

Корневой Удостоверяющий Центр

Руководство пользователя

Версия УЦ 2.2.0

История изменений документа

Версия	Дата	Перечень изменений
1.0	30.08.2018	Первоначальная версия
1.1	14.09.2020	Актуализация скриншотов и добавление информации о выгрузке/загрузке сертификатов/CRL в формате base64. Добавлен пункт 10

Содержание

1. Используемые сокращения и обозначения	4
2. Введение	4
3. Краткое описание Корневого Удостоверяющего центра ИНПАС	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. Создание сертификатов и CRL в разделе – X509.....	12
8.1. Выпуск корневого сертификата (X509)	12
8.2. Выпуск CRL (X509)	16
8.3. Выпуск сертификата подчиненного УЦ (X509)	18
9. Создание сертификатов в разделе EMV	21
9.1. Выпуск корневого сертификата (EMV).....	21
9.2. Выпуск сертификата подчиненного УЦ (EMV).....	23
10. Изменение настроек.....	25

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 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 Корневого Удостоверяющего центра ИНПАС и порядок работы с ним.

Данный документ предназначен для прочтения пользователем, осуществляющим работу с Корневым Удостоверяющим центром ИНПАС через web-интерфейс.

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

3. Краткое описание Корневого Удостоверяющего центра ИНПАС

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

Основные функции системы:

- Формирование и удостоверение самоподписанного сертификата публичного ключа для УЦ Root;
- Хранение и предоставление сертификата своего публичного ключа;
- Прием запросов на выдачу сертификатов публичного ключа для УЦ Prod;
- Удостоверение сертификата публичного ключа для УЦ Prod;
- Прием запросов на выдачу сертификатов публичного ключа для УЦ Distr;
- Удостоверение сертификата публичного ключа для УЦ Distr;
- Формирование, удостоверение и предоставление списка отозванных сертификатов (CRL) УЦ Distr и УЦ Prod.

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

4. Описание web-интерфейса

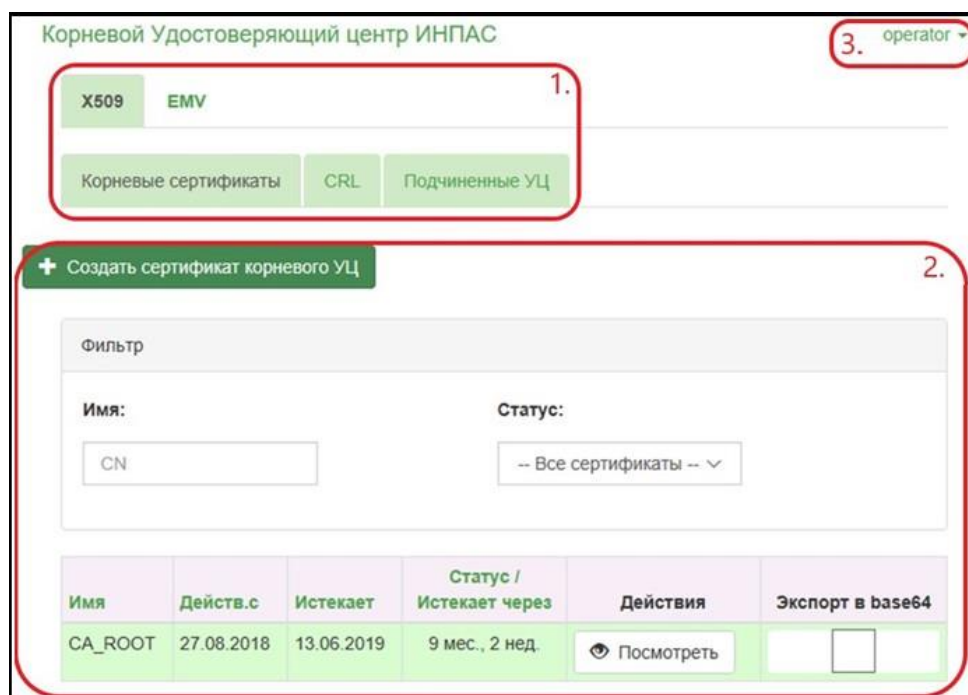


Рисунок 1. Главное окно системы "Корневого Удостоверяющего центра ИНПАС"

Web-интерфейс системы «Корневого Удостоверяющего центра Инпас» представляет собой страницу, содержащую следующие элементы:

1. Главное меню, состоящее из следующих разделов:
 - **X509** – позволяет выполнить выпуск цепочек SSL сертификатов;
 - **Корневые сертификаты** - формирование и удостоверение самоподписанного сертификата публичного ключа;
 - **CRL** - формирование, удостоверение и предоставление списка отозванных сертификатов (CRL) УЦ Distr и УЦ Prod;
 - **Подчиненные УЦ** - формирование, удостоверение и предоставление сертификатов УЦ Distr.
 - **EMV** – позволяет выполнять выпуск цепочек сертификатов для взаимодействия терминала и пинпада;
 - **Корневые сертификаты** - формирование и удостоверение самоподписанного сертификата публичного ключа;
 - **Подчиненные УЦ** - формирование, удостоверение и предоставление сертификатов УЦ Prod.
2. Основное содержание вкладки.
 - **Создание сертификата корневого УЦ** (назначение кнопки изменяется в зависимости от выбранной вкладки);
 - **Фильтра** – 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;
 - **Действия** – отображается кнопка «Посмотреть», «Скачать», при нажатии на которую выполняется экспорт сертификата;

- **Экспорт в base64** – при выставлении флага в чекбоксе 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).

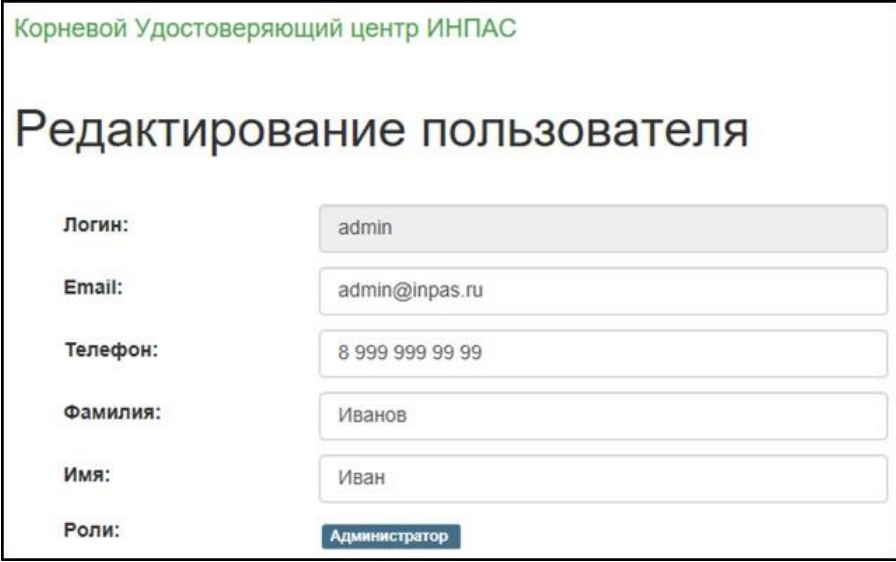
Логин	Роли	Действия
admin	Администратор	Редактировать

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").



