**

6.1 Должны быть определены правила и процедуры управления доступом субъектов к объектам, включая принципы минимальных привилегий;

6.2 Должны быть предусмотрены механизмы защиты от вредоносного кода и злоумышленников при использовании общесистемного программного обеспечения;

6.3 Должны быть определены процедуры и правила безопасности для использования общесистемного программного обеспечения;

6.4 Должна быть предусмотрена возможность аудита доступа, для регистрации действий субъектов, связанные с доступом к объектам, создаваемым общесистемным программным обеспечением;

6.5 Управление доступом к объектам, создаваемым общесистемным программным обеспечением, должно быть осуществлено с учетом требований к производительности и масштабируемости системы;

6.6 Должны быть разработаны и реализованы процедуры резервного копирования и восстановления данных, создаваемых общесистемным программным обеспечением, для обеспечения защиты от случайной потери данных;

6.7 Управление доступом к объектам, создаваемым общесистемным программным обеспечением, должно регулярно проверяться и анализироваться для обеспечения соответствия установленным требованиям и выявления возможных уязвимостей.

6.8 Должны быть определены пользователи и группы пользователей, которые имеют право на доступ к объектам, создаваемым общесистемным программным обеспечением;

6.9 Должен быть разработан список контроля доступа (СКД), который содержит список пользователей и групп пользователей, имеющих доступ к объектам, создаваемым общесистемным программным обеспечением, а также уровень доступа (чтение, запись, исполнение и т.д.);

6.10 Для реализации управления доступом к объектам, создаваемым общесистемным программным обеспечением, необходимо использовать базу данных, которая будет содержать информацию о пользователях, группах пользователей и уровнях доступа;

6.11 Должны быть определены процедуры и правила безопасности для использования объектов, создаваемых общесистемным программным обеспечением;

6.12 Должна быть предусмотрена возможность ограничения доступа к объектам, создаваемым общесистемным программным обеспечением, для пользователей и групп пользователей, которые не имеют необходимого уровня доступа;

6.13 Управление доступом к объектам, создаваемым общесистемным программным обеспечением, должно регулярно проверяться и анализироваться для обеспечения соответствия установленным требованиям и выявления возможных уязвимостей.

### УПД.1. ****Управление (заведение, активация, блокирование и уничтожение) учетными записями пользователей, в том числе внешних пользователей****

1. Определение типа учетной записи и группы:

1.1 Внутренний пользователь (группа внутренних пользователей) - пользователь, являющийся сотрудником организации и имеющий учётную запись в системе.

1.2 Внешний пользователь (группа внешних пользователей) - пользователь, не являющийся сотрудником организации, но имеющий учётную запись для доступа к определенным ресурсам системы.

1.3 Системная учётная запись (группа системных учётных записей) - учётная запись, используемая системой для аутентификации и авторизации действий Системы при взаимодействии со связанными системами и сервисами организации.

1.4 Учётная запись приложения (группа учётных записей приложений) - учётная запись, используемая внешними системами для аутентификации и авторизации действий, связанных с доступом к ресурсам Системы.

1.5 Гостевая (анонимная) учётная запись - учётная запись внешнего пользователя, предоставляющая доступ к ресурсам системы не требующих доступа к конфиденциальным данным и/или пользовательским (функциональным) интерфейсам.

1.6 Привилегированная учётная запись — учётная запись типа «внутренний пользователь», которой назначен один или несколько мандатов, связанных с авторизацией административных, установочных (настроечных) функций или функций мониторинга Системы. При создании привилегированной учётной записи необходимо определить права доступа к системе и ограничить их на уровне минимально необходимого доступа. Привилегированные учётные записи должны быть защищены ключами доступа (со стойкой парольной защитой) и двух(много)факторной аутентификацией и использоваться только для выполнения необходимых задач (функции, характерные для других типов учётных записей должны быть недоступны). Доступ к привилегированным учётным записям должен быть ограничен и отслеживаться в журналах системы.

Учётные записи могут обладать периодами действия и доступа. В этом случае, они должны группироваться в виртуальную коллекцию временных учётных записей.

Внешние учётные записи, учётные записи приложений должны обладать обязательным списком договоров/соглашений, на основании которых должны определяться периоды действия, группы доступа и мандаты пользователей.

2. Верификация пользователя (проверка личности пользователя, его должностных и/или функциональных обязанностей) при создании учетной записи.

При создании учетной записи пользователя необходимо провести верификацию его личности и должностных обязанностей[[6]](#footnote-6). Для этого необходимо выполнить следующие действия:

2.1 Определение типа учетной записи. После выполнения верификации личности и должностных обязанностей пользователя необходимо определить тип учетной записи в соответствии с регламентом определения типа учетной записи. Это позволит определить группы доступа и мандаты пользователя в системе за счёт чего установить соответствующие ограничения.

3. Создание, активация, блокирование и уничтожение учетных записей пользователей.

Описание процедур создания, активации, блокирования и уничтожения учетных записей пользователей.

Создание учётной записи:

3.1 Для создания учётной записи необходимо выполнить верификацию личности и должностных обязанностей пользователя в соответствии с регламентом верификации пользователя.

3.2 После создания учётной записи необходимо предоставить пользователю информацию об учетных данных (логин, пароль/сертификат, список резервных кодов для двух(много)факторной аутентификации) и установленных группах доступа и мандатах/правах в Системе.

Технические требования к реализации данного пункта:

3.2.1 В системе Keycloak необходимо перейти в раздел "Управление пользователями" и нажать кнопку "Создать".

3.2.2 Затем необходимо заполнить все обязательные поля, такие как имя пользователя, адрес электронной почты, выбрать способ аутентификации: пароль / ключ / сертификат.

3.2.3 После этого необходимо присвоить пользователю группы и назначить в их рамках мандаты (система автоматически должна определить наборы ролей и права на действия) в соответствии с его должностными обязанностями.

Активация учётной записи

3.3 Для активации учётной записи необходимо получить от пользователя подтверждение ознакомления с правилами использования системы и согласие на их соблюдение. Зафиксировать юридически значимое действие.

3.4 Обеспечить активацию учётной записи пользователя за счёт верификации контактных данных, после чего настроить использование подсистемы поддержки двух(много)факторной аутентификации.

3.5 После получения подтверждения активации и включения 2FA необходимо активировать учётную запись пользователя в системе.

Блокирование учётной записи

3.6 Учётная запись пользователя может быть заблокирована в случае нарушения правил использования системы или при угрозе безопасности системы вручную или автоматически (при выполнении критериев, таких как максимальное количество неуспешных входов).

3.7 Учётная запись пользователя может быть заблокирована на определённый срок или бессрочно.

3.8 При блокировке учетной записи необходимо уведомить пользователя о причинах блокировки и предоставить инструкции по дальнейшим действиям.

Уничтожение учётной записи

В соответствии с законодательством, организация обязана сохранять данные пользователей в течение определенного периода времени и предоставлять их по запросу судебных или иных органов. При сохранении данных пользователей необходимо соблюдать все требования, установленные законодательством, включая требования к защите персональных данных. Удаление учётных записей должно происходить автоматизированным способом с обязательной записью в журнал.

3.8 Учетная запись пользователя может быть отключена в случае увольнения пользователя или иных обстоятельствах, когда учетная запись больше не нужна.

3.9 Отключенные учётные записи, предельный срок хранения которых закончен, могут быть удалены из системы. При этом:

* должны выполняться процедуры контроля ссылочной целостности данных, при которых, в частности, должна происходить замена ссылок на фиксированную учётную запись «пользователь удалён», которая расширяет перечень типов учётных записей и не предполагает аутентификацию и авторизацию каких бы то ни было действий в Системе;
* в журнал Системы должна попасть запись об удалении пользователя и замены идентификатора пользователя на учётную запись «пользователь удалён» с указанием удаляемого идентификатора.

4. Пересмотр и корректировка учётных записей пользователей с периодичностью, определяемой документом, на основании которого учётные записи были созданы.

Пересмотр учётных записей

4.1 Периодичность пересмотра учётных записей определяется оператором системы;

4.2 В процессе пересмотра учётных записей необходимо проверить корректность данных пользователя и права доступа в системе;

4.3 При обнаружении несоответствий или изменений в должностных обязанностях пользователя необходимо внести соответствующие изменения в учётную запись.

Корректировка учетных записей

4.4. Корректировка учётных записей может быть проведена в любое время по запросу пользователя или по инициативе оператора системы;

4.5 При корректировке учётных записей необходимо проверить корректность данных пользователя и права доступа в системе;

4.6 При необходимости внести изменения в учётную запись, необходимо уведомить пользователя об изменениях и предоставить инструкции по использованию учётной записи.

5. Оповещение администратора об изменении сведений о пользователях

Оповещение администратора

5.1 Изменения сведений о пользователях и их учетных записях должны быть зарегистрированы в журнале системы.

5.2 При обнаружении изменений, связанных с пользовательскими учетными записями, необходимо немедленно оповестить администратора системы.

6. Предоставление пользователям прав доступа к объектам доступа информационной системы, основываясь на задачах, решаемых пользователями в информационной системе и взаимодействующими с ней информационными системами.

Принцип предоставления прав доступа пользователям к объектам доступа информационной системы, основываясь на задачах, решаемых пользователями в информационной системе и взаимодействующими с ней информационными системами.

Предоставление прав доступа

6.1 При создании учётной записи пользователя необходимо определить права доступа к объектам информационной системы на основании его задач и функций;

6.2 Права доступа к информационной системе должны быть регулируемыми и соответствовать принципу необходимости минимального доступа;

6.3 При изменении задач и функций пользователя в информационной системе необходимо изменять и его права доступа к объектам информационной системы;

6.4 При взаимодействии между информационными системами, необходимо учитывать задачи и функции пользователей в этих информационных системах и предоставлять им соответствующие права доступа;

Предоставление прав доступа при использовании удаленного доступа и мобильных устройств, в том числе через VPN

6.5 При использовании удаленного доступа с использованием мобильных устройств необходимо определить права доступа к объектам информационной системы на основании задач и функций пользователя и учитывая риски, связанные с доступом к конфиденциальной информации за пределами организации;

6.6 Права доступа к информационной системе при использовании удаленного доступа с использованием мобильных устройств должны быть регулируемыми и соответствовать принципу необходимости минимального доступа;

6.7 При использовании удаленного доступа с использованием мобильных устройств необходимо использовать механизмы защиты, такие как шифрование и аутентификацию, для предотвращения несанкционированного доступа к конфиденциальной информации;

6.8 При взаимодействии между информационными системами через удаленный доступ и мобильные устройства необходимо учитывать задачи и функции пользователей в этих информационных системах и предоставлять им соответствующие права доступа.

7. Регламент использования автоматизированных средств поддержки управления учётными записями пользователей

Использование автоматизированных средств

7.1 Автоматизированные средства поддержки управления учётными записями пользователей должны использоваться для создания, изменения и удаления учётных записей пользователей, а также для управления правами доступа к информационной системе.

7.2 Использование автоматизированных средств поддержки управления учётными записями пользователей должно осуществляться в соответствии с установленными процедурами безопасности.

7.3 Администраторы не должны иметь возможностей использования автоматизированных средств поддержки управления учетными записями пользователей для получения доступа к конфиденциальной информации без необходимых разрешений.

8. Автоматическая блокирование временных учетных записей

8.1 При создании временной учетной записи необходимо определить срок, на который будет выдан доступ к системе.

8.2 При истечении срока действия временной учетной записи, необходимо автоматически заблокировать ее.

8.3 При блокировке временной учетной записи необходимо уведомить пользователя об этом и предоставить инструкции по ее восстановлению.

8.4 Временные учетные записи должны быть автоматически удалены из системы после окончания установленного периода времени для их использования.

9. Регламент автоматического блокирования неактивных учетных записей.

9.1 Если учётная запись пользователя остается неактивной в течение периода времени, равного или превышающего 90 дней, то она должна быть автоматически заблокирована; Об этом должна быть сделана запись в системный журнал.

9.2 Заблокированная учётная запись может быть восстановлена.

### УКФ.4. Документирование информации (данных) об изменениях в конфигурации информационной системы и системы защиты персональных данных.

1. Система документирования должна быть интегрирована с системой контроля версий и позволять фиксировать изменения в конфигурации информационной системы и системе защиты персональных данных.
   * Система документирования должна автоматически создавать новый документ при каждом изменении.
   * В документе должны фиксироваться дата и время изменения, а также пользователь, который внес изменения.
2. Документация должна содержать подробное описание каждого изменения, включая его характеристики, цель и принятые меры для защиты персональных данных.
   * Документация должна быть структурированной и легко доступной для всех уполномоченных лиц в организации.
3. Документация должна содержать информацию о текущей конфигурации информационной системы и системы защиты персональных данных.
   * Документация должна содержать информацию о версиях используемых программных компонентов, настройках безопасности и правах доступа.
4. Документация должна быть защищена от несанкционированного доступа и сохранена в надежном хранилище.
   * Доступ к документации должен быть ограничен только для уполномоченных лиц в организации.
   * Документация должна регулярно резервироваться и храниться в надежном месте.
5. Документация должна регулярно проверяться и обновляться в соответствии с изменениями в конфигурации информационной системы и системы защиты персональных данных.
   * Проверка документации должна проводиться не реже одного раза в месяц.
   * Обновление документации должно происходить незамедлительно после каждого изменения в конфигурации информационной системы и системе защиты персональных данных.

### УКФ.3. ****Анализ потенциального воздействия планируемых изменений в конфигурации информационной системы и системы защиты персональных данных на обеспечение защиты персональных данных и согласование изменений в конфигурации информационной системы с должностным лицом (работником), ответственным за обеспечение безопасности персональных данных****

**Общие положения:**

1. Целью цикла безопасной разработки является повышение уровня безопасности разрабатываемого программного обеспечения.
2. Цикл безопасной разработки включает в себя следующие этапы: планирование, проектирование, разработку, тестирование, внедрение и поддержку.
3. Все этапы цикла безопасной разработки должны проходить с учетом требований к безопасности, установленных организацией.
4. Разработчики и тестировщики обязаны проходить обучение по вопросам безопасности перед началом работы.

**Разработка:**

1. Разработчики должны следовать правилам безопасного кодирования.
2. Весь код должен проходить процедуры code review и merge request ответственным за безопасность.
3. Перед внесением изменений в продуктивную среду должен быть проведен тест на безопасность.

**Тестирование:**

1. Все приложения должны проходить тестирование на безопасность перед передачей в эксплуатацию.
2. При обнаружении уязвимостей необходимо незамедлительно устранять их.

**Внедрение:**

1. Внесение изменений в продуктивную среду должно осуществляться только после проведения теста на безопасность.
2. При внесении изменений в продуктивную среду необходимо соблюдать процедуры code review и merge request ответственным за безопасность.

### УКФ.2. Управление изменениями конфигурации информационной системы и системы защиты персональных данных

**Определения**

* **Информационная система (ИС)** - комплекс взаимосвязанных между собой программных и аппаратных компонентов, предназначенных для обработки, хранения и передачи данных.
* **Система защиты персональных данных (СЗПД)** - комплекс мероприятий, направленных на обеспечение безопасности персональных данных при их обработке в информационной системе.
* **Конфигурация ИС** - состояние информационной системы, описывающее состояние ее компонентов и связей между ними.

Процесс управления изменениями конфигурации ИС и СЗПД

1. Инициирование изменений. Изменения конфигурации ИС и СЗПД могут быть инициированы внутренними или внешними источниками. Информация о планируемых изменениях должна быть документирована в специальной форме и предоставлена ответственному за управление изменениями конфигурации ИС и СЗПД.
2. Оценка изменений. Ответственный за управление изменениями конфигурации ИС и СЗПД должен оценить планируемые изменения и определить их влияние на ИС и СЗПД в целом. В случае необходимости могут быть проведены дополнительные исследования или консультации.
3. Анализ изменений. Должен быть проведен анализ технической и финансовой целесообразности планируемых изменений.
4. Утверждение изменений. Одобренные изменения должны быть утверждены ответственным за управление изменениями конфигурации ИС и СЗПД.
5. Реализация изменений. Изменения должны быть реализованы в соответствии с утвержденной документацией и процедурами. Перед реализацией изменений должны быть проведены необходимые испытания и проверки.
6. Тестирование изменений. После реализации изменений должно быть проведено тестирование, которое должно включать как функциональное, так и регрессионное тестирование.
7. Внедрение изменений. После успешного тестирования изменения должны быть внедрены в ИС и СЗПД.
8. Мониторинг изменений. Ответственный за управление изменениями конфигурации ИС и СЗПД должен следить за влиянием изменений на ИС и СЗПД и своевременно принимать меры для устранения проблем, возникающих в процессе эксплуатации ИС и СЗПД.

**Ответственности**

* Ответственный за управление изменениями конфигурации ИС и СЗПД должен контролировать процесс управления изменениями и гарантировать его правильную реализацию.
* Руководители структурных подразделений должны осуществлять контроль за своевременным и правильным выполнением документированных процедур по управлению изменениями конфигурации ИС и СЗПД.
* Сотрудники, участвующие в процессе управления изменениями, должны соблюдать установленные процедуры и правила.

### СОВ.1\_СОВ.2. Обнаружение вторжений

**Требования:**

1. Компоненты для записи событий безопасности (сенсоры), которые должны обеспечивать надежный и бесперебойный мониторинг информационной системы.
2. Компоненты для анализа событий безопасности и обнаружения компьютерных атак (анализаторы), которые должны обладать высокой степенью точности и надежности.
3. База данных решающими правилами, содержащую информацию о характеристиках компьютерных атак, которые должны обновляться регулярно.

Обнаружение (предотвращение) вторжений должно осуществляться на внешней границе информационной системы:

**Требования:**

1. Система обнаружения вторжений на внешнем уровне должна быть размещена на границе информационной системы и сети.
2. Система обнаружения вторжений на внешнем уровне должна быть способна обнаруживать компьютерные атаки с высокой степенью точности и надежности.
3. Система обнаружения вторжений на внешнем уровне должна быть способна регистрировать и сохранять информацию о всех событиях безопасности, происходящих на границе информационной системы.
4. База данных решающих правил должна содержать информацию о характеристиках компьютерных атак.
5. База данных решающих правил должна обновляться регулярно.
6. Мониторинг систем обнаружения вторжений должен осуществляться круглосуточно.
7. Системы обнаружения вторжений должны быть способны автоматически уведомлять о нарушениях безопасности.
8. Системы обнаружения вторжений должны быть способны генерировать отчёты о событиях безопасности и сохранять их в базе данных.

**Требования к отчётности:**

1. Отчёты о событиях безопасности должны создаваться регулярно.
2. Отчёты о событиях безопасности должны содержать информацию о характеристиках компьютерных атак.
3. Отчёты о событиях безопасности должны быть сохранены в базе данных.

### РСБ.7\_АВЗ.1\_АВЗ.2. ****Защита информации о событиях безопасности****

**Требования:**

1. Для защиты от вирусов и других вредоносных программ на всех компьютерах серверах и виртуальных машинах установливается антивирусный софт;
2. Антивирусное ПО настривается на автоматическое обновление баз вирусов не реже одного раза в сутки;
3. При возникновении подозрительных событий (например, обнаружение вредоносного ПО) антивирусное ПО уведомляет пользователя и админтстратора об этом;
4. Все подозрительные файлы помещаются в карантин, а затем удаляются или отправляются на анализ в службу информационной безопасности;
5. При обнаружении вредоносного ПО на компьютере, сервере или антивирусной защиты, антивирусное ПО производит его удаление;
6. Для обнаружения вторжений на компьютеры, серверы, виртуальные машины может быть установлено специальное ПО;
7. Система обнаружения вторжений настраивается на автоматическое обновление своих баз данных не реже одного раза в сутки;
8. Система обнаружения вторжений производит мониторинг событий, связанных с доступом к файлам и папкам, а также с сетевым трафиком;
9. При возникновении подозрительных событий система обнаружения вторжений уведомляет пользователя и админстратора об этом;
10. Все подозрительные события занесятся в журналы и передаются на анализ в службу информационной безопасности;

### РСБ.6. Генерирование временных меток и (или) синхронизация системного времени в информационной системе

В информационной системе (далее ИС) может возникнуть проблема не синхронизации времени между сервисами и серверами, что может привести к ошибкам в работе ИС и потере данных.

**Требования:**

1. ИС должна иметь возможность получения точного времени из источника, такого как NTP сервер. Для этого ИС должна иметь соответствующее программное обеспечение или модуль, который позволит получить данные о точном времени и дате от NTP сервера.
2. ИС может иметь функционал синхронизации времени во всех сервисах и серверах в сети с точностью до нескольких миллисекунд. Для этого ИС может использовать точное время от NTP сервера и распространять его на все сервисы и серверы в сети.
3. Синхронизация времени должна происходить автоматически с определенной периодичностью, например, раз в час (более точное время синхронизации будет определено во время технического проектирования). Это позволит обеспечить постоянную синхронизацию времени на всех сервисах и серверах в ИС, даже в случае изменения времени на NTP сервере. Автоматическая синхронизация также облегчит управление временем в ИС и снизит вероятность ошибок.
4. ИС должна иметь возможность установить свой часовой пояс и корректировать время в соответствии с летним и зимним временем. Для этого ИС должна иметь соответствующие настройки времени, которые позволят установить нужный часовой пояс и корректировать время в соответствии с летним и зимним временем.
5. Если ИС не может получить точное время от NTP сервера, она может использовать локальную системные часы в качестве времени по умолчанию.
6. ИС отображает время в формате 24-часа формат или AM/PM. Например, ЧЧ:ММ:СС.
7. ИС отображает дату в формате: ДД:ММ:ГГГГ. Функциональные требования будут учтены на стадии технического проектирования
8. ИС может иметь возможность настройки NTP сервера, для получения точного времени.
9. ИС может иметь возможность установки интервала синхронизации времени с NTP сервером.
10. ИС может иметь возможность отображения статуса синхронизации времени с NTP сервером.

### РСБ.1\_РСБ.2\_РСБ.3\_РСБ.4\_РСБ.5\_ЗСВ.3. Техническое задание на подсистему учёта событий в информационной системе и процесс структурированного описания этих событий

**Требования:**

1. Система должна регистрировать события, происходящие в информационной системе, включая ошибки, угрозы информационной безопасности, предупреждения и действия пользователей. Запись в журнал содержит следующую информацию: 1.1 идентификатор пользователя + статус пользователя в системе; 1.2 идентификатор рабочего места; 1.3 дата и время события (формат timestamp и формат понятный для восприятия человеком RFC 2822); 1.4 идентификатор объекта; 1.5 сервис (имя и протокол); 1.6 расположение кода: имя скрипта, имя модуля; 1.7 адрес источника (например, идентификатор устройства);
2. Регистрация событий делится на 3 разных журнала: 2.1 прикладной (запись действий ПО) 2.2 системный (запись действий ОС); 2.3 аудит безопасности (общая запись действий в системе);
3. Детализированный сбор событий позволит оперативно реагировать на сбои, в том числе аппаратные и программные ошибки и так далее.
4. Система может обеспечивать возможность просмотра журналов событий. Данный функционал позволит отслеживать работу системы и реагировать на возможные проблемы.
5. Зарегистрированные события передаются в систему сбора логов SIEM. В данной системе можно производить мониторинг результатов регистрации.
6. Период хранения определяется на стадии технического проектирования.

### ОЦЛ.6\_ОЦЛ.7\_ОЦЛ.8. В информационной системе должно осуществляться ограничение прав пользователей по вводу информации в информационную систему

**Требования:**

1. Вводить значения только в поля, предназначенные для конкретного типа данных;
2. Не вводить значения, превышающие максимально допустимый размер поля;
3. Не вводить значения, не соответствующие формату поля;
4. Не вводить значения, не являющиеся допустимыми для конкретного типа данных;
5. Вводить значения с учетом всех специальных символов и ограничений, присущих конкретному полю.
6. Контроль ошибочных действий пользователей по вводу и (или) передаче персональных данных и предупреждение пользователей об ошибочных действиях
7. Система должна контролировать ввод данных и предупреждать пользователя в случае нарушения требований к вводу данных.

* При попытке ввода значения, превышающего максимально допустимый размер поля, должно выводиться сообщение об ошибке.
* При попытке ввода значения, не соответствующего формату поля, должно выводиться сообщение об ошибке.
* При попытке ввода значения, не являющегося допустимым для конкретного типа данных, должно выводиться сообщение об ошибке.
* При вводе и (или) передаче персональных данных, система должна предупреждать пользователя о том, что передаются персональные данные.

Пример тест кейса для проверки:

Шаги:

1. Ввести целочисленное значение в поле для целочисленных значений.
   * Ожидаемый результат: значение сохраняется корректно.
2. Ввести дробное число в поле для дробных значений.
   * Ожидаемый результат: значение сохраняется корректно.
3. Ввести строковое значение в поле для строковых значений.
   * Ожидаемый результат: значение сохраняется корректно.
4. Ввести булево значение в поле для булевых значений.
   * Ожидаемый результат: значение сохраняется корректно.
5. Ввести значение, превышающее максимально допустимое для целочисленных значений, в поле для целочисленных значений.
   * Ожидаемый результат: значение не сохраняется и выводится сообщение об ошибке.
6. Ввести значение, не являющееся числом, в поле для дробных значений.
   * Ожидаемый результат: значение не сохраняется и выводится сообщение об ошибке.
7. Ввести значение, содержащее специальные символы, в поле для строковых значений.
   * Ожидаемый результат: значение сохраняется корректно.
8. Ввести значение, не являющееся булевым, в поле для булевых значений.
   * Ожидаемый результат: значение не сохраняется и выводится сообщение об ошибке.

### ОЦЛ.4. ****Обнаружение и реагирование на поступление в информационную систему незапрашиваемых электронных сообщений (писем, документов) и иной информации, не относящихся к функционированию информационной системы (защита от спама)****

**Требования**

1. Администраторы системы могут устанавливать ограничения на загрузку файлов с определенными расширениями или из определенных источников. Например, администраторы **могут** заблокировать загрузку файлов .exe, .bat, .xlsxm которые могут содержать вредоносный код. Также, они могут блокировать загрузку файлов из внешних источников, которые не являются доверенными.
2. Система может быть настроена таким образом, чтобы автоматически блокировать определенные типы данных при их загрузке. Например, система может блокировать загрузку архивов, которые могут содержать вредоносные файлы, или файлов, которые содержат исполняемый код.
3. Система может использовать аналитические инструменты для мониторинга и анализа потока данных, чтобы выявлять и блокировать незапрашиваемые сообщения и файлы.
4. Все устройства, используемые для доступа к информационной системе, должны быть защищены паролем или другими методами аутентификации, чтобы предотвратить несанкционированный доступ к системе и загрузку нежелательных данных. Кроме того, рекомендуется использовать многопользовательскую систему с различными уровнями доступа, чтобы предотвратить несанкционированный доступ к конфиденциальным данным.
5. Важно регулярно обновлять программное обеспечение, используемое в информационной системе, в том числе операционную систему, браузер, антивирусное ПО и другие приложения. Это поможет устранить уязвимости в системе, которые могут быть использованы злоумышленниками для загрузки нежелательных данных.
6. Все сообщения, попадающие в систему, могут быть подвержены обязательной процедуре аутентификации сервиса отправителя. Этот шаг позволит удостовериться в подлинности каждого сообщения, принимаемого информационной системой. Процесс аутентификации может быть выполнен с использованием локального сервера сертификации. Этот метод требует поддержки как со стороны разрабатываемой системы, так и со стороны систем, сосуществующих взаимодействие с ней.
7. Наконец, рекомендуется проводить регулярные проверки системы на наличие нежелательных данных и проводить анализ данных о блокированных сообщениях и файлах. Это поможет определить эффективность принятых мер и внести необходимые изменения в регламент по предотвращению загрузки нежелательных данных.

### ОЦЛ.3. Обеспечение возможности восстановления программного обеспечения, включая программное обеспечение средств защиты информации, при возникновении нештатных ситуаций

1.Определения

* Восстановление ПО - процедура восстановления работоспособности программного обеспечения в случае его отказа или повреждения.
* Нештатная ситуация - ситуация, которая может привести к невозможности использования ПО.

2. Требования

2.1. Резервное копирование

* Вся информация, необходимая для восстановления ПО, должна регулярно резервироваться на внешние носители.
* Резервное копирование должно проводиться не реже одного раза в неделю.

2.2. Архивация

* Архивирование должно проводиться на регулярной основе для сохранения исходного кода ПО и его версий.
* Архивы должны храниться отдельно от основного хранилища.

2.3. Мониторинг состояния ПО

* Необходимо регулярно проводить мониторинг состояния ПО для выявления сбоев и ошибок.
* Для мониторинга можно использовать специальные программы или сервисы.

3. Восстановления ПО

3.1. Определение нештатной ситуации

* Нештатная ситуация может быть обнаружена как автоматически, так и вручную.
* В случае обнаружения нештатной ситуации, необходимо немедленно приступить к восстановлению ПО.

3.2. Последовательность восстановления ПО

* Последовательность восстановления ПО должна быть строго определена и документирована.

3.3. Оценка результата восстановления ПО

* После восстановления ПО необходимо провести тестирование его работоспособности.
* В случае недостаточного уровня работоспособности ПО, необходимо повторить процедуру восстановления или принять меры по устранению проблемы.

3.4. Документирование результатов восстановления ПО

* Все результаты восстановления ПО должны быть документированы.
* Документация должна включать информацию о причинах возникновения нештатной ситуации, последовательности восстановления ПО и оценке результата.

### ОЦЛ.2. Контроль целостности персональных данных, содержащихся в базах данных информационной системы

**Требования:**

1. **Авторизация и аутентификация:**

* Доступ к персональным данным должен быть разрешен только авторизованным пользователям.

1. **Методы защиты данных: -** Контроль доступа. Ограничение доступа к данным только на основе полномочий пользователей;

* Аудит. Фиксация событий, связанных с доступом к данным, чтобы можно было отследить любые нарушения безопасности;
* Мониторинг. Отслеживание действий пользователей в системе, чтобы можно было быстро обнаружить любые подозрительные действия.

1. **Контроль правильности ввода данных:**

* Данные должны проверяться на правильность ввода с помощью автоматических проверок;

1. **Резервное копирование данных:**

* Регулярно должны создаваться резервные копии данных. Резервные копии должны храниться в надежном месте, защищенном от несанкционированного доступа;

1. **Обновление программного обеспечения:** Программное обеспечение должно регулярно обновляться, чтобы исправлять уязвимости и проблемы, которые могут повлиять на целостность данных.

### ОЦЛ.1\_ЗСВ.8. Контроль целостности программного обеспечения, включая программное обеспечение средств защиты информации

**Процедура контроля целостности**

1. Контроль целостности выполняется ежемесячно, а также после установки любых новых программных компонентов или обновлений.
2. Для каждого программного компонента или обновления вычисляется хэш-сумма.
3. Полученные хэш-суммы сравниваются с оригинальными значениями, которые были получены от поставщика программного обеспечения.
4. Если хэш-суммы не совпадают, то программный компонент или обновление считается нецелостным и должен быть удален.
5. Если не удалось получить оригинальную хэш-сумму от поставщика программного обеспечения, необходимо связаться с ним и получить ее.
6. В случае обнаружения нецелостного программного компонента или обновления необходимо провести расследование, чтобы выяснить, каким образом это произошло.

**Процедура контроля целостности средств защиты информации**

1. Контроль целостности средств защиты информации выполняется ежедневно и во время каждой загрузки/перезагрузки ОС.
2. Для каждого средства защиты информации вычисляется хэш-сумма.
3. Полученные хэш-суммы сравниваются с оригинальными значениями, которые были получены от поставщика средств защиты информации.
4. Если хэш-суммы не совпадают, то средство защиты информации считается нецелостным и должно быть заменено на новое.
5. Если не удалось получить оригинальную хэш-сумму от поставщика средства защиты информации, необходимо связаться с ним и получить ее.
6. В случае обнаружения нецелостного средства защиты информации необходимо провести расследование, чтобы выяснить, каким образом это произошло.

**Список терминов**

* Хэш-сумма – это результат применения алгоритма хэширования к файлу или куску данных. Это уникальная строка фиксированной длины, которая обычно используется для проверки целостности данных.
* Программный компонент – это отдельный компонент программного обеспечения, который может выполнять определенную функцию.
* Обновление – это изменение программного компонента, выпущенное после его первоначального выпуска.
* Средство защиты информации – это программный компонент, который обеспечивает защиту компьютерной системы от несанкционированного доступа и других угроз безопасности.
* Поставщик программного обеспечения – это организация или физическое лицо, которое разрабатывает и поставляет программное обеспечение.

### ОПС.2. ****Управление установкой (инсталляцией) компонентов программного обеспечения, в том числе определение компонентов, подлежащих установке, настройка параметров установки компонентов, контроль за установкой компонентов программного обеспечения****

**Требования:**

1.1 Система может иметь возможность обновления списка программного обеспечения и его версий;

1.2 Система может иметь возможность автоматически загрузить и установить обновления для программного обеспечения;

1.3 Система может иметь возможность создания отчетов о текущей версии программного обеспечения и обновлениях, которые были установлены;

1.4 Система может иметь возможность удалять программное обеспечение из списка, если оно больше не используется;

1.5 Система должна иметь возможность сохранять историю обновлений программного обеспечения для последующего анализа.

**Поддержка списка программного обеспечения:**

2.1 Список с используемым программным обеспечением поддерживается в актуальном состоянии, включая все используемые библиотеки и дополнения. В этом списке указывается:

* Название программного обеспечения;
* Версия программного обеспечения;
* Дата установки;
* Дата последнего обновления;

2.2 Сотрудник обновляет список программного обеспечения и его версий по мере необходимости. Обновление списка должно происходить в течение 3 рабочих дней после установки нового программного обеспечения или обновления уже используемого;

2.3 Сотрудник проверяет наличие обновлений для всех программ в списке и устанавливает их по мере доступности всех систем для обновления;

2.4 Сотрудник удаляет, при необходимости, программное обеспечение из списка, если оно больше не используется.

