|  |  |
| --- | --- |
|  | **УТВЕРЖДАЮ**  \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  «\_\_\_» \_\_\_\_\_\_\_\_\_\_\_\_\_\_ 2024 г. |

**Руководство администратора**

«Электронный архив (ЭАД)»

Страниц: 37

|  |  |
| --- | --- |
| **СОГЛАСОВАНО:** |  |
| АО «РДТеХ»  Руководитель проекта  \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  «\_\_\_»\_\_\_\_\_\_\_\_\_\_\_\_\_\_ 2024 г. | ПАО «\_\_\_\_»  \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  «\_\_\_» \_\_\_\_\_\_\_\_\_\_\_\_\_\_ 2024 г. |
| АО «РДТеХ»  \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  «\_\_\_»\_\_\_\_\_\_\_\_\_\_\_\_\_\_ 2024 г. | ПАО «\_\_\_\_»  \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  «\_\_\_» \_\_\_\_\_\_\_\_\_\_\_\_\_\_ 2024 г. |
| АО «РДТеХ»  \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  «\_\_\_»\_\_\_\_\_\_\_\_\_\_\_\_\_\_ 2024 г. | ПАО «\_\_\_\_»  \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  «\_\_\_» \_\_\_\_\_\_\_\_\_\_\_\_\_\_ 2024 г. |

Москва

2024

**Содержание**

[**1. Введение** 3](#_Toc189153329)

[**2. Назначение системы** 4](#_Toc189153330)

[**3. Установка и настройка** 5](#_Toc189153331)

[**3.1. Установка Keycloak, MinIO, OpenSearch, Monolith** 5](#_Toc189153332)

[**3.1.1. Развертывание Keycloak** 5](#_Toc189153333)

[**3.1.2. Развертывание MinIO** 7](#_Toc189153334)

[**3.1.3. OpenSearch и OpenSearch Dashboards** 10](#_Toc189153335)

[**3.1.4. Monolith** 17](#_Toc189153336)

[**3.2. BACKEND** 22](#_Toc189153337)

[**3.3. FRONTEND** 24](#_Toc189153338)

[**3.4. Конфигурация NGINX сервисов EAD** 28](#_Toc189153339)

[**3.5. Конфигурация Keycloak клиентов** 35](#_Toc189153340)

[**3.6. Метаданные** 47](#_Toc189153341)

[**3.7. Аудит, логирование** 47](#_Toc189153342)

[**3.8. Конфигурационные файлы KeyCloak, MinIO, OpenSearch OpenSearch-Dashboards** 50](#_Toc189153343)

[**3.8.1. KeyCloak** 50](#_Toc189153344)

[**3.8.2. MinIO** 50](#_Toc189153345)

[**3.8.3. OpenSearch, OpenSearch-Dashboards** 52](#_Toc189153346)

[**3.9. Конфигурации системы ЭА** 63](#_Toc189153347)

[**4. Описание действий в системе** 64](#_Toc189153348)

[**4.1. Вход в систему и доступ к административному функционалу** 64](#_Toc189153349)

[**4.2. Управление ролями и группами** 64](#_Toc189153350)

[**4.3. Работа со списком пользователей** 71](#_Toc189153351)

[**4.4. Управление организационной структурой** 73](#_Toc189153352)

[**4.5. Просмотр журнала активности** 75](#_Toc189153353)

[**4.6. Мониторинг маршрутов** 77](#_Toc189153354)

# **1. Введение**

Руководство предназначено для администраторов системы электронного архива. Система обеспечивает хранение, управление и поиск документов, а также поддержку процессов, связанных с клиентами, договорами и организационной структурой. В руководстве подробно описаны ключевые разделы системы, включая настройку, администрирование, работу с документами, клиентами и мониторинг состояния системы.

**Администратор должен иметь понимание как работать со следующими функциями:**

- Установка и настройка обновлений электронного архива

- Управление пользователями и группами пользователей в архиве

- Просмотр журналов активности и мониторинг работы системы

- Интеграция с MS AD

- Просмотр логов работы электронного архива

**Для работы с архивом администратору необходимо иметь базовые знания в области работы со следующими программными средствами (ПС):**

- Операционная система CentOS 7 x64;

- Web-сервер Apache Tomcat 9;

- Nginx 1.24 или старше;

- Система управления доступом Keycloak

- Облачное хранилище объектов MinIO

- Система OpenSearch;

- Программный компонент Monolith

- Prometheus и Grafana

# **2. Назначение системы**

rdtex.chive – программный продукт, предназначенный для формирования и поддержки единого хранилища электронных документов организации с возможностью гибкой адаптации системы под конкретную предметную область на уровне типов документов, структуры хранения данных, правил документооборота, прав доступа к данным, интеграции с другими корпоративными системами и подключения дополнительных сервисных возможностей.

**Основные возможности системы:**

1. Поддержка базовых функций работы с документами (загрузка файлов в систему, ведение метаданных, управление версиями и статусами документов и др.).

2. Создание и поддержка иерархической системы хранения документов.

3. Поиск документов и других объектов системы по их атрибутам или с использованием полнотекстового поиска.

4. Управление правами доступа к объектам и функциям системы на основе иерархической ролевой модели.

5. Системное и функциональное администрирование системы (управление ролями и пользователями, доступ к журналам событий, ведение справочников и классификаторов, настройка алгоритмов обработки документов).

6. Интеграция электронного архива с другими корпоративными системами (active directory)

Пользователь имеющий доступ к роли Администратора должен быть зарегистрирован в системе электронного архива, где ему должна быть присвоена роль Администратора.

# **3. Установка и настройка**

## **3.1. Установка Keycloak, MinIO, OpenSearch, Monolith**

Для развертывания и настройки электронного архива необходимо подготовить инфраструктуру, состоящую из нескольких ключевых компонентов: Keycloak, EAD Application, MinIO, OpenSearch, OpenSearch Dashboards и Monolith Service.

|  |  |  |
| --- | --- | --- |
| **Keycloak** | **25.0.1** | [https://rauth.rdtex.msk.ru](https://rauth.rdtex.msk.ru/) |
| **EAD application** | **V2** | [https://rchive.rdtex.msk.ru](https://rchive.rdtex.msk.ru/) |
| **MinIO** | **RELEASE.2024-08-17T01-24-54Z** | <https://minio-stage.rdtex.msk.ru:8445/login> |
| **OpenSearch** | **2.14** | [https://os-stage.rdtex.msk.ru:9205](https://os-stage.rdtex.msk.ru:9205/)  API |
| **OpenSearch Dashboards** | **2.14** | [https://os-stage.rdtex.msk.ru:5605](https://os-stage.rdtex.msk.ru:5605/) |

### **3.1.1. Развертывание Keycloak**

devops@ead-02:/opt/keycloak\_stage

|  |
| --- |
| drwxrwxr-x 2 devops 4096 ноя  6 13:56 providers  drwxrwxr-x 2 devops 4096 ноя  6 17:20 certs  -rwxrwxr-x 1 devops devops 1401 ноя  8 22:54 docker-compose.yml |

Развертывание Keycloak с помощью docker-compose

|  |
| --- |
| # /opt/keycloak\_stage/docker-compose.yml    version: '3'    services:    keycloak:      image: quay.io/keycloak/keycloak:25.0.1      restart: on-failure      container\_name: keycloak      environment:        KC\_DB: postgres        KC\_DB\_URL: jdbc:postgresql://shell-db.rdtex.msk.ru/rauth        KC\_DB\_USERNAME: rauth        KC\_DB\_PASSWORD: \*\*\*\*\*\*\*\*        KC\_DB\_SCHEMA: public        KC\_HOSTNAME: rauth.rdtex.msk.ru        KEYCLOAK\_ADMIN: admin        KEYCLOAK\_ADMIN\_PASSWORD: \*\*\*\*\*\*\*\*        KC\_HTTPS\_CERTIFICATE\_FILE: /opt/keycloak/demo/certs/tls.crt        KC\_HTTPS\_CERTIFICATE\_KEY\_FILE: /opt/keycloak/demo/certs/tls.key        KC\_HTTP\_ENABLED: 'true'        KC\_HTTP\_PORT: **8080**        KC\_HTTPS\_PORT: **443**      volumes:  **-** ./providers:/opt/keycloak/providers  **-** ./certs:/opt/keycloak/demo/certs        #- ./import/realm.json:/opt/keycloak/data/import/realms.json      command:  **-** start-dev      # - start-dev --import-realm  **-** --proxy=edge              # - --proxy=reencrypt              #- --proxy=passthrough              #- --hostname-strict=false              #- --hostname-strict-https=false              #- --hostname-strict-https=true              #- --https-port=8443              #-  --hostname=keycloak-shell.rdtex.msk.ru      networks:  **-** eadnwk      hostname: rauth.rdtex.msk.ru      ports:  **-** 9081:8080  **-** 8444:443    networks:    eadnwk:      name: eadnwk      driver: bridge      ipam:        config:  **-** subnet: 172.32.0.0/16 |

Конфигурация nginx-proxy

|  |
| --- |
| #/usr/local/openresty/nginx/conf/conf.d/rauth.conf    server {    listen 0.0.0.0:80;    listen [:]:80;    server\_name rauth.rdtex.msk.ru;    return 302 https://rauth.rdtex.msk.ru$request\_uri;  }        server {    listen 443 ssl;    server\_name rauth.rdtex.msk.ru;    ssl\_certificate /etc/ssl/shell/shell.crt;    ssl\_certificate\_key /etc/ssl/shell/shell.key;    root /var/www/html;    index index.html index.htm index.nginx-debian.html;    server\_name \_;    location ^~/ {      proxy\_pass http://rauth.rdtex.msk.ru:9081;             proxy\_redirect off;             proxy\_set\_header Host $host;             proxy\_set\_header X-Real-IP $remote\_addr;             proxy\_set\_header X-Forwarded-For $remote\_addr;             proxy\_set\_header X-Forwarded-Proto $scheme;             proxy\_set\_header X-Forwarded-Port 443;    }  } |

Запуск/останов

|  |
| --- |
| devops@ead-02  cd /opt/keycloak\_stage  docker-compose up -d  docker-compose stop keycloak |

### **3.1.2. Развертывание MinIO**

devops@ead-02:/opt/ead\_stage

|  |
| --- |
| -rwxrwxr-x 1 devops 391 ноя 7 10:41 security\_admin.sh  -rwxr-xr-x 1 devops 995 ноя 7 10:41 startup.sh  -rwxr-xr-x 1 devops 926 ноя 7 10:52 Dockerfile  drwxrwxr-x 2 devops 4096 ноя 7 11:13 scripts  drwxrwxr-x 3 devops 4096 ноя 7 11:52 minio  -rwxrwxr-x 1 devops 3364 ноя 8 11:35 docker-compose.yml  drwxrwxr-x 3 devops 4096 ноя 8 12:06 opensearch |

Развертывание MinIO с помощью docker-compose

|  |
| --- |
| # /opt/ead\_stage/docker-compose.yml  version: '3.7'    x-minio-common: &minio-common    image: quay.io/minio/minio: RELEASE.2024-08-17T01-24-54Z    command: server --certs-dir /opt/minio/certs --console-address ":443" https://minio-stage.rdtex.msk.ru/data{1...2}    ports:  **-** "9005:9000"  **-** "8445:443"    environment:      MINIO\_ROOT\_USER: admin      MINIO\_ROOT\_PASSWORD: \*\*\*\*\*\*\*\*      MINIO\_SCHEME: https      MINIO\_DEFAULT\_BUCKETS: devbucket    healthcheck:      test: ["CMD", "mc", "ready", "local"]      interval: 5s      timeout: 5s      retries: **5**    services:      minio-stage:      <<: \*minio-common      container\_name: minio-stage      restart: always      hostname: minio-stage.rdtex.msk.ru      volumes:  **-** data1-1:/data1  **-** data1-2:/data2  **-**. /minio/certs:/opt/minio/certs  **-** ./minio/certs/CA/ca.pem:/opt/minio/certs/CAs/root\_pem\_globalsign\_ssl\_dv\_wildcard\_1.crt      #networks:      #  - eadnwk |

Сертификаты для MinIO

|  |
| --- |
| devops@ead-02:/opt/ead\_stage$ ls -ltr minio/certs/  итого 16  -rw------- 1 devops 1703 ноя 7 10:41 private.key  -rw-r--r-- 1 devops 2252 ноя 7 10:41 public.crt  drwxr-xr-x 3 devops 4096 ноя 7 10:41 CAs  drwxrwxr-x 3 devops 4096 ноя 7 10:41 CA |

Конфигурация nginx-proxy для MinIO

|  |
| --- |
| # /usr/local/openresty/nginx/conf/conf.d/minio.conf    # Default server configuration  #  server {    listen 0.0.0.0:80;    listen [:]:80;    server\_name minio-stage.rdtex.msk.ru;    return 302 https://minio-stage.rdtex.msk.ru$request\_uri;  }      server {    listen 443 ssl;    server\_name minio-stage.rdtex.msk.ru;    ssl\_certificate /etc/ssl/shell/shell.crt;    ssl\_certificate\_key /etc/ssl/shell/shell.key;    root /var/www/html;    index index.html index.htm index.nginx-debian.html;    server\_name \_;    #ssl on;    #add\_header Strict-Transport-Security "max-age=0;";    location ^~/ {      #proxy\_pass [http://localhost:9002](http://localhost:9002/);      proxy\_pass http://minio-stage.rdtex.msk.ru:9002;      #proxy\_set\_header X-Real-IP $remote\_addr;      #proxy\_set\_header X-Forwarded-For $proxy\_add\_x\_forwarded\_for;      #proxy\_set\_header Host $http\_host;      #add\_header Access-Control-Allow-Origin [https://shell-app.rdtex.msk.ru](https://shell-app.rdtex.msk.ru/);      #add\_header Access-Control-Allow-Origin [https://gw-shell.rdtex.msk.ru](https://gw-shell.rdtex.msk.ru/);      #add\_header Access-Control-Allow-Origin \*;               proxy\_redirect off;             proxy\_set\_header Host $host;             proxy\_set\_header X-Real-IP $remote\_addr;             proxy\_set\_header X-Forwarded-For $remote\_addr;             proxy\_set\_header X-Forwarded-Proto $scheme;             proxy\_set\_header X-Forwarded-Port 443;    }  } |

### **3.1.3. OpenSearch и OpenSearch Dashboards**

devops@ead-02:/opt/ead\_stage

|  |
| --- |
| -rwxrwxr-x 1 devops 391 ноя 7 10:41 security\_admin.sh  -rwxr-xr-x 1 devops 995 ноя 7 10:41 startup.sh  -rwxr-xr-x 1 devops 926 ноя 7 10:52 Dockerfile  drwxrwxr-x 2 devops 4096 ноя 7 11:13 scripts  drwxrwxr-x 3 devops 4096 ноя 7 11:52 minio  -rwxrwxr-x 1 devops 3364 ноя 8 11:35 docker-compose.yml  drwxrwxr-x 3 devops devops 4096 ноя 8 12:06 opensearch |

Подготовка кастомного образа с предустановленными плагинами **repository-s3** и **ingest-attachment**

|  |
| --- |
| #/opt/ead\_stage/Dockerfile    FROM opensearchproject/opensearch:2.14.0    #ARG HTTP\_PROXY  #ARG HTTPS\_PROXY  #ENV HTTP\_PROXY=[http://172.24.0.254:3128](http://172.24.0.254:3128/)  #ENV HTTPS\_PROXY=[http://172.24.0.254:3128](http://172.24.0.254:3128/)    RUN /usr/share/opensearch/bin/opensearch-plugin install --batch repository-s3  RUN /usr/share/opensearch/bin/opensearch-plugin install --batch ingest-attachment |

Билд кастомного docker image

|  |
| --- |
| docker build --tag=opensearchproject/opensearch\_plugin:2.14.0. |

Развертывание OpenSearch and OpenSearch-Dashboards с помощью docker-compose

|  |
| --- |
| # /opt/ead\_stage/docker-compose.yml  version: '3.7'    services:    os01-stage:      image: opensearchproject/opensearch\_plugin:2.14.0      container\_name: os01-stage      restart: on-failure      environment:        OPENSEARCH\_JAVA\_OPTS: "-Xms1024m -Xmx1024m -Djavax.net.ssl.trustStore=/usr/share/opensearch/jdk/lib/security/cacerts -Djavax.net.ssl.trustStorePassword=changeit -Djavax.net.debug=ssl -Djdk.tls.client.protocols=TLSv1.2"        # minimum and maximum Java heap size, recommend setting both to 50% of system RAM        node.name: os01        JAVA\_HOME: /usr/share/opensearch/jdk        bootstrap.memory\_lock: "true" # along with the memlock settings below, disables swapping        network.host: "0.0.0.0"      ulimits:        memlock:          soft: -1          hard: -1      volumes:  **-** "os-data1:/usr/share/opensearch/data"  **-** "./opensearch/certs:/usr/share/opensearch/config/certificates:ro"  **-** "./opensearch/opensearch.yml:/usr/share/opensearch/config/opensearch.yml"  **-** "./opensearch/config.yml:/usr/share/opensearch/config/opensearch-security/config.yml"  **-** "./opensearch/roles\_mapping.yml:/usr/share/opensearch/config/opensearch-security/roles\_mapping.yml"  **-** "./opensearch/log4j2.properties:/usr/share/opensearch/config/log4j2.properties" ### added trace logs for diagnostics      logging:        driver: "json-file"        options:          max-size: "100m"          max-file: "1"      ports:  **-** 9205:9200  **-** 9605:9600 # required for Performance Analyzer      kibana-stage:      image: opensearchproject/opensearch-dashboards:2.14.0      container\_name: kibana-stage      restart: on-failure      environment:        OPENSEARCH\_HOSTS: '["[https://os01-stage:9200](https://os01-stage:9200/)"]'        DISABLE\_INSTALL\_DEMO\_CONFIG: "true"      logging:        driver: "json-file"        options:          max-size: "100m"          max-file: "1"      volumes:  **-** "./opensearch/certs:/usr/share/opensearch-dashboards/config/certificates"  **-** "./opensearch/opensearch-dashboards.yml:/usr/share/opensearch-dashboards/config/opensearch\_dashboards.yml"      ports:  **-** 5605:5601    volumes:    data1-1:    data1-2:    os-data1: |

Сертификаты для OpenSearch и OpenSearch-Dashboards

|  |
| --- |
| devops@ead-02:/opt/ead\_stage/opensearch/certs$ ls -ltr    -rwxrwxrwx 1 devops devops 1703 ноя  7 21:15 shell.key  -rwxrwxrwx 1 devops devops 5170 ноя  7 21:15 shell.crt |

