РАЗРАБОТКА ВЕДОМСТВЕННОЙ ИНФОРМАЦИОННОЙ СИСТЕМЫ «ЛЕСОПОЛЬЗОВАНИЕ»

# ВВЕДЕНИЕ

С 2009 года функционирует государственный некоммерческий интернет-портал «Госуслуги». Система обеспечивает доступ юридическим и физическим лицам к получению в электронной форме государственных и муниципальных услуг. Все услуги, размещенные на портале, соотнесены с конкретным регионом России. К концу 2023 года на данном портале зарегистрировано 109 млн россиян.

В Свердловской области существует информационная система для организации мониторинга социально-экономического развития. Система состоит из следующих подсистем:

* Система управления социально-экономическими показателями,
* Подсистема автоматизации технологических процессов ИОГВ,
* Региональная геоинформационная система,
* Система управления информацией здравоохранения,
* Региональная интеграционная платформа.

С системой интегрированы следующие ведомственные информационные системы для оказания услуг со следующими названиями:

* Инвестиционный комплекс
* Недропользование
* Кадастр ООПТ
* Водопользование
* Экология
* Агропромышленный комплекс

12.04.2022 на портале «ЕИС ЗАКУПКИ» был размещен открытый конкурс в электронной форме с номером [№ 0162200011822000790](https://zakupki.gov.ru/epz/order/notice/ok20/view/common-info.html?regNumber=0162200011822000790). Объектом закупки, в рамках конкурса, является выполнение работ по созданию ведомственной информационной системы «Лесопользование Свердловской области». Размещение осуществил департамент государственных закупок Свердловской области. Исполнителем, по результатам конкурса, стала компания ООО «Техноком» в которой я проходил практики, предусмотренные в рамках обучения в ТюмГУ. В рамках дипломной работы будет представлен процесс анализа предметной области, проектирования программного продукта и реализации этого продукта.

На этом введение в диплом заканчивается, но для отчета по практике я продолжу

ООО «Техноком» предоставляет услуги полного цикла по разработке, внедрению и сопровождению программных решений. Компания имеет ряд программных продуктов собственной разработки: BDSA-GIS, UIP\_ESERVICE, BDSA-REPORTING, NOVAGIS и еще 6 других.

!Сказать про другие проекты! – животные, газпром, мигранты

# ОПИСАНИЕ ПРЕДМЕТНОЙ ОБЛАСТИ

## Основная проблема

Министерство предоставляет некоторый список услуг. Для каждой услуги пакет документов и атрибутивный состав заявления уникальный. Министерству приходится совершать лишнюю работу – объяснять заявителям какое заявление необходимо заполнить и какие документы необходимо приложить.

При оформлении права пользования участком необходимо приложить картографическую информацию. До момента разработки и внедрения системы министерство пользовалось бумажными картами.

При подаче заявления для образования участка необходимо проверить пересечение границ образуемого участка с другими участками: охраняемые зоны, заповедники, водоохранные зоны и др.

Также разрабатываемая система формализует путь работы над заявлением.

Бывали случаи, когда министерство забывало позвонить заявителю о готовности итоговых документов, заявителю самому приходилось звонить/приходить в министерство для получения информации о готовности итоговых документов/отказе в предоставлении услуги.

**Цель разработки системы, определенная заказчиком:** повышение эффективности принятия решений по управлению лесным хозяйством, носящих заявительный характер (мне кажется, что важно сказать про заявления как можно раньше). в части обеспечения органов государственной власти точной, полной и непротиворечивой информацией о лесах, об их использовании, охране, защите, воспроизводстве, а также оптимизировать процесс сбора, хранения и предоставления информации государственного лесного реестра.

## Первоначальные требования заказчика

Первоначальные требования заказчика к ИС предоставлены в описании объекта закупки (<https://zakupki.gov.ru/44fz/filestore/public/1.0/download/priz/file.html?uid=DC589E20FC353859E05334548D0AAAD7>).

Система предназначена для двух категорий лиц: заявители (юридические, физические, ИП) и сотрудников Министерства природных ресурсов Свердловской области отдела учета земель и организации использования лесов.