Корневой Удостоверяющий центр ИНПАС

Редактирование пользователя

Логин: admin

Email: admin@inpas.ru

Телефон: 8 999 999 99 99

Фамилия: Иванов

Имя: Иван

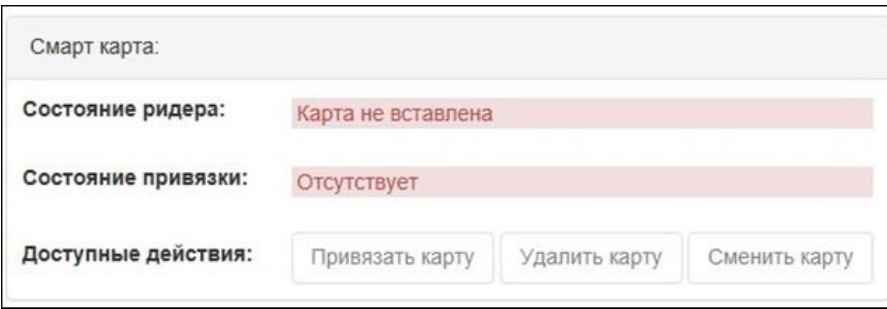
Роли: Администратор

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».



Смарт карта:

Состояние ридера: Карта не вставлена

Состояние привязки: Отсутствует

Доступные действия: Привязать карту Удалить карту Сменить карту

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).

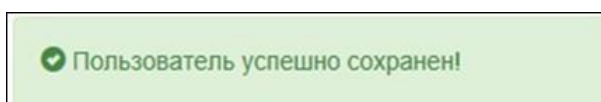


Рисунок 9. Информационное сообщение об успешном сохранении пользователя

7. Регистрация пользователей

После того как выполнили регистрацию системного администратора, необходимо добавить других пользователей для работы с системой «Корневого Удостоверяющего центра Инпас».

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 «Корневой Удостоверяющий центр Инпас» как системный администратор, отобразится страница «Пользователи», где нужно нажать кнопку «Добавить» (Рисунок 10. Страница "Пользователи". Добавление пользователя).

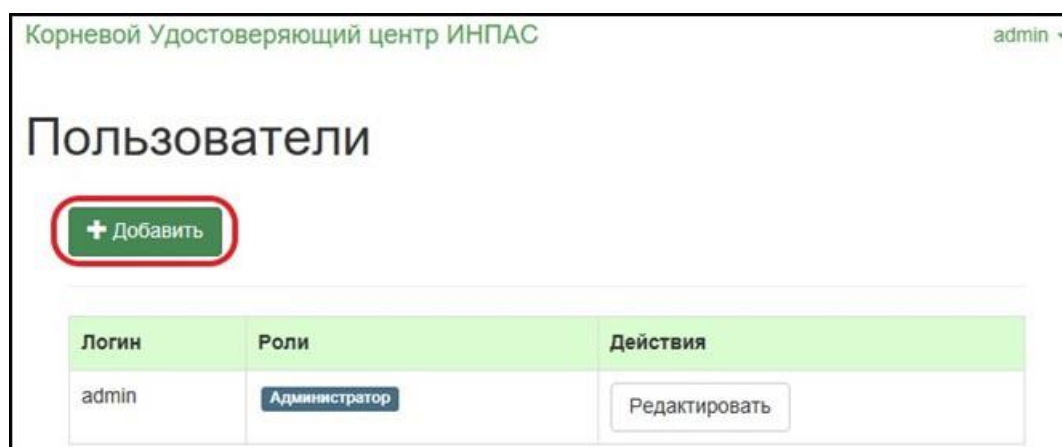


Рисунок 10. Страница "Пользователи". Добавление пользователя

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 «НСМ»;
 - 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).

Корневой Удостоверяющий центр ИНПАС

Создание нового пользователя

Логин:

Пароль:

Email:

Телефон:

Фамилия:

Имя:

Роли: ☒ Администратор ☐ Оператор ☐ Офицер безопасности

Смарт карта:

Состояние ридера: 1.

Состояние привязки:

Доступные действия:

2.

Смарт карта:

Состояние ридера:

Состояние привязки:

Доступные действия:

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").

Корневой Удостоверяющий центр ИНПАС 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").

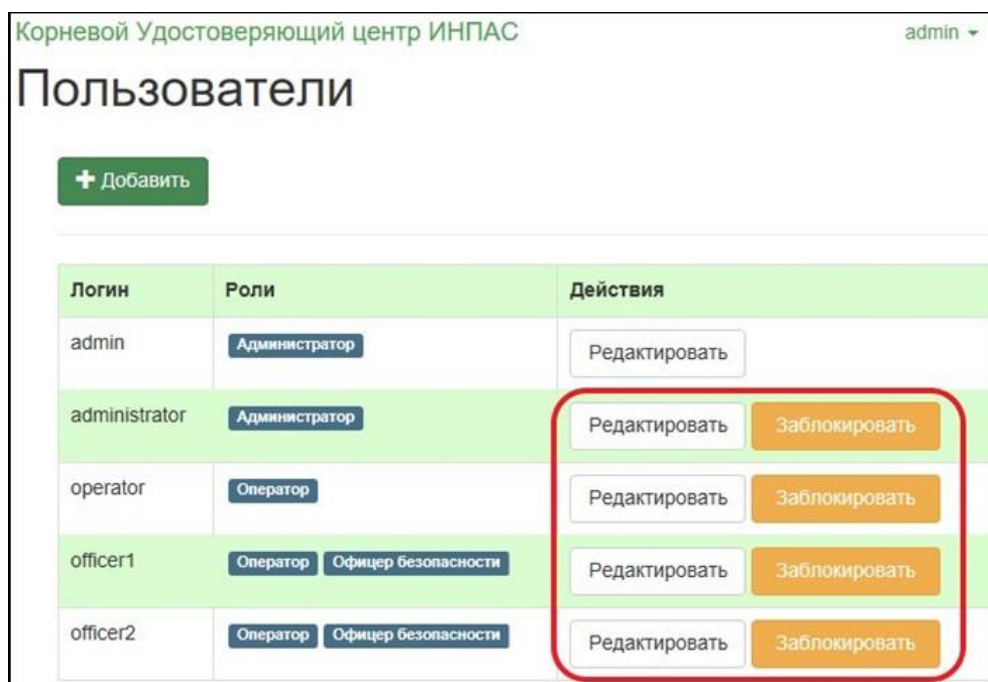


Рисунок 13. Кнопки "Редактировать" и "Заблокировать"

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).