2.5 Название и версия удалённого программного обеспечения должно быть сохранено в каком-либо отчёте.

**История обновлений:**

3.1 Система сохраняет историю обновлений программного обеспечения для последующего анализа. История должна содержать следующие данные:

* Название программного обеспечения;
* Версия программного обеспечения;
* Дата установки обновления;
* Описание изменений;

### ОПС.1. ****Управление запуском (обращениями) компонентов программного обеспечения, в том числе определение запускаемых компонентов, настройка параметров запуска компонентов, контроль за запуском компонентов программного обеспечения****

Безопасность является критически важным аспектом любого проекта, поэтому разработчики должны следовать базовым требованиям для обеспечения безопасности приложений. Ниже приведены основные требования к разработчикам по безопасной разработке.

**Требования:**

1. Необходимо соблюдать принцип наименьшего доступа, чтобы уменьшить риски нарушения безопасности. Разработчики должны иметь доступ только к тем ресурсам, которые им необходимы для выполнения своих задач.
2. Разработчики должны использовать только проверенные и надежные библиотеки и фреймворки для создания приложений.
3. Необходимо обеспечить безопасность хранилищ данных. Разработчики должны использовать только надежные методы шифрования данных, чтобы защитить конфиденциальность пользователей.
4. Разработчики должны проверять все входные данные, включая данные, получаемые от пользователей, а также данные, получаемые из сторонних источников. Это позволит избежать уязвимостей, связанных с инъекциями.
5. Необходимо обеспечить безопасность приложения на всех этапах его жизненного цикла, включая проектирование, разработку, тестирование и эксплуатацию. Разработчики должны уделять особое внимание безопасности, чтобы избежать уязвимостей в приложении.
6. Разработчики в процессе разработки приложения, должны регулярно обновлять все компоненты приложения, включая библиотеки и другие программные компоненты. Обновление позволит исправить уязвимости, которые могут быть использованы злоумышленниками.
7. Необходимо обеспечить безопасность приложения на всех уровнях, включая серверную и клиентскую части. Разработчики должны уделять особое внимание безопасности, чтобы защитить приложение от всех видов угроз.
8. Разработчики должны учитывать возможность атак при проектировании приложения и предусматривать меры по защите от них.
9. Необходимо обеспечить безопасность передачи данных между клиентом и сервером.
10. Разработчики должны уметь обнаруживать уязвимости в приложениях и знать, как их устранять.
11. Необходимо обеспечить защиту от вредоносного кода, такого как вирусы, трояны и другие вредоносные программы.
12. Разработчики должны уметь реагировать на инциденты безопасности и быстро устранять уязвимости. Для этого нужно иметь четкие процедуры реагирования на инциденты безопасности и готовность к быстрому устранению проблем.

### 

### ОДТ.4\_ОДТ.5. Периодическое резервное копирование персональных данных на резервные машинные носители персональных данных

**Основные требования**

1. Система должна иметь план резервного копирования и восстановления данных. Это позволит минимизировать потерю данных и быстро восстановить их работоспособность в случае их повреждения.
2. План резервного копирования и восстановления данных должен регулярно проверяться и обновляться. Это необходимо для того, чтобы план был актуальным и соответствовал текущим потребностям проекта.
3. Контроль целостности данных должен производиться регулярно и автоматически. Это позволит быстро выявить ошибки в данных и принять меры по их исправлению.
4. Резервные копии должны храниться в надежном месте и регулярно проверяться на целостность. Это необходимо для того, чтобы в случае повреждения основных данных была возможность быстрого восстановления из резервных копий.
5. План резервного копирования и восстановления данных должен включать следующие процедуры и рекомендации:

* Определение критических данных и приоритетов их восстановления. Это позволит определить, какие данные необходимо восстанавливать в первую очередь и какие могут быть восстановлены во вторую очередь.
* Определение периодичности резервного копирования и места их хранения. Это позволит определить, как часто необходимо создавать резервные копии и где их необходимо хранить для обеспечения их сохранности.
* Определение процедур восстановления данных и проверки их целостности. Это позволит быстро восстановить работоспособность данных в случае их повреждения и проверить их целостность после восстановления.

1. План резервного копирования и восстановления данных должен быть доступен для всех участников проекта. Это позволит всем участникам проекта знать, какие данные являются критическими и как их восстановить в случае их повреждения.
2. Контроль целостности данных должен производиться с помощью специализированных программных решений. Это позволит автоматически выявлять ошибки в данных и принимать меры по их исправлению.
3. Резервные копии должны храниться в надежном месте, защищенном от несанкционированного доступа. Это позволит обеспечить сохранность резервных копий и исключить возможность их утраты.
4. Резервные копии должны регулярно проверяться на целостность и актуальность. Это позволит быстро выявлять ошибки в резервных копиях и принимать меры по их исправлению.

### ОДТ.1\_ОДТ.2\_ОДТ.3. Использование отказоустойчивых технических средств

**Требования**:

1. Дублирование оборудования:
   * Система должна иметь механизм мониторинга работоспособности каждого экземпляра оборудования.
   * В случае обнаружения отказа оборудования, система автоматически переключается на другой экземпляр.
2. Использование резервных каналов связи:
   * Система должна иметь механизм мониторинга работоспособности каждого канала связи.
   * В случае обнаружения отказа канала связи, система автоматически переключается на другой канал.
3. Резервное копирование данных:
   * Система должна иметь механизм мониторинга работоспособности системы резервного копирования.
   * В случае обнаружения отказа системы резервного копирования, ответственный инженер немедленно уведомляет о проблеме и начинает процесс восстановления системы.
4. Использование кластерных систем:
   * Система должна иметь механизм мониторинга работоспособности каждого узла кластера.
   * В случае обнаружения отказа узла, система автоматически переключается на другой узел.

### ИНЦ.3 / ИНЦ.4 / ИНЦ.5 / ИНЦ.6. Своевременное информирование лиц, ответственных за выявление инцидентов и реагирование на них, о возникновении инцидентов в информационной системе пользователями и администраторами

1. Архитектура системы
   * Использование защищенных протоколов
   * Разделение функций на отдельные серверы
   * Ограничение доступа к сервисам с помощью брандмауэра
   * Шифрование данных на всех уровнях
2. Мониторинг и обнаружение инцидентов
   * Установка средств мониторинга уязвимостей и обнаружения вторжений
   * Регулярное сканирование на наличие уязвимостей и слабых мест
   * Настройка системы регистрации событий для быстрого обнаружения инцидентов
   * Разработка системы оповещения для быстрого реагирования на инциденты
3. Резервное копирование и восстановление данных
   * Регулярное резервное копирование данных
   * Хранение резервных копий в безопасном месте
   * Тестирование процедуры восстановления данных
   * Разработка плана действий в случае критических потерь данных
   1. Принятие мер по устранению последствий

* Разработка четкой процедуры реагирования на инциденты
* Определение ответственных лиц и их контактных данных
* Регулярное обновление процедуры и контактных данных
* Тестирование процедуры реагирования на инциденты

1. Принятие мер по предотвращению повторного возникновения инцидентов

* Анализ причин инцидента с целью выявления слабых мест в системе
* Разработка плана действий по устранению обнаруженных слабых мест
* Регулярное обновление и тестирование системы защиты для предотвращения повторного возникновения инцидентов

### ИНЦ.2. Обнаружение, идентификация и регистрация инцидентов

**DDos атака**

* Мониторинг сетевой активности для обнаружения аномального трафика
* Блокировка IP-адресов, с которых идет атака
* Увеличение пропускной способности сети и серверов
* Связь с интернет-провайдером для обнаружения и блокировки источников атаки
* Оповещение службы безопасности и правоохранительных органов при необходимости

**Подмена сайта**

* Отключение сервера, на котором находится подмененный сайт
* Копирование логов для дальнейшего анализа
* Проверка целостности файлов и баз данных на сервере
* Восстановление сайта из резервной копии
* Изменение паролей доступа к серверу и сайту
* Анализ обнаруженных уязвимостей, которые могли привести к инциденту

**Несанкционированный доступ к интерфейсу управления**

* Блокировка доступа к управляющему интерфейсу
* Анализ логов аутентификации для выявления источника атаки
* Изменение паролей доступа к управляющему интерфейсу и аккаунтам пользователей
* Проверка логов на предмет действий злоумышленника
* Изменение параметров безопасности сервера и интерфейса управления

**Обнаружение утечки административных учетных данных, ключа или секрета**

* Блокировка доступа к системе с использованием скомпрометированных данных
* Изменение паролей и ключей доступа к системе
* Анализ логов аутентификации на предмет выявления источника утечки
* Изменение параметров безопасности, связанных с аутентификацией, идентификацией и авторизацией

**Обнаружение утечки пользовательских данных**

* Блокировка доступа к скомпрометированным данным
* Изменение паролей доступа пользователей к системе
* Оповещение пользователей о возможной утечке и рекомендации по смене паролей
* Анализ логов на предмет выявления источника утечки
* Изменение параметров безопасности, связанных с хранением и обработкой пользовательских данных

### ИАФ.5 (скрытие пароля)

Для обеспечения безопасности данных важно, чтобы пароль не был виден при вводе. Для этого необходимо соблюдать следующий регламент:

1. При вводе пароля необходимо использовать поле ввода типа "password". При вводе пароль он будет маскироваться.
2. При вводе пароля на общедоступных компьютерах и устройствах следует убедиться, что никто не может наблюдать за процессом ввода пароля.
3. Пароль не должен сохраняться в открытом виде в истории браузера или на устройстве.

### ИАФ.4\_УПД.6\_АНЗ.5 (парольная политика)

**Требования к паролю**

1. Минимальная длина пароля должна составлять не менее 6 символов.
2. Алфавит пароля не должен быть менее 60 символов, и должен включать в себя символы различных регистров, цифры и специальные символы.
3. Пользователи не должны использовать пароли, которые были использованы ранее.

**Правила смены пароля**

1. Максимальный срок действия пароля по умолчанию составляет 120 дней, но может быть изменён админимтратором. После истечения этого срока пароль должен быть изменен.
2. Минимальный срок действия пароля составляет 1 неделю.

**Правила блокировки учетной записи**

1. При количестве неудачных попыток ввода пароля от 3 до 10, учетная запись пользователя блокируется на 5-30 минут. При этом пользователю будет запрещен доступ к информационным ресурсам компании.
2. Если пользователь не может войти в систему после блокировки, он должен связаться с администратором для разблокировки учетной записи.

### ИАФ.3. Управление идентификаторами, в том числе создание, присвоение, уничтожение идентификаторов

**Требования по созданию и присвоению:**

1. Создаваемый идентификатор должен быть уникальным и не назначенным другому пользователю. В качестве идентификатора выступает адрес электронной почты;
2. Адрес электронной почты, используемый в качестве идентификатора пользователя, должен принадлежать пользователю;
3. Для токенов SSO идентификатор должен создаваться с использованием адреса электронной почты пользователя.
4. Идентификатора должен быть недоступен для повторного использования в течении не менее одного года;
5. Идентификатор должен быть блокирован через период неиспользования равным не более 90 дней;
6. Идентификатор пользователя должен быть утвержден отделом ИТ перед использованием, чтобы гарантировать соблюдение политик безопасности и конфиденциальности.

**Требования по уничтожению идентификатора пользователя:**

1. Полностью удалять идентификатор пользователя не рекомендуется, потому что в связи с возможностью поступления запросов от государственных органов, идентификаторы может потребоваться предоставить;
2. Вместо полного удаления, идентификатор пользователя помечается как неактивный или заблокированный, чтобы предотвратить его дальнейшее использование;

### ИАФ.1\_ИАФ.2\_ИАФ.6\_ЗСВ.1. Идентификация и аутентификация пользователей, являющихся работниками оператора

Идентификация и аутентификация - это процессы, которые обеспечивают безопасность доступа к информации и ресурсам. Идентификация - это процесс определения личности пользователя на основе уникального идентификатора. Аутентификация - это процесс проверки подлинности пользователя на основе учетных данных, таких как логин и пароль. Эти процессы важны для защиты информации и ресурсов от несанкционированного доступа и обеспечивают конфиденциальность и целостность данных.

Идентификация и аутентификация - это два разных процесса, которые обеспечивают безопасность доступа к информации и ресурсам.

**Идентификация** - это процесс определения личности пользователя на основе уникального идентификатора, например, имени пользователя или электронной почты. Этот процесс позволяет системе установить, кто запросил доступ к информации или ресурсам.

**Аутентификация** - это процесс проверки подлинности пользователя на основе учетных данных, таких как логин и пароль или токен. Этот процесс позволяет системе проверить, является ли пользователь тем, за кого себя выдаёт, и имеет ли он право на доступ к запрашиваемой информации или ресурсам.

Идентификация и аутентификация важны для защиты информации и ресурсов от несанкционированного доступа и обеспечивают конфиденциальность и целостность данных. Они помогают гарантировать, что только авторизованные пользователи получают доступ к информации, и что эта информация не попадает в руки злоумышленников.

Важно отметить, что идентификация и аутентификация обычно выполняются вместе, и часто их называют идентификацией и аутентификацией (ИАФ).

При аутентификации и идентификации пользователей в информационной системе используется аутентификация по логину и паролю или с помощью SSO Leader-ID. Существуют два типа пользователей:

* пользователь (все пользователи в соответствии с ролевой моделью);
* администратор (ограниченное число пользователей, обладающих расширенными правами относительно пользователей)

Информационная системы поддерживает функционал регистрации и аудита (журналирование) действий пользователей в системе.

**Описание процесса идентификации**

1. Для идентификации пользователей в системе используется уникальный идентификатор, назначенный при регистрации;
2. Многофакторная система аутентификации должна включать в себя следующие компоненты:

* Система аутентификации по логину и паролю (учётной записи Active Directory);

или

* Токены SSO (Leader-ID);

1. Система проверяет корректность идентификатора;
2. Если идентификатор верен, пользователь может продолжить процесс аутентификации.
3. Пользователю доступна только та информация, которая относится к его роли в системе.

**Идентификация и аутентификация пользователей, не являющихся работниками оператора**

**Требования:**

Внешние пользователи, это пользователи, которые не являются сотрудниками Агенства, но получили доступ в системы Агенства для выполнения каких-либо задач. Идентификация и аутентификация происходит в стандртном порядке, за исключением того, что:

1. **Ограничение доступа**. После успешной аутентификации внешний пользователь получает доступ только к ограниченному набору сегментов системы, которые ему разрешены. Для этого могут использоваться различные методы, такие как ограничение прав доступа, фильтрация контента и т.д.

### ЗТС.4. Размещение устройств вывода (отображения) информации, исключающее ее несанкционированный просмотр

**Требования к функциональности**

1.1. Выключение экранов

1.1.1. Система должна иметь возможность выключать экраны автоматически через определенное время бездействия пользователя.

1.1.2. Время бездействия должно быть настраиваемым параметром.

1.1.3. Экраны должны выключаться полностью, а не переходить в режим ожидания.

1.2. Включение экранов

1.2.1. Включение экранов должно быть возможно только после ввода логина и пароля пользователя.

1.2.2. После ввода логина и пароля пользователь должен иметь доступ только к своим данным.

1.2.3. Время нахождения пользователя в системе должно быть ограничено, чтобы предотвратить несанкционированный доступ к данным.

### ЗТС.3. Контроль и управление физическим доступом к техническим средствам, средствам защиты информации, средствам обеспечения функционирования, а также в помещения и сооружения, в которых они установлены, исключающие несанкционированный физический доступ к средствам обработки информации, средствам защиты информации и средствам обеспечения функционирования информационной системы, в помещения и сооружения, в которых они установлены

**Требования**

1. Контроль доступа
   * Контроль доступа на основе ролей
   * Контроль доступа на основе полномочий
2. Безопасность сетевого трафика
   * Использование протоколов шифрования
   * Ограничение доступа к сети только для авторизованных пользователей
3. Мониторинг
   * Регулярный мониторинг состояния системы
   * Мониторинг доступа к системе
4. Физический контроль
   * Установка контрольных точек на входах в помещения
   * Использование биометрических технологий для идентификации пользователей
5. Резервное копирование
   * Регулярное создание резервных копий данных
   * Хранение резервных копий в безопасном месте

### ЗСВ.10. Разбиение виртуальной инфраструктуры на сегменты (сегментирование виртуальной инфраструктуры) для обработки персональных данных отдельным пользователем и (или) группой пользователей

**Требования:**

1. Все персональные данные хранятся в отдельных сегментах виртуальной инфраструктуры.
2. Разбиение на сегменты может быть выполнено на основе критериев, определенных компанией и соответствующих требованиям законодательства о защите персональных данных.
3. Может быть реализована система контроля доступа к персональным данным в каждом сегменте.
4. Для каждого сегмента могут быть определены права доступа к персональным данным на основе ролей и задач пользователей.
5. Могут быть установлены механизмы мониторинга и аудита доступа к персональным данным в каждом сегменте.
6. Все данные, хранящиеся в сегментах, должны быть защищены с использованием современных методов шифрования данных.
7. Должна быть реализована система резервного копирования данных для каждого сегмента.

### ЗСВ.7. Контроль целостности виртуальной инфраструктуры и ее конфигураций

**Технические требования для контроля целостности виртуальной инфраструктуры**

1. Контроль цифровых подписей
   * Проверка подлинности файлов и программного обеспечения
   * Использование алгоритмов шифрования для защиты цифровых подписей
2. Сравнение хеш-сумм
   * Создание хеш-сумм для файлов и программного обеспечения
   * Сравнение хеш-сумм для выявления изменений в файлах и программном обеспечении
3. Мониторинг событий в системе
   * Отслеживание действий пользователей и системных процессов
   * Обнаружение необычных активностей, которые могут указывать на наличие угроз
4. Регулярное обновление программного обеспечения и системных файлов
   * Обновление для исправления уязвимостей и устранения ошибок
   * Обновление для внесения изменений в конфигурацию системы
5. Ограничение доступа к системным файлам и программному обеспечению
   * Установка прав доступа на основе ролей и обязанностей пользователей
   * Ограничение возможности изменения системных файлов и программного обеспечения

### ЗСВ.6.Управление перемещением виртуальных машин (контейнеров) и обрабатываемых на них данных

**Технические требования**

1. Требования к системе управления

* Система управления должна обеспечивать гибкость и масштабируемость виртуальных машин и контейнеров.
  + Система должна позволять легко добавлять и удалять виртуальные машины.
  + Система должна поддерживать автоматическое масштабирование в зависимости от нагрузки.
  + Система должна поддерживать миграцию виртуальных машин между физическими хостами без прерывания работы приложений.
* Система управления должна обеспечивать высокую доступность приложений.
  + Система должна поддерживать кластеризацию виртуальных машин.
  + Система должна обнаруживать и устранять отказы автоматически.
  + Система должна поддерживать резервное копирование данных.

2. Требования к безопасности данных

* Система управления должна обеспечивать безопасность данных.
  + Система должна поддерживать шифрование данных в покое и в движении.
  + Система должна обеспечивать контроль доступа к данным.
  + Система должна поддерживать аудит доступа к данным.
* Система управления должна обеспечивать безопасность приложений.
  + Система должна обеспечивать изоляцию приложений друг от друга.
  + Система должна обеспечивать обнаружение и защиту от вредоносных атак.
  + Система должна поддерживать контроль целостности приложений.

3. Требования к производительности

* Система управления должна обеспечивать высокую производительность.
  + Система должна обеспечивать оптимальное распределение ресурсов между виртуальными машинами.
  + Система должна обеспечивать минимальное время отклика приложений.
  + Система должна поддерживать мониторинг производительности и оптимизацию расходов ресурсов.

4. Требования к совместимости

* Система управления должна совместима с различными операционными системами и приложениями.
  + Система должна поддерживать виртуализацию как для Linux, так и для Windows.
  + Система должна поддерживать различные типы приложений, включая веб-сервера, базы данных и другие.

5. Требования к управлению

* Система управления должна обеспечивать удобный интерфейс для управления виртуальными машинами и контейнерами.
  + Система должна поддерживать графический интерфейс пользователя.
  + Система должна поддерживать командную строку.
  + Система должна предоставлять API для автоматизации управления.

6. Требования к сопровождению

* Система управления должна обеспечивать удобные инструменты для сопровождения и обслуживания.
  + Система должна поддерживать мониторинг состояния системы.
  + Система должна предоставлять логи и отчеты об использовании ресурсов.
  + Система должна обеспечивать удобный доступ к документации и руководствам пользователя.

### ЗСВ.5. ****Доверенная загрузка серверов виртуализации, виртуальной машины (контейнера), серверов управления виртуализацией****

Для реализации доверенной загрузки на серверах виртуализации необходимо использовать следующие технологии:

* Trusted Platform Module (TPM) версии 2.0 или выше
* Unified Extensible Firmware Interface (UEFI) версии 2.6 или выше
* Операционная система, поддерживающая UEFI Boot Manager

Кроме того, необходимо выполнить следующие шаги:

1. Включить функцию доверенной загрузки в BIOS или UEFI на серверах виртуализации.
2. Установить и настроить TPM на серверах виртуализации.
3. Настроить UEFI Boot Manager для загрузки только из доверенных и аутентифицированных компонентов загрузки.
4. Подготовить и настроить операционную систему для поддержки доверенной загрузки.
5. Убедиться, что все установленные драйверы и приложения также поддерживают доверенную загрузку.

### ЗСВ.4. Управление (фильтрация, маршрутизация, контроль соединения, однонаправленная передача) потоками информации между компонентами виртуальной инфраструктуры, а также по периметру виртуальной инфраструктуры

**Фильтрация потоков информации**

1. Установка правил фильтрации:
   * Определение списка источников данных
   * Определение списка получателей данных
   * Определение типов данных, которые необходимо фильтровать
   * Определение действий, которые должны быть выполнены при обнаружении запрещенных данных
2. Мониторинг фильтрации:
   * Определение частоты мониторинга
   * Определение методов уведомления о нарушениях фильтрации
   * Определение методов анализа и логирования результатов фильтрации

**Маршрутизация потоков информации**

1. Установка правил маршрутизации:
   * Определение списка источников данных
   * Определение списка получателей данных
   * Определение метода маршрутизации (например, основанный на IP-адресах или на содержании данных)
   * Определение действий, которые должны быть выполнены при невозможности маршрутизации
2. Мониторинг маршрутизации:
   * Определение частоты мониторинга
   * Определение методов уведомления о нарушениях маршрутизации
   * Определение методов анализа и логирования результатов маршрутизации

**Контроль соединения**

1. Установка правил контроля соединения:
   * Определение списка источников данных
   * Определение списка получателей данных
   * Определение метода контроля соединения (например, основанный на TCP или UDP)
   * Определение действий, которые должны быть выполнены при обнаружении нарушений соединения
2. Мониторинг контроля соединения:
   * Определение частоты мониторинга
   * Определение методов уведомления о нарушениях контроля соединения
   * Определение методов анализа и логирования результатов контроля соединения

**Однонаправленная передача**

1. Установка правил однонаправленной передачи:
   * Определение списка источников данных
   * Определение списка получателей данных
   * Определение метода передачи данных (например, основанный на потоке или на пакетах)
   * Определение действий, которые должны быть выполнены при обнаружении нарушений передачи
2. Мониторинг однонаправленной передачи:
   * Определение частоты мониторинга
   * Определение методов уведомления о нарушениях передачи
   * Определение методов анализа и логирования результатов передачи

**Периметр виртуальной инфраструктуры**

1. Определение периметра виртуальной инфраструктуры:
   * Определение списка компонентов виртуальной инфраструктуры
   * Определение списка сетевых узлов, связанных с виртуальной инфраструктурой
   * Определение списка узлов, которые не должны иметь доступ к виртуальной инфраструктуре
2. Мониторинг периметра виртуальной инфраструктуры:
   * Определение частоты мониторинга
   * Определение методов уведомления о нарушениях периметра
   * Определение методов анализа и логирования результатов мониторинга периметра

### ЗНИ.8. Уничтожение (стирание) или обезличивание персональных данных на машинных носителях при их передаче между пользователями, в сторонние организации для ремонта или утилизации, а также контроль уничтожения (стирания) или обезличивания.

**Общие требования:**

1.1 Сбор персональных данных в информационной системе является необходимым для обеспечения ее функционирования и предоставления услуг пользователям;

1.2 Кроме того, сбор персональных данных может быть необходим для выполнения требований законодательства в области защиты персональных данных. Законодательство устанавливает требования к сбору, хранению и обработке персональных данных, чтобы обеспечить их конфиденциальность и защиту от несанкционированного доступа;

1.3 Система должна обеспечивать возможность удаления персональных данных пользователя по его запросу или по истечении срока их хранения. Это поможет предотвратить утечки данных и защитить конфиденциальность пользователей.

**Требования:**

1. Аутентификация пользователя при входе в систему. Для того, чтобы пользователь мог получить доступ к системе, ему необходимо предоставить свои персональные данные, такие как логин и пароль.
2. Сохранение настроек пользователя. Информационная система может сохранять настройки пользователя, чтобы обеспечить ему удобство при использовании системы в будущем.
3. Выполнение требований законодательства в области защиты персональных данных. Законодательство устанавливает требования к сбору, хранению и обработке персональных данных, чтобы обеспечить их конфиденциальность и защиту от несанкционированного доступа.
4. Обеспечение функционирования информационной системы. Сбор персональных данных является необходимым условием для обеспечения функционирования информационной системы.
5. Предоставление пользователю доступа к функциональности системы. Для того, чтобы пользователь мог использовать функции информационной системы, ему необходимо предоставить свои персональные данные.

### ЗНИ.2. ****Управление доступом к машинным носителям информации****

**Требования:**

1.1 Агентство формирует список белых IP-адресов, с которых возможна выгрузка персональных данных. В список могут быть включены только те IP-адреса, которые Агентство считает безопасными и доверенными. Список белых IP-адресов не является статичным и может изменяться в зависимости от потребностей организации;

1.2 Добавление новых IP-адресов в список должно происходить только после проверки их безопасности и доверенности;

1.3 Удаление IP-адресов из списка также может происходить только после проверки. Это может быть необходимо, например, при обнаружении нарушений безопасности;

1.4 Доступ к списку белых IP-адресов должен быть ограничен и контролируем только ответственным за управление доступом. Это позволит предотвратить возможность несанкционированного изменения списка;

1.5 Изменения в списке белых IP-адресов должны фиксироваться в журнале доступа. Это позволит отслеживать, кто и когда вносил изменения в список;

1.6 Формирование списка белых IP-адресов должно сопровождаться постоянным мониторингом безопасности сети организации.

### ЗИС.20. Защита беспроводных соединений, применяемых в информационной системе

1. Аутентификация пользователей:
   * Система может обеспечивать аутентификацию пользователей перед подключением к беспроводной сети.
   * Аутентификация может осуществляется с использованием безопасных протоколов, поддерживающих шифрование данных.
   * Система может имеет возможность ограничивать доступ к беспроводной сети только для авторизованных пользователей.
2. Контроль доступа:
   * Система может обеспечивать контроль доступа к ресурсам сети на основе уровня полномочий пользователей.
   * Система может иметь возможность ограничивать доступ к ресурсам сети для различных категорий пользователей.
   * Система может обеспечивать контроль доступа к сети внешних устройств.
3. Шифрование данных:
   * Система может обеспечивать шифрование данных, передаваемых по беспроводной сети.
   * Система может иметь возможность обеспечивать защиту данных на всех уровнях передачи.
4. Защита от внешних угроз:
   * Система может обеспечивать защиту от внешних угроз, таких как взломы, атаки на сетевые протоколы и т.д.
   * Система может иметь возможность обнаруживать и предотвращать атаки на сеть.
   * Система может иметь возможность блокировать доступ к сети для потенциально опасных устройств.
5. Мониторинг и анализ:
   * Система может иметь возможность мониторинга и анализа сетевой активности.
   * Система может иметь возможность обнаруживать аномальную сетевую активность и предупреждать об этом администраторов сети.

### ЗИС.17. Разбиение информационной системы на сегменты (сегментирование информационной системы) и обеспечение защиты периметров сегментов информационной системы

**Технические требования:**

1. Система сегментации должна обеспечивать:
   * Разделение информационной системы на сегменты на основе логических группировок
   * Изоляцию данных и приложений в каждом сегменте
   * Ограничения доступа к данным и приложениям сегментов на основе ролей и прав доступа
2. Система защиты периметров сегментов должна обеспечивать:
   * Автоматическое обнаружение и блокирование атак на периметр сегмента
   * Контроль целостности данных на периметре сегмента
   * Доступ к периметру сегмента только посредством аутентификации и авторизации
3. Система обеспечения безопасности информационной системы должна обеспечивать:
   * Шифрование данных во всех сегментах
   * Регулярное обновление программного обеспечения и компонентов системы
   * Регулярный аудит безопасности информационной системы
   * Резервное копирование данных и наличие планов восстановления после сбоев

### ЗИС.16. ****Выявление, анализ и блокирование в информационной системе скрытых каналов передачи информации в обход реализованных мер или внутри разрешенных сетевых протоколов****

**1. Мониторинг сетевой активности**

* Необходимо использовать специальные инструменты для мониторинга сетевой активности
* Инструменты должны анализировать трафик и определять наличие скрытых каналов передачи информации
* Мониторинг должен производиться в реальном времени
* Инструменты мониторинга должны иметь функцию оповещения в случае обнаружения подозрительной активности

**2. Контроль доступа**

* Необходимо использовать методы контроля доступа для управления доступом к информации и ресурсам системы
* Методы контроля доступа должны включать авторизацию и аутентификацию пользователей
* Методы контроля доступа должны иметь возможность настройки уровней доступа для разных пользователей
* Методы контроля доступа должны включать механизмы аудита доступа

**3. Шифрование**

* Необходимо использовать методы шифрования для защиты передаваемых данных от несанкционированного доступа
* Методы шифрования должны обеспечивать высокую степень защиты данных
* Шифрование должно производиться на всех этапах передачи данных
* Должны использоваться современные алгоритмы шифрования

**4. Ограничение доступа к системе**

* Необходимо ограничить доступ к информационной системе только для авторизованных пользователей
* Для доступа к системе необходимо использовать пароли или другие методы аутентификации
* Должны использоваться средства многофакторной аутентификации
* Необходимо ограничить доступ к системе с помощью механизмов брандмауэра и других средств безопасности

**5. Регулярное обновление системы**

* Необходимо регулярно обновлять систему защиты информационной безопасности
* Обновления должны производиться в соответствии с появляющимися угрозами и новыми технологиями
* Необходимо обеспечить актуальность базы угроз и вирусных баз данных
* Обновления должны производиться без прерывания работы информационной системы

### ЗИС.15. ****Защита архивных файлов, параметров настройки средств защиты информации и программного обеспечения и иных данных, не подлежащих изменению в процессе обработки персональных данных****

**Хранение персональных данных**

* ПДн пользователей не должны храниться в открытом виде
* Для каждой записи ПДн пользователя необходимо реализовать криптографическое преобразование с использованием уникальной величины
* Необходимо использовать эффективные методы шифрования и аутентификации, чтобы обеспечить конфиденциальность данных и защитить их от несанкционированного доступа
* Ключи шифрования должны храниться в надежном месте и быть доступны только авторизованным пользователям

**Защита данных**

* Необходимо регулярно обновлять программные средства защиты
* Программное обеспечение должно включать механизмы обнаружения и предотвращения несанкционированного доступа к данным
* Должна быть реализована система аудита, позволяющая отслеживать доступ к данным и действия пользователей
* Необходимо проводить тестирование программных средств защиты и оценивать их эффективность

**Резервное копирование данных**

* Необходимо регулярно создавать резервные копии данных
* Резервные копии должны храниться в отдельном месте и быть защищены паролем
* Для восстановления данных необходимо иметь инструкции и процедуры

Резервные копии должны быть проверены на целостность и доступность.

### ЗИС.11. ****Обеспечение подлинности сетевых соединений (сеансов взаимодействия), в том числе для защиты от подмены сетевых устройств и сервисов****

**1. Обеспечение защиты сетевых соединений**

* Поддержка аутентификации узлов сети по различным методам, таким как парольная аутентификация, аутентификация по сертификату и другие.
* Использование шифрования для защиты данных, передаваемых по сети, от несанкционированного доступа.
* Работа с протоколами, обеспечивающими безопасность сетевых соединений, такими как SSL/TLS и другие.
* Использование контроля доступа для управления правами доступа к сетевым ресурсам и определения, какие узлы сети имеют доступ к каким данным и сервисам.

**2. Обеспечение стабильности и производительности сети**

* Поддержка высокоскоростных сетевых соединений для обеспечения высокой производительности.
* Возможность масштабирования сети для поддержки роста количества узлов и объема передаваемых данных.
* Поддержка гибридной сетевой архитектуры для обеспечения балансировки нагрузки и повышения стабильности сети.
* Работа с протоколами, обеспечивающими оптимизацию и ускорение передачи данных, такими как TCP Fast Open и другие.

**3. Обеспечение высокой доступности сетевых ресурсов**

* Использование технологий и методов, обеспечивающих отказоустойчивость и непрерывность работы сетевых ресурсов.
* Работа со средствами мониторинга и управления сетью для быстрого обнаружения и устранения проблем.
* Использование резервирования каналов и узлов для обеспечения доступности сетевых ресурсов при возникновении сбоев.
* Поддержка механизмов автоматического восстановления после сбоев и обновления сетевых ресурсов без остановки работы сети.

**4. Обеспечение безопасности сетевой инфраструктуры**

* Использование средств мониторинга и анализа сетевого трафика для обнаружения и предотвращения атак.
* Поддержка механизмов контроля и защиты от вредоносных программ.
* Работа с протоколами, обеспечивающими фильтрацию и блокировку нежелательного трафика.
* Поддержка механизмов обнаружения и реагирования на инциденты безопасности сети.

**5. Обеспечение совместимости и расширяемости сетевой инфраструктуры**

* Поддержка работы с различными сетевыми устройствами и технологиями.
* Возможность интеграции с различными средствами управления и мониторинга сети.
* Поддержка гибкой настройки и конфигурации сетевых устройств.
* Возможность расширения и модернизации сетевой инфраструктуры для поддержки новых технологий и возможностей.

