

Настройка клиента Континент TLS без установленного Крипто ПРО

1. Установка Клиента TLS

Требуется установить на ОС Windows ПО Континент TLS Клиент версии 2.0.1482.0. Дистрибутив может быть скачен с официального сайта https://www.securitycode.ru/download_center/?section=downloads&product=Континент%20TLS&version=Клиент%202.0 предоставлен администратором ИБ.

Запустите файл **Континент TLS-клиент.exe** (распаковав архив), поставьте галочку «Я принимаю условия лицензионного соглашения» и нажмите кнопку **Установить**. Сохраните все открытые вкладки и документы и нажмите кнопку **Перезагрузить**.

Регистрация Континет TLS Клиент

Программа необходимо зарегистрировать для ведение журналов учета СКЗИ. Регистрация проводится онлайн с указанием достоверных сведений, после регистрации будет предоставлен регистрационный код и сняты ограничения с программы

2. Выпуск сертификата пользователя без установленного Крипто ПРО

При запуске ПО Клиента TLS отобразится окно, в котором требуется выбрать меню Управления сертификатами (рисунок 1). Требуется нажать на кнопку «Создать запрос».

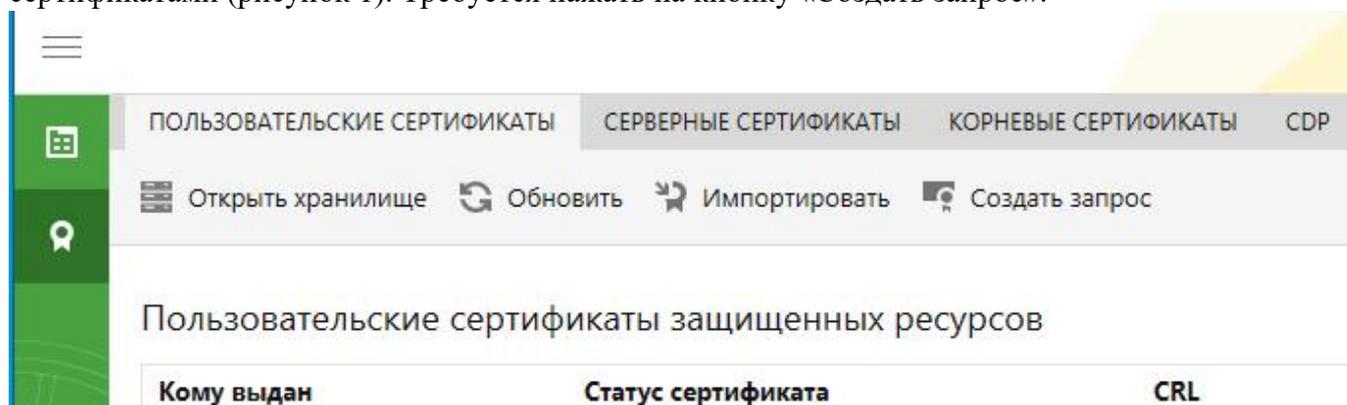


Рисунок 1

Отобразится окно параметров запроса сертификата. Пример настроек указан на рисунке 2.