Заказчик требует обеспечить возможность прохождения цикла процесса комплексного лесопользования. Комплексное лесопользование состоит из следующих бизнес-процессов:

1. оформление права пользования лесным участком отдела организации лесопользования, лесовосстановления и государственной экспертизы проектов освоения лесов;
2. проведение государственной экспертизы проектов освоения лесов, расположенных на землях лесного фонда;
3. согласование проекта рекультивации нарушенных земель/проекта лесовосстановления;
4. утверждение акта лесопатологического обследования;
5. предоставление выписки из государственного лесного реестра;
6. прием лесной деклараций и отчетов об использовании лесов.

Обобщенно каждый из бизнес-процессов, кроме последнего, подразумевает следующий порядок действий: регистрация заявления, рассмотрение заявления, вынесение решения по заявлению, выдача подписанного итогового документа (акт, выписка, договор, решение, извещение) или уведомление об отказе в предоставлении услуги. Процесс под номером 7 – подается лесная декларация, проверяется правильность заполнения декларации, выносится решение о принятии декларации.

## Описание бизнес-процессов

Атрибутивный состав заявлений, обязательных прилагаемых документов, итоговых документов будет рассмотрен в следующей части главы.

* + 1. Описание оформления права пользования лесным участком

Заявитель подает заявление на предварительное согласование лесного участка, прикладывая проектную документацию. Министерство регистрирует заявление в своем документообороте и проверяет его на корректность. Если заявителю предварительно согласовали участок, то заявителю необходимо подать заявление о предоставлении в пределах земель лесного фонда лесного участка в пользование. После рассмотрения заявления министерство направляет заявителю копии решения уполномоченного органа о предоставлении лесного участка, либо извещения об отказе в предоставлении услуги.

* + 1. Проведение государственной экспертизы

Заявитель подает заявление о предоставлении государственной услуги по проведению государственной экспертизы проектов освоения лесов, расположенных на землях лесного фонда. Министерство регистрирует заявление в своем документообороте и проверяет его на корректность. Проводит экспертизу, подготавливает заключение (положительное либо отрицательное) государственной экспертизы проекта освоения лесов, расположенных на землях лесного фонда. Утверждает и выдаёт заключение государственной экспертизы проекта освоения лесов, расположенных на землях лесного фонда.

* + 1. Согласование проекта рекультивации нарушенных земель/проекта лесовосстановления

Заявитель подает заявление на согласование проекта. Министерство регистрирует заявление в своем документообороте и проверяет его на корректность. Рассматривает заявку и приложенные документы. Направляет заявителю извещение о приеме проекта или отказе в приеме проекта рекультивации нарушенных земель/ проекта лесовосстановления.

* + 1. Утверждение акта лесопатологического обследования

Заявитель подает заявление на проведение лесопатологического обследования. Министерство регистрирует заявление в своем документообороте и проверяет его на корректность. После проведения лесопатологического обследования министерство принимает акт обследования, утверждает его.

* + 1. Предоставление выписки из государственного лесного реестра

Заявитель подает заявление на предоставление выписки из государственного лесного реестра. Министерство регистрирует заявление в своем документообороте и проверяет его на корректность, принимает решение о предоставлении выписки из государственного лесного реестра либо об отказе в предоставлении такой выписки. Уведомление заявителя о размере платы за предоставление выписки. Получение документа, подтверждение перечисление платы. Подготовка и выдача выписки.

* + 1. Прием лесной деклараций и отчетов об использовании лесов

Заявитель подает лесную декларацию/отчет об использовании лесов. Министерство регистрирует заявление в своем документообороте и проверяет его на корректность. Принимает лесную декларацию/отчет об использовании лесов/Отказывает в принятии заявления с обоснованием причин отказа. Уведомляет заявителя о принятом решении.

## Атрибутивный состав заявлений

Сведения о заявителе в каждой из услуг одинаковые, вынесем их в отдельный пункт, чтобы не повторяться.

* + 1. Сведения о заявителе

Заявитель – физическое лицо

* фамилия, имя, отчество,
* дата рождения,
* ИНН,
* СНИЛС,
* Адрес проживания
* Контактный телефон
* Электронная почта

Заявитель – юридическое лицо

* Полное наименование организации
* Кратное наименование организации
* ИНН
* КПП
* ОГРН
* Почтовый адрес
* Юридический адрес
* Контактный телефон
* Электронная почта

Заявитель – индивидуальный предприниматель

* Наименование
* ИНН
* ОГРН ИП
* Почтовый адрес
* Юридический адрес
* Контактный телефон
* Электронная почта
  + 1. Описание оформления права пользования лесным участком
* **Лесной участок**
* Вид использования лесов
* Цель, под которую испрашивается лесной участка
* Срок использования лесного участка
* Обоснование цели, вида, срока использования лесного участка
* Банковские реквизиты

Дополнительные документы при получении данной услуги не нужны.