Конфигурация OpenSearch - opensearch.yml

|  |
| --- |
| # /opt/ead\_stage/opensearch/opensearch.yml    cluster.name: os-stage  network.host: 0.0.0.0    # Отключаем обнаружение других узлов для однонодового кластера  discovery.type: single-node    bootstrap.memory\_lock: "true" # along with the memlock settings below, disables swapping    #######################################################  ###          OpenSearch Cluster Settings            ###  #######################################################  cluster.routing.allocation.disk.threshold\_enabled: true  cluster.routing.allocation.disk.watermark.low: 93%  cluster.routing.allocation.disk.watermark.high: 95%    #######################################################  ###        Common configuration settings            ###  #######################################################  # plugins.security.nodes\_dn (Static): Specifies a list of distinguished names (DNs) that denote the other nodes in the cluster.  # This setting supports wildcards and regular expressions. The list of DNs are also read from the security index in addition to the YAML configuration  # when plugins.security.nodes\_dn\_dynamic\_config\_enabled is true.  plugins.security.nodes\_dn:  **-** 'CN=\*.rdtex.msk.ru'  # plugins.security.authcz.admin\_dn (Static): Defines the DNs of certificates to which admin privileges should be assigned. Required.  plugins.security.authcz.admin\_dn:  **-** 'CN=\*.rdtex.msk.ru'  #######################################################  ###  OpenSearch Transport layer TLS settings        ###  #######################################################  plugins.security.ssl.transport.enabled: true  plugins.security.ssl.transport.pemcert\_filepath: certificates/shell.crt  plugins.security.ssl.transport.pemkey\_filepath: certificates/shell.key  plugins.security.ssl.transport.pemtrustedcas\_filepath: certificates/shell.crt  plugins.security.ssl.transport.enforce\_hostname\_verification: false    #######################################################  ###       OpenSearch REST layer TLS settings        ###  #######################################################  plugins.security.ssl.http.enabled: true  plugins.security.ssl.http.pemcert\_filepath: certificates/shell.crt  plugins.security.ssl.http.pemkey\_filepath: certificates/shell.key  plugins.security.ssl.http.pemtrustedcas\_filepath: certificates/shell.crt    #######################################################  plugins.security.allow\_unsafe\_democertificates: true  plugins.security.allow\_default\_init\_securityindex: true  plugins.security.ssl\_cert\_reload\_enabled: true  plugins.security.cache.ttl\_minutes: **0**  plugins.security.restapi.admin.enabled: true  plugins.security.restapi.roles\_enabled: [ "all\_access", "security\_rest\_api\_access" ] |

Конфигурация OpenSearch - config.yml

|  |
| --- |
| # /opt/ead\_stage/opensearch/config.yml    ############    \_meta:    type: "config"    config\_version: **2**    config:    dynamic:      # Set filtered\_alias\_mode to 'disallow' to forbid more than 2 filtered aliases per index      # Set filtered\_alias\_mode to 'warn' to allow more than 2 filtered aliases per index but warns about it (default)      # Set filtered\_alias\_mode to 'nowarn' to allow more than 2 filtered aliases per index silently      #filtered\_alias\_mode: warn      #do\_not\_fail\_on\_forbidden: false      #kibana:      # Kibana multitenancy      #multitenancy\_enabled: true      #private\_tenant\_enabled: true      #default\_tenant: ""      #server\_username: kibanaserver      #index: '.kibana'      http:        anonymous\_auth\_enabled: false        xff:          enabled: true          internalProxies: '192\.168\.0\.10|192\.168\.0\.11' # regex pattern          #internalProxies: '.\*' # trust all internal proxies, regex pattern          remoteIpHeader:  'x-forwarded-for'          ###### see <https://docs.oracle.com/javase/7/docs/api/java/util/regex/Pattern.html> for regex help          ###### more information about XFF <https://en.wikipedia.org/wiki/X-Forwarded-For>          ###### and here <https://tools.ietf.org/html/rfc7239>          ###### and <https://tomcat.apache.org/tomcat-8.0-doc/config/valve.html#Remote_IP_Valve>      authc:        basic\_internal\_auth\_domain:          description: "Authenticate via HTTP Basic against internal users database"          http\_enabled: true          transport\_enabled: true          order: **0**          http\_authenticator:            type: basic            challenge: false          authentication\_backend:            type: intern        openid\_auth\_domain:          http\_enabled: true          transport\_enabled: true          order: **1**          http\_authenticator:            type: openid            challenge: false            config:              subject\_key: preferred\_username              roles\_key: roles              openid\_connect\_idp:                enable\_ssl: true                verify\_hostnames: false                pemtrustedcas\_filepath: /usr/share/opensearch/config/certificates/shell.crt              openid\_connect\_url: "<https://rauth.rdtex.msk.ru/realms/ead/.well-known/openid-configuration>"              client\_id: "opensearch"              client\_secret: \*\*\*\*\*\*\*\*              kibana\_url: https://os-stage.rdtex.msk.ru:5605          authentication\_backend:            type: noop |

Дополнительные настройки маппинга roles на backend\_roles

|  |
| --- |
| **---**  # In this file users, backendroles and hosts can be mapped to Security roles.  # Permissions for OpenSearch roles are configured in roles.yml    \_meta:    type: "rolesmapping"    config\_version: **2**    # Define your roles mapping here    ## Demo roles mapping    all\_access:    reserved: false    backend\_roles:  **-** "admin"  **-** "os-admin"    description: "Maps admin to all\_access"    own\_index:    reserved: false    users:  **-** "\*"    description: "Allow full access to an index named like the username"    logstash:    reserved: false    backend\_roles:  **-** "logstash"    kibana\_user:    reserved: false    backend\_roles:  **-** "kibanauser"    description: "Maps kibanauser to kibana\_user"    readall:    reserved: false    backend\_roles:  **-** "readall"    manage\_snapshots:    reserved: false    backend\_roles:  **-** "snapshotrestore"    kibana\_server:    reserved: true    users:  **-** "kibanaserver" |

Инициализация Security Plugin либо применение изменений после изменения конфигурационных файлов OpenSearch

|  |
| --- |
| # /opt/ead\_stage/security\_admin.sh    docker-compose exec os01 bash -c "chmod +x /usr/share/opensearch/plugins/opensearch-security/tools/securityadmin.sh && bash /usr/share/opensearch/plugins/opensearch-security/tools/securityadmin.sh -cd /usr/share/opensearch/config/opensearch-security/ -icl -nhnv -cacert config/certificates/ca/ca.pem -cert config/certificates/ca/admin.pem -key config/certificates/ca/admin.key -h localhost" |

### **3.1.4. Monolith**

Сборка разворачивается посредством CI/CD Jenkins. Репозитарии в BitBucket.

devops@ead-02:/etc/systemd/system$ cat /var/apps/rchivemonolith/ecm-module-monolith-0.0.1-SNAPSHOT.jar

|  |
| --- |
| devops@ead-02:/etc/systemd/system$ ls -ltr /var/apps/rchivemonolith/  -rw-r--r-- 1 ead ead 183050 ноя 5 15:26 audit\_events.log  -rw-r--r-- 1 ead ead 80895 ноя 8 11:05 os.trace.db  -rw-r--r-- 1 ead ead 438272 ноя 12 17:26 os.mv.db  -rw-r--r-- 1 ead ead 270 ноя 18 18:27 os\_db.trace.db  -rw-r--r-- 1 ead ead 111725694 ноя 18 18:42 ecm-module-monolith-0.0.1-SNAPSHOT.jar  -rw-r--r-- 1 ead ead 9020506 ноя 18 18:43 monolith.log  -rw-r--r-- 1 ead ead 626688 ноя 18 18:43 os\_db.mv.db |

Запускается как сервис rchivemonolith.service

|  |
| --- |
| # /etc/systemd/system/rchivemonolith.service    [Unit]  Description=Spring Boot Monolith Application  After=network.target    [Service]  User=ead  Group=ead  WorkingDirectory=/var/apps/rchivemonolith  ExecStart=/usr/bin/java -Xms256m -Xmx2048m -jar /var/apps/rchivemonolith/ecm-module-monolith-0.0.1-SNAPSHOT.jar --server.port=8088 >> /var/apps/rchivemonolith/monolith.log  2>&1  #ExecStart=/usr/bin/java -agentlib:jdwp=transport=dt\_socket,server=y,suspend=n,address=\*:8000 -Xms256m -Xmx2048m -jar /var/apps/rchivemonolith/ecm-module-monolith-0.0.1-SNAPSHOT.jar  >> /var/apps/rchivemonolith/monolith.log  2>&1  Environment=TZ=Europe/Moscow  Environment=HTTP\_PROXY=http://172.24.0.254:3128  Environment=HTTPS\_PROXY=http://172.24.0.254:3128  Environment=KEYCLOAK\_URL=https://rauth.rdtex.msk.ru  Environment=OPENSEARCH\_URL=https://os-stage.rdtex.msk.ru:9205  Environment=MINIO\_URL=https://minio-stage.rdtex.msk.ru:9005  Environment=MINIO\_LOGIN=admin  Environment=MINIO\_PASSWORD=\*\*\*\*\*\*\*\*  Environment=MINIO\_BUCKET=rchive  Environment=OTEL\_EXPORTER\_OTLP\_ENDPOINT=http://ead-02.rdtex.msk.ru:4317  Environment=OTEL\_METRIC\_EXPORT\_INTERVAL=5s  Environment=KEYCLOAK\_REALM=ead  Environment=KEYCLOAK\_CLIENT\_ID=ead-app  Environment=KEYCLOAK\_CLIENT\_SECRET=\*\*\*\*\*\*\*\*  Environment=KEYCLOAK\_WEBDAV\_CLIENT=ead-webdav-client  Environment=KEYCLOAK\_WEBDAV\_CLIENT\_SECRET=\*\*\*\*\*\*\*\*  Environment=TOMCAT\_CONN\_TIMEOUT=-1  Environment=JAVA\_OPTS="-Xms256m -Xmx2048m -Dotel.metrics.exporter=console"  Environment=SPRING\_DATASOURCE\_URL=jdbc:h2:file:./os\_db;DB\_CLOSE\_DELAY=-1  Environment=SPRING\_DATASOURCE\_USERNAME=sa  Environment=SPRING\_DATASOURCE\_PASSWORD=\*\*\*\*\*\*\*\*    ExecReload=/bin/kill -s HUP $MAINPID  Restart=no  #RestartSec=10    StandardOutput=append:/var/apps/rchivemonolith/monolith.log  StandardError=append:/var/apps/rchivemonolith/monolith.log    [Install]  WantedBy=multi-user.target |

Конфигурация nginx-proxy для Monolith service

|  |
| --- |
| # /usr/local/openresty/nginx/conf/conf.d/rchive.conf  server {         listen 443 ssl;         listen [::]:99;        ssl\_certificate /etc/ssl/shell/msk.crt;      ssl\_certificate\_key /etc/ssl/shell/key.pem;        # Укажите резолвер, который будет использовать Nginx              resolver 172.24.0.128;           server\_name  rchive.rdtex.msk.ru;           access\_log    /var/log/nginx/rchive.access.log;         error\_log     /var/log/nginx/rchive.error.log;           root /var/www/rchive-app/out;         index index.html;           location / {                 #try\_files $uri $uri/ =404;          if (-f $request\_filename) {                  expires max;                  break;           }             if ($request\_filename !~ "\.(js|ico|gif|jpg|png|css)$") {                  rewrite ^(.\*) /index.html last;           }         }            location /api/v1/ {     #    ssl\_certificate /etc/ssl/shell/msk.crt;      #ssl\_certificate\_key /etc/ssl/shell/key.pem;          proxy\_pass http://rchive.rdtex.msk.ru:8088$request\_uri;         # add\_header 'Access-Control-Allow-Origin' '[http://rchive.rdtex.msk.ru:3000](http://rchive.rdtex.msk.ru:3000/)' always;   add\_header 'Access-Control-Allow-Origin' '[http://localhost:3000](http://localhost:3000/)' always;          add\_header 'Access-Control-Allow-Methods' 'GET, POST, PUT, DELETE, OPTIONS' always;          add\_header 'Access-Control-Allow-Headers' 'Content-Type, Authorization' always;            # Обработка preflight запросов          if ($request\_method = 'OPTIONS') {          #    add\_header 'Access-Control-Allow-Origin' '[http://rchive.rdtex.msk.ru:3000](http://rchive.rdtex.msk.ru:3000/)' always;    add\_header 'Access-Control-Allow-Origin' '[http://localhost:3000](http://localhost:3000/)' always;              add\_header 'Access-Control-Allow-Methods' 'GET, POST, PUT, DELETE, OPTIONS' always;              add\_header 'Access-Control-Allow-Headers' 'Content-Type, Authorization' always;              add\_header 'Access-Control-Max-Age' 86400;              return 204;  # 204 No Content для успешного завершения preflight запроса          }            # Проксификация запросов на backend сервер          proxy\_set\_header Host $host;          proxy\_set\_header X-Real-IP $remote\_addr;          proxy\_set\_header X-Forwarded-For $proxy\_add\_x\_forwarded\_for;          proxy\_set\_header X-Forwarded-Proto $scheme;      }        location /process-api {            #    ssl\_certificate /etc/ssl/shell/msk.crt;      #ssl\_certificate\_key /etc/ssl/shell/key.pem;          proxy\_pass http://rchive.rdtex.msk.ru:8088$request\_uri;         # add\_header 'Access-Control-Allow-Origin' '[http://rchive.rdtex.msk.ru:3000](http://rchive.rdtex.msk.ru:3000/)' always;          #add\_header 'Access-Control-Allow-Origin' '\*' always;          add\_header 'Access-Control-Allow-Origin' '[http://localhost:3000](http://localhost:3000/)' always;          add\_header 'Access-Control-Allow-Methods' 'GET, POST, PUT, DELETE, OPTIONS' always;          add\_header 'Access-Control-Allow-Headers' 'Content-Type, Authorization' always;            # Обработка preflight запросов          if ($request\_method = 'OPTIONS') {          proxy\_pass http://rchive.rdtex.msk.ru:8088$request\_uri;          #add\_header 'Access-Control-Allow-Origin' '\*' always;           add\_header 'Access-Control-Allow-Origin' '[http://localhost:3000](http://localhost:3000/)' always;                add\_header 'Access-Control-Allow-Methods' 'GET, POST, PUT, DELETE, OPTIONS' always;              add\_header 'Access-Control-Allow-Headers' 'Content-Type, Authorization' always;              add\_header 'Access-Control-Max-Age' 86400;              return 204;  # 204 No Content для успешного завершения preflight запроса          }            # Проксификация запросов на backend сервер          proxy\_set\_header Host $host;          proxy\_set\_header X-Real-IP $remote\_addr;          proxy\_set\_header X-Forwarded-For $proxy\_add\_x\_forwarded\_for;          proxy\_set\_header X-Forwarded-Proto $scheme;      }        location /auth/ {          proxy\_pass https://rauth.rdtex.msk.ru/;          proxy\_ssl\_verify off;            proxy\_set\_header Host $host;          proxy\_set\_header X-Real-IP $remote\_addr;          proxy\_set\_header X-Forwarded-For $proxy\_add\_x\_forwarded\_for;          proxy\_set\_header X-Forwarded-Proto $scheme;            proxy\_connect\_timeout 60s;          proxy\_send\_timeout 60s;          proxy\_read\_timeout 60s;            proxy\_buffer\_size 128k;          proxy\_buffers 4 256k;          proxy\_busy\_buffers\_size 256k;      }    } |

## **3.2. BACKEND**

BACKEND состоит из двух приложений monolith и bpm-engine

Сборка происходит в среде Jenkins:

\* Выполнить команду shell:

|  |
| --- |
| export JAVA\_HOME=/usr/lib/jvm/graalvm-community-openjdk-21.0.2+13.1  export PATH=$JAVA\_HOME/bin:$PATH  cp ~/cacerts $WORKSPACE  export JAVA\_OPTS="-Djavax.net.ssl.trustStore=./cacerts -Djavax.net.ssl.trustStorePassword=changeit"  export KEYCLOAK\_URL=https://keycloak.rdtex.msk.ru  export OPENSEARCH\_URL=https://os01:9200 |

\* Вызвать цели Maven верхнего уровня

clean install -Dmaven.repo.local=$HOME/.m2/repository-${BRANCH}

\*Выполнить команду

sudo cp ./opt/monolith/target/\* /var/apps/monolith/ && sudo chown ead:ead /var/apps/monolith/\* && sudo systemctl restart monolith.service

Конфигурация сервиса

/etc/systemd/system/monolith.service

|  |
| --- |
| [Unit]  Description=Spring Boot Monolith Application  After=network.target    [Service]  User=ead  Group=ead  WorkingDirectory=/var/apps/monolith  ExecStart=/usr/bin/java -Xms256m -Xmx4096m -jar /var/apps/monolith/ecm-module-monolith-0.0.1-SNAPSHOT.jar  >> /var/apps/monolith/monolith.log  2>&1  Environment=TZ=Europe/Moscow  Environment=HTTP\_PROXY=http://172.24.0.254:3128  Environment=HTTPS\_PROXY=http://172.24.0.254:3128  Environment=KEYCLOAK\_URL=https://keycloak.rdtex.msk.ru  Environment=OPENSEARCH\_URL=https://ead-01.rdtex.msk.ru:9200  Environment=MINIO\_URL=https://ead-01.rdtex.msk.ru:9090  Environment=MINIO\_LOGIN=minioadmin  Environment=MINIO\_PASSWORD=\*\*\*\*\*\*\*\*\*\*  Environment=MINIO\_BUCKET=test  Environment=OTEL\_EXPORTER\_OTLP\_ENDPOINT=http://ead-02.rdtex.msk.ru:4317  Environment=OTEL\_METRIC\_EXPORT\_INTERVAL=5s  Environment=KEYCLOAK\_REALM=ead  Environment=KEYCLOAK\_CLIENT\_ID=ead-app  Environment=KEYCLOAK\_CLIENT\_SECRET=\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*  Environment=KEYCLOAK\_WEBDAV\_CLIENT=ead-webdav-client  Environment=KEYCLOAK\_WEBDAV\_CLIENT\_SECRET=\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*  Environment=TOMCAT\_CONN\_TIMEOUT=-1  Environment=JAVA\_OPTS="-Xms256m -Xmx4096m -Dotel.metrics.exporter=console"  Environment=SPRING\_DATASOURCE\_URL=jdbc:h2:file:./os\_db;DB\_CLOSE\_DELAY=-1  Environment=SPRING\_DATASOURCE\_USERNAME=sa  Environment=SPRING\_DATASOURCE\_PASSWORD=sa  Environment=LOGAUDIT\_ENABLE=true  Environment=LOGSTASH\_DESTINATION=ead-01.rdtex.msk.ru:5001  ExecReload=/bin/kill -s HUP $MAINPID  Restart=no    StandardOutput=append:/var/apps/monolith/monolith.log  StandardError=append:/var/apps/monolith/monolith.log    [Install]  WantedBy=multi-user.target |

Запуск BACKEND

sudo systemctl start monolith.service

## **3.3. FRONTEND**

Конфиг файл .env.ead-01 с переменными для сборки статического front-end

|  |
| --- |
| ###############  # BACKEND #  ###############  # OIDC credentials  OIDC\_TRUSTED\_DOMAINS="https://keycloak.rdtex.msk.ru, https://ead-01.rdtex.msk.ru"  # Workaround for self-signed SSL  NODE\_TLS\_REJECT\_UNAUTHORIZED=0  # Output mode  NEXT\_PUBLIC\_OUTPUT=export  ################  # FRONTEND #  ################  # OIDC credentials  NEXT\_PUBLIC\_OIDC\_CLIENT\_ID="ead\_frontend"  NEXT\_PUBLIC\_OIDC\_ISSUER\_URI="https://keycloak.rdtex.msk.ru/realms/ead"  NEXT\_PUBLIC\_OIDC\_SERVICEWORKER=1  # APIs  NEXT\_PUBLIC\_APP\_API="https://ead-01.rdtex.msk.ru/api/v1" |