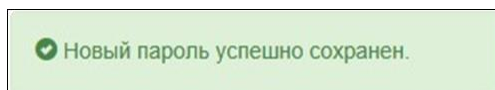


Рисунок 15. Информационное сообщение об успешном сохранении нового пароля

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

8. Создание сертификатов и CRL в разделе – X509

8.1. Выпуск корневого сертификата (X509)

Для выпуска корневого сертификата для УЦ Root необходимо выполнить авторизацию пользователем с ролью «**Оператор**».

После успешной авторизации система отобразит главное окно (Рисунок 16. Главное окно системы. Кнопка "Создать сертификат корневого УЦ"), где нужно нажать кнопку «**Создать сертификат корневого УЦ**».

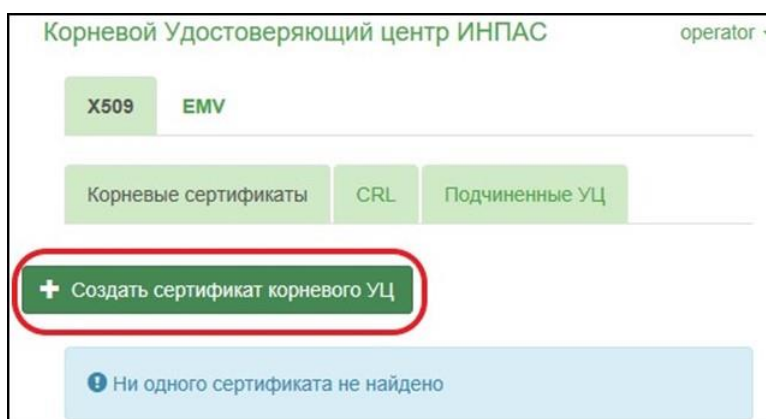


Рисунок 16. Главное окно системы. Кнопка "Создать сертификат корневого УЦ"

На отобразившейся странице «**Создание корневого сертификата – шаг 1**» заполняем все поля, а именно (Рисунок 17. Создание корневого сертификата - 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 которой 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**»;

- **Срок действия сертификата:**
 - **Начало** – указывается дата начала действия сертификата;
 - **Окончание** – указывается дата окончания действия сертификата.

Рисунок 17. Создание корневого сертификата - шаг 1

После заполнения всех полей нажимаем кнопку «**Далее**».

Отобразится страница «**Создание корневого сертификата – шаг 2**», в верхней части которой представлены параметры создаваемого сертификата (Рисунок 18. Верхняя часть страницы «Создание корневого сертификата - шаг 2»).

Рисунок 18. Верхняя часть страницы «Создание корневого сертификата - шаг 2»

В нижней части страницы «**Создание корневого сертификата – шаг 2**» отображаются поля «**Логин**» и «**Пароль**» для подтверждения офицерами безопасности выпуска корневого сертификата УЦ (Рисунок 19. Нижняя часть страницы "Создание корневого сертификата - шаг 2").



Рисунок 19. Нижняя часть страницы "Создание корневого сертификата - шаг 2"

Далее необходимо ввести логин и пароль и вставить смарт-карту в картридлер первого офицера безопасности и нажать кнопку «**Проверить**» (Рисунок 20. Подтверждение первым офицером безопасности).

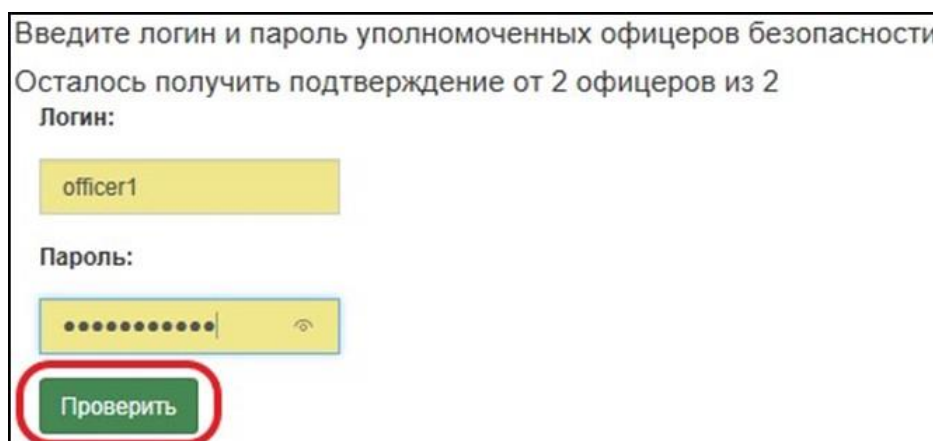


Рисунок 20. Подтверждение первым офицером безопасности

Далее необходимо ввести логин и пароль и вставить смарт-карту в картридлер второго офицера безопасности и нажать кнопку «**Проверить**» (Рисунок 21. Подтверждение вторым офицером безопасности).

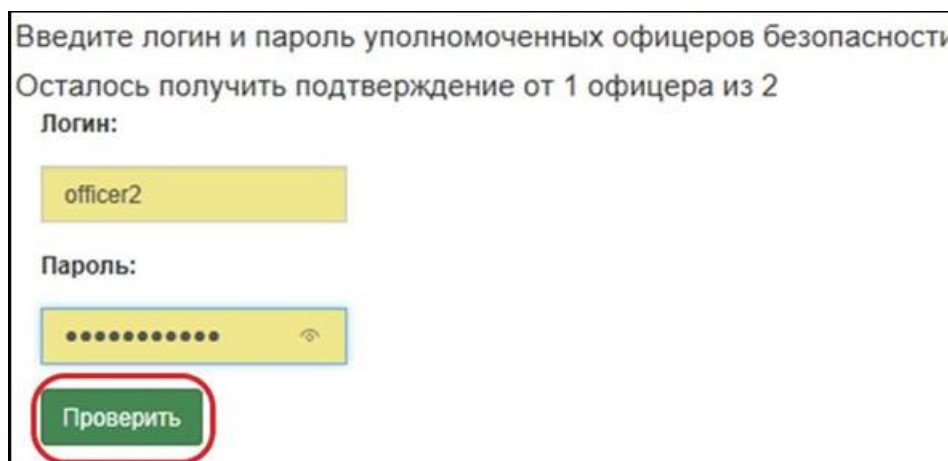


Рисунок 21. Подтверждение вторым офицером безопасности

После второй проверки в нижней части экрана станет доступна кнопка «Генерировать», нажимаем на неё (Рисунок 22. Кнопка "Генерировать").

Корневой Удостоверяющий центр ИНПАС

Создание корневого сертификата - шаг 2

Параметры создаваемого сертификата:

Наименование:	CA_ROOT	Алгоритм ключа:	RSA
e-mail:	CA_root@inpas.ru	Размер ключа (бит):	2048
Подразделение:	Security Department	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/CA_ROOT.crl		

Срок действия сертификата:

Начало:	27.08.2018	Окончание:	13.06.2019
---------	------------	------------	------------

Рисунок 22. Кнопка "Генерировать"

В отобразившемся окне «Создание корневого сертификата – заключительный шаг» нужно нажать кнопку «Готово» (Рисунок 23. Страница "Создание корневого сертификата - заключительный шаг").