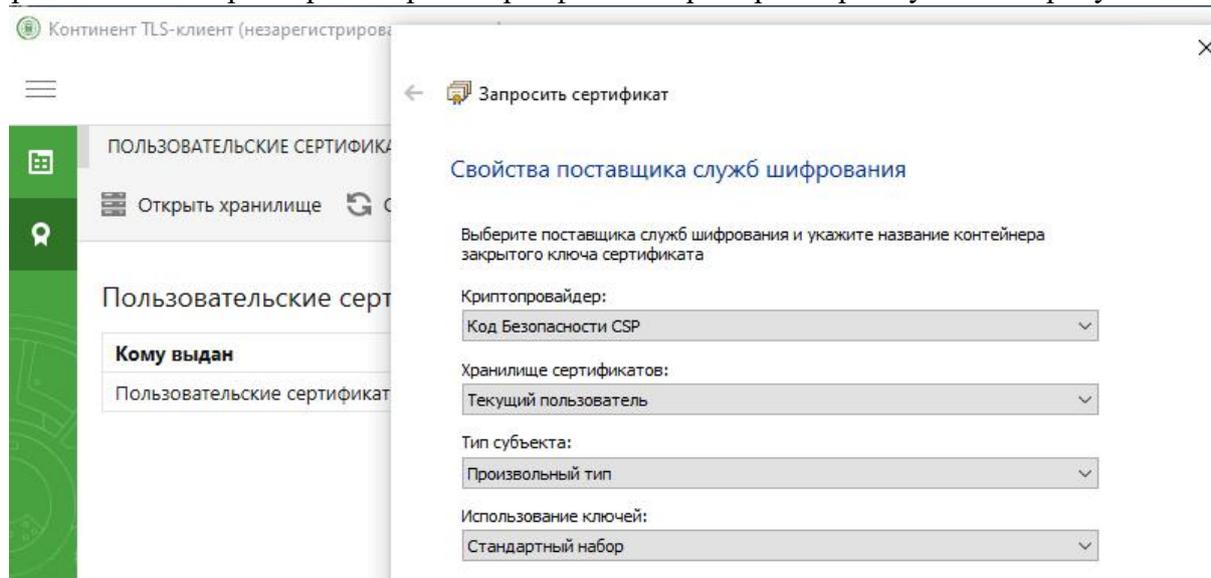


Рисунок 2

На следующем этапе необходимо заполнить запрос (рисунок 3), обязательно необходимо заполнить поля: **общее имя (ФИО полностью), Организация, Подразделение, Должность, Область.**

В запросе не должно быть специальных символов «\», «/», «?» и «'»!

The screenshot shows a window titled 'Запросить сертификат' (Request Certificate) with a sub-header 'Параметры сертификата пользователя' (User Certificate Parameters). Below the sub-header is a note: 'Заполните обязательные поля для выпуска запроса сертификата пользователя. В полях должны быть указаны полные официальные названия без сокращений.' (Fill in the required fields for issuing a user certificate request. The fields must contain full official names without abbreviations.)

The form contains the following fields:

- Фамилия: [text input]
- Имя Отчество: [text input]
- Общее имя: [text input, placeholder: 'Обязательное поле']
- Организация: [text input]
- Подразделение: [text input]
- Должность: [text input]
- Страна: [dropdown menu, value: 'RU']
- Область: [text input]
- Населенный пункт: [text input]
- Адрес: [text input]
- Электронная почта: [text input]
- ИНН: [text input]
- СНИЛС: [text input]
- ОГРН: [text input]

At the bottom right, there are two buttons: 'Далее' (Next) and 'Отмена' (Cancel).

Рисунок 3

На следующем этапе требуется выбрать формат «base64», место сохранения запроса (рисунок 4).

Место запроса необходимо запомнить для отправки его на выпуск сертификата!

The screenshot shows the 'Имя файла' (File Name) section of the 'Запросить сертификат' (Request Certificate) window. It contains the following fields and options:

- Имя ключевого контейнера: [text input, value: 'user1 (15-10-2023 09:17:08)']
- Имя файла для запроса сертификата: [text input, value: 'C:\TLS\newreq-user 1.req']
- Формат файла: [radio buttons, 'Base64' is selected]
- Бланк запроса на сертификат: [checkbox, 'Подготовить бланк запроса на сертификат' is unchecked]

A 'Обзор...' (Browse...) button is located next to the file name input field.

Рисунок 4

Далее, мастер предложит создать пароль для контейнера закрытого ключа. Требуется ввести пароль длиной 8 символов или более (рисунок 5). Так же, требуется выбрать место хранения закрытого ключа (рекомендуется использовать Рутокен или реестр Windows).

Пароль контейнера необходимо запомнить, он необходим для использования сертификата!

