

Удостоверяющий центр хоста удаленной загрузки ключей

Руководство пользователя

Версия УЦ 2.2.0

История изменений документа

Версия	Дата	Перечень изменений
1.0	04.09.2018	Первоначальная версия
1.1	14.09.2020	Актуализация скриншотов и добавление информации о выгрузке/загрузке сертификатов/CRL в формате base64. Добавлен пункт 11

Содержание

1. Используемые сокращения и обозначения	4
2. Введение	4
3. Краткое описание Удостоверяющего центра хоста удаленной загрузки ключей.....	4
4. Описание web-интерфейса.....	5
5. Вход / выход в (из) системы.....	6
6. Первый вход в систему.....	7
7. Регистрация пользователей	9
7.1. Блокировка и редактирование пользователей	11
7.2. Первая авторизация нового пользователя.....	11
8. Импорт сертификата и CRL корневого УЦ.....	12
8.1. Импорт сертификата корневого УЦ	12
8.2. Импорт CRL корневого УЦ.....	14
9. Создание запроса на сертификат, импорт сертификата, создание CRL в разделе УЦ Distr.....	15
9.1. Создание запроса на сертификат УЦ Distr	15
9.2. Импорт сертификата УЦ Distr	19
9.3. Выпуск CRL.....	21
10. Выпуск сертификата KDH.....	23
11. Изменение настроек.....	26

1. Используемые сокращения и обозначения

УЦ	Удостоверяющий центр
CRL	(Certificate Revocation List) – список отозванных сертификатов, заверенный цифровой подписью УЦ, выпускающего данные сертификаты
HSM	Аппаратный модуль безопасности, который генерирует наборы секретных криптографических ключей для последующей загрузки в целевое устройство
KDH	(Keys Distribution Host) – сервер удаленной загрузки ключей
УЦ Root	Корневой Удостоверяющий центр ИНПАС
УЦ Distr	Удостоверяющий центр хоста удаленной загрузки ключей
УЦ Prod	Удостоверяющий центр выдачи сертификатов POS-терминалам
Смарт-карта	Пластиковая карта со встроенной микросхемой.
Картридер	Устройство для чтения смарт-карт.

2. Введение

Данный документ описывает web-интерфейс Удостоверяющего центра хоста удаленной загрузки ключей и порядок работы с ним.

Данный документ предназначен для прочтения пользователем, осуществляющим работу с Удостоверяющим центром хоста удаленной загрузки ключей через web-интерфейс.

Данный документ не содержит информации по установке, настройке и запуску сервера Удостоверяющего центра хоста удаленной загрузки ключей, эти данные представлены в руководстве по установке удостоверяющего центра (Руководство по установке.pdf).

3. Краткое описание Удостоверяющего центра хоста удаленной загрузки ключей

Удостоверяющий центр хоста удаленной загрузки ключей является программным продуктом, представляет из себя сервер для формирования, удостоверения, предоставления, хранения и приема запросов на выдачу сертификатов для подчиненных KDH (хоста удаленной загрузки ключей).

Основные функции системы:

- Формирование запроса на выдачу сертификата своего публичного ключа;
- Хранение и предоставление сертификата своего публичного ключа;
- Прием запросов на выдачу сертификатов публичного ключа для KDH;
- Удостоверение сертификата публичного ключа для KDH;
- Формирование, удостоверение и предоставление списка отозванных сертификатов (CRL) KDH.

Взаимодействие пользователя с УЦ Distr осуществляется через web-интерфейс данного сервера.

4. Описание web-интерфейса

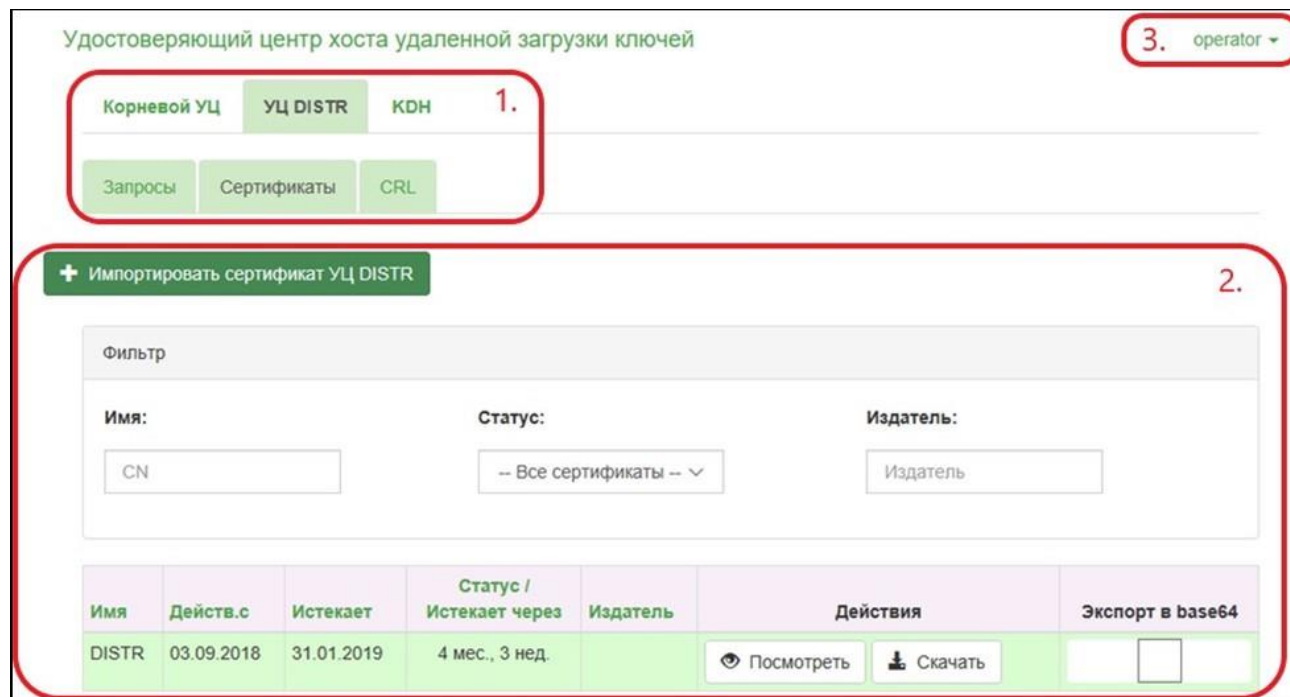


Рисунок 1. Главное окно системе "Удостоверяющего центра хоста удаленной загрузке ключей"

Web-интерфейс системы «Удостоверяющего центра хоста удаленной загрузке ключей» представляет собой страницу, содержащую следующие элементы:

- Главное меню, состоящее из следующих разделов:
 - Корневой УЦ** – позволяет импортировать и хранить сертификат и CRL корневого УЦ;
 - Сертификаты – позволяет импортировать и хранить сертификат корневого УЦ;
 - CRL – позволяет импортировать и хранить список отозванных сертификатов (CRL) корневого УЦ.
 - УЦ Distr** – позволяет выполнить выпуск цепочек SSL сертификатов;
 - Запросы** - формирование и хранение запроса на выдачу сертификата своего публичного ключа;
 - Сертификаты** - хранение и предоставление сертификата публичного ключа УЦ Distr;
 - CRL** - формирование, удостоверение и предоставление списка отозванных сертификатов (CRL) KDH.
 - KDH** – позволяет выполнять выпуск сертификатов для хоста удаленной загрузки ключей;
 - Сертификаты** – прием запросов на выдачу и удостоверение сертификатов публичного ключа для KDH;
- Основное содержание вкладки.
 - Создание сертификата корневого УЦ** (назначение кнопки изменяется в зависимости от выбранной вкладки);
 - Фильтр** – позволяет выполнить фильтрацию списка;
 - Таблица со списком выпущенных сертификатов/ CRL** (название столбцов и количество может отличаться в зависимости от выбранной вкладки);
 - Имя** – отображается имя сертификата;
 - Действует с** – отображается дата, с которой начинает действовать сертификат;
 - Истекает** – отображается дата истечения действия сертификата;
 - Статус/ Истекает через** – отображается статус сертификата и время, через которое сертификат становится не действительным;

- **Издатель** – отображает какой сертификат был использован при формировании сертификата публичного ключа УЦ Distr;
 - **Действия** – отображается кнопка «Посмотреть», «Скачать», при нажатии на которую выполняется экспорт сертификата;
 - **Экспорт в base64** – при выставлении флага в чек боксе данного столбца, при нажатии кнопки «Посмотреть», выполняется экспорт сертификата в формате «base64».
3. Функциональная кнопка пользователя – позволяет выполнить операции «Настройки», «Пользователя», «Смена пароля» и «Выход».

Примечание.

Перечень доступных операций для «Функциональной кнопки пользователя» может быть разным, в зависимости от роли пользователя.

5. Вход / выход в (из) системы

Вход в систему выполняется после авторизации пользователя путем ввода логина/ пароля и ввода смарт-карты в картридер на странице авторизации пользователя (Рисунок 2. Страница авторизации пользователя).

Рисунок 2. Страница авторизации пользователя

При первом запуске сервера авторизация может быть выполнена под пользователем с правами роли **Administrator**, созданным системой по умолчанию со следующими данными:

- Логин – **admin**;
- Пароль – **admin**.

