Электронная Площадка РСХБ (ЭП РСХБ).

Руководство администратора

Всего 16 листов

Москва, 2023

Оглавление

1 Общие сведения

1.1 О документе

Настоящий документ представляет собой руководство по настройке и использованию ЭП РСХБ. Конечными пользователями системы являются системные администраторы, осуществляющие настройку и эксплуатацию ЭП РСХБ, в том числе настройки интеграции с внешними информационными системами.

1.2 О продукте

Электронная площадка РСХБ (далее, ЭП РСХБ) обеспечивает взаимодействие и организует совместную работу различных прикладных информационных систем с внешними информационными системами или источниками информации.

1.3 Состав продукта

Продукт состоит из модулей (сервисов):

- Бизнес-функции
- Функции транспорта сообщений/данных
- Маршрутизация сообщений/данных
- Преобразование форматов сообщений/данных
- Конвертация протоколов

Часть компонентов ЭП РСХБ реализованы как standalone сервисы:

- Java 8
- Kotlin
- React
- Javascript
- PostgreSQL

Часть компонентов ЭП РСХБ функционируют как сервисы внутри Kubernetes.

2 Работа с продуктом

2.1 Управление пользователями сервиса авторизации

Сервис авторизации позволяет:

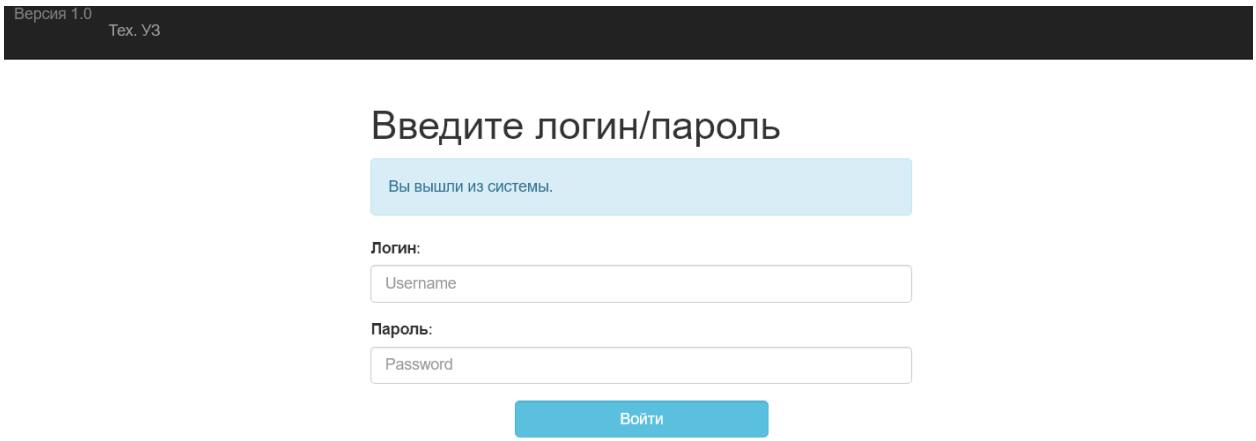
- Создавать новых пользователей
- Удалять учетные записи пользователей
- Редактировать права доступа отдельно взятого пользователя к системам, которые интегрированы к ЭП РСХБ.

2.1.1 Управление ролями

Для доступа к управлению ролями:

- Откройте браузер
- В адресной строке введите
- Авторизуйтесь под учетной записью администратора

