**Контур хранения персональных данных и данных о юридических лицах, и аутентификации пользователей РЦИСID**

Инструкция по эксплуатации комплекса технических средств

(Руководство администратора)

Листов 20

2023

содержание

[1 Общие указания 4](#_Toc155949820)

[1.1 Обозначение и наименование системы 4](#_Toc155949821)

[1.2 Функции системы 4](#_Toc155949822)

[1.3 Режимы работы 5](#_Toc155949823)

[2 Меры безопасности 7](#_Toc155949824)

[2.1 Функции системы 7](#_Toc155949825)

[2.2 Описание принципа функционирования 7](#_Toc155949826)

[3 Порядок работы 9](#_Toc155949827)

[3.1 Состав и квалификация персонала 9](#_Toc155949828)

[3.2 Порядок проверки знаний персонала и допуска его к работе 10](#_Toc155949829)

[3.3 Описание работы и последовательность их выполнения 10](#_Toc155949830)

[3.3.1 Установка системы 10](#_Toc155949831)

[3.3.2 Добавление клиентов 12](#_Toc155949832)

[3.3.3 Панель администрирования 13](#_Toc155949833)

[3.3.4 Логирование 14](#_Toc155949834)

[3.3.5 Метрики 14](#_Toc155949835)

[3.3.6 Отправка email 15](#_Toc155949836)

[3.3.7 Отправка SMS 16](#_Toc155949837)

[3.3.8 Резервное копирование 17](#_Toc155949838)

[3.3.9 Восстановление из резервной копии 17](#_Toc155949839)

[4 Проверка правильности функционирования 18](#_Toc155949840)

[5 Указания о действиях в разных режимах 19](#_Toc155949841)

[6 Основные понятия и определения 20](#_Toc155949842)

**АННОТАЦИЯ**

В документе даётся описание порядка работы и мер безопасности при эксплуатации контура хранения персональных данных и данных о юридических лицах, и аутентификации пользователей РЦИСID (далее по тексту – РЦИСID). Приводятся указания о действиях в разных режимах.

Документ составлен в соответствии с ГОСТ Р 59795-2021 Автоматизированные системы. Требования к содержанию документов.

# Общие указания

## Обозначение и наименование системы

Наименование системы: Контур хранения персональных данных и данных о юридических лицах, и аутентификации пользователей РЦИСID.

Обозначение системы: РЦИСID.

Система функционирует на следующем оборудовании:

* Процессор: 2 процессора Xeon Bronze 3106 на 8 ядер каждый или мощнее.
* ОЗУ: 64 ГБ и более
* Дисковая подсистема: 2 SSD-накопителя объёмом 240 ГБ каждый и 2 SSD-накопителя объёмом 2 ТБ каждый.

Системное программное обеспечение, необходимое для функционирования программы для РЦИСID:

* Операционная система Linux, к примеру Ubuntu LTS 20.04;
* Система докеризации (развёртывания) Docker 18.03.

Канал связи должен обеспечивать скорость передачи данных не менее 100 Мбит/с до других узлов РЦИСID.

## Функции системы

Областью применения РЦИСID являются следующие функции:

1. Хранение персональных данных физических лиц (далее - идентификаторов) - участников цифровой экономики интеллектуальной собственности. К примеру: авторов, правообладателей, лицензиатов, сублицензиатов, экспертов, представителей и т.д.
2. Хранение цифровых копий документов, содержащих идентификаторы.
3. Реализация протокола OAuth 2.0, для предоставления идентификаторов сервисам цифровой экономики интеллектуальной собственности.

## Режимы работы

РЦИСID функционирует в двух режимах – штатном и аварийном.

* Штатный (режим повседневной деятельности) – основной режим функционирования. В данном программные интерфейсы выполняют свои функции в соответствии с техническими и организационными инструкциями;
* Аварийный – режим, который позволяет устранять неисправности оборудования с максимально возможным сохранением информации и работающих компонентов.