При успешной авторизации открывается доступ к web-интерфейсу.

Доступность разделов главного меню, выполняемых операций и отображаемых данных, определяется ролью пользователя, под которым была выполнена авторизация.

Для выхода из системы нужно нажать «Функциональную кнопку» в правом верхнем углу страницы и выбрать пункт «Выход» (Рисунок 3. Выход из системы).

Рисунок 3. Выход из системы

6. Первый вход в систему

После успешного входа в систему отобразится страница «**Редактирование пользователя**».

На данной странице необходимо заполнить информацию о пользователе, а именно: «**Email**», «**Телефон**», «**Фамилия**» и «**Имя**» (Рисунок 4. Страница "Редактирование пользователя").

Рисунок 4. Страница "Редактирование пользователя"

В области «**Смарт карта**» отображается информация (смарт-карта не вставлена в картридер)

(Рисунок 5. Область "Смарт-карта". Карта не вставлена в картридер):

- **Состояние ридера** – Карта не вставлена;
- **Состояние привязки** – Отсутствует;
- **Доступные действия** (неактивные кнопки):
 - **Привязать карту** – позволяет привязать смарт-карту к пользователю;
 - **Удалить карту** – позволяет удалить привязанную к пользователю смарт-карту;
 - **Сменить карту** – позволяет перепривязать другую смарт-карту, не выполняя «Удаление карты».

Рисунок 5. Область "Смарт-карта". Карта не вставлена в картридер

Как только заполнили все поля, нужно привязать смарт-карту к данному пользователю, для этого вставляем смарт-карту в картридер (Рисунок 6. Смарт-карта установленная в картридер).



Рисунок 6. Смарт-карта установленная в картридер

Значения полей в области «Смарт-карта» изменятся: «Состояние ридера – Карта вставлена» и станет активной кнопка «Привязать карту» (Рисунок 7. Область "Смарт-карта". Карта вставлена в картридер).

Рисунок 7. Область "Смарт-карта". Карта вставлена в картридер

Для привязки карты к пользователю нажимаем на кнопку «Привязать карту» в области «Смарт карта / Доступные действия».

После успешной привязки смарт-карты значение поля «Состояние привязки» изменится на «Есть привязка к карте», далее нужно нажать кнопку «Сохранить» (Рисунок 8. Сохранение данных пользователя "admin" с привязанной смарт-картой).

Рисунок 8. Сохранение данных пользователя "admin" с привязанной смарт-картой

После нажатия кнопки «Сохранить» система выведет информационное сообщение «Пользователь успешно сохранен» (Рисунок 9. Информационное сообщение об успешном сохранении пользователя). Система перейдет на страницу авторизации пользователя (Рисунок 2. Страница авторизации пользователя).

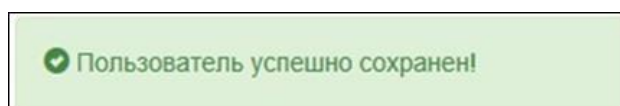


Рисунок 9. Информационное сообщение об успешном сохранении пользователя

7. Регистрация пользователей

После того как выполнили регистрацию системного администратора, необходимо добавить других пользователей для работы с системой «Удостоверяющего центра хоста удаленной загрузки ключей».

Минимальный список пользователей:

- **Администратор** – 1 пользователь;
- **Оператор** – 1 пользователь;
- **Офицер безопасности** – 2 пользователя.

Примечание.

Для пользователя с ролью «Офицер безопасности» необходимо также указывать роль «Оператор», чтобы в дальнейшем пользователь мог изменить свой пароль.

Выполняем вход в «Удостоверяющий центр хоста удаленной загрузки ключей» как системный администратор, отобразится страница «Пользователи», где нужно нажать кнопку «Добавить» (Рисунок 10. Страница "Пользователи". Добавление пользователя).

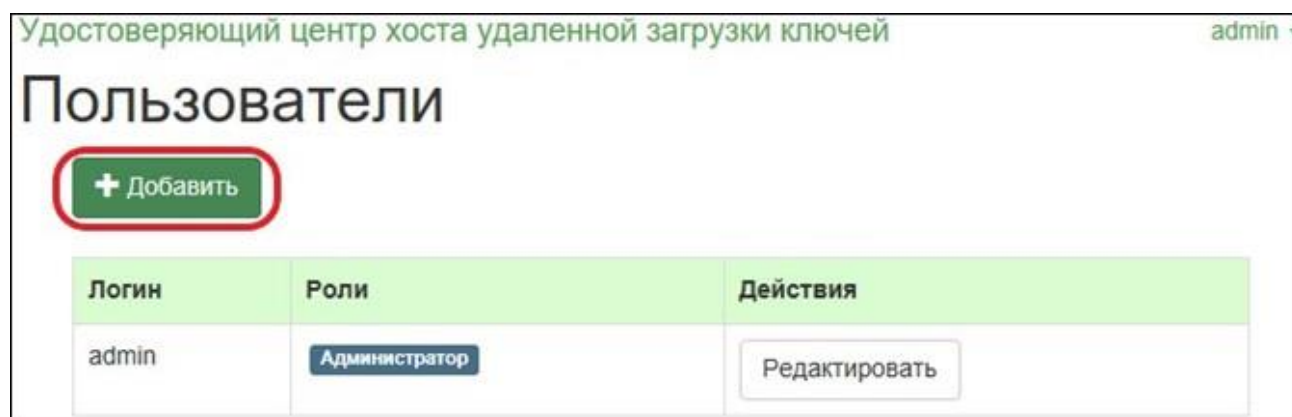


Рисунок 10. Страница "Пользователи". Добавление пользователя

В отобразившемся окне «Создание нового пользователя» заполняем поля:

- **Логин** – указывается логин пользователя для входа в систему (обязательное поле);
- **Пароль** – указывается пароль пользователя для входа в систему (обязательное поле);

Примечание.

Пароль должен состоять из латинских букв и должен содержать минимум: 1 заглавную букву, 1 цифру, 1 символ. Минимальная длина – 8 (восемь) символов.

- **Email** – указывается E-mail пользователя (обязательное поле);
- **Телефон** – указывается телефон пользователя (необязательное поле);
- **Фамилия** – указывается фамилия пользователя (необязательное поле);
- **Имя** – указывается имя пользователя (необязательное поле);
- **Роли** – выбирается роль пользователя:
 - Роль «Администратор» - добавление пользователей, блокировка пользователей и настройка подключения к «HSM»;
 - Роль «Оператор» - выпуск корневого сертификата, выпуск CRL, создание сертификата, подчиненного УЦ;
 - Роль «Офицер безопасности» - подтверждает выпуск корневого сертификата, выпуск CRL, создание сертификата, подчиненного УЦ.

После заполнения полей вставляем смарт-карту в картридер, значение поля «Состояние ридера» изменяется на «Карта вставлена» и нажимаем кнопку «Привязать карту».

После привязки карты значение поля «Состояние привязки» изменяется на «Есть привязка к карте», далее нажимаем кнопку «Сохранить» (Рисунок 11. Создание пользователя).

Удостоверяющий центр хоста удаленной загрузки ключей

Создание нового пользователя

Логин:

Пароль:

Email:

Телефон:

Фамилия:

Имя:

Роли: Администратор Оператор Офицер безопасности

Смарт карта:

Состояние ридера: Карта вставлена

Состояние привязки: Отсутствует

Доступные действия: Привязать карту Удалить карту Сменить карту

2.

Смарт карта:

Состояние ридера: Карта вставлена

Состояние привязки: Есть привязка к карте

Доступные действия: Привязать карту Удалить карту Сменить карту

3.

Рисунок 11. Создание пользователя

После нажатия кнопки **«Сохранить»** система выведет информационное сообщение **«Пользователь успешно сохранен»** (Рисунок 9. Информационное сообщение об успешном сохранении пользователя). Система перейдет на страницу **«Пользователи»** (Рисунок 12. Страница "Пользователи").

Удостоверяющий центр хоста удаленной загрузки ключей admin ▾

Пользователи

Логин	Роли	Действия
admin	Администратор	Редактировать
administrator	Администратор	Редактировать Заблокировать

Рисунок 12. Страница "Пользователи"

7.1. Блокировка и редактирование пользователей

На странице «Пользователи» возможно «Заблокировать» и «Редактировать» пользователя. Для этого нужно нажать на соответствующую кнопку (Рисунок 13. Кнопки "Редактировать" и "Заблокировать").