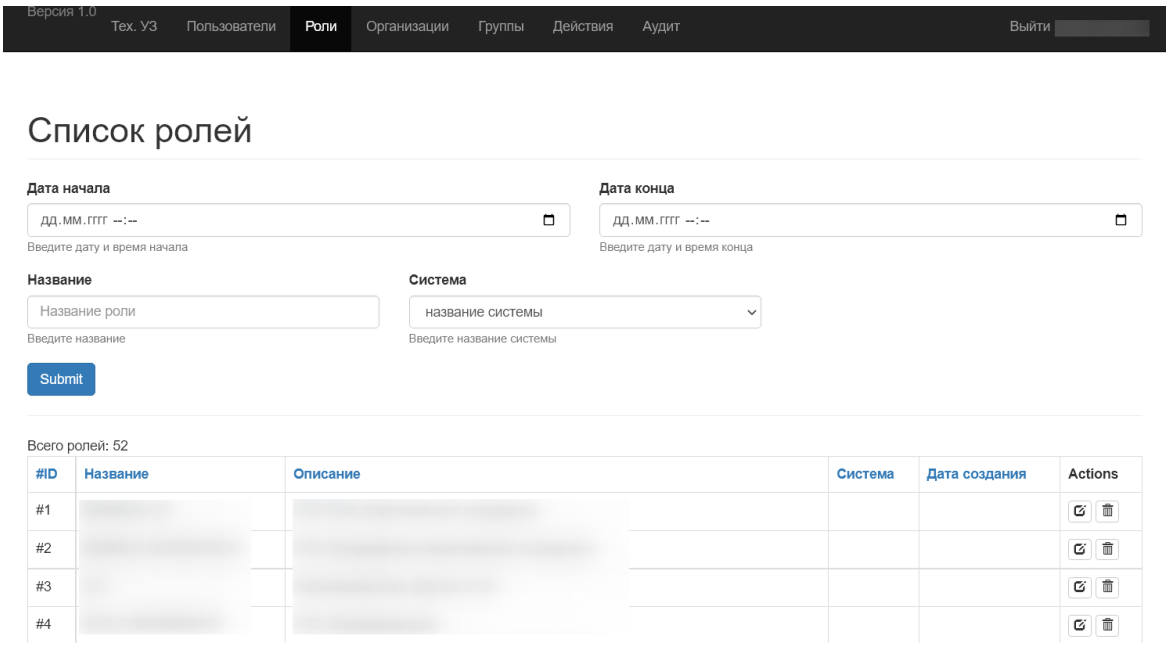
Рисунок 1



- В верхнем меню навигации выберите **Роли**.
  Откроется главное окно управления ролями[1]
  Администратор может искать роли, редактировать/удалять/добавлять роли.

[1] Роль — это некоторая сущность, которая помогает разделять права между сервисами/пользователями системы. В рамках одного сервиса может быть предусмотрено несколько ролей

Рисунок 2

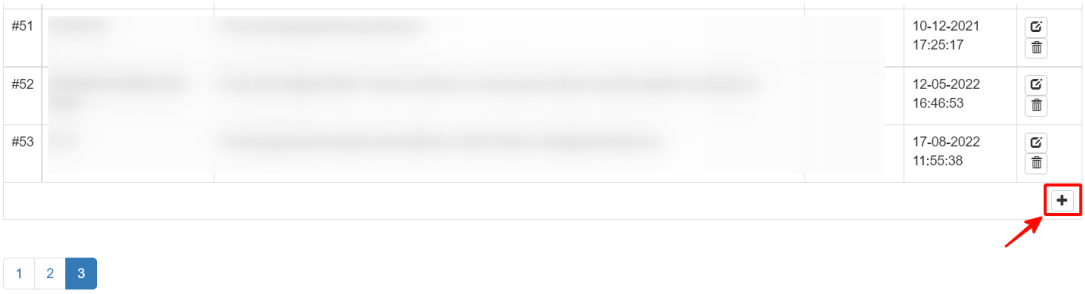


2.1.2 Создание ролей

Чтобы создать новую роль:

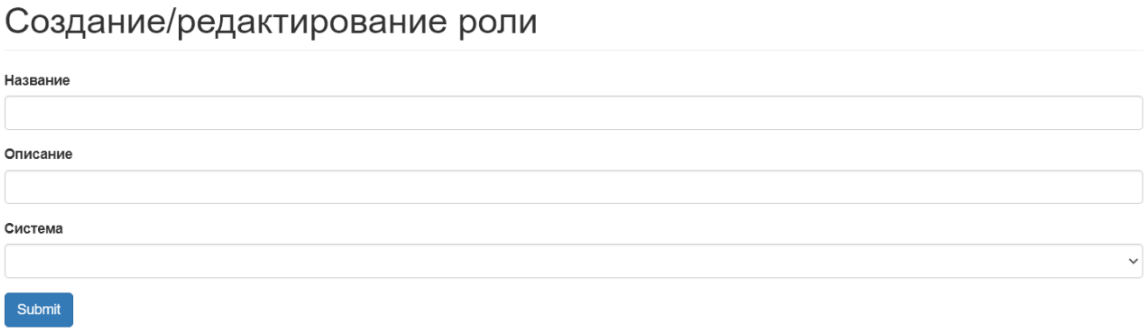
- Пролистайте вниз список ролей
- В правом нижнем углу, в конце списка ролей, нажмите на знак **+**

Рисунок 3



- В открывшемся окне *Создание/редактирование роли* заполните поля:
  - **Название** — название роли
  - **Описание** — пояснение о назначении роли
  - **Система** — доступ к какой информационной системе запрашивается

