## Development of the infrastructure of automatic interaction of the university with GIS "Postupaj v vuz onlajn"

Keywords: REST, superservice, Python, JWT, entrant, admission, EDS, Windows services

The article discusses the development and implementation of information system components for interaction with the state information system "Superservice: Postupaj v vuz onlajn" on the basis of the Pacific State University. The prerequisites for the development, legislative, functional and information protection requirements for this development are considered.

## Разработка инфраструктуры автоматического взаимодействия ВУЗ-а с ГИС "Поступай в вуз онлайн"

Ключевые слова: REST, суперсервис, Python, JWT, абитуриент, поступление, ЭЦП, службы Windows

В статье рассматривается разработка и реализация компонентов информационной системы для взаимодействия с государственной информационной системой «Суперсервис: Поступай в вуз онлайн» на базе Тихоокеанского государственного университета. Рассматриваются предпосылки к разработке, законодательные, функциональные и требования к защите информации для данной разработки.

## Термины и определения

**ЭВМ** – электронно-вычислительная машина.

**СУБД** – система управления базами данных.

**REST** – Representational State Transfer, репрезентативная передача состояния – это архитектурный стиль, который позволяет создавать реализацию клиента и сервера независимо друг от друга. Сервисы в REST API взаимодействуют по протоколу HTTP.

**API** – это установка функций и правил позволяющая взаимодействовать между программным обеспечением, которое предоставляет API и другими программными компонентами. В Веб разработке, под API обычно подразумевают набор стандартных методов, свойств, событий и URL ссылок для взаимодействия с Веб контентом.

**СКЗИ** — Система(средства) Контроля и Защиты Информации

**JWT** - (сокр. от англ. JSON Web Token) – это JSON-объект, который определен в открытом стандарте RFC 7519. JWT состоит из трех частей: Header, Payload и Signature, представляющих собой строки в формате Base64, разделенные символом точка.

**ЭЦП (ЭП)** — Электронная Цифровая Подпись

**ORM** - Object-Relational Mapping, технология программирования, которая связывает базы данных с концепциями объектно-ориентированных языков программирования, создавая «виртуальную объектную базу данных»

## Введение

В рамках Федерального проекта «Цифровое государственное управление» национальной программы «Цифровая экономика Российской Федерации» c 2020 года активно проводятся мероприятия по Цифровой трансформации государственных и муниципальных услуг. [2]

**Цифровая трансформация и оптимизация государственных и муниципальных услуг будет базироваться на следующих принципах: [2]**

* в государстве нет физических документов кроме удостоверения личности гражданина;
* запрет на запрос у граждан информации, которая имеется в распоряжении государства, все необходимые документы запрашиваются из электронных реестров органов власти;
* принцип комплексного подхода к решению жизненных ситуаций заявителей посредством **суперсервисов**;
* минимизация участия чиновников в принятии решений по оказанию услуг, перевод услуг в режим online;
* омниканальность (взаимная интеграция) взаимодействия с использованием любых удобных пользователю инструментов обращения за услугами (мобильные устройства, соцсети, сайты, банковские приложения, email);
* проактивное (беспристрастное) предоставление услуг на основании изменения статусов граждан в ведомственных реестрах;
* исключение бумажных носителей в процессах оказания услуг, межведомственного взаимодействия и документооборота между органами власти.

Оптимизация государственных услуг ведется по 2-м направлениям: комплексное решение жизненных ситуаций граждан и бизнеса (далее – Суперсервисы) и цифровая трансформация приоритетных государственных и муниципальных услуг (моносервисы). Одно из направлений реализации т. н. «суперсервисов» - это образование. В рамках него разработана государственная ГИС «Сервис Приема» цели и задачи которой заключаются в выступлении посредником при обмене данными от Единого Портала Государственных Услуг РФ и ВУЗ-ом. Непосредственное требование интеграции устанавливается постановлениями Правительства РФ №958 от 22.05.2022 и №89 от 26.01.2022.

## Постановка задачи, требования

Модуль API Сервиса приема выполнен с применением методологии REST API. Взаимодействие с Сервисом приема посредством API может осуществляется в синхронном или асинхронном режиме. [7]

**Синхронный режим**

При синхронном режиме Сервис приема, получив запрос на выполнение операции, сразу направляет в ответ результаты ее выполнения.