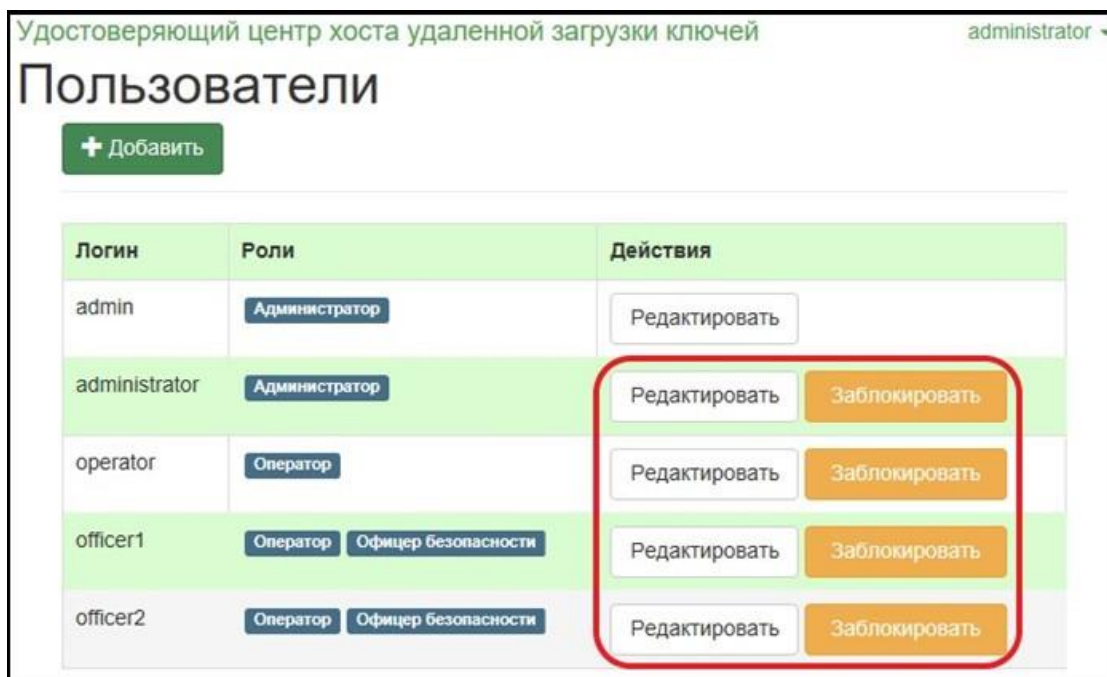


Рисунок 13. Кнопки "Редактировать" и "Заблокировать"

Примечание.

Удалить пользователя - невозможно.

7.2. Первая авторизация нового пользователя

При выполнении первой авторизации нового пользователя система предложит изменить пароль, отобразится страница «Смена пароля пользователя» (Рисунок 14. Страница "Смена пароля пользователя"), где нужно указать «Текущий пароль», «Новый пароль» и «Подтверждение пароля» (повторный ввод нового пароля).

Примечание.

При авторизации любого пользователя происходит двойная аутентификация:

1. Проверка соответствия логина и пароля;
2. Проверка смарт-карты пользователя, установленной в картридер (прикрепляется к пользователю на этапе его создания).

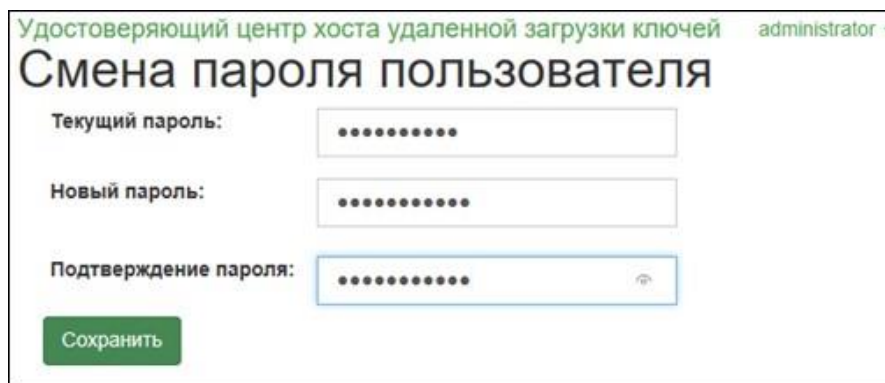


Рисунок 14. Страница "Смена пароля пользователя"

Нажимаем кнопку «Сохранить». Система выведет информационное сообщение «Новый пароль успешно сохранен.» (Рисунок 15. Информационное сообщение об успешном сохранении нового пароля).

✓ Новый пароль успешно сохранен.

Рисунок 15. Информационное сообщение об успешном сохранении нового пароля

После сохранения система перейдет к старнице авторизации пользователя (Рисунок 2. Страница авторизации пользователя).

8. Импорт сертификата и CRL корневого УЦ

8.1. Импорт сертификата корневого УЦ

Для импорта корневого сертификата УЦ необходимо выполнить авторизацию пользователем с ролью «Оператор».

После успешной авторизации необходимо перейти в раздел «**Корневой УЦ**» вкладка «**Сертификаты**» (Рисунок 16. Раздел «Корневой УЦ». Вкладка «Сертификаты». Кнопка "Импортировать сертификат корневого УЦ"), где нужно нажать кнопку «**Импортировать сертификат корневого УЦ**».

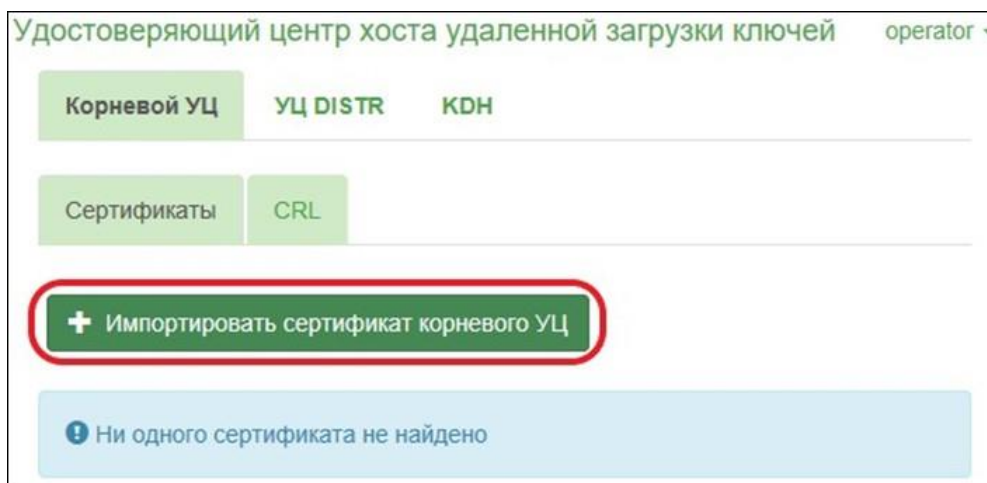


Рисунок 16. Раздел «Корневой УЦ». Вкладка «Сертификаты». Кнопка "Импортировать сертификат корневого УЦ"

На отобразившейся странице «**Импорт корневого сертификата – шаг 1**» необходимо нажать кнопку «**Выберите файл**» и выбрать файл сертификата корневого УЦ (Рисунок 17. Страница «Импорт корневого сертификата - шаг 1». Кнопка «Выберите файл»).

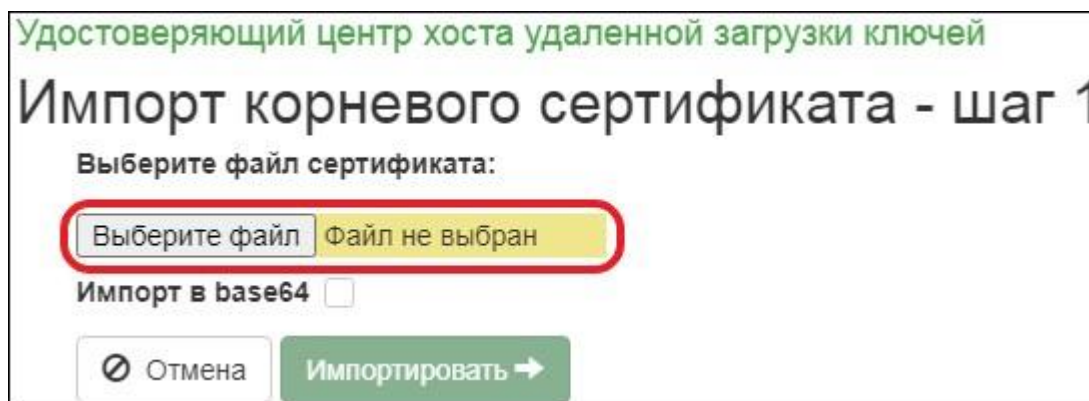


Рисунок 17. Страница «Импорт корневого сертификата - шаг 1». Кнопка «Выберите файл»

После выбора файла отобразится информация о импортируемом сертификате и появится кнопка «**Импортировать**», нажимаем её (Рисунок 18. Страница "Импорт корневого сертификата - шаг 1". Кнопка «Импортировать»).

Если файл сертификата корневого УЦ был экспортирован в формате «**base64**», то необходимо выставить флаг в чек боксе «**Импортировать в base64**».

Удостоверяющий центр хоста удаленной загрузки ключей

Импорт корневого сертификата - шаг 1

Выберите файл сертификата:

Выберите файл

Импорт в base64 ☐

Наименование:

e-mail:

Подразделение:

Организация:

Город:

Страна:

Адрес публикации:

CRL:

Алгоритм ключа:

Размер ключа (бит):

Признак УЦ:

Длина цепочки сертификации:

Использование ключа:

Рисунок 18. Страница "Импорт корневого сертификата - шаг 1". Кнопка «Импортировать»

В отобразившемся окне «Импорт корневого сертификата – заключительный шаг» нужно нажать кнопку «Готово» (Рисунок 19. Страница "Импорт корневого сертификата - заключительный шаг").