Рисунок 4

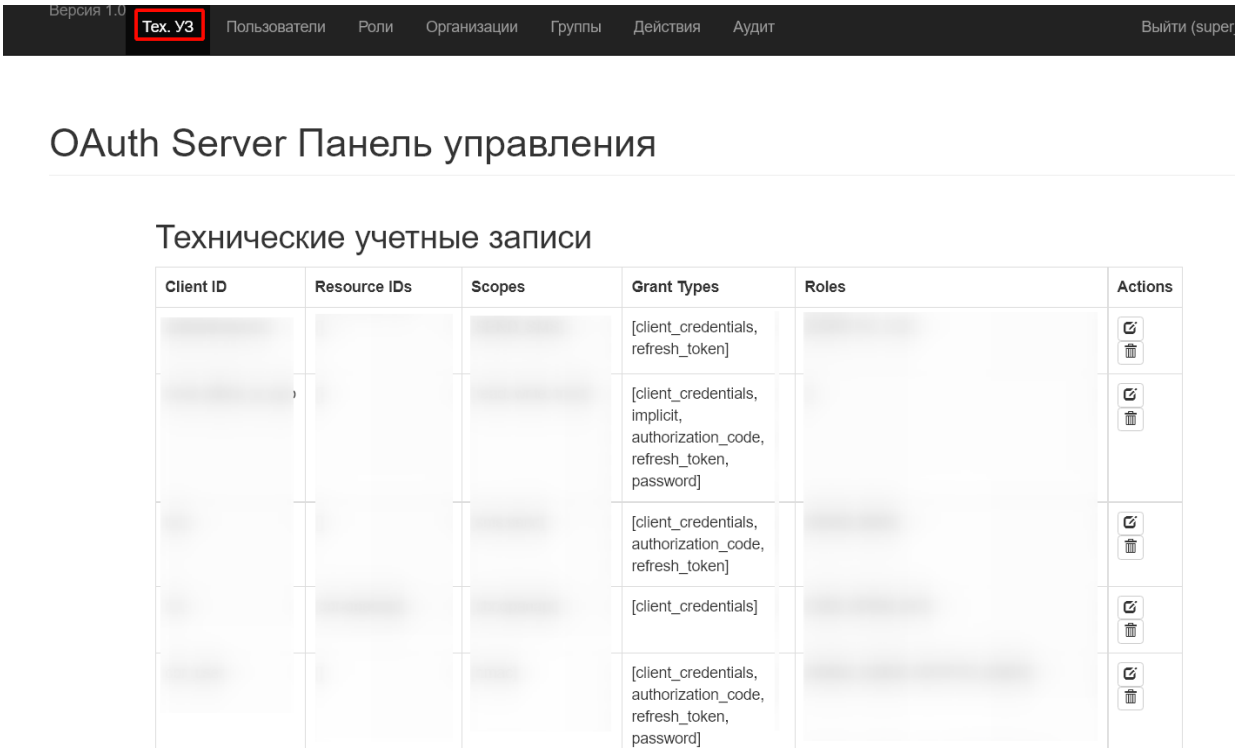


- Для применения настроек нажмите **Submit**

2.1.3 Добавление, редактирование, удаление технических учетных записей

- Авторизуйтесь в браузере.
- В верхнем меню управления выберите **Тех. УЗ**.

Рисунок 5

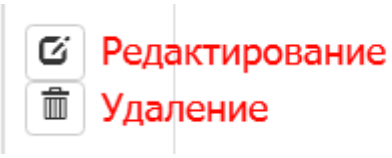


- Появится окно управления системными записями[2].

Учетную запись можно либо отредактировать, нажав на соответствующий значок напротив УЗ, либо удалить.

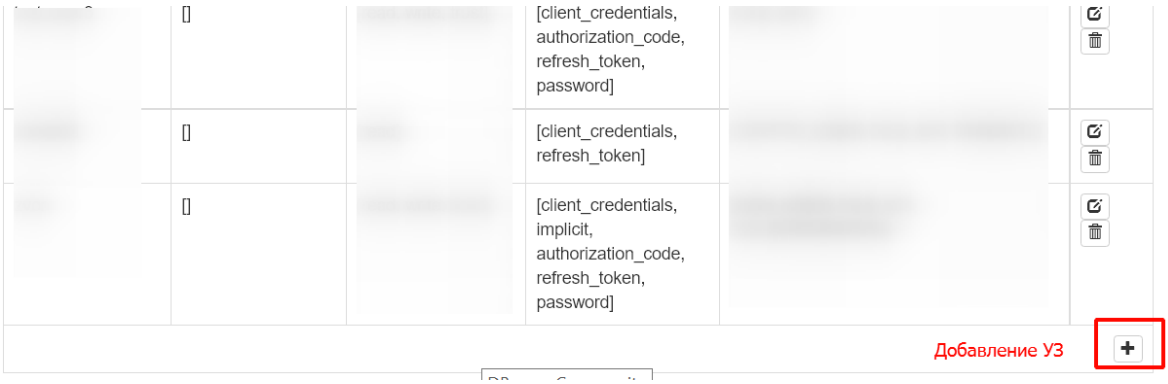
[2] Под системной учетной записью понимается система, которой предоставляется доступ, а не физический пользователь