сборка архива

|  |
| --- |
| rm -rf ./out  npm i  npm run build:ead-01  rar a -r out-01.rar ./out |

после сборки появится архив out-01.rar , который надо распакавать в папку

указанную в конфиге nginx /etc/nginx/sites-enabled/ead-static

(в данном случае /var/www/nextjs-app/out )

|  |
| --- |
| server {         listen 443 ssl;         listen [::]:99;        ssl\_certificate /etc/ssl/shell/msk.crt;      ssl\_certificate\_key /etc/ssl/shell/key.pem;            # Укажите резолвер, который будет использовать Nginx              resolver 172.24.0.128;  # Используем DNS-серверы Google           server\_name  ead-01.rdtex.msk.ru;           access\_log    /var/log/nginx/ead.access.log;         error\_log     /var/log/nginx/ead.error.log;           root /var/www/nextjs-app/out;         index index.html;           location / {                 #try\_files $uri $uri/ =404;             if (-f $request\_filename) {                      expires max;                      break;              }                if ($request\_filename !~ "\.(js|ico|gif|jpg|png|css)$") {                      rewrite ^(.\*) /index.html last;              }         }    location /monologs/ {      alias /var/apps/monolith/;      autoindex on;      access\_log off;      log\_not\_found off;      sendfile on;  }          location /api/v1/ {        #    ssl\_certificate /etc/ssl/shell/msk.crt;      #ssl\_certificate\_key /etc/ssl/shell/key.pem;          proxy\_pass http://ead-01.rdtex.msk.ru:8080$request\_uri;         # add\_header 'Access-Control-Allow-Origin' '[http://ead-01.rdtex.msk.ru:3000](http://ead-01.rdtex.msk.ru:3000/)' always;      add\_header 'Access-Control-Allow-Origin' '[http://localhost:3000](http://localhost:3000/)' always;          add\_header 'Access-Control-Allow-Methods' 'GET, POST, PUT, DELETE, OPTIONS' always;          add\_header 'Access-Control-Allow-Headers' 'Content-Type, Authorization' always;            # Обработка preflight запросов          if ($request\_method = 'OPTIONS') {          #    add\_header 'Access-Control-Allow-Origin' '[http://ead-01.rdtex.msk.ru:3000](http://ead-01.rdtex.msk.ru:3000/)' always;       add\_header 'Access-Control-Allow-Origin' '[http://localhost:3000](http://localhost:3000/)' always;              add\_header 'Access-Control-Allow-Methods' 'GET, POST, PUT, DELETE, OPTIONS' always;              add\_header 'Access-Control-Allow-Headers' 'Content-Type, Authorization' always;              add\_header 'Access-Control-Max-Age' 86400;              return 204;  # 204 No Content для успешного завершения preflight запроса          }            # Проксификация запросов на backend сервер          proxy\_set\_header Host $host;          proxy\_set\_header X-Real-IP $remote\_addr;          proxy\_set\_header X-Forwarded-For $proxy\_add\_x\_forwarded\_for;          proxy\_set\_header X-Forwarded-Proto $scheme;      }        location /process-api {            #    ssl\_certificate /etc/ssl/shell/msk.crt;      #ssl\_certificate\_key /etc/ssl/shell/key.pem;          proxy\_pass http://ead.rdtex.msk.ru:8080$request\_uri;         # add\_header 'Access-Control-Allow-Origin' '[http://ead.rdtex.msk.ru:3000](http://ead.rdtex.msk.ru:3000/)' always;          #add\_header 'Access-Control-Allow-Origin' '\*' always;          add\_header 'Access-Control-Allow-Origin' '[http://localhost:3000](http://localhost:3000/)' always;          add\_header 'Access-Control-Allow-Methods' 'GET, POST, PUT, DELETE, OPTIONS' always;          add\_header 'Access-Control-Allow-Headers' 'Content-Type, Authorization' always;            # Обработка preflight запросов          if ($request\_method = 'OPTIONS') {          proxy\_pass http://ead.rdtex.msk.ru:8080$request\_uri;          #add\_header 'Access-Control-Allow-Origin' '\*' always;           add\_header 'Access-Control-Allow-Origin' '[http://localhost:3000](http://localhost:3000/)' always;                add\_header 'Access-Control-Allow-Methods' 'GET, POST, PUT, DELETE, OPTIONS' always;              add\_header 'Access-Control-Allow-Headers' 'Content-Type, Authorization' always;              add\_header 'Access-Control-Max-Age' 86400;              return 204;  # 204 No Content для успешного завершения preflight запроса          }            # Проксификация запросов на backend сервер          proxy\_set\_header Host $host;          proxy\_set\_header X-Real-IP $remote\_addr;          proxy\_set\_header X-Forwarded-For $proxy\_add\_x\_forwarded\_for;          proxy\_set\_header X-Forwarded-Proto $scheme;      }        location /auth/ {      #proxy\_pass [https://keycloak.rdtex.msk.ru:8444](https://keycloak.rdtex.msk.ru:8444/);          proxy\_pass https://keycloak.rdtex.msk.ru/;          proxy\_ssl\_verify off;            proxy\_set\_header Host $host;          proxy\_set\_header X-Real-IP $remote\_addr;          proxy\_set\_header X-Forwarded-For $proxy\_add\_x\_forwarded\_for;          proxy\_set\_header X-Forwarded-Proto $scheme;            proxy\_connect\_timeout 60s;          proxy\_send\_timeout 60s;          proxy\_read\_timeout 60s;            proxy\_buffer\_size 128k;          proxy\_buffers 4 256k;          proxy\_busy\_buffers\_size 256k;      }  } |

## **3.4. Конфигурация NGINX сервисов EAD**

Конфигурация nginx proxy для сервисов нагрузочного стенда

\*\*\*\* FOR FRONTEND SERVICE

/etc/nginx/sites-available/ead-static

|  |
| --- |
| server {         listen 443 ssl;         listen [::]:99;        ssl\_certificate /etc/ssl/shell/msk.crt;      ssl\_certificate\_key /etc/ssl/shell/key.pem;        # Укажите резолвер, который будет использовать Nginx              resolver 172.24.0.128;  # Используем DNS-серверы Google           server\_name  ead-01.rdtex.msk.ru;           access\_log    /var/log/nginx/ead.access.log;         error\_log     /var/log/nginx/ead.error.log;           root /var/www/nextjs-app/out;         index index.html;           location / {                 #try\_files $uri $uri/ =404;                 if (-f $request\_filename) {                          expires max;                          break;                  }                    if ($request\_filename !~ "\.(js|ico|gif|jpg|png|css)$") {                          rewrite ^(.\*) /index.html last;                  }         }    location /monologs/ {      alias /var/apps/monolith/;      autoindex on;      access\_log off;      log\_not\_found off;      sendfile on;  }          location /api/v1/ {            proxy\_pass http://ead-01.rdtex.msk.ru:8080$request\_uri;          add\_header 'Access-Control-Allow-Origin' '[http://localhost:3000](http://localhost:3000/)' always;          add\_header 'Access-Control-Allow-Methods' 'GET, POST, PUT, DELETE, OPTIONS' always;          add\_header 'Access-Control-Allow-Headers' 'Content-Type, Authorization' always;            # Обработка preflight запросов          if ($request\_method = 'OPTIONS') {              add\_header 'Access-Control-Allow-Origin' '[http://localhost:3000](http://localhost:3000/)' always;              add\_header 'Access-Control-Allow-Methods' 'GET, POST, PUT, DELETE, OPTIONS' always;              add\_header 'Access-Control-Allow-Headers' 'Content-Type, Authorization' always;              add\_header 'Access-Control-Max-Age' 86400;              return 204;  # 204 No Content для успешного завершения preflight запроса          }            # Проксификация запросов на backend сервер          proxy\_set\_header Host $host;          proxy\_set\_header X-Real-IP $remote\_addr;          proxy\_set\_header X-Forwarded-For $proxy\_add\_x\_forwarded\_for;          proxy\_set\_header X-Forwarded-Proto $scheme;      }        location /process-api {            proxy\_pass http://ead.rdtex.msk.ru:8080$request\_uri;          add\_header 'Access-Control-Allow-Origin' '[http://localhost:3000](http://localhost:3000/)' always;          add\_header 'Access-Control-Allow-Methods' 'GET, POST, PUT, DELETE, OPTIONS' always;          add\_header 'Access-Control-Allow-Headers' 'Content-Type, Authorization' always;            # Обработка preflight запросов          if ($request\_method = 'OPTIONS') {          proxy\_pass http://ead.rdtex.msk.ru:8080$request\_uri;              add\_header 'Access-Control-Allow-Origin' '[http://localhost:3000](http://localhost:3000/)' always;                add\_header 'Access-Control-Allow-Methods' 'GET, POST, PUT, DELETE, OPTIONS' always;              add\_header 'Access-Control-Allow-Headers' 'Content-Type, Authorization' always;              add\_header 'Access-Control-Max-Age' 86400;              return 204;  # 204 No Content для успешного завершения preflight запроса          }            # Проксификация запросов на backend сервер          proxy\_set\_header Host $host;          proxy\_set\_header X-Real-IP $remote\_addr;          proxy\_set\_header X-Forwarded-For $proxy\_add\_x\_forwarded\_for;          proxy\_set\_header X-Forwarded-Proto $scheme;      }        location /auth/ {          proxy\_pass https://keycloak.rdtex.msk.ru/;          proxy\_ssl\_verify off;            proxy\_set\_header Host $host;          proxy\_set\_header X-Real-IP $remote\_addr;          proxy\_set\_header X-Forwarded-For $proxy\_add\_x\_forwarded\_for;          proxy\_set\_header X-Forwarded-Proto $scheme;            proxy\_connect\_timeout 60s;          proxy\_send\_timeout 60s;          proxy\_read\_timeout 60s;            proxy\_buffer\_size 128k;          proxy\_buffers 4 256k;          proxy\_busy\_buffers\_size 256k;      }  } |

\*\*\*\* FOR KEYCLOAK SERVICE

/etc/nginx/sites-enabled/keycloak

|  |
| --- |
| server {  listen 0.0.0.0:80;  listen [::]:80;  server\_name keycloak-shell.rdtex.msk.ru;  return 302 https://keycloak-shell.rdtex.msk.ru$request\_uri;  }      server {  listen 443 ssl ;  server\_name keycloak-shell.rdtex.msk.ru;  ssl\_certificate /etc/ssl/shell/shell.crt;  ssl\_certificate\_key /etc/ssl/shell/shell.key;  root /var/www/html;  index index.html index.htm index.nginx-debian.html;  server\_name \_;  location ^~/ {  proxy\_pass http://keycloak-shell.rdtex.msk.ru:9080;  proxy\_redirect off;  proxy\_set\_header Host $host;  proxy\_set\_header X-Real-IP $remote\_addr;  proxy\_set\_header X-Forwarded-For $remote\_addr;  proxy\_set\_header X-Forwarded-Proto $scheme;  proxy\_set\_header X-Forwarded-Port 443;  }  }    server {  listen 8444 ssl;  server\_name keycloak-shell.rdtex.msk.ru;    ssl\_certificate /etc/ssl/shell/tls.crt;  ssl\_certificate\_key /etc/ssl/shell/tls.key;    location / {  proxy\_pass https://localhost:8843;  proxy\_set\_header Host $host;  proxy\_set\_header X-Real-IP $remote\_addr;  proxy\_set\_header X-Forwarded-For $proxy\_add\_x\_forwarded\_for;  proxy\_set\_header X-Forwarded-Proto $scheme;  }  }        \*\*\*\* FOR OPENSEARCH SERVICES    conf.d/opensearch.conf  upstream opensearch\_cluster {  server os-01.rdtex.msk.ru:9200;  server os-02.rdtex.msk.ru:9200;  server os-03.rdtex.msk.ru:9200;  server os-04.rdtex.msk.ru:9200;  server os-05.rdtex.msk.ru:9200;    keepalive 132; # Поддерживать до 32 постоянных соединений  }    # Формат логов с указанием upstream-узла  log\_format upstream\_logging '$remote\_addr - $remote\_user [$time\_local] '  '"$request" $status $body\_bytes\_sent '  '"$http\_referer" "$http\_user\_agent" '  '$request\_time $upstream\_addr';      server {  listen 9200 ssl;  server\_name ead-01.rdtex.msk.ru;  # Путь к SSL сертификатам  ssl\_certificate /etc/nginx/ssl/minio.crt;  ssl\_certificate\_key /etc/nginx/ssl/minio.key;    # Пути для логов  access\_log /var/log/nginx/opensearch\_access.log upstream\_logging;  error\_log /var/log/nginx/opensearch\_error.log warn;    # Лимит времени ожидания  proxy\_read\_timeout 90;  proxy\_connect\_timeout 90;  proxy\_send\_timeout 90;    # Настройка заголовков  proxy\_set\_header Host $host;  proxy\_set\_header X-Real-IP $remote\_addr;  proxy\_set\_header X-Forwarded-For $proxy\_add\_x\_forwarded\_for;    location / {  proxy\_pass https://opensearch\_cluster;  proxy\_http\_version 1.1;  proxy\_set\_header Connection ""; # Открытые соединения для Keep-Alive  }  } |

\*\*\*\* FOR MINIO SERVICES

/etc/nginx/conf.d/minio.conf

|  |
| --- |
| upstream minio {      least\_conn;      server minio-01.rdtex.msk.ru:9091;      server minio-02.rdtex.msk.ru:9091;      server minio-03.rdtex.msk.ru:9091;      server minio-04.rdtex.msk.ru:9091;      server minio-05.rdtex.msk.ru:9091;  }      upstream console {      least\_conn;      server minio-01.rdtex.msk.ru:9092;      server minio-02.rdtex.msk.ru:9092;      server minio-03.rdtex.msk.ru:9092;      server minio-04.rdtex.msk.ru:9092;      server minio-05.rdtex.msk.ru:9092;  }    server {      listen       9090 ssl;      listen  [::]:9090 ssl;      server\_name ead-01.rdtex.msk.ru;        # Путь к SSL сертификатам      ssl\_certificate /etc/nginx/ssl/minio.crt;      ssl\_certificate\_key /etc/nginx/ssl/minio.key;        # Allow special characters in headers      ignore\_invalid\_headers off;      # Allow any size file to be uploaded.      # Set to a value such as 1000m; to restrict file size to a specific value      client\_max\_body\_size 0;      # Disable buffering      proxy\_buffering off;      proxy\_request\_buffering off;        location / {            proxy\_set\_header Host $http\_host;          proxy\_set\_header X-Real-IP $remote\_addr;          proxy\_set\_header X-Forwarded-For $proxy\_add\_x\_forwarded\_for;          proxy\_set\_header X-Forwarded-Proto $scheme;          proxy\_connect\_timeout 300;          proxy\_read\_timeout 300;          proxy\_send\_timeout 300;          send\_timeout 300;            #rewrite ^/(.\*) $1 break;          proxy\_pass https://minio;      }  }    server {      listen       9092 ssl;      listen  [::]:9092 ssl;      server\_name ead-01.rdtex.msk.ru;        # Путь к SSL сертификатам      ssl\_certificate /etc/nginx/ssl/minio.crt;      ssl\_certificate\_key /etc/nginx/ssl/minio.key;        # Allow special characters in headers      ignore\_invalid\_headers off;      # Allow any size file to be uploaded.      # Set to a value such as 1000m; to restrict file size to a specific value      client\_max\_body\_size 0;      # Disable buffering      proxy\_buffering off;      proxy\_request\_buffering off;        location / {          #rewrite ^/minio/ui/(.\*) /$1 break;          #rewrite ^/console/(.\*) /$1 break;          proxy\_set\_header Host $http\_host;          proxy\_set\_header X-Real-IP $remote\_addr;          proxy\_set\_header X-Forwarded-For $proxy\_add\_x\_forwarded\_for;          proxy\_set\_header X-Forwarded-Proto $scheme;          proxy\_set\_header X-NginX-Proxy true;            # This is necessary to pass the correct IP to be hashed          real\_ip\_header X-Real-IP;            proxy\_connect\_timeout 300;            # To support websockets in MinIO versions released after January 2023          proxy\_http\_version 1.1;          proxy\_set\_header Upgrade $http\_upgrade;          proxy\_set\_header Connection "upgrade";          # Some environments may encounter CORS errors (Kubernetes + Nginx Ingress)          # Uncomment the following line to set the Origin request to an empty string          # proxy\_set\_header Origin '';            chunked\_transfer\_encoding off;            proxy\_pass https://console; # This uses the upstream directive definition to load balance     }  } |