### ЗИС.10. Подтверждение происхождения источника информации, получаемой в процессе определения сетевых адресов по сетевым именам или определения сетевых имен по сетевым адресам

1. Безопасность
   * Защита от подмены данных
   * Проверка подписей DNSSEC
   * Проверка действительности SSL/TLS сертификатов
   * Аутентификация и авторизация
2. Производительность
   * Минимальное время ответа на запросы
   * Поддержка высоких нагрузок
   * Резервирование серверов
   * Оптимизация маршрутизации
3. Надежность
   * Резервирование серверов
   * Резервное копирование данных
   * Мониторинг работы системы
   * Быстрое восстановление после сбоев
4. Совместимость
   * Поддержка различных протоколов и форматов данных
   * Совместимость с различными операционными системами
   * Совместимость с различными программными и аппаратными средствами

Возможность интеграции с другими системами.

### ЗИС.7. Контроль санкционированного и исключение несанкционированного использования технологий мобильного кода, в том числе регистрация событий, связанных с использованием технологий мобильного кода, их анализ и реагирование на нарушения, связанные с использованием технологий мобильного кода

1. Мониторинг использования технологий мобильного кода
   * Определение типов используемых технологий мобильного кода
   * Регистрация всех событий, связанных с использованием технологий мобильного кода
   * Обнаружение утечек данных и других нарушений безопасности
   * Автоматическое оповещение о нарушениях безопасности
2. Оценка уязвимостей и устранение их
   * Анализ уязвимостей в приложениях и настройка механизмов защиты
   * Использование современных инструментов для обнаружения уязвимостей
   * Регулярное проведение аудитов безопасности
   * Быстрое устранение обнаруженных уязвимостей
3. Мониторинг сетевого трафика
   * Регистрация всего сетевого трафика, связанного с мобильными устройствами
   * Обнаружение аномального сетевого трафика
   * Анализ сетевого трафика на наличие угроз безопасности
   * Предотвращение несанкционированного доступа к сети
4. Анализ и управление учетными записями
   * Управление доступом к учетным записям и паролям
   * Мониторинг использования учетных записей
   * Автоматическое отключение неактивных учетных записей
   * Ограничение доступа к административным функциям
5. Резервное копирование и восстановление
   * Регулярное резервное копирование данных
   * Периодическая проверка копий на целостность и возможность восстановления
   * Разработка планов восстановления в случае нарушения безопасности
   * Тестирование планов восстановления на регулярной основе

### ЗИС.6. ****Передача и контроль целостности атрибутов безопасности (меток безопасности), связанных с персональными данными, при обмене ими с иными информационными системами****

**Шифрование данных**

* Использование алгоритмов шифрования, обеспечивающих надежную защиту данных.
* Использование достаточно длинных ключей шифрования для обеспечения надежности защиты.
* Обеспечение безопасности ключей шифрования в процессе их хранения и передачи.

**Аутентификация**

* Использование надежных методов аутентификации, включая многофакторную аутентификацию.
* Обеспечение безопасности паролей и идентификационных данных пользователей.
* Использование протоколов аутентификации, обеспечивающих защиту от атак типа man-in-the-middle.

**Цифровые подписи**

* Использование надежных алгоритмов цифровой подписи для защиты данных.
* Обеспечение безопасности ключей цифровой подписи в процессе их хранения и передачи.
* Использование протоколов цифровой подписи, обеспечивающих защиту от атак типа replay.

**Защита данных в процессе хранения и обработки**

* Использование средств защиты данных, таких как шифрование и многофакторная аутентификация, для защиты данных при их хранении.
* Использование средств защиты данных, таких как защита от DDoS-атак и противодействие вредоносным программам, для защиты данных при их обработке.
* Обеспечение безопасности доступа к базам данных и файловым системам, содержащим персональные данные пользователей.

### ЗИС.4. Обеспечение доверенных канала, маршрута между администратором, пользователем и средствами защиты информации (функциями безопасности средств защиты информации)

1. Каналы связи
   * Установление доверенных каналов между администратором, пользователем и средствами защиты информации
   * Использование протоколов шифрования для защиты передаваемых данных
2. Аутентификация и авторизация
   * Использование сложных паролей
   * Регулярная смена паролей
   * Использование двухфакторной аутентификации
3. Защита от внешних угроз
   * Установка средств защиты от вирусов и других видов вредоносного ПО
   * Обновление средств защиты информации
4. Защита от внутренних угроз
   * Ограничение доступа к конфиденциальным данным только необходимым сотрудникам
5. Контроль доступа к данным
   * Установление прав доступа на основе ролей
   * Мониторинг доступа к данным и аудит действий пользователей

### ЗИС.3. Обеспечение защиты персональных данных от раскрытия, модификации и навязывания (ввода ложной информации) при ее передаче (подготовке к передаче) по каналам связи, имеющим выход за пределы контролируемой зоны, в том числе беспроводным каналам связи

**Технические требования:**

1. Общие требования:
   * ИС должна обеспечивать доступ в режиме защищенного HTTPS-соединения (протокол не ниже TLS 1.2).
   * Взаимодействие между front-end и back-end происходит через защищенное HTTPS-соединение.
   * При передаче защищаемой информации вне контролируемых зон должны применяться существующие средства криптографической защиты.
2. Шифрование:
   * Использование надежных алгоритмов шифрования для защиты передаваемых данных.
   * Использование достаточной длины ключа для шифрования.
   * Использование симметричного и асимметричного шифрования в зависимости от требований безопасности.
3. Контроль доступа:
   * Определение ролей и прав доступа для пользователей системы.
   * Авторизация пользователей перед доступом к защищаемым ресурсам.
   * Мониторинг доступа к защищаемым ресурсам и обнаружение несанкционированного доступа.
4. Проверка системы защиты:
   * Регулярное тестирование системы на наличие уязвимостей.
   * Мониторинг системы на наличие необычной активности.
   * Анализ логов и событий для выявления потенциальных угроз.
5. Обновление программного обеспечения:
   * Следить за обновлением программного обеспечения и применять последние патчи безопасности.
   * Установка только лицензионного и проверенного программного обеспечения.
   * Следить за устаревшим программным обеспечением и заменять его на актуальное.
6. Управление рисками:
   * Оценка рисков и управление ими.
   * Создание плана действий при возникновении инцидента.
   * Проведение регулярных аудитов безопасности для выявления потенциальных угроз.

### ЗИС.1. Разделение в информационной системе функций по управлению (администрированию) информационной системой, управлению (администрированию) системой защиты персональных данных, функций по обработке персональных данных и иных функций информационной системы

**Требования**

* Разделение функций по управлению информационной системой
  + Мониторинг работы системы
  + Управление доступом к информации и ресурсами системы
  + Контроль эффективности и безопасности системы
* Функции по управлению системой защиты персональных данных
  + Контроль доступа к персональным данным
  + Защита информации от несанкционированного доступа
  + Безопасность хранения информации
* Функции по обработке персональных данных
  + Сбор, хранение и обработка персональных данных
  + Защита персональных данных от несанкционированного доступа и использования
* Иные функции информационной системы
  + Поддержка пользовательского интерфейса

Техническая поддержка пользователей.

**АНЗ.4**. **Контроль состава технических средств, программного обеспечения и средств защиты информации**

**Требования:**

**Сбор информации о всех технических средствах, программном обеспечении и средствах защиты информации, используемых на предприятии.**

1. Составление полного списка всех технических средств, программного обеспечения и средств защиты информации, используемых на предприятии.
2. Получение от руководства предприятия информации о всех технических средствах, программном обеспечении и средствах защиты информации, используемых на предприятии.
3. Сбор информации о всех технических средствах, программном обеспечении и средствах защиты информации, используемых на предприятии, с помощью специального программного обеспечения для автоматического сбора информации.

**Анализ требований безопасности информации, применяемых на предприятии.**

1. Получение от руководства предприятия информации о требованиях безопасности информации, применяемых на предприятии.
2. Изучение нормативных документов, регулирующих требования безопасности информации, применяемых на предприятии.
3. Анализ требований безопасности информации, применяемых на предприятии, с помощью специальных программных средств.

**Проверка соответствия каждого технического средства, программного обеспечения и средства защиты информации требованиям по безопасности информации.**

1. Анализ каждого технического средства, программного обеспечения и средства защиты информации на предмет соответствия требованиям по безопасности информации.
2. Тестирование каждого технического средства, программного обеспечения и средства защиты информации на наличие уязвимостей.
3. Оценка рисков, связанных с использованием каждого технического средства, программного обеспечения и средства защиты информации.

**Принятие мер по устранению выявленных нарушений требований безопасности информации.**

1. Составление списка выявленных нарушений требований безопасности информации.
2. Разработка плана мероприятий по устранению выявленных нарушений требований безопасности информации.
3. Проведение мероприятий по устранению выявленных нарушений требований безопасности информации.

**Требования по контролю сроков действия сертификатов**

1. Необходимо вести учет всех сертификатов, используемых на предприятии, и контролировать сроки их действия.
2. Перед истечением срока действия сертификата необходимо провести его обновление или замену.

**Требования по исключению или восстановлению технических средств**

1. При выявлении неисправности технического средства необходимо исключить его из использования и провести его ремонт или замену.
2. В случае необходимости восстановления технического средства необходимо провести его тщательную проверку перед возвращением в эксплуатацию.

**Регистрация событий безопасности**

1. Обеспечить возможность регистрации событий безопасности, связанных с изменением состава технических средств, программного обеспечения и средств защиты информации.
2. Информировать ответственных лиц о произошедших событиях безопасности.
3. Анализировать зарегистрированные события безопасности и принимать меры по устранению выявленных нарушений безопасности информации.

**АНЗ.3 (Примеры тест-кейсов). Тест-кейсы для нагрузочного тестирования**

**Пример тест-кейса**

Номер: 001 Название: Тестирование производительности функции поиска.

Описание: Проверка производительности функции поиска при большом объеме данных.

Шаги:

1. Загрузить в программу базу данных с 1 000 000 записей.
2. Ввести запрос на поиск записи.
3. Измерить время выполнения запроса.
4. Повторить шаги 2-3 для 10 различных запросов.
5. Сравнить время выполнения запросов с требованиями производительности.

Ожидаемый результат:

* Время выполнения запросов удовлетворяет требованиям производительности.
* Нет ошибок в коде функции.

**Пример тест-кейса**

Номер: 002 Название: Тестирование производительности функции обновления данных.

Описание: Проверка производительности функции обновления данных при большом объеме данных.

Шаги:

1. Загрузить в программу базу данных с 1 000 000 записей.
2. Ввести запрос на обновление записей.
3. Измерить время выполнения запроса.
4. Повторить шаги 2-3 для 10 различных запросов.
5. Сравнить время выполнения запросов с требованиями производительности.

Ожидаемый результат:

* Время выполнения запросов удовлетворяет требованиям производительности.
* Нет ошибок в коде функции.

**Тест-кейсы для тестирования на проникновение**

**Пример тест-кейса**

Номер: 001 Название: Тестирование на проникновение веб-приложения.

Описание: Проверка на проникновение веб-приложения для определения уязвимостей и оценки уровня защиты.

Шаги:

1. Использовать сканер уязвимостей для определения уязвимых точек веб-приложения.
2. Использовать инструменты для брутфорса паролей, чтобы проверить устойчивость системы к подбору паролей.
3. Попытаться провести SQL-инъекции, чтобы проверить защиту от атак на внедрение SQL-кода.
4. Попытаться провести XSS-атаки и проверить защиту от внедрения JavaScript-кода.
5. Применить другие инструменты для тестирования на проникновение и оценить общую защищенность веб-приложения.

Ожидаемый результат:

* Найдены и устранены найденные уязвимости.
* Веб-приложение защищено от распространенных атак.

**Пример тест-кейса**

Номер: 002 Название: Тестирование на проникновение сетевого приложения.

Описание: Проверка на проникновение сетевого приложения для определения уязвимостей и оценки уровня защиты.

Шаги:

1. Использовать сканер уязвимостей для определения уязвимых точек сетевого приложения.
2. Попытаться провести атаку на переполнение буфера, чтобы проверить защиту от таких атак.
3. Попытаться провести атаки на перехват и подмену данных, чтобы проверить защиту от подобных атак.
4. Проверить защиту от DoS-атак, попытавшись перегрузить сетевое приложение.
5. Применить другие инструменты для тестирования на проникновение и оценить общую защищенность сетевого приложения.

Ожидаемый результат:

* Найдены и устранены найденные уязвимости.
* Сетевое приложение защищено от распространенных атак.

**Тест-кейсы для модульного тестирования**

**Пример тест-кейса**

Номер: 001 Название: Тестирование функции расчета суммы элементов списка.

Описание: Проверка правильности работы функции расчета суммы элементов списка.

Шаги:

1. Подготовить список из 5 элементов.
2. Передать список в функцию расчета суммы элементов.
3. Сравнить результат с ожидаемым значением.

Ожидаемый результат:

* Результат суммирования элементов списка соответствует ожидаемому значению.
* Нет ошибок в коде функции.

**Пример тест-кейса**

Номер: 002 Название: Тестирование функции поиска максимального элемента списка.

Описание: Проверка правильности работы функции поиска максимального элемента списка.

Шаги:

1. Подготовить список из 10 элементов.
2. Передать список в функцию поиска максимального элемента.
3. Сравнить результат с ожидаемым значением.

Ожидаемый результат:

* Результат поиска максимального элемента списка соответствует ожидаемому значению.
* Нет ошибок в коде функции.

**Тест-кейсы для тестирования на контроль работоспособности**

**Пример тест-кейса**

Номер: 001 Название: Тестирование на устойчивость к перегрузке сети.

Описание: Проверка устойчивости программного обеспечения к перегрузке сети.

Шаги:

1. Сгенерировать трафик сети, превышающий нормальную нагрузку.
2. Измерить время отклика системы на нагрузку.
3. Повторить шаги 1-2 для различных уровней нагрузки.
4. Сравнить время отклика системы с требованиями к работоспособности.

Ожидаемый результат:

* Система работает стабильно при нормальной и повышенной нагрузке.

**Пример тест-кейса**

Номер: 002 Название: Тестирование на устойчивость к сбоям питания.

Описание: Проверка устойчивости программного обеспечения к сбоям питания.

Шаги:

1. Имитировать сбой питания системы.
2. Проверить, что система корректно перезагружается после сбоя.
3. Повторить шаги 1-2 для различных типов сбоев.
4. Сравнить поведение системы с требованиями к работоспособности.

Ожидаемый результат:

* Система корректно перезагружается после возникновения сбоев питания.

**Пример тест-кейса**

Номер: 003 Название: Тестирование на устойчивость к ошибкам ввода-вывода.

Описание: Проверка устойчивости программного обеспечения к ошибкам ввода-вывода.

Шаги:

1. Имитировать ошибки чтения и записи на диске.
2. Проверить, что система корректно обрабатывает ошибки ввода-вывода и продолжает работу.
3. Повторить шаги 1-2 для различных типов ошибок ввода-вывода.
4. Сравнить поведение системы с требованиями к работоспособности.

Ожидаемый результат:

* Система корректно обрабатывает ошибки ввода-вывода и продолжает работу.

**Пример тест-кейса**

Номер: 004 Название: Тестирование на устойчивость к ошибкам в работе с памятью.

Описание: Проверка устойчивости программного обеспечения к ошибкам в работе с памятью.

Шаги:

1. Имитировать ошибки в работе с памятью, такие как выделение большого количества памяти или обращение к неверному адресу.
2. Проверить, что система корректно обрабатывает ошибки в работе с памятью и продолжает работу.
3. Повторить шаги 1-2 для различных типов ошибок в работе с памятью.
4. Сравнить поведение системы с требованиями к работоспособности.

Ожидаемый результат:

* Система корректно обрабатывает ошибки в работе с памятью и продолжает работу.

**Пример тест-кейса**

Номер: 005 Название: Тестирование на устойчивость к ошибкам в работе с сетью.

Описание: Проверка устойчивости программного обеспечения к ошибкам в работе с сетью.

Шаги:

1. Имитировать ошибки в работе с сетью, такие как потеря пакетов или недоступность узла.
2. Проверить, что система корректно обрабатывает ошибки в работе с сетью и продолжает работу.
3. Повторить шаги 1-2 для различных типов ошибок в работе с сетью.
4. Сравнить поведение системы с требованиями к работоспособности.

Ожидаемый результат:

* Система корректно обрабатывает ошибки в работе с сетью и продолжает работу.

**проверка правильности функционирования (тестирование на тестовых данных, приводящих к известному результату) программного обеспечения и средств защиты информации, объем и содержание которой определяется оператором**

**Пример тест-кейса**

Номер: 003 Название: Проверка правильности работы средства защиты информации.

Описание: Проверка правильности работы средства защиты информации на тестовых данных, приводящих к известному результату.

Шаги:

1. Подготовить тестовые данные, которые приведут к известному результату при использовании средства защиты информации.
2. Запустить средство защиты информации на тестовых данных.
3. Сравнить результат с ожидаемым результатом.

Ожидаемый результат:

* Результат работы средства защиты информации соответствует ожидаемому результату.
* Средство защиты информации корректно обрабатывает все тестовые данные.

**контроль соответствия настроек программного обеспечения и средств защиты информации параметрам настройки, приведенным в эксплуатационной документации на систему защиты информации и средства защиты информации**

**Пример тест-кейса**

Номер: 006 Название: Тестирование на контроль соответствия настроек программного обеспечения и средств защиты информации параметрам настройки, приведенным в эксплуатационной документации на систему защиты информации и средства защиты информации.

Описание: Проверка соответствия настроек программного обеспечения и средств защиты информации параметрам настройки, приведенным в эксплуатационной документации на систему защиты информации и средства защиты информации.

Шаги:

1. Ознакомиться с эксплуатационной документацией на систему защиты информации и средства защиты информации.
2. Проверить настройки программного обеспечения и средства защиты информации на соответствие параметрам, указанным в документации.
3. Если есть расхождения, поправить настройки и повторить шаг 2.
4. Протестировать работу программного обеспечения и средства защиты информации в соответствии с настройками.

Ожидаемый результат:

* Настройки программного обеспечения и средства защиты информации соответствуют параметрам, указанным в эксплуатационной документации на систему защиты информации и средства защиты информации.
* Программное обеспечение и средство защиты информации работают корректно в соответствии с настройками.

**восстановление работоспособности (правильности функционирования) и параметров настройки программного обеспечения и средств защиты информации (при необходимости), в том числе с использованием резервных копий и (или) дистрибутивов**

**Пример тест-кейса**

Номер: 007 Название: Тестирование восстановления работоспособности и настройки ПО и СЗИ с использованием резервных копий и дистрибутивов.

Описание: Проверка возможности восстановления работоспособности и настройки программного обеспечения и средств защиты информации с использованием резервных копий и дистрибутивов.

Шаги:

1. Создать резервную копию программного обеспечения и средств защиты информации.
2. Изменить настройки программного обеспечения и средств защиты информации.
3. Выполнить восстановление работоспособности и настройки программного обеспечения и средств защиты информации с использованием резервной копии и дистрибутивов.
4. Проверить, что настройки программного обеспечения и средств защиты информации восстановлены корректно.
5. Протестировать работу программного обеспечения и средств защиты информации в соответствии с настройками.

Ожидаемый результат:

* Работоспособность и настройки программного обеспечения и средств защиты информации восстановлены корректно.
* Программное обеспечение и средства защиты информации работают корректно в соответствии с восстановленными настройками.

**Контроль работоспособности, параметров настройки и правильности функционирования программного обеспечения и средств защиты информации проводится с периодичностью, установленной оператором в организационно-распорядительных документах по защите информации.**

**Пример тест-кейса**

Номер: 009 Название: Проверка работоспособности, параметров настройки и правильности функционирования программного обеспечения и средств защиты информации согласно установленной периодичности.

Описание: Проверка работоспособности, параметров настройки и правильности функционирования программного обеспечения и средств защиты информации согласно установленной периодичности, указанной в организационно-распорядительных документах по защите информации.

Шаги:

1. Ознакомиться с организационно-распорядительными документами по защите информации, чтобы узнать периодичность проверки работоспособности, параметров настройки и правильности функционирования программного обеспечения и средств защиты информации.
2. Выполнить контроль работоспособности, параметров настройки и правильности функционирования программного обеспечения и средств защиты информации согласно установленной периодичности.
3. Записать результаты контроля в соответствующую документацию.

Ожидаемый результат:

* Работоспособность, параметры настройки и правильность функционирования программного обеспечения и средств защиты информации соответствуют установленной периодичности контроля и требованиям организационно-распорядительных документов по защите информации.

**АНЗ.1\_АНЗ.2. Выявление, анализ уязвимостей информационной системы и оперативное устранение вновь выявленных уязвимостей**

**Введение**

Open Web Application Security Project (OWASP) - некоммерческая организация, посвященная улучшению безопасности программного обеспечения. OWASP выявила десять наиболее распространенных уязвимостей веб-приложений, которые могут создавать риски для бизнеса и пользователей. Целью данного документа является предоставление обзора OWASP Top 10 уязвимостей и методов защиты, которые помогут организациям снизить эти риски.

**OWASP Top 10 уязвимостей**

**1. Инъекции**

Недостатки инъекций, такие как SQL, NoSQL, OS и LDAP инъекции, происходят, когда ненадежные данные отправляются интерпретатору в качестве части команды или запроса. Это может привести к несанкционированному доступу к конфиденциальным данным или даже полному захвату хоста.

**Методы защиты**

* Использование параметризованных запросов для предотвращения SQL-инъекций
* Валидация и санитизация ввода для данных, управляемых пользователем
* Использование подготовленных операторов для запросов
* Использование хранимых процедур для доступа к базе данных

**2. Нарушение аутентификации и управления сессиями**

Эта уязвимость возникает, когда злоумышленник получает доступ к учетной записи или сессии пользователя, позволяя им получить доступ к конфиденциальным данным или выполнить несанкционированные действия.

**Методы защиты**

* Использование надежных паролей и многофакторной аутентификации
* Реализация безопасного управления сессиями
* Использование безопасных сессионных токенов
* Применение политик паролей

**3. Межсайтовый скриптинг (XSS)**

Атаки XSS возникают, когда злоумышленник внедряет вредоносные скрипты на веб-страницу, просматриваемую другими пользователями. Эта уязвимость может использоваться для кражи пользовательских данных или выполнения несанкционированных действий от имени пользователя.

**Методы защиты**

* Использование валидации и санитизации ввода для данных, управляемых пользователем
* Использование политики безопасности содержимого (CSP) для предотвращения атак XSS
* Использование файлов cookie с атрибутом HTTPOnly для предотвращения доступа к файлам cookie сессии с помощью кода JavaScript

**4. Нарушение контроля доступа**

Эта уязвимость возникает, когда злоумышленник может получить доступ к данным или выполнить действия, которые должны быть ограничены авторизованными пользователями.

**Методы защиты**

* Реализация контроля доступа для всех ресурсов
* Использование контроля доступа на основе ролей (RBAC)
* Использование принципа наименьших привилегий
* Реализация безопасного управления сессиями

**5. Неправильная конфигурация безопасности**

Неправильная конфигурация безопасности возникает, когда программное обеспечение не настроено безопасно, что делает его уязвимым для атак.

**Методы защиты**

* Реализация безопасных конфигураций программного обеспечения
* Использование безопасных практик развертывания
* Использование сканеров уязвимостей для выявления проблем конфигурации
* Регулярное обновление и патчинг программного обеспечения

**6. Небезопасное криптографическое хранилище**

Эта уязвимость возникает, когда конфиденциальные данные не хранятся безопасно, что делает их уязвимыми для кражи.

**Методы защиты**

* Использование надежных алгоритмов шифрования
* Использование соленых хешей для хранения паролей
* Использование безопасных методов управления ключами
* Защита ключей шифрования от несанкционированного доступа

**7. Недостаточное ведение журналов и мониторинг**

Недостаточное ведение журналов и мониторинг затрудняет обнаружение и реагирование на атаки.

**Методы защиты**

* Реализация ведения журналов и мониторинга для всех компонентов программного обеспечения
* Использование систем обнаружения и предотвращения вторжений
* Регулярный просмотр журналов на наличие необычной активности
* Реализация автоматизированных оповещений о необычной активности

**8. Небезопасное общение**

Небезопасное общение возникает, когда конфиденциальные данные передаются по незащищенной сети, что делает их уязвимыми для перехвата.

**Методы защиты**

* Использование безопасных протоколов связи, таких как HTTPS
* Использование шифрования для конфиденциальных данных в пути сообщения
* Реализация безопасных механизмов аутентификации
* Использование безопасной аутентификации на основе токенов

**9. Нарушение авторизации на уровне функций**

Эта уязвимость возникает, когда злоумышленник может получить доступ к функциональности, которая должна быть ограничена авторизованным пользователям.

**Методы защиты**

* Реализация контроля доступа для всей функциональности
* Использование контроля доступа на основе ролей (RBAC)
* Использование принципа наименьших привилегий
* Реализация безопасного управления сессиями

**10. Использование компонентов с известными уязвимостями**

Использование компонентов с известными уязвимостями может сделать программное обеспечение открытым для атак.

**Методы защиты**

* Регулярное обновление и патчинг компонентов программного обеспечения
* Использование сканеров уязвимостей для выявления уязвимых компонентов
* Использование безопасных методов разработки программного обеспечения
* Мониторинг предупреждений о безопасности для компонентов программного обеспечения

# Состав и содержание работ по развитию системы

Доработка системы должна проходить в несколько этапов:

**Этап 1. Проектирование Системы:**

* 1. Аналитика
* Сбор требований ко всем разделам и функциональным возможностям системы с подготовкой письменного отчета с итогами;
  1. Разработка архитектуры системы
* Проектирование архитектуры системы, выбор технологического стека разработки;
* Разработка инструментов логирования и рассылки.
  1. Пользовательский интерфейс
* Доработка существующего UI-kit;
* Проектирование и согласование экранных форм для всех разделов ИСУП.
  1. Разработка и согласование технического проекта, включая частные технические задания для каждого блока разработки.

**Этап 2. Разработка/доработка функционал:**

* Доработка раздела «Список проектов» (п. 4.1)
* Заявка проекта (п. 4.2)
* Дорожная карта проекта (п. 4.3)
* Паспорт проекта (п. 4.4)
* Оптимизация ролевой интеграции в связке систем Leader-ID, SSO (п. 4.5)
* Доработки уведомлений (п. 4.6)
* Создание страницы авторизации (п. 4.7)
* Задание критериев оценки проектов (п. 4.8)
* Рейтинг проектов (п. 4.9)

**Этап 3. Разработка/доработка функционала**

* Разработка раздела «Отчеты» (п. 4.10)
* Управление коллегиальными органами (п. 4.11)
* Подписание согласия на передачу персональных данных и на поддержку проектов (п. 4.12)
* Реализация требований информационной безопасности (п. 4.13)
* Регистрация согласий субъектов об обработке персональных данных (п.4.14)
* Административная часть (п. 4.15)
* Доработка ролевой модели (п. 4.16)
* API для интеграции (экспорт/импорт) (п. 4.17)
* История изменений (п. 4.18)

**Этап 4. Разработка/доработка функционала:**

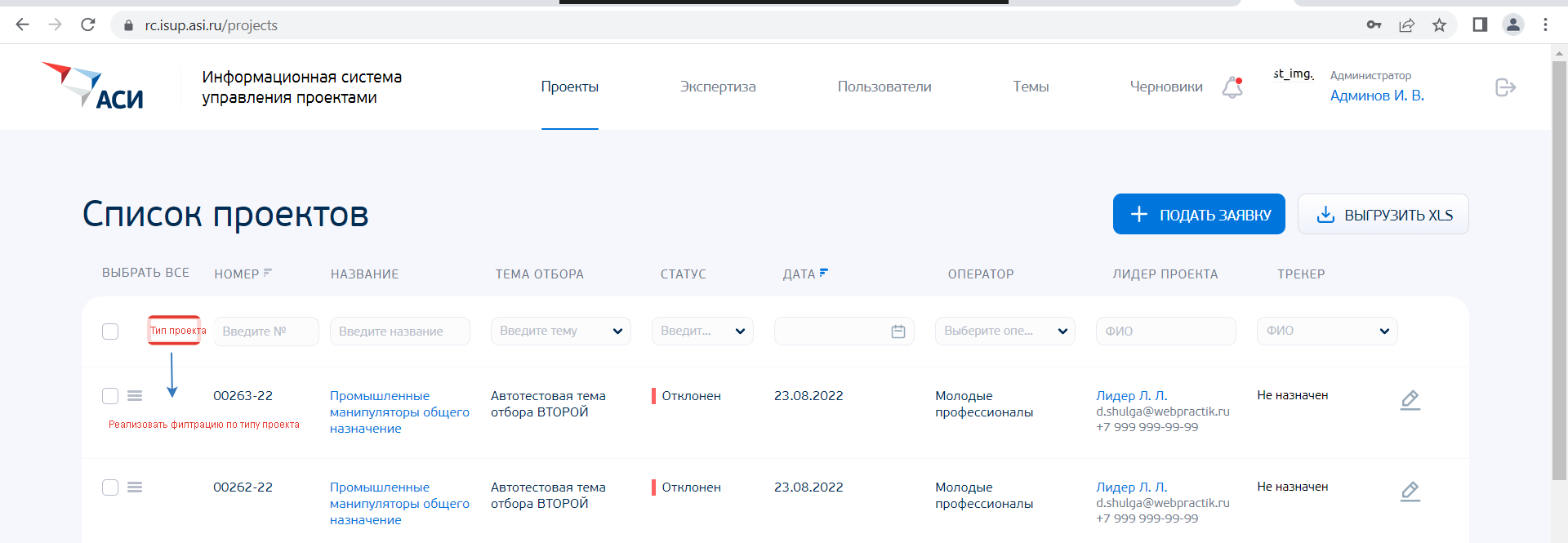
* Адаптация системы под мобильную версию (п. 4.19)
* Партнеры (п. 4.20)
* Доработка личного кабинета пользователя (п. 4.21)
* Сертификаты для экспертов/лидеров (п. 4.22)
* Сквозной поиск по компонентам разделов системы (п. 4.23)

# Перечень работ

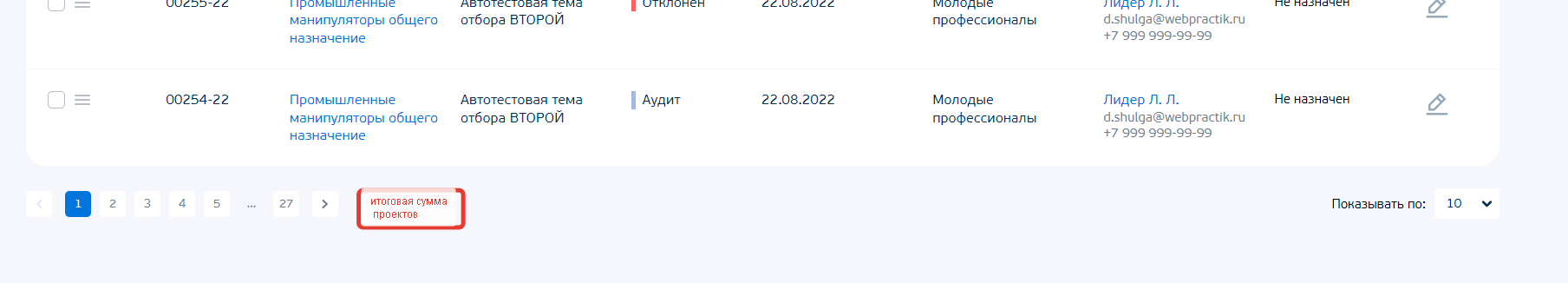
## Доработка раздела «Список проектов»

Необходимо добавить атрибут «Тип проекта» для проектов. Формат данного поля – выпадающий список, настраиваемый из справочника в административной части, например, лидерские проекты, практики, сильные идеи, молодежные проекты, соглашения и т.д. Верхнеуровневое отображение проектов в разделе «Список проектов» происходит по типу проекта, далее должны быть предусмотрены различные фильтры каждого из типа проектов.

После регистрации/авторизации пользователи должны переходить в раздел «Список проектов», где отображаются данные, определенные правами доступа для каждой категории пользователей для лидерских проектов, практик, молодежных проектов, проектов с типом «соглашение» и т.д.



На странице «Список проектов» должно выводиться общее количество проектов в базовом состоянии страницы (до применения фильтров) и после применения фильтров (Например, «Показано 37 из 400»).



### Возможность вывода всех полей из заявки и паспорта проекта на странице списка проектов

Реализовать возможность для пользователя настраивать выводимые поля на странице «список проектов». Предусмотреть для пользователя возможность сохранить выбранный набор полей для повторного использования. Предусмотреть возможность указать набор полей по умолчанию для конкретных групп пользователей через административную часть.

Для удобного взаимодействия с большими таблицами необходимо реализовать горизонтальную прокрутку содержимого (скроллинг) внутри таблицы.

При выгрузке в Excel должна выводиться структура полей, примененная пользователем, либо структура по умолчанию, если пользователь не задавал иную структуру. Использование типов полей для выгрузки должно зависеть от полномочий пользователя[[7]](#footnote-7).

## Заявка проекта

### Единая заявка

Необходимо реализовать возможность пользователям с соответствующими ролями задавать структуру заявки для отбора из набора предопределенных полей. В Приложении 2 указан примерный базовый набор полей заявки проекта. Полный список полей будет уточнен при подготовке технического проекта в рамках реализации договора.

Так как данный список полей создавался как единый для любых типов проектов, при выборе полей для отображения в заявке необходимо реализовать визуальные подсказки (шаблоны) для различных типов проектов в системе (лидерские проекты, практики, молодежные проекты, соглашения и др.) и темы проекта (технологические, образовательные, социальные, экологические), разбив наборы полей по блокам (о проекте, о лидере, об организации, о команде, общее). Для пользователей с соответствующими правами в Системе необходимо предусмотреть возможность задавать базовый набор полей для заявки проекта в зависимости от типа проекта или темы проекта.