Рисунок 6



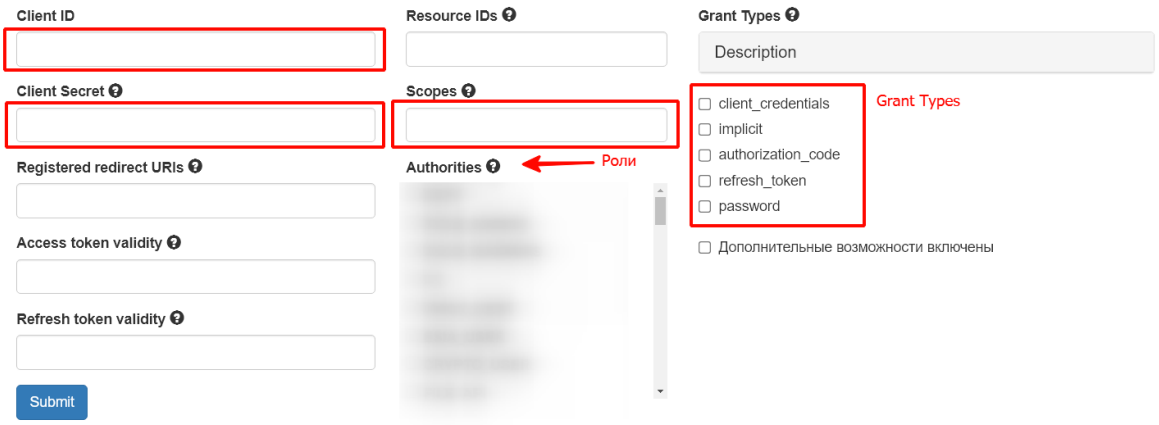
Для добавления учетной записи пролистайте список вниз, в правом нижнем углу нажмите на знак **+**

Рисунок 7



Откроется форма заполнения данных об учетной записи.

Рисунок 8

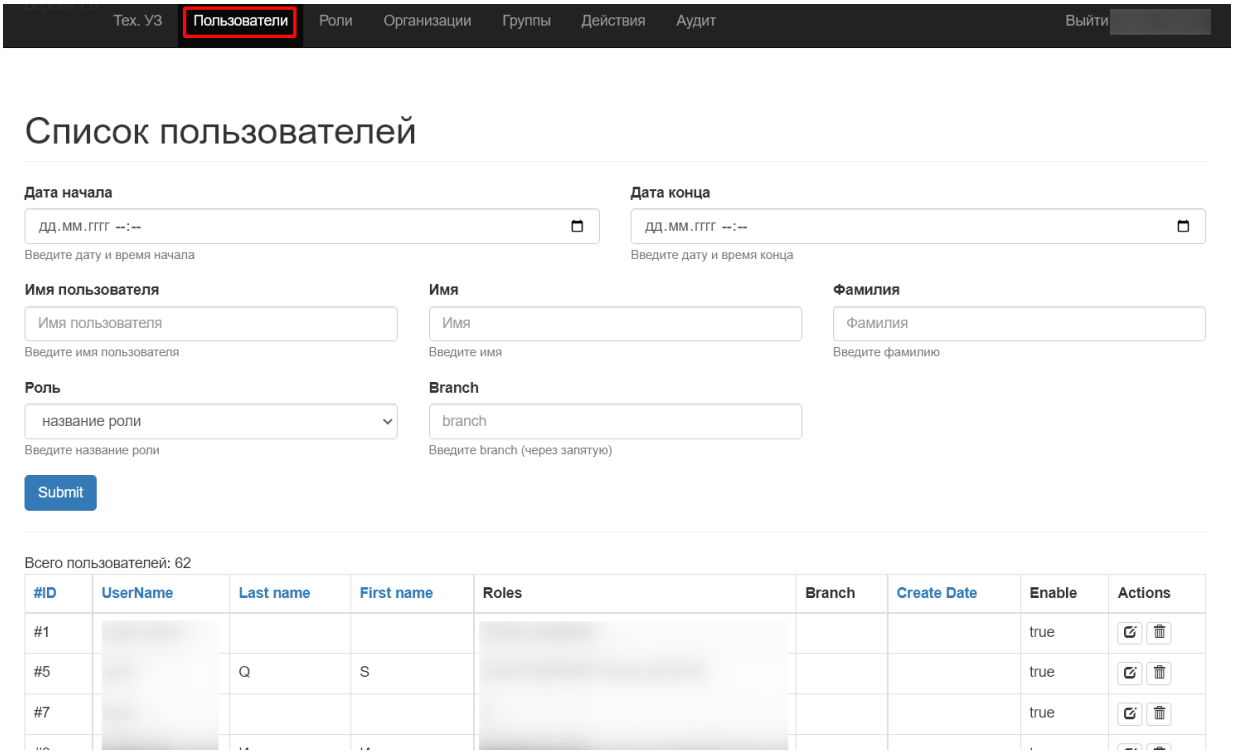


Для сохранения внесенных изменений нажмите **Submit**.

