Руководство системного администратора

На 30 листах

2024 г.

СОДЕРЖАНИЕ

СПИСОК СОКРАЩЕНИЙ

Сокращение	Расшифровка сокращения
БД	База данных
ЛПУ	Лечебно-профилактическое учреждение
МО	Медицинская организация
МДЛП	Мониторинг движения лекарственных препаратов
ПО	Программное обеспечение
РВ	Регистратор выбытия
ФИО	Фамилия, Имя, Отчество
ЦОД	Центр обработки данных

1. ПОДКЛЮЧЕНИЕ ОРГАНИЗАЦИИ К БОЛЬНИЧНОЙ АПТЕКЕ

Для подключения медицинской организации необходимо выполнить следующие шаги:

1. Добавить организацию в справочник ЛПУ через соответствующий интерфейс (см. Инструкцию по работе в Едином справочнике ЛПУ).

2. Добавить руководителя организации через сервис аккаунтов (*в режиме администрирования*) в добавленную организацию (шаг 1) с ролью «Руководитель организации».

3. Развернуть базу данных аптеки на сервере организации или ЦОД в PostgreSQL.

4. Добавить через сервис хостов под руководителем организации (шаг 2) новое подключение к развернутой базе данных аптеки (шаг 3).

5. Добавить через сервис аккаунтов (в режиме администрирования) под руководителем организации пользователей этой организации, которые будут работать в Системе, назначить им роли, дать разрешение для работы с хостом аптеки (шаг 4). Назначение разрешения «Вход в хосты организаций» позволяет пользователю видеть хосты всех аптек. После авторизации пользователь может выбрать, с какими хостом работать. Без этого разрешения пользователю доступны только хосты, указанные в аккаунте пользователя. При наличии доступа к единственному хосту после авторизации пользователь автоматически в него переходит. Если хостов несколько, выбирает его из списка.

6. Выполнить обновление базы данных аптеки через сервис аптеки под руководителем организации (*в режиме администрирования*).

7. Выполнить загрузку справочников через сервис аптеки под руководителем организации (*в режиме администрирования*).

2. СЕРВИС АККАУНТОВ

Сервис аккаунтов предназначен для выполнения настройки и администрирования учетных записей пользователей Системы. Благодаря централизованному хранению учетных записей, пользователи получают доступ в различные сервисы Системы в соответствии с назначенными ролями (разрешениями).

Сервис предусматривает два режима работы:

- *режим работы пользователя* – доступен всем авторизованным пользователям и позволяет осуществлять персональные настройки.
- *режим работы администратора* – доступен пользователям с разрешениями

«Управление учетными записями региональных пользователей», «Управление учетными записями пользователей организаций», «Управление учетными записями организации пользователя» или «Полный доступ» и позволяет осуществлять администрирование учетных записей других пользователей.

2.1 Настройки сканера пользователя

Пользователь может сам произвести настройку сканера.

Для этого необходимо авторизоваться в сервисе аккаунтов и выбрать раздел «Настройки сканера» (Рисунок 1). Отобразится список доступных устройств.

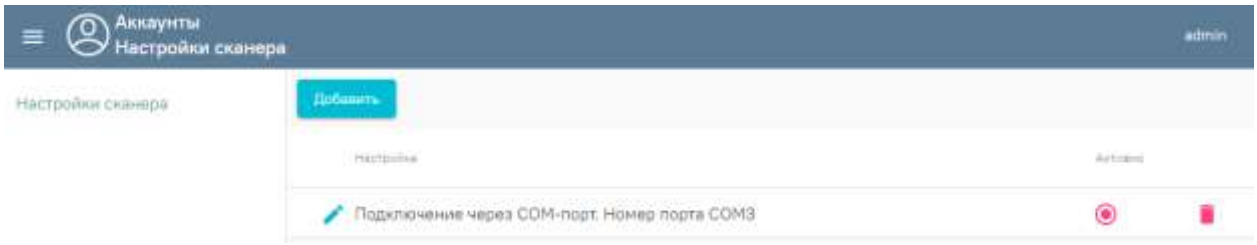

Рисунок 1. Вкладка «Настройки сканера»

Для добавления нового сканера следует нажать кнопку «Добавить». Отобразится новое окно «Настройка сканера», в котором необходимо выбрать тип подключения COM или USB.