В рамках создания заявки для отбора необходимо предусмотреть следующий функционал:

– выведение/скрытие конкретного поля в заявке;

– заведения ограничения по символам конкретного поля заявки;

– установки обязательность/необязательность заполнения конкретного поля заявки;

– установки раздела заявки для вывода поля;

– редактирование названия поля;

– размещения подсказку-описание для конкретного поля заявки.

Помимо полей, указанных в Приложении 2, необходимо предусмотреть возможность добавления дополнительных полей формы заявки примитивных или ссылочных типов. У пользователей, помимо редактирования атрибутов полей из базового набора, должна быть возможность редактировать название данных полей, а также указывать раздел заявки, в котором данное поле будет выводиться. Необходимо использовать архитектурные шаблоны Event Sourcing и CQRS с целью фиксирования и сохранения последовательности всех изменений (хронологический метод совокупно для состояний и событий), вносимых в систему.

После запуска отбора возможность изменения заявки блокируется.

Все шаблоны заявок должны сохраняться в виде списка с указанием темы отбора, типа проекта, вида проекта, даты создания шаблона и наборами связанных с шаблонами полей. Система должна предусматривать возможность установки периода действия отдельных свойств заявок.

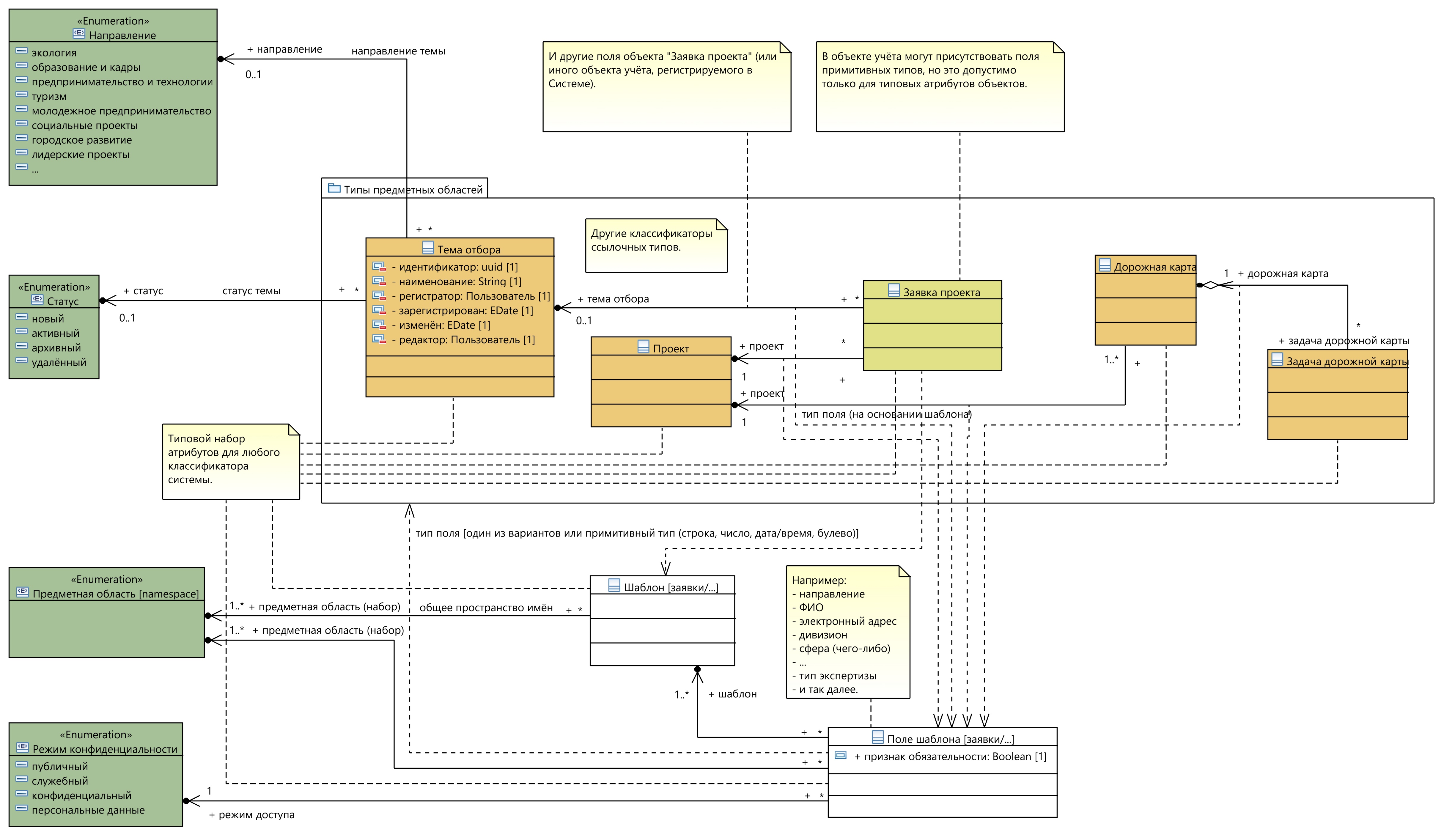
Архитектурные шаблоны Event Sourcing и CQRS для хранения и управления метаданными не должны применяться. Вместо этого, система не должна предоставлять возможностей удаления метаданных из баз данных системы (а только возможность установки пометок на удаление). Удаление должно быть возможным только с помощью специальных технических средств с обязательным контролем ссылочной целостности.

Модель метаданных должна предлагать администратору возможность ввода полей вида «Категория»[[8]](#footnote-8), обладающих фиксированным набором значений, примитивным типом или типом, заданным любым системным классификатором (справочником или реестром), с помощью которых в списочных или структурных (древовидных, например) представлениях использовать их в качестве фильтров для отборов или правил для сортировки. Созданные таким образом категории могут быть связаны администратором системы с любым предметным справочником и/или реестром Системы.

В Приложении 2 указан примерный набор полей единой карточки проекта, поля которой доступны для выбора в заявку. Конкретная структура данных должна быть создана в ходе разработки технического проекта, включающего в себя[[9]](#footnote-9):

* структуры метаданных, определяющие архитектуру хранилища базовых объектов предметных областей;
* структуры метаданных и их взаимосвязи для произвольным образом добавляемых атрибутов и характеристик, с учётом типов значений, периодов актуальности и области доступности (персональные данные, конфиденциальная информация, открытые данные, служебные данные).

Предусмотреть возможность масштабирования по формату и количеству дополнительных полей в рамках последующих доработок системы.



Модель 1: Модель формирования предметных областей Системы на примере Заявки проекта

### Создание заявки

При заполнении заявки, в рамках подачи проекта пользователем каждый раздел должен быть оформлен отдельным шагом в виде раскрывающегося блока.

При сохранении заявки создается карточка проекта с присвоением номера проекта. Пользователям отправляется уведомление существующими каналами коммуникации о создании проекта. Для проектов с указанными значениями «Поступает повторно» или «Акселерация» (см. п. 4.2.3) необходимо выводить данные значения в теме сообщения/письма.

Необходимо реализовать возможность изменения всех атрибутов проекта, включая значения «Поступает повторно» и «Акселерация» в соответствии с ролевой моделью. В интерфейсе системы, а также в отчетах необходимо отражать привязку первичных проектов с повторно поданными.

### Копирование заявки

Предусмотреть для пользователей возможность подачи заявки на отбор из карточки поданного ранее проекта.

При подаче заявки на отбор система должна предоставить пользователю возможность выбора темы текущих отборов, в который пользователь хочет подать проект. После выбора темы, пользователю должна быть предоставлена возможность выбора: «Подать новый проект» или «Подать существующий проект». Если пользователь выберет вариант «Подать существующий проект», ему открывается форма с возможностью выбора проекта из списка существующих. После выбора существующего проекта, пользователю выводится форма заявки, заполненная значениями полей из существующего проекта с возможностью редактирования, кроме номера заявки. В случае, если в существующем проекте именование произвольных полей отличаются от заполняемой заявки, перенос заполненных данных не производится.

При сохранении проекту присваивается новый номер. После того, как все поля будут заполнены корректно, заявка регистрируется в системе со статусом «экспертиза».

Предусмотреть указание в карточке такого проекта ID проекта, на основании которого заполнена новая заявка, и гиперссылку на данный проект.

Также нужно предусмотреть возможность подачи проекта на отбор повторно через карточку самого проекта. Для этого из списка проектов, у которых текущий пользователь является лидером, он выбирает проект, копию которого он хочет создать, и переходит в карточку этого проекта, где размещена кнопка «Подать повторно». При нажатии на кнопку «Подать проект повторно» система должна вывести интерактивное окно с запросом тем текущих отборов, в который пользователь хочет подать повторно данный проект. После выбора темы, пользователю выводится форма заявки, заполненная значениями полей из существующего проекта с возможностью редактирования.

### Импорт заявок

Необходимо предусмотреть возможность массовой загрузки проектов в систему для пользователей в соответствии с ролевой моделью. Для этого, в интерфейсе пользователя, предусмотреть кнопку «Загрузка проектов», при нажатии на которую выводится интерфейсное окно для выбора файла загрузки и указания отбора, в который предполагается импортировать проекты. Также в интерфейсе пользователя предусмотреть ссылку на актуальный шаблон загрузки в формате Excel таблицы. Шаблон файла импорта должен быть разработан и согласован с Заказчиком в рамках подготовки технического проекта.

Импорт возможен только через файл excel (расширение .xls, .xlsx).

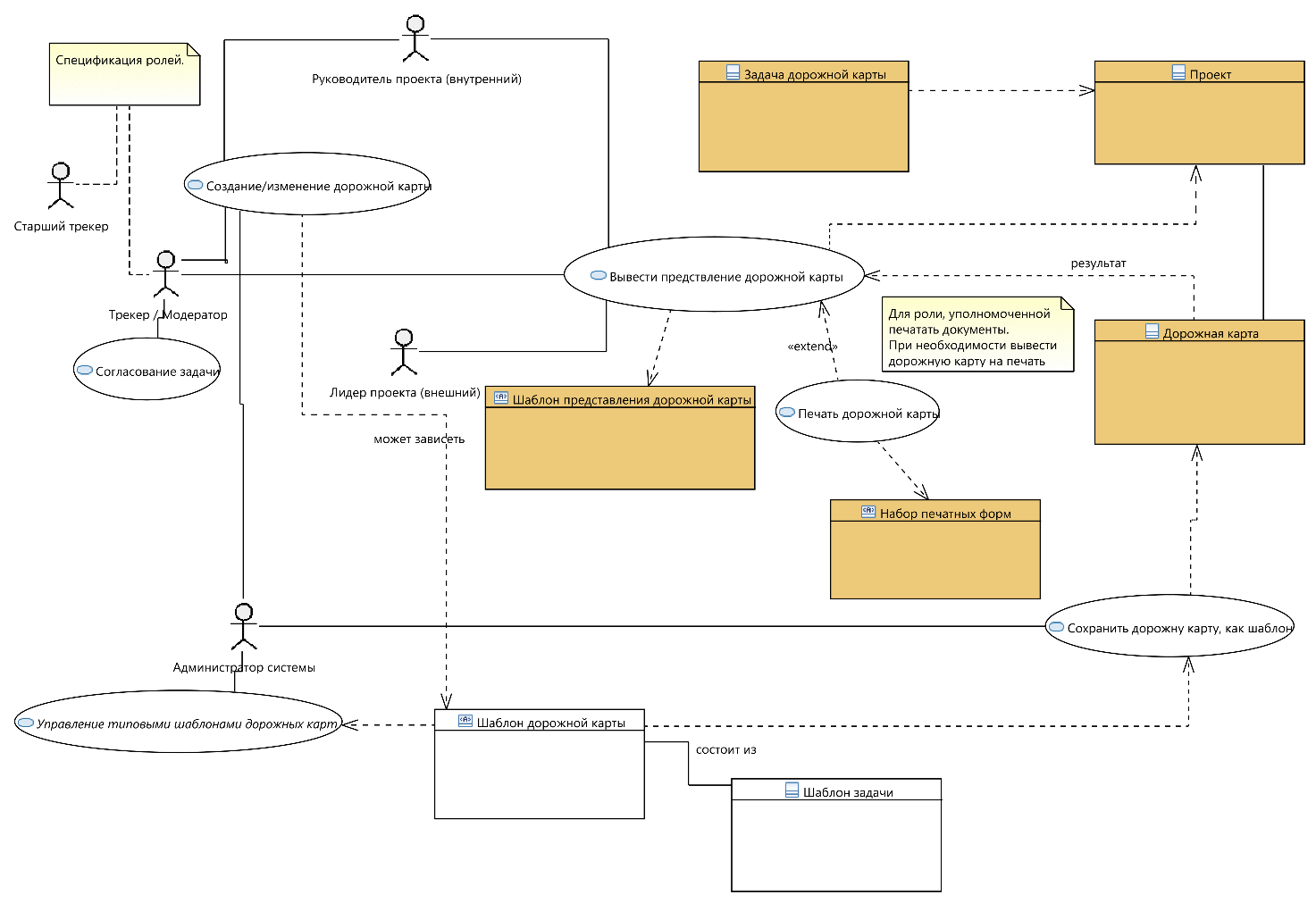
При импорте проектов необходимо проводить валидацию импортируемых данных на соответствие типам данных, количеству символов и прочим ограничениям полей, в которые импортируются данные. Пользователю должно быть выведено отдельное интерфейсное окно для разрешения ошибок при импорте. Ошибкой при импорте также считается пустое поле в импортируемом файле, отмеченное в заявке к отбору как обязательное. Также, в данном окне пользователи должны загрузить согласия лидеров проектов на обработку данных и прочие файлы с привязкой к конкретному проекту.

Также предусмотреть аналогичный функционал выбора импортируемого файла, согласно заданного шаблона, но с ограничением количества импортируемых проектов не более одного. После импорта файла пользователю необходимо вывести форму заявки для подтверждения согласия на обработку данных.

Создание проектов в системе и присвоение им номеров производится для всех ролей только после разрешения всех конфликтов и указания всех обязательных полей.

## Дорожная карта проекта

Дорожная карта (ДК) проекта — это система управления задачами, которая позволяет сотрудникам АСИ автоматизировать работу с проектом: вести список мероприятий, назначать ответственных за них, контролировать сроки выполнения.

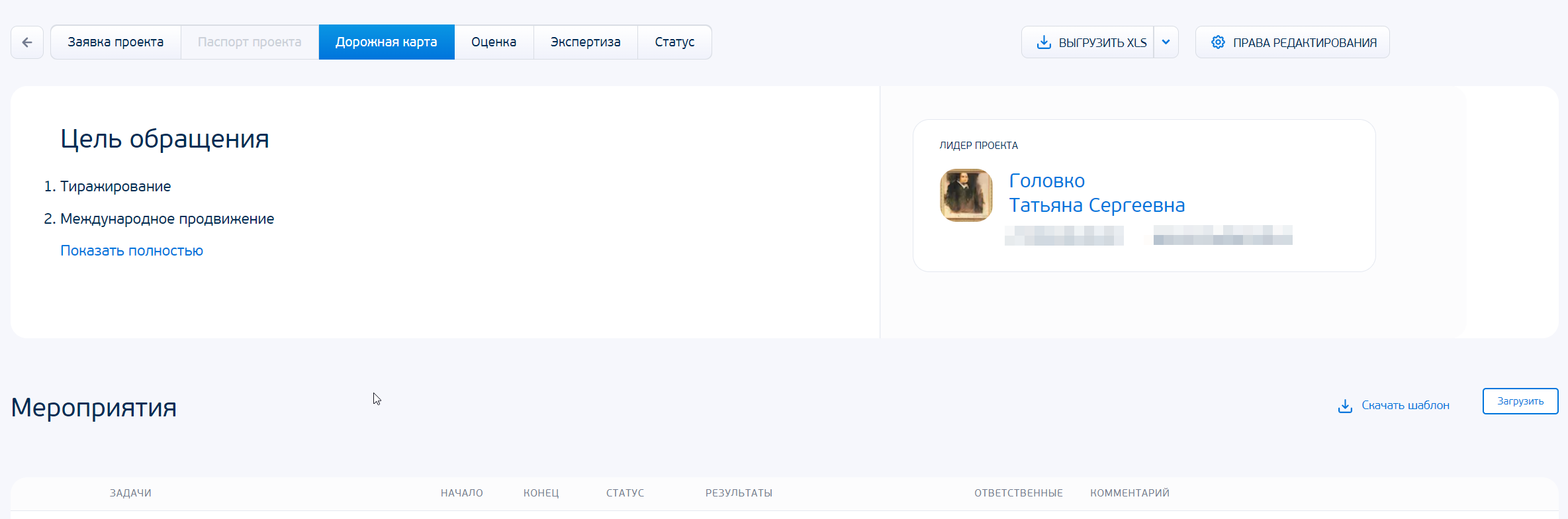


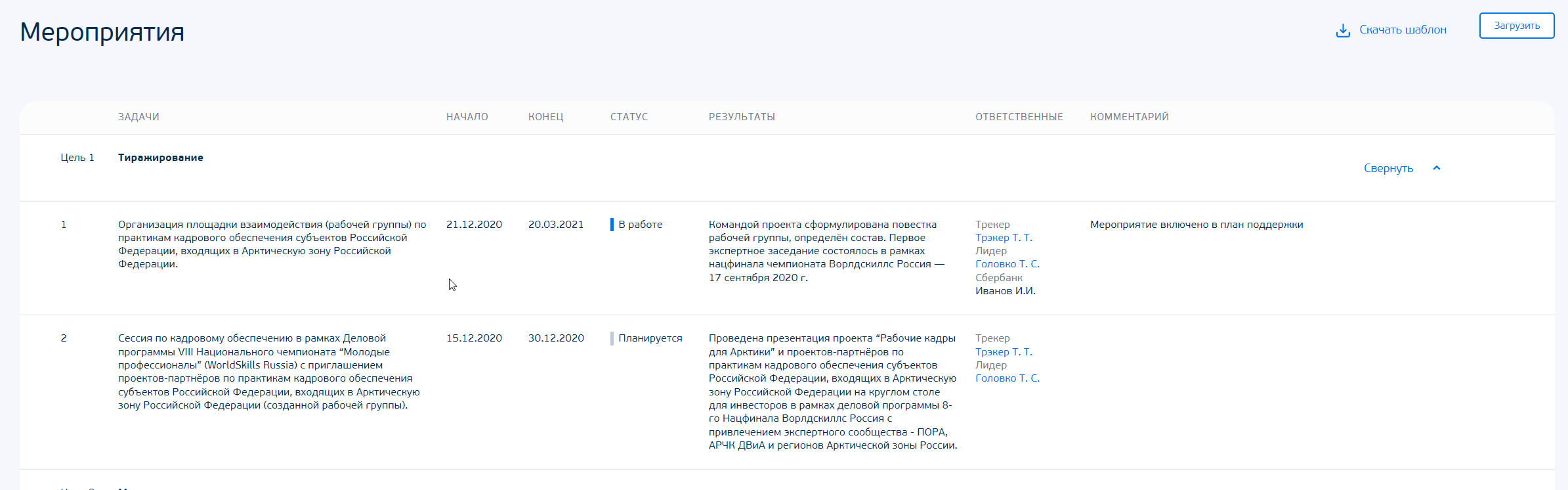
**Модель 2: Карта прецедентов управления дорожной карты**

Дорожная карта проекта находится внутри детальной страницы [проекта на отдельной вкладке.](https://w6p.ru/NTdlMWF.png)

В текущей версии функционал создания дорожных карт реализован с помощью парсера Excel-файлов. Информация в блоке «Цели обращения» подтягиваются из заявки проекта. Информация в блоке «Лидер проекта» подтягивается из профиля лидера.

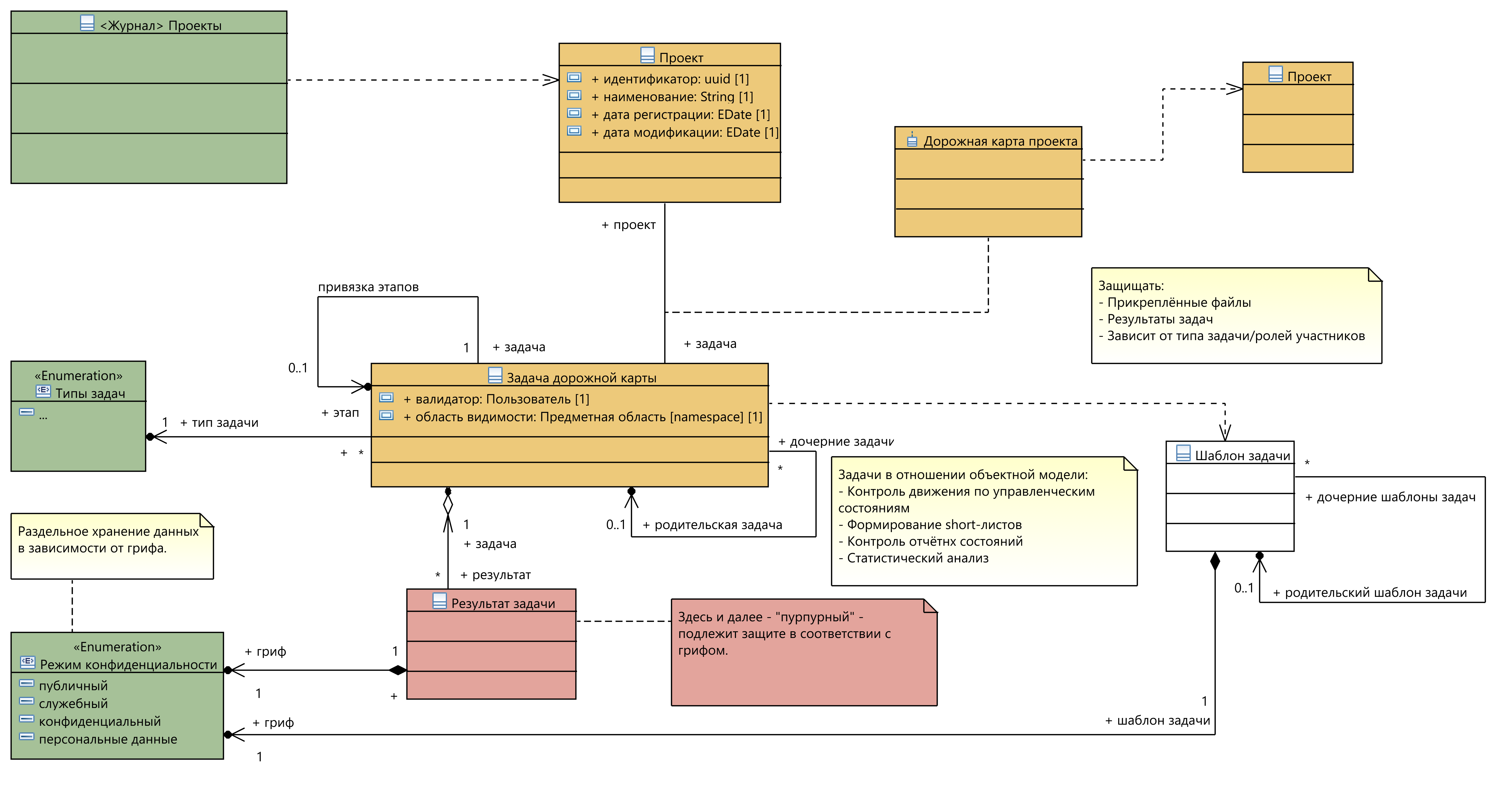
Информация в блоке «Мероприятия» заполняются полностью путем загрузки Excel файла, заполненного по определенному шаблону.





### Содержание дорожной карты

В новой версии функционала дорожной карты проекта информация в блоке «Мероприятия» должна формироваться путем создания задач проекта. Для реализации требуется разработать отдельную сущность «Задача» со атрибутами, указанными в таблице 3.

Модель 3: Предметная область «Задачи дорожной карты»

Результаты задач — могут содержать объекты (на основании указанных видов), требующие защиты информации:

* персональные данные: доступ только персоналу, установленному соответствующим приказом;
* конфиденциальная информация: доступ персоналу, установленному руководством функционального заказчика;
* служебные данные: доступ только пользователям, принадлежащим конкретным группам и/или обладающим соответствующим мандатом.

Вся уже введенная информация в блок «Мероприятия» путем загрузки Excel-файла должна быть сохранена и переведена в формат задач.

Таблица 3

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Наименование атрибута** | **Тип данных** | **Ограничения** | **Обязательное** | **Комментарий** |
| Наименование | Текстовое поле | Не более 100 символов | Да | Краткое наименование задачи |
| Описание | Текстовое поле | - | Да | Полное описание задачи |
| Дата начала | Дата | - | Да | Дата начала исполнения задачи |
| Дата окончания | Дата | - | Нет | Дата окончания исполнения задачи |
| Длительность | Число | - | Нет | Количество рабочих дней- длительность выполнения задачи. |
| Тип | Список | Возможность выбрать только значения из справочника «Типы задач» | Да | Для реализации гибкого управления проектом |
| Результат | Текстовое поле | - | Нет | Описание требуемого результата выполнения задачи в свободной форме. Для ряда типов проектов и типов задач ввод и вывод в отдельном окне (детализация в техническом проекте) |
| Ответственные | Поле со списком пользователей  И  Текстовое поле | - | Да | Выбор ответственных из списка пользователей либо указание ответственного внешнего сотрудника и/или ответственной организации текстом вручную |
| Дочерняя задача | Число | - | Нет | Привязка к задачам более низкого уровня для построения иерархии задач. В карточку дочерней задачи должна указываться ссылка на родительскую задачу и наоборот |
| Родительская задача | Число | - | Нет | Привязка к задачам более высокого уровня для построения иерархии задач |
| Задачи-последователи | Число |  | Нет | Привязка к задачам, которые не могут быть выполнены без завершения текущей задачи, для построения иерархии задач |
| Задачи-предшественники | Число |  | Нет | Привязка к задачам, которые должны быть завершены до старта текущей задачи, для построения иерархии задач |
| Статус | Список | Возможность выбрать только значения из справочника «Статусы задач» | Да |  |
| Прикрепленные файлы | Загрузка файлов | - | Нет |  |
| Согласующий | Поле со списком пользователей |  | Нет | Выбор согласующего из списка пользователей |
| Согласование выполнения задачи | Булево | Доступно только пользователю, указанному как Согласующий в задаче | Нет |  |
| Комментарии | Текстовое поле | Доступно трекеру | нет | Множественные комментарии в формате ленты сообщений |

Предусмотреть в административной части системы возможность настройки отображения и признака обязательности атрибутов задач дорожной карты.

Для добавления задачи в дорожную карту необходимо разместить в карточке проекта кнопку «Добавить задачу», при нажатии на которую будет выводиться интерфейсное окно с полями для заполнения, согласно таблице выше. Сохранение задачи возможно только в случае, если заполнены все обязательные поля.

В интерфейсе дорожной карты необходимо предусмотреть возможность изменения полей конкретной задачи. При изменении данных через дорожную карту, данные в полях карточки задачи должны автоматически изменяться.

Необходимо предусмотреть перерасчет дат начала и окончания на основании введённой длительности задачи и привязки к прочим задачам дорожных карт.

### Шаблоны дорожных карт

В системе необходимо предусмотреть создание шаблонов дорожных карт как наборов предсозданных задач. Для этого необходимо предусмотреть в разделе «Дорожная карта» карточки проекта кнопку «Сохранить дорожную карту как шаблон». При нажатии на эту кнопку выводится интерфейсное окно для указания пользователем типов проектов (из выпадающего списка), тематик отборов (из выпадающего списка) и комментария пользователя (текстовое поле).

Для заполнения задач в дорожной карте из шаблона необходимо разместить кнопку «Заполнить задачами из шаблона». Предусмотреть возможность пользователю указать место в дорожной карте, начиная с которого необходимо вставлять задачи из шаблона. При нажатии на эту кнопку пользователю должен выводиться список сохраненных шаблонов с указанием типов проектов и комментариев. Пользователь должен иметь возможность фильтровать представленный список по представленным атрибутам и осуществлять поиск по любому полю. Пользователь должен иметь возможность добавлять мероприятия в шаблон, а также удалять мероприятия из шаблона.

Необходимо разработать подраздел «Шаблоны ДК» в административной части системы, в котором вывести сохраненные шаблоны для редактирования. Пользователь должен иметь возможность указать шаблон по умолчанию для новых проектов с определенными атрибутами. В этом случае, при создании проекта с указанными атрибутами дорожная карта заполняется из шаблона по умолчанию.

Детализация и уточнение требований для шаблона дорожных карт необходимо уточнить в техническом проекте.

### Типы задач

Для заполнения атрибута задачи «Тип задачи» в системе необходимо создать справочник «Типы задач». Возможность редактировать данный список должна быть обеспечена в разделе «Настройки системы» административной части системы. Типы задач, используемые в логике работы системы (аудит, экспертиза и т.д. – подробный список событий должен быть уточнен в техническом проекте), должны отмечаться в интерфейсе системы и не должны быть доступны для удаления. В зависимости от типа задач необходимо предусмотреть возможность настройки полей задач, а также условий выполнения задачи.

### Просрочка задач

В системе необходимо предусмотреть возможность устанавливать допустимый период просрочки. В случае смены статуса задачи в срок, превышающий допустимый период просрочки с момента плановой даты («Дата начала» или «Дата окончания») пользователю необходимо вывести обязательное для заполнения окно «Причина задержки». Необходимо также предусмотреть в дорожной карте цветовую индикацию статуса просрочки задач. Введенный пользователем ответ хранить как комментарии к задаче.

### Экспорт дорожной карты и плана поддержки

Разработать механизм частичного или полного экспорта ДК в doc, pdf и xlsx.

Примерные формы выгрузки ДК:

1. Вариант полной ДК указан в Приложении 3.
2. Форма выгрузки части задач дорожной карты с типом задачи «Поддержка проекта» указан в Приложении 4.
3. Форма выгрузки части задач дорожной карты с типом задачи «Поддержка проекта» на этапе «сопровождение» указан в Приложении 5.

## Паспорт проекта

Требуется разработать раздел «Паспорт проекта» внутри подробной страницы [проекта.](https://w6p.ru/NTdlMWF.png)

Паспорт проекта — это модуль в ИСУП, который позволяет сотрудникам агентства автоматизировать работу с проектом: просматривать и редактировать данные по проекту, формировать выгрузки данных для представления на Рабочие группы и Бюро экспертного совета, а также подготавливать проект перед публикацией на внешние витрины.

Паспорт проекта – это раздел, который находится внутри подробной страницы [проекта и представляет собой набор полей и данных о проекте.](https://w6p.ru/NTdlMWF.png)

Шапка страницы и плашка с вкладками для навигации по странице должны быть закреплены, чтобы при прокручивании страницы вниз были видны данные, размещенные в них.

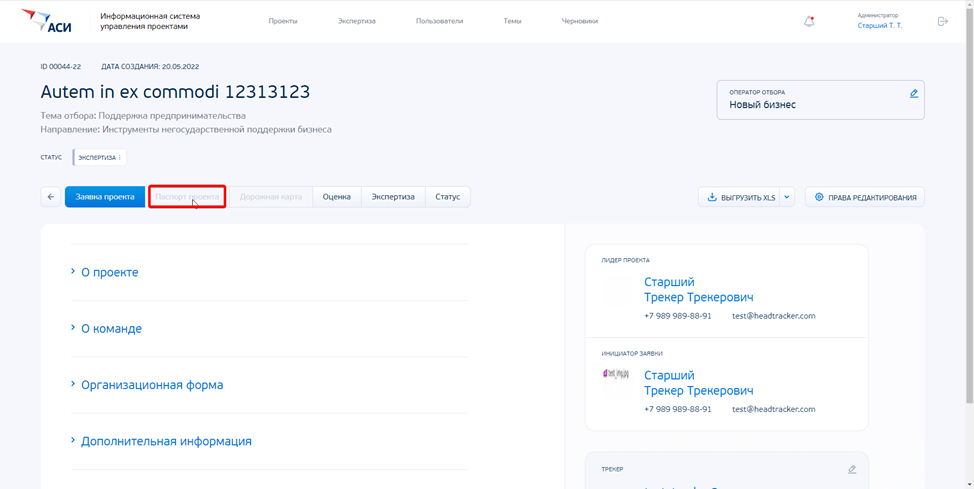
Данные в Паспорте первично должны заполняться из Заявки проекта. Необходимо предусмотреть возможность изменения полей Заявки проекта на определенных статусах, которые должны быть определены на этапы разработки технического проекта. Необходимо предусмотреть возможность редактирования полей в разделе «Паспорт проекта» на любых статусах проекта.

Структура разделов паспорта проекта должна соответствовать структуре разделов Заявки проекта, а также необходимо предусмотреть добавление дополнительных полей в паспорт проекта, которые будут уточнены на этапе подготовки технического проекта.

При редактировании текста необходимо реализовать в полях паспорта визуальный редактор для форматирования текста, с базовым набором функций (размер шрифта, заголовки, маркеры, списки и др.).

Необходимо предусмотреть функционал публикации полей паспорта проекта на внешние витрины. Для этого необходимо предусмотреть возможность установки атрибута «Готов к публикации» в паспорте проекта.

Детальный список полей паспорта и их группировка будут уточнены в ходе подготовки технического проекта.

В карточке проекта предусмотреть возможность выгрузки данных, введенных в Паспорте проекта в виде .pdf или .doc файлов. Выгрузка должна производиться в двух форматах: без блока «Результаты поддержки» и с блоком «Результаты поддержки».