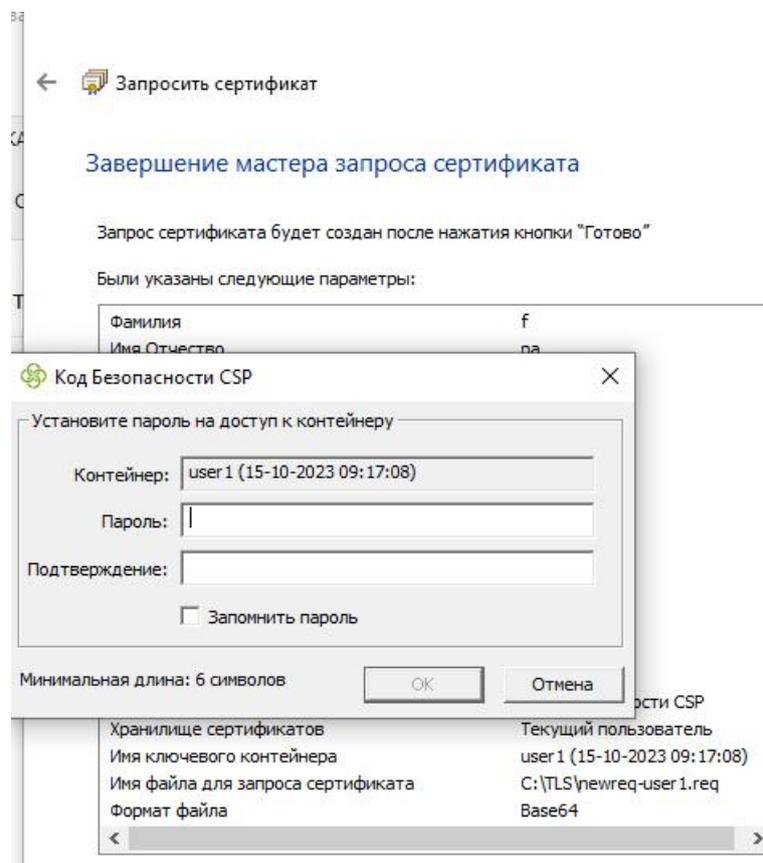


Рисунок 5

После ввода требуемых параметров отобразится окно успешного создания запроса на сертификат (рисунок 6).

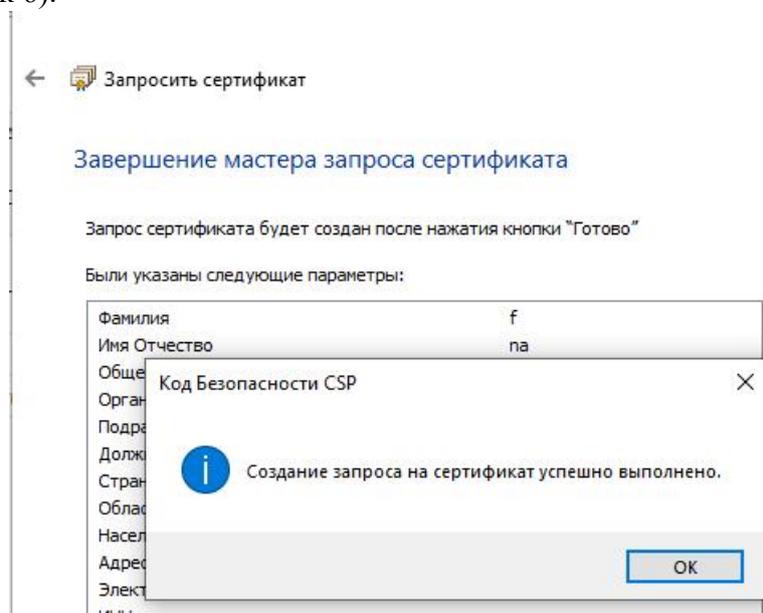


Рисунок 6

Файл запроса на сертификат требуется передать администратору ИБ. Передача запроса сертификата осуществляется направлением письма на почту rwec@rwec.ru в теме указать «Выпуск сертификатов «наименование организации»», в письме указать ФИО и E-Mail сотрудника(-ов).

3. Установка сертификата пользователя

Администратор ИБ направляет следующие файлы на указанный адрес сотрудника для установки на TLS Клиенте:

- Сертификат пользователя, выпущенный по файлу запроса;
- Корневой сертификат УЦ;
- Сертификат TLS сервера;
- Файл CRL (списка отзыва).

Для установки сертификата пользователя в Континент TLS клиент требуется перейти в меню Управления сертификатами с нажать Импортировать (рисунок 1). Далее, в мастере требуется выбрать путь хранения сертификата (рисунок 7). Рекомендуется для пользователя путь хранения «Личное».