Создание корневого сертификата - заключительный шаг

Сертификат успешно сохранен!

Рисунок 23. Страница "Создание корневого сертификата - заключительный шаг"

После нажатия кнопки «Готово» отобразится главное окно системы с созданным сертификатом корневого УЦ (Рисунок 24. Отображение созданного сертификата корневого УЦ).

Далее необходимо выполнить экспорт созданного сертификата, для этого нужно нажать кнопку «Посмотреть» в столбце «Действия». Для загрузки 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 «Удостоверяющий центр хоста удаленной загрузки ключей».

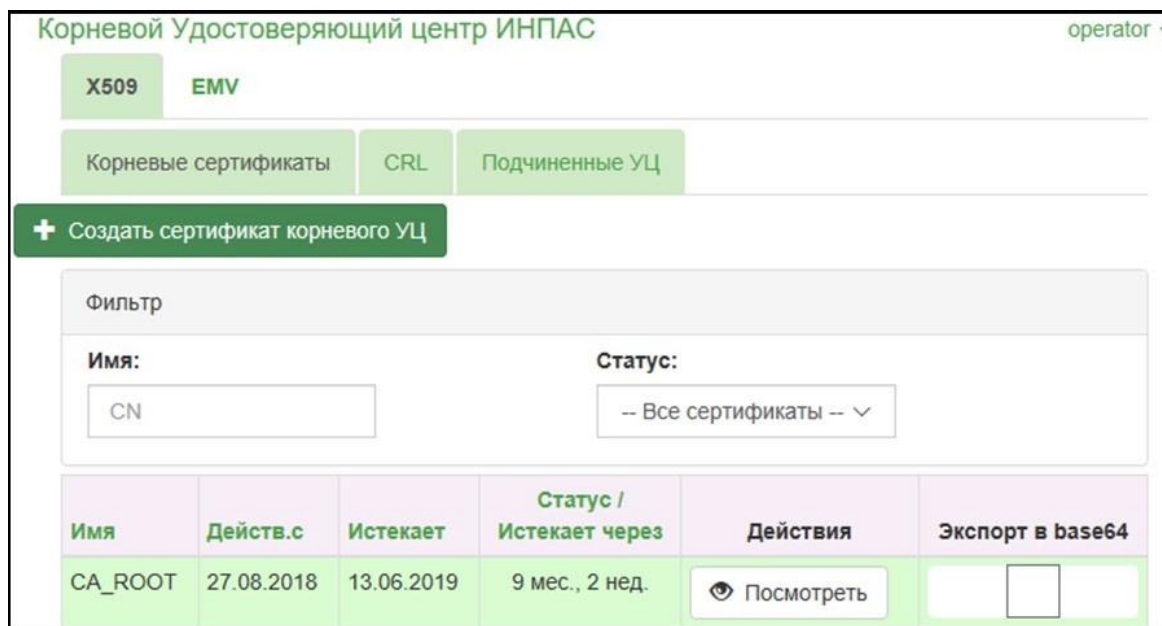


Рисунок 24. Отображение созданного сертификата корневого УЦ

8.2. Выпуск CRL (X509)

После выпуска сертификата корневого УЦ необходимо выпустить список отозванных сертификатов «CRL». Для этого нужно перейти на вкладку «CRL», расположенную в разделе «X509» и нажать кнопку «Создание CRL» (Рисунок 25. Вкладка "CRL").

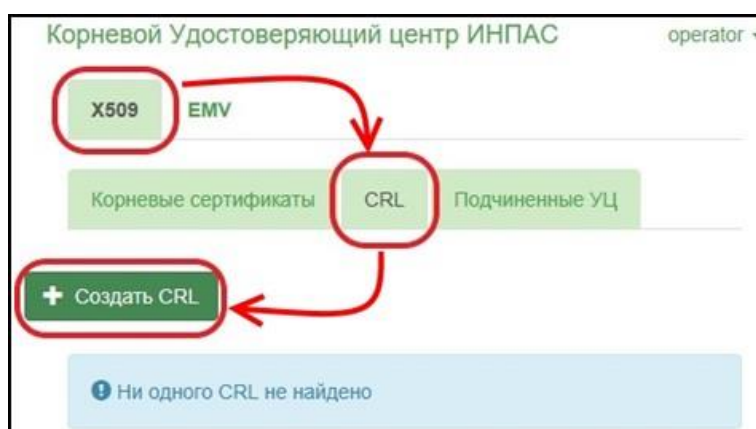


Рисунок 25. Вкладка "CRL"

На отобразившейся странице «Создание CRL – шаг 1» нужно выбрать корневой сертификат издателя CRL из выпадающего списка (Рисунок 27. 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 26. Информационное сообщение о неизданном CRL).



Рисунок 26. 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 27. Страница "Создание CRL - шаг 1").

Рисунок 27. 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 выпуск CRL.

Далее вводим логин и пароль и вставляем смарт-карту в картридер поочередно для каждого офицера безопасности и нажимаем кнопку «**Проверить**» (Рисунок 20. Подтверждение первым офицером безопасности и Рисунок 21. Подтверждение вторым офицером безопасности).

После второй проверки станет доступна кнопка «**Генерировать**», нажимаем на неё (Рисунок 28. Страница "Создание CRL - шаг 2").

Рисунок 28. Страница "Создание CRL - шаг 2"

В отобразившемся окне «**Создание CRL – заключительный шаг**» нужно нажать кнопку «**Готово**» (Рисунок 29. Страница "Создание CRL - заключительный шаг").

Рисунок 29. Страница "Создание CRL - заключительный шаг"

После нажатия кнопки «Готово» отобразится главное окно системы с созданным CRL (Рисунок 30. Отображение созданного CRL).