**Асинхронный режим**

При асинхронном режиме обмена операции выполняются с помощью последовательной отправки различных запросов. Как правило, в первом запросе отправляется информация, необходимая для выполнения операции. В ответ получается идентификатор операции. По этому идентификатору пользователь может, с помощью выполнения других запросов, узнать статус выполнения операции или получить результат выполнения операции. [7]

Некоторые запросы требуют включения в JWT отделенной ЭЦП по ГОСТ 34.10-2012.

Таблица 1. Перечень запросов для взаимодействия с ГИС «Сервис Приема»

|  |  |
| --- | --- |
| **Запрос** | **Назначение** |
| /api/session/new | Получение сессионного ключа |
| /api/cls/get | Получение значений классификаторов |
| /api/token/new | Запрос на выполнение асинхронной операции с сущностями |
| /api/token/delay/get | Получение приблизительной оценки времени выполнения асинхронной операции от получения запроса на выполнение (/api/token/new) до выполнения запроса на получение результата (/api/token/own/get) |
| /api/token/own/get | Получение результата выполнения асинхронной операции по идентификатору операции или списка идентификаторов операций, ожидающих получения результата |
| /api/token/despatch/get | Получение JWT, сформированных при выполнении операций, инициатором которых была не образовательная организация (сообщения от ЕПГУ) |
| /api/file/get | Получение файла |
| /api/token/certificate/check | Полная проверка Header и Signature из JWT |

**Взаимосвязи сущностей**

Описанные в документации «Сервиса Приема» сценарии включают в себя выполнение запросов, с помощью которых производятся операции над сущностями, описывающими образовательную организацию, приемную кампанию или поступающего.

Последовательность обращения к сущностям схематично изображена на рисунках ниже.

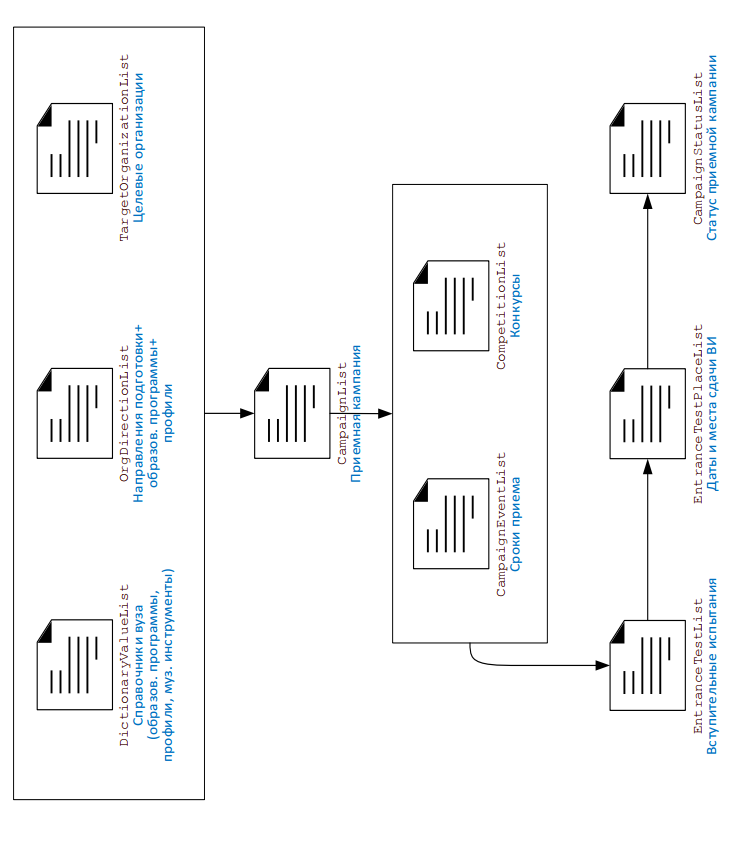


Рисунок 1. Последовательность обращения к сущностям, описывающим приемную кампанию