Удостоверяющий центр хоста удаленной загрузки ключей operator

Импорт корневого сертификата - заключительный шаг

Сертификат успешно импортирован!

Рисунок 19. Страница "Импорт корневого сертификата - заключительный шаг"

После нажатия кнопки «Готово» отобразится вкладка «Сертификаты» с импортированным сертификатом корневого УЦ (Рисунок 20. Отображение импортированного сертификата корневого УЦ).

Удостоверяющий центр хоста удаленной загрузки ключей operator

Корневой УЦ УЦ DISTR KDN

Сертификаты CRL

+ Импортировать сертификат корневого УЦ

Фильтр

Имя:

Статус:

Имя	Действ.с	Истекает	Статус / Истекает через	Действия	Экспорт в base64
CA_Root	31.08.2018	31.01.2019	5 мес., 4 ч.	Посмотреть	

Рисунок 20. Отображение импортированного сертификата корневого УЦ

Если необходимо выполнить экспорт загруженного сертификата, для этого нужно нажать кнопку «Посмотреть» в столбце «Действия». Далее сохраняем файл сертификата в нужную нам директорию на компьютере. Для выгрузки сертификата в формате «base64» необходимо установить флаг в чекбокс в столбце «Экспорт в base64».

8.2. Импорт CRL корневого УЦ

Для импорта CRL корневого УЦ необходимо перейти в раздел «Корневой УЦ» вкладка «CRL» (Рисунок 21. Раздел «Корневой УЦ». Вкладка «CRL». Кнопка "Импортировать сертификат корневого УЦ"), где нужно нажать кнопку «Импортировать CRL корневого УЦ».

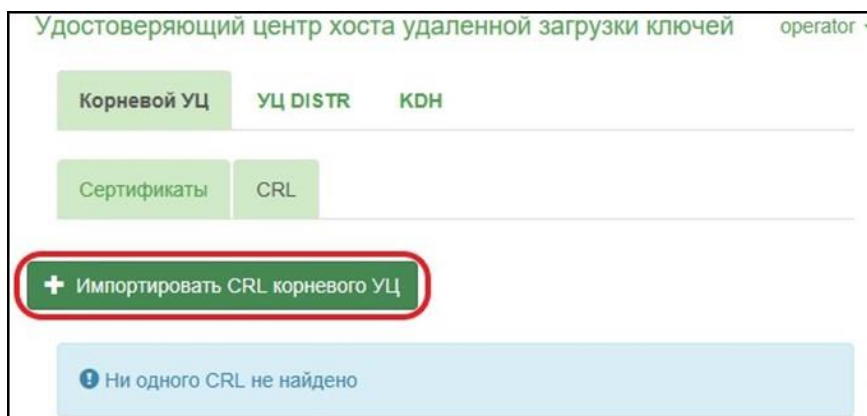


Рисунок 21. Раздел «Корневой УЦ». Вкладка «CRL». Кнопка "Импортировать сертификат корневого УЦ"

На отобразившейся странице «Импорт CRL корневого УЦ – шаг 1» необходимо нажать кнопку «Выберите файл» и выбрать файл сертификата корневого УЦ (Рисунок 22. Страница «Импорт CRL корневого УЦ – шаг 1». Кнопка «Выберите файл»).

Если файл CRL корневого УЦ был экспортирован в формате «base64», то необходимо выставить флаг в чек боксе «Импортировать в base64».

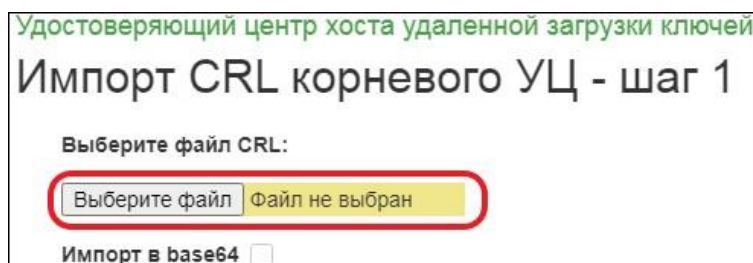


Рисунок 22. Страница «Импорт CRL корневого УЦ – шаг 1». Кнопка «Выберите файл»

После выбора файла отобразится информация о импортируемом CRL и появится кнопка «Импортировать», нажимаем её (Рисунок 23. Страница "Импорт CRL корневого УЦ - шаг 1". Кнопка «Импортировать»).



Рисунок 23. Страница "Импорт CRL корневого УЦ - шаг 1". Кнопка «Импортировать»

В отобразившемся окне «Импорт корневого сертификата – заключительный шаг» нужно нажать кнопку «Готово» (Рисунок 24. Страница "Импорт CRL корневого УЦ - заключительный шаг").

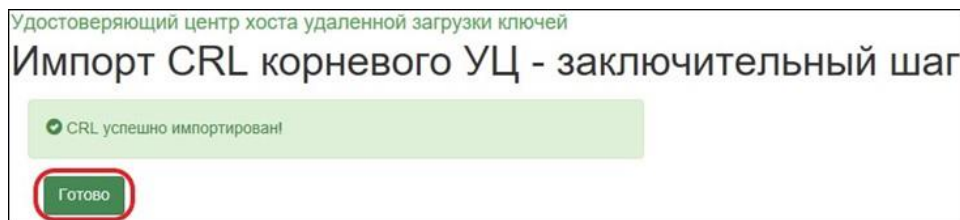


Рисунок 24. Страница "Импорт CRL корневого УЦ - заключительный шаг"

После нажатия кнопки «Готово» отобразится вкладка «Сертификаты» с импортированным сертификатом корневого УЦ (Рисунок 25. Отображение импортированного CRL корневого УЦ).

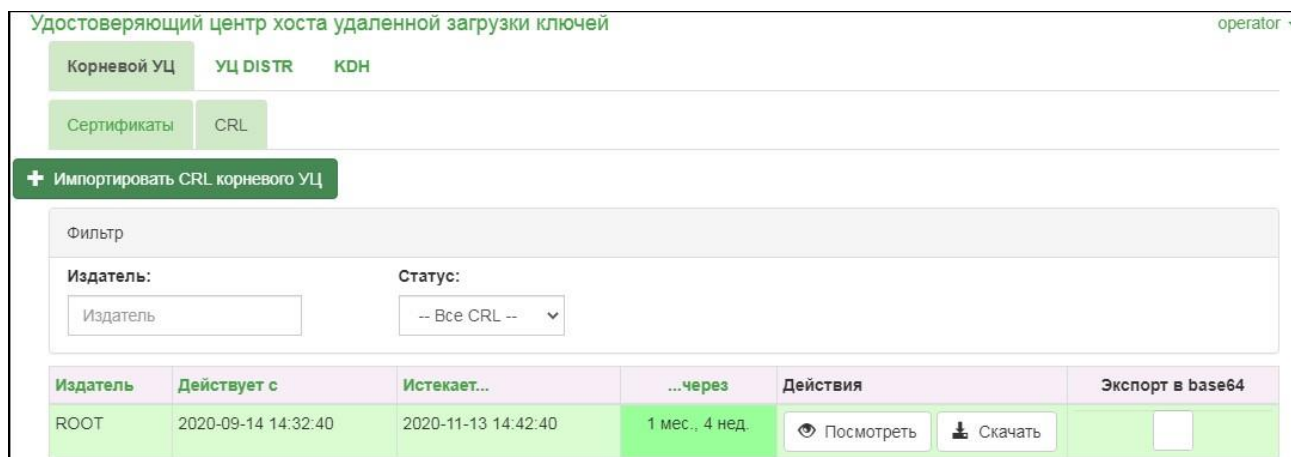


Рисунок 25. Отображение импортированного CRL корневого УЦ

Если необходимо выполнить экспорт загруженного CRL, для этого нужно нажать кнопку «Посмотреть» или «Скачать» в столбце «Действия». Далее сохраняем файл CRL в нужную нам директорию на компьютере. Для выгрузки CRL в формате «base64» необходимо установить флаг в чекбокс в столбце «Экспорт в base64».

9. Создание запроса на сертификат, импорт сертификата, создание CRL в разделе УЦ Distr

9.1. Создание запроса на сертификат УЦ Distr

Перед импортом сертификата необходимо выпустить файл запроса на получение сертификата. Для этого необходимо в системе «Удостоверяющего центра хоста удаленной загрузки ключей» перейти на вкладку «УЦ Distr» вкладка «Запросы» и нажать на кнопку «Создать запрос на сертификат» (Рисунок 26. Выпуск файла запроса на сертификат).



Рисунок 26. Выпуск файла запроса на сертификат

Далее на отобразившейся странице «Создание запроса на сертификат – шаг 1» нужно заполнить все поля, а именно (Рисунок 27. Страница «Создание запроса на сертификат – шаг 1»):

Примечание.

Все значения должны быть введены латинскими буквами.

- **Наименование** – указывается наименование сертификата;
- **E-mail** – указывается электронная почта организации, выпускающей данный сертификат;
- **Подразделение** – указывается название подразделения, выпускающего данный сертификат;
- **Организация** - указывается название организации, выпускающей данный сертификат;
- **Город** - указывается название города, в котором находится организация, выпускающая данный сертификат;
- **Страна** - указывается страна, в котором находится организация, выпускающая данный сертификат;

Примечание.