Настройка сканера проводится в зависимости от варианта подключения сканера: **COM** или **USB.**

Перед настройкой необходимо сбросить сканер на заводские настройки:

- настроить на линейный штрих код;
- настроить на PDF-417;
- настроить на Datamatrix.

Настройка сканера с вариантом подключения сканера COM

Провести эмуляцию COM-порта для сканера.

- Для этого необходимо установить утилиту qrcodereader.exe

Утилиту можно запускать как приложение или службу. Запуски приложения производится запуском файла qrcodereader.exe на рабочем месте.

Настройка запуска службы для ОС Windows

1. Скачать актуальную версию qrcodereader.exe и положить в рабочую директорию, например, *C:\Program Files\qrcodereader*

2. Скачать утилиту nssm (https://nssm.cc/download)

3. Распаковать архив с утилитой. Запустить консоль *CMD.exe* от имени администратора. В консоли перейти в директорию утилиты при помощи команды *cd*, далее перейти в директорию согласно вашей архитектуре ОС (/win32 или /win64).

Пример:

C:\Users\PC>cd d:\
D:\>cd\nssm-2.24\win64

4. Выполнить в консоли команду

nssm install QrcodeReaderService

, где *QrcodeReaderService* – наименование создаваемой службы.

5. Появится окно настроек создаваемой службы. В поле *Path* выбрать путь до утилиты *qrcodereader*. По умолчанию служба будет запускаться вместе с операционной системой (Рисунок 2).

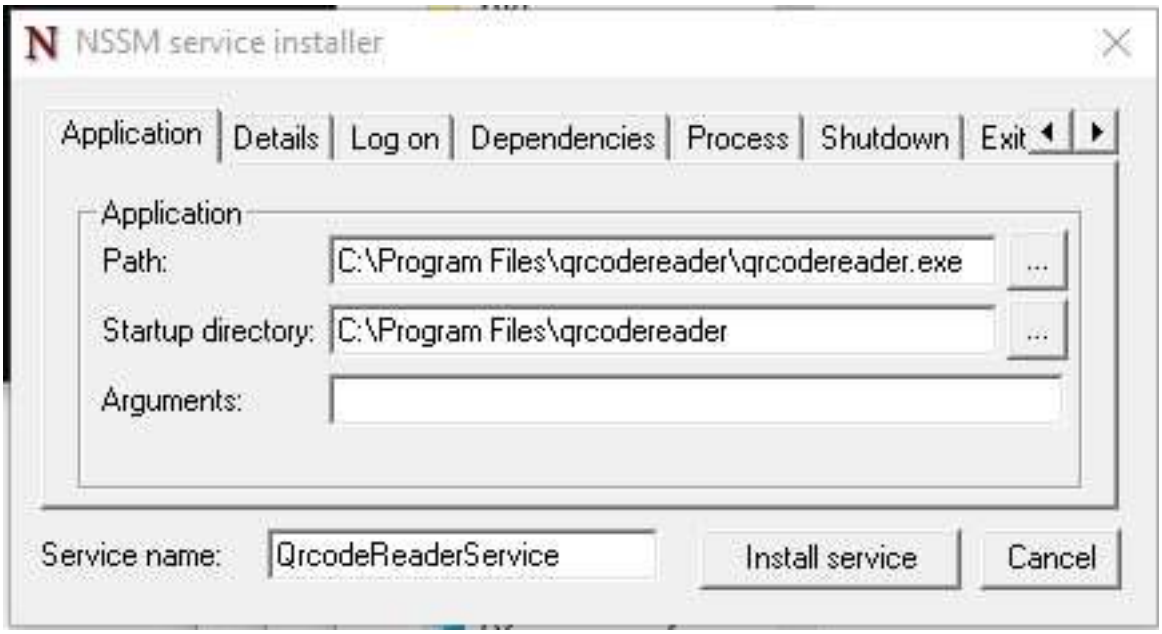

Рисунок 2. Окно настроек

6. Перейти в список служб Windows и найти созданную службу по указанному имени. Вызвать контекстное меню службы по правому клику мыши и выбрать «Запустить».