## **3.5. Конфигурация Keycloak клиентов**

На стороне Keycloak необходимо создать следующих клиентов:

opensearch\_cluster

ead\_frontend

ead-webdav-client

Файлы конфигурации клиентов:

opensearch\_cluster.json

|  |
| --- |
| {    "clientId": "opensearch\_cluster",    "name": "opensearch\_cluster",    "description": "opensearch\_cluster",    "rootUrl": "",    "adminUrl": "",    "baseUrl": "",    "surrogateAuthRequired": false,    "enabled": true,    "alwaysDisplayInConsole": false,    "clientAuthenticatorType": "client-secret",    "secret": "GgbKmmKEy9Ak4prBSyKFsoh3frtOpQAL",    "redirectUris": [      "[https://os-01.rdtex.msk.ru:5601/\*](https://os-01.rdtex.msk.ru:5601/*)"    ],    "webOrigins": [      "/\*"    ],    "notBefore": 0,    "bearerOnly": false,    "consentRequired": false,    "standardFlowEnabled": true,    "implicitFlowEnabled": false,    "directAccessGrantsEnabled": true,    "serviceAccountsEnabled": true,    "publicClient": false,    "frontchannelLogout": true,    "protocol": "openid-connect",    "attributes": {      "oidc.ciba.grant.enabled": "false",      "client.secret.creation.time": "1722946533",      "backchannel.logout.session.required": "true",      "oauth2.device.authorization.grant.enabled": "false",      "display.on.consent.screen": "false",      "backchannel.logout.revoke.offline.tokens": "false"    },    "authenticationFlowBindingOverrides": {},    "fullScopeAllowed": true,    "nodeReRegistrationTimeout": -1,    "protocolMappers": [      {        "name": "Client IP Address",        "protocol": "openid-connect",        "protocolMapper": "oidc-usersessionmodel-note-mapper",        "consentRequired": false,        "config": {          "user.session.note": "clientAddress",          "id.token.claim": "true",          "introspection.token.claim": "true",          "access.token.claim": "true",          "claim.name": "clientAddress",          "jsonType.label": "String"        }      },      {        "name": "Client Host",        "protocol": "openid-connect",        "protocolMapper": "oidc-usersessionmodel-note-mapper",        "consentRequired": false,        "config": {          "user.session.note": "clientHost",          "id.token.claim": "true",          "introspection.token.claim": "true",          "access.token.claim": "true",          "claim.name": "clientHost",          "jsonType.label": "String"        }      },      {        "name": "Client ID",        "protocol": "openid-connect",        "protocolMapper": "oidc-usersessionmodel-note-mapper",        "consentRequired": false,        "config": {          "user.session.note": "client\_id",          "id.token.claim": "true",          "introspection.token.claim": "true",          "access.token.claim": "true",          "claim.name": "client\_id",          "jsonType.label": "String"        }      }    ],    "defaultClientScopes": [      "web-origins",      "acr",      "profile",      "roles",      "basic",      "openid-connect",      "email"    ],    "optionalClientScopes": [      "address",      "phone",      "offline\_access",      "microprofile-jwt"    ],    "access": {      "view": true,      "configure": true,      "manage": true    }  } |

ead\_fron\_end.json

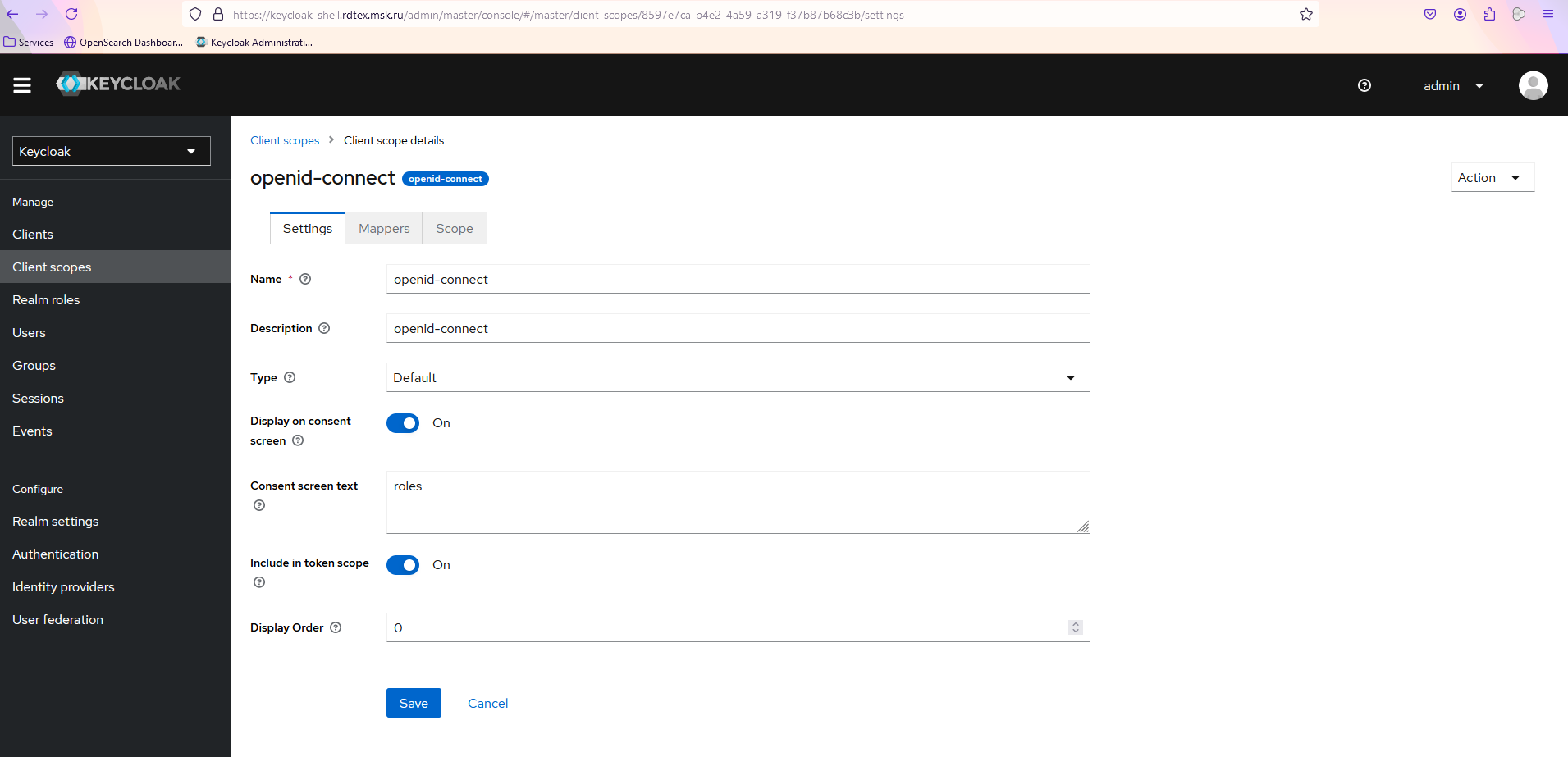
|  |
| --- |
| {    "clientId": "ead\_frontend",    "name": "ead\_frontend",    "description": "ead\_frontend",    "rootUrl": "",    "adminUrl": "",    "baseUrl": "/\*",    "surrogateAuthRequired": false,    "enabled": true,    "alwaysDisplayInConsole": false,    "clientAuthenticatorType": "client-secret",    "redirectUris": [      "\*"    ],    "webOrigins": [      "\*"    ],    "notBefore": 0,    "bearerOnly": false,    "consentRequired": false,    "standardFlowEnabled": true,    "implicitFlowEnabled": false,    "directAccessGrantsEnabled": true,    "serviceAccountsEnabled": false,    "publicClient": true,    "frontchannelLogout": true,    "protocol": "openid-connect",    "attributes": {      "client.introspection.response.allow.jwt.claim.enabled": "false",      "login\_theme": "ead",      "post.logout.redirect.uris": "\*",      "oauth2.device.authorization.grant.enabled": "false",      "backchannel.logout.revoke.offline.tokens": "false",      "use.refresh.tokens": "true",      "oidc.ciba.grant.enabled": "false",      "client.use.lightweight.access.token.enabled": "false",      "backchannel.logout.session.required": "true",      "client\_credentials.use\_refresh\_token": "false",      "tls.client.certificate.bound.access.tokens": "false",      "require.pushed.authorization.requests": "false",      "acr.loa.map": "{}",      "display.on.consent.screen": "false",      "token.response.type.bearer.lower-case": "false"    },    "authenticationFlowBindingOverrides": {},    "fullScopeAllowed": true,    "nodeReRegistrationTimeout": -1,    "protocolMappers": [      {        "name": "Client Host",        "protocol": "openid-connect",        "protocolMapper": "oidc-usersessionmodel-note-mapper",        "consentRequired": false,        "config": {          "user.session.note": "clientHost",          "introspection.token.claim": "true",          "userinfo.token.claim": "true",          "id.token.claim": "true",          "lightweight.claim": "false",          "access.token.claim": "true",          "claim.name": "clientHost",          "jsonType.label": "String",          "access.tokenResponse.claim": "false"        }      }    ],    "defaultClientScopes": [      "web-origins",      "acr",      "profile",      "roles",      "basic",      "openid-connect",      "email"    ],    "optionalClientScopes": [      "address",      "phone",      "offline\_access",      "microprofile-jwt"    ],    "access": {      "view": true,      "configure": true,      "manage": true    }  } |

ead-webdav-client.json

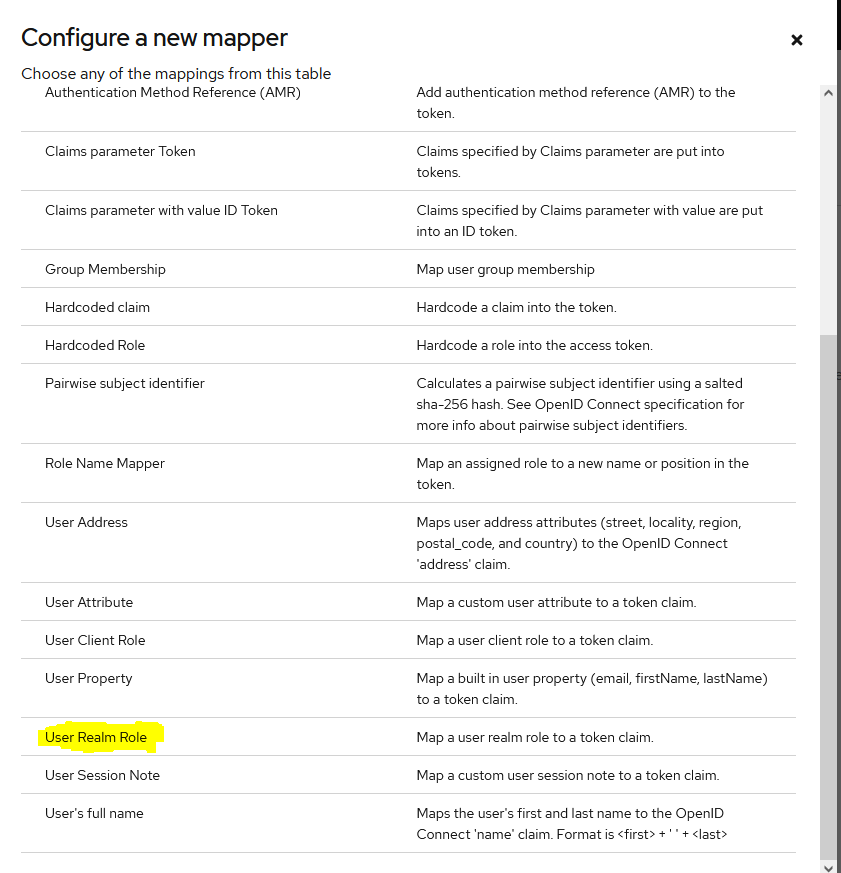
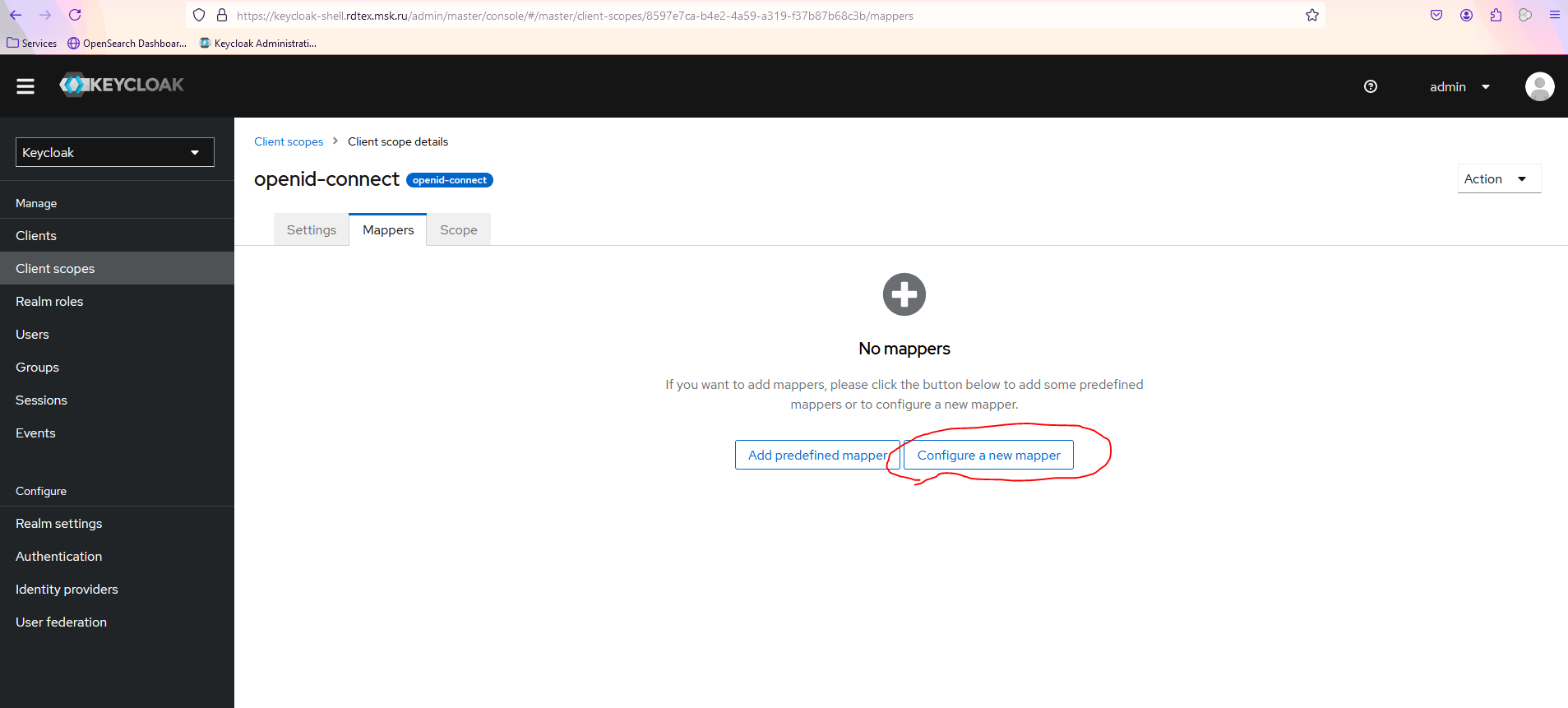
|  |
| --- |
| {    "clientId": "ead-webdav-client",    "name": "",    "description": "",    "rootUrl": "",    "adminUrl": "",    "baseUrl": "",    "surrogateAuthRequired": false,    "enabled": true,    "alwaysDisplayInConsole": false,    "clientAuthenticatorType": "client-secret",    "secret": "dPAhXM27beBplD4baHNTRpPp9dGp7lPG",    "redirectUris": [      "/\*"    ],    "webOrigins": [      "/\*"    ],    "notBefore": 0,    "bearerOnly": false,    "consentRequired": false,    "standardFlowEnabled": true,    "implicitFlowEnabled": false,    "directAccessGrantsEnabled": true,    "serviceAccountsEnabled": true,    "authorizationServicesEnabled": true,    "publicClient": false,    "frontchannelLogout": true,    "protocol": "openid-connect",    "attributes": {      "oidc.ciba.grant.enabled": "false",      "client.secret.creation.time": "1722604836",      "backchannel.logout.session.required": "true",      "oauth2.device.authorization.grant.enabled": "false",      "backchannel.logout.revoke.offline.tokens": "false"    },    "authenticationFlowBindingOverrides": {},    "fullScopeAllowed": true,    "nodeReRegistrationTimeout": -1,    "protocolMappers": [      {        "name": "Client IP Address",        "protocol": "openid-connect",        "protocolMapper": "oidc-usersessionmodel-note-mapper",        "consentRequired": false,        "config": {          "user.session.note": "clientAddress",          "id.token.claim": "true",          "introspection.token.claim": "true",          "access.token.claim": "true",          "claim.name": "clientAddress",          "jsonType.label": "String"        }      },      {        "name": "Client Host",        "protocol": "openid-connect",        "protocolMapper": "oidc-usersessionmodel-note-mapper",        "consentRequired": false,        "config": {          "user.session.note": "clientHost",          "id.token.claim": "true",          "introspection.token.claim": "true",          "access.token.claim": "true",          "claim.name": "clientHost",          "jsonType.label": "String"        }      },      {        "name": "Client ID",        "protocol": "openid-connect",        "protocolMapper": "oidc-usersessionmodel-note-mapper",        "consentRequired": false,        "config": {          "user.session.note": "client\_id",          "id.token.claim": "true",          "introspection.token.claim": "true",          "access.token.claim": "true",          "claim.name": "client\_id",          "jsonType.label": "String"        }      }    ],    "defaultClientScopes": [      "web-origins",      "acr",      "profile",      "roles",      "basic",      "openid-connect",      "email"    ],    "optionalClientScopes": [      "address",      "phone",      "offline\_access",      "microprofile-jwt"    ],    "access": {      "view": true,      "configure": true,      "manage": true    }  } |