* + 1. проведение государственной экспертизы
* Банковские реквизиты
* Правоустанавливающий документ
* Срок использования (до какой даты)

Для получения услуги необходимо предоставить проект освоения лесов

* + 1. согласование проекта рекультивации нарушенных земель/проекта лесовосстановления
* Исполнитель услуги
* Правоустанавливающий документ
* **Участок, подлежащий восстановлению**

Для получения услуги необходимо предоставить XML-файл проекта лесовосстановления.

* + 1. утверждение акта лесопатологического обследования
* Правоустанавливающий документ
* **Лесопатологический выдел**
* Кадастровый номер
* Способ лесопатологического обследования

Для получения услуги необходимо предоставить проект освоения лесов

* + 1. предоставление выписки из государственного лесного реестра
* Наименование запрашиваемой информации
* Уточнение запрашиваемых сведений
* **Местоположение**

Для подачи заявления обязательных документов нет, но для получения услуги необходимо предоставить документ-подтверждение оплаты

* + 1. прием лесной деклараций и отчетов об использовании лесов
* Номер лесной декларации
* Декларируемый период
* Наименование органа государственной власти, ОМСУ
* Правоустанавливающий документ
* Виды использования лесов
* **Объекты лесной инфраструктуры**
* Отметка о согласии на обработку персональных данных

Для получения услуги необходимо предоставить XML-файл декларации с приложениями

В большей части предоставляемых услуг заявителю необходимо приложить картографическую информацию (выделено жирным ранее), а сотруднику министерства необходимо проверить на пересечение с другими участками, водоохранными зонами, заповедниками и др.

## Обоснование необходимости разработки программы

* + 1. Со стороны государства

Данная система разрабатывается в рамках государственной стратегии развития информационного общества в Российской Федерации <http://pravo.gov.ru/proxy/ips/?docbody=&nd=102431687>. «Целью развития информационной и коммуникационной инфраструктуры Российской Федерации является обеспечение свободного доступа граждан и организаций, органов государственной власти Российской Федерации, органов местного самоуправления к информации на всех этапах ее создания и распространения.»

* + 1. Со стороны министерства

Уменьшение времени для работы над заявлением.

* + 1. Со стороны заявителя

Упрощение подготовки заявления. Прозрачность работы над заявлением.

## Аналоги госуслуг

Аналогов нет, т. к. система разрабатывается для каждого округа отдельно.

## Постановка задач

Стадии разработки, этапы работ выделены в госте 19.102–77. Напишем задачи к каждому этапу работ основываясь на этапах, прописанных в госте.

* + 1. Обоснование необходимости разработки
* Определить цели
* Поставить задачи
* Проанализировать наличие аналогов
  + 1. Научно-исследовательские работы
* Изучить структуру министерства
* Изучить документооборот министерства
* Определить структуру потоков данных внутри системы и при обмене с внешними системами
* Определить требования к техническим средствам
* Определить бизнес-процесс в нотации BPMN после внедрения системы
  + 1. Разработка технического проекта
* Определить классы в нотации UML
* Уточнить структуры данных для внутреннего и внешнего обмена
* Разработка логической модели данных в нотации UML для хранения в базе данных
* Разработка серверного приложения для работы с данными
* Планирование интеграции с системой авторизации и идентификации
* Планирование интеграции с геосервером
* Планирование интеграции с электронным документооборотом Свердловской области
  + 1. Утверждение технического проекта
* Согласование и утверждение технического проекта
  + 1. Разработка программы
* Разработка физической модели базы данных
* Программирование и тестирование программы
* Программирование интеграций между запланированными системами
  + 1. Подготовка и передача программы
* Подготовка программной документации
* Оформление и утверждение акта о передаче программы

## Функциональные требования

Без авторизации (гость):

* Просмотр главной страницы
* Просмотреть каталог предоставляемых услуг для юридических лиц, для предпринимателей, для физических лиц
* Просмотр детальной информации о каждой услуге:
  + Административный регламент;
  + Стоимость и сроки оказания услуги;
  + Основания отказа;
  + Документы, необходимые для получения услуги;
* Авторизация через госуслуги
* Авторизация по логину и паролю

Функции личного кабинета доступные заявителю (авторизация через госуслуги):