При возникновении технических сбоев система автоматически переходит в аварийный режим, при котором отвечает HTTP-ошибкой c кодом 500 на все поступающие запросы, либо не отвечает вовсе. В таком случае, эксплуатационный персонал должен предпринять действия по возврату системы в штатный режим. К основным операциям по возврату системы в штатный режим относятся:

* Перезапуск контейнеров в соответствии с руководством по работе с Docker;
* Перезапуск среды контейнеризации в соответствии с руководством по работе с Docker;
* Проверка доступности сети и настроек сетевого оборудования в соответствии с инструкцией производителя инфраструктуры;
* Проверка ресурсов и компонентов серверного оборудования в соответствии с инструкцией к используемому оборудованию;
* Развёртывание нового экземпляра на другом оборудовании в соответствии с документом путём подключения к репозиториям repo.ipcenter.ru, registry.ipcenter.ru и установки актуальной версии РЦИСID.
* Восстановление из резервной копии данных.

# Меры безопасности

## Функции системы

Целью создания РЦИСID является повышение эффективности исполнения процессов, необходимых для обеспечения сохранности объектов участников цифровой экономики интеллектуальной собственности. Эффективность достигается за счет следующих функций:

1. Сохранение идентификаторов и их дополнительных атрибутов. К примеру: паспортные данные гражданина РФ, данные заграничного паспорта гражданина РФ, водительское удостоверение, номер телефона, ИНН, СНИЛС, идентификатор физического лица в Гиперграф - информационной системе управления правами в РАО, ВОИС
2. Запрос на получение ActorId физического лица в каналах сети РЦИС.РФ по внешним (по отношению к Сети РЦИС.РФ) идентификаторам. К примеру запрос ActorID по: Фамилии Имени Отчеству и серии/номеру паспорта гражданина РФ.
3. Предоставление идентификаторов и цифровых копий документов, содержащих идентификаторы сервисам, работающим с Контуром ПДн. Разрешение сервису на доступ к идентификаторам физическое лицо предоставляет самостоятельно при авторизации в сервисе. Использование протокола OAuth 2.0.

## Описание принципа функционирования

Система функционирует в виде сервиса предоставления аутентфикационной информации по протоколу OAuth 2.0 РЦИСID.

РЦИСID выполняет следующие задачи:

* Хранение персональных данных физических лиц (далее - идентификаторов) - участников цифровой экономики интеллектуальной собственности. К примеру: авторов, правообладателей, лицензиатов, сублицензиатов, экспертов, представителей и т.д. READY;
* Хранение цифровых копий документов, содержащих идентификаторы. READY;
* Реализация протокола OAuth 2.0, для предоставления идентификаторов сервисам цифровой экономики интеллектуальной собственности. READY.

# Порядок работы

## Состав и квалификация персонала

Специалисты, обеспечивающие техническую поддержку приложения, должны обладать следующими знаниями и навыками:

* Владение персональным компьютером и почтовыми программами;
* Знание функциональных возможностей Сети и особенностей работы с ними;
* Умение работать в основных операционных системах – Windows и Linux актуальных версий;
* Навыки работы в системе управления задачами Jira;

Техническая поддержка пользователей оказывается с помощью электронной почты support@ipcenter.ru

В процессе технической поддержки приложения задействовано \*\*\* сотрудников, на каждого сотрудника приходится до ста обращений в месяц. При необходимости штат может быть расширен.

Специалисты, осуществляющие развёртывание и обновление ПО, должны иметь квалификацию в зависимости от сферы разработки:

* Специалисты, участвующие в разработке back-end части, должны владеть навыками разработки на языке GoLang, владеть языком запросов к базам данных SQL, уметь работать с СУБД PostgreSQL, используя любой из следующих инструментов: DBeaver или Intellij DataGrip, иметь навыки написания docker compose файлов автоматизации развёртывания (навыки devops), иметь навыки написания unit-тестов, используемых в процессе разработки для самоконтроля разработчиков, иметь понимание о клиент-серверной архитектуре на основе REST, знать спецификацию OpenAPI 3.0.
* Специалисты, участвующие в разработке front-end части, должны владеть навыками разработки на языке программирования TypeScript с использованием фреймворков Vue3 и Nuxt, языками разметки текста HTML, с использованием CSS, уметь пользоваться системами сборки проекта пользовательского интерфейса webpack или Vite, иметь понимание о клиент-серверной архитектуре на основе REST, знать спецификацию OpenAPI 3.0