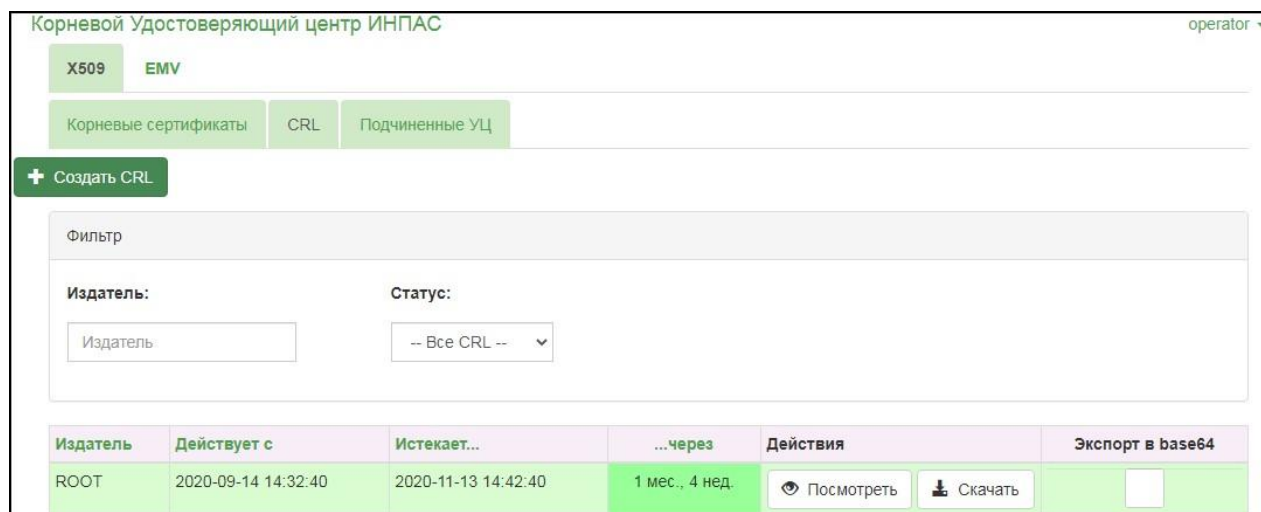


Рисунок 30. Отображение созданного CRL

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

8.3. Выпуск сертификата подчиненного УЦ (X509)

Для создания сертификата подчиненного УЦ необходимо выпустить файл запроса на получение сертификата подчиненного УЦ. Данную информацию можно найти в документе «Руководство пользователя УЦ хоста удаленной загрузки ключей».

После получения файла запроса, необходимо перейти на вкладку «Подчиненные УЦ» раздела «X509» и нажать на кнопку «Создать сертификат подчиненного УЦ» (Рисунок 31. Создание сертификата подчиненного УЦ).

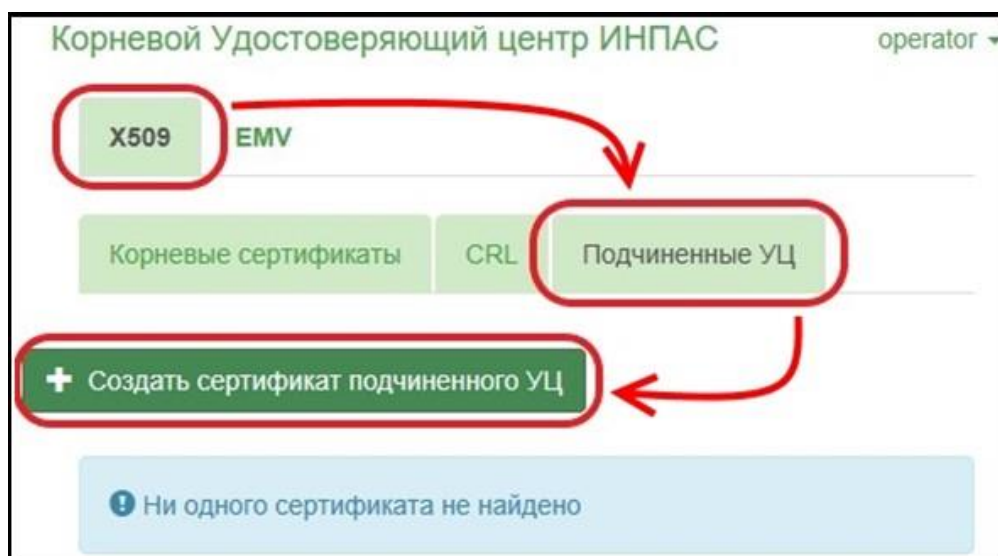


Рисунок 31. Создание сертификата подчиненного УЦ

В отобразившемся окне «Создание подчиненного сертификата – шаг 1» необходимо выбрать сертификат издателя из выпадающего списка и в появившемся поле «Выберите файл CSR-запроса для сертификата:» нажимаем на кнопку «Выберите файл» (Рисунок 32. Выбор сертификата издателя и файла запроса).

Рисунок 32. 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 33. Страница "Создание подчиненного сертификата - шаг 1").

Рисунок 33. Страница "Создание подчиненного сертификата - шаг 1"

Далее вводим логин и пароль и вставляем смарт-карту в картридер поочередно для каждого офицера безопасности и нажимаем кнопку «Проверить» (Рисунок 20. Подтверждение первым офицером безопасности и Рисунок 21. Подтверждение вторым офицером безопасности).

После второй проверки станет доступна кнопка «Генерировать», нажимаем на неё (Рисунок 34. Страница "Создание подчиненного сертификата - шаг 2").

Корневой Удостоверяющий центр ИНПАС

Создание подчиненного сертификата - шаг 2

Сертификат издателя: CA_ROOT (Security Department, INPAS, Moscow, RU, CA_root@inpas.ru)

Параметры создаваемого сертификата:

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

Адрес публикации CRL:

Срок действия сертификата:

Начало:	30.08.2018	Окончание:	31.12.2018
---------	------------	------------	------------

Рисунок 34. Страница "Создание подчиненного сертификата - шаг 2"

В отобразившемся окне «Создание подчиненного сертификата – заключительный шаг» нужно нажать кнопку «Готово» (Рисунок 35. Страница "Создание подчиненного сертификата - заключительный шаг").

Корневой Удостоверяющий центр ИНПАС

Создание подчиненного сертификата - заключительный шаг

Сертификат успешно сохранен!

Рисунок 35. Страница "Создание подчиненного сертификата - заключительный шаг"

После нажатия кнопки «Готово» отобразится главное окно системы с созданным сертификатом подчиненного УЦ (Рисунок 36. Отображение созданного сертификата подчиненного УЦ).

Корневой Удостоверяющий центр ИНПАС operator

X509 EMV

Корневые сертификаты CRL Подчиненные УЦ

+ Создать сертификат подчиненного УЦ

Фильтр

Имя: Статус: Издатель:

Имя	Действ.с	Истекает	Статус / Истекает через	Издатель	Действия	Экспорт в base64
CA_Distr	30.08.2018	31.12.2018	4 мес., 16 ч.		Посмотреть Скачать Отозвать	

Рисунок 36. Отображение созданного сертификата подчиненного УЦ

Далее необходимо выполнить экспорт созданного сертификата подчиненного УЦ, для этого нужно нажать кнопку «Посмотреть» или «Скачать» в столбце «Действия». Для выгрузки созданного сертификата подчиненного УЦ 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 «Удостоверяющий центр хоста удаленной загрузки ключей».

9. Создание сертификатов в разделе EMV

9.1. Выпуск корневого сертификата (EMV)

Для выпуска корневого сертификата для УЦ Root перейти в раздел «EMV» на вкладку «Корневые сертификаты» и нажать кнопку «Создать сертификат корневого УЦ» (Рисунок 37. Раздел «EMV». Вкладка «Корневые сертификаты»).