2.1.4 Добавление, редактирование, удаление пользовательских учетных записей

Для работы с пользовательскими учетными записями имеется отдельная вкладка. Для перехода в меню управления пользовательскими учетными записями в верхнем меню управления выберите **Пользователи.**

Рисунок 9



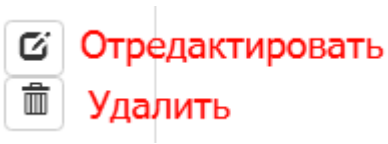
В открывшемся меню у администратора есть возможность осуществлять:

- Поиск по имеющимся в базе данных записях об учетных записях пользователей
- Создавать, удалять учетные записи пользователей
- Вносить изменения в данные учетных записей пользователей.

Для каждой зарегистрированной учетной записи пользователя присваивается своя роль.

Роли можно редактировать или удалять.

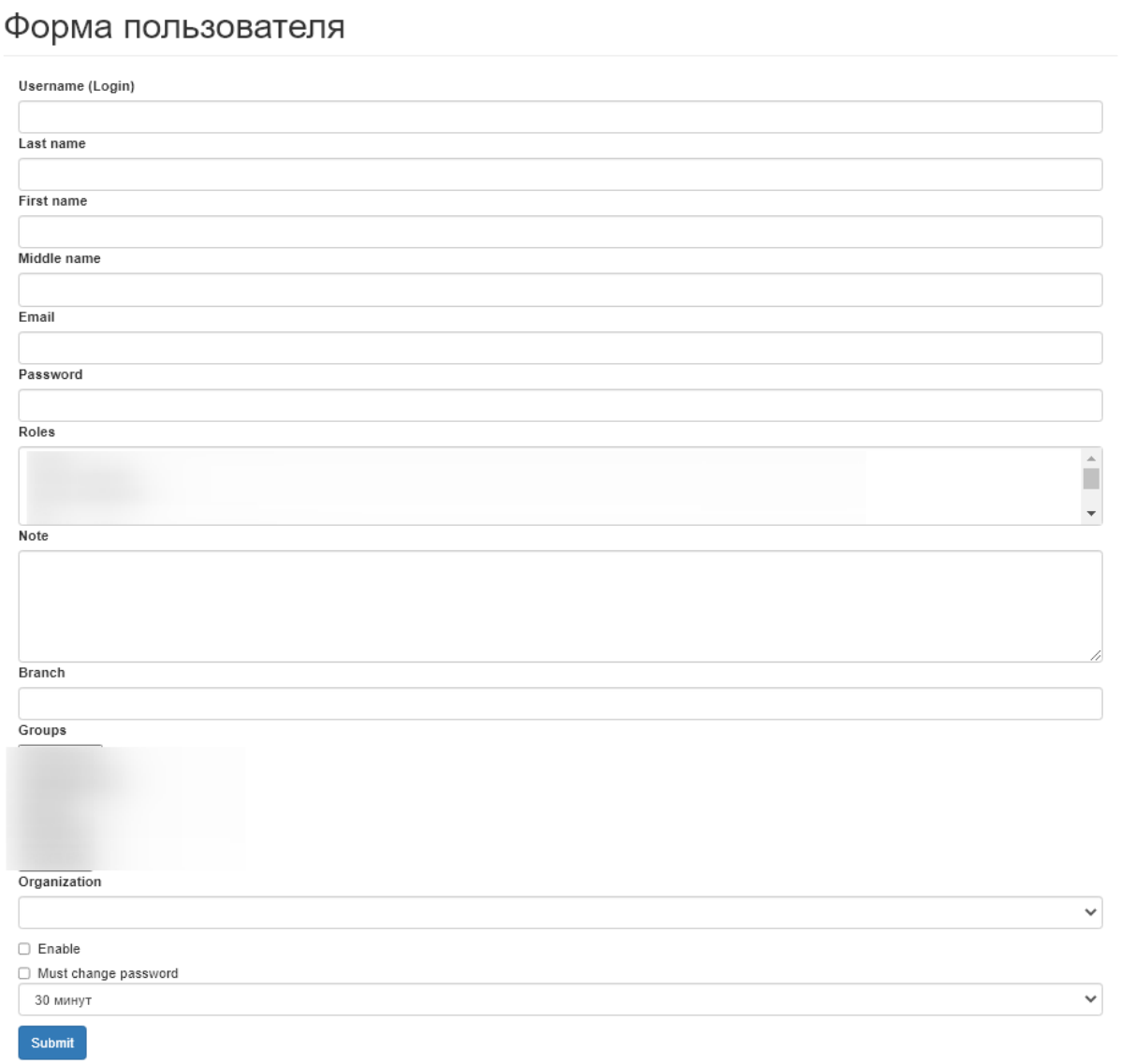
Рисунок 10