Поле «Страна» поддерживает ввод только двух символов (например, «RU»).

- **Область публикации CRL:**
 - **URL-папка** – указывается путь, куда будет публиковаться CRL;
 - **Имя файла** – указывается имя файла CRL при публикации. Заполняется автоматически, при заполнении поля «Наименование»;

Удостоверяющий центр хоста удаленной загрузки ключей

Создание запроса на сертификат - шаг 1

Наименование: * DISTR

e-mail: ca_distr@mail.ru

Подразделение: Security Department

Организация: INPAS

Город: Moscow

Страна: * RU

Адрес публикации CRL

URL-папка: http://ca.inpas.ru/crl/ Имя файла: DISTR.crl

Отмена **Далее →**

Рисунок 27. Страница «Создание запроса на сертификат – шаг 1»

После заполнения всех полей нажимаем кнопку «Далее».

Отобразится страница «Создание запроса на сертификат – шаг 2», в верхней части которой представлены параметры создаваемого запроса, в нижней части страницы отображаются поля «Логин» и «Пароль» для подтверждения офицерами безопасности выпуска файла запроса сертификата (Рисунок 28. Страница "Создание запроса на сертификат - шаг 2").

Удостоверяющий центр хоста удаленной загрузки ключей operator ▾

Создание запроса на сертификат - шаг 2

Параметры создаваемого сертификата:

Наименование:	DISTR	Алгоритм ключа:	RSA
e-mail:	ca_distr@mail.ru	Размер ключа (бит):	2048
Подразделение:	Security Departme	Признак УЦ:	Да
Организация:	Inpas	Длина цепочки сертификации:	не ограничена
Город:	Moscow	Использование ключа:	134
Страна:	RU		

Адрес публикации CRL:

Введите логин и пароль уполномоченных офицеров безопасности
Осталось получить подтверждение от 2 офицеров из 2

Логин:

Пароль:

Рисунок 28. Страница "Создание запроса на сертификат - шаг 2"

Далее необходимо ввести логин и пароль и вставить смарт-карту в картридер первого офицера безопасности и нажать кнопку «**Проверить**» (Рисунок 29. Подтверждение первым офицером безопасности).

Введите логин и пароль уполномоченных офицеров безопасности
Осталось получить подтверждение от 2 офицеров из 2

Логин:

Пароль:

Рисунок 29. Подтверждение первым офицером безопасности

Далее необходимо ввести логин и пароль и вставить смарт-карту в картридер второго офицера безопасности и нажать кнопку «**Проверить**» (Рисунок 30. Подтверждение вторым офицером безопасности).

Введите логин и пароль уполномоченных офицеров безопасности
Осталось получить подтверждение от 1 офицера из 2

Логин:

officer2

Пароль:

.....

Проверить

Рисунок 30. Подтверждение вторым офицером безопасности

После второй проверки в нижней части экрана станет доступна кнопка «Генерировать», нажимаем на неё (Рисунок 31. Кнопка "Генерировать").

Удостоверяющий центр хоста удаленной загрузки ключей operator

Создание запроса на сертификат - шаг 2

Параметры создаваемого сертификата:

Наименование:	DISTR	Алгоритм ключа:	RSA
e-mail:	ca_distr@mail.ru	Размер ключа (бит):	2048
Подразделение:	Security Departarr	Признак УЦ:	Да
Организация:	Inpas	Длина цепочки сертификации:	не ограничена
Город:	Moscow	Использование ключа:	134
Страна:	RU		
Адрес публикации CRL:	http://ca.inpas.ru/crl/DISTR.crl		

Отмена ← Назад **Генерировать →**

Рисунок 31. Кнопка "Генерировать"

В отобразившемся окне «Создание запроса на сертификат – заключительный шаг» нужно нажать кнопку «Готово» (Рисунок 32. Страница "Создание запроса на сертификат - заключительный шаг").

Удостоверяющий центр хоста удаленной загрузки ключей

Создание запроса на сертификат - заключительный шаг

✔ Запрос успешно создан!

Готово

Рисунок 32. Страница "Создание запроса на сертификат - заключительный шаг"

После нажатия кнопки «Готово» отобразится вкладка «Запросы» раздела «УЦ Distr» с созданным запросом на сертификат (Рисунок 33. Отображение созданного запроса на сертификат УЦ Distr).

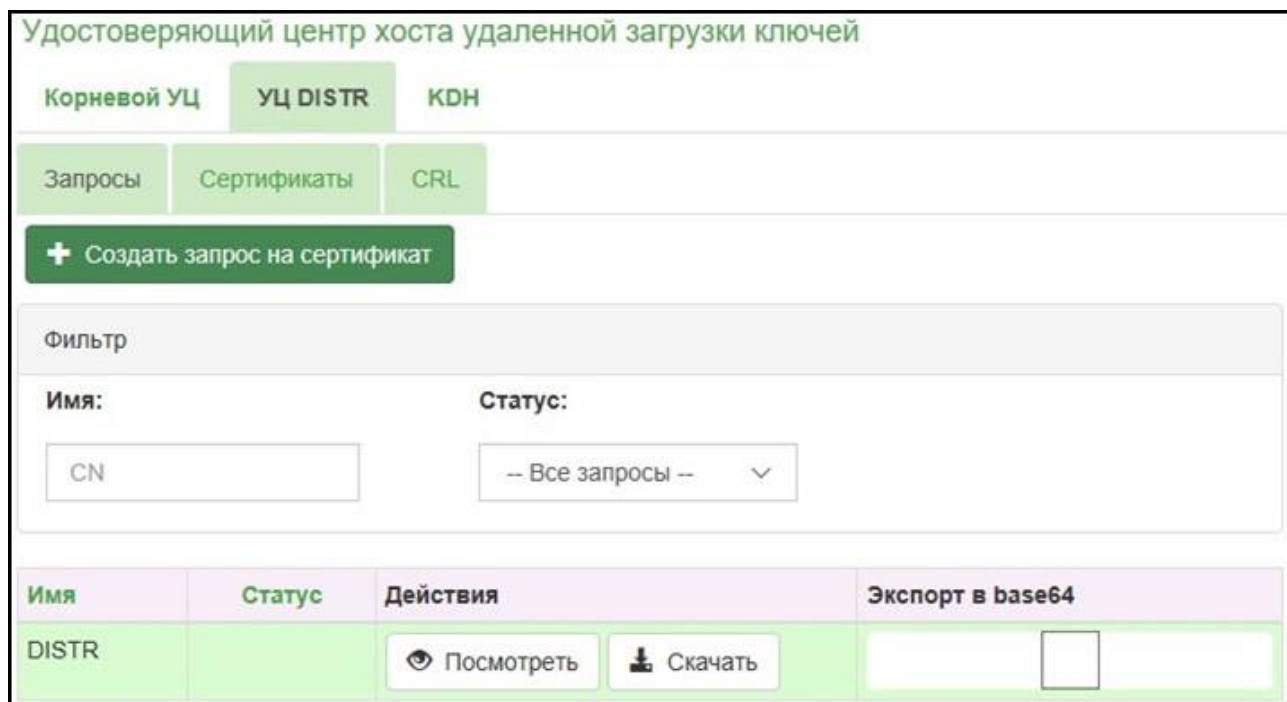


Рисунок 33. Отображение созданного запроса на сертификат УЦ Distr

Далее необходимо выполнить экспорт созданного запроса на выпуск сертификата, для этого нужно нажать кнопку «**Посмотреть**» или «**Скачать**» в столбце «**Действия**». Далее сохраняем файл запроса на выпуск сертификата в нужную нам директорию на компьютере. Для выгрузки созданного запроса на выпуск сертификата в формате «**base64**» необходимо установить флаг в чекбокс в столбце «**Экспорт в base64**». В дальнейшем этот файл понадобится для импорта его в «**Корневой Удостоверяющий центр Инпас**».

9.2. Импорт сертификата УЦ Distr

Для импорта сертификата УЦ Distr необходимо выпустить файл сертификата в системе «**Корневой Удостоверяющий центр Инпас (УЦ Root)**». Данную информацию можно найти в документе «**Руководство пользователя Корневого УЦ**».

После получения сертификата необходимо перейти на вкладку «**Сертификаты**» раздела «**УЦ Distr**» и нажать на кнопку «**Импортировать сертификат УЦ Distr**» (Рисунок 34. Импорт сертификата УЦ Distr).

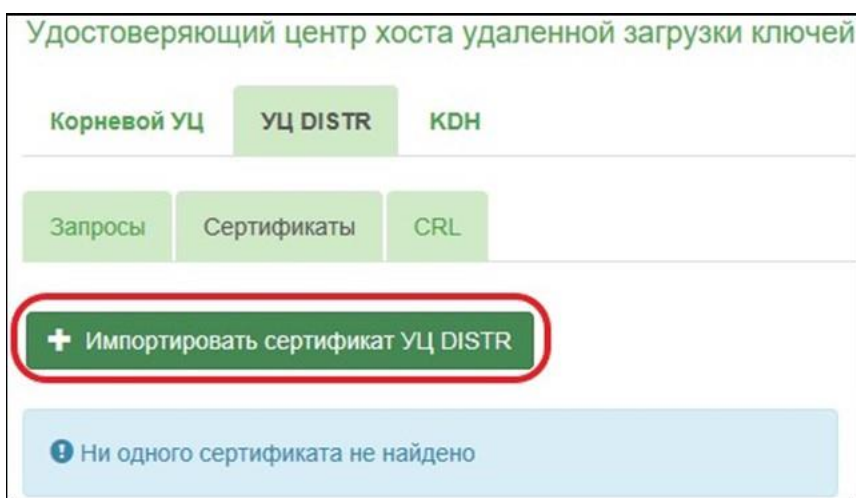


Рисунок 34. Импорт сертификата УЦ Distr

На отобразившейся странице «**Импорт сертификата – шаг 1**» необходимо нажать кнопку «**Выберите файл**» и выбрать файл сертификата (Рисунок 35. Страница «Импорт сертификата». Кнопка «Выберите файл»).