Аппаратное обеспечение узла должно соответствовать:

* Процессор: 2 процессора Xeon Bronze 3106 на 8 ядер каждый или мощнее.
* ОЗУ: 64 ГБ и более
* Дисковая подсистема: 2 SSD-накопителя объёмом 240 ГБ каждый и 2 SSD-накопителя объёмом 2 ТБ каждый.

## Порядок проверки знаний персонала и допуска его к работе

Персонал получает допуск к работе после проверки знаний по соответствующим должностным инструкциям, а также после изучения документации к системе.

Допуск к работе выдаёт руководитель подразделения, эксплуатирующего РЦИСID.

## Описание работы и последовательность их выполнения

### Установка системы

Для установки РЦИСID должен быть подготовлен комплекс технических средств, указанный в документе «РЦИСID Технический паспорт для ПО».

Установка РЦИСID осуществляется из исходных кодов в репозитории https://repo.ipcenter.ru:

1. Выполнить клонирование репозитория через http или git. Для использования ssh необходимо добавить ключ сервера (~/.ssh/id\_rsa.pub) в разрешенные в профиле gitlab (<https://repo.ipcenter.ru>).

mkdir -p /opt/pds

apt -y install git make ansible

git clone https://repo.ipcenter.ru/ipcenter/id/pds-install.git /opt/pds

#or

git clone ssh://git@repo.ipcenter.ru:2222/ipcenter/id/pds-install.git /opt/pds

cd /opt/pds

1. Настроить параметры доступа к репозиторию в файле .repo-access.

cp .repo-access.sample .repo-access

1. Задать URL-адрес (FQDN) будущего сервиса в файле .env.template.
2. Запустить установку.

make run

Будет произведена установка Docker, docker compose, скачаны образы контейнеров и выполнен запуск.

1. Настроить nginx.

make setup-nginx

1. Настройка системы отправки почтовых уведомлений

make setup-dkim

Полученную запись ./dkim/<ДОМЕН>.txt необходимо внести в DNS. Для беспроблемной доставки почты необходимо также внести IP сервера в SPF-запись, а также сделать PTR DNS-запись для сервера. В этом случае шансы попадания писем в спам минимизируются.

1. Чтобы зарегистрировать **тестовых** пользователей можно инициализировать их командой

ansible-playbook devClients.yml

В файле указаны dev\_client\_1, dev\_client\_2, пароль password. Пароль возможно сменить в /admin.

### Добавление клиентов

Добавление новых клиентов в РЦИС ID производится вручную через подключение к БД и занесение новых строк в таблицы. А именно:

PDS:

1. Таблица «client» заполняется полями:
* «id»: идентификатор клиента (a-Z0-9\_, например «nris»). Необходим для идентификации клиента в API запросах. Необходим для входа в панель администрирования.
* «type»: тип клиента (всегда «confidential»)
* «description»: описание клиента. Нигде не показывается - только внутренняя структура.
* «secretHash»: результат хэш функции «bcrypt» от пароля. Необходим для получения токенов работы в API запросах. Необходим для входа в панель администрирования.
* «logo»: логотип (в формате base64). Показывается персонам в авторизации от этого клиента.
* «background»: задний фон авторизации (в формате base64). Показывается персонам в авторизации от этого клиента.
* «name»: Имя клиента (например, «NRIS»). Показывается персонам в авторизации от этого клиента.
* «isAP»: Разрешение на использование панели администрирования
* «loginText»: json структура с полями, где ключом выступает код языка в формате ISO-639-1, а значением - приветственная фраза (например, {"en": "to continue to", "ru": "для продолжения в" }). Показывается персонам в авторизации от этого клиента.