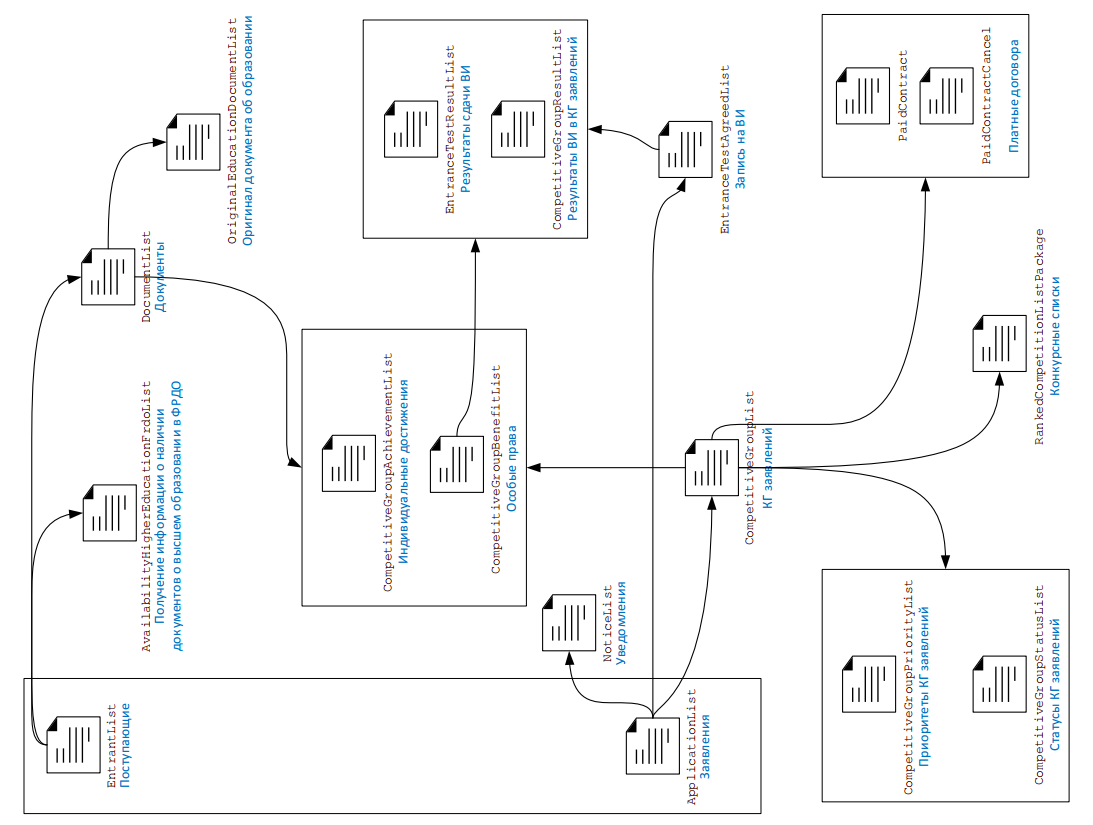
****

Рисунок 2. Последовательность обращения к сущностям, описывающим поступающего и заявление

## Особенности реализации, ключевые особенности

Исходя из выдвинутых спецификацией требований — программный комплекс АИС ТОГУ для взаимодействия с ССПВО должен содержать следующие части:

1. Модуль для приведения вида данных к требуемому виду из БД АИС ТОГУ
2. Модуль для генерации Электронной Цифровой Подписи по алгоритму ГОСТ 34.10-2012
3. Модуль «синхронного» взаимодействия с «Сервисом Приема» по протоколу REST
4. Модуль «асинхронного взаимодействия» с «Сервисом Приема»
5. Удовлетворение требований ФСТЭК по аттестации рабочего места для доступа к закрытой сети №13833
6. Пользовательский интерфейс для взаимодействия оператора с системой

Определим наиболее подходящие в контексте Тихоокеанского Государственного Университета технологии для реализации частей программного комплекса.