* Все функции гостя, кроме авторизации,
* Выйти из учетной записи,
* Просмотреть все свои черновики заявлений, поданные заявления
* Просмотреть зарегистрированные участки на карте
* Выбрать участок на цифровой карте
* Просмотреть информацию и местоположение на карте о выбранном лесном участке:
  + Наименование
  + Вид рубки
  + Способ рубки
  + Лесничество
  + Участковое лесничество
  + Участок (урочище)
  + Квартал
  + Выдел
  + Лесопользователь
  + Договор аренды лесного участка
  + Номер лесной декларации
  + Декларируемый период
* Редактировать свой профиль,
* Создать черновик заявления,
* Удалить черновик своего заявления,
* Редактировать черновик своего заявления
* Загрузить файлы (электронные документы) к заявлению,
* Подать заявление,
* Отменить подачу заявления (до момента взятия заявления в работу),
* Скачать файлы (итоговые документы).

Функции личного кабинета доступные сотруднику (авторизация по корпоративному логину и паролю):

* Все функции личного кабинета заявителя,
* Открыть поданные заявления,
* Открыть заявления, назначенные на сотрудника,
* Зарегистрировать заявление в СЭД ПСО,
* Скачать приложенные файлы,
* Сгенерировать файл .docx (итоговый документ),
* Вынесение решения по заявлению (Одобрено, оказано, не вынесено),
* Подписать итоговые документы (файлы) в СЭД ПСО
* Завершить работу с заявлением.
  1. Интеграции со сторонними системами

Анализируя все вышесказанное и уже эксплуатирующиеся системы и подсистемы напрашиваются интеграции со следующими системами: интеграция с геосервером для работы с пространственной информацией; интеграция с ЕСИА для идентификации и авторизации заявителей и автоматического пред заполнения профиля, заявлений; интеграция с интеграционным блоком – для взаимодействия с СЭД ПСО через посредника, интеграция нужна для регистрации заявлений и подписания итоговых документов.

* 1. Средства разработки
* Язык программирования Java 17
* Серверный фреймворк – Spring Boot 2.7.6
* ORM – Hibernate
* Модульное тестирование - JUnit v5.9.1
* Тестирование HTTP запросов – Postman v10.23.5
* Средство для проектирования базы данных – StarUML
* СУБД – PostgreSQL

1. па

# Проектирование архитектуры ИС

## Описание бизнес-логики

В системе будет следующий список ролей: гость, сотрудник, заявитель.

Гость имеет доступ к каталогу услуг, странице авторизации, главной странице

Заявитель имеет доступ к личному кабинету (заявления, карта Свердловской области, уведомления), странице получения услуги (создание черновика заявления), к странице учетной записи (информация о пользователе, организации)

Сотрудник имеет доступ к списку поданных заявлений, к странице поданного заявления, к странице с реестрами, к странице с заявителями, к странице с уведомлениями, к странице с отчетностью (статистической, управленческой)

**Открытая часть без авторизации:**

Пользователь авторизуется через ЕСИА (единая система идентификации и авторизации), после авторизации профиль пользователя автоматически создаётся, присваивается роль заявитель.

**Заявитель после авторизации:**

* Изменение данных профиля – после перехода на страницу учетной записи пользователь может поменять ФИО, Дата рождения, ИНН, СНИЛС, Адрес проживания, Адрес регистрации, Контактный телефон, Электронная почта. Привязать, отвязать организации.
* Работа с заявлением – пользователь выбирает необходимую услугу. Нажимает на кнопку «Получить услугу». Создаётся черновик заявления. Данные заявителя автоматически подставляется в созданное заявление. Пользователю необходимо заполнить блок «дополнительных данных» - индивидуален для каждой услуги. Прикладывается комплект документов в виде сканов документов. Система не даст подать заявление, если не заполнены все обязательные поля, приложены все обязательные документы (файлы), если в заявлении используется картографическая информация, то система автоматически проверит образуемый участок на пересечения с охранными зонами или уже образованными участками. Рассмотрим в следующем пункте выбор/создание земельного(лесного) участка при заполнении дополнительных данных заявления.
* Создание/Выбор земельного участка – Для определения местоположения участка выбирается лесничество, квартал. После выбора, в зависимости от выбранного местоположения, пользователю необходимо ввести границы участка в границах выбранного квартала/лесничества.