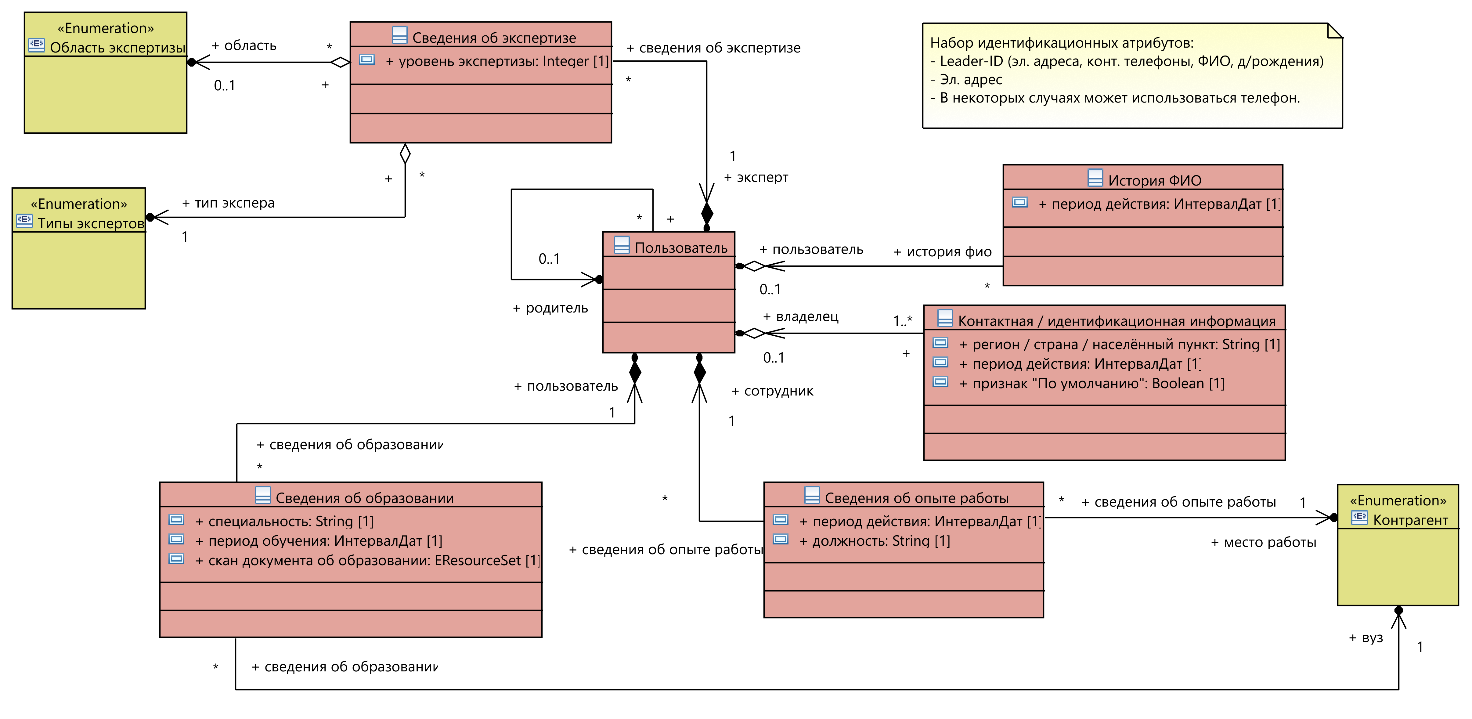
Пример выгрузки в doc представлен в Приложении 6.

Шапка детальной страницы проекта (везде проверить, убрать карточку) и плашка с вкладками для навигации по странице должны быть закреплены при прокручивании страницы.

Пример выгрузки в pdf представлен в Приложении 7.

## Оптимизация интеграции с Единым сервисом авторизации (SSO) и Leader-ID

В системе предусмотрена интеграция с Единым сервисом авторизации (SSO) и Leader-ID в части авторизации пользователей, получения доступных пользователю прав и данных профиля.



**Модель 4: Предметная область «Интеграция с Leader-ID и единым сервисом авторизации»**

Необходимо оптимизировать интеграцию с SSO в части аутентификации пользователей. Для этого: изменить набор данных в токене, которые будут использоваться для идентификации и последующей аутентификации пользователей через SSO.

В настоящий момент аутентификация пользователей происходит с помощью фамилии, имени, почты и идентификатора Leader-ID. Необходимо идентифицировать и аутентифицировать пользователей с помощью идентификатора Leader-ID.

Дополнительными идентификаторами пользователя могут быть:

* электронный адрес;
* контактный телефон;
* ФИО + дата рождения.

Должна быть возможность настроить их использование при объединении и верификации учётных записей пользователей.



**Модель 5: Карта прецедентов по интеграции ИСУП с Leader-ID и единым сервисом авторизации**

Синхронизация новых профилей пользователей с Leader-ID должна осуществляться с помощью идентификатора Leader-ID.

Необходимо предусмотреть возможность объединения учетных записей пользователей (профилей), если по разным профилям в системе уже присвоен один и тот же набор идентификационных атрибутов (Leader-ID, почта, телефон, фамилия и имя и взаимные их комбинации, например, Leader-ID и почта).

При этом, если в результате идентификации найдено большего одного профиля, формировать в системе административный реестр для разрешения конфликта. Система должна предусматривать возможность объединения двух и более учетных записей в одну на стороне ИСУП.

Также должна быть возможность разделения ранее ошибочно объединенных профилей.

Необходимо реализовать одностороннюю синхронизацию всех следующих атрибутов из Leader-ID в профиль пользователя в ИСУП:

* Фамилия (текстовое поле)
* Имя (текстовое поле)
* Отчество (текстовое поле)
* Почта (e-mail)
* Телефон
* Идентификатор Leader-ID (числовой формат)
* Учебное заведение (текстовое поле)
* Специализация (текстовое поле)
* Год начала обучения (формат даты «ГГГГ»)
* Год окончания обучения (формат даты «ГГГГ»)
* Организация (текстовое поле)
* Должность (текстовое поле)
* Год начала работы (формат даты «ГГГГ»)
* Год окончания работы (формат даты «ГГГГ»)
* Дополнительная информация (текстовое поле)
* Регион проживания пользователя

Необходимо настроить обновление данных текущей системы с Единым сервисом авторизации (SSO). При обновлении данных в SSO (создание новых учетных записей, назначение/снятие ролей, изменение данных профиля Leader-ID) необходимо настроить автоматические обновление данных в ИСУП при помощи функции обратных вызовов (вебхуков) SSO. Данные в ИСУП должны обновляться автоматически без совершения дополнительных действий.

Также необходимо разработать в ИСУП функции обратных вызовов (вебхуки), которые будут оповещать внешние системы о событиях смены данных в профилях пользователей.

Универсальный набор синхронизируемых идентификаторов пользователя ИСУП должен состоять из идентификаторов {Leader-ID, Keycloak}. Синхронизации подлежат наборы атрибутов, не содержащие идентификатор Leader-ID. Получение связанных атрибутов допускается только при условии указания одного из идентификаторов набора.

Исполнителю необходимо предоставить на утверждение Заказчику технический проект и ЧТЗ на технологическое решение.

## Доработки уведомлений

Необходимо реализовать возможность создания в системе шаблонов уведомлений. Необходимо реализовать возможность отправления рассылок по шаблонам в двух форматах:

* событийные уведомления: если в шаблоне уведомления указаны конкретные события, при выполнении которых должно отсылаться уведомление.
* информационный и технические уведомления: уведомления, которые отправляются при необходимости и не завязаны на совершение конкретных событий.

Для этого в административной части системе предусмотреть соответствующий раздел, в котором будет выведен список существующих шаблонов уведомлений, а также предоставлен функционал создания новых шаблонов, при использовании которого должен выводиться текстовый редактор с базовыми возможностями форматирования текста и изображений (выделение жирным, курсивом, подчеркивание, создание списков, добавление абзацев, заголовков, медиафайлов).

В рамках функционала редактирования шаблона необходимо предусмотреть возможность прикрепления гиперссылок к изображениям и тексту, тегов для персонализации уведомлений, прикрепления вложений к уведомлению. Необходимо реализовать возможность изменять и удалять созданные шаблоны уведомлений.

Предусмотреть возможность привязки шаблонов уведомлений к событиям системы, а также атрибутов для каждого события (например, срок и периодичность отправки уведомления с момента события). Список событий системы и атрибутов событий будет уточнен на этапе технического проекта.

Предусмотреть возможность привязки шаблонов уведомлений к задачам дорожной карты с указанием события, при котором должно отправляться уведомление. Список событий задач будет уточнен на этапе технического проекта.

Реализовать функционал управления списками рассылок (создание, редактирования, удаления) с возможностью подбора получателей из числа пользователей системы на основе атрибутов из профиля.

Уведомления должны отправляться с помощью существующих каналов коммуникации (например, внутренняя система уведомлений, с помощью электронной почты, мессенджеры и т.д.). Необходимо предоставить пользователю возможность выбрать, с помощью какого канала коммуникации необходимо рассылать уведомление.

Необходимо предусмотреть возможность интеграции с внешними сервисами управления рассылками в части создания шаблонов уведомлений.

## Создание страницы авторизации

Реализовать стартовую страницу авторизации с обновленным дизайном.

При входе в систему неавторизованному пользователю должна отображаться стартовая страница авторизации с возможность входа через Leader-ID, если пользователь не является сотрудником АСИ. Если пользователь является сотрудником АСИ и подключен к контуру рабочей сети АСИ, то помимо входа через Leader-ID у него должна быть возможность ввода доменного имени и пароля сотрудников АСИ.

Перед началом разработки необходимо создать-дизайн макет стартовой страницы для неавторизованного пользователя. Созданный дизайн-макет необходимо согласовать с Заказчиком.

## Задание критериев оценки проектов

Предусмотреть возможность пользователям указывать критерии оценки при создании нового отбора. Пользователь должен иметь возможность указать:

* Наименование критерия
* Вес критерия
* Метод оценки (баллы, «Да/нет»)
* Комментарий

Настройка критериев отбора должна быть доступна в разделе «Настройки системы» в соответствии с требованиями в разделе 4.15.3.

## Рейтинг проектов

В систему необходимо ввести подсчет рейтинга проектов на основе выставленных оценок экспертов на соответствие критериям 2 уровня. В рейтинге учитывается балл двух экспертов. Если на проекте меньше или больше двух экспертов, то рейтинг рассчитываться не будет.

Вес одного и того же критерия может отличаться в зависимости от вида и типа проекта.

Итоговая оценка проекта представляет собой среднюю оценок экспертов.

*Оценка эксперта = k1\*w1+k2\*w2+….+k9\*w9*

*kn – оценка критерия номер n*

*wn – вес критерия номер n*

*Итоговая оценка = (Оценка эксперта 1 + Оценка эксперта 2)/2*

Рейтинг и количество баллов каждого проекта, при его наличии, необходимо отображать:

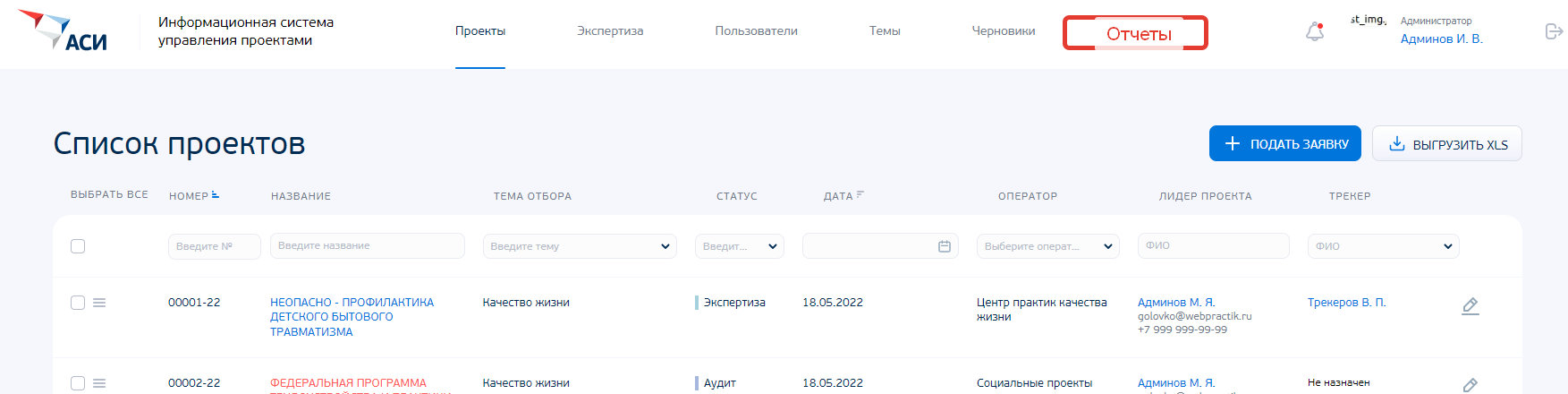
* в таблице всех проектов в отдельном столбце
* в карточке проекта на вкладке Экспертиза
* в выгрузке по форме Рейтинг проектов

В выгрузку по форме Рейтинг проектов, помимо места проекта в рейтинге и количество баллов каждого проекта, необходимо выгружать ID проекта, название проекта, комментарии экспертов (общий комментарий от каждого из двух экспертов), ФИО экспертов, проводивших оценку.

Шаблон печатной формы Рейтинга проектов будет предоставлен Заказчиком на этапе подготовки технического проекта.

## Разработка раздела «Отчеты»

Необходимо создать раздел системы «Отчеты». Пример реализации интерфейса (раздел доступен по кнопке из верхней панели):



При нажатии на данную кнопку открывается выпадающее меню с возможными вариантами отчетов доступных пользователю, которые будет перечислены далее.

### Отчет по статусам задач

Реализовать в системе отчет по статусам задач, доступный по ссылке в выпадающем меню «Отчеты». Данный отчет должен представлять собой отдельную страницу в интерфейсе системы, в которой будут отображаться список задач с детализацией атрибутов задач согласно п. 4.1.1 в виде таблицы аналогичной странице «Список проектов». Задачи должны группироваться в несколько уровней. Пример:

* Тема Отбора
  + Проект1
    - Задача 1
    - Задача 2
    - Задача 3
  + Проект2
    - Задача 1

Пользователь должен иметь возможность группировать и разгруппировать как весь уровень группировки, так и отдельные группы отборов и проектов.

В списке задач предусмотреть цветовую индикацию статуса задачи - «светофор». Индикатор должен иметь зеленый цвет в случае, если задача не имеет просрочки по срокам смены статуса. Желтый – в случае, если просрочка составляет не более половины допустимого периода просрочки. Красный – если просрочка равна или превышает допустимый период просрочки. Для задач с «красной» индикацией выводить поле «Причина задержки».

Необходимо предусмотреть возможность перехода в карточку каждой задачи из данного отчета.

Пользователю необходимо предоставить возможность применения фильтров и сортировок к списку задач с возможностью сохранения выбранных настроек отображения для последующего использования. Для этого в верхней части интерфейса предусмотреть кнопку «Фильтры» при нажатии на которую будет выводиться:

* список пользовательских настроек отображения
* кнопка «новое», по нажатию на который будет выведен список полей к отображению в списке
* кнопка «сохранить настройки»

Реализовать возможность настраивать выводимые поля. Для этого предусмотреть возможность выбора столбцов отчета из списка атрибутов задач. А также необходимо предусмотреть для пользователя возможность сохранить выбранный набор полей для повторного использования.

Для удобного взаимодействия с большими таблицами необходимо реализовать горизонтальную прокрутку содержимого (скроллинг) внутри таблицы.

Пользователи должны иметь возможность выгрузить отчет в формате PDF и excel с примененными настройками фильтрации и отображения.

### Отчет по проектной деятельности

Реализовать в системе интегральный отчет по проектной деятельности, доступный по ссылке в выпадающем меню «Отчеты». Пользователи должны иметь возможность выгрузить отчет в формате PDF и Excel. Макет отчета приведен в Приложении 8.

Должна быть возможность выводить отчеты по разным типам проектов (лидерские проекты, практики, молодежные проекты и др.)

Содержимое отчета:

**Графики и диаграммы** представлены для следующих показателей:

* Всего проектов – общее количество проектов, находящихся в ИСУП во всех статусах, за исключением статуса «Подготовка». Показатели: перечень статусов, количество проектов с разбивкой по статусам, темам, типам и видам проектов. Форма отображения – гистограмма. Показатель всех проектов – интегральный. Форма отображения – число.
* Проекты по направлениям – эта диаграмма представляет собой разбивку проектов по виду проектов. Показатели: перечень направлений (технологии, качество жизни, экология, образование и кадры), количество проектов в каждом направлении. Форма отображения – гистограмма.
* Проекты по темам – эта диаграмма представляет собой разбивку проектов относительно тем. Сколько подано заявок по каждой теме.
* Визуализация отчета по итогам мониторинга целевых отборов (статус) (выгрузка) - в каком статусе какое количество проектов находится с разбивкой по регионам.
* Общая диаграмма с фильтрами: по каким темам у каких операторов больше всего проектов по конкретным статусам по годам: кол-во проектов по конкретным темам (добавляются) с фильтрами по операторам (фикс) и статусам (фикс). Можно выбрать несколько параметров в фильтре одновременно. Результат, выводимый на странице, может быть выгружен в виде PDF файла (как видим страницу, так и выгружаем).

Примерный вид отчета представлен в Приложении 8.

## Управление коллегиальными органами

Для принятия ключевых решений в ходе жизненного цикла проектов, в Агентстве проводятся различные заседания групп экспертов в формате коллегиальных органов (КО). В системе необходимо организовать функционал по управлению данными мероприятиями.

### Раздел «Коллегиальные органы»

В системе необходимо создать новый раздел «Коллегиальные органы». Пользователь при переходе в данный раздел попадает на отдельную страницу, в которой выведен список заседаний коллегиальных органов с указанием типа заседания, номера заседания, темы заседания, статуса и даты проведения. В системе необходимо создать справочник с типами заседаний, управление которым должно осуществляться через раздел «Настройки системы» в административной части.

Необходимо предусмотреть возможность сортировки, фильтрации и поиска по списку заседаний.

При нажатии на конкретное заседание должна открываться карточка заседания, в которой должно быть указано:

* Тип заседания
* Тема заседания
* Дата проведения
* Статус. Возможные значения:
  + Запланировано
  + Активно
  + Завершено
* Вопросы, вынесенные на заседания
* Группа участников – возможность добавлять либо группу и/или конкретных пользователей
* Проекты, прикрепленные к вопросам
* История голосования
* Результаты голосования по каждому из проектов (Проголосовавшие «За», «Против», «Воздержались», общее количество голосовавших)
* Выгрузка документов по голосованию (см. п. 4.11.3)
* Загрузка документов по голосованию

Необходимо для пользователя с соответствующим доступом предусмотреть возможность создавать, удаляться и редактировать карточки заседаний. Должна быть возможность редактировать любые поля карточки заседания (в том числе смена, статусов, загрузка файлов). Необходимо предусмотреть возможность настройки автоматической смены статуса проектов, прикрепленных к карточке заседания, при создании карточки заседания.

Необходимо предусмотреть привязку проектов к конкретному вопросу в карточке заседания. Для этого напротив каждого вопроса в списке вопросов добавить возможность подобрать проекты с возможность отфильтровать проекты по типу проекта и по наличию активной задачи требуемого типа в дорожной карте проектов. У пользователя должна быть возможность удалить конкретный проект из карточки заседания.

Необходимо предусмотреть возможность массового добавления проектов для конкретного вопроса.

При сохранении карточки заседания необходимо отправлять уведомления доступными каналами коммуникаций пользователям с ролью, соответствующей типу заседания с указанием прямой ссылки на форму голосования по данному заседанию.

### Функционал для проведения голосований

При переводе карточки заседания в статус «Активно» пользователям, имеющим права на проведение голосования, должны быть отправлены уведомления с прямой ссылкой на страницу для голосования.

На странице голосования пользователю выводится список вопросов, проекты, прикрепленные к вопросам и кнопки голосования («За», «Против, «Воздержался»). Добавление и изменение данных на странице голосования возможно только для заседаний в статусе «Активно». Система по итогам голосования всех членов коллегиальных органов рассчитывает среднее по каждому проекту/списку проектов. В карточке проекта должны отображаться результаты голосования по каждому вопросу/проекту.

Пользователям, имеющим права на проведение голосования, также должен быть доступен список заседаний коллегиальных органов, в которых он добавлен как член коллегиального органа (активные, архивные и запланированные заседания, по аналогии с интерфейсом экспертной оценки лидерским проектами).

По результатам голосования членов КО пользователь с соответствующим доступом должен иметь возможность управлять полями карточки заседания.

### Печатные формы

#### Формы для предоставления на Комиссию по аудиту проектов (КАП)

Необходимо предусмотреть 3 вида выгрузок:

* Статистика по поступившим проектам на отборы
* Форма представления проектов, рекомендуемых для перевода на этап «экспертиза» (по итогам оценки по критериям 1 уровня)
* Форма представления проектов, рекомендуемых к отклонению с этапа «аудит» (по итогам оценки по критериям 1 уровня)
* Форма повестки заседания коллегиального органа

Структура форм для предоставления на Комиссию по аудиту проектов (КАП) указана в Приложении 9.

#### Формы для предоставления на Рабочую группу экспертного совета

Необходимо предусмотреть 3 вида выгрузок:

* Рейтинг проектов, прошедших оценку по критериям 2 уровня
* Проекты, рекомендуемые к переводу на этап «сопровождение»
* Проекты, рекомендуемые к отклонению с этапа «экспертиза»
* Форма повестки заседания коллегиального органа

Структура форм для предоставления на Рабочую группу экспертного совета указана в Приложении 10.

#### Формы отчетов по мониторингу отборов проектов

Необходимо предусмотреть 2 вида выгрузок:

* Отчет по итогам мониторинга отборов проектов (количественные показатели)
* Отчет по итогам мониторинга отбора проектов (соблюдение сроков исполнения похождения этапов жизненного цикла проектов)

Структура форм отчетов по мониторингу отборов проектов указана в Приложении 11.

#### Форма протокола заседания коллегиального органа

Необходимо предусмотреть вывод печатных форм протоколов заседаний коллегиальных органов (для каждого типа заседания своя форма) по шаблонам, предоставленными Заказчиком. Шаблоны протоколов должны быть уточнены на этапе подготовки технического проекта.

## Подписание согласия на передачу персональных данных и на поддержку проектов

Для того, чтобы пользователь системы имел возможность создавать заявки на поддержку проектов, его контактные данные (электронная почта и сотовый телефон) должны быть подтверждены системой с помощью электронного письма со ссылкой и SMS-сообщения с кодом подтверждения соответственно. При отсутствии указанных подтверждений, пользователь должен видеть текстовое сообщение в соответствующем разделе сайта системы о том, что его намерение подать заявку требует от него выполнения указанных выше условий.

Своевременное предоставление сервисов отправки электронной почты и SMS-рассылки для разработки, отладки и эксплуатации соответствующих функций — ответственность Заказчика.

Перед отправкой заявки необходимо получить согласие на обработку персональных данных, согласие обработку персональных данных, разрешённых для распространения соглашения на поддержку проекта. Без принятия пользователем оферт, заявка на поддержку проекта не может быть отправлена. Подтверждением принятия условий является конклюдентное[[10]](#footnote-10) действие пользователя:

* установка всех флажков, соответствующих согласиям / офертам;
* переход по разблокированной ссылке с помощью специального элемента управления на форме, например, кнопки или гипер-ссылки.

Реализовать механизм управления согласиями пользователей. При реализации требований руководствоваться параграфом 4.14.

## Реализация требований информационной безопасности

### 4.13.1. Миграция с СУБД MySQL на СУБД PostgreSQL

Необходимо выполнить миграцию схем и конвертацию данных текущей базе данных c СУБД MySQL на СУБД PostgreSQL версии 14.1.1. Провести анализ применяемых репозиториев и запросов к базе данных в программном коде и, в случае необходимости, адаптировать их под СУБД PostgreSQL.

### 4.13.2. Раздельное хранение и резервное копирование данных

Необходимо реализовать раздельное хранение данных проекта, согласно пунктам 6.1. – 6.4. таблицы из Приложения 1 настоящего ТЗ. Разделить на сегменты нужно персональные данные пользователей и бизнес-данные (проекты, презентации, экспертизы и т.д).

Резервное копирование должно осуществляться раздельно, согласно пункту 2.4 настоящего ТЗ, для персональных данных пользователей и бизнес-данных, должны создаваться отдельные файлы дампов. Восстановление из резервных копий должно поддерживать раздельный формат.

### 4.13.3. Журналирование действий и изменений

Согласно требованиям пункта 2.2 настоящего ТЗ необходимо реализовать журналирование действий пользователя и автоматических подсистем, работающих по расписанию.

## Регистрация согласий субъектов об обработке персональных данных

Система должна регистрировать согласия субъектов в отношении своих персональных данных (раздельно):

* Согласие на обработку персональных данных, разрешённых для распространения, регистрировать отдельно от иных согласий на обработку. При этом система должна предоставить возможность определить перечень видов персональных данных по каждой категории (в соответствии с действующим соглашением), разрешённых субъектом для распространения.
* Общее согласие на обработку персональных данных, не подразумевающее распространение. Состав обрабатываемых таким образом персональных данных не может быть уже перечня видов персональных данных разрешаемых (запрещаемых) субъектом для распространения.

Перечень категорий и видовой состав персональных данных в отношении Системы определяется и фиксируется внешним по отношению к Системе сервисом (далее «Сервис регистрации событий ПДн»), интегрированным с ней. Каждая операция, осуществляемая Системой в отношении персональных данных должна отражаться в локальном журнале событий Системы и регистрироваться в Сервисе регистрации событий ПДн. Регистрируемая информация должна включать в себя:

* момент регистрации;
* вид операции;
* видовой состав персональных данных, в отношении которых регистрируется событие;
* идентификатор субъекта персональных данных;
* цели обработки (согласно с действующим соглашением, в отношении которого было дано согласие);
* направление передачи (информационная система, юридическое лицо);
* идентификатор ответственного сотрудника или идентификатор сервиса, получивших авторизацию действия.

Невозможность определения направления передачи должно вызывать ошибку авторизации операции. Запрос на авторизацию направления передачи Система должна отправлять в Сервис регистрации событий ПДн.

Регистрация событий обработки персональных данных, а также события предоставления (отзыва) согласий на обработку персональных данных должны предоставлять возможность сбора подтверждений регистрации таких событий.

В случаях недоступности Сервис регистрации событий ПДн, Система должна накапливать журнал для последующей регистрации (отложенная регистрация). При необходимости авторизации действия (Сервис регистрации событий ПДн не доступен), Система должна требовать её у администратора обработки персональных данных, закреплённого за Системой.

Система должна предоставлять интерфейс для регистрации событий отзыва или изменения согласий / разрешений на обработку персональных данных (в части распространения, предоставления или доступа) частично или полностью. Для регистрации отзыва Система должна предоставить интерфейс для регистрации такого требования (и получить подтверждение), содержащее следующие персональные данные:

* ФИО;
* контактную информацию (номер телефона, адрес эл. почты или почтовый адрес);
* перечень видов персональных данных, в отношении которых регистрируется требование.

Событие регистрации требования об отзыве согласия должно журналироваться Системой в соответствии с требованиями пункта 2.3.

Система должна предоставлять интерфейс для регистрации событий полного прекращения обработки персональных данных. Подтверждение этой операции должно запрашиваться у пользователя по каналам связи (эл. почта и/или телефон). Система должна предоставлять возможности обезличивания и уничтожения персональных данных в течение 10 рабочих дней с момента регистрации соответствующего требования, включая данные, находящиеся в резервных копиях персональных данных Системы. Авторизацию такого действия Система может получить со стороны Сервиса регистрации событий ПДн, о чём должна внести запись в журнал.

О фактах регистрации событий, связанных с отзывом согласий, должны отправляться оперативные уведомления администраторам обработки персональных данных, закреплённых за Системой.

Система должна предоставлять возможность сбора информации о том, какие персональные данные, когда и кому были переданы (или кем обрабатывались) на основании данных локальных журналов.

Пользователю системы должны быть доступны все версии Политики конфиденциальности, пользовательских соглашений и текстов согласий на обработку персональных данных, а также механизм хранения истории этих документов.

Модель данных, предназначенная для хранения персональных данных, должна формироваться на основании схемы метаданных, синхронизируемой с Сервисом регистрации событий ПДн.

## Административная часть

Необходимо разработать раздел «Настройки системы». В данном разделе должен быть реализован следующий функционал:

### Загрузка и настройка шаблонов писем, рассылка уведомлений (группе пользователей или одному)

Необходимо разработать отдельный подраздел административной части, в котором будет реализован функционал управления уведомлениями согласно пункту 4.6.

### Работа со справочниками

Необходимо реализовать отдельный подраздел административной части, в котором будет реализован функционал управления следующих справочников:

- Типы задач (с указанием задач, которые задействованы в логике работы системы, типов проектов)

- Типы заседаний коллегиальных органов

- Статусы проектов (с указанием типов проектов)

- Справочники по атрибутам заявки проектов:

* Статусы проектов (с указанием типов проектов)
* Типы проектов
* Виды проектов (с указанием привязки к типам проектов)
* Направления проекта: возможность настройки разных направлений для разных типов проекта
* Подкатегории практик
* Теги
* Тип организации, от которой подается проект
* Цели обращения
* Тип поддержки
* Юридический статус занятости
* Стадия реализации проекта
* Стоимость реализации проекта
* Регионы
* Направления и показатели рейтинга качества жизни
* Направления и показатели национального инвестиционного рейтинга
* Список ФОИВ
* Список комиссий Госсовета

- Справочники по полям карточки партнеров

* Направление АСИ, ответственное за партнера
* Направление сотрудничества с партнером
* Бренд компании
* Статус партнера

В рамках данного функционала необходимо реализовать следующий единый подход по управлению справочниками:

- все интерфейсные элементы по управлению всеми справочниками должны быть одинаковыми;

- у каждого элемента справочника должен быть набор обязательных атрибутов:

1. Идентификатор

2. Наименование

3. Список объектов системы, использующих элементы данного справочника или отметка о том, что таких объектов нет.

- в случае, если одним из атрибутов справочника является элемент другого справочника, то при создании элемента необходимо предусмотреть возможность выбора значения атрибута из содержимого других справочников

- общий поиск по элементам справочников

- возможность добавления новых элементов в справочник, изменения и удаления текущих элементов справочника.

- элементы справочников, используемые в прочих объектах системы, удалить нельзя. Пользователю при попытке удаления данных элементов должно выводиться диалоговое окно с уведомление о невозможности удаления и списком объектов, использующих данные элементы справочника. Если элемент нигде не используется, то он должен быть доступен для удаления. Элементы, используемые в системной логике, удалению не подлежат.

- в интерфейсе отображения каждого справочника предусмотреть возможность разбиения элементов справочника на страницы с отображением количества элементов на каждой станице.

- в общем интерфейсе отображения общего списка справочников предусмотреть возможность группировки и разгруппировки.

### Настройка отборов

Реализовать отдельный подраздел административной части для управления отборами проектов.

В данном разделе необходимо предусмотреть функционал:

- Создание, изменение, копирование и удаление тем отборов и привязка тем отборов к типам проектов

- Создание, изменение, копирование и удаление шаблонов заявки и паспорта проекта и привязка шаблона к теме отбора

- Управление шаблонами дорожных карт – отображение существующих шаблонов, возможность создать новый шаблон, возможность назначить шаблон по умолчанию для отборов, удаление, редактирование существующих шаблонов

- Управление критериями оценки отборов – возможность создания, изменения и удаления критериев в привязке к конкретному отбору, возможность указания методики оценки для каждого отбора и обязательности оценки и обязательности комментария к критерию.

- Управление бизнес процессом отбора – возможность настраивать статусы для каждого отбора, возможность указания статусов, на которых заявках проекта может редактироваться, настройка автоматизированного перехода с одного статуса на другой при свершении определенных событий.

Необходимо реализовать возможность скопировать отбор со всеми атрибутами.

В административной части необходимо разработать подраздел для настройки шаблонов заявки в соответствии с требованиями из пункта 4.2.

### Настройка Шаблонов дорожных карт

Необходимо разработать подраздел в административной части для управления шаблонами дорожных карт. В рамках данного подраздела предусмотреть возможность назначения шаблонов по умолчанию с выбором из существующего списка шаблонов дорожных карт и привязкой их к существующим элементам справочников «Типы проектов» и «Статусы проектов». Для задач в шаблоне пользователь может

В случае наличия такой привязки при создании проекта соответствующего типа дорожная карта в карточке проекта должна заполняться из соответствующего шаблона.

При присвоении шаблона определенному типу проектов предусмотреть проверку на наличие дублирующийся шаблонов.

Необходимо реализовать возможность добавления новых шаблонов, удаления и изменения, копирования существующих шаблонов и привязок к типам и статусам проектов.

При создании шаблонов задач пользователь должен иметь возможность указать, какие из задач являются фиксированными. Список фиксированных задач и их влияние на функционал системы должны быть отдельно уточнены в рамках разработки технического проекта.

### Управление коллегиальными органами

Необходимо разработать подраздел в административной части для управления коллегиальными органами. В рамках данного подраздела необходимо предусмотреть возможность создания шаблонов карточек заседаний, изменения и удаления старых шаблонов.

### Настройка логики бизнес-процессов системы

Необходимо предусмотреть подраздел административной части для привязки событий закрытия задач дорожной карты определенных типов к событиям бизнес-логики системы.

Для этого в системе необходимо предусмотреть:

* возможность указания события-инициатора и типа задачи из дорожной карты, которая должна быть закрыта по факту наступления события-инициатора. Например, при проведении экспертизы экспертами в соответствующем разделе необходимо переводить статус задачи с типом «Проведение экспертизы» на «Закрыто».
* возможность указания типа задачи из дорожной карты, при переводе которых в статус «Закрыто» должно происходить определенное событие бизнес-логики системы. Пример, при переводе задачи с типом «Влияет на КПЭ» в статус «Закрыто» в системе добавляется счетчик факта выполнения КПЭ в определенном отчете.

В административной части у пользователя должна быть возможность выбора событий из установленного списка. Список событий бизнес-логики системы должен быть уточнен на этапе подготовки технического проекта.

### Функционал управления ролевой моделью

Необходимо разработать отдельный подраздел административной части, в котором будет реализован функционал управления ролевой моделью согласно пункту 4.16.