Пункт 5 уже реализован ВУЗ в рамках рабочего места с помощью ПАК ViPNet Coordinator. [3]

Для исполнения пункта 2 воспользуемся проприетарным программным обеспечением КриптоПро csp соответствующим крипто провайдером ГОСТ 34.10-2012, устанавливающимся вместе с программой. Выбор КриптоПро обусловлен тем что данный пакет имеет все необходимые сертификаты по реализации криптографических функций, обширную документацию и широкий набор библиотек, утилит и плагинов для интеграции.

Для исполнения пунктов 1, 3, 4 удобно использовать язык программирования Python, исходя из простоты интеграции в АИС ТОГУ. Язык имеет широкие возможности для Объектно-Ориентированного подхода к реализации логики взаимодействия, множество написанных открытых прикладных библиотек, отличную кроссплатформенность, возможность асинхронного программирования и работы с потоками.

Пункт 1 и 3 в более узком смысле будут требовать также задействования дополнительных библиотек:

- СУБД — PostgreSQL, свободная кроссплатформенная объектно-реляционная система управления базами данных

- для взаимодействия с СУБД — SQLAlchemy. Это многофункциональная ORM-библиотека, позволяющая быстро конфигурировать запросы к БД, обезопасить пользовательский ввод, используемый в запросах, а также создавать сложные запросы взаимосвязанные (databinding) с сущностями используемого языка программирования.

- связка Message Queueing broker сервера (RabbitMQ) и библиотеки Celery – для «отправки» потока сообщений от «веб-интерфейса пользователя» и «получение» их Celery для последующего параллельного основному серверу АИС ТОГУ исполнения. [6]

- библиотека Memcached - программное обеспечение, реализующее сервис кэширования данных в оперативной памяти на основе хеш-таблицы, используется в программном комплексе для сопутствующего кэширования и общего хранилища памяти между разными исполнителями задач для «синхронизации».

Исходя из требований и технологий, которые необходимо использовать можно составить схему архитектуры программного комплекса:

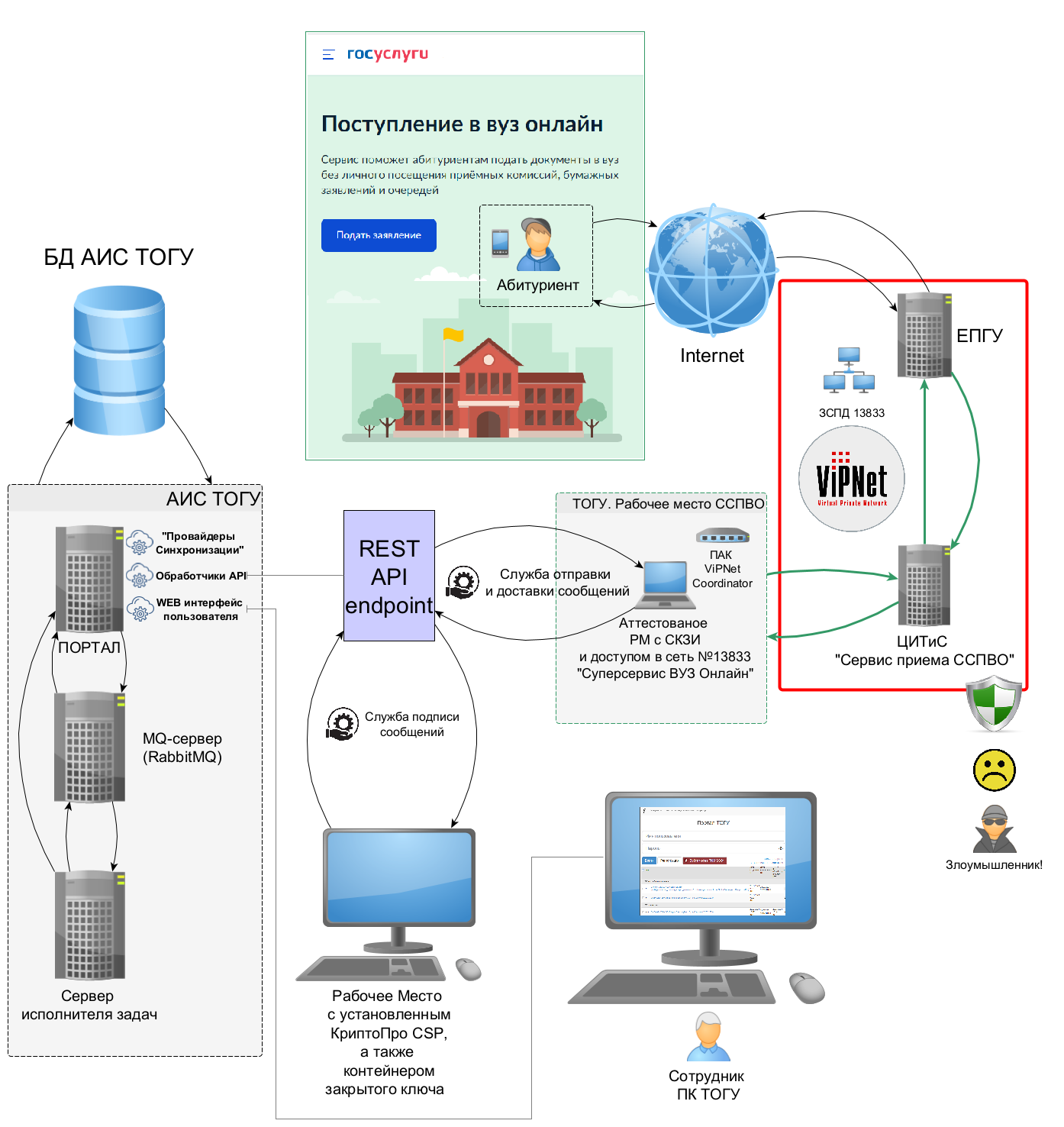


Рисунок 3. Схема взаимодействия с суперсервисом «Поступи в вуз онлайн»

**Описание программного комплекса**

Программный комплекс состоит из трех групп, разделенных по узлам схемы взаимодействия.

1. «ПОРТАЛ ТОГУ».

В рамках этой группы сформирована концепция "Провайдер синхронизации" – это сущность АИС ТОГУ, реализованная на ЯП Python, заключающая

а) логику трансформации исходящих данных, интерфейса пользователя и отдельного обработчика ответа, асинхронно пришедшего от ССПВО. Результат исполнения провайдера есть сущность "сообщение ССПВО" которое доставляется по маршруту дальше. Провайдер может исполнятся с определенным «контекстом вызова» как автоматически, по достижению каких-то условий в АИС ТОГУ, так и в ручном режиме. Провайдер может инициировать запуск дочерних провайдеров.

б) логику трансформации входящих данных (сообщений ССПВО) в АИС ТОГУ, логирование изменений АИС ТОГУ внутри неподтвержденной транзакции БД - для получения того как сообщение ССПВО потенциально изменит БД без проведенных изменений.

Web интерфейс работы с сообщениями ССПВО представлен на рисунке ниже.