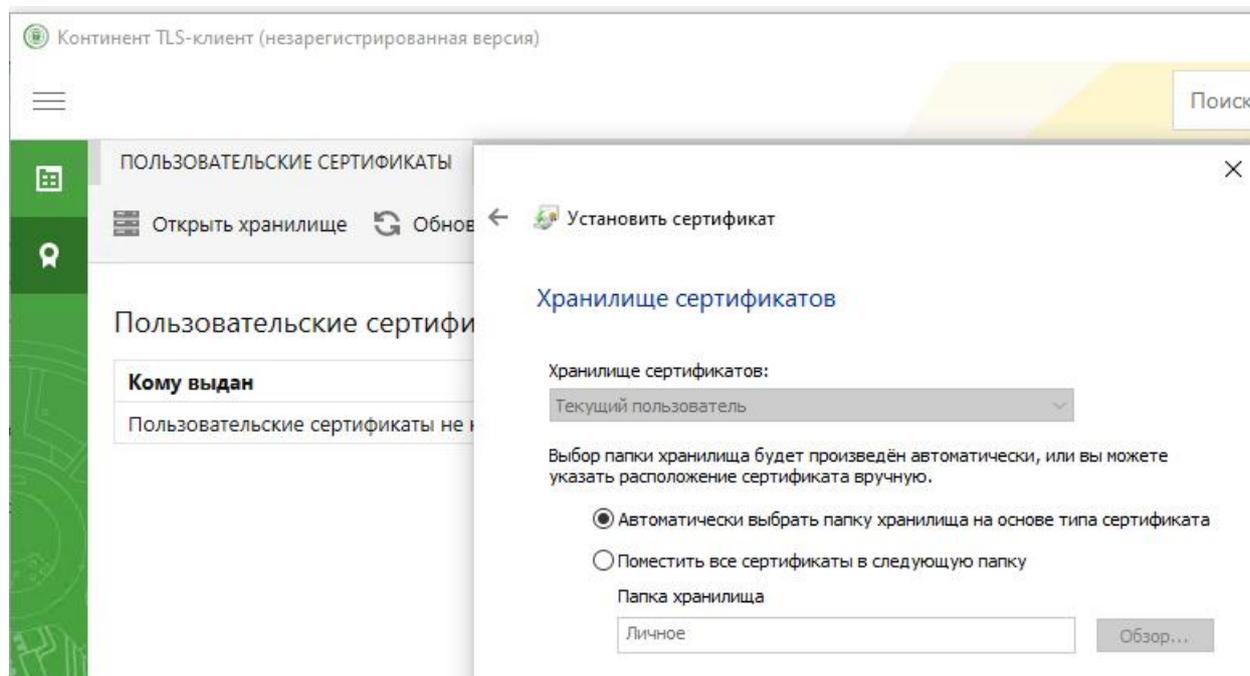


Рисунок 7

После установки отобразится окно успешной установки сертификата (рисунок 8).

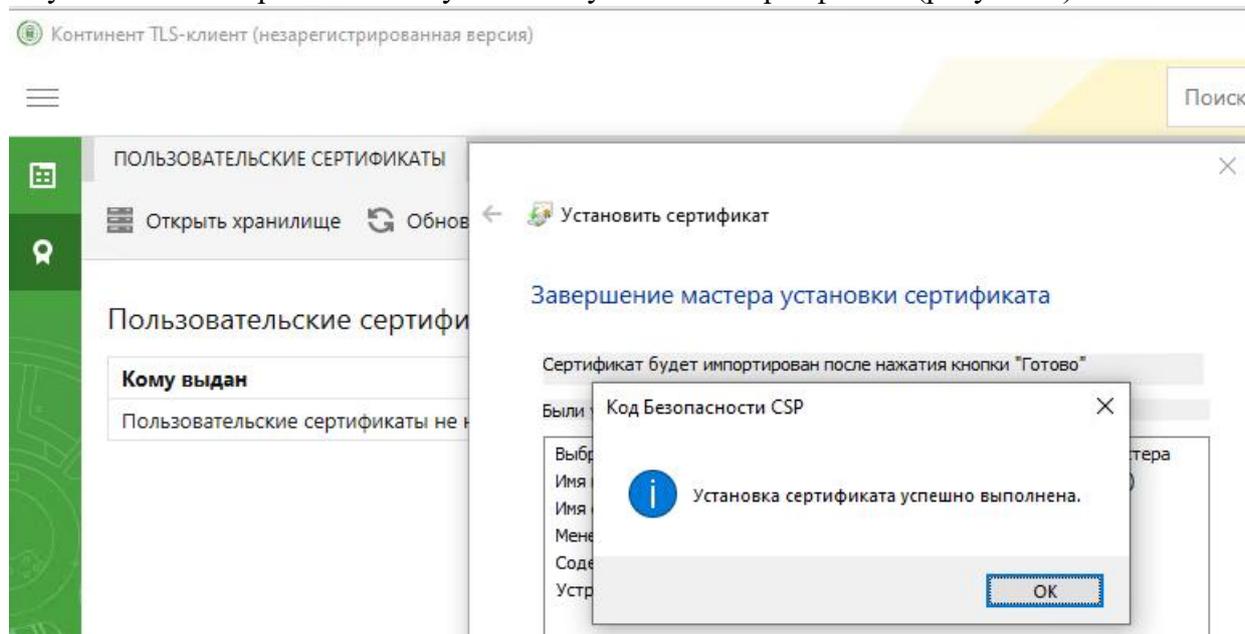


Рисунок 8

4. В разделе «Серверные сертификаты» импортируется файл «_favr.ru.cer», в разделе «Корневые сертификаты» импортируется «CA GIS Voda TLS.cer». На вкладке CDP, выбрать импорт CRL (список отзыва сертификатов) (рисунок 9).