**Сотрудник, после авторизации через корпоративную учетную запись:**

* Работа с заявлениями – сотрудник открывает заявление, проверяет приложенные документы, выносит решение по заявлению, система автоматически формирует итоговый документ. Сотрудник проверяет его и отправляет на подписание в СЭД ПСО. После подписания документа заявитель оповещается о готовности итогового документа. Сотрудник завершает работу над заявлением.

<https://uslugi.egov66.ru/forest/workspace/requests/2262912#data>

## Диаграмма бизнес-процессов после внедрения разработки в нотации BPMN

Построена диаграмма модели бизнес-процесса с использованием разрабатываемой системы в нотации BPMN.

НАРИСОВАТЬ

## Описание диаграммы бизнес-процессов

Участники: Система, сотрудник организации, заявитель, заявитель, геосервер, ЕСИА, интеграционный блок.

Вход: Заявление

Выход: Итоговый(е) документ(ы)

Документы:

Задачи:

## Схема классов для работы с заявлениями в нотации UML

## Словарь схемы классов для работы с заявлениями

## Логическая модель данных

## Словарь логической модели данных

## Взаимодействие информационной системы другими системами

Разберем подробнее правила обмена данными с каждой из системы.

* + 1. Описание взаимодействия с ЕСИА
       1. **Изучение механизмов ЕСИА**

ЕСИА предоставляет два механизма аутентификации:

* механизм, основанный на стандарте SAML версии 2.0;
* механизм, основанный на модели OpenID Connect 1.0.

**Аутентификация с использованием стандарта SAML**

ЕСИА использует стандарт SAML версии 2.0, который был разработан в 2005 году концерном OASIS. SAML базируется на языке XML и определяет способы обмена информацией об аутентификации пользователей, их полномочиях и идентификационных данных. В соответствии с принятой в этом стандарте терминологией, ЕСИА выступает в роли доверенного поставщика идентификации (Identity Provider), а система выступает в роли поставщика услуг (Service Provider).

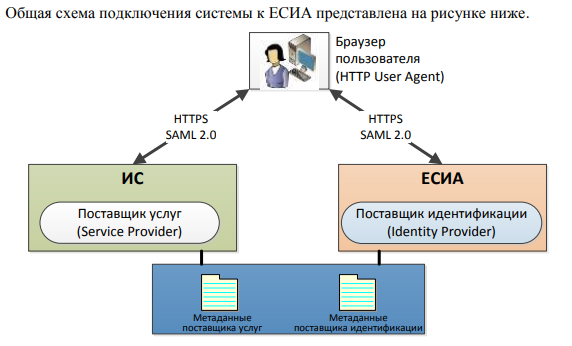


Рисунок 1 - Схема взаимодействия ИС с ЕСИА с целью идентификации и аутентификации с использованием стандарта SAML 2.0

**Аутентификация с использованием модели OpenID Connect**

В ЕСИА создан механизм аутентификации пользователей, основанный на спецификациях OAuth 2.0 и расширении OpenID Connect 1.0.

Протокол определяет взаимодействие следующих сторон:

* владелец ресурса (resource owner) – сущность, которая может предоставить доступ к защищаемому ресурсу (например, физическое лицо, заявитель);
* система-клиент (client) – приложение, которое запрашивает доступ к защищаемому ресурсу от имени его владельца;
* сервис авторизации (authorization server) – сервис, который выпускает для системы клиента маркеры идентификации с разрешениями от владельца ресурса, а также маркеры доступа, позволяющие получать доступ к данным;
* поставщик ресурса (resource server) – сервис, обеспечивающий доступ к защищаемому ресурсу на основе проверки маркеров идентификации и маркеров доступа (например, к идентификационным данным пользователя).

Расширение OpenID Connect 1.0 предполагает использование маркера идентификации (ID Token) в целях проведения идентификации и аутентификации пользователя. Маркер идентификации содержит идентификационные данные пользователя, а также ряд служебных параметров (дата выдачи, время окончания срока действия и пр.).

Для иллюстрации использования OpenID Connect 1.0 в ЕСИА принята следующая терминология:

* владелец ресурса – это пользователь;
* система-клиент – это информационная система, интегрированная с ЕСИА с целью идентификации и аутентификации, например региональный портал услуг;
* сервис авторизации и поставщик ресурса – это ЕСИА.

Общая схема подключения системы к ЕСИА для проведения аутентификации представлена на рисунке ниже.