- Указать в настройках сканера сервиса аккаунтов (Рисунок 3):
  - режим работы – COM;
  - адрес демона – http://localhost:8101;
  - наименование порта – (COM1).

Рисунок 3. Настройка сканера

Настройка сканера с вариантом подключения сканера USB

Перевести сканер в режим эмуляции клавиатуры (по инструкции сканера) (Рисунок 4).

Для этого необходимо:

- запрограммировать сканер на спец. символы (F7, F8, например) для суффикса и префикса согласно инструкции;
- указать тип подключения – USB;

Рисунок 4. Перевод сканера в режим эмуляции клавиатуры

- задать суффикс и префикс.

Далее следует нажать кнопку «Сохранить».

После сохранения созданный сканер появится в списке. Для использования добавленного сканера следует выбрать переключатель «Активно».

Для проверки работы сканера необходимо осуществить тест (Рисунок 5).

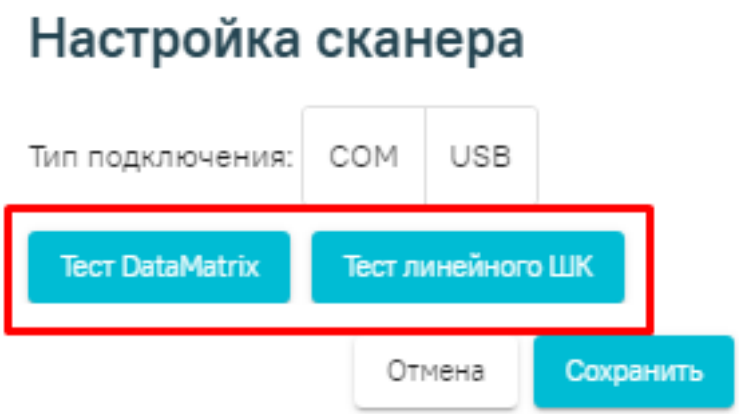

Рисунок 5. Тестирование сканера

2.2 Администрирование

2.2.1 Управление пользователями

Раздел «Пользователи» предназначен для управления пользователями в режиме администратора. В разделе отображается список пользователей в зависимости от разрешений, назначенных текущей учетной записи администратора:

- Управление учетными записями региональных пользователей – Администратор видит список пользователей, не относящихся к конкретным организациям, например, других администраторов.
- Управление учетными записями пользователей организаций – Администратор видит список пользователей всех доступных организаций.
- Управление учетными записями организации пользователя – Администратор видит список пользователей только той организации, к которой относится сам.

Внимание! Для управления пользователями, относящимся к организациям, необходимо осуществлять добавление учетных записей через вкладку «Организации».

2.2.1.1 Создание учетной записи пользователя

Для создания новой учетной записи следует выбрать раздел «Пользователи» и нажать кнопку «Добавить». Откроется форма для ввода информации о пользователе (Рисунок 6).

Рисунок 6. Форма создания нового пользователя

Поля «Логин» и «Пароль» являются обязательными для заполнения. В поле «Логин» следует указать уникальное имя без пробелов, например, логин от электронной почты. При попытке сохранения пользователя выполняется проверка уникальности логина в рамках Системы в целом. При наличии совпадений будет выдано сообщение об ошибке.

После успешного сохранения данных отобразится форма редактирования параметров созданного пользователя, включающая следующие вкладки: «Данные пользователя», «Роли», «Настройка сканера», «Сертификаты».