Кроме того, необходимо создать Client Scope для opensearch\_cluster

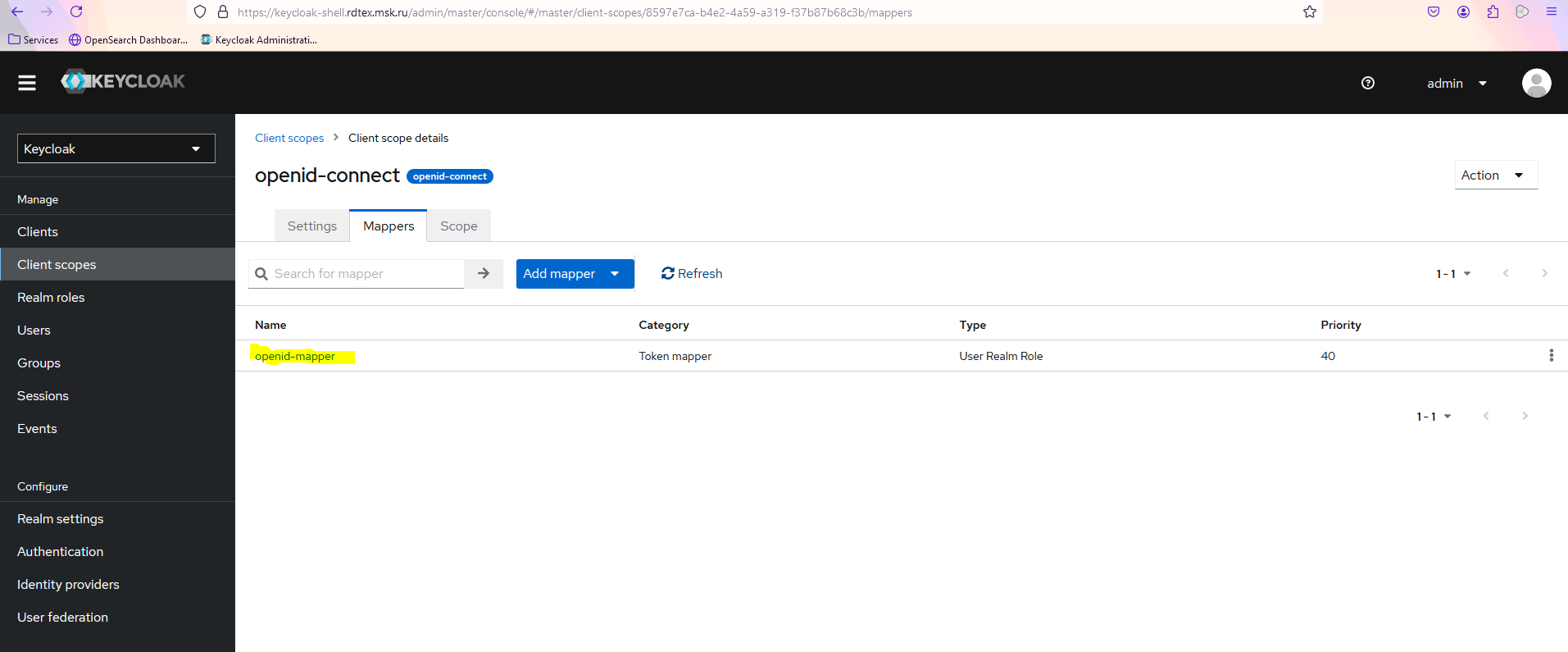
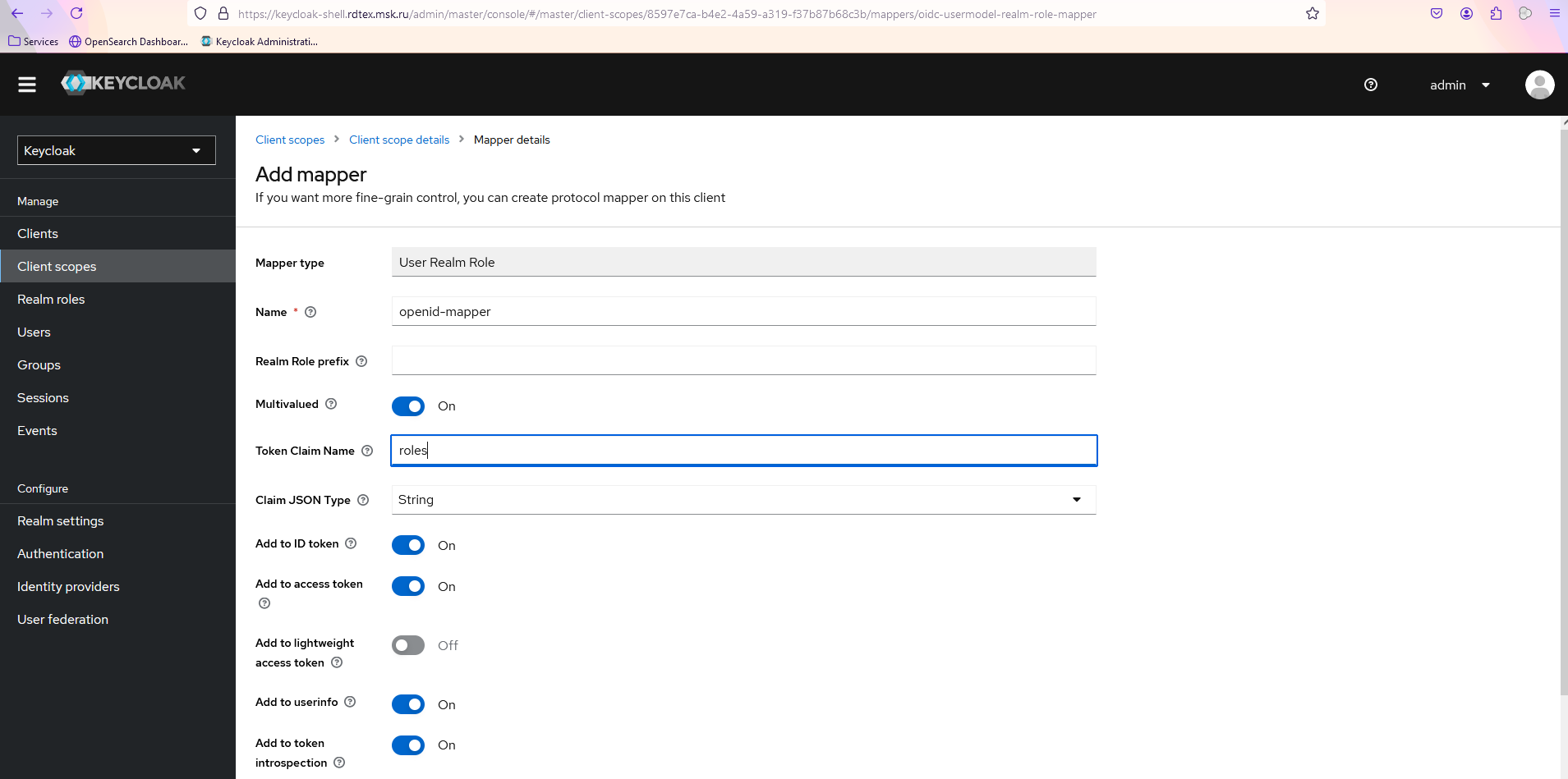
Creating Client Scope



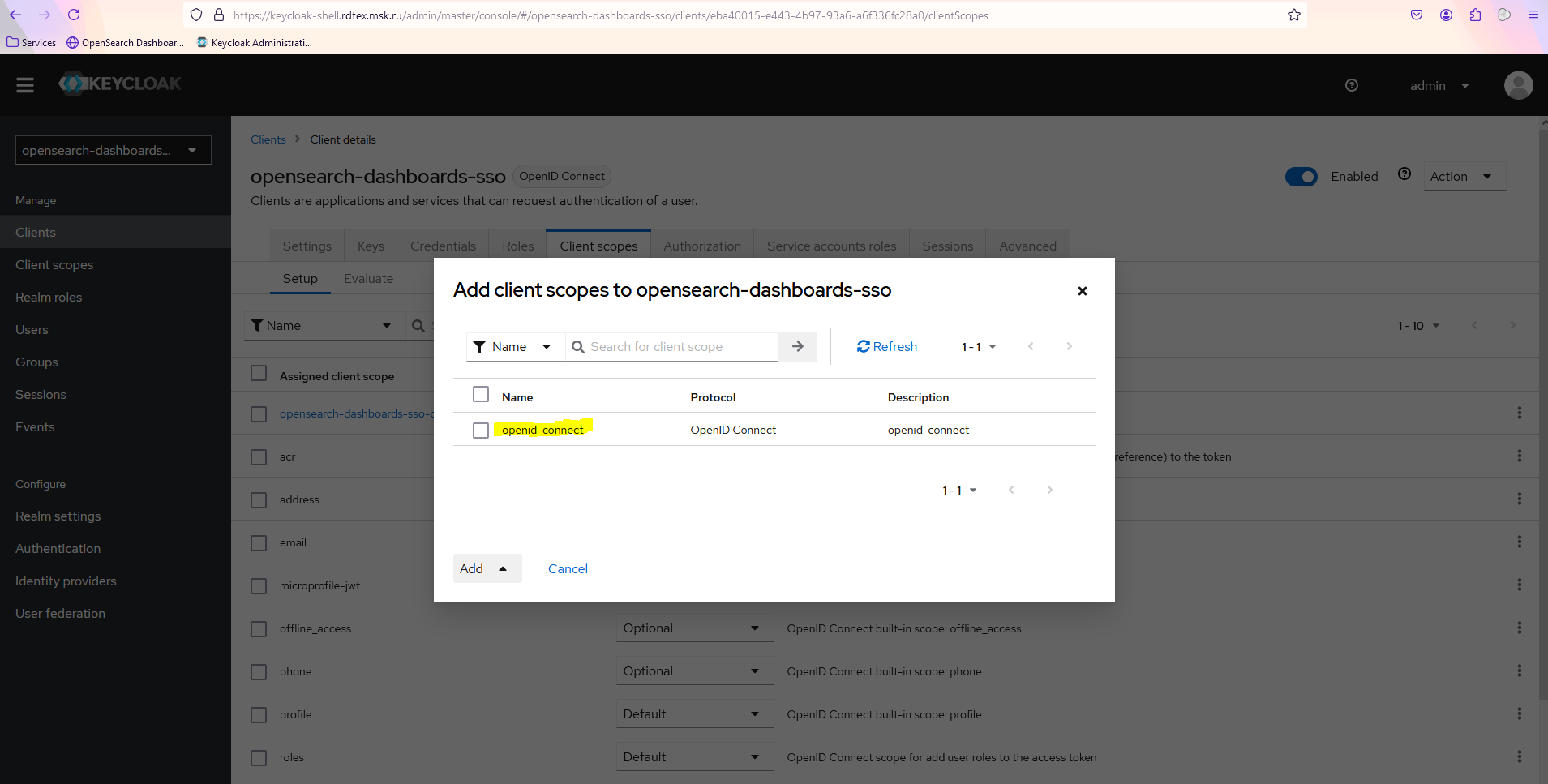
Configure Mappers for Client Scope



Mappers configuration:



4.3. Add Client Scope to Client



## **3.6. Метаданные**

Все метаданные хранятся в верхнеуровневом бакете MinIO (например, archive), где лежит файл metadata.json.

Доступ к метаданным можно получить либо через сам MinIO (консоль/CLI), либо через API.

Использование API:

Для загрузки (обновления) метаданных вызывается PUT /api/v1/meta-data. Метод принимает JSON (объект MetaData), после чего сервис сохраняет этот JSON-файл (metadata.json) в бакет archive.

Файл с метаданными:



## **3.7. Аудит, логирование**

В ecm-module-monolith: src/main/resources/logback-spring.xml

|  |
| --- |
| <?xml version="1.0" encoding="UTF-8"?>  <!DOCTYPE xml>  <configuration>  <include resource="org/springframework/boot/logging/logback/defaults.xml" />  <include resource="org/springframework/boot/logging/logback/console-appender.xml" />    <springProperty name="logstashDestination" source="logstash.destination" />    <appender name="OPEN\_TELEMETRY" class="io.opentelemetry.instrumentation.logback.appender.v1\_0.OpenTelemetryAppender">  <encoder class="ch.qos.logback.classic.encoder.JsonEncoder" />  </appender>    <springProfile name="prod">  <!-- AUDIT -->  <appender name="AUDIT" class="net.logstash.logback.appender.LogstashTcpSocketAppender">  <param name="Encoding" value="UTF-8"/>  <destination>${logstashDestination}</destination>  <encoder class="net.logstash.logback.encoder.LogstashEncoder">  <fieldNames>  <message>[ignore]</message>  </fieldNames>  </encoder>  <filter class="ch.qos.logback.core.filter.EvaluatorFilter">  <evaluator class="ch.qos.logback.classic.boolex.OnMarkerEvaluator">  <marker>AUDIT</marker>  </evaluator>  <onMatch>ACCEPT</onMatch>  <onMismatch>DENY</onMismatch>  </filter>  </appender>  <!-- AUDIT -->    <root level="INFO">  <appender-ref ref="CONSOLE" />  <appender-ref ref="OPEN\_TELEMETRY" />  <appender-ref ref="AUDIT" />  </root>  </springProfile>    <springProfile name="!prod">  <root level="INFO">  <appender-ref ref="CONSOLE" />  <appender-ref ref="OPEN\_TELEMETRY" />  </root>  </springProfile>  </configuration> |

Основной конфигурационный файл Logstash

/opt/logstash/config/pipelines.yml

|  |
| --- |
| - pipeline.id: pipeline\_1    path.config: "/usr/share/logstash/pipeline/pipeline\_1.conf"    pipeline.workers: **3**  - pipeline.id: pipeline\_2    path.config: "/usr/share/logstash/pipeline/pipeline\_2.conf"    pipeline.workers: **3** |

Описание pipelines

- pipeline\_1.conf

- pipeline\_2.conf

pipeline\_1.conf

|  |
| --- |
| input {      tcp {          port => "5001"          type => syslog          codec => json\_lines      }  }    output {     opensearch {       hosts => ["[https://shell-app.rdtex.msk.ru:9203](https://shell-app.rdtex.msk.ru:9203/)"]       index => "logstash-audit-data"       user => "admin"       password => "\*\*\*\*\*"       ssl => false       ssl\_certificate\_verification => false     }  } |

pipeline\_2.conf

|  |
| --- |
| input {      tcp {          port => "5015"          type => syslog          codec => json\_lines     }  }  output {     opensearch {       hosts => ["[https://shell-app.rdtex.msk.ru:9203](https://shell-app.rdtex.msk.ru:9203/)"]       index => "logstash-audit-data-test"       user => "admin"       password => "\*\*\*\*\*"       ssl => false       ssl\_certificate\_verification => false     }  } |

## **3.8. Конфигурационные файлы KeyCloak, MinIO, OpenSearch OpenSearch-Dashboards**

### **3.8.1. KeyCloak**

Конфигурация REALM EAD

realm-export.json



### **3.8.2. MinIO**

Конфигурационный файл MiniO

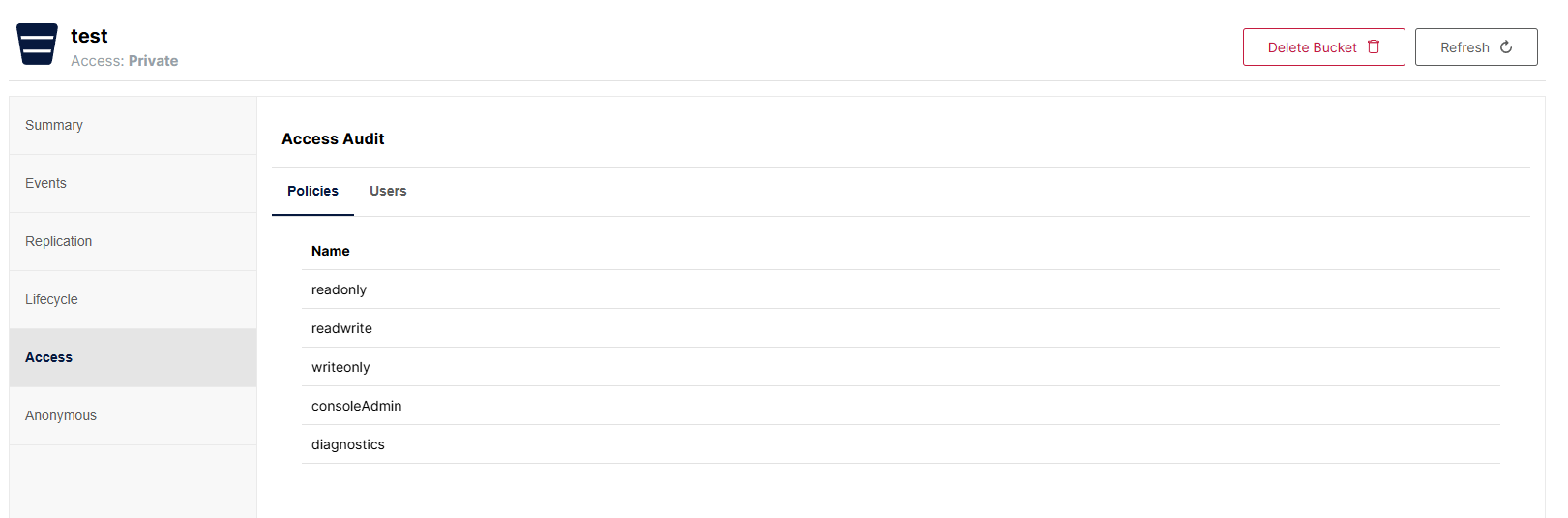
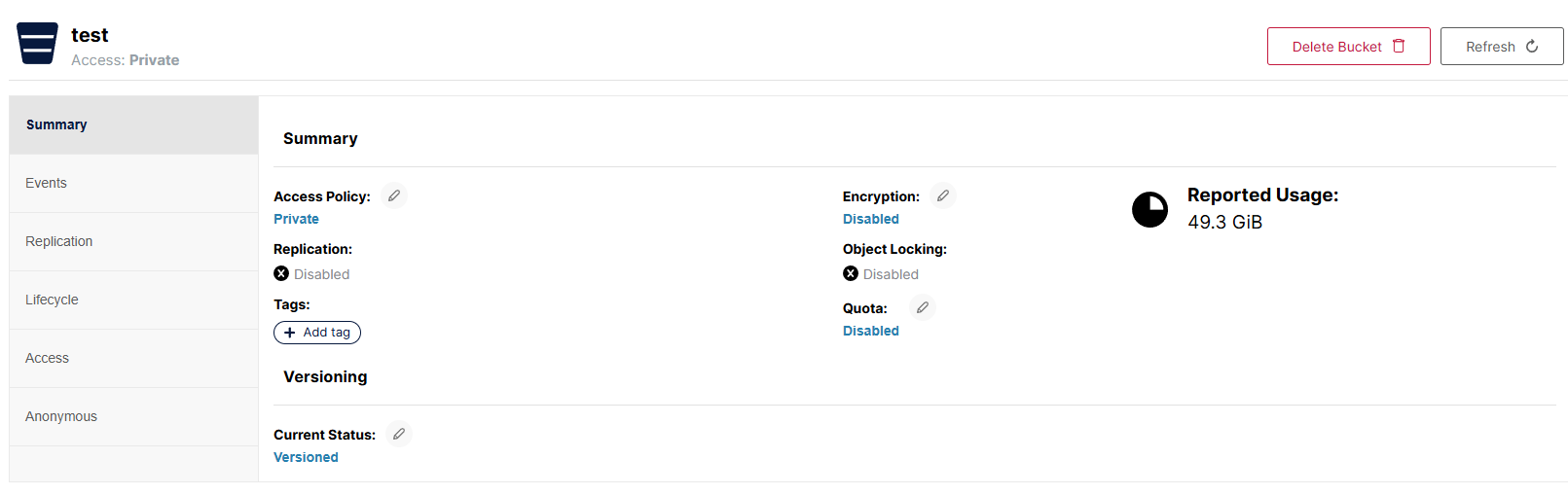
/etc/minio/minio.conf

|  |
| --- |
| #  # Ansible managed  #    # Minio local/remote volumes.  MINIO\_VOLUMES="[https://minio-0](https://minio-0/){1...5}.rdtex.msk.ru:9091/mnt/data/disk{1...4}"    # Minio cli options.  MINIO\_OPTS="--address :9091 --console-address :9092 --certs-dir /etc/minio/ssl"    # Access Key of the server.  MINIO\_ROOT\_USER="minioadmin"  # Secret key of the server.  MINIO\_ROOT\_PASSWORD="\*\*\*\*\*\*"    # Minio server region  MINIO\_SITE\_REGION="eu-west-1"    # Minio server URL  # MINIO\_SERVER\_URL="[https://minio-01.rdtex.msk.ru:9091](https://minio-01.rdtex.msk.ru:9091/)" |

/etc/systemd/system/minio.service

|  |
| --- |
| [Unit]  Description=MinIO  Documentation=https://docs.min.io  Wants=network-online.target  After=network-online.target  AssertFileIsExecutable=/usr/local/bin/minio    [Service]  WorkingDirectory=/usr/local/    User=minio  Group=minio  ProtectProc=invisible    EnvironmentFile=/etc/minio/minio.conf  ExecStartPre=/bin/bash -c "if [ -z \"${MINIO\_VOLUMES}\" ]; then echo \"Variable MINIO\_VOLUMES not set in /etc/minio/minio.conf\"; exit 1; fi"    ExecStart=/usr/local/bin/minio server $MINIO\_OPTS $MINIO\_VOLUMES    # Let systemd restart this service always  Restart=always    # Specifies the maximum file descriptor number that can be opened by this process  LimitNOFILE=65536    # Specifies the maximum number of threads this process can create  TasksMax=infinity    # Disable timeout logic and wait until process is stopped  TimeoutStopSec=infinity  SendSIGKILL=no      [Install]  WantedBy=multi-user.target |