## Доработка ролевой модели

### Управление доступом к данным и полномочия пользователей

В системе должна быть реализована мандатно-избирательная(групповая) модель доступа к данным, основанная на принципах разграничения доступа на основе атрибутов. Ключевыми элементами такой модели должны являться:

* **Мандаты**: или режим конфиденциальности для информационных полей (атрибутов) системы, используемых для расширения базовой модели метаданных (классификаторов, категорий, справочников, реестров объектов, сведений о событиях и так далее — см. 4.2.1).
* **Группы доступа**: «Сотрудники», «Трекеры», «Эксперты», …[[11]](#footnote-11)
* **Правила**: структуры вида:
  + Цель: функция системы, в отношении которой проверяется правило; определяется по идентификатору функции в системе.
  + Действие: эффект, который должен быть достигнут в результате вычисления логического выражения; таковым может быть одно из значений: «разрешить», «отказать», «не применимо»[[12]](#footnote-12) или «не определено»[[13]](#footnote-13).
  + Условие: вычислимое логическое выражение, возвращающее значение булевого типа. Например:

((Субъект.Группа В («Трекеры», «Эксперты)[[14]](#footnote-14) И Объект.ВидМероприятия = «Отбор»[[15]](#footnote-15) И ТекущаяДата() В ПериодДействия(Объект.Мероприятие)) ИЛИ Субъект.Группа = «Администратор») И Мандат В («Персональные данные», «Конфиденциальная информация»)[[16]](#footnote-16)

* + Обязательства[[17]](#footnote-17):
    - ДО: Журнал(«События безопасности»).Зарегистрировать(«Функция „%S“ для пользователя „%S“: статус „%S“», «Регистрация проекта на открытый отбор», «Иванов П.С.», «Разрешено»
    - ПОСЛЕ: Журнал(«События подсистемы»).Зарегистрировать(«Функция „%S“ для пользователя „%S“: статус „%S“», «Регистрация проекта на открытый отбор», «Иванов П.С.», «Выполнено успешно»
* **Политики**: группы правил с возможностью реализации методов (механизмов) приоритезации, разрешения[[18]](#footnote-18) и/или вытеснения.

Таким образом, в код системы должны попасть только идентификаторы функций системы определённые в виде литералов вида «UC\_<SUBSISTEM>\_<FUNCTION|OPERATION NAME>», которые должны быть доступны в подсистеме управления доступом и разрешения полномочий, классификатор мандатов и действий в виде перечислений.

Код условий и обязательств должен быть выполнен на любом интерпретируемом императивном языке, поддерживающем вычисление логических выражений.

Базовые (обязательные) атрибуты[[19]](#footnote-19) субъектов:

* признак «Заблокировано»
* признак «Действует с … по ...»
* признак принадлежности группе(ам)
* признак «Мандат» общий и в контексте групп(ы)

Базовые (обязательные) атрибуты групп:

* наименование / идентификатор
* список «Состав группы»[[20]](#footnote-20)

Кроме того, код правил должен позволять обращаться к базовым (заданных архитектурой) и расширенным (заданных пользователем) метаданным объектов системы.

Правила и политики должны выгружаться / загружаться пользователем, принадлежащим группе «Администраторы» с мандатом «Настройки системы» в формате XACML.

При загрузке правил должна проводиться их верификация:

* поддерживаемая версия;
* целостность формата по DTD для XACML.

Сервис SSO (KeyCloak) должен предоставлять возможности аутентификации пользователей и сопровождать идентификаторы пользователей информацией о его мандатах и принадлежности к группам.

Исполнитель должен выполнить базовую настройку политик и правил доступа к данным и полномочий пользователей на основе «Матрицы ролей». В качестве возможной реализации в Приложении 12 «Матрица ролей» представлена модель с учётом существующих (реализованных в системе) правил.

## API для интеграции

ИСУП API предназначен для веб-сервисов и приложений, которые работают с задачами и данными по проектам. При этом возможность выполнять те или иные действия через API зависит от прав доступа пользователя, от имени которого выполняются запросы.

ИСУП API должен позволять отдать смежным системам все данные из заявки проекта и паспорта проекта. Примерный список полей заявки и паспорта проекта представлен в таблице 4:

Таблица 4

|  |
| --- |
| ID проекта |
| Название проекта |
| Статус проекта |
| Направление или категория проекта |
| Тема отбора |
| Стадия реализации проекта |
| Страна реализации |
| Регионы реализации |
| Цели проекта |
| Задачи проекта |
| Проблемы, которые решает проект |
| Целевая аудитория проекта |
| Суть проекта (Краткое описание) |
| Конкурентные преимущества |
| Продукт проекта |
| Необходимость инвестиций / Ваш проект является инвестиционным |
| Вопрос к проекту |
| Как проект решает описанную проблему |
| Приведите описание базовой технологии |
| Опишите основные направления коммерциализации Вашего проекта |
| Тип проекта |
| Вид проекта |
| Презентация проекта |
| Заключения/отзывы о проекте/продукте/технологии |
| Дополнительные материалы проекта |
| Загрузка фото и видео о проекте |
| Обложка карточки проекта |
| Веб-сайт проекта |
| Ссылки на социальные сети проекта |
| Регион первого внедрения |
| Эффекты от реализации |
| Где уже было апробировано решение, запущены пилотные проекты, каких результатов удалось достичь? |
| Бизнес-план проекта |
| Финансовая модель проекта |
| Ресурсное обеспечение проекта |
| Цель обращения в АСИ |
| Что мешает реализации проекта |
| Какие регуляторные изменения для поддержки развития вашего типа бизнеса/проекта необходимы на системном уровне |
| Откуда вы узнали об отборе проектов АСИ? |
| Каким образом можно внедрить практику в другом регионе? |
| Опишите основные шаги плана реализации практики |
| Стоимость реализации проекта |
| Выбор наставника |
| Укажите, сколько времени потребовалось для запуска практики |
| Были ли задействованы сторонние организации для реализации? |
| Организация |
| Формат участия |
| Какую поддержку, кроме консультационной, вы готовы оказать при внедрении? |
| Есть ли особенности, которые необходимо учесть при внедрении? |
| Отношение проекта к Рейтингу качества жизни |
| Отношение проекта к Национальному инвестиционному рейтингу |
| Одобрение комиссиями Госсовета |
| Одобрение ФОИВ |
| Теги |
| Подкатегория проекта |
| ФИО лидера |
| Возраст лидера |
| Резюме лидера |
| Регион проживания |
| Должность лидера |
| Юридический статус занятости (выбор из списка) |
| Название организации |
| ИНН |
| Юридический адрес |
| Фактический адрес |
| ФИО члена команды |
| Должность или роль члена команды в заявленном проекте |
| Опыт работа члена команды |
| Указание организации - партнера |
| Направление сотрудничества с партнером |
| Роли на проекте: лидер, трекер, эксперт, старший трекер, сотрудник АСИ |

А также необходимо предусмотреть API следующих данных: об оценке 1-го уровня, 2-го уровня (данные о пользователях, оценках, комментарии), истории изменений статусов по проектам, данные о задачах из дорожной карты, данные о взаимодействии с партнерами, данные об участии пользователя в заседания коллегиальных органов и другие данные о деятельности пользователей в системе.

Методы API должны поддерживать базовую авторизацию и принимать токен доступа в заголовке X-Auth

Authorization: Basic Auth

login: \_\_\_

password: \_\_\_

Полный список данных будет уточнен при подготовке технического проекта в рамках реализации договора.

## История изменений

Реализовать функцию отслеживания истории изменений данных о проектах: дата изменения, автор изменения, старое значение и новое значение.  
Отслеживаемые изменения по каждому полю заявки, проекта, добавленным/измененным полям, статусам экспертизы, изменениям оценки и т.д.

Необходимо реализовать в карточке проекта пользовательский интерфейс для просмотра изменений в проекте в соответствии с ролевой моделью.

## Адаптация системы под мобильную версию

В ИСУП должна быть реализована отзывчивая верстка – верстка HTML-страниц, обеспечивающая отображение на различных устройствах, подключенных к интернету и динамически подстраивающаяся под заданные размеры окна.

Адаптивная верстка ИСУП должна корректно отображаться на следующих устройствах и браузерах:

* **Ios**
  + iPhone 13 Pro Max, iPhone 12 Pro Max **(428x926)**
  + iPhone 13 Pro, iPhone 12, iPhone 12 Pro, iPhone 12 **(390x844)**
  + iPhone 13 Mini, iPhone 11 Pro, iPhone XS, iPhone X **(375x812)**
  + iPhone 12 Mini **(360x780)**
  + iPhone SE **(320x568)**
  + iPhone SE 2020, iPhone 8, iPhone 7, iPhone 6S, iPhone 6+, iPhone 6 **(375x667)**
  + iPhone 11 Pro Max, iPhone 11, iPhone XR, iPhone XS Max **(414x896)**
  + iPhone 8+, iPhone 7+, iPhone 6S+ **(414x736)**
* **Android**
  + Samsung Galaxy A03, [Xiaomi Redmi 10A](https://phonesdata.com/ru/smartphones/xiaomi/redmi-10a-5462200/) **(720x1600)**
  + Samsung Galaxy A13, Samsung Galaxy A23, [Samsung Galaxy A23 5G](https://phonesdata.com/ru/smartphones/samsung/galaxy-a23-5g-5462628/), [Samsung Galaxy F13](https://phonesdata.com/ru/smartphones/samsung/galaxy-f13-5462478/)**,** [Samsung Galaxy F23](https://phonesdata.com/ru/smartphones/samsung/galaxy-f23-5462140/)**,** [Samsung Galaxy M13 (Global)](https://phonesdata.com/ru/smartphones/samsung/galaxy-m13-5462364/)**,** [Samsung Galaxy M23](https://phonesdata.com/ru/smartphones/samsung/galaxy-m23-5462133/)**,** [Samsung Galaxy M33 5G](https://phonesdata.com/ru/smartphones/samsung/galaxy-m33-5g-5461986/)**,** Samsung Galaxy M53**,** Samsung Galaxy Xcover6 Pro, [Xiaomi Poco M4 5G](https://phonesdata.com/ru/smartphones/xiaomi/poco-m4-5g-5462174/)**,** [Xiaomi Redmi 10 5G](https://phonesdata.com/ru/smartphones/xiaomi/redmi-10-5g-5462176/)**,** [Xiaomi Redmi 10 Prime+ 5G](https://phonesdata.com/ru/smartphones/xiaomi/redmi-10-prime-5g-5462177/)**,** Xiaomi Redmi 11**,** [Xiaomi Redmi Note 11E](https://phonesdata.com/ru/smartphones/xiaomi/xiaomi-redmi-note-11e-5462109/) **(1080x2408)**
  + [Samsung Galaxy A33 5G](https://phonesdata.com/ru/smartphones/samsung/galaxy-a33-5g-5462171/), [Samsung Galaxy A53 5G](https://phonesdata.com/ru/smartphones/samsung/galaxy-a53-5g-5461953/)**,** [Samsung Galaxy A73 5G](https://phonesdata.com/ru/smartphones/samsung/galaxy-a73-5461927/)**,** [Samsung Galaxy M34 5G](https://phonesdata.com/ru/smartphones/samsung/galaxy-m34-5g-5462135/)**,** [Samsung Galaxy S20 FE](https://phonesdata.com/ru/smartphones/samsung/galaxy-s20-fe-2022-5462222/)**,** [Samsung Galaxy S21 FE 5G](https://phonesdata.com/ru/smartphones/samsung/galaxy-s21-fe-5g-5461707/)**,** [Samsung Galaxy Xcover Pro 2](https://phonesdata.com/ru/smartphones/samsung/galaxy-xcover-pro-2-5462212/), [Xiaomi 11i](https://phonesdata.com/ru/smartphones/xiaomi/11i-5461784/)**,** [Xiaomi 11i HyperCharge](https://phonesdata.com/ru/smartphones/xiaomi/11i-hypercharge-5461783/)**,** [Xiaomi 12 Lite](https://phonesdata.com/ru/smartphones/xiaomi/xiaomi-12-lite-5462149/)**,** [Xiaomi 12S](https://phonesdata.com/ru/smartphones/xiaomi/12s-5462501/)**,** [Xiaomi Black Shark 5](https://phonesdata.com/ru/smartphones/xiaomi/black-shark-5-5462215/)**,** [Xiaomi Black Shark 5 Pro](https://phonesdata.com/ru/smartphones/xiaomi/black-shark-5-pro-5462213/)**,** [Xiaomi Black Shark 5 RS](https://phonesdata.com/ru/smartphones/xiaomi/black-shark-5-rs-5462214/), [Xiaomi Civi 1S](https://phonesdata.com/ru/smartphones/xiaomi/xiaomi-civi-1s-5462252/), [Xiaomi Poco F4](https://phonesdata.com/ru/smartphones/xiaomi/poco-f4-5462480/), [Xiaomi Poco F4 GT](https://phonesdata.com/ru/smartphones/xiaomi/poco-f4-gt-5462245/)**,** [Xiaomi Poco M4 Pro](https://phonesdata.com/ru/smartphones/xiaomi/poco-m4-pro-5462136/)**,** [Xiaomi Poco X4 NFC](https://phonesdata.com/ru/smartphones/xiaomi/poco-x4-nfc-5461887/)**,** [Xiaomi Poco X4 Pro 5G](https://phonesdata.com/ru/smartphones/xiaomi/poco-x4-pro-5g-5462082/)**,** [Xiaomi Redmi 10 2022](https://phonesdata.com/ru/smartphones/xiaomi/redmi-10-2022-5462065/)**,** [Xiaomi Redmi 10 Prime 2022](https://phonesdata.com/ru/smartphones/xiaomi/redmi-10-prime-2022-5462297/)**,** [Xiaomi Redmi 20X](https://phonesdata.com/ru/smartphones/xiaomi/redmi-20x-5461709/)**,** [Xiaomi Redmi K40S](https://phonesdata.com/ru/smartphones/xiaomi/redmi-k40s-5462178/)**,** [Xiaomi Redmi K50 Ultra](https://phonesdata.com/ru/smartphones/xiaomi/redmi-k50-ultra-5462399/)**,** [Xiaomi Redmi Note 11 4G](https://phonesdata.com/ru/smartphones/xiaomi/redmi-note-11-5462033/)**,** [Xiaomi Redmi Note 11 Pro 4G](https://phonesdata.com/ru/smartphones/xiaomi/redmi-note-11-pro-5462032/)**,** [Xiaomi Redmi Note 11 Pro 5G](https://phonesdata.com/ru/smartphones/xiaomi/redmi-note-11-pro-5g-5462031/)**,** [Xiaomi Redmi Note 11E Pro](https://phonesdata.com/ru/smartphones/xiaomi/xiaomi-redmi-note-11e-pro-5462110/)**,** [Xiaomi Redmi Note 11S](https://phonesdata.com/ru/smartphones/xiaomi/xiaomi-redmi-note-11s-5462024/)**,** [Xiaomi Redmi Note 11S 5G](https://phonesdata.com/ru/smartphones/xiaomi/redmi-note-11s-5g-5462157/)**,** [Xiaomi Redmi Note 11SE](https://phonesdata.com/ru/smartphones/xiaomi/redmi-note-11se-5462367/)**,** [Xiaomi Redmi Note 12 Pro](https://phonesdata.com/ru/smartphones/xiaomi/xiaomi-redmi-note-12-pro-5462413/)**,** Honor 30, Honor 30i, Honor 10X Lite **(1080x2400)**
  + [Samsung Galaxy S22 5G](https://phonesdata.com/ru/smartphones/samsung/galaxy-s22-5g-5462045/)**,** [Samsung Galaxy S22+ 5G](https://phonesdata.com/ru/smartphones/samsung/galaxy-s22-5g-5461921/) **(1080x2340)**
  + [Samsung Galaxy S22 Ultra 5G](https://phonesdata.com/ru/smartphones/samsung/galaxy-s22-ultra-5g-5461920/) **(1440x3088)**
  + Samsung Galaxy Z Flip4 **(1080x2640)**
  + [Samsung Galaxy Z Fold4](https://phonesdata.com/ru/smartphones/samsung/galaxy-z-fold4-5462630/) **(1812x2176)**
  + [Xiaomi 12 Pro (Dimensity)](https://phonesdata.com/ru/smartphones/xiaomi/12-pro-dimensity-5462512/)**,** [Xiaomi 12S Pro](https://phonesdata.com/ru/smartphones/xiaomi/12s-pro-5462513/)**,** [Xiaomi 12S Ultra](https://phonesdata.com/ru/smartphones/xiaomi/12s-ultra-5462500/)**,** [Xiaomi Redmi K50](https://phonesdata.com/ru/smartphones/xiaomi/redmi-k50-5462180/)**,** [Xiaomi Redmi K50 Pro](https://phonesdata.com/ru/smartphones/xiaomi/redmi-k50-pro-5462083/) **(1440x3200)**
  + [Xiaomi Poco C40](https://phonesdata.com/ru/smartphones/xiaomi/poco-c40-5462232/)**,** [Xiaomi Redmi 10 Power](https://phonesdata.com/ru/smartphones/xiaomi/redmi-10-power-5462251/)**,** [Xiaomi Redmi 10C](https://phonesdata.com/ru/smartphones/xiaomi/xiaomi-redmi-10c-5462155/) **(720x1650)**
* **Поддержка браузеров:**
  + Ios: Safari, Chrome, Yandex, Edge, Opera, Firefox.
  + Android: Chrome, Yandex, Edge, Opera, Firefox.

Компоновка страниц должна обеспечивать автоматическое масштабирование страниц в зависимости от ширины рабочего поля браузера пользователя. Перестроение и позиционирование блоков при изменении ширины рабочего поля браузера пользователя, утверждается при согласовании дизайн-макетов ИСУП. Страницы, которые не согласовывались в формате дизайн-макетов, должны иметь поведение при перестроении и позиционировании блоков аналогичное согласованному.

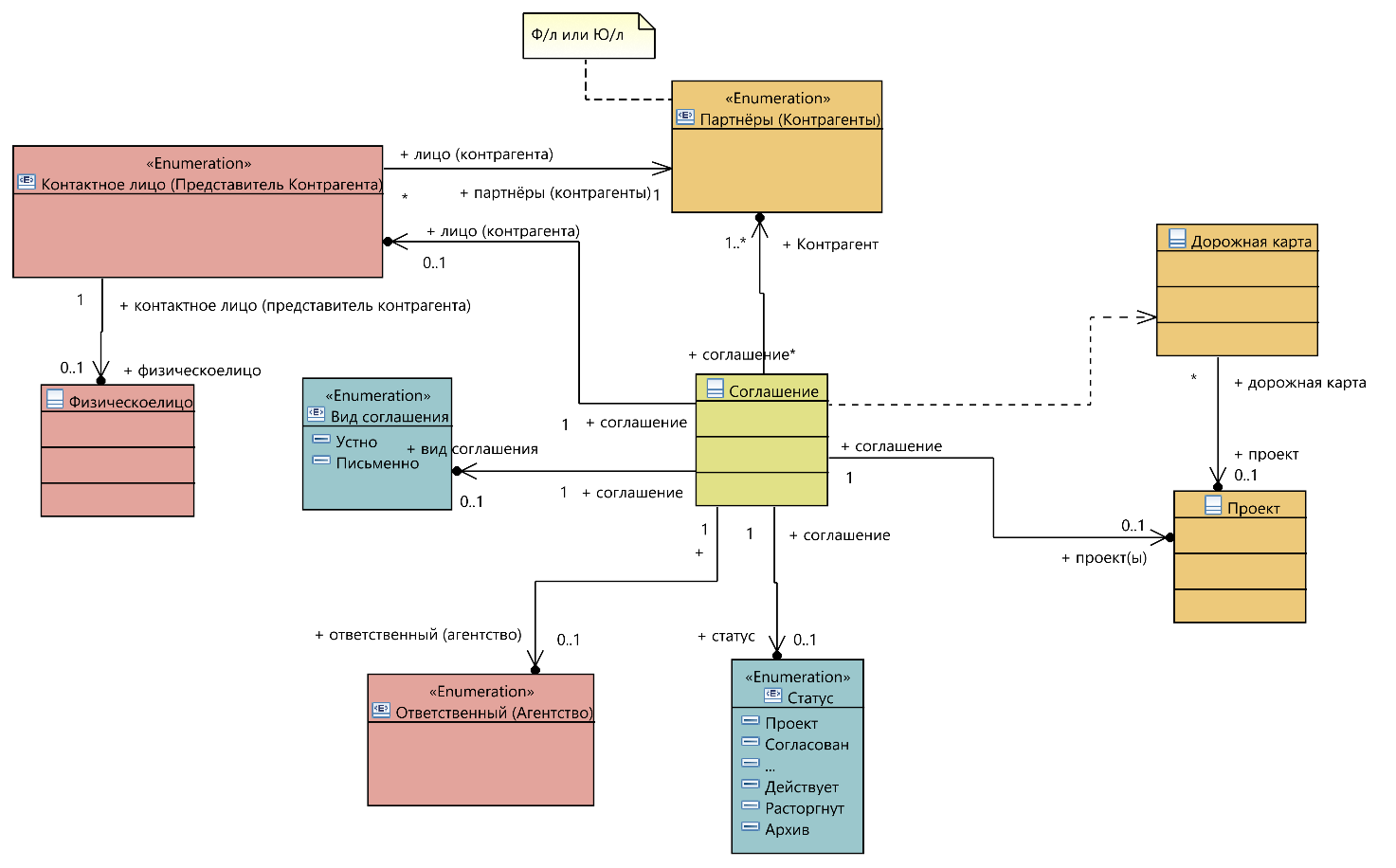
Страницы Сайта должны корректно отображаться без полосы горизонтальной прокрутки и автоматически масштабироваться.

Перестроение и позиционирование блоков при изменении ширины рабочего поля браузера пользователя для разрабатываемых дизайн-макетов утверждается на этапе согласования дизайн-макетов.

В рамках договора необходимо реализовать мобильную верстку существующих и вновь создаваемых страниц сайта.

## Партнеры

Для эффективного управления проектами, реализуемыми совместно с организациями партнерами, в системе необходимо наряду с сущностью «Проект» создать сущность «Партнер».



**Модель 6: Предметная область раздела «Партнеры»**

Для управления сущностью «Партнер» необходимо создать отдельный раздел «Партнеры». В данном разделе необходимо отражать список партнеров, заведенных в системе. В списке партнеров должна содержаться, как минимум, следующая информация:

* ID партнера – формируется автоматически системой
* ИНН
* Название организации
* КПП
* Бренд
* ФИО контактного лица от партнера
* Телефон контактного лица от партнера
* ФИО контактного лица от АСИ
* Телефон контактного лица от АСИ
* Регионы присутствия партнера
* Направления сотрудничества с АСИ
* Ответственные лица от АСИ с указанием направлений
* Отрасль (с указанием кода ОКВЭД)
* Статус партнера

Необходимо предусмотреть возможность фильтрации, сортировки и поиска таблицы. При фильтрации и поиске количество отображаемых партнеров должно меняться в интерфейсе.

В разделе необходимо предусмотреть счетчик партнеров, выведенных в интерфейсе, в соответствии с фильтрами.

В паспорте проекта необходимо добавить атрибут «Партнер», доступный для заполнения из списка партнеров.

При нажатии на строку в списке должна открываться отдельная страница с карточкой партнера, в которой будет отражаться детальная информация о партнере, проекты, реализуемые совместно с партнером и список контактных лиц со ссылкой на профили пользователей системы (при их наличии). Внутри карточки партнера информация должна быть разбита на смысловые блоки.

Реализовать возможность настраивать выводимые поля. Для этого предусмотреть возможность выбора столбцов из карточки партнера. А также необходимо предусмотреть для пользователя возможность сохранить выбранный набор полей для повторного использования.

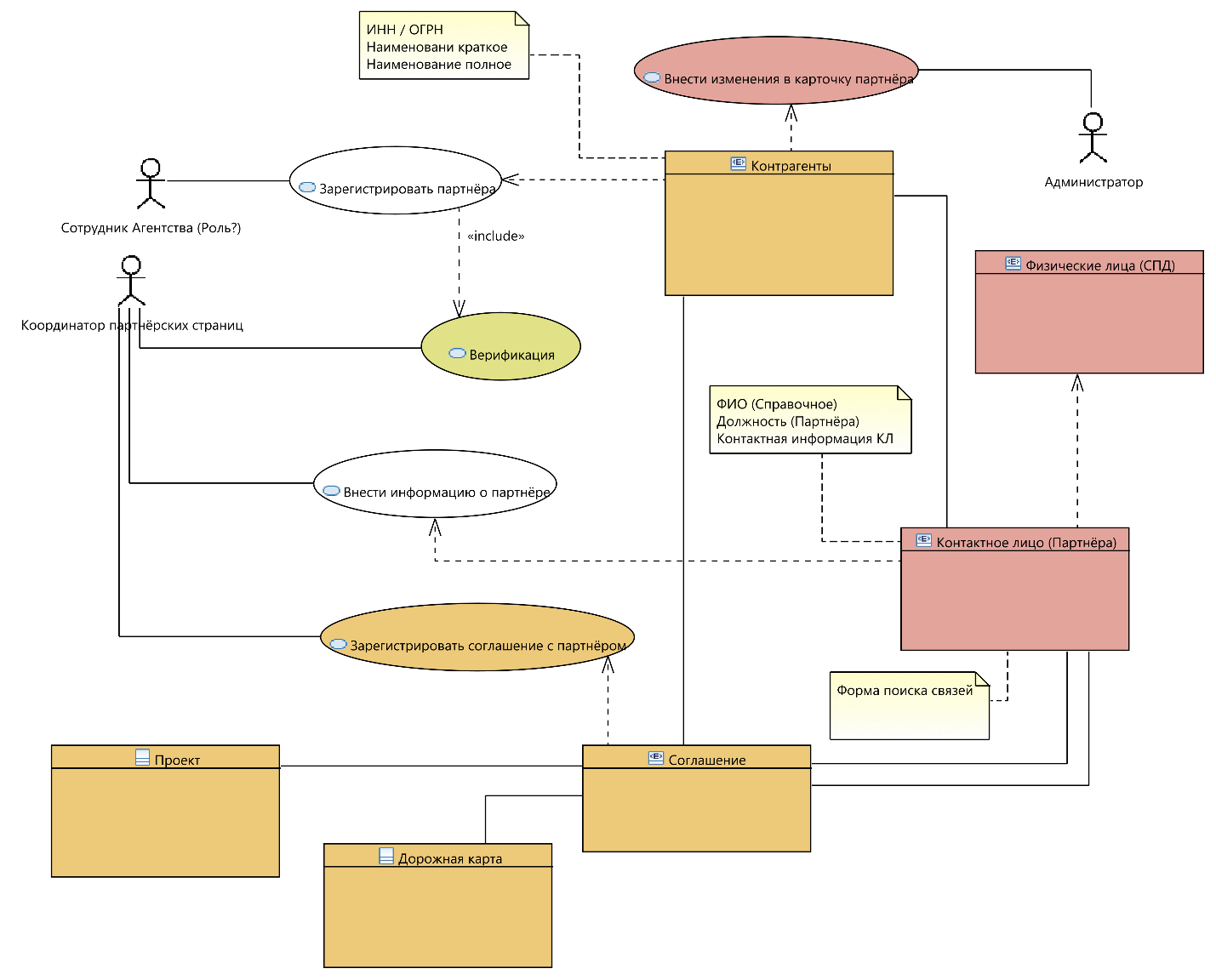
Для удобного взаимодействия с большими таблицами необходимо реализовать горизонтальную прокрутку содержимого (скроллинг) внутри таблицы.

Пользователи с соответствующей ролью должны иметь возможность выгрузить отчет в формате excel с примененными настройками фильтрации и отображения.

В Приложении 13 представлен примерный набор полей карточки партнера. Список полей может быть скорректирован Заказчиком в ходе уточнения технического проекта.

### Создание и редактирование карточки партнера

В разделе «Партнеры» необходимо предусмотреть кнопку для создания карточки партнера. При нажатии на кнопку добавления карточки пользователю открывается форма для заполнения обязательных и необязательных полей. Поля формы должны быть разбиты на смысловые разделы.



**Модель 7: Карта прецедентов раздела «Партнеры»**

В качестве основного идентификатора организации должен использоваться ИНН. После ввода ИНН форму должны подтягиваться данные об организации из существующего реестра юридических лиц. Для этого необходимо предусмотреть интеграцию с существующими справочниками юридических лиц (например, ЕГРЮЛ).

Количество, формат и обязательность полей, которые выводятся в форму заполнения должны настраиваться в разделе «Настройки системы». Для детализации требований к набору полей единой карточки партнера должно быть разработано частное техническое задание.

## Личный кабинет пользователя

### Общая информация

Личный кабинет пользователя ИС должен учитывать многоролевую модель. В рамках этой модели необходимо реализовать функционал переключения между ролями с соблюдением всех прав, доступов, привилегий, ограничений каждой роли и взаимоисключающих случаев согласно таблице, представленной в Приложении 12.

Ниже представлена общая логика работы личного кабинета пользователя ИСУП. В ходе работы над проектом Исполнителю необходимо предусмотреть проектирования нескольких итераций реализации личного кабинета на основе проведения Заказчиком интервью различных фокус-групп. По итогам проведения интервью Заказчиком будет подготовлено финальный технический проект на личный кабинет.

### Логика работы личного кабинета

Доступ к функционалу любой роли осуществляется единой комбинацией логина и пароля, используемой при авторизации пользователя через Leader-id.

Переход в раздел Личный кабинет возможен с помощью одноименной кнопки в правом верхнем углу общесистемного хэдера. При переходе в раздел пользователь попадает на стартовую страницу, где расположены следующие внутренние разделы:

1. Анкета пользователя.
2. Список доступных ролей.
3. Левостороннее меню.

На стартовой странице Личного кабинета отсутствует общесистемный хэдер. Взамен содержания общесистемного хэдера доступна строка сквозного поиска. Хэдер появляется при переключении пользователя на конкретную роль. Содержание хэдера должно соответствовать правам, доступам, привилегиям, ограничениям роли, на которую перешел пользователь. В хэдере каждой роли отображаются те разделы ИС, которые доступны пользователю для работы над проектами. Детализация содержания хэдера для каждого вида роли будет предоставлена в рамках технического проекта.

Переключение между ролями осуществляется с помощью внутренних вкладок личного кабинета. Вкладки расположены на стартовой странице под анкетой пользователя в виде кликабельных блоков с названием роли и типизированной заглушки в формате плиточного списка на стартовой странице личного кабинета.

### Содержание личного кабинета для сторонних пользователей ИС

Личный кабинет доступен на просмотр сторонним пользователям ИС при нажатии на ФИО пользователя в разделах системы, а также при переходе из результатов поиска.

При попадании на страницу личного кабинета сторонние пользователи видят следующие вкладки:

1. Анкета
2. Список бизнес ролей пользователя.

Часть полей анкеты пользователей может быть недоступна для просмотра другими группами ролей, в частности поля с контактной информацией (телефон, e-mail). Детализация по закрытию полей для групп ролей будет предоставлена в техническом проекте.

Список бизнес ролей пользователя представлен в виде плиточного списка, где карточки ролей содержат название роли и типизированную некликабельную заглушку. В списке отражаются только внутренние, экспертные и внешние роли пользователя согласно таблице Матрицы ролей.

### Стартовая страница личного кабинета

**Анкета**

Анкета пользователя является стартовым экраном личного кабинета. Примерный список блоков и полей анкеты пользователя:

*Блок Персональные данные*

1. Фамилия
2. Имя
3. Отчество
4. Фото
5. Телефон
6. E-mail
7. Leader-ID номер
8. Дата рождения
9. Пол
10. Страна проживания
11. Регион проживания
12. Населенный пункт

*Блок Образование*

1. Учебное заведение
2. Специализация
3. Годы обучения
4. Документ об образовании (поле для загрузки).

Кнопка для добавления дополнительного учебного заведения с дублирующимися полями блока Образование.

*Блок Опыт*

1. Организация
2. Должность
3. Годы работы
4. Выбор текущего места работы

Кнопка для добавления дополнительной организации с дублирующимися полями блока Опыт.

1. Дополнительная информация
2. Ссылки на социальные сети

Для группы экспертных ролей необходимо предусмотреть дополнительные поля в анкете. К ним относятся:

*Блок Профиль компетенций*

Компетенция (поле с выпадающим списком)

Кнопка для добавления дополнительной компетенции.

Список полей и разделов Анкеты пользователя должен быть уточнен в рамках технического проекта.

**Редактирование анкеты**

Анкета пользователя может редактироваться с помощью кнопки. При нажатии на кнопку пользователь попадает на страницу редактирования анкеты, где в том числе к редактированию представлены дополнительные поля, относящиеся к конкретным видам ролей.

**Список доступных ролей**

Данный блок расположен на стартовой странице личного кабинета под блоком Анкеты. В блоке представлены все группы ролей, доступные пользователю.

Карточка роли представляет собой блок с типизированной заглушкой-изображением и названием роли. Карточка кликабельна. При нажатии на карточку перед пользователем открывается страница с рабочим пространством (воркфлоу) для выбранной роли.

**Рабочее пространство роли**

Пользователь попадает в рабочее пространство конкретной роли при нажатии на одноименную ролевую карточку на стартовой странице личного кабинета.

Рабочее пространство конкретной роли включает следующие функциональные блоки:

1. Хэдер, содержание которого соответствует доступу роли.
2. Список проектов, к которым у роли есть доступ.
3. Левостороннее меню.

Хэдер содержит доступные для каждой роли основные разделы ИС. Детализация по содержанию хэдера для каждой группы ролей будет предоставлена в техническом проекте.

Список проектов представлен в рабочем пространстве в виде плиточного списка карточек проектов. Карточка проекта кликабельна и состоит из обложки проекта (подтягивается из заявки), названия проекта, статуса проекта. Список содержит все, доступные данной роли проекты. Расположение проектов в списке первично доступно пользователю в хронологическом порядке согласно дате добавления роли к проекту: от новых проектов к старым. Над списком расположены фильтры, позволяющие сортировать проекты рабочего пространства по заданным параметрам. Детализация параметров фильтров будет предоставлена в техническом проекте.