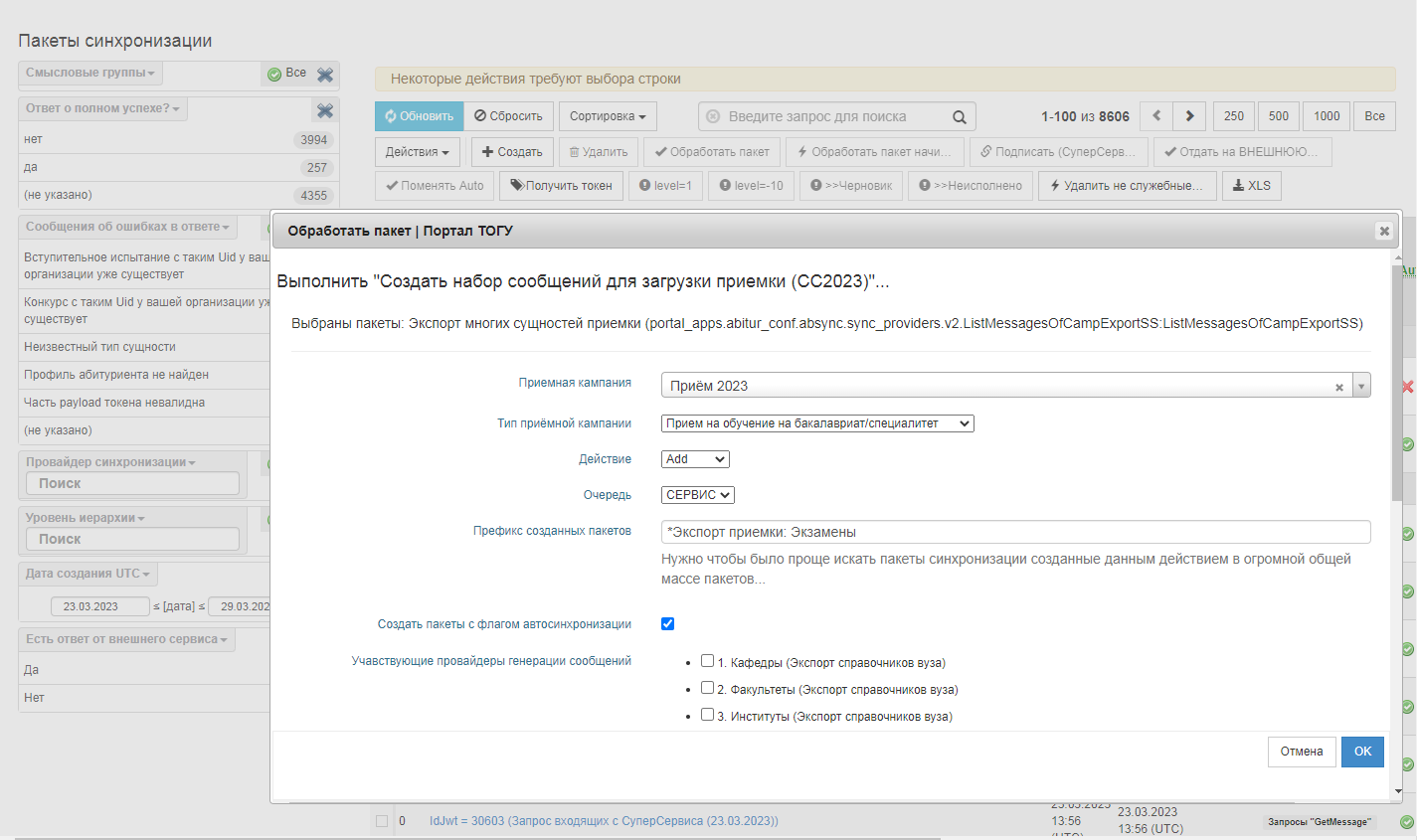


Рисунок 4. Интерфейс управления системой для пользователя

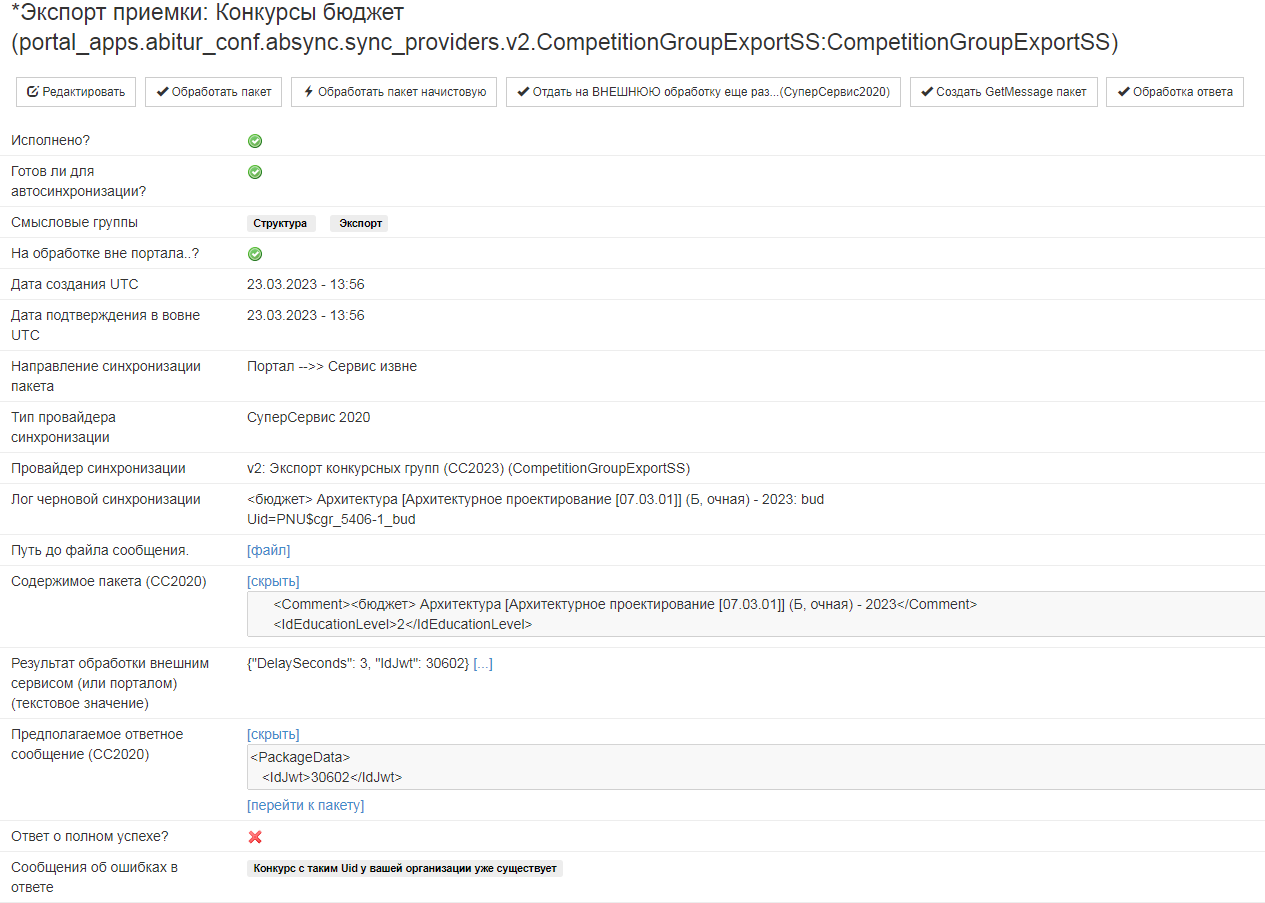


Рисунок 5. Интерфейс просмотра и редактирования сообщений ССПВО

После формирования сообщений ССПВО (в автоматическом режиме, после определенных условий) или в ручном, ограниченные операции над ними станут доступны по REST API ТОГУ.

2. «Узел ЭЦП».

Далее, по документации устанавливающей взаимодействие сказано, что некоторые типы сообщений ССПВО будут требовать указания в сообщения отделённой ЭЦП. Подпись таких сообщений осуществляется в автоматическом