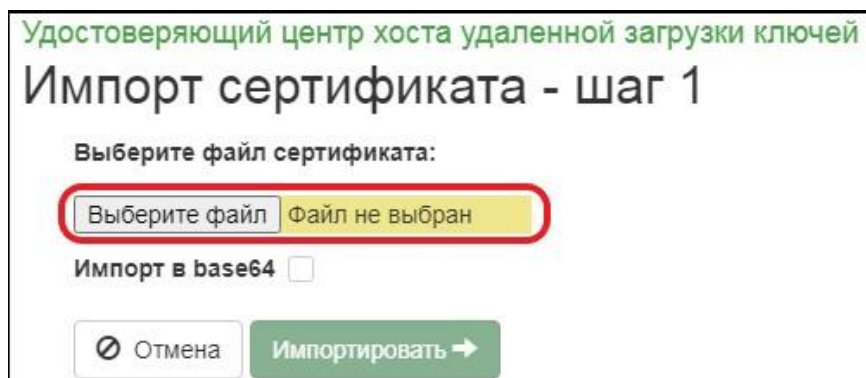


Рисунок 35. Страница «Импорт сертификата». Кнопка «Выберите файл»

После выбора файла отобразится информация о импортируемом сертификате и появится кнопка «**Импортировать**», нажимаем её (Рисунок 36. Страница "Импорт сертификата - шаг 1". Кнопка «Импортировать»).

Если файл сертификата корневого УЦ был экспортирован в формате «**base64**», то необходимо выставить флаг в чек боксе «**Импортировать в base64**».

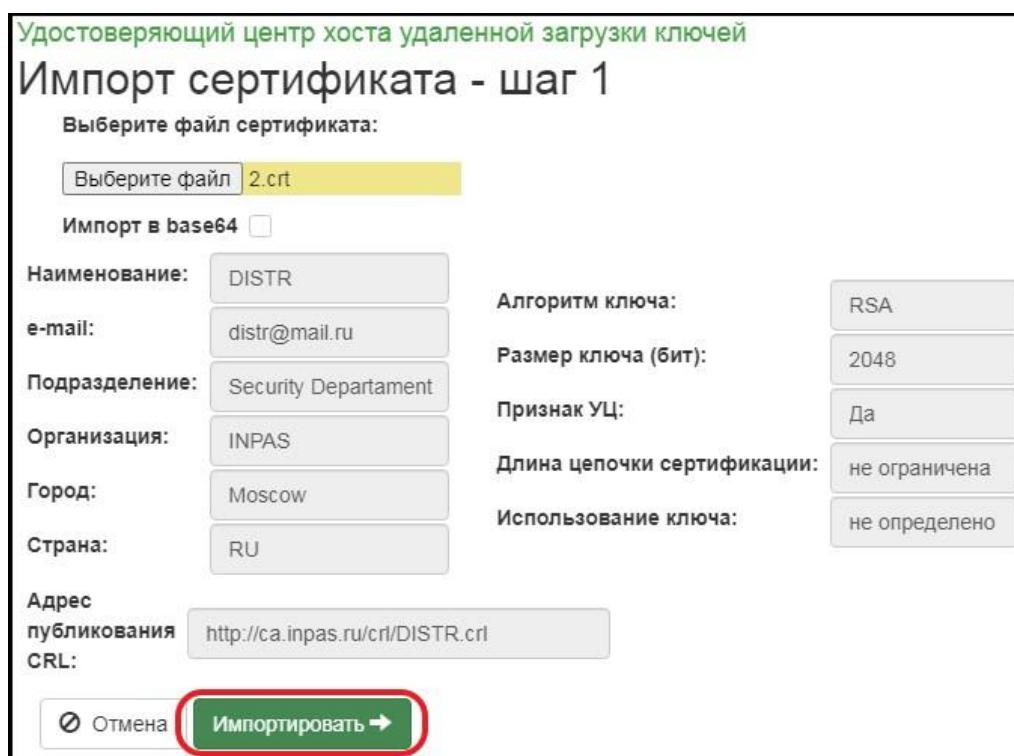


Рисунок 36. Страница "Импорт сертификата - шаг 1". Кнопка «Импортировать»

В отобразившемся окне «**Импорт сертификата – заключительный шаг**» нужно нажать кнопку «**Готово**» (Рисунок 37. Страница "Импорт сертификата - заключительный шаг").

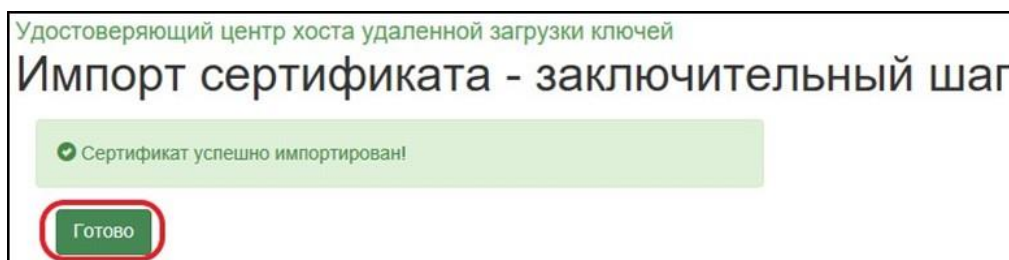


Рисунок 37. Страница "Импорт сертификата - заключительный шаг"

После нажатия кнопки «**Готово**» отобразится вкладка «**Сертификаты**» раздела «**УЦ Distr**» с импортированным сертификатом УЦ Distr (Рисунок 38. Отображение импортированного сертификата корневого УЦ).

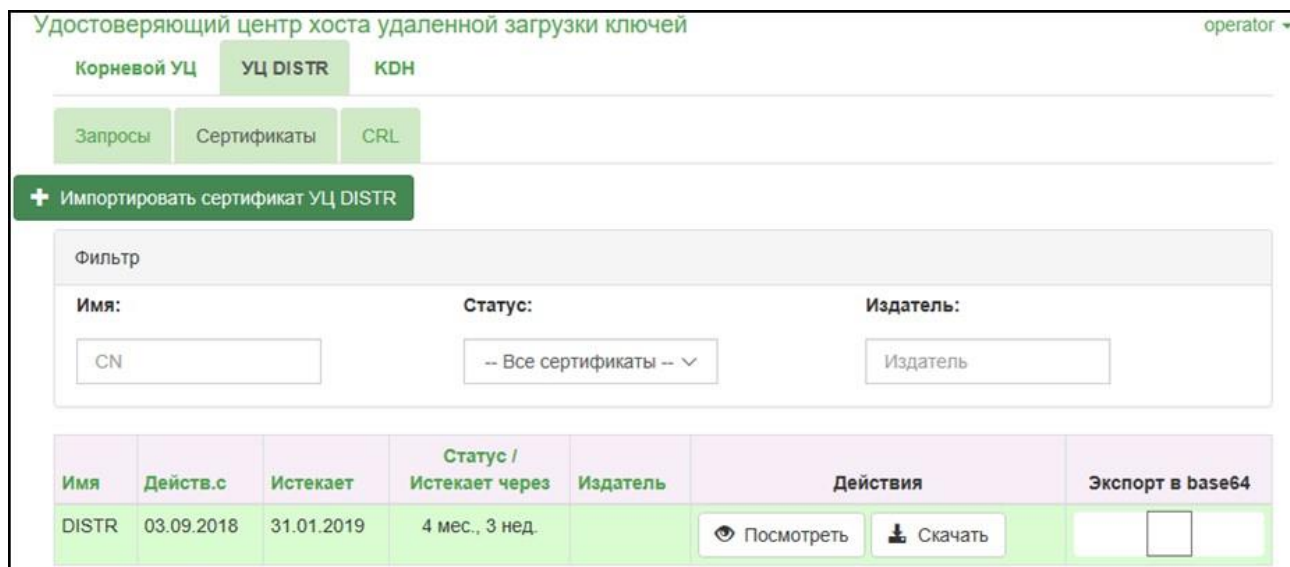


Рисунок 38. Отображение импортированного сертификата корневого УЦ

Далее необходимо выполнить экспорт созданного сертификата, для этого нужно нажать кнопку «Посмотреть» или «Скачать» в столбце «Действия». Для экспорта загруженного сертификата в формате «base64» необходимо установить флаг в чекбокс в столбце «Экспорт в base64». Далее сохраняем файл сертификата в нужную нам директорию на компьютере. В дальнейшем этот файл понадобится для импорта его в «Хост удаленной загрузки ключей».