Изображение выглядит как текст, снимок экрана, диаграмма, линия

Автоматически созданное описание

Рисунок 2 - Схема подключения системы к ЕСИА

Изучив оба механизма, было принято решение использовать второй механизм аутентификации.

* + - 1. **Описание сценария работы с ЕСИА**

Сценарий включает следующие шаги:

1. Пользователь нажимает на веб-странице системы-клиента кнопку «Войти через ЕСИА».

2. Система-клиент формирует и отправляет в ЕСИА запрос на аутентификацию и перенаправляет браузер пользователя на специальную страницу предоставления доступа.

3. ЕСИА осуществляет аутентификацию пользователя одним из доступных способов. Если пользователь ещё не зарегистрирован в ЕСИА, то он может перейти к процессу регистрации.

4. Когда пользователь аутентифицирован, ЕСИА сообщает пользователю, что система-клиент запрашивает данные о нем в целях проведения идентификации и аутентификации, предоставляя перечень запрашиваемых системой-клиентом сведений.

5. Если пользователь дает разрешение на проведение аутентификации системой-клиентом, то ЕСИА выдает системе-клиенту специальный авторизационный код.

6. Система-клиент формирует в адрес ЕСИА запрос на получение маркера идентификации, включая в запрос полученный ранее авторизационный код.

7. ЕСИА проверяет корректность запроса (например, что система-клиент зарегистрирована в ЕСИА) и авторизационного кода и передает системе-клиенту маркер идентификации.

8. Система-клиент извлекает идентификатор пользователя из маркера идентификации. Если идентификатор получен, а маркер проверен, то система-клиент считает пользователя аутентифицированным.

После получения маркера идентификации система-клиент использует REST-сервисы ЕСИА для получения дополнительных данных о пользователе, предварительно получив соответствующий маркер доступа.

Изображение выглядит как текст, снимок экрана, Параллельный, линия

Автоматически созданное описание

* + - 1. **Технологии интеграции**

Интеграция с ЕСИА (получение данных о пользователе) реализуется через REST запросы к сервису единой идентификации и авторизации.

* + - 1. **Используемые конечные точки**

Рассмотрим запросы, отправляемые в ЕСИА и получаемые из ЕСИА.

* + - * 1. **Получение авторизационного кода**

GET <https://esia.gosuslugi.ru/aas/oauth2/ac>

некоторые параметры запроса:

* client\_id - идентификатор системы-клиента (мнемоника системы в ЕСИА);
* client\_secret – подпись запроса в формате PKCS#7 detached signature в кодировке UTF8 от значений четырех параметров HTTP–запроса: scope, timestamp, clientId, state (без разделителей). должен быть закодирован в формате base64 url safe. Используемый для проверки подписи сертификат должен быть предварительно зарегистрирован в ЕСИА и привязан к учетной записи системы-клиента в ЕСИА. ЕСИА поддерживает сертификаты в формате X.509. ЕСИА поддерживает алгоритмы формирования электронной подписи RSA с длиной ключа 2048 и алгоритмом криптографического хэширования SHA-256, а также алгоритм электронной подписи ГОСТ Р 34.10–2001 и алгоритм криптографического хэширования ГОСТ Р 34.11-94.
* redirect\_uri – ссылка, по которой должен быть направлен пользователь после того, как даст разрешение на доступ к ресурсу, в нашем случае: <https://esia.egov66.ru/auth/realms/rgis/broker/esia/endpoint>;
* scope – область доступа, т. е. запрашиваемые права; например, если система-клиент запрашивает доступ к сведениям о сотрудниках организации, то scope должна иметь значение http://esia.gosuslugi.ru/org\_inf (с необходимыми параметрами); если запрашивается scope http://esia.gosuslugi.ru/usr\_inf58 (данные о пользователе), то не нужно в качестве параметра указывать oid этого пользователя;
* state – набор случайных символов, имеющий вид 128-битного идентификатора запроса (необходимо для защиты от перехвата), генерируется по стандарту UUID;
* scope – область доступа, т.е. запрашиваемые права; передаётся наименование полей с личной информацией, пример: fullname, birthdate, snils, email¸ gender, citizenship, birthplace, addresses.

Если в ходе авторизации не возникло ошибок, то ЕСИА осуществляет редирект пользователя по ссылке, указанной в redirect\_uri, а также возвращает обязательные параметры:

code – значение авторизационного кода;

state – значение параметра state, который был получен в запросе на авторизацию; система-клиент должна провести сравнение отправленного и полученного параметра state.