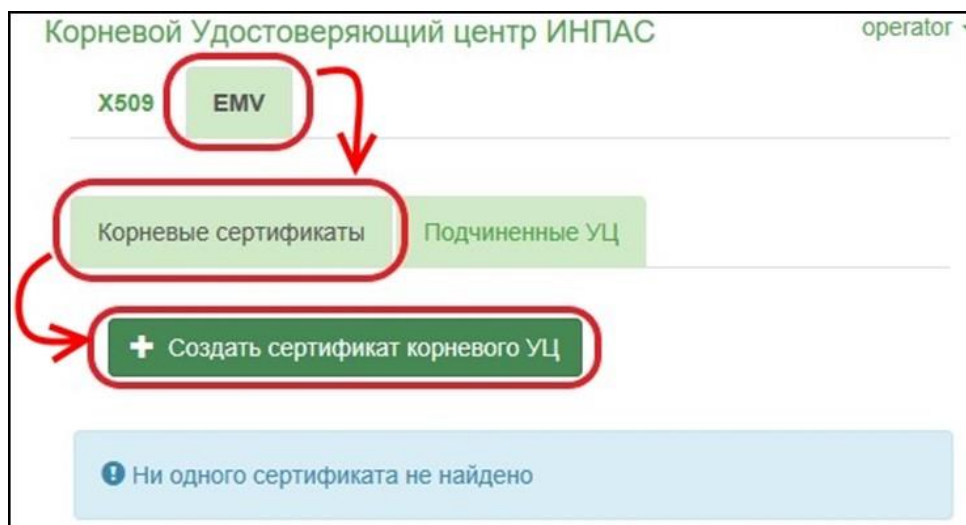


Рисунок 37. Раздел «EMV». Вкладка «Корневые сертификаты»

На отобразившейся странице «Создание корневого сертификата – шаг 1» заполняем все поля, а именно (Рисунок 38. Раздел «EMV». Страница «Создание корневого сертификата - шаг 1»):

- **Наименование** – указывается наименование сертификата;
- **Окончание** – указывается дата окончания действия сертификата.

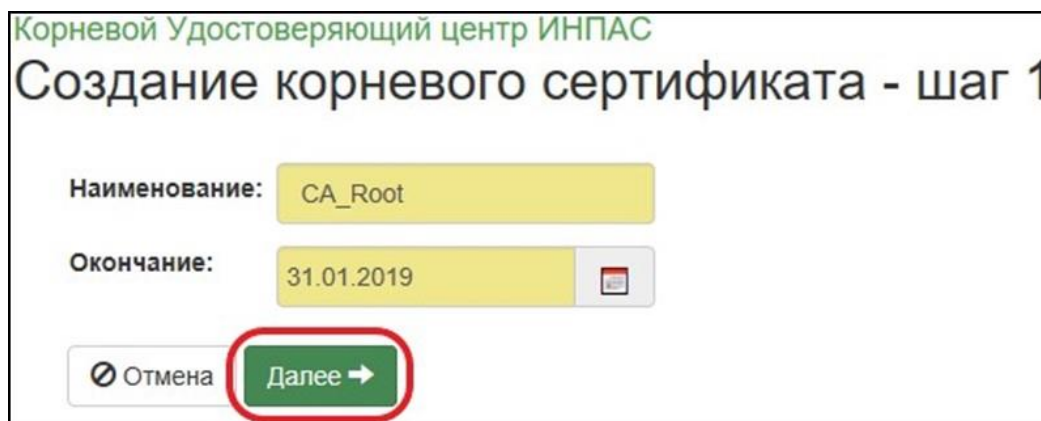


Рисунок 38. Раздел «EMV». Страница «Создание корневого сертификата - шаг 1»

После заполнения полей нажимаем кнопку «Далее».

Отобразится страница «Создание корневого сертификата – шаг 2», на которой представлены параметры создаваемого сертификата и поля «Логин» и «Пароль», для подтверждения офицерами безопасности выпуска корневого сертификата УЦ (Рисунок 39. Раздел «EMV». Страница «Создание корневого сертификата - шаг 2»).

Рисунок 39. Раздел «EMV». Страница "Создание корневого сертификата - шаг 2"

Далее вводим логин и пароль и вставляем смарт-карту в картридер поочередно для каждого офицера безопасности и нажимаем кнопку «**Проверить**» (Рисунок 20. Подтверждение первым офицером безопасности и Рисунок 21. Подтверждение вторым офицером безопасности).

После второй проверки в нижней части экрана станет доступна кнопка «**Генерировать**», нажимаем на неё (Рисунок 40. Раздел «EMV». Кнопка "Генерировать").

Рисунок 40. Раздел «EMV». Кнопка "Генерировать"

В отобразившемся окне «**Создание корневого сертификата – заключительный шаг**» нужно нажать кнопку «**Готово**» (Рисунок 23. Страница "Создание корневого сертификата - заключительный шаг").

После нажатия кнопки «**Готово**» отобразится главное окно системы с созданным сертификатом корневого УЦ (Рисунок 41. Раздел «EMV». Отображение созданного сертификата корневого УЦ).

Далее необходимо выполнить экспорт созданного сертификата, для этого нужно нажать кнопку «**Посмотреть**» в столбце «**Действия**». Далее сохраняем файл сертификата в нужную нам директорию на компьютере. В дальнейшем этот файл понадобится для импорта его в «**Удостоверяющий центр выдачи сертификатов POS-терминалам**».

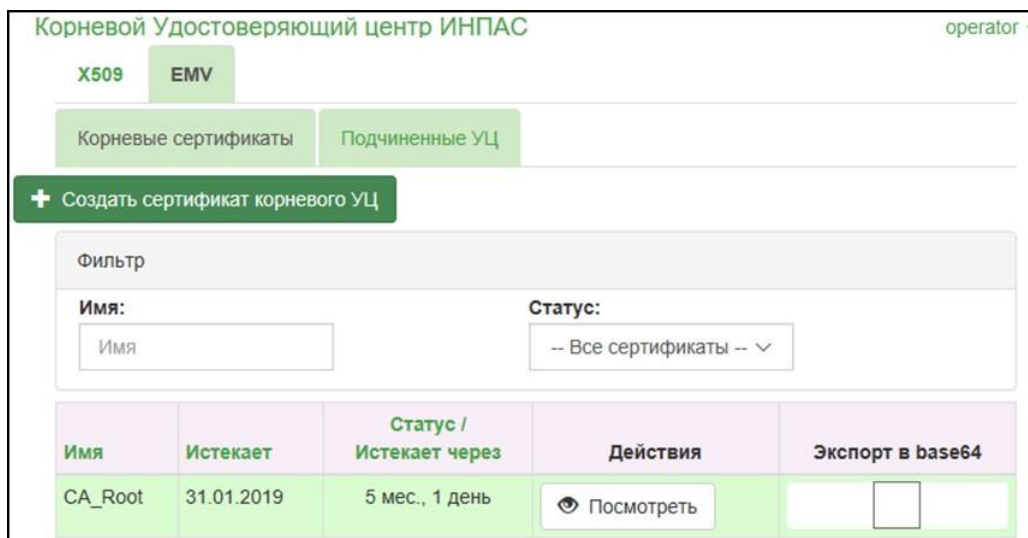


Рисунок 41. Раздел «EMV». Отображение созданного сертификата корневого УЦ

9.2. Выпуск сертификата подчиненного УЦ (EMV)

Для создания сертификата подчиненного УЦ необходимо выпустить файл запроса на получение сертификата подчиненного УЦ. Данную информацию можно найти в документе «**Руководство пользователя УЦ выдачи сертификатов POS-терминалам**».