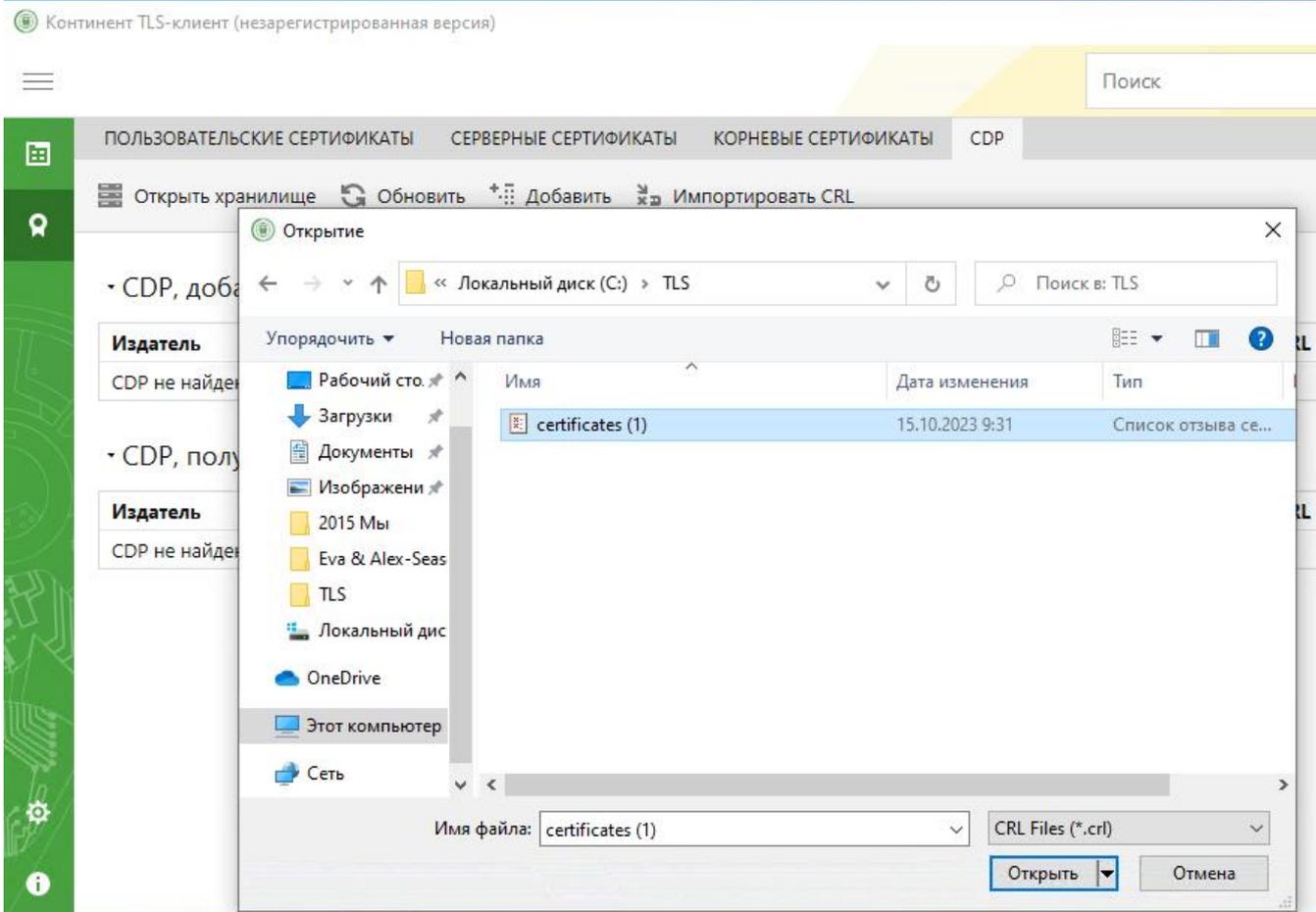


Рисунок 9

Выбрать файл «certificates.crl», полученный от администратора ИБ и загрузить его в Клиент TLS. Отобразится окно успешной загрузки (рисунок 10).