При клике на карточку, пользователь попадает на ту вкладку проекта, которая доступна ему согласно роли. Детализация по переходам ролей будет предоставлена в техническом проекте.

**Левостороннее меню**

Левосторонее меню статично и наследуется для всех вкладок личного кабинета пользователя. Представляет собой кликабельный список внутренних вкладок кабинета:

1. Настройка анкеты
2. Настройка пользовательских согласий.
3. Уведомления.

Указанные выше три пункта статичны для всех ролей и наследуются для всех вкладок личного кабинета. При этом для ряда групп ролей при переходе на рабочую область необходимо предусмотреть расширение списка за счет следующий пунктов:

1. Сертификаты.
2. Мои заявки.
3. Мои оценки.
4. Сохраненные шаблоны.

Детализация по

**Настройка анкеты**

При нажатии на пункт меню открывается страница редактирования анкеты пользователя.

**Настройка пользовательских согласий**

При нажатии на пункт меню открывается страница с чек-бокс системой согласий, а также списком документов, на которые пользователь дал согласие при регистрации в системе.

Функционал страницы должен позволять редактировать пользовательские согласия в чек-бокс системе и отзывать согласие.

Бизнес-логика процессов и детализация по функционалу страницы будут предоставлены в техническом проекте.

**Уведомления**

При нажатии на пункт меню открывается раздел Уведомления.

**Сертификаты**

При нажатии на пункт меню открывается раздел Сертификаты. Содержание и функционал страницы зависит от группы ролей.

Внешние роли: хранение выданных сертификатов с возможностью их выгрузки для печати.

Экспертные роли: хранение выданных сертификатов с возможностью их выгрузки для печати.

Внутренние роли: хранение и управление шаблонами сертификатов. Создание адресных сертификатов для пользователей внешних и экспертных ролей. Согласование сертификатов перед отправкой адресату внутри системы.

Технические роли: управление шаблонами сертификатов. Создание и изменение маршрутов согласования сертификатов. Управление уже выданными сертификатами.

Детализация по содержанию и функционалу для каждой группы ролей будет предоставлено в техническом проекте.

**Мои заявки**

При нажатии на пункт списка открывается отдельная страница, где собраны все заявки пользователя.

Пункт доступен для группы внешних ролей. В данном разделе хранятся все заявки, поданные пользователем в ИС.

Заявки представлены в виде списка в плиточном формате. Карточка заявки представляет собой типизированное изображение с заглушкой или обложкой проекта (если данное поле заполнено), название проекта и статус.

Для работы со списком необходимо предусмотреть фильтры для сортировки заявок по типу отборов, статусу, дате. Детализация по фильтрам будет предоставлена в техническом проекте. Базовая сортировка проектов должна быть реализована в хронологическом порядке по дате подачи ее в ИС: от новых к старым.

**Мои оценки (принципиальное отличие от списка проектов рабочей области: общая солянка всех оценок в одном месте)**

При нажатии на пункт списка открывается отдельная страница, где собраны все оценки пользователя в виде карточек проектов.

Пункт доступен для внутренних и внешних групп ролей.

Карточки представлены в виде списка в плиточном формате. Карточка проекта представляет собой типизированное изображение с заглушкой или обложкой проекта (если данное поле заполнено), название проекта и статус.

Для работы со списком необходимо предусмотреть фильтры для сортировки проектов по типу отборов, статусу, дате. Детализация по фильтрам будет предоставлена в техническом проекте. Базовая сортировка проектов должна быть реализована в хронологическом порядке по дате отправки на оценку или экспертизу: от новых к старым.

### Сохраненные шаблоны

При нажатии на пункт меню пользователь попадает на страницу, где размещены все сохраненные им ранее шаблоны.

Пункт доступен для группы внутренних и технических ролей. Сортировка блоков страницы и детальное описание содержания страницы будет предоставлено в техническом проекте.

## Сертификаты для пользователей

В системе необходимо предусмотреть функционал генерации и присвоения сертификатов пользователям.

Для этого в административной части необходимо разработать отдельный раздел для создания шаблонов сертификатов. В данном разделе необходимо предусмотреть функционал добавления, изменения, удаления шаблонов сертификатов. В рамках данного функционала необходимо указать подложку для шаблона, возможность заведения текста с использованием текстовых тегов. Для редактирования текста необходимо предусмотреть возможность использования текстового редактора.

В системе необходимо предусмотреть возможность генерации сертификатов в формате pdf из шаблона с заполнением данных на основе текстовых тегов.

Сгенерированные сертификаты должны быть доступны для скачивания.

В Приложении 14 указан пример сертификата пользователя.

Предусмотреть в системе отдельный интерфейс, в котором можно изменять и согласовывать текст каждого сертификата.

Пользователи, имеющие соответствующий доступ, должны иметь возможность изменять текст сертификата конкретного пользователя.

Кроме этого, нужно предусмотреть возможность загрузки сертификатов пользователям: система должна поддерживать возможность единичной и массовой загрузки.

## Сквозной поиск

Метаданные системы (предопределённые при создании и добавленные пользователями) должны предусматривать возможность установки признаков «Индексировать» и «Полнотекстовый поиск». Система должна индексировать только те значения полей, которым установлены соответствующие признаки.

Система должна предлагать внешним системам интерфейс отправки поисковых запросов, который, при обнаружении запрошенной информации, должен возвращать реестр ссылок (в контексте Системы) на объекты системы с перечнем значений атрибутов (и дополнительных полей), в которых обнаружены искомые значения.

Система должна предлагать возможность устанавливать расписание обновления индексов.

Для реализации полнотекстового поиска информации, необходимо интегрировать в систему средства, аналогичные по функциональности Solr. Допускается развёртывание сервиса полнотекстового индексирования в виде отдельно стоящего интегрированного с системой сервиса.

Полнотекстовый поиск должен распространяться на объекты-вложения следующих типов: PDF, DOC(X), XLS(X), TDF/ODF (ODP, ODT и других), XML, RTF, TXT, PPT(X). В системе должна быть глобальная настройка включения / выключения полнотекстового поиска.

Необходимо разместить в пользовательском интерфейсе элементы управления, позволяющие использовать индекс (с возможностью составлять логические выражения) и полнотекстовый поиск, реализующие вызов соответствующего сервиса.

# Порядок контроля и приёмки системы

## Порядок оформления и предъявления заказчику результатов работ

Система передаётся в виде функционирующего комплекса на базе средств вычислительной техники Заказчика в сроки, установленные календарном планом выполнения работ. Приёмка системы осуществляется комиссией в составе уполномоченных представителей Заказчика и Исполнителя. Совместно с предъявлением системы производится сдача разработанного Исполнителем комплекта документации согласно разделу 6 настоящего документа.

К моменту передачи системы должны быть завершены все квалификационные тесты, включая тесты информационной безопасности. Отчёты о тестировании не должны содержать дефектов и особенностей реализации, противоречащим требованиям надёжности, целостности и доступности (безопасности), установленным настоящим ТЗ.

Заказчик по запросу предоставляет регламент взаимодействия, в котором определяются контакты и детали для направления результатов работ по договору.

Передачу исходного кода, документации, изменений конфигурационных файлов, изменений Баз данных требуется выполнять только через средства, согласованные с Заказчиком. Взаимные консультации и координация действий выполняются через почту, чат и программные интерфейсы Заказчика. Форматы и протокол передачи также определяются в регламенте взаимодействия.

Факт установки в продуктивную среду подтверждается информационным письмом со стороны Заказчика.

## Порядок приёмки результатов работ

Исполнитель формирует реестр изменений исходного кода (Merge Request) в системе управления версиями Gitlab Заказчика, которые нужно внести в тестовую ветку, для проверки Заказчиком изменений (Code Review) на: соответствие принятому стилю оформления кода, корректность реализации, соответствие бизнес-логике, принятые архитектурные решения, наличие уязвимостей в коде и прочие требования, согласованные Заказчиком. При наличии замечаний у Заказчика, Исполнитель устраняет их для проведения повторной проверки. После согласования функционала Заказчиком, Исполнитель выполняет поставку изменений в тестовую ветку и среду.

Исполнитель описывает и согласовывает с Заказчиком инструкцию по публикации изменений с пошаговым руководством, условия которого необходимо выполнить, для поставки изменений в исходный код, базу данных (миграции), метаданные, модель доступа и конфигурацию системы, а также методы отката изменений, которые необходимо выполнить при наличии критических ошибок публикации результатов работ в опытной и продуктивной среде.

Исполнитель готовит и согласует с Заказчиком Программу и Методику Испытаний (ПМИ), которую Стороны используют на этапе проверки готовности функционала и квалификационного тестирования системы.

Для проведения функционального и регрессионного тестирования проекта, Исполнитель готовит средства автоматического тестирования и ручные сценарии (в рамках ПМИ) для функционала проекта, готового к передаче в опытную эксплуатацию согласно плану-графику выполнения работ. Дальнейшие разработанные разделы ПМИ дополняют или актуализируют ранее составленный ПМИ с учётом реализованных изменений.

По факту подтверждения Заказчиком готовности функционала в среде для опытной эксплуатации, Заказчик инициирует квалификационные испытания с участием функционального заказчиком системы.

Для проведения ПСИ формируется комиссия из членов рабочей группы проекта, ответственных за приемку требований в среде для опытной эксплуатации.

На основании ПСИ, Заказчиком формирует протокол ПСИ. Исполнитель в течении двух рабочих дней формирует план устранения замечаний с указанием сроков, на основании которого Заказчик назначает дату проведения повторных ПСИ.

По факту подтверждения Заказчиком успешного прохождения опытной эксплуатации функционала Исполнитель осуществляет подготовку изменений для его публикации в продуктивную среду. Стороны осуществляют установленные настоящим техническим заданием виды анализа и тестирования системы и, при отсутствии замечаний, выполняют поставку функционала на продуктовую среду. При наличии замечаний Исполнитель формирует план их устранения с указанием сроков и назначает дату проведения повторной проверки.

При наличии критических ошибок в продуктовой среде, Заказчик использует инструкцию по откату изменений описанную Исполнителем. Заказчиком формируется план их устранения Исполнителем с указанием сроков и назначает дату проведения повторной проверки.

По результатам работы приёмочной комиссии Стороны оформляют протокол приемо-сдаточных испытаний. Функционал, принятый комиссией, считается реализованным корректно. В отношении выявленных отклонения реализации функционала, Стороны составляют и утверждают план-график устранения дефектов. Выявленные в течение срока гарантийного обслуживания дефекты Исполнитель устраняет согласно требованиям гарантийного обслуживания, указанных в договоре на выполнение работ по настоящему техническому заданию.

**Разработка методики предварительных и приёмочных испытаний**. Методика предварительных и приёмочных испытаний разрабатывается специалистами Исполнителя на основе настоящего технического задания и существующей документации на Систему и согласуется с Заказчиком.

Документ включает в себя:

* Описание проверяемого требования (с указанием пункта ТЗ)
* Описание действий, требуемых для валидации требования
* Описание ожидаемого результата при проверке требования

Допускается введение ПМИ в системах управления тестированием, при согласовании типа системы с Заказчиком, с дальнейшей выгрузкой тест-планов в формат документа из Приложения 15 «Программа и методика испытания».

**Предварительные испытания**. Данные испытания проводятся после развёртывания программного обеспечения системы в тестовой среде на оборудовании Заказчика. Выявленные в ходе предварительных испытаний ошибки и недоработки направляются Исполнителю для исправления. Если в результате предварительных испытаний система в целом отвечает требованиям Частного технического задания, то её рекомендуется передать в опытную эксплуатацию. Результаты предварительных испытаний оформляются в виде протокола.

**Опытная эксплуатация**. В течение установленного договором срока опытной эксплуатации проводится комплексная проверка функционирования системы. Выявленные замечания тщательно фиксируются и своевременно передаются Исполнителю для устранения.

**Приёмочные испытания**Приёмочные испытания проводятся после окончания опытной эксплуатации. Выявленные в ходе приёмочных испытаний ошибки и недоработки направляются Исполнителю для исправления. Если в результате приёмочных испытаний система в целом отвечает требованиям Частного технического задания, то её рекомендуется принять в промышленную эксплуатацию. При этом Исполнителю устанавливается срок для устранения выявленных замечаний. Результаты приёмочных испытаний оформляются в виде протокола.

# Требования к документированию

В ходе выполнения работ Исполнителем должна быть обновлена/создана следующая документация[[21]](#footnote-21):

* проектная документация, включающая в себя спецификации функциональных требований и разработанные на их основе тестовые сценарии (которые в последствии будут включены в ПМИ).
* конструкторская документация, включающая в себя общесистемную и архитектурную спецификацию Системы, а также программу и методику испытаний (ПМИ);
* эксплуатационная документация, включающая в себя: руководство пользователя, руководство администратора, руководство по развёртыванию Системы и пуско-наладочным работам.

Требования к составлению документации представлены в соответствующих шаблонах.

# Приложение №1. Требуемые методы защиты информации с указанием уровня ответственности Исполнителя и Заказчик

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **№** | **Подсистема ИБ** | **Требуемые методы защиты** | **Зона ответственности** | |
| **Исполнитель** | **Заказчик** |
| 1.1. | Подсистема контроля и управления доступом | Идентификации и аутентификации пользователей в интерфейсах:  Исполнитель реализует интеграцию с сервисом авторизации и в рамках полученных токенов реализует механизм защищенного доступа авторизованных пользователей.  Заказчик отвечает за доступность сервиса авторизации (Keycloack). | ✓ | ✓ |
| 1.2. | Усиленная аутентификация администраторов и пользователей.   Заказчик отвечает за доступность сервиса авторизации (Keycloack). |  | ✓ |
| 1.3. | Разграничение доступа субъектов к объектам доступа согласно ролям пользователя. | ✓ |  |
| 2.1. | Подсистема регистрации и учёта событий | Регистрация событий аутентификации пользователей*(интерактивных/технических)* | ✓ | ✓ |
| 2.2. | Регистрация изменений полномочий субъектов доступа и статуса объектов доступа |  | ✓ |
| 2.3. | Регистрация попыток несанкционированного доступа к защищаемым информационным ресурсам | ✓ |  |
| 2.4. | Регистрация попыток доступа к защищаемым объектам доступа *(ОС АСО, ОС АРМ, ОС серверов, каналы связи, периферийное оборудование, программы, томы, каталоги, файлы, записи).* Исполнитель регистрирует только попытки доступа на уровне приложения. | ✓ | ✓ |
| 2.5. | Регистрация действий администраторов *(создание/редактирование пользователей создание/редактирование системных объектов, изменение конфигураций)*    Исполнитель регистрирует только действия в рамках приложения | ✓ | ✓ |
| 2.6. | Регистрация событий по изменению данных (п. 2.2) | ✓ | ✓ |
| 3. | Подсистема защиты от вредоносного кода / ПО | Контроль качества и безопасности кода (SAST/DAST).   Исполнитель внедряет в CI pipeline автоматизированный статический анализ кода (согласно п. 1.5.1.3). | ✓ |  |
| 4.1. | Подсистема контроля защищенности | Автоматизированный аудит: периодический инструментальный анализ защищенности при помощи сканеров безопасности (иных специализированных СЗИ) |  | ✓ |
| 4.2. | Автоматизированный аудит: формирование статистических отчетов о результатах периодического инструментального анализа защищенности |  | ✓ |
| 4.3. | Автоматизированный аудит: регулярное обновление и поддержание в актуальном состоянии баз уязвимостей |  | ✓ |
| 4.4. | Ручной аудит: анализ конфигурационных файлов средств обработки, хранения и передачи информации. |  | ✓ |
| 5.1. | Подсистема централизованного управления и мониторинга | Централизованный сбор и отображение событий ИБ, событий о состоянии СЗИ (SIEM) |  | ✓ |
| 5.2. | Оповещение Администратора ИБ о критичных событиях ИБ и инцидентах ИБ |  | ✓ |
| 5.3. | Регистрация событий прикладного слоя и событий безопасности с помощью централизованного сервиса (на стороне Заказчика) с обеспечением отказоустойчивости за счёт резервирования в системном журнале | ✓ | ✓ |
| 6.1. | Подсистема резервного копирования и восстановления | Обеспечение создания резервных копий данных (и/или): - встроенными возможностями - подсистемой резервного копирования персональных данных (2-ой уровень защищённости, приказ ФСТЭК №21). | ✓ | ✓ |
| 6.2. | Возможность оповещения, отчетности и анализа для всех элементов резервного копирования |  | ✓ |
| 6.3. | Возможность оперативного масштабирования.  Подрядчик должен обеспечить возможность работу приложения в условиях горизонтального и/или вертикального масштабирования | ✓ | ✓ |

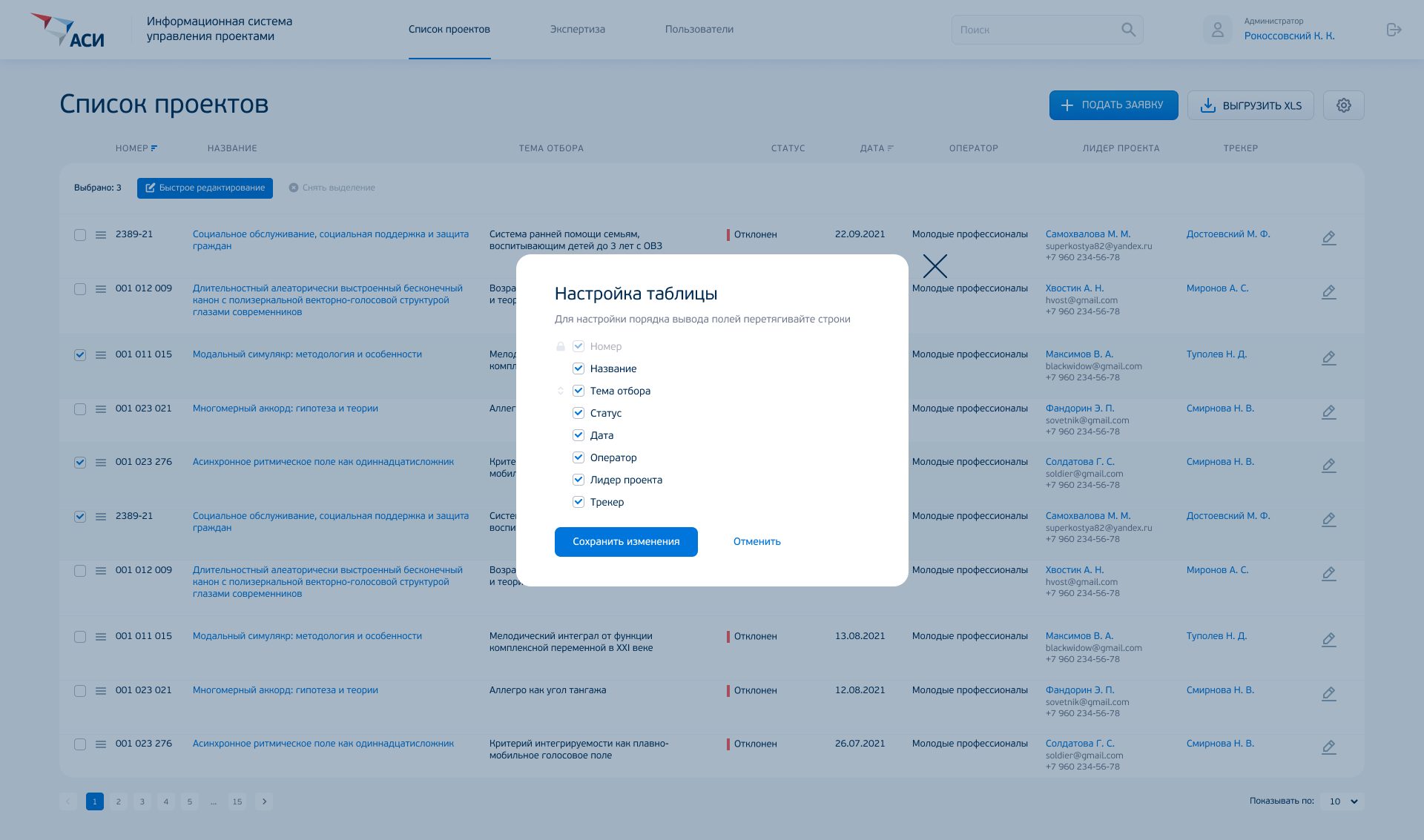
# Приложение №2. Пример единой карточки проекта

к пункту 4.2.1 к Технического задания

|  |  |  |
| --- | --- | --- |
| Блок карточки | Поле карточки | Формат поля |
| О проекте | Название проекта | Текст |
| Направление или категория проекта | Выбор 1 из списка. Настраиваемый справочник |
| Тема отбора | Выбор 1 из списка. Настраиваемый справочник |
| Стадия реализации проекта | Выбор 1 из списка |
| Страна реализации | Выбор 1 из списка |
| Регионы реализации | Выбор нескольких из списка |
| Цели проекта | Текстовые поля (с возможностью добавить) |
| Задачи проекта | Текстовые поля (с возможностью добавить) |
| Проблемы, которые решает проект | Текстовые поля (с возможностью добавить) |
| Целевая аудитория проекта | Текстовые поля (с возможностью добавить) |
| Суть проекта (Краткое описание) | Текстовое поле |
| Конкурентные преимущества | Текстовое поле |
| Продукт проекта | Текстовое поле |
| Необходимость инвестиций / Ваш проект является инвестиционным | Радиобаттон (Да/Нет) |
| Вопрос к проекту | Текстовое поле |
| Как проект решает описанную проблему | Текстовое поле |
| Приведите описание базовой технологии | Текстовое поле |
| Опишите основные направления коммерциализации Вашего проекта | Текстовое поле |
| Тип проекта | Выбор 1 из списка. Настраиваемый справочник |
| Вид проекта | Выбор 1 из списка. Настраиваемый справочник |
| Материалы проекта | Презентация проекта | Загрузка файла |
| Заключения/отзывы о проекте/продукте/технологии | Загрузка файлов |
| Дополнительные материалы проекта | Загрузка файлов |
| Загрузка фото и видео о проекте | Загрузка изображений и видео  Либо Ссылка |
| Обложка карточки проекта | Загрузка изображения |
| Веб-сайт проекта | Текстовое поле (ссылка) |
| Ссылки на социальные сети проекта | Текстовое поле (ссылка) |
| О пилотных запусках | Регион первого внедрения | Выбор 1 из списка |
| Эффекты от реализации (качественный показатель) | Текстовое поле |
| Эффекты от реализации (количественный показатель) | Текстовое поле |
| Где уже было апробировано решение, запущены пилотные проекты, каких результатов удалось достичь? | Текстовое поле |
| Инвестиционный блок (открывается, если пользователь выбирает «Да» в поле «Необходимость инвестиций) | Бизнес-план проекта | Загрузка файлов |
| Финансовая модель проекта | Загрузка файлов |
| Ресурсное обеспечение проекта | Текстовое поле |
| Для поддержки проектов | Цель обращения в АСИ | Текстовое поле |
| Что мешает реализации проекта | Текстовое поле |
| Какие регуляторные изменения для поддержки развития вашего типа бизнеса/проекта необходимы на системном уровне | Текстовое поле |
| Откуда вы узнали об отборе проектов АСИ? | Текстовое поле |
| Для тиражирования проектов | Каким образом можно внедрить практику в другом регионе? | Выбор нескольких из списка |
| Опишите основные шаги плана реализации практики | Текстовое поле |
| Стоимость реализации проекта | Выбор 1 из списка |
| Выбор наставника | Чек-бокс (выбор из карточек пользователей) |
| Укажите, сколько времени потребовалось для запуска практики | Числовое поле |
| Были ли задействованы сторонние организации для реализации? | Радиобаттон (Да/Нет)  Если выбирают «Да», то открываются поля «Организация» и «Формат участия» |
| Организация | Выбор карточки организации из списка |
| Формат участия | Текстовое поле |
| Какую поддержку, кроме консультационной, вы готовы оказать при внедрении? | Текстовое поле |
| Есть ли особенности, которые необходимо учесть при внедрении? | Радиобаттон (Да/Нет)  Если выбирают «Да», то открывается текстовое поле для заполнения. |
| Для разметки проектов | Отношение проекта к Рейтингу качества жизни | Выбор нескольких из списка |
| Отношение проекта к Национальному инвестиционному рейтингу | Выбор нескольких из списка |
| Одобрение комиссиями Госсовета | Выбор нескольких из списка |
| Одобрение ФОИВ | Выбор нескольких из списка |
| Теги | Выбор нескольких из списка |
| Подкатегория проекта | Выбор нескольких из списка |
| О команде | Выбор пользователей | Выбор из зарегистрированных пользователей или приглашение нового пользователя по e-mail (подтягивается карточка пользователя) |
| Выбор лидера | Чек-бокс |
| Описание роли в команде | Текстовое поле |
| Организационная форма | Юридический статус занятости | Выбор 1 из списка |
| Если выбирает ЮЛ или ИП: Выбор компании | Выбор карточки организации из списка |
| Партнерство | Указание организации - партнера | Выбор карточки организации |
| Срок действия соглашения | Числовое поле / формат даты |
| Дата подписания | Формат даты |
| Направление АСИ, ответственное за подписание | Выбор из списка. Справочник |
| Предмет сотрудничества | Текстовое поле или выбор из списка. |
| Направление сотрудничества с партнером | Выбор из списка. Справочник |

**Макет реализации добавления новых полей**

к пункту 4.1.1 к Технического задания



# Приложение №3. Вариант полной дорожной карты

к пункту 4.3.5 к Технического задания

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **Тема отбора** | | | | | | |
| **Дата поступления заявки:** дд.мм.гг. | | | | | | |
| **ID проекта**  **Название проекта:** | | | | | | |
| **Лидер проекта:** ФИО, должность | | | | | | |
| **Цели обращения в Агентство:** | | | | | | |
| № | Мероприятия | Начало (мм.гг.) | Окончание (мм.гг.) | Результаты | Ответственные | Комментарий |
| 1 | Аудит |  |  |  |  |  |
|  | 1.1. Задача 1 |  |  |  |  |  |
|  | 1.2. Задача 2 |  |  |  |  |  |
| 2 | Экспертиза |  |  |  |  |  |
|  | Оценка экспертом 1 |  |  |  |  |  |
|  | Оценка экспертом 2 |  |  |  |  |  |
| 3 | Поддержка |  |  |  |  |  |
|  | 1.1. Задача 1 |  |  |  |  |  |
|  | 1.2. Задача 2 |  |  |  |  |  |
|  | 1.3. Задача 3 и т.д. |  |  |  |  |  |
| 4 | Мониторинг |  |  |  |  |  |
|  | 2.1. Задача 1 |  |  |  |  |  |
|  | 2.2. Задача 2 |  |  |  |  |  |
|  | 2.3. Задача 3 и т.д. |  |  |  |  |  |

# Приложение №4. Вариант выгрузки части задач дорожной карты с типом задачи «Поддержка проекта»

к пункту 4.3.5 к Технического задания

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **Тема отбора**  **Дата поступления заявки:** дд.мм.гг. | | | | | | |
| **ID проекта**  **Название проекта:** | | | | | | |
| **Лидер проекта: ФИО, должность** | | | | | | |
| **Цели обращения в Агентство:** | | | | | | |
| № | Мероприятия | Начало (мм.гг.) | Окончание (мм.гг.) | Результаты | Ответственные | Комментарий |
| 1 | Мероприятие 1 |  |  |  |  |  |
|  | 1.1. Задача 1 |  |  |  |  |  |
|  | 1.2. Задача 2 |  |  |  |  |  |
|  | 1.3. Задача 3 и т.д. |  |  |  |  |  |
| 2 | Мероприятие 2 |  |  |  |  |  |
|  | 2.1. Задача 1 |  |  |  |  |  |
|  | 2.2. Задача 2 |  |  |  |  |  |
|  | 2.3. Задача 3 и т.д. |  |  |  |  |  |
|  | План поддержки проекта согласован  *(отметка лидера)* |  |  |  |  |  |
| Лидер проекта  ФИО\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ подпись Директор центра …  ФИО\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_подпись  Дата: | | | | | | |

# Приложение №5. Вариант выгрузки части задач дорожной карты с типом задачи «Поддержка проекта» на этапе «сопровождение

к пункту 4.3.5 к Технического задания

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **Тема отбора**  **Дата поступления заявки:** дд.мм.гг. | | | | | | |
| **ID проекта**  **Название проекта:** | | | | | | |
| **Лидер проекта: ФИО, должность** | | | | | | |
| **Цели обращения в Агентство:** | | | | | | |
| № | Мероприятия | Начало (мм.гг.) | Окончание (мм.гг.) | Результаты | Ответственные | Комментарий |
| 1 | Мероприятие 1 |  |  |  |  |  |
|  | 1.1. Задача 1 |  |  |  |  |  |
|  | 1.2. Задача 2 |  |  |  |  |  |
|  | 1.3. Задача 3 и т.д. |  |  |  |  |  |
| 2 | Мероприятие 2 |  |  |  |  |  |
|  | 2.1. Задача 1 |  |  |  |  |  |
|  | 2.2. Задача 2 |  |  |  |  |  |
|  | 2.3. Задача 3 и т.д. |  |  |  |  |  |
|  | План поддержки проекта согласован  *(отметка лидера)* |  |  |  |  |  |
| Все мероприятия дорожной карты выполнены  Лидер проекта  ФИО\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ подпись Директор центра …  ФИО\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_подпись  Дата: | | | | | | |

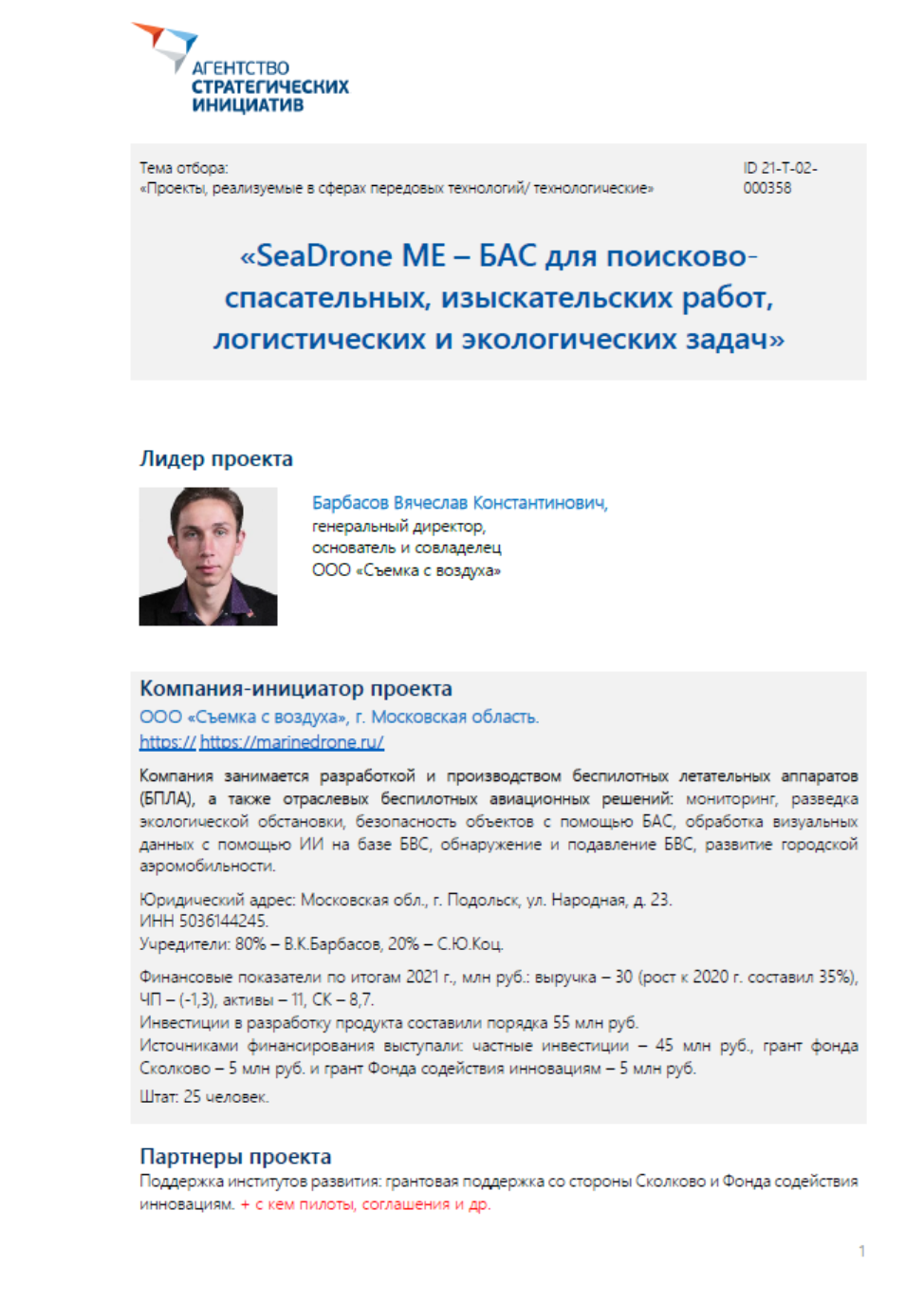
# Приложение №6. Пример выгрузки паспорта проекта в формате word