После получения файла запроса необходимо перейти на вкладку «Подчиненные УЦ» раздела «EMV» и нажать на кнопку «Создать сертификат подчиненного УЦ» (Рисунок 42. Раздел «EMV». Создание сертификата подчиненного УЦ).

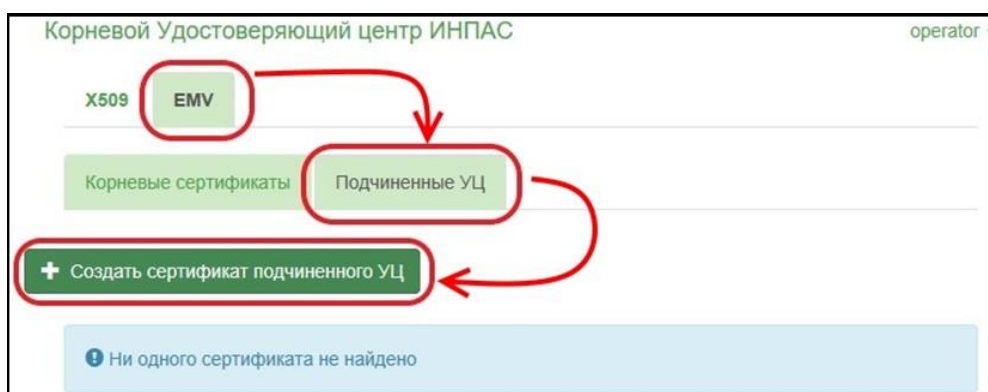


Рисунок 42. Раздел «EMV». Создание сертификата подчиненного УЦ

В отобразившемся окне «Создание подчиненного сертификата – шаг 1» необходимо выбрать сертификат издателя из выпадающего списка и в появившемся поле «Выберите файл CSR-запроса для сертификата:» нажать на кнопку «Выберите файл» (Рисунок 43. Раздел «EMV». Выбор сертификата издателя и файла запроса).

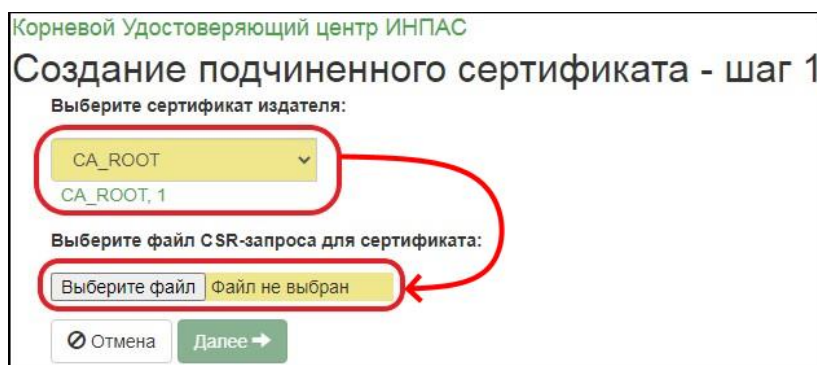


Рисунок 43. Раздел «EMV». Выбор сертификата издателя и файла запроса

После выбора файла запроса система попросит ввести название сертификата в поле «**Наименование**» и дату окончания действия сертификата в поле «**Окончание**», нажимаем кнопку «**Далее**» (Рисунок 44. Раздел «EMV». Страница "Создание подчиненного сертификата - шаг 1").

Рисунок 44. Раздел «EMV». Страница "Создание подчиненного сертификата - шаг 1"

Далее вводим логин и пароль и вставляем смарт-карту в картридер поочередно для каждого офицера безопасности и нажимаем кнопку «**Проверить**» (Рисунок 20. Подтверждение первым офицером безопасности и Рисунок 21. Подтверждение вторым офицером безопасности).

После второй проверки станет доступна кнопка «**Генерировать**», нажимаем на неё (Рисунок 45. Раздел «EMV». Страница "Создание подчиненного сертификата - шаг 2").

Рисунок 45. Раздел «EMV». Страница "Создание подчиненного сертификата - шаг 2"

В отобразившемся окне «**Создание подчиненного сертификата – заключительный шаг**» нужно нажать кнопку «**Готово**» (Рисунок 35. Страница "Создание подчиненного сертификата - заключительный шаг").

После нажатия кнопки «**Готово**» отобразится раздел «EMV» вкладка «Подчиненные сертификаты» с созданным сертификатом подчиненного УЦ (Рисунок 46. Раздел «EMV». Отображение созданного сертификата, подчиненного УЦ).

Далее необходимо выполнить экспорт созданного сертификата подчиненного УЦ, для этого нужно нажать кнопку «**Скачать**» в столбце «**Действия**». Для выгрузки созданного сертификата подчиненного УЦ 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 «**Удостоверяющий центр выдачи сертификатов POS-терминалам**».