ODS:

1. Таблица «client» заполняется полями:
* «id»: идентификатор клиента (a-Z0-9\_, например «nris»). Необходим для идентификации клиента в API запросах.
* «type»: тип клиента (всегда «confidential»)
* «description»: описание клиента. Нигде не показывается - только внутренняя структура.
* «secretHash»: результат хэш функции «bcrypt» от пароля. Необходим для получения токенов работы в API запросах. Необходим для входа в панель администрирования.

### Панель администрирования

Панель администрирования располагается по адресу <uri PDS>/admin и доступна только в PDS. Для входа в панель администрирования в БД должно быть разрешение в поле «isAP».

Вход в панель администрирования осуществляется через ввод client\_id / secret на странице авторизации.

В случае первого входа появится обязательная регистрация через 2FA путем сканирования QR-кода. В случае повторных входов необходимо будет подтвердить вход через 2FA.

Панель администрирования содержит 3 вкладки и позволяет:

1. Вкладка Client:
* Изменение «Name» клиента - имя, видимое на OAuth персон через данного клиента;
* Изменение «Login text» клиента - приветственная фраза на OAuth персон через данного клиента;
* Изменение «Redirect links» - перечень ссылок, доступных для конечного редиректа персон после OAuth  через данного клиента;
* Изменение «Registration links» - перечень ссылок, доступных для редиректа персоны для регистрации через данного клиента;
* Изменение «Logo» клиента;
* Изменение «Background» клиента;
* Изменение «Secret» клиента;
* Получение нового токена клиента;
* Сохранение изменений;
* Выход из панели администрирования.
1. Вкладка «Persons»:

Просмотр основной информации персон, выдавшим вам разрешение.

1. Вкладка «Templates»:

Загрузка и выбор шаблонов отображения шагов OAuth персон через данного клиента.

### Логирование

Логирование осуществляется на уровне HTTP-запросов к роутеру и сохраняет:

* Время запроса;
* HTTP Status Code ответа;
* Время выполнения запроса;
* IP запрашиваемой стороны;
* HTTP Method;
* client\_id инициатора запроса (при возможности);
* URL запроса;
* Внутреннюю ошибку (при наличии).

Данные логи хранятся в докере. Существует возможность настроить перенаправление логов в используемую систему централизованного сбора журнала.

### Метрики

Роутер предоставляет эндпоинт для запроса метрик по авторизации

Собираются 2 метрики:

1. request\_total - количество запросов с label по:
* code - HTTP Status Code;
* method - HTTP Method;
* url  - запрашиваемый эндпоинт.
1. request\_duration - время запроса с label по:
* code - HTTP Status Code;
* method - HTTP Method;
* url  - запрашиваемый эндпоинт.

Для сбор метрик может быть использована система Prometheus. Для отображения метрик может использоваться система Grafana.

### Отправка email

Отправка электронной почты осуществляется через свой поднятый SMTP-сервис. Для корректной доставки почты необходимо корректно настроить записи в DNS. IP нужно внести в SPF-запись, а также настроить DKIM:

Пример генерации DKIM ключа:

mkdir -p /host/keys; cd /host/keys

for DOMAIN in example.com example.org; do

    # Generate a key with selector "mail"

    opendkim-genkey -b 2048 -h rsa-sha256 -r -v --subdomains -s pds -d $DOMAIN

    # Fixes https://github.com/linode/docs/pull/620

    sed -i 's/h=rsa-sha256/h=sha256/' mail.txt

    # Move to proper file

    mv mail.private $DOMAIN.private

    mv mail.txt $DOMAIN.txt

done

...

opendkim-genkey обычно находится в пакете  opendkim-tools или  opendkim-utils. после этого  <domain>.txt файлы надо внести в DNS. Папку с DKIM ключами необходимо смонтировать в контейнер smtp и они подключаться автоматически:

Пример из docker-compose.yml

  pds-smtp:  # SMTP для отправки писем

    container\_name: pds-smtp

    restart: always

    image: boky/postfix

    environment:

      - HOSTNAME=<host> # Hostname (например, «pds.ipcenter.ru»)

      - ALLOWED\_SENDER\_DOMAINS=<sender> # Allowed sender domain (например, «id.ipcenter.ru»)

      - DKIM\_SELECTOR=pds

    volumes:

      - ./dkim/:/etc/opendkim/keys

Примечание: dkim-selector может быть любым, главное сгенерировать ключ с таким же selector.