Конфигурация MinIO bucket



### **3.8.3. OpenSearch, OpenSearch-Dashboards**

Конфигурация сервиса opensearch.service

|  |
| --- |
| [Unit]  Description=opensearch  Wants=network-online.target  After=network-online.target    [Service]  RuntimeDirectory=opensearch  PrivateTmp=true    WorkingDirectory=/usr/share/opensearch    User=opensearch  Group=opensearch    ExecStart=/usr/share/opensearch/bin/opensearch -p /usr/share/opensearch/opensearch.pid -q    StandardOutput=journal  StandardError=inherit    # Specifies the maximum file descriptor number that can be opened by this process  LimitNOFILE=65536    # Specifies the memory lock settings  LimitMEMLOCK=infinity    # Specifies the maximum number of processes  LimitNPROC=4096    # Specifies the maximum size of virtual memory  LimitAS=infinity    # Specifies the maximum file size  LimitFSIZE=infinity    # Disable timeout logic and wait until process is stopped  TimeoutStopSec=0    # SIGTERM signal is used to stop the Java process  KillSignal=SIGTERM    # Send the signal only to the JVM rather than its control group  KillMode=process    # Java process is never killed  SendSIGKILL=no    # When a JVM receives a SIGTERM signal it exits with code 143  SuccessExitStatus=143    [Install]  WantedBy=multi-user.target |

Основная конфигурация OpenSearch

/usr/share/opensearch/config/opensearch.yml

|  |
| --- |
| # ======================== OpenSearch Configuration =========================  #  # NOTE: OpenSearch comes with reasonable defaults for most settings.  # Before you set out to tweak and tune the configuration, make sure you  # understand what are you trying to accomplish and the consequences.  #  # The primary way of configuring a node is via this file. This template lists  # the most important settings you may want to configure for a production cluster.  #  # Please consult the documentation for further information on configuration options:  # https://www.opensearch.org  #  # ---------------------------------- Cluster -----------------------------------  #  # Use a descriptive name for your cluster:  #  #cluster.name: my-application  #  # ------------------------------------ Node ------------------------------------  #  # Use a descriptive name for the node:  #  #node.name: node-1  #  # Add custom attributes to the node:  #  #node.attr.rack: r1  #  # ----------------------------------- Paths ------------------------------------  #  # Path to directory where to store the data (separate multiple locations by comma):  #  #path.data: /path/to/data  #  # Path to log files:  #  #path.logs: /path/to/logs  #  # ----------------------------------- Memory -----------------------------------  #  # Lock the memory on startup:  #  #bootstrap.memory\_lock: true  #  # Make sure that the heap size is set to about half the memory available  # on the system and that the owner of the process is allowed to use this  # limit.  #  # OpenSearch performs poorly when the system is swapping the memory.  #  # ---------------------------------- Network -----------------------------------  #  # Set the bind address to a specific IP (IPv4 or IPv6):  #  #network.host: 192.168.0.1  #  # Set a custom port for HTTP:  #  #http.port: 9200  #  # For more information, consult the network module documentation.  #  # --------------------------------- Discovery ----------------------------------  #  # Pass an initial list of hosts to perform discovery when this node is started:  # The default list of hosts is ["127.0.0.1", "[::1]"]  #  #discovery.seed\_hosts: ["host1", "host2"]  #  # Bootstrap the cluster using an initial set of cluster-manager-eligible nodes:  #  #cluster.initial\_cluster\_manager\_nodes: ["node-1", "node-2"]  #  # For more information, consult the discovery and cluster formation module documentation.  #  # ---------------------------------- Gateway -----------------------------------  #  # Block initial recovery after a full cluster restart until N nodes are started:  #  #gateway.recover\_after\_nodes: 3  #  # For more information, consult the gateway module documentation.  #  # ---------------------------------- Various -----------------------------------  #  # Require explicit names when deleting indices:  #  #action.destructive\_requires\_name: true  #  # ---------------------------------- Remote Store -----------------------------------  # Controls whether cluster imposes index creation only with remote store enabled  # cluster.remote\_store.enabled: true  #  # Repository to use for segment upload while enforcing remote store for an index  # node.attr.remote\_store.segment.repository: my-repo-1  #  # Repository to use for translog upload while enforcing remote store for an index  # node.attr.remote\_store.translog.repository: my-repo-1  #  # ---------------------------------- Experimental Features -----------------------------------  # Gates the visibility of the experimental segment replication features until they are production ready.  #  #opensearch.experimental.feature.segment\_replication\_experimental.enabled: false  #  # Gates the functionality of a new parameter to the snapshot restore API  # that allows for creation of a new index type that searches a snapshot  # directly in a remote repository without restoring all index data to disk  # ahead of time.  #  #opensearch.experimental.feature.searchable\_snapshot.enabled: false  #  #  # Gates the functionality of enabling extensions to work with OpenSearch.  # This feature enables applications to extend features of OpenSearch outside of  # the core.  #  #opensearch.experimental.feature.extensions.enabled: false  #  #  # Gates the optimization of datetime formatters caching along with change in default datetime formatter  # Once there is no observed impact on performance, this feature flag can be removed.  #  #opensearch.experimental.optimization.datetime\_formatter\_caching.enabled: false  #  # Gates the functionality of enabling Opensearch to use pluggable caches with respective store names via setting.  #  #opensearch.experimental.feature.pluggable.caching.enabled: false  ## BEGIN opensearch main configuration ##  cluster.name: "development-cluster"    node.name: "os-01"  network.host: "192.168.28.127"  http.port: 9200  bootstrap.memory\_lock: true  discovery.seed\_hosts: ["os-01","os-02","os-03","os-04","os-05"]    node.roles: [data,master,ingest]  ## END opensearch main configuration ##  ## BEGIN OpenSearch Security common configuration ##    plugins.security.allow\_default\_init\_securityindex: true  plugins.security.audit.type: internal\_opensearch  plugins.security.enable\_snapshot\_restore\_privilege: true  plugins.security.check\_snapshot\_restore\_write\_privileges: true  plugins.security.restapi.roles\_enabled: ["all\_access", "security\_rest\_api\_access"]  ## END OpenSearch Security common configuration ##  ## BEGIN opensearch Security Node & Admin certificates configuration ##  # This is a configuration snippet for the node os-01  # This snippet needs to be inserted into the file config/elasticsearch.yml of the respective node.  # If the config file already contains SearchGuard configuration, this needs to be replaced.  # Furthermore, you need to copy the files referenced below into the same directory.  # Please refer to http://docs.search-guard.com/latest/configuring-tls for further configuration of your installation.    plugins.security.ssl.transport.pemcert\_filepath: os-01.pem  plugins.security.ssl.transport.pemkey\_filepath: os-01.key  plugins.security.ssl.transport.pemtrustedcas\_filepath: root-ca.pem  plugins.security.ssl.transport.enforce\_hostname\_verification: false  plugins.security.ssl.transport.resolve\_hostname: false  plugins.security.ssl.http.enabled: true  plugins.security.ssl.http.pemcert\_filepath: os-01\_http.pem  plugins.security.ssl.http.pemkey\_filepath: os-01\_http.key  plugins.security.ssl.http.pemtrustedcas\_filepath: root-ca.pem  plugins.security.nodes\_dn:  - CN=os-01.rdtex.msk.ru,OU=Ops,O=rdtex.msk.ru\, Inc.,DC=rdtex.msk.ru  - CN=os-02.rdtex.msk.ru,OU=Ops,O=rdtex.msk.ru\, Inc.,DC=rdtex.msk.ru  - CN=os-03.rdtex.msk.ru,OU=Ops,O=rdtex.msk.ru\, Inc.,DC=rdtex.msk.ru  - CN=os-04.rdtex.msk.ru,OU=Ops,O=rdtex.msk.ru\, Inc.,DC=rdtex.msk.ru  - CN=os-05.rdtex.msk.ru,OU=Ops,O=rdtex.msk.ru\, Inc.,DC=rdtex.msk.ru  plugins.security.authcz.admin\_dn:  - CN=admin.rdtex.msk.ru,OU=Ops,O=rdtex.msk.ru\, Inc.,DC=rdtex.msk.ru  ## END opensearch Security Node & Admin certificates configuration ##  opensearch.experimental.feature.telemetry.enabled: true  telemetry.feature.metrics.enabled: true |

/usr/share/opensearch/config/opensearch-security/config.yaml

|  |
| --- |
| ---    # This is the main OpenSearch Security configuration file where authentication  # and authorization is defined.  #  # You need to configure at least one authentication domain in the authc of this file.  # An authentication domain is responsible for extracting the user credentials from  # the request and for validating them against an authentication backend like Active Directory for example.  #  # If more than one authentication domain is configured the first one which succeeds wins.  # If all authentication domains fail then the request is unauthenticated.  # In this case an exception is thrown and/or the HTTP status is set to 401.  #  # After authentication authorization (authz) will be applied. There can be zero or more authorizers which collect  # the roles from a given backend for the authenticated user.  #  # Both, authc and auth can be enabled/disabled separately for REST and TRANSPORT layer. Default is true for both.  # http\_enabled: true  # transport\_enabled: true  #  # For HTTP it is possible to allow anonymous authentication. If that is the case then the HTTP authenticators try to  # find user credentials in the HTTP request. If credentials are found then the user gets regularly authenticated.  # If none can be found the user will be authenticated as an "anonymous" user. This user has always the username "anonymous"  # and one role named "anonymous\_backendrole".  # If you enable anonymous authentication all HTTP authenticators will not challenge.  #  #  # Note: If you define more than one HTTP authenticators make sure to put non-challenging authenticators like "proxy" or "clientcert"  # first and the challenging one last.  # Because it's not possible to challenge a client with two different authentication methods (for example  # Kerberos and Basic) only one can have the challenge flag set to true. You can cope with this situation  # by using pre-authentication, e.g. sending a HTTP Basic authentication header in the request.  #  # Default value of the challenge flag is true.  #  #  # HTTP  # basic (challenging)  # proxy (not challenging, needs xff)  # kerberos (challenging)  # clientcert (not challenging, needs https)  # jwt (not challenging)  # host (not challenging) #DEPRECATED, will be removed in a future version.  # host based authentication is configurable in roles\_mapping    # Authc  # internal  # noop  # ldap    # Authz  # ldap  # noop        \_meta:  type: "config"  config\_version: 2    config:  dynamic:  # Set filtered\_alias\_mode to 'disallow' to forbid more than 2 filtered aliases per index  # Set filtered\_alias\_mode to 'warn' to allow more than 2 filtered aliases per index but warns about it (default)  # Set filtered\_alias\_mode to 'nowarn' to allow more than 2 filtered aliases per index silently  #filtered\_alias\_mode: warn  #do\_not\_fail\_on\_forbidden: false  #kibana:  # Kibana multitenancy  #multitenancy\_enabled: true  #server\_username: kibanaserver  #index: '.kibana'  # OpenID settings  http:  anonymous\_auth\_enabled: false  xff:  enabled: false  internalProxies: ".\*"  remoteIpHeader: "x-forwarded-for"  authc:  # In order for Dashboards to access OpenSearch, you must first use  # authentication\_backend.type: internal  basic\_internal\_auth\_domain:  description: "Authenticate via HTTP Basic against internal users database"  http\_enabled: true  transport\_enabled: false  order: 0  http\_authenticator:  type: basic  challenge: false  authentication\_backend:  type: internal  openid\_auth\_domain:  description: "Authenticate via OpenID"  http\_enabled: true  transport\_enabled: true  order: 1  http\_authenticator:  type: openid  challenge: false  config:  openid\_connect\_idp:  enable\_ssl: true  verify\_hostnames: false  pemtrustedcas\_filepath: /usr/share/opensearch/config/oidc\_ca.pem  verify\_hostnames: false  subject\_key: preferred\_username  roles\_key: roles  openid\_connect\_url: https://keycloak.rdtex.msk.ru:8444/realms/ead/.well-known/openid-configuration  kibana\_url: https://os-01.rdtex.msk.ru:5601  authentication\_backend:  type: noop  authz: {} |

Конфигурация сервиса dashboards.service

|  |
| --- |
| [Unit]  Description=opensearch-dashboards  Wants=network-online.target  After=network-online.target    [Service]  RuntimeDirectory=opensearch-dashboards  PrivateTmp=true    WorkingDirectory=/usr/share/opensearch-dashboards    User=kibana  Group=kibana    ExecStart=/usr/share/opensearch-dashboards/bin/opensearch-dashboards -q    StandardOutput=journal  StandardError=inherit    # Specifies the maximum file descriptor number that can be opened by this process  LimitNOFILE=65536    # Specifies the maximum number of processes  LimitNPROC=4096    # Specifies the maximum size of virtual memory  LimitAS=infinity    # Specifies the maximum file size  LimitFSIZE=infinity    # Disable timeout logic and wait until process is stopped  TimeoutStopSec=0    # SIGTERM signal is used to stop the Java process  KillSignal=SIGTERM    # Send the signal only to the JVM rather than its control group  KillMode=process    # Java process is never killed  SendSIGKILL=no    # When a JVM receives a SIGTERM signal it exits with code 143  SuccessExitStatus=143    [Install]  WantedBy=multi-user.target |

Основная конфигурация OpenSearch Dashboards

/usr/share/opensearch-dashboards/config/opensearch\_dashboards.yml

|  |
| --- |
| server.port: **5601**  server.name: os\_dashboards  server.host: "0.0.0.0"  opensearch.hosts: ["[https://os-01.rdtex.msk.ru:9200](https://os-01.rdtex.msk.ru:9200/)","[https://os-02.rdtex.msk.ru:9200](https://os-02.rdtex.msk.ru:9200/)","[https://os-03.rdtex.msk.ru:9200](https://os-03.rdtex.msk.ru:9200/)","[https://os-04.rdtex.msk.ru:9200](https://os-04.rdtex.msk.ru:9200/)","[https://os-05.rdtex.msk.ru:9200](https://os-05.rdtex.msk.ru:9200/)"]  opensearch.ssl.verificationMode: none  opensearch.username: "kibanaserver"  opensearch.password: "\*\*\*\*\*\*\*\*\*\*\*\*"      # Encrypt traffic between the browser and OpenSearch-Dashboards  server.ssl.enabled: true  server.ssl.certificate: "/usr/share/opensearch-dashboards/config/certificates/os-dashboards/os-dashboards.pem"  server.ssl.key: "/usr/share/opensearch-dashboards/config/certificates/os-dashboards/os-dashboards.key"    # Encrypt traffic between OpenSearch-Dashboards and Opensearch  opensearch.ssl.certificateAuthorities: ["/usr/share/opensearch-dashboards/config/certificates/ca/root-ca.pem"]    opensearch\_security.multitenancy.enabled: true  opensearch\_security.multitenancy.tenants.preferred: ["Private", "Global"]  opensearch\_security.readonly\_mode.roles: ["kibana\_read\_only"]  # Enable OpenID authentication  opensearch\_security.auth.type: ["basicauth","openid"]  opensearch\_security.auth.multiple\_auth\_enabled: true    # The IdP metadata endpoint  opensearch\_security.openid.connect\_url: "<https://keycloak.rdtex.msk.ru/realms/ead/.well-known/openid-configuration>"  # The ID of the OpenID Connect client in your IdP  opensearch\_security.openid.client\_id: "opensearch\_cluster"  # The client secret of the OpenID Connect client  opensearch\_security.openid.client\_secret: "\*\*\*\*\*\*\*\*\*\*\*"    # mTLS Options for obtaining endpoints from IdP  opensearch\_security.openid.root\_ca: "/usr/share/opensearch-dashboards/config/certificates/ca/rdtex\_ca.pem"  opensearch\_security.openid.base\_redirect\_url: https://os-01.rdtex.msk.ru:5601  opensearch\_security.openid.verify\_hostnames: "false"    # The maximum payload size in bytes for incoming server requests.  server.maxPayloadBytes: **104857600** |

## **3.9. Конфигурации системы ЭА**



Приведенные конфигурации рекомендуемые, система не ограничивается данным набором.

Средний размер файла 5 Mb.

# **4. Описание действий в системе**

## **4.1. Вход в систему и доступ к административному функционалу**

Для работы с системой необходимо выполнить вход под учетной записью с правами Администратора.

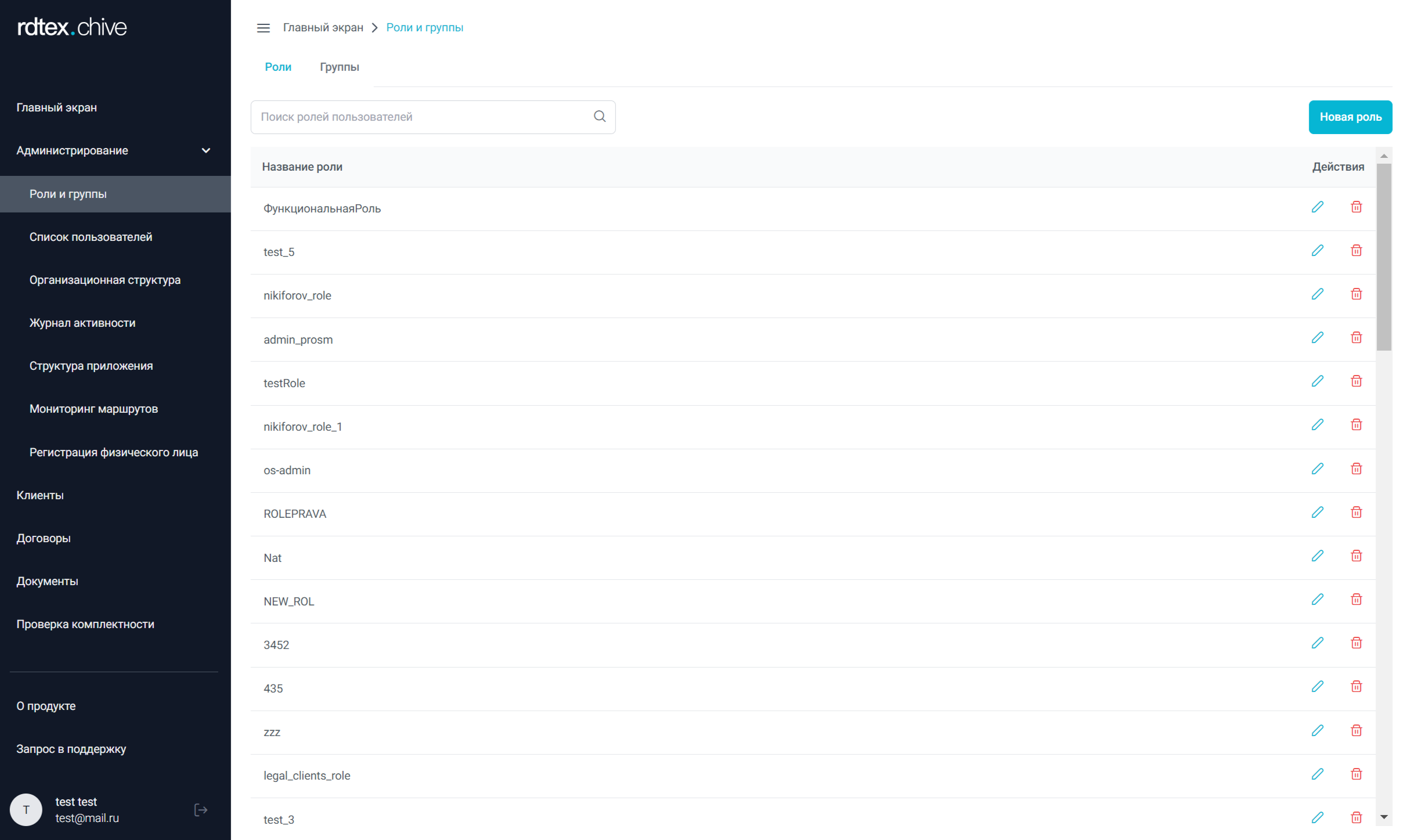
Все функции управления системой доступны во вкладке "Администрирование", доступ к которой ограничен ролевой моделью. Количество функций зависит от уровня доступа, но они всегда находятся в этом разделе, даже если он содержит лишь один пункт. Навигация осуществляется через раскрытие подпунктов меню.