режиме службой, установленной на рабочем месте с токеном закрытого ключа с помощью криптопровайдера «Crypto-Pro GOST R 34.10-\* Cryptographic Service Provider». Закрытый ключ не передается ни по каким каналам, формирование подписи происходит на локальной машине на которой была запущена служба. Служба реализована на языке программирования Python 3.7 с помощью библиотеки асинхронных HTTP запросов aiohttp. [1]

Окно работы службы показано на рисунке ниже.

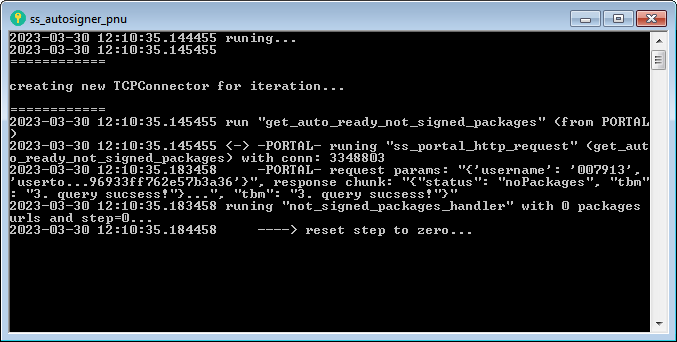


Рисунок 6. Служба подписи сообщений ССПВО перед отправкой

3. «Узел отправки и получения сообщений ССПВО».