* + - * 1. **Получение маркера доступа в обмен на авторизационный код**

Когда авторизационный код получен, система-клиент может сформировать запрос методом POST: <https://esia.gosuslugi.ru/aas/oauth2/te> для получения маркера доступа. В тело запроса должны быть включены следующие сведения:

client\_id – идентификатор системы-клиента (мнемоника системы в ЕСИА);

code – значение авторизационного кода, который был ранее получен от ЕСИА и который необходимо обменять на маркер доступа;

grant\_type – принимает значение “authorization\_code”, если авторизационный код обменивается на маркер доступа;

client\_secret – подпись запроса в формате PKCS#7 detached signature в кодировке UTF8 от значений четырех параметров HTTP–запроса: scope, timestamp, clientId, state (без разделителей). client\_secret должен быть закодирован в формате base64 url safe.

state – набор случайных символов, имеющий вид 128-битного идентификатора запроса (необходимо для защиты от перехвата), генерируется по стандарту UUID; этот набор символов должен отличаться от того, который использовался при получении авторизационного кода;

redirect\_uri – ссылка, по которой должен быть направлен пользователь после того, как даст разрешение на доступ (то же самое значение, которое было указано в запросе на получение авторизационного кода);

scope – область доступа, т.е. запрашиваемые права (то же самое значение, которое было указано в запросе на получение авторизационного кода);

timestamp – время запроса маркера в формате yyyy.MM.dd HH:mm:ss Z (например, 2013.01.25 14:36:11 +0400), необходимое для фиксации начала временного промежутка, в течение которого будет валиден запрос с данным идентификатором (<state>);

token\_type – тип запрашиваемого маркера, в настоящее время ЕСИА поддерживает только значение “Bearer”.

Если запрос успешно прошел проверку, то ЕСИА возвращает ответ в формате JSON:

access\_token – маркер доступа для данного ресурса;

expires\_in – время, в течение которого истекает срок действия маркера (в секундах);

state – набор случайных символов, имеющий вид 128-битного идентификатора запроса, генерируется по стандарту UUID (совпадает с идентификатором запроса);

token\_type – тип предоставленного маркера, в настоящее время ЕСИА поддерживает только значение “Bearer”;

refresh\_token – маркер обновления для данного ресурса.

Пример ответа:

{

“access\_token” :

“eyJhbGciOiJSUzI1NiIsInNidCI6ImFjY2VzcyIsInR5cCI6IkpXVCIsInZlciI6MX0.eyJleHAiOjEzNTk1NDAxODcsInNjb3BlIj

oiaHR0cDpcL1wvZXNpYS5nb3N1c2x1Z2kucnVcL2VtcF9pbmY\_b3JnX29pZD0xMDAwMDAwMzU3IiwiaXNzIjoiaHR0cDpcL1wvZXNpY

S5nb3N1c2x1Z2kucnUiLCJuYmYiOjEzNTk1MzY1ODcsInVybjplc2lhOnNpZCI6IjE2ZDdmOTNkLTZjZTgtNDE3OS04ZmFmLTdmZDQ2

ZDMyMDhhNiIsInVybjplc2lhOnNial9pZCI6MTAwMDAwMDM4NSwiY2xpZW50X2lkIjoiRVNJQSIsImlhdCI6MTM1OTUzNjU4N30”,

“expires\_in” : 3600,

“state” : “9be638a9-0e05-42e1-b4f8-a3e30457fbdd”,

“token\_type” : “Bearer”,

“refresh\_token” : “54039d1f-9917-43cd-961a-2729c891ef8c”