2.2.1.1.1 Вкладка «Данные пользователя»

Вкладка предназначена для просмотра и редактирования сведений о пользователе, а также для назначения пользователю нового пароля.

Для изменения пароля необходимо нажать кнопку «Изменить пароль» в правом нижнем углу страницы. Далее в открывшемся окне ввести новый пароль и нажать кнопку «Сохранить».

2.2.1.1.2 Вкладка «Роли»

Вкладка предназначена для добавления ролей и просмотра списка назначенных пользователю ролей. Подробнее о работе с ролями см. в п. 2.2.2.

Для назначения пользователю определенной роли необходимо нажать «Добавить роль» и выбрать подходящую из предложенного списка или при помощи поиска (Рисунок 7).

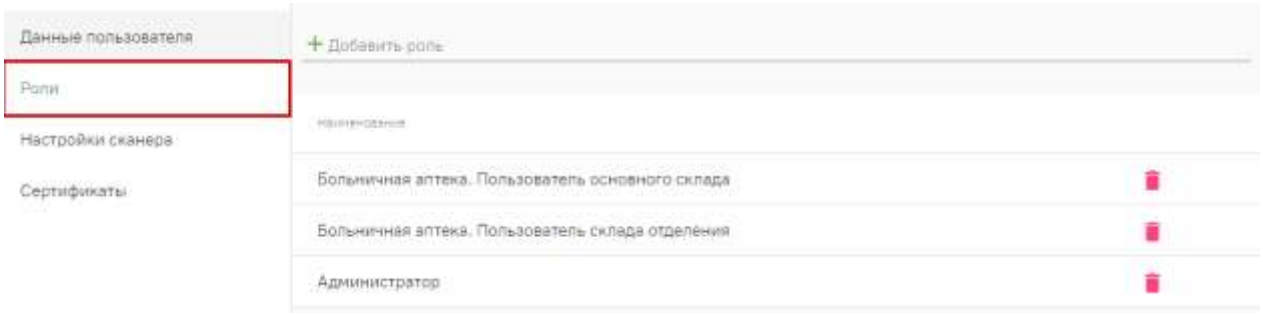

Рисунок 7. Вкладка «Роли»

2.2.1.1.3 Вкладка «Настройки сканера»

Вкладка предназначена для выполнения настройки сканера для учетной записи пользователя (Рисунок 8). Настройка сканера может быть также выполнена самим пользователем.

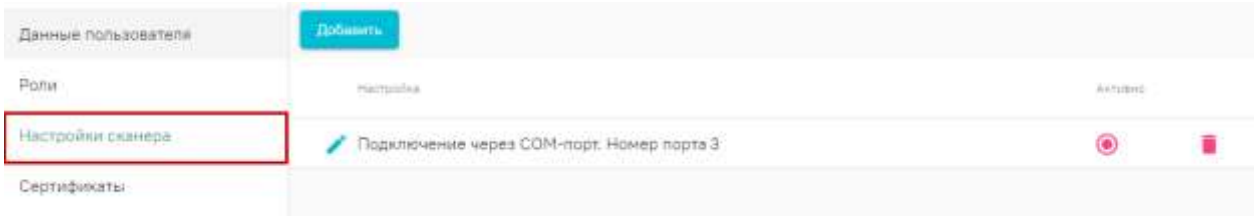

Рисунок 8. Вкладка «Настройка сканера»

Подключение сканера осуществляется непосредственно на рабочем месте пользователя.