Далее, после успешной подписи (если она требовалась сообщению), другая служба, уже на рабочем месте внутри защищенной сети № 13833, отправляет «ожидающие отправки» сообщения из АИС ТОГУ в Сервис приема ССПВО, и по REST API возвращает АИС ТОГУ результат отправки. Также служба принимает входящие сообщения от сервиса приема ССПВО (ЕПГУ) и по REST API записывает их в АИС ТОГУ. Служба реализована на языке программирования Python 3.7 с помощью библиотеки асинхронных HTTP запросов aiohttp. [1]

Окно работы службы показано на рисунке ниже:

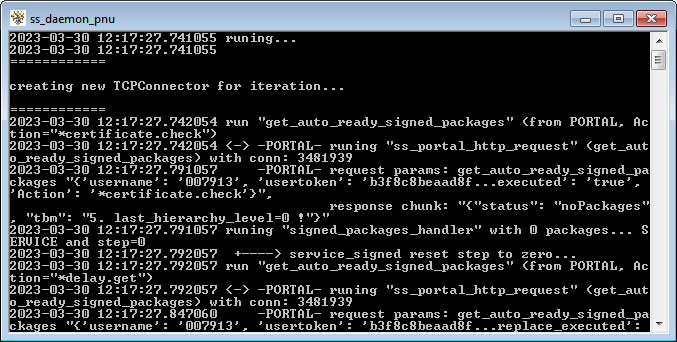


Рисунок 7. Служба отправки/приема сообщений ССПВО

## Заключение

В ходе работ по проектированию программного комплекса для взаимодействия с ГИС "Поступай в вуз онлайн" была создана целая инфраструктура, включающая несколько узлов, программ и каналов взаимодействия между ними. Реализация включила в себя создание подходящих таблиц в СУБД, программирование логики трансформации сущностей БД ТОГУ, событий обработки сообщений, проектирование интерфейса пользователя, написание служб автоматической отправки и получения сообщений. Выбранные технологические решения, хотя и имеют незначительные проблемы с пиковой производительностью, однако благодаря выбранной асинхронной микросервисной архитектуре очень хорошо горизонтально масштабируется – при надобности можно поднимать дополнительные узлы, также узлы не зависят от «совместимости решений» - например в части межсетевых экранов и криптопровайдеров различных компаний, а также отдельные части платформо-независимы в части ОС.

## Список использованных источников

1. AIOHTTP documentation. – Текст: электронный // AIOHTTP: официальный сайт. – URL:

https://docs.aiohttp.org/en/stable/ (дата обращения: 30.03.2023).

2. Постановление Правительства РФ № 89 от 26.03.2023. – Текст: электронный // Официальный интернет-портал правовой информации: официальный сайт. – URL:

http://publication.pravo.gov.ru/Document/View/0001202301270024?index=0&rangeSize=1 (дата обращения: 30.03.2023).

3. Компоненты виртуальной сети ViPNet. – Текст: электронный // Infotecs: официальный сайт. – URL:

https://infotecs.ru/about/press-centr/publikatsii/printsipy-marshrutizatsii-i-preobrazovaniya-ip-trafika-v-vpn-seti-sozdannoy-s-ispolzovaniem-tekhnolo.html (дата обращения: 30.03.2023).

4. Семафор (программирование). – Текст: электронный // Wikipedia: официальный сайт. – URL:

https://ru.wikipedia.org/wiki/Семафор\_(программирование) (дата обращения: 30.03.2023).

5. ГОСТ 34.10-2018. – Текст: электронный // Wikipedia: официальный сайт. – URL:

https://ru.wikipedia.org/wiki/%D0%93%D0%9E%D0%A1%D0%A2\_34.10-2018 (дата обращения: 30.03.2023).

6. RabbitMQ Documentation. – Текст: электронный // RabbitMQ: официальный сайт. – URL:

https://www.rabbitmq.com/documentation.html (дата обращения: 30.03.2023).

7. Документация АПИ Сервиса приема ССПВО . – Текст: электронный // Сервис приема ССПВО (тестовый контур): официальный сайт. – URL:

http://85.142.162.21:8032/ (дата обращения: 30.03.2023).