Чтобы добавить учетную запись для нового пользователя, нажмите на знак **+** в правом нижнем углу списка.

После нажатия откроется экран *Форма пользователя*.

Рисунок 11



В форме заполняются следующие данные:

- Username (Login)
- Lastname
- Firstname
- Middle name
- Email
- Password
- Roles
- Note
- Branch
- Groups

- Organization

Дополнительно есть возможность выставить чекбокс:

- **Enable** — статус учетной записи пользователя
- **Must change password** — необходимость менять пароль через заданное время (задается отдельно)

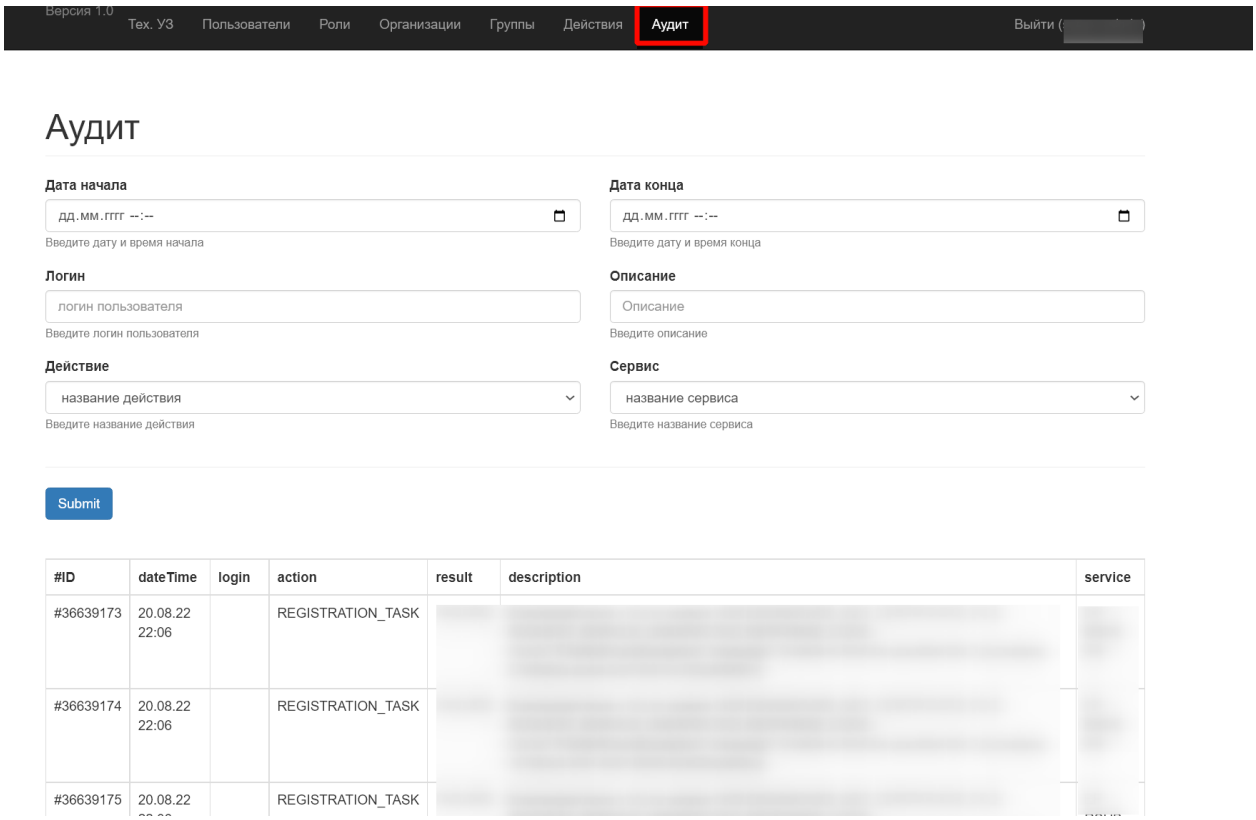
2.1.5 Просмотр событий аудита

Для просмотра событий аудита:

- Авторизуйтесь под учетной записью администратора
- В верхнем меню навигации выберите вкладку **Аудит**

  На экране отобразится форма поиска записанных событий.