9.3. Выпуск CRL

После выпуска сертификата УЦ Distr необходимо выпустить список отозванных сертификатов «CRL». Для этого нужно перейти на вкладку «CRL», расположенную в разделе «УЦ Distr» и нажать кнопку «Создание CRL» (Рисунок 39. Вкладка "CRL").

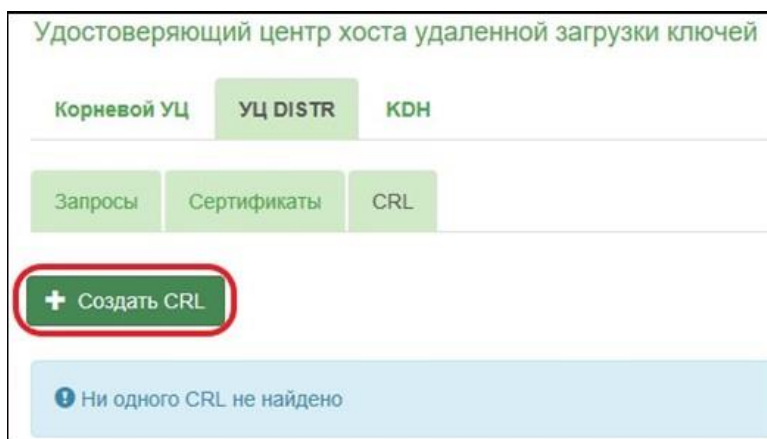


Рисунок 39. Вкладка "CRL"

На отобразившейся странице «Создание CRL – шаг 1» нужно выбрать сертификат издателя CRL из выпадающего списка (Рисунок 41. Страница "Создание CRL - шаг 1").

Если CRL издается впервые, то система отобразит информационное сообщение «CRL до сих пор не издан! Необходимо срочно издать CRL.» (Рисунок 40. Информационное сообщение о неизданном CRL).



Рисунок 40. Информационное сообщение о неизданном CRL

После выбора сертификата издателя CRL отобразится строка «Задайте срок действия нового CRL», в которой необходимо указать срок действия CRL в днях. В строках «Начало» и «Окончание»

отобразится дата начала и окончания действия сертификата. Следующим шагом нужно нажать кнопку «Далее» (Рисунок 41. Страница "Создание CRL - шаг 1").

Рисунок 41. Страница "Создание CRL - шаг 1"

Отобразится страница «Создание CRL – шаг 2», на которой будет информация о создаваемом CRL, а также поля «Логин» и «Пароль» для подтверждения офицерами безопасности выпуска CRL.

Далее вводим логин и пароль и вставляем смарт-карту в картридер поочередно для каждого офицера безопасности и нажимаем кнопку «Проверить» (Рисунок 29. Подтверждение первым офицером безопасности и Рисунок 30. Подтверждение вторым офицером безопасности).

После второй проверки станет доступна кнопка «Генерировать», нажимаем на неё (Рисунок 42. Страница "Создание CRL - шаг 2").

Рисунок 42. Страница "Создание CRL - шаг 2"

В отобразившемся окне «Создание CRL – заключительный шаг» нужно нажать кнопку «Готово» (Рисунок 43. Страница "Создание CRL - заключительный шаг").

Рисунок 43. Страница "Создание CRL - заключительный шаг"

После нажатия кнопки «Готово» отобразится главное окно системы с созданным CRL (Рисунок 44. Отображение созданного CRL).

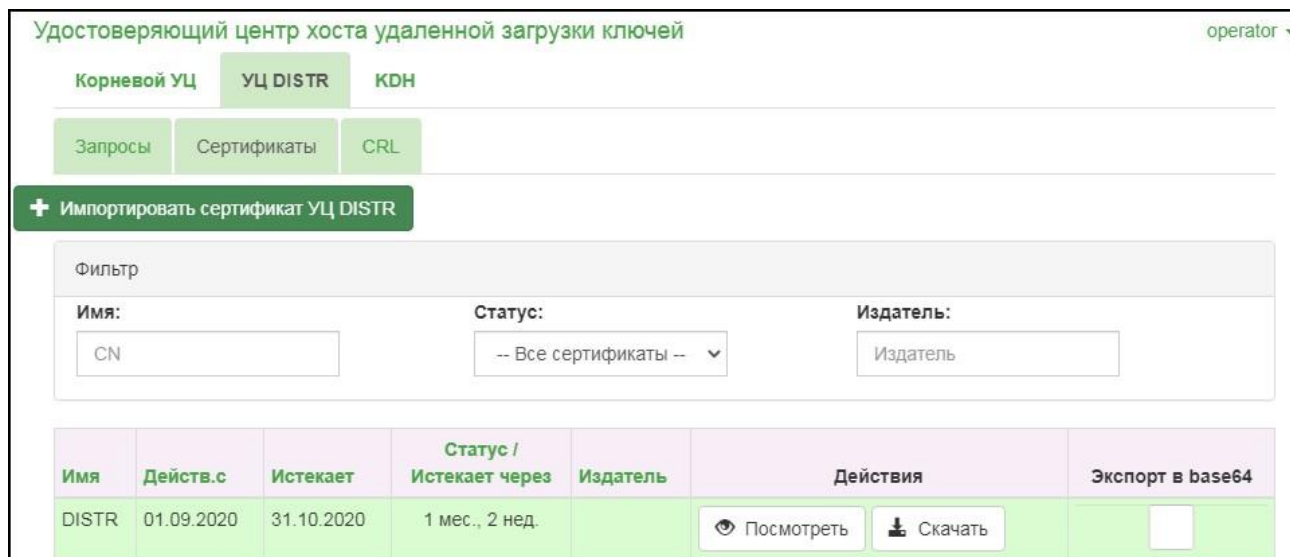


Рисунок 44. Отображение созданного CRL

Далее необходимо выполнить экспорт созданного CRL, для этого нужно нажать кнопку «Посмотреть» или «Скачать» в столбце «Действия». Для экспорта, созданного CRL в формате «base64» необходимо установить флаг в чекбокс в столбце «Экспорт в base64». Далее сохраняем файл сертификата в нужную нам директорию на компьютере. В дальнейшем этот файл понадобится для импорта его в «Хост удаленной загрузки ключей».

10. Выпуск сертификата KDH

Для выпуска сертификата KDH необходимо получить файл запроса на выдачу сертификата. Данную информацию можно найти в документе «KDH_User_Guide».

После получения файла запроса необходимо Перейти в раздел «KDH» вкладка «Сертификаты» и нажать на кнопку «Создать сертификат KDH» (Рисунок 45. Создание сертификата KDH).

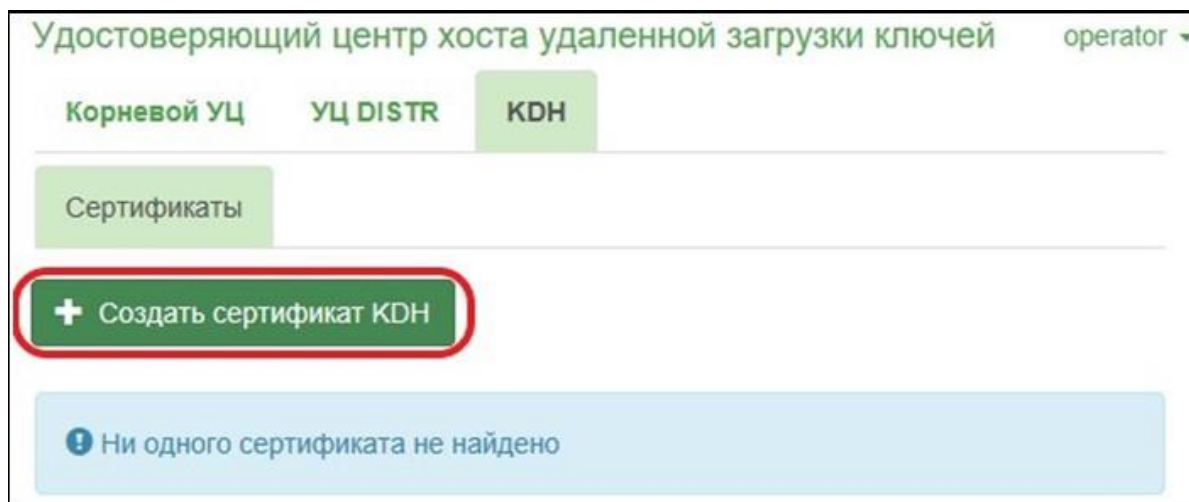


Рисунок 45. Создание сертификата KDH

В отобразившемся окне «Создание сертификата KDH – шаг 1» необходимо выбрать сертификат из выпадающего списка и в появившемся поле «Выберите файл CSR-запроса для сертификата:» нажать на кнопку «Выберите файл» (Рисунок 46. Выбор сертификата издателя и файла запроса).

Удостоверяющий центр хоста удаленной загрузки ключей

Создание сертификата KDH - шаг 1

Выберите сертификат издателя:

DISTR
INPAS, Security Departament, Moscow, RU, distr@mail.ru

Выберите файл CSR-запроса для сертификата:

Выберите файл Файл не выбран

Отмена Далее →

Рисунок 46. Выбор сертификата издателя и файла запроса

После выбора файла запроса система отобразит информацию о создаваемом сертификате и попросит ввести срок действия сертификата в полях «Начало» и «Окончание», нажимаем кнопку «Далее» (Рисунок 47. Страница "Создание сертификата KDH - шаг 1").