### Отправка SMS

Отправка SMS осуществляется через обращение к центру рассылки сообщений/ Для отправки SMS настраиваются параметры через установленные переменные окружения:

APP\_ADAPTER\_SMSSENDER\_API\_HOST=<host> # Хост для отправки SMS

APP\_ADAPTER\_SMSSENDER\_API\_TYPE=<type> # Тип отправки SMS (например, «sms-c»)

APP\_ADAPTER\_SMSSENDER\_API\_KEY=<secret> # Пароль для отправки SMS

### Резервное копирование

Необходимо производить резервное копирование файлов pds-db (БД Postgres) и pds-storage (minio S3) расположение файлов /opt/pds/storage.

ods:

* файлы в /opt/ods/storage
* postgres DB: доступы можно брать из файла /opt/ods/docker-compose.yml - сервис ods-db.
* docker-compose.yml

pds:

* файлы /opt/pds/storage
* postgres DB: доступы можно брать из файла /opt/pds/docker-compose.yml - сервис pds-db.
* docker-compose.yml

Резервное копирование файлов БД осуществляется штатными утилитами PostgreSQL – pg\_dump или сторонними средствами, например, restic.

Время хранения резервных копий не должно превышать 2 месяца. Резервные копии должны храниться строго в зашифрованном виде.

Частота создания резервных копий 3 часа.

### Восстановление из резервной копии

Для восстановления базы данных из резервной копии воспользуйтесь стандартной утилитой pg\_restore или альтернативными приложениями в соответствии с рекомендациями производителя. Восстановите информацию из последней актуальной резервной копии.

Для восстановления файлового хранилища выполните копирование файлов из последней актуальной резервной копии.

# Проверка правильности функционирования

Для проверки правильности функционирования требуется в соответствии с документом «РЦИСID Руководство программиста» выполнить следующие действия:

1. Аутентифицироваться на сервисе РЦИСID при помощи персональных client\_id и client\_secret;
2. Получить access\_token;
3. Выполнить метод GET /info с полученным access\_token.

Если в результате выполнения метода возвращён ответ с кодом 200, то сервис функционирует правильно.

Для более детальной проверки корректности функционирования РЦИСID следует воспользоваться сценариями, приведёнными в документе «Программа и методика испытаний для программного обеспечения «Контур хранения персональных данных и данных о юридических лицах, и аутентификации пользователей РЦИСID».

# Указания о действиях в разных режимах

В ходе штатного функционирования системы требуется следить за показателями мониторинга КТС и предпринимать действия, предотвращающие возникновение ошибок. Дополнительно требуется контролировать успешность выполнения операций резервного копирования и поддержания актуальности резервной копий.

Об аварийном отключении оборудования необходимо немедленно проинформировать оперативный персонал, осуществляющий поддержку КТС о наступлении аварии и приступать к восстановлению функционирования системы, которое может включать в себя подготовку резервного КТС, развёртывания нового экземпляра системы и восстановление последней актуальной резервной копии.

# Основные понятия и определения

Основные понятия и определения приведены в таблице ниже:

Таблица Термины и сокращения

|  |  |  |
| --- | --- | --- |
| **№** | **Термин** | **Определение** |
|  | CPU | Англ. Central Processing Unit. Центральный процессор. Характеризуется числом ядер |
|  | Docker  | Программное обеспечение для автоматизации развёртывания и управления приложениями в средах с поддержкой контейнеризации |
|  | Hyperledger fabric | Распределенная блокчейн сеть, состоящая из различных функциональных компонентов, которые устанавливаются на узлы сети |
|  | Сеть РЦИС.РФ | Распределенный реестр, в котором фиксируются операции с правами и объектами интеллектуальной собственности |
|  | Ubuntu  | Дистрибутив операционной системы семейства Linux |
|  | chaincode | Идентификатор блока распределённой Сети РЦИС.РФ |