Рисунок 12



- Функциональность системы позволяет:
  - Искать логи по определенной дате/времени
  - Выводить логи отдельно взятого сервиса
  - Фильтровать данные логов по названию события, логину или идентификатору *clientid*.

2.2 Управление сервисом ЭЦП

Сервис ЭЦП является одним из основных сервисов системы.

Он выполняет следующие задачи:

- Назначение меток целостности на файлы и документы
- Подписание документов электронной цифровой подписью
- Проверка ЭЦП на уже подписанных документах
- Шифрование и дешифрование сообщений и документов.

2.2.1 Типы ролей

Чтобы система-потребитель могла использовать сервис ЭЦП, в сервисе авторизации должны быть созданы роли для сервиса-потребителя:

- HMAC_USER — роль, позволяющая использовать метки целостности
- CRYPTO_USER — роль, позволяющая использовать ЭЦП и механизм шифрования.

2.2.2 Настройка сервиса ЭЦП

Для корректной работы сервиса ЭЦП требуется:

- Метки целостности, которые используются в интеграционных процессах, должны располагаться в директории *./hmacs*
- Контейнеры ключей, используемые в процессах, должны располагаться в директории */var/opt/cprocsp/keys/<USER_NAME>/*
  Примечание: в зависимости от параметров установки Крипто Про JCP 2.0 может измениться путь к контейнерам ключей.

Для установки сертификата в доверенные:

- Перейдите в директорию *<JAVA_HOME>/jre/bin*

```
cd <JAVA_HOME>/jre/bin
```

- Импортируйте сертификат

```
keytool -importcert -alias <ALIAS_NAME> -file <CERT_PATH>/<CERT_NAME>.cer -keystore ../jre/lib/security/cacerts
```

В ходе настройки сервиса ЭЦП задайте параметры конфигурации:

Таблица 1 Параметры конфигурации

Параметр	Значение	Описание
crl-cache-evict-minutes:	60	Время инвалидации кэша для CRL-файлов
tsp-server-url:	http://testca2012.cryptopro.ru/tsp/tsp.srf	Адрес сервера TSP(временных меток)

Параметр	Значение	Описание
enable-audit:	**true** или **false**	Включение/отключение логирования событий для аудита
audit-url:		Адрес сервиса аудита
app.enc	**true** или **false**	Включение/отключение шифрования паролей внутри конфигурации
ext-loader.api	/api/v1/extload/	Позволяет скачивать сертификаты и CRL через прокси API

Для логирования событий сервиса ЭЦП настраивается файл **./logback.xml**

```
<logger name="<your_domain>.cryptopro" level="INFO">
    <appender-ref ref="ROLLING-FILE"/>
</logger>
<logger name="ru.CryptoPro" level="INFO">
    <appender-ref ref="ROLLING-FILE"/>
</logger>
<logger name="ru.CryptoPro.JCP.tools.JCPLogger" level="INFO">
    <appender-ref ref="ROLLING-FILE"/>
</logger>
<logger name="org.bouncycastle.cms" level="INFO">
    <appender-ref ref="ROLLING-FILE"/>
</logger>
```

2.3 Управление сервисом FileApi

Сервис FileApi позволяет:

- Загружать/скачивать файлы из различных источников данных, например: JDBC, S3 хранилища, File storage и др.
- Проверять обрабатываемые файлы на вирусы.

2.3.1 Типы используемых хранилищ

Хранилища, с которыми умеет работать FileApi, декларируются в системной таблице **stores**

Типы поддерживаемых хранилищ перечислены в таблице ниже:

Таблица 2

Тип хранилища	**store_type**	**Параметры подключения**
Файловая система	FS	Задается в *store_path* как директория на файловом сервере. Например: */mnt/some_directory*
База данных	JDBC	База данных задается в настройка *application.yml*
S3 хранилище	MINIO	Настройки для взаимодействия с S3 MinIO посредством API задаются в *application.yml*
Сервис проверки файлов на вирусы без длительного хранения (Polygon Group IB)	POLYGON	

2.3.2 Настройки процессов

В ходе работы сервиса FileApi каждый файл привязан к своему процессу[3].

Список задекларированных процессов хранится в системной таблице **process**. Для каждого процесса задаются следующие параметры:

Таблица 3

Параметр	**Назначение**
owner	Владелец процесса
proc_name	Название процесса *Например:* «Розничный кредитный процесс»

[3] Под процессом подразумевается абстрактная сущность, которая декларирует описание процесса, в рамках которого может загружаться конкретный файл.