Удостоверяющий центр хоста удаленной загрузки ключей

Создание сертификата KDH - шаг 1

Выберите сертификат издателя:

DISTR
Inpas, Security Departament, Moscow, RU, ca_distr@mail.ru

Выберите файл CSR-запроса для сертификата:

C:\Users\an_obukhov\Do Обзор...

Наименование: KDH

e-mail:

Подразделение: DRPP

Организация: INPAS SOFT

Город: Moscow

Страна: RU

Адрес публикации CRL:

Алгоритм ключа: RSA

Размер ключа (бит): 2048

Признак УЦ: Нет

Длина цепочки сертификации: не применимо

Использование ключа: не определено

Задайте срок действия сертификата:

Начало: 04.09.2018 Окончание: 31.01.2019

Отмена Далее →

Рисунок 47. Страница "Создание сертификата KDH - шаг 1"

Далее вводим логин и пароль и вставляем смарт-карту в картридер поочередно для каждого офицера безопасности и нажимаем кнопку «Проверить» (Рисунок 29. Подтверждение первым офицером безопасности и Рисунок 30. Подтверждение вторым офицером безопасности).

После второй проверки станет доступна кнопка «Генерировать», нажимаем на неё (Рисунок 48).
Страница "Создание сертификата KDH - шаг 2").

Рисунок 48. Страница "Создание сертификата KDH - шаг 2"

В отобразившемся окне «Создание сертификата KDH – заключительный шаг» нужно нажать кнопку «Готово» (Рисунок 49. Страница "Создание сертификата KDH - заключительный шаг").

Рисунок 49. Страница "Создание сертификата KDH - заключительный шаг"

После нажатия кнопки «Готово» отобразится главное окно системы с созданным сертификатом подчиненного УЦ (Рисунок 50. Отображение созданного сертификата KDH).

Далее необходимо выполнить экспорт созданного сертификата KDH, для этого нужно нажать кнопку «Скачать» в столбце «Действия». Для сохранения созданного сертификата в формате «base64» необходимо установить флаг в чекбокс в столбце «Экспорт в base64». Далее сохраняем файл сертификата в нужную нам директорию на компьютере. В дальнейшем этот файл понадобится для импорта его в «Хост удаленной загрузки ключей».

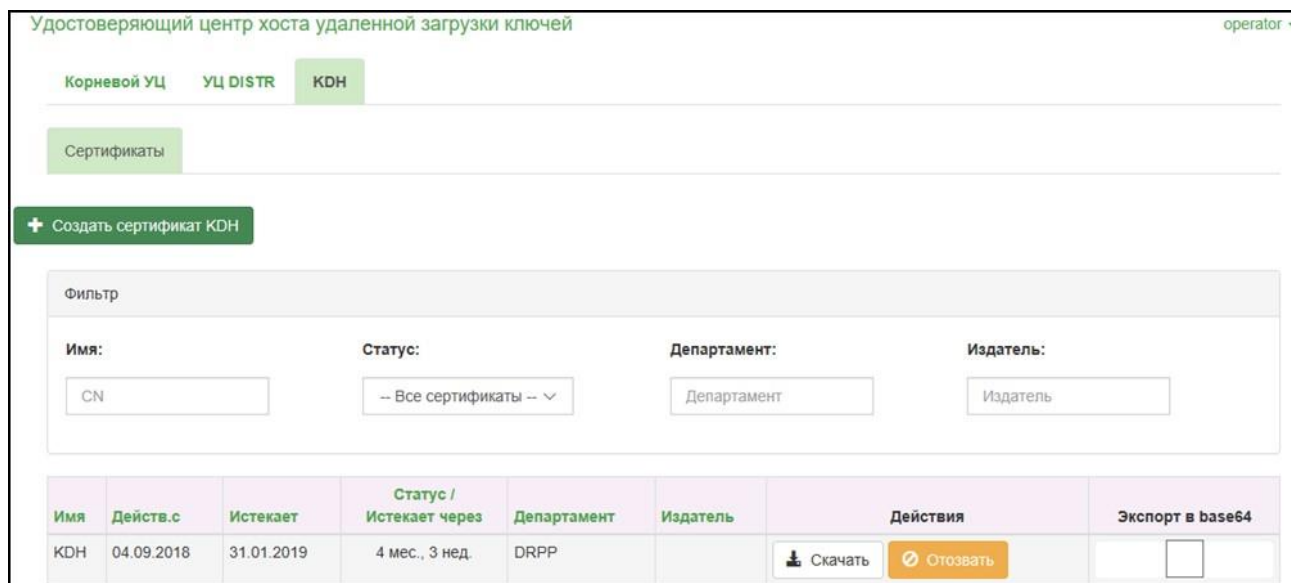


Рисунок 50. Отображение созданного сертификата KDН

11. Изменение настроек

Для изменения настроек «Удостоверяющего центра хоста удаленной загрузки ключей» необходимо пройти авторизацию пользователем с ролью «Администратор».

После успешной авторизации система отобразит меню «Пользователи», где в правом верхнем углу нужно нажать функциональную кнопку пользователя и из выпадающего списка выбрать пункт «Настройки» (Рисунок 51. Переход на страницу «Настройки»).

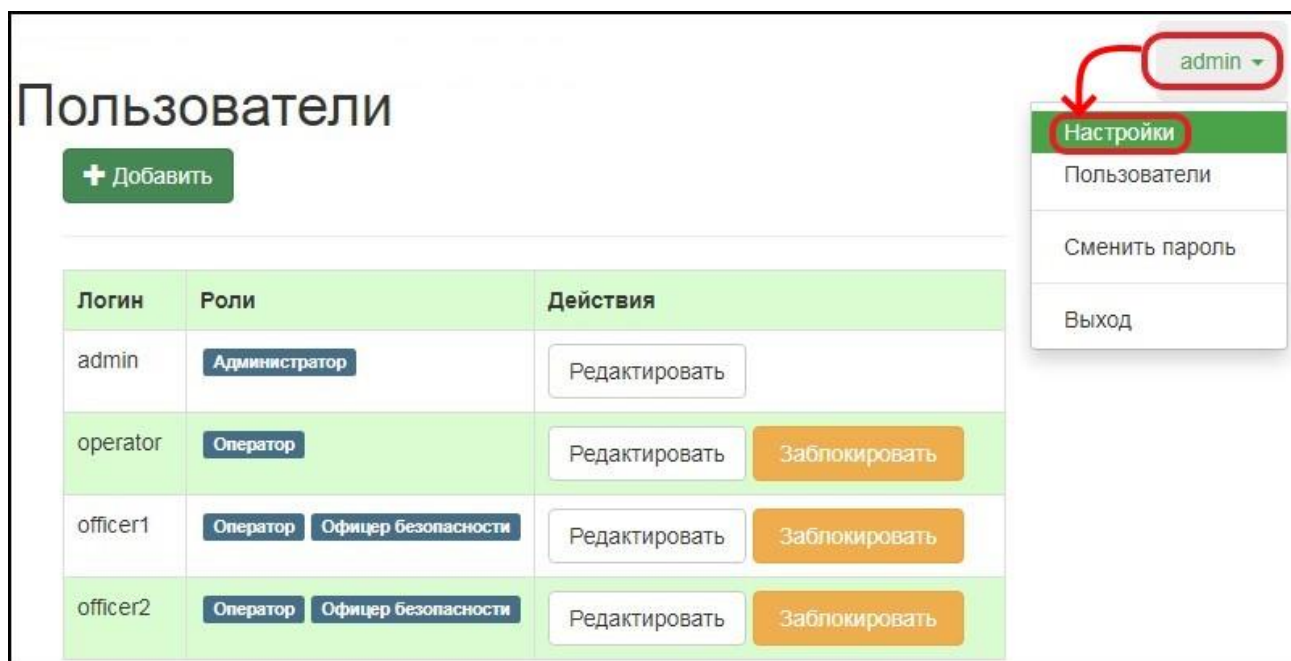


Рисунок 51. Переход на страницу «Настройки»

На отобразившейся странице «Настройки» нужно внести необходимые изменения в параметры и нажать кнопку «Сохранить» (Рисунок 52. Страница "Настройки").

Ниже описано название параметров и их назначение:

- **HSM_ADDRESS** – устанавливает IP-адрес хоста HSM;
- **HSM_PORT** – устанавливает порт хоста HSM;
- **OFFICERS_REQUIRED** – устанавливает количество офицеров безопасности для выпуска сертификатов;

- **LOG_EXPORT_DIRECTORY** – устанавливает директорию, куда будут экспортироваться логи с подписью из базы данных;
- **LMK_ID** – указывает, в какой ячейке хранится ключ «**Variant LMK**»;
- кнопка «Сменить сертификат подписи логов» - позволяет повторно сгенерировать сертификат для подписи логов с сохранением файла «log_cipher_key.txt».

Настройки

HSM_ADDRESS:

HSM_PORT:

OFFICERS_REQUIRED:

LOG_EXPORT_DIRECTORY:

LMK_ID:

Сменить сертификат подписи логов

Отмена Сохранить

Рисунок 52. Страница "Настройки"