## **4.2. Управление ролями и группами**

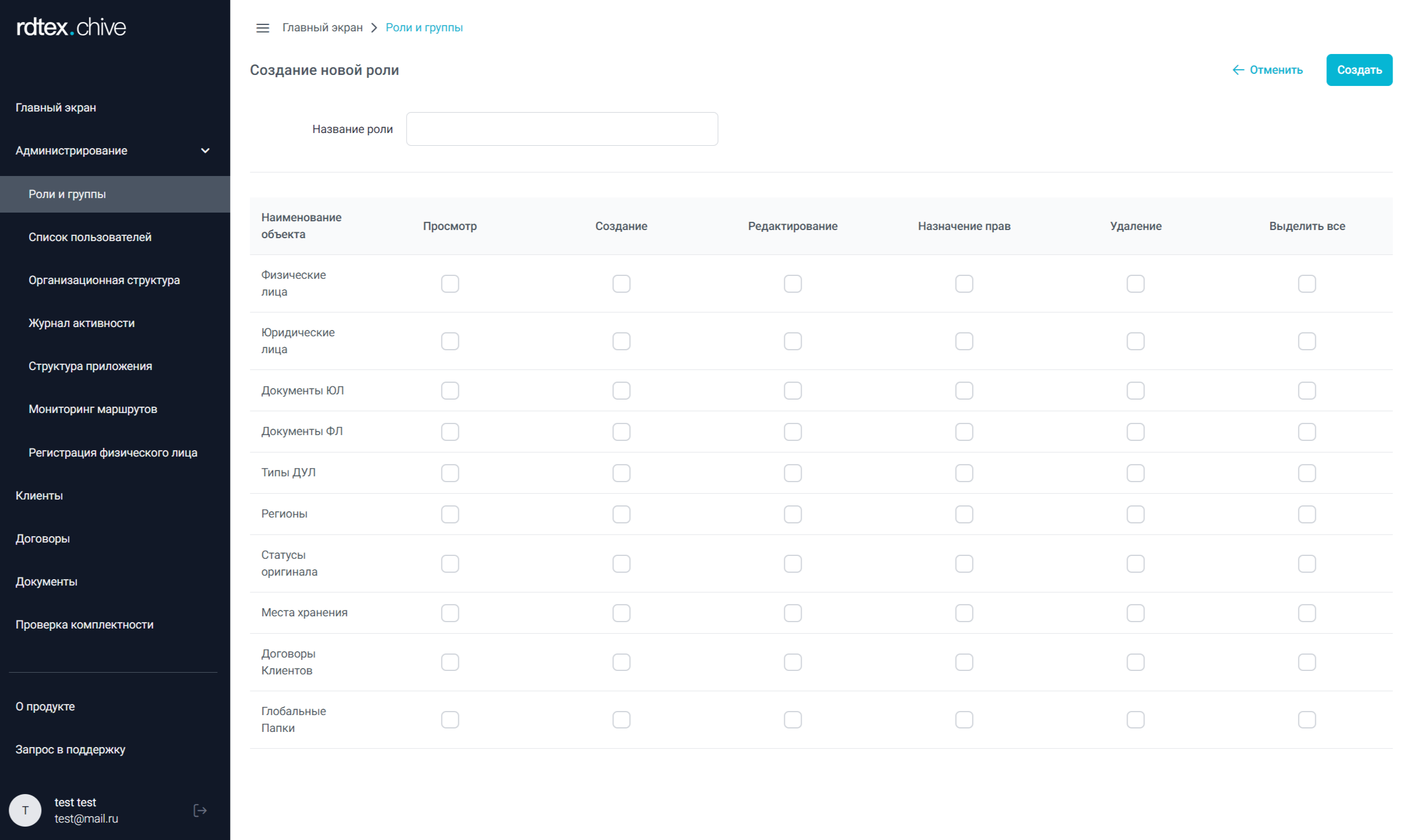
Навигация: Администрирование -> Роли и группы

Раздел "Управление ролями и группами" предназначен для настройки прав доступа и организации пользователей в системе электронного архива. Здесь вы можете создавать, редактировать, удалять роли и группы, а также управлять назначением ролей пользователям.

В разделе ролей отображается список всех доступных ролей в системе. Для каждой роли указывается её название, а также доступны действия "Редактировать" и "Удалить". Чтобы создать новую роль, нужно нажать на кнопку "Новая роль", ввести её название и настроить права доступа с помощью матрицы. После заполнения всех полей нужно нажать "Создать". Если всё введено корректно, система уведомит об успешном создании. Для редактирования роли достаточно выбрать нужную роль из списка, изменить её параметры и сохранить изменения. Удаление роли происходит через подтверждение действия в модальном окне.



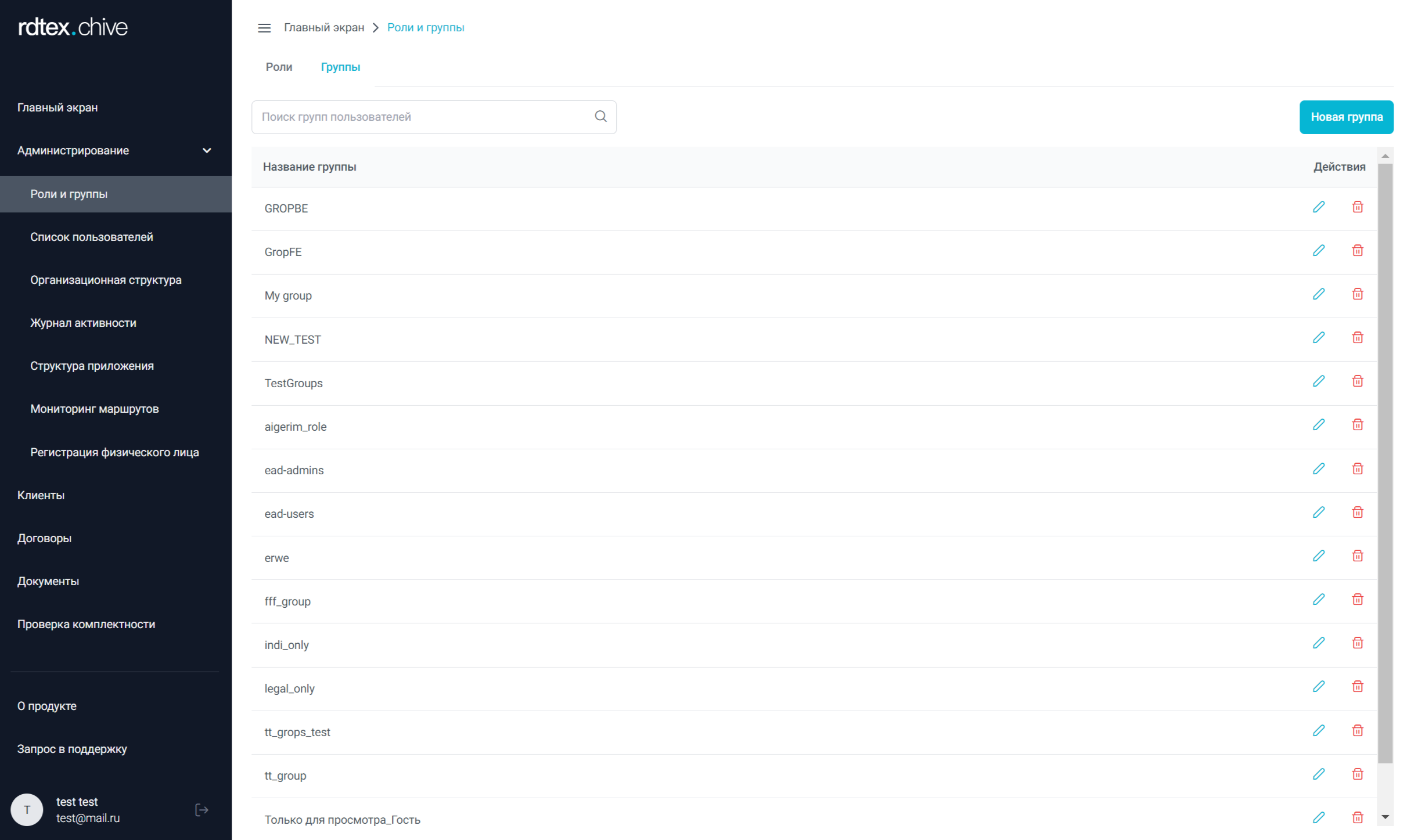
**Рисунок 1. Страница ролей**



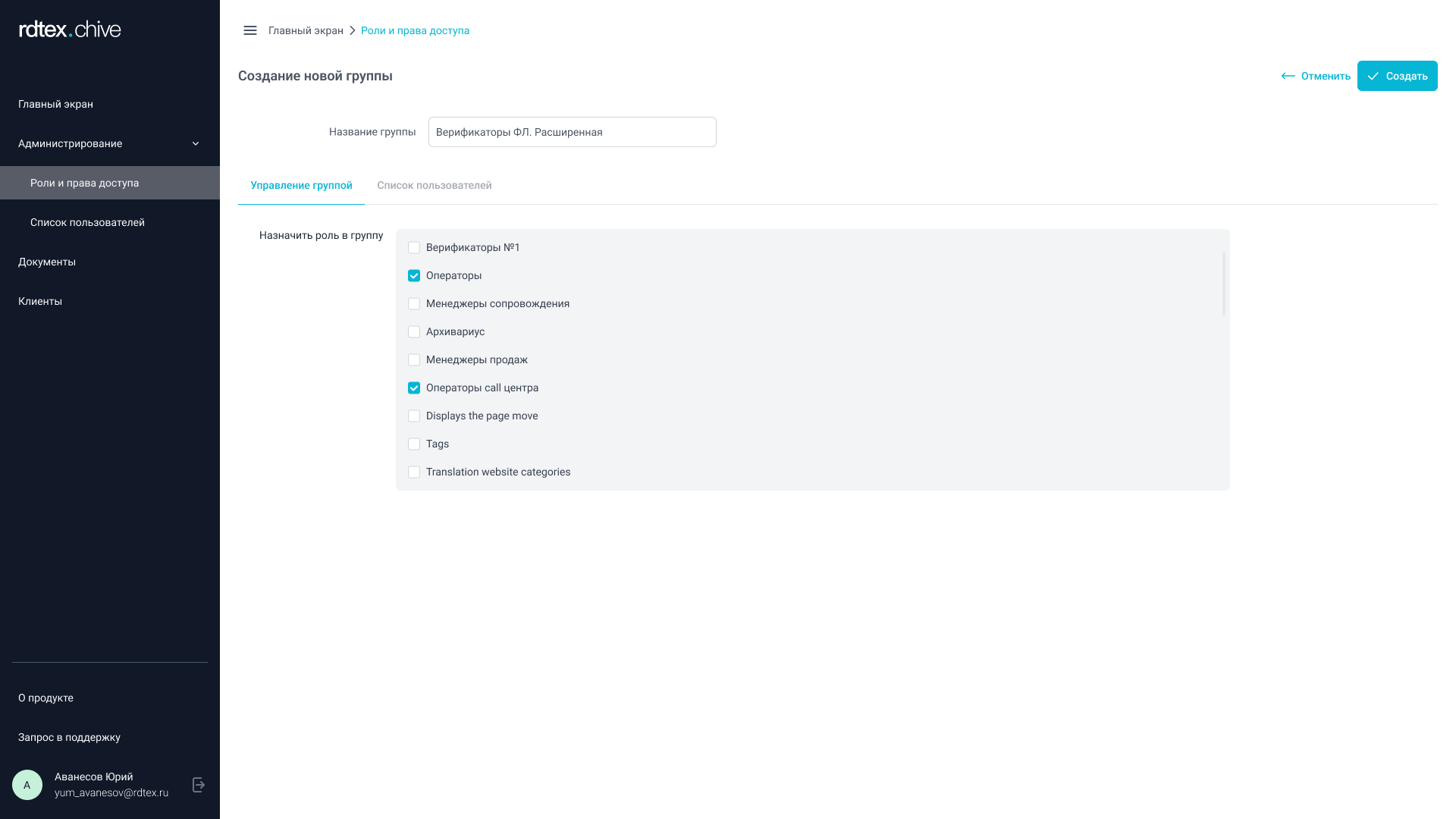
**Рисунок 2. Добавление ролей**

Навигация: Администрирование -> Роли и группы -> Группы

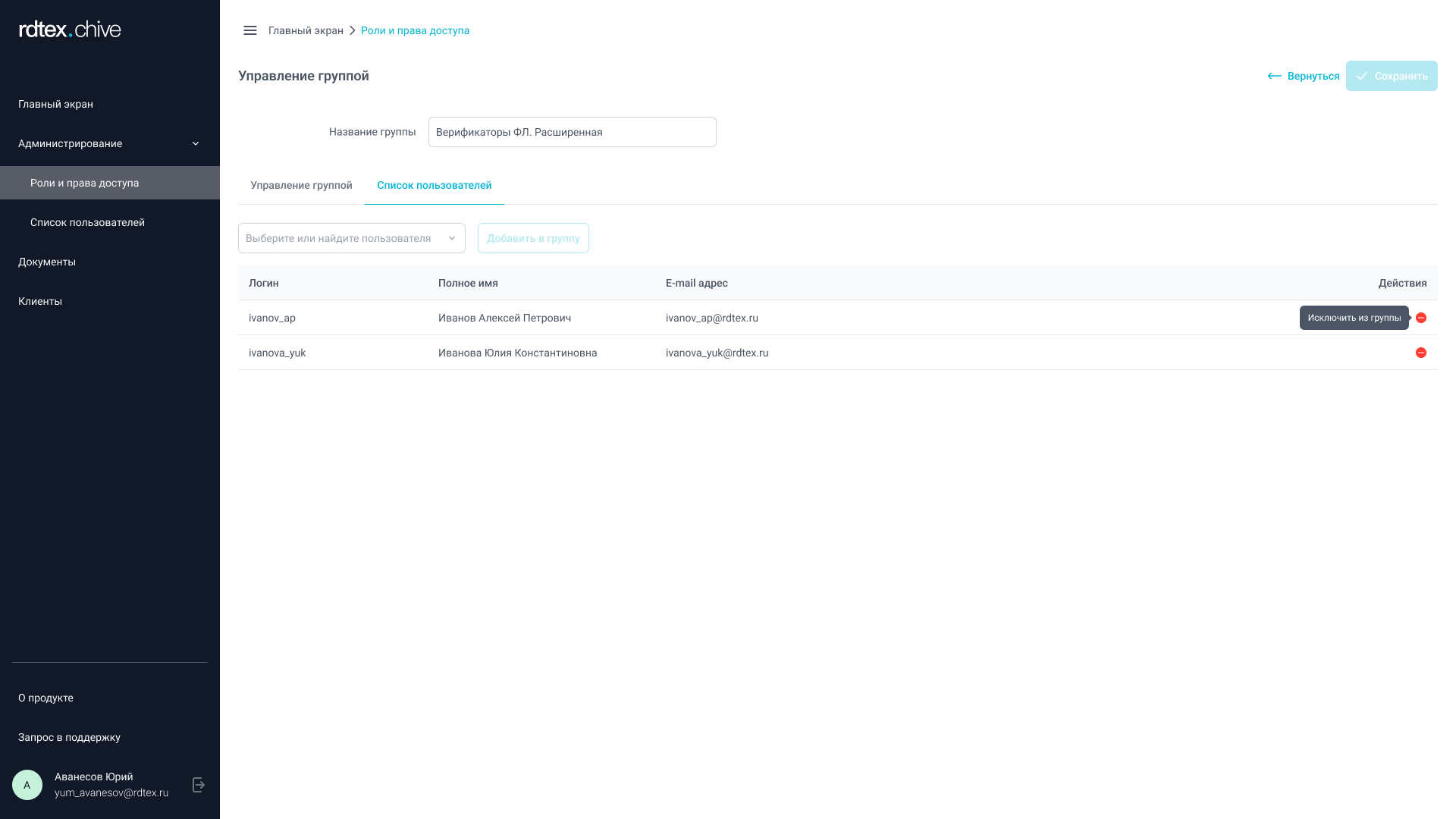
В разделе групп можно просматривать список групп ролей, создавать новые группы, редактировать или удалять их. Чтобы создать новую группу, нужно нажать на кнопку "Новая группа". При создании новой группы нужно указать её название, выбрать роли из предложенного списка. После завершения настройки группы нужно сохранить изменения. Редактирование существующей группы позволяет обновить её название, состав ролей или добавить/удалить пользователей, для этого доступны инструменты поиска и добавления пользователей во вкладке "Список пользователей" при управлении группой. Удаление группы также требует подтверждения действия через модальное окно.



**Рисунок 3. Страница групп**



**Рисунок 4. Добавление групп**



**Рисунок 5. Добавление пользователей в группу**

Для всех действий система выполняет проверку корректности введённых данных. Названия ролей и групп должны быть уникальными и обязательны для заполнения. При успешном выполнении операции пользователю показывается соответствующее уведомление, а в случае ошибок — пояснение, что именно нужно исправить.