}

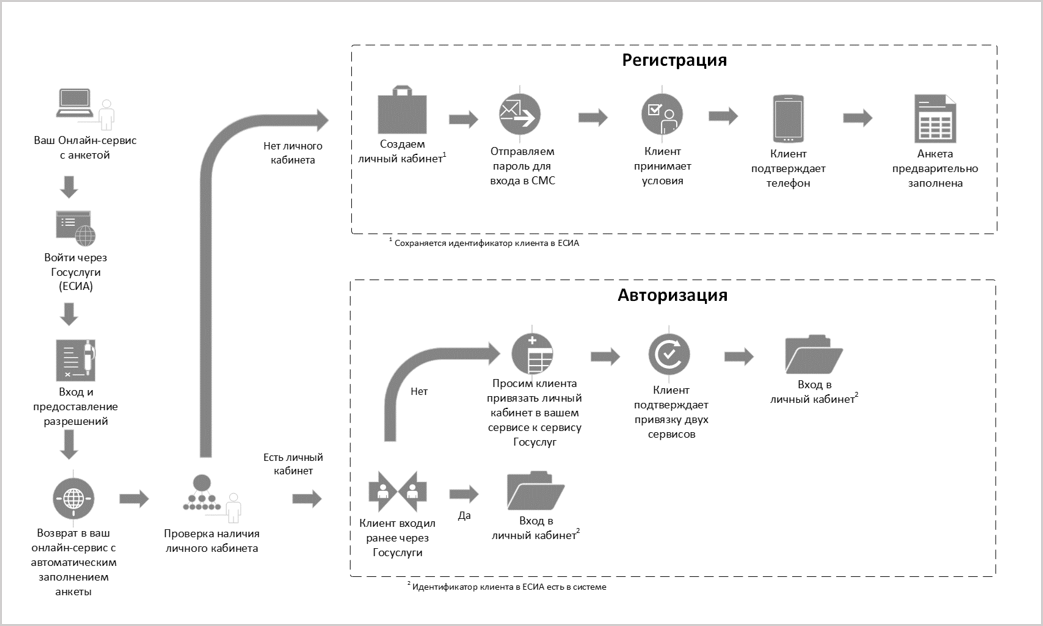


Рисунок 3 - Взаимодействие с ЕСИА

* + - 1. **Диаграмма классов сообщений**
    1. **Описание взаимодействия с геосервером**
       1. **Технология интеграции**

Интеграция с геосервером осуществляется через REST API.

* + - 1. **Используемые конечные точки**
         1. **Поиск пересечений**

POST <http://dkrekb.rusoft.tech:8104/intersector/intersector-controller/findIntersect>

BODY

{

"cad\_num": "66:41:0210047:32",

"sourceGuid": "0bdf48cc-a607-4b66-bbc2-67eee5d8dd59",

"sourceLayer": "master:params\_land",

"bufferSize": 0,

"intersectLayers": [

"master:zone\_egrn",

"master:forest\_qrtrs\_off"

}

* + - 1. **Диаграмма классов сообщений**
    1. **Описание взаимодействия с интеграционным блоком. Интеграция с СЭД ПСО**

Сотрудник отправляет на подписание документ в СЭД ПСО, система формирует сообщение в виде зип пакета и сохраняет в условленной исходящей директории, откуда интеграционный блок перенаправляет его в СЭД ПСО. Система мониторит входящую директорию – в эту директорию интеграционный блок направляет пакет от СЭД ПСО с информацией о получении нашего пакета и, после регистрации или подписания документа, направляет пакет с регистрационными данными или с подписанным документом. Логику обработки ответных сообщений рассмотрим позже.

* + - 1. **Технологии интеграции**

Технологии интеграции определены технологией интеграционного блока.

Интеграция с интеграционным блоком проходит через файловую систему. Сообщениями при таком обмене являются ZIP файлы – пакеты. Пакет содержит в себе XML файл с описанием содержимого зип пакета и со служебной информацией, файлы, приложенные к заявлению, или подписываемый документ.

* + - 1. **Диаграмма классов сообщений**

В обмене с сообщениями используются 4 вида документов:

* входящий документ
* внутренний документ
* распорядительный документ
* исходящий документ
  + - 1. **Рассмотрим логику обработки ответных пакетов:**
* **Квитанция о получении пакета**: логируется дата и время получения сообщения, меняется статус пакета.
* **Регистрационные данные**: логируется дата и время получения пакета с регистрационными данными, у заявления устанавливаются регистрационный номер и дата, статус заявления меняется на «Зарегистрировано»
* **Подписанный документ**: логируется дата и время получения пакета с подписью. В документ запроса устанавливается регистрационный номер, дата, обновляется наименование документа, статус документа меняется на "Подписан". Статус заявления меняется на Завершено. Так же в пакете присылают файл-документ с прикрепленной и открепленной подписью. Пакет сохраняется на ФХ нашей системы и прикрепляется к заявлению.
  + - 1. **Типы документов использующиеся в каждом бизнес-процессе**

# Разработка технического решения

Подтверждение, что система в промышленной эксплуатации: <https://midural.ru/news/vministerstvah/page1/document222264/>

RgisRoleAssignmenter <https://javarush.com/quests/lectures/questspringsecurity.level01.lecture10> - прочитать