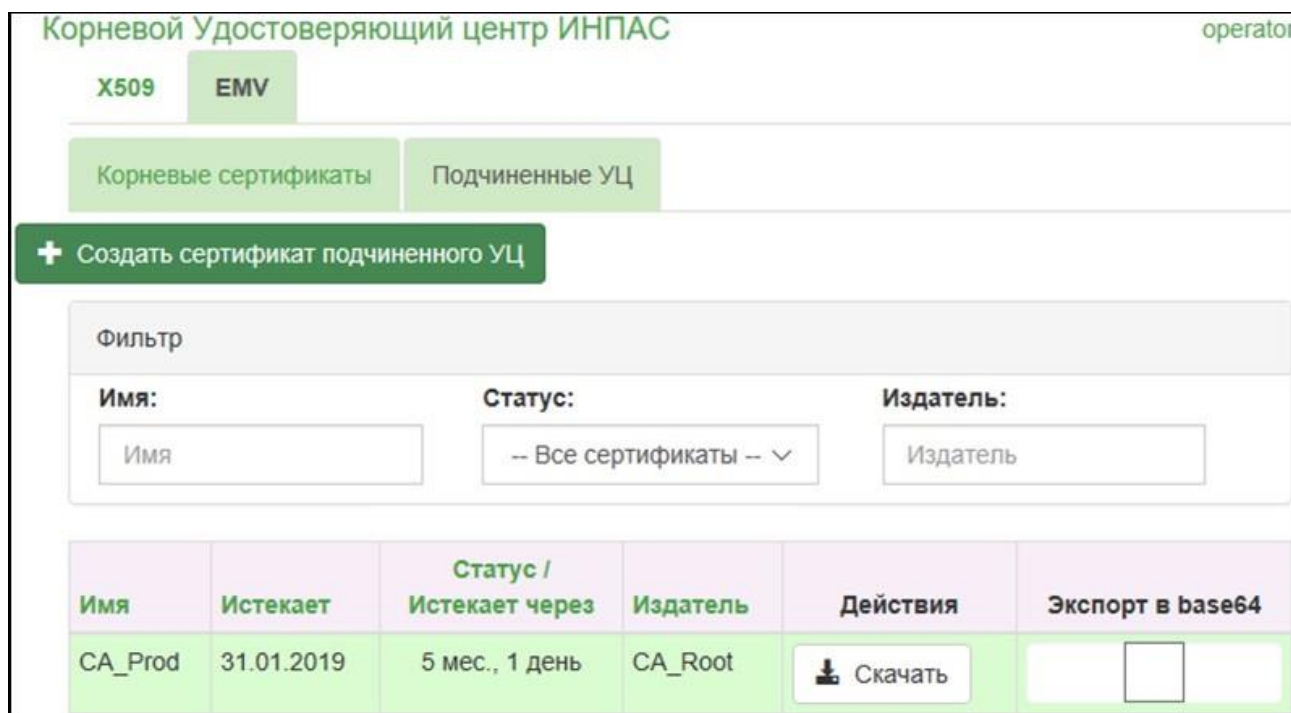


Рисунок 46. Раздел «EMV». Отображение созданного сертификата, подчиненного УЦ

10. Изменение настроек

Для изменения настроек «Корневого удостоверяющего центра Инпас» 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 47. Переход на страницу «Настройки»).

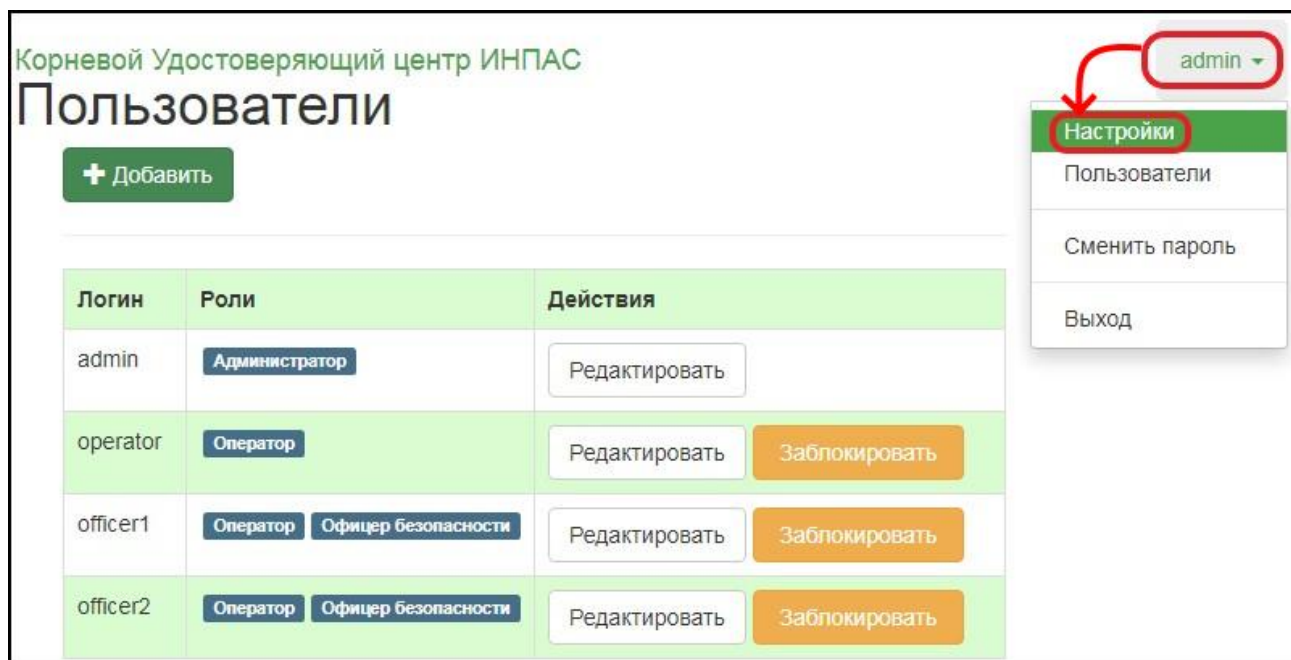
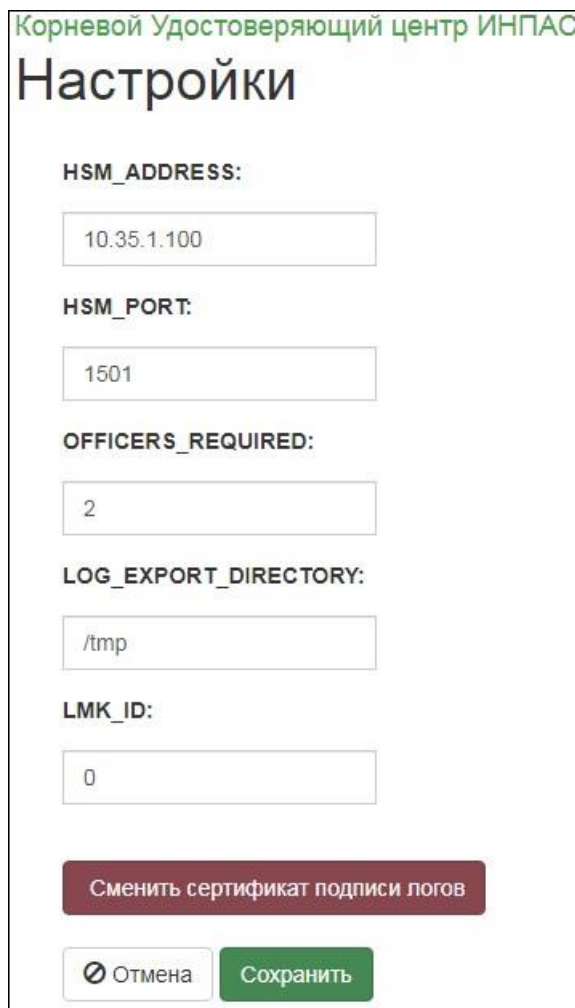


Рисунок 47. Переход на страницу «Настройки»

На отобразившейся странице «Настройки» нужно внести необходимые изменения в параметры и нажать кнопку «Сохранить» (Рисунок 48. 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».



Корневой Удостоверяющий центр ИНПАС

Настройки

HSM_ADDRESS:

HSM_PORT:

OFFICERS_REQUIRED:

LOG_EXPORT_DIRECTORY:

LMK_ID:

Сменить сертификат подписи логов

Отмена Сохранить

Рисунок 48. Страница "Настройки"