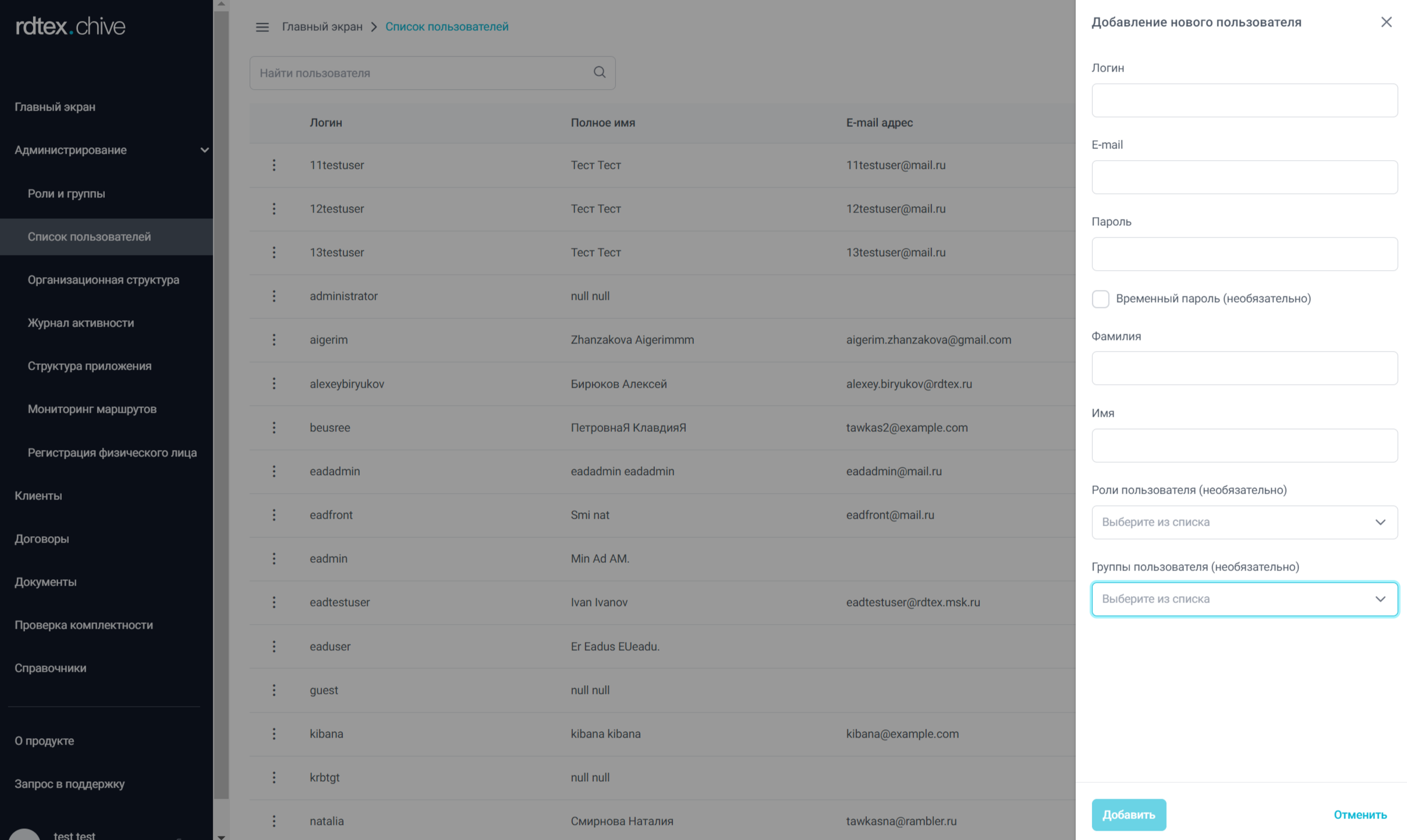
## **4.3. Работа со списком пользователей**

Навигация: Меню -> Администрирование -> Список пользователей.

Список пользователей позволяет управлять учетными записями. На странице отображается таблица с логином, полным именем, email и статусом блокировки (да/нет).

В верхнем правом углу расположена кнопка «Добавить пользователя», которая открывает форму для создания новой учетной записи. В форме необходимо указать логин, email, пароль, фамилию, имя и выбрать группу пользователя, а также можно назначить роли.

В таблице есть кнопки для действий с пользователями. Кнопка «Редактировать» открывает форму для изменения данных. Кнопка «Удалить» позволяет удалить выбранных пользователей. Кнопка «Заблокировать» включает или отключает доступ к системе. Перед выполнением удаления или блокировки появляется окно подтверждения. Все изменения сопровождаются уведомлениями об успехе или ошибках.



**Рисунок 6. Страница Списка пользователей**

## **4.4. Управление организационной структурой**

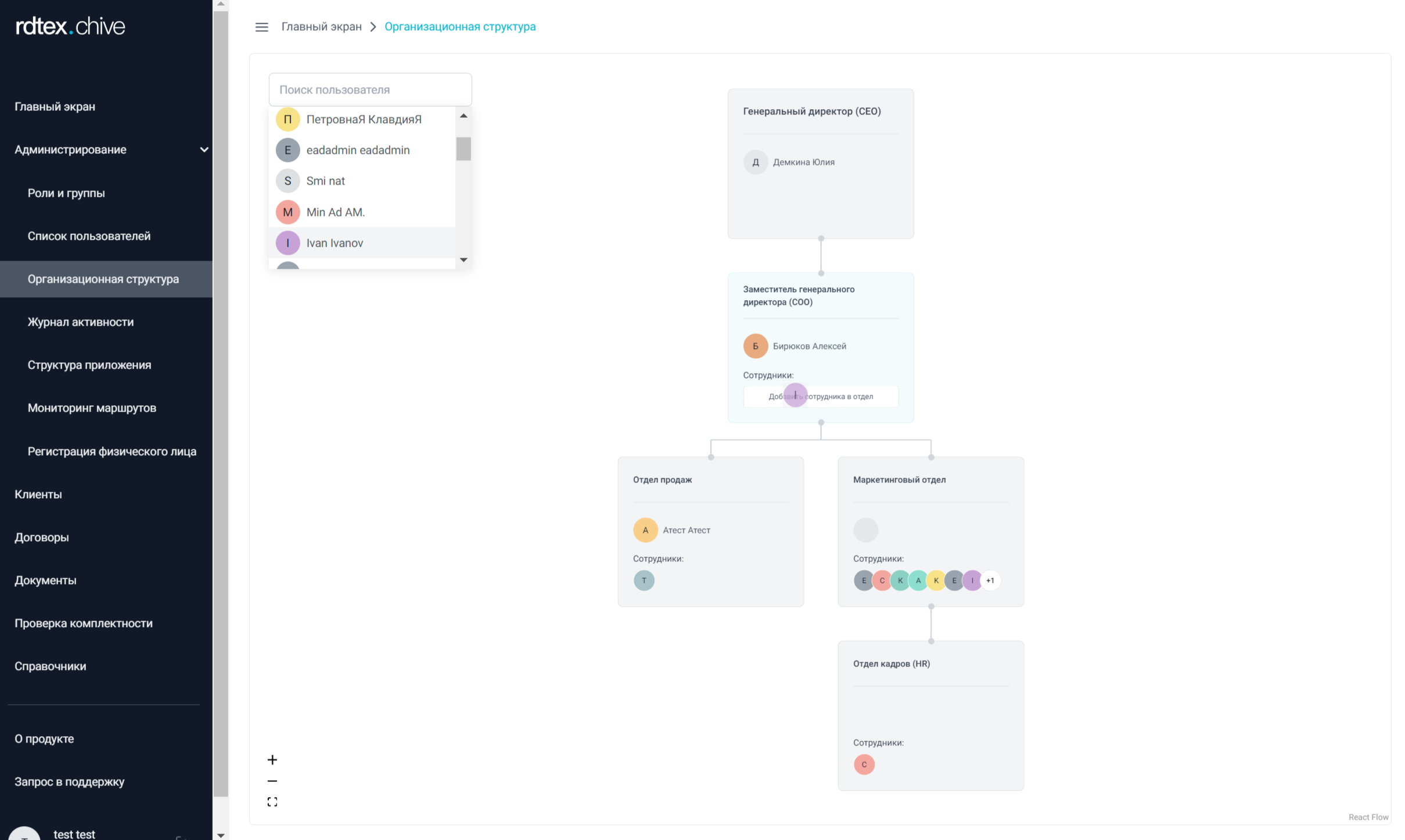
Навигация: Меню -> Администрирование -> Организационная структура.

Администратор может создавать организации и их отделы, назначать сотрудников и руководителей, а также редактировать, перемещать и удалять элементы структуры. Вся информация о структуре доступна через интерфейс, где можно легко добавлять новые отделы, изменять их название (нажатием на него) и назначать руководителей.

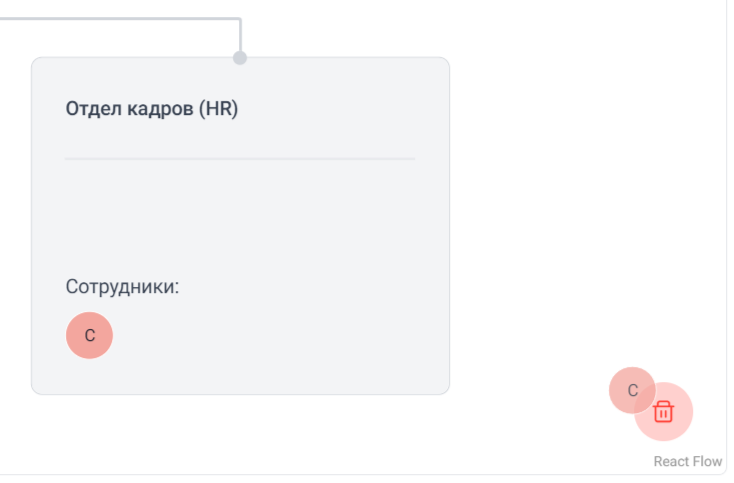
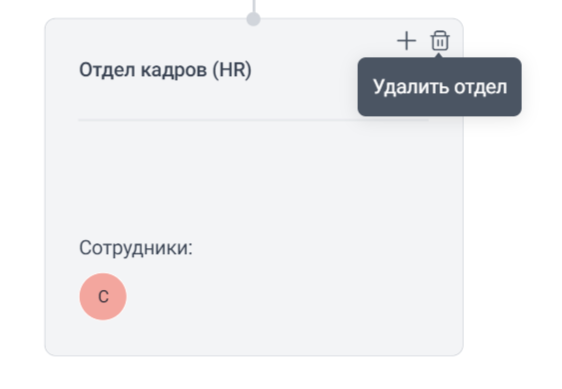
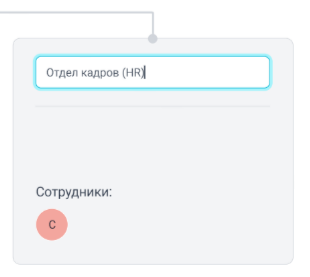
Сотрудников можно легко добавлять в отделы с помощью зажатия левой кнопки мыши и перетаскивания. Для этого достаточно выбрать сотрудника и перетащить его в нужный отдел. Для назначения руководителя, сотрудника нужно перетащить в верхнюю часть отдела. Также можно использовать поиск для нахождения сотрудников, как в рамках конкретного отдела (если сотрудников больше 7 человек), так и по всей организационной структуре. Для этого в верхней левой части экрана предусмотрена строка поиска, которая позволяет быстро находить сотрудников по имени.

Отделы могут быть добавлены или удалены с помощью кнопок в правом верхнем углу отдела. Также удалять отдел или сотрудника можно перенеся его в нижнюю правую часть экрана. В случае необходимости, отдел можно переместить, и все его подчиненные сотрудники останутся в структуре.

Помимо кнопок в левом нижнем углу, управлять масштабом можно колёсиком мыши, а для перемещения всей организационной структуры – зажатием правой кнопки мыши.



**Рисунок 7. Страница Организационной структуры.**



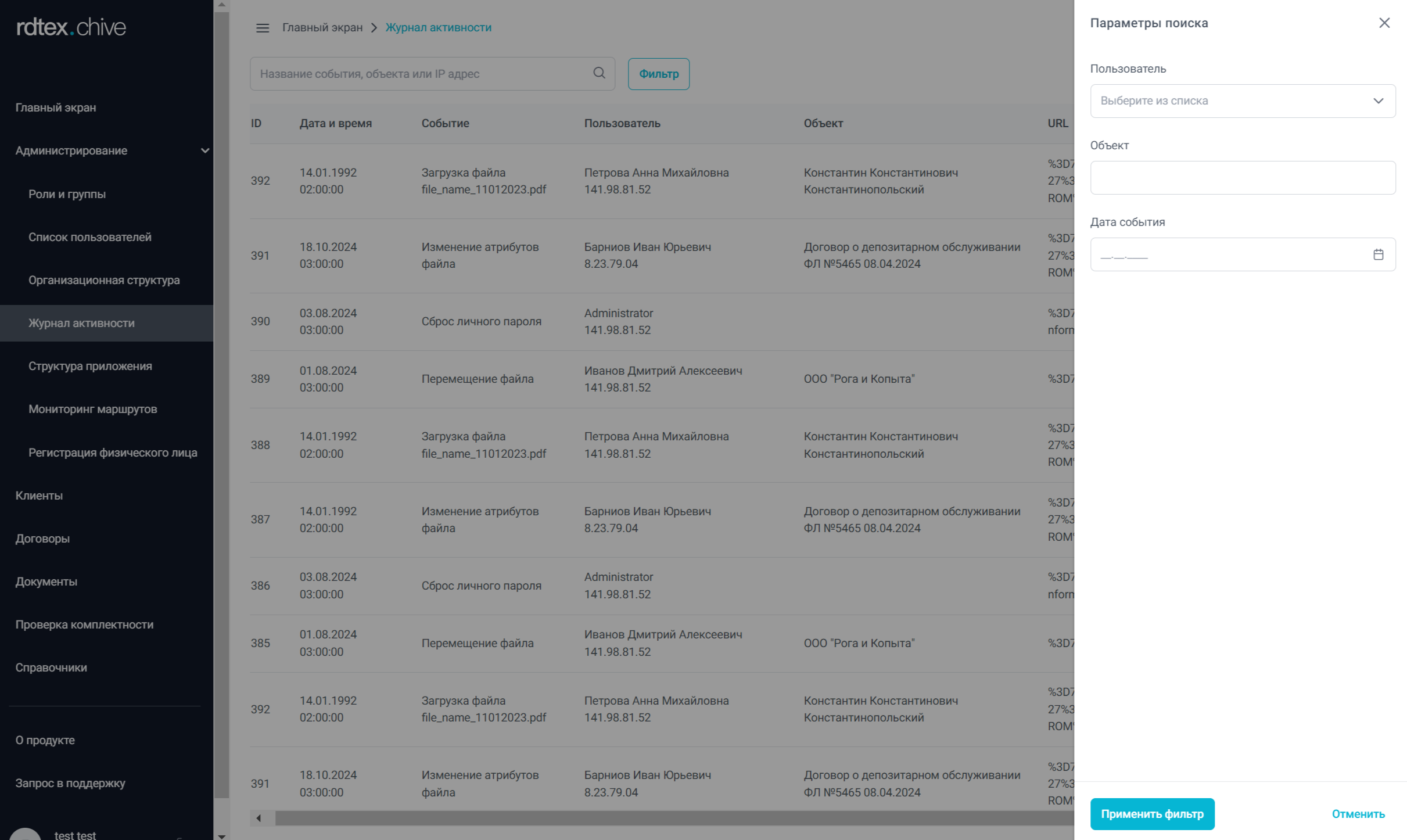
**Рисунок 8. Элементы управления Организационной структурой.**

## **4.5. Просмотр журнала активности**

В разделе "Журнал активности" отображаются все события, связанные с действиями пользователей в системе. Это помогает отслеживать, какие операции были выполнены, кем и когда. Журнал активности показывает события с датой, описанием, пользователем, объектом и URL запроса.

В интерфейсе предусмотрены функции поиска и фильтрации. Поиск позволяет находить записи по названию события, объекту или IP-адресу. Фильтры позволяют сузить результаты по таким параметрам, как пользователь, объект и дата события.

Кроме того, есть кнопка "Скачать .csv", которая позволяет экспортировать данные журнала в формат CSV для дальнейшего анализа или отчётности в Excel.

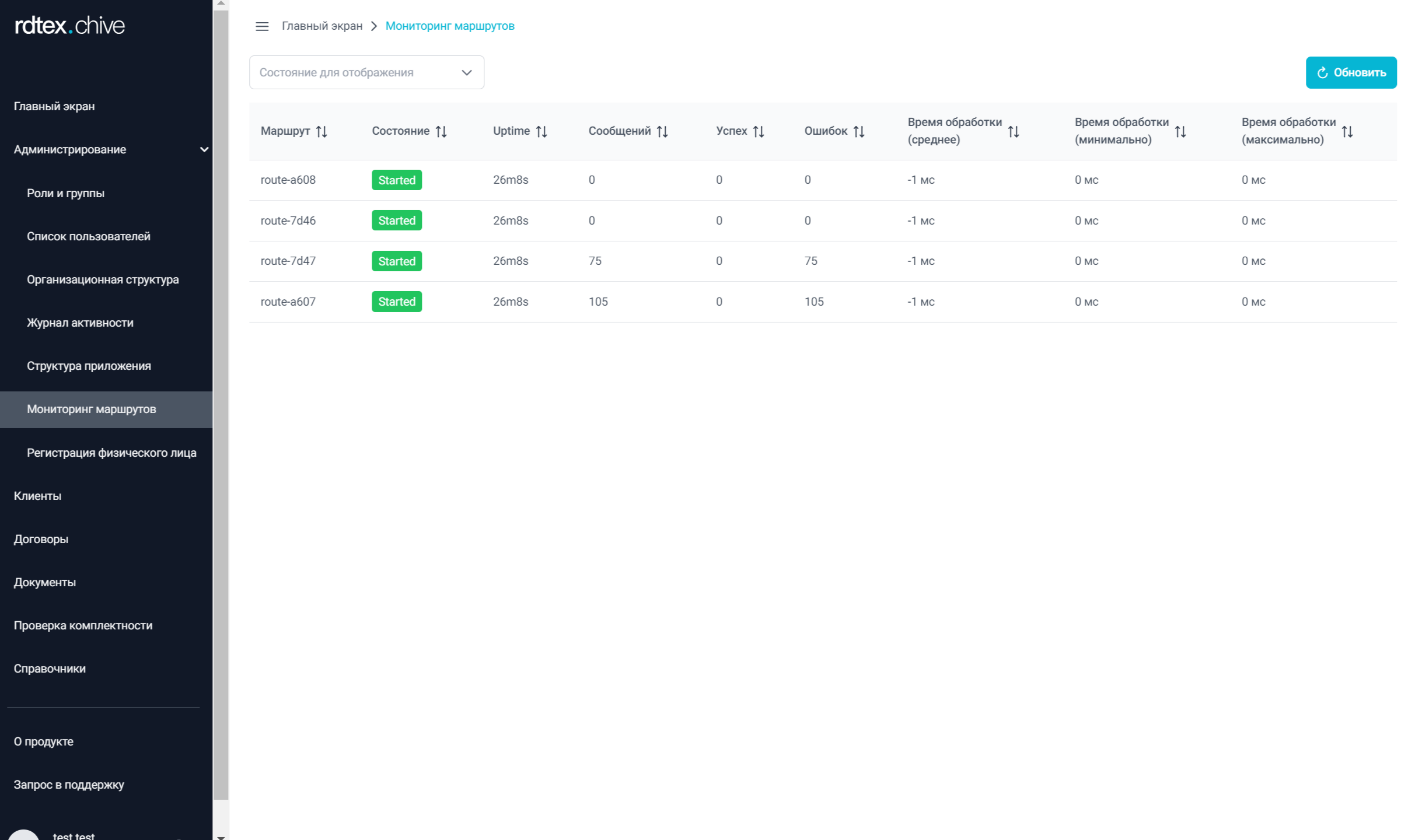


**Рисунок 9. Страница Журнала активности.**

## **4.6. Мониторинг маршрутов**

На странице мониторинга маршрутов отображается таблица с состоянием роутеров и важными метриками. Администратор видит информацию о роутерах, такую как текущее состояние, время работы, количество обработанных сообщений и время их обработки.

Таблица позволяет сортировать данные по любому из столбцов и фильтровать их по состоянию роутера (например, отображать только запущенные или остановленные роутеры). Также есть возможность обновить данные вручную через кнопку "Обновить".



**Рисунок 10. Страница Мониторинга маршрутов.**