к пункту 4.4 Технического задания

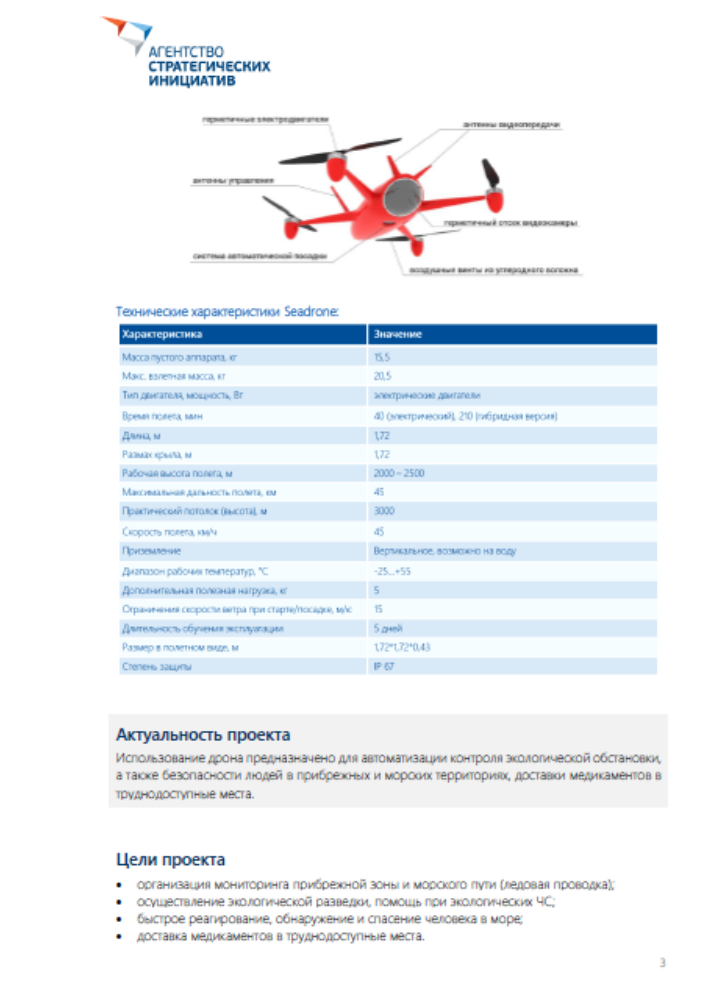
|  |
| --- |
| **Тема целевого отбора « »**  **Направление проектов (**технологии, качество жизни, экология, образование и кадры)  **Дата поступления проекта:** |
| **О проекте** |
| ID |
| Название проекта |
| Лидер проекта (ФИО, должность, контакты) |
| Компания-инициатор проекта (наименование, ИНН, участники, бенефициары, финансовые показали по последнему отчетному периоду, штат, поддержка институтов развития) |
| Партнеры проекта |
| Проблема, которую решает проект (актуальность) |
| Цель проекта |
| Суть проекта |
| Продукт проекта, особенности проекта/технологии/методики/решения |
| Конкурентные преимущества |
| Стадия реализации (стартап, пилотирование, внедрение, производство, др.; имеет ли проект минимально жизнеспособный продукт - MVP) |
| Результаты апробаций/внедрений |
| Бизнес-модель проекта |
|  |
| Ресурсное обеспечение проекта (источники финансирования, кадровые, инфраструктурные ресурсы, права на интеллектуальную собственность, производственные возможности и др.) |
|  |
| Целевая аудитория |
| Анализ рынка, целевые сегменты |
| **Проект в Агентстве** |
| Цель обращения в Агентство |
| Срок работы над проектом (с…по…) |
| Результаты экспертизы (источник экспертной оценки, коротко – результат) |
| Ожидаемый результат по итогам поддержки проекта |
|  |
| Трекер (ФИО, e-mail) |
| **Результат поддержки**  *отчет заполняется к бюро экспертного совета по результатам поддержки проекта* |
| **Динамика целевых показателей проекта**  *Результат представляется в виде количественных и качественных показателей проекта в сравнении «было-стало» по итогам поддержки.*  «было» «стало» |
| **Социально-экономический эффект**  *Результат представляется в виде описания эффекта по итогам реализации проекта (например - изменение законодательной, нормативно-правовой базы; тиражирование проекта; тиражирование через Смартеку как лучшей практики; создание активного сообщества; создание модельных решений, программ, методического инструментария – с потенциалом для распространения и др.)* |

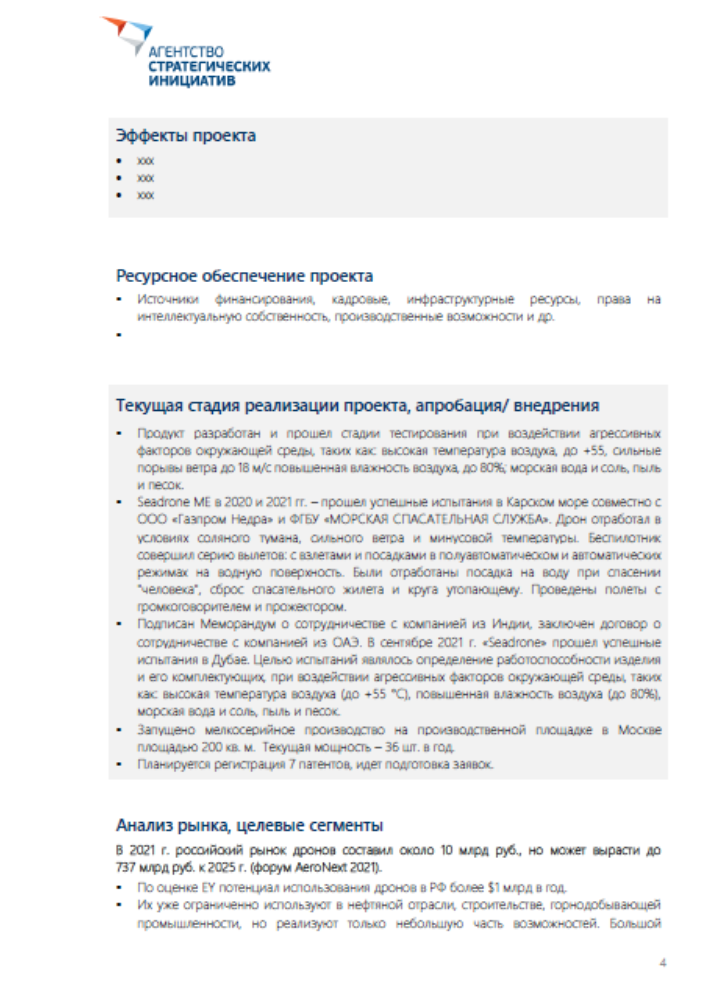
# Приложение №7. Пример выгрузки паспорта проекта

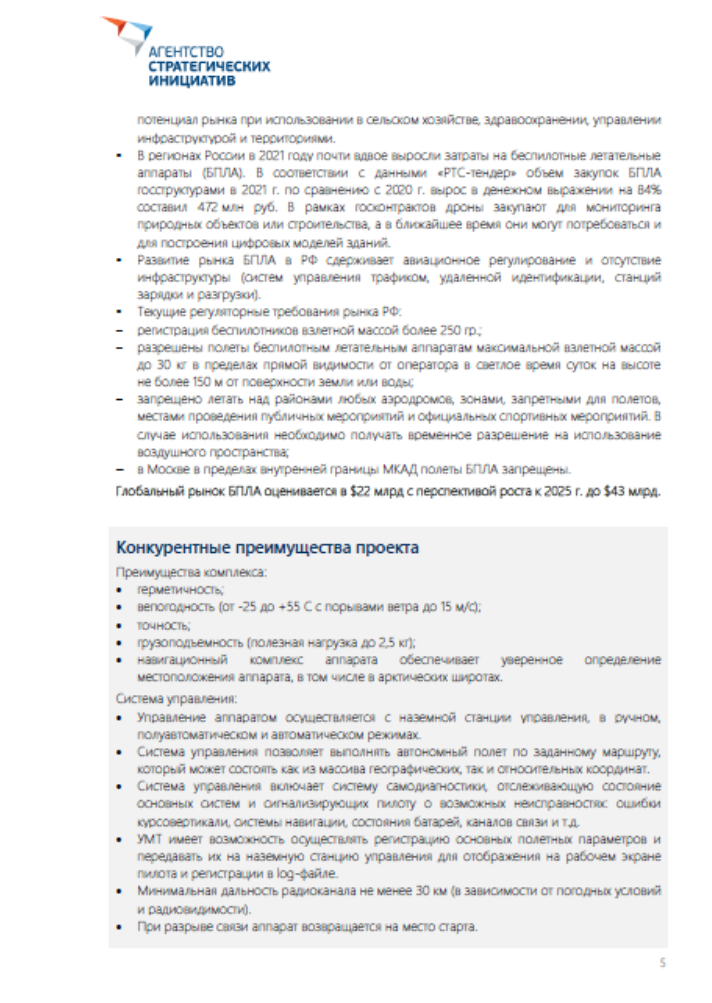
к пункту 4.4 Технического задания

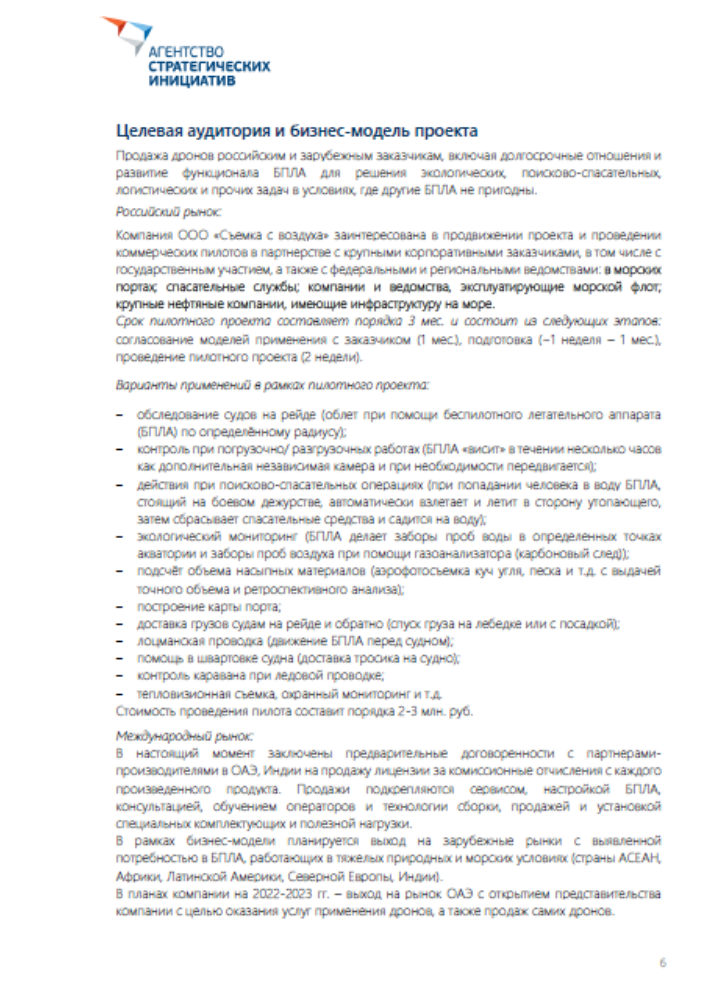


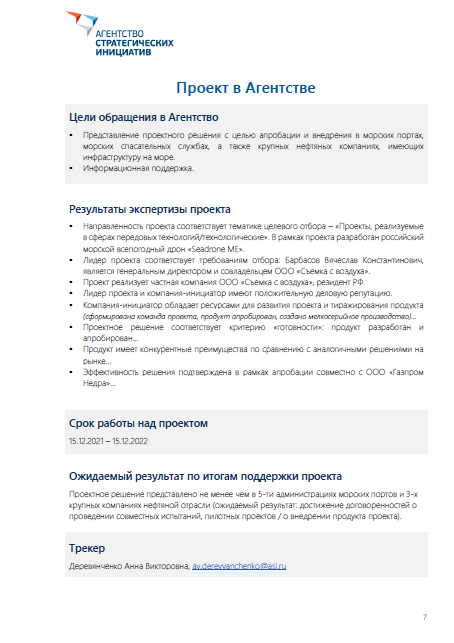


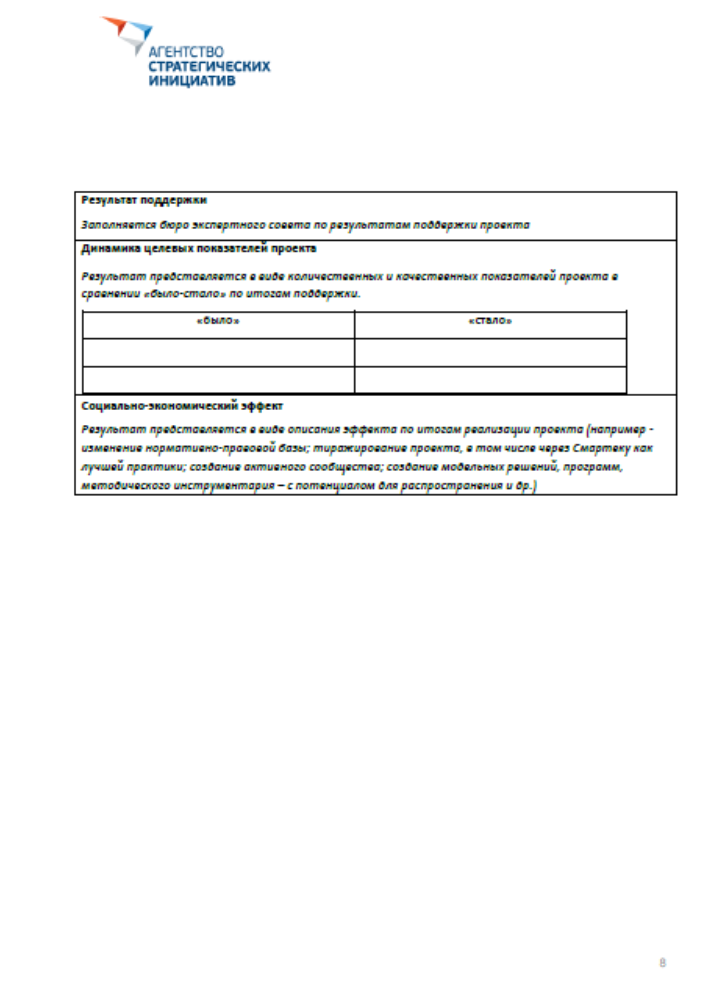






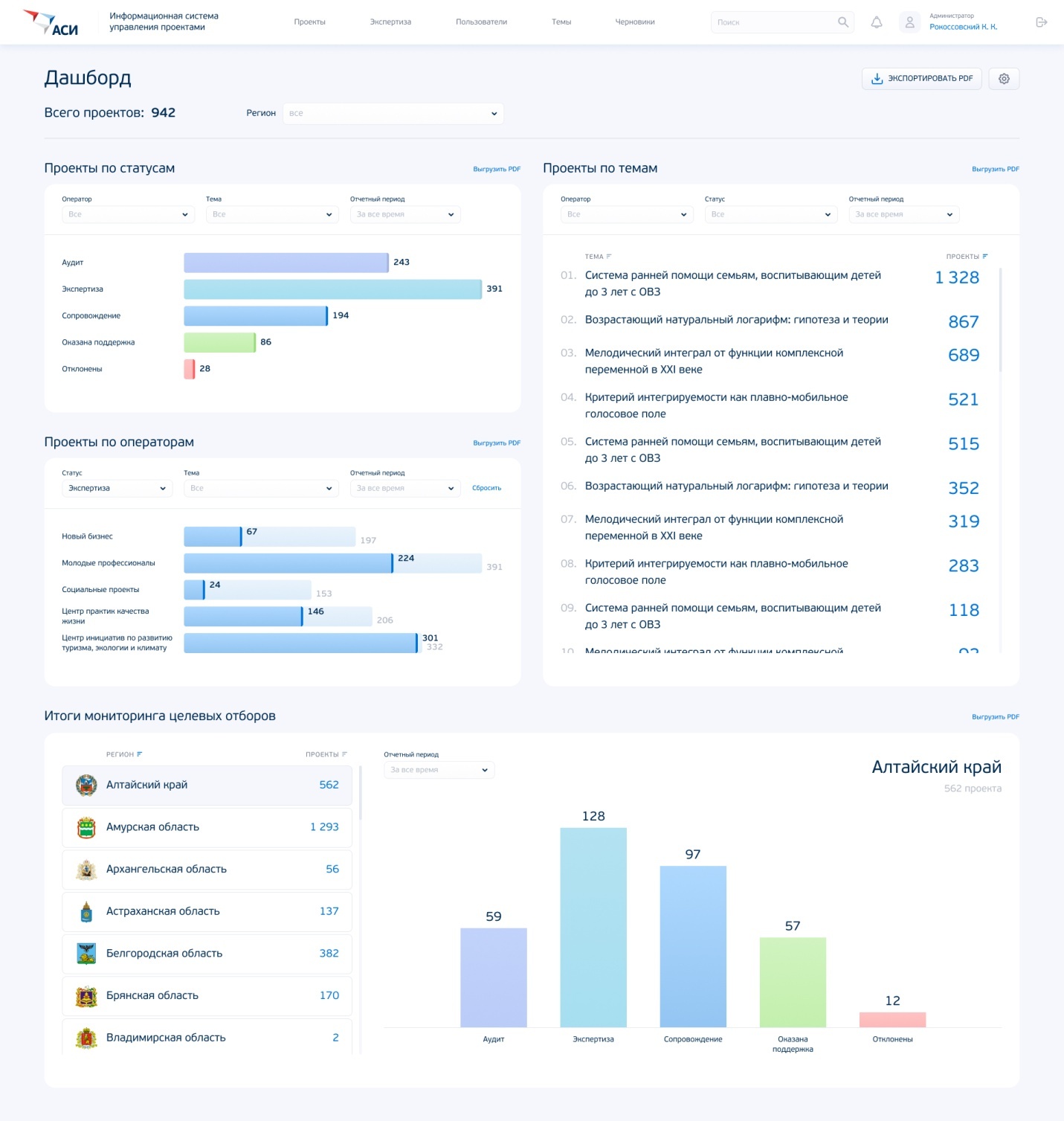






# Приложение №8. Пример отображения отчета

к пункту 4.10.2 Технического задания



# Приложение №9. Формы для предоставления на Комиссию по аудиту проектов (КАП)

к пункту 4.11.3 Технического задания

**Статистика по поступившим проектам на отборы**

Срок приема заявок: дд.мм.гг. – дд.мм.гг.

|  |  |  |  |
| --- | --- | --- | --- |
| **Тема отбора** | **Поступило проектов** | **Рекомендовано на этап «экспертиза»** | **Отклонено** |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
| **Всего** |  |  |  |

**Форма представления проектов, рекомендуемых для перевода на этап «экспертиза»**

**(по итогам оценки по критериям 1 уровня)**

**Проекты, рекомендуемые для перевода на этап «экспертиза»**

Срок приема заявок: дд.мм.гг. – дд.мм.гг.

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **№** | **Тема отбора** | **ID проекта** | **Название проекта** | **Краткое описание проекта** | **ФИО трекера** |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |

**Форма представления проектов, рекомендуемых к отклонению с этапа «аудит»**

**(по итогам оценки по критериям 1 уровня)**

**Проекты, рекомендуемые к отклонению с этапа «аудит»**

Срок приема заявок: дд.мм.гг. – дд.мм.гг.

|  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **№** | **Тема отбора** | **ID** | **Название проекта и краткое описание** | **Отметка о несоответствии критериям первого уровня** | | | | | | **Обоснование отклонения** | **Рекомендации**  **по доработке** | **ФИО трекера** |
|  |  | **1** | **2** | **3** | **4** | **5** | **6** |
| Критерий 1 | КРитерий 2 | Критерий 3 | Критерий 4 | Критерий 5 | Критерий n |

# Приложение №10. Формы для предоставления на Рабочую группу экспертного совета

к пункту 4.11.3 Технического задания

**Рейтинг проектов, прошедших оценку по критериям 2 уровня**

Тема отбора

Срок приема заявок: дд.мм.гг. – дд.мм.гг.

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **№** | **Номер в рейтинге** | **Количество баллов** | **ID проекта** | **Название проекта** | **Комментарий эксперта** | **ФИО эксперта** |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |

**Проекты, рекомендуемые к переводу на этап «сопровождение»**

Тема отбора

Срок приема заявок: дд.мм.гг. – дд.мм.гг.

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **№** | **Номер в рейтинге** | **Количество баллов** | **ID проекта** | **Название проекта** | **Комментарий эксперта** | **ФИО эксперта** |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |

**Проекты, рекомендуемые к отклонению с этапа «экспертиза»**

Тема отбора

Срок приема заявок: дд.мм.гг. – дд.мм.гг.

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **№** | **Номер в рейтинге** | **Количество баллов** | **ID проекта** | **Название проекта** | **Комментарий эксперта /обоснование отклонения** | **ФИО эксперта** |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |

# Приложение №11. Формы отчетов по мониторингу отборов проектов

к пункту 4.11.3 Технического задания

**Отчет по итогам мониторинга отборов проектов   
(количественные показатели)**

Дата отчета: дд.мм.гггг

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| № | **Тема отбора** | **Всего** | **Аудит** | **Экспертиза** | **Поддержка** | **Оказана поддержка** | **Отклонен** |
|  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |
|  | **Всего** |  |  |  |  |  |  |

**Отчет по итогам мониторинга отбора проектов (соблюдение сроков исполнения похождения этапов жизненного цикла проектов)**

Выгружаются только проекты, у которых нарушен срок прохождения этапа

Дата отчета: дд.мм.гггг

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **№** | **ID / Проект** | **Тема отбора проектов** | **Статус проекта / реквизиты протокола** | **Обоснование несоблюдения сроков** |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |

# Приложение №12. Матрица ролей

к пункту 4.16 Технического задания

Матрица ролей приложена отдельным Excel файлом.

# Приложение №13. Пример карточки партнера

к пункту 4.20 Технического задания

|  |  |  |
| --- | --- | --- |
| Блок карточки | Поле карточки | Формат поля |
| Общая информация | Страна организации | Выбор 1 из списка |
| Регионы присутствия | Выбор нескольких из списка |
| ИНН | Числовое поле. Интеграция с ЕГРЮЛ |
| Название организации | Текстовое поле. Автоматически подтягивается при вводе ИНН |
| КПП | Числовое поле. Автоматически подтягивается при вводе ИНН |
| Юридический адрес юрлица | Текстовое поле. Автоматически подтягивается при вводе ИНН |
| Фактический адрес юрлица | Текстовое поле. Автоматически подтягивается при вводе ИНН |
| ОГРН | Текстовое поле. Автоматически подтягивается при вводе ИНН |
| Тип организации | Выбор 1 из списка. Настраиваемый справочник |
| Бренд | Текстовое поле |
| Латинское наименование | Текстовое поле |
| Описание организации | Текстовое поле |
| Отрасль компании | Выбор нескольких из списка Настраиваемый справочник |
| Отчетность компании | Загрузка файлов |
| Контактная информация | Общий телефон | Текстовое поле |
| Общий e-mail | Текстовое поле |
| Контактное лицо от организации (ФИО) | Текстовое поле / выбор карточки пользователя из списка |
| Контактное лицо от организации (телефон) | Подтягиваются из карточки пользователя |
| Контактное лицо от организации (e-mail) | Подтягиваются из карточки пользователя |
| Контактное лицо из АСИ (ФИО) | Текстовое поле / выбор карточки пользователя из списка |
| Контактное лицо из АСИ (телефон) | Подтягиваются из карточки пользователя |
| Контактное лицо из АСИ (e-mail) | Подтягиваются из карточки пользователя |
| Сайт организации | Текстовое поле (ссылка) |
| Команда организации | Выбор членов команды организации | Текстовое поле / выбор карточки пользователя из списка |
| Взаимодействие с АСИ | Статус партнерства | Выбор 1 из списка |
| Направления сотрудничества | Выбор из нескольких списка. Настраиваемый справочник |
| Тип поддержки | Выбор нескольких вариантов из списка. Настраиваемый справочник |
| Аккредитация АСИ | Радиобаттон (Да/Нет) |
| Номер соглашения | Числовое поле |
| Документ | Загрузка файла |
| Экспорт | Являетесь ли Вы действующим экспортером | Радиобаттон (Да/Нет)  Если выбирают «да», открываются 2 следующих поля для заполнения: |
| В какие страны экспортируете | Выбор из нескольких из списка. Справочник |
| Какую продукцию вы экспортируете | Текстовое поле |
| Проекты | Партнерские проекты | Выбор карточки проекта |
| Соглашение | Выбор карточки проекта с типом «Соглашение» |
| Дата окончания соглашения | Должна подтягиваться автоматические из карточки проекта с типом «Соглашение» |

# Приложение №14. Пример сертификата

к пункту 4.22 Технического задания



# Приложение № 15. Программа и методика испытания

к пункту 5.2 Технического задания

<Наименование проекта>

Программа и методика испытаний

Заметка по использованию: Внутри настоящего шаблона присутствуют процедурные руководства, оформленные стилем InfoBlue. Этот стиль имеет атрибут «скрытый», предлагающий возможность скрывать или делать видимым текст. Атрибут влияет на представление документа при выводе на печать.

* + - 1. **Область применения**

Настоящая программа и методика испытаний устанавливает требования к структуре и содержанию программы и методики испытаний <**Наименование информационной системы**>, определяет порядок проведения испытаний, организацию подготовки и производства работ при проведении испытаний.

Настоящий документ предназначен для применения следующими организациями / подразделениями организаций:

* <Намиенование организации, подразделения: роль в отношении проекта>
* <Намиенование организации, подразделения: роль в отношении проекта>
* <Намиенование организации, подразделения: роль в отношении проекта>

осуществляющими разработку, производство и внедрение информационных систем Автономной некоммерческой организации «Агентство стратегических инициатив по продвижению новых проектов» (Далее «Агентство»).

* + - 1. **Общие положения**
  1. **Наименование и обозначение испытываемого изделия**

[Приведите наименование испытываемого изделия: информационной системы, компоненты или сервиса. Её полное и сокращённое именование]

* 1. **Виды и цель испытаний**

[Приведите виды испытаний, их цели и основания]

|  |  |  |  |
| --- | --- | --- | --- |
| Информационная компонента | Вид испытаний | Цель испытаний | Основание |
|  |  |  |  |

* 1. **Условия предъявления изделия на испытания**

[Приведите все предварительные условия, которые должны быть выполнены для запуска процедур проведения испытаний. При необходимости укажите сроки контрольных событий. Например, ввод в эксплуатацию систем, от которых зависит изделие, проведение закупочных процедур и так далее.]

* 1. **Состав приёмочной комиссии**

[Приведите состав приёмочной комиссии: председатель, постоянные члены комиссии, привлекаемые представители контрагентов и систем, в отношении которых они привлекаются к испытаниям. Укажите ответственного руководителя испытаний, а также права и обязанности всех участников испытаний.]

* + - 1. **Общие требования к условиям, обеспечению и проведению испытаний**
  1. **Место проведения испытаний**

[Укажите место (если применимо) и формат проведения испытаний.]

* 1. **Средства проведения испытания**

[Приведите перечень средств, которые будут использованы для проведения испытаний. Например, для замера производительности должны применяться <такие-то средства трассировки>, <средства имитации работы пользователя> или <инструменты генерации нагрузки>. Приведите также требования к испытательному оборудованию или полигону (вычислительные мощности, объёмы хранилищ, пропускная способность каналов связи и так далее).]

* 1. **Условия проведения испытаний**

[Приведите требования к условиям проведения испытаний. Например, система должна быть испытана под рабочей нагрузкой смежных систем и коммутационного оборудования при загрузке процессорных устройств в интервале от … до …]

* 1. **Подготовка оборудования и вычислительных площадок к проведению испытаний**

[Приведите описание вычислительных сред, в рамках которых будут проводиться испытания: их конфигурация и эксплуатационные атрибуты.]

* 1. **Эксплуатация системы после проведения испытаний**

[Указать условия, описать состояние в котором система должна находиться после проведения испытаний. Например: система должна быть пригодна к эксплуатации пользователями. Или: система может перестать обслуживать пользователей, но обеспечивать целостность данных, сохранять транзакции, зафиксированные в системе до момента … И так далее.]

* 1. **Требования к персоналу, осуществляющему испытания**

[Например, персонал, проводящий испытания должен пройти вводный инструктаж, ознакомиться с эксплуатационной документацией и так далее.]

* + - 1. **Требования целостности, доступности и информационной безопасности**

[Привести общие требования к целостности, доступности и информационной безопасности во время проведения испытаний. Указать требования при подготовке, проведению и завершению испытаний.]

* + - 1. **Определяемые показатели**

[Привести перечень определяемых показателей, допустимые интервалы и погрешности (если применимо) измерений.]

* + - 1. **Режимы испытаний**
  1. **Режимы испытаний**

[Например: нормальный режим или режим повышенной загрузки, стресс-режим.]

* 1. **Ограничения и указания**

[Приведите ограничения или критерии выполнения испытаний, а также указания, которые должны быть исполнены в результате возникновения таких условий. Например: Корректировка плана и последовательности испытаний не должна влиять на качество и объём выполнения проверок.]

* 1. **Условия останова, прекращения и возобновления испытаний**

[Привести условия при которых испытания могут быть остановлены, прекращены или возобновлены, а также допустимые состояния испытуемых изделий.]

* + - 1. **Методы и сценарии испытаний**

[Привести методы контроля результатов испытаний, а также перечень методов испытаний.]

* 1. **<Метод испытаний 1>**

[Привести условия при которых испытания могут быть остановлены, прекращены или возобновлены, а также допустимые состояния испытуемых изделий.]

| Наименование теста | | <Наименование теста> | | | |
| --- | --- | --- | --- | --- | --- |
| Пользовательский сценарий: | | <Наименование пользовательского сценария> | | | |
| Описание теста: | | [Привести детальное описание процедуры, используемой настоящим тестовым сценарием.] | | | |
| Предварительные условия | | [Привести все предварительные условия, которые должны быть выполнены перед началом теста.] | | | |
| Состояние системы после теста | | [Описать состояние системы после выполнения теста.] | | | |
| Замечания: | |  | | | |
| Результат (Pass/Fail/Warning/Incomplete) | |  | | | |
|  | TEST STEP | | EXPECTED TEST RESULTS | P | F |
| 1. |  | |  |  |  |
| 2. |  | |  |  |  |
| 3. |  | |  |  |  |

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Таблица результатов (в данных)** | | | | | |
|  | **1** | **2** | **3** | **4** | **5** |
| [Поле данных 1] | [набор данных 1 входные данные поля 1] |  |  |  |  |
| [Поле данных 2] | [набор данных 1 входные данные поля 2] |  |  |  |  |
| [Поле данных 3] | [набор данных 1 входные данные поля 3] |  |  |  |  |

* 1. **<Метод испытаний 2>**

[…]

* 1. **…**

[…]

* + - 1. **Отчётность**

[Опишите порядок оформления отчётности по итогам выполнения настоящей программы и методики испытаний: акты приёмки, мотивированные отказы, иные документы, которые должны подписать стороны в зависимости от результатов.]

1. В соответствии с образцами, прилагаемыми к настоящему ТЗ. [↑](#footnote-ref-1)
2. Элемент конструкторской документации. Должен быть составлен Исполнителем в соответствии с образцом, прилагаемым к настоящему ТЗ, согласован Заказчиком и включён в состав технического проекта (приобщён к результатам работ). [↑](#footnote-ref-2)
3. Тестирование безопасности, которое обнаруживает ошибки кодирования и лазейки в программном обеспечении, операционных средах или сетях. Фаззинг включает в себя ввод большого количества случайных данных, называемых fuzz, в тестируемое программное обеспечение, чтобы заставить его дать сбой или прорвать его защиту. [↑](#footnote-ref-3)
4. <https://github.com/AFLplusplus/AFLplusplus> [↑](#footnote-ref-4)
5. Запись на носитель, в базу данных, на экран, на печать, передачу по сети и так далее. [↑](#footnote-ref-5)
6. Могут быть получены за счёт указания договоров/соглашений при наличии соответствующей связи. [↑](#footnote-ref-6)
7. Так, например, выгрузка персональных данных связанных с объектами предметных областей запрещена для всех групп пользователей, кроме принадлежащих к группе «Операторы персональных данных». Их состав может быть установлен администратором Системы в соответствии с распорядительными документами Агентства. Здесь и далее, во всех выгрузках должно применяться настоящее требование. [↑](#footnote-ref-7)
8. Для реализации модели данных, содержащих признаки статусов («поступает повторно», «акселерация» и т. д.), классификации записей («направление», «дивизион» и т. д.) в реестрах и прочих методов категоризации данных. [↑](#footnote-ref-8)
9. Требование является «сквозным», действующим для всех подсистем, описываемых настоящим техническим заданием, в которых идёт речь об управлении данными, относящимися к непосредственной деятельности Агентства. [↑](#footnote-ref-9)
10. Конклюдентное действие — действие, показывающее желание вступления в правоотношения в форме демонстрации определённого поведения, подтверждающего волеизъявление субъекта. [↑](#footnote-ref-10)
11. Здесь имеется ввиду полный перечень групп пользователей, характерных для системы. В том числе тех, которые на момент утверждения технического задания были не определены. Справочник может расширяться, быть репликой любого другого, в том числе, внешнего справочника. [↑](#footnote-ref-11)
12. Может возникать в случае, когда для конкретной функции системы ожидаемый эффект неприменим (запрет регистрации некого события невозможен, например). [↑](#footnote-ref-12)
13. Может возникать в случае ошибки или невозможности установить группу правил, подходящих для вычисления действия. [↑](#footnote-ref-13)
14. Обращение к справочнику групп: предопределённое значение группы или обращение к функции разыменования элемента справочника. [↑](#footnote-ref-14)
15. Обращение к классификатору видов мероприятий: предопределённое значение группы или обращение к функции разыменования элемента справочника. [↑](#footnote-ref-15)
16. Обращение к классификатору мандатов: предопределённое значение группы или обращение к функции разыменования элемента справочника. [↑](#footnote-ref-16)
17. Может быть пустым. [↑](#footnote-ref-17)
18. Определения способа устранения конфликтов правил. [↑](#footnote-ref-18)
19. Речь идёт об атрибутах, доступных для обращения к ним из исходных кодов правил. [↑](#footnote-ref-19)
20. Может включать пользователей и группы. [↑](#footnote-ref-20)
21. Шаблоны документов оформлены в виде приложений к настоящему техническому заданию. [↑](#footnote-ref-21)