Параметр	Назначение
store_id	Тип используемого в рамках процесса хранилища
time_to_live	Время хранения файлов в миллисекундах, после которого файлы будут удалены
antivirus	Включение/отключение обязательной проверки файлов на вирусы (с помощью сервиса Polygon Group IB)

2.3.3 Типы ролей

Чтобы сервис FileApi работал, требуется создать отдельную роль *FILE_API* внутри сервиса авторизации. Аналогичная роль должна быть настроена на стороне сервиса-потребителя.

2.3.4 Настройка сервиса FileApi

- Задайте конфигурацию базы данных, с которой будет работать сервис

```
spring:
  datasource:
    driver-class-name: org.postgresql.Driver
    url: jdbc:${PG_SQL_URL}
    username: ${PG_SQL_USER}
    password: ${PG_SQL_PSWD}
    default_schema: ${SCHEMA}
    hikari:
      minimum-idle: 1
      maximum-pool-size: 4
  liquibase:
    change-log: classpath:db/changelog/db.changelog-master.xml
    drop-first: false
```

- Задайте настройки для сервиса авторизации

```
spring:
  security:
    oauth2:
      resourceserver:
        jwt:
          jwk-set-uri: ${OAUTH_URL}/.well-known/jwks.json
```

- Задайте настройки для подключения к S3 хранилищу

```
minio:
  host: ${S3_URL}
  bucket: ${S3_BUCKET}
```

```
  accessKey: ${S3_ACCESS}
  secretKey: ${S3_SECRET}
```

2.4 Управление сервисом СМЭВ 3

Сервис СМЭВ 3 предоставляет REST API для взаимодействия с Адаптером СМЭВ 3.0. Сервис реализует механизм подписки на сообщения и ответы.

2.4.1 Настройка ролей

Для использования сервиса СМЭВ 3 создайте роль *SMEV_USER* внутри сервиса авторизации. Аналогичная роль должна быть создана для сервиса-потребителя

2.4.2 Настройка сервиса СМЭВ 3

- Задайте настройки для сервиса авторизации

```
spring:
  security:
    oauth2:
      resourceserver:
        jwt:
          jwk-set-uri: ${OAUTH_URL}/.well-known/jwks.json
```

- Задайте конфигурацию базы данных, с которой будет работать сервис СМЭВ 3

```
spring:
  datasource:
    driver-class-name: org.postgresql.Driver
    url: jdbc:${PG_SQL_URL}
    username: ${PG_SQL_USER}
    password: ${PG_SQL_PSWD}
    default_schema: ${SCHEMA}
    hikari:
      minimum-idle: 1
      maximum-pool-size: 4
  liquibase:
    change-log: classpath:db/changelog/db.changelog-master.xml
    drop-first: false
```

- Настройте планировщики событий

```
scheduler:
  ### Отправка исходящий запросов/ответов, из таблицы SEND
  ### Периодичность отправки в миллисекундах
  sender: 15000
  ### Периодичность переотправки ошибочных запросов/ответов
  sender-fault: 900000
  ### Количество попыток переотправки ошибочных запросов/ответов
  sender-fault-count: 2
  ### Обработка входящих запросов/ответов в таблицу RECEIVE
  ### Периодичность получения входящих запросов/ответов
  receiver: 3000
```

```
  ### Повторная отправка Callback-ов, интервал
  ### Периодичность переотправки ошибочных Callback-ов
  callback-pending: 900000
  ### Количество попыток переотправки ошибочных Callback-ов
  callback-pending-count: 2
  ### Отправка Callback-ов входящих запросов
  callback-req-enabled: true
  callback-req: 3000
  ### Отправка Callback-ов входящих ответов
  callback-resp-enabled: true
  callback-resp: 3000
  ### Размер пакета на отправку сообщений с приоритетом > 1
  senderBatchSize: 200
  ### Размер пакета колбеков
  callbackBatchSize: 40
```

- Задайте общие настройки

```
smev:
  adapter:
  ### Мнемоника Адаптера СМЭВ
    mnemonic: ${ADAPTER_MNEMONIC}
  ### Тип отправляемых сообщений
    testMessage: false
  ### Директория исходящих вложений
  outDir: ${SMEV3_ADAPTER_DIR}/out/
  ### Директория входящих вложений
  storageDir: ${SMEV3_ADAPTER_DIR}/in/
```

- Для логирования событий сервиса FileApi настраивается файл *./logback.xml*

```
    <logger
name="<your_domain>intech.integrations.ckep.electronicplatform.smev"
level="INFO">
        <appender-ref ref="ROLLING-FILE"/>
    </logger>
```