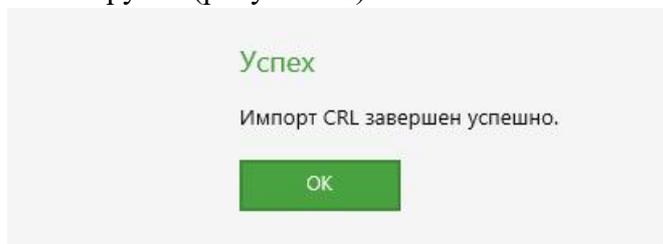


Рисунок 10

Для автоматического обновления CRL, можно добавить CDP и указать адрес «tls.favr.ru/certificates.crl»

5. Проверка сертификатов

В Клиенте TLS требуется перейти во вкладки «Пользовательские сертификаты», «Серверные сертификаты», «Корневые сертификаты». Все загруженные сертификаты должны иметь статус Действителен (рисунок 11).

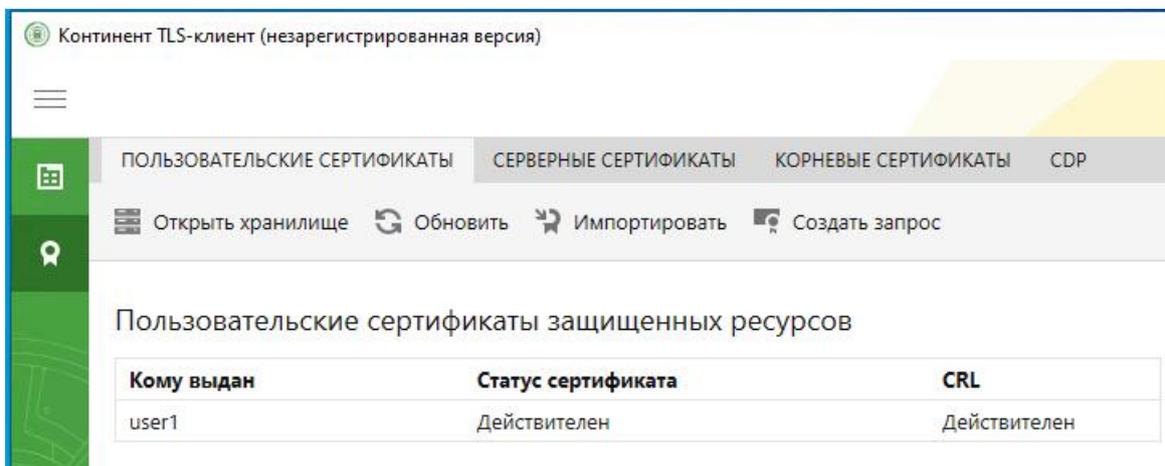


Рисунок 11

6. Настройка подключения к Серверу TLS

В меню «Главная» требуется нажать «Добавить / Ресурс». В открывшемся окне требуется указать имя сервера «*sslgis.favr.ru*». Параметры настройки указаны на рисунке 12 и сохранить. После сохранения в браузере будет доступен закрытый контур ГИС ЦП Вода <https://sslgis.favr.ru/>.

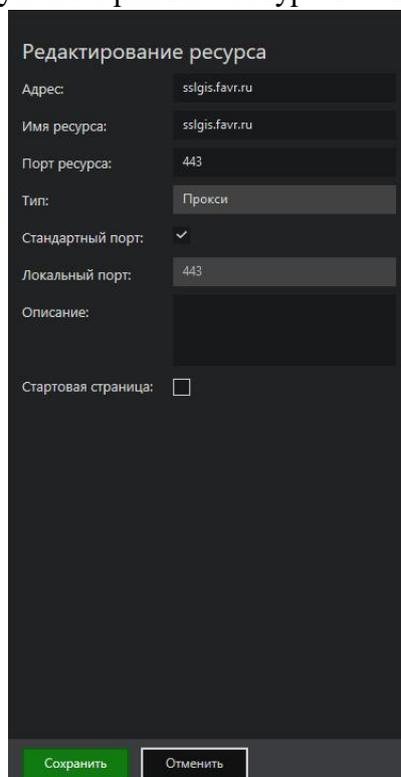


Рисунок 12