Для добавления нового сканера следует нажать кнопку «Добавить». Отобразится новое окно «Настройка сканера», в котором необходимо выбрать тип подключения. В зависимости от выбранного типа изменится состав полей формы (Рисунок 9):

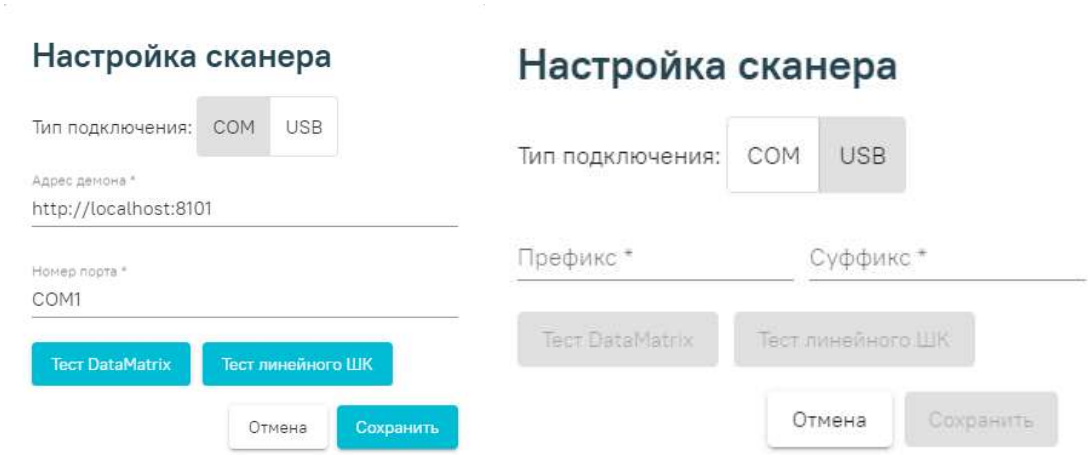

Рисунок 9. Состав полей формы «Настройка сканера» в зависимости от выбранного типа подключения

После сохранения созданный сканер появится в списке. Для выбора сканера, с которым будет осуществляться работа, следует установить переключатель «Активно».

Подробнее о работе со сканером представлено в п. 2.1.

2.2.1.1.4 Вкладка «Сертификаты»

На вкладке определяются сертификаты пользователя, с которыми он может работать.

Для добавления нового сертификата следует нажать кнопку «Добавить». В открывшейся форме необходимо выбрать тип сертификата:

- Клиентский – устанавливается на рабочем месте пользователя для подписания его документов.
- Серверный – устанавливается на сервере медицинской организации или ЦОД. Для серверного сертификата необходимо выбрать адрес сервиса из предложенного списка. Подробнее о добавлении адреса сервиса подписи см. в п. 2.2.3.

Затем в поле «Номер» необходимо скопировать серийный номер сертификата из свойств сертификата (без пробелов и специальных символов). Подробнее о том, где найти номер сертификата см. в п. 5.1. В поле «Доступ» необходимо указать роли пользователей, для которых будет доступно использование сертификата, например, в случае когда организации был выдан единственный сертификат на имя её руководителя (Рисунок 10).

Рисунок 10. Состав полей вкладки «Сертификаты» в зависимости от выбранного типа сертификата

2.2.2 Роли пользователя

Роль – это именованный набор разрешений, выдаваемый пользователю. Разрешение определяет доступ к конкретному действию пользователя в Системе.

Роли бывают региональные и организационные.

- «Региональные роли» – назначаются только региональному администратору. Недоступны для пользователей, прикрепленных к организациям.
- «Организационные роли» – назначаются администраторам и сотрудникам медицинских организаций. Пользователи могут создавать организационные роли и

определять для них разрешения.

В Системе существует стандартный набор организационных ролей, который недоступен для изменения сотрудникам организаций. Для назначения пользователям, прикрепленным к медицинской организации, роль должна иметь признак «Доступно для организаций».

Раздел «Роли» предназначен для управления ролями в режиме администратора.

Для работы с ролями пользователь должен обладать следующими правами:

- «Управление региональными ролями» – для управления ролями пользователей, не относящихся к организациям, например, ролью администратора.
- «Управление ролями организаций» – для управления ролями всех доступных организаций.
- «Управление ролями организации пользователя» – для управления ролями организации, к которой прикреплен текущий пользователь.

2.2.2.1 Создание роли

Для создания новой роли следует выбрать раздел «Роли» и нажать кнопку «Добавить». Отобразится страница создания новой роли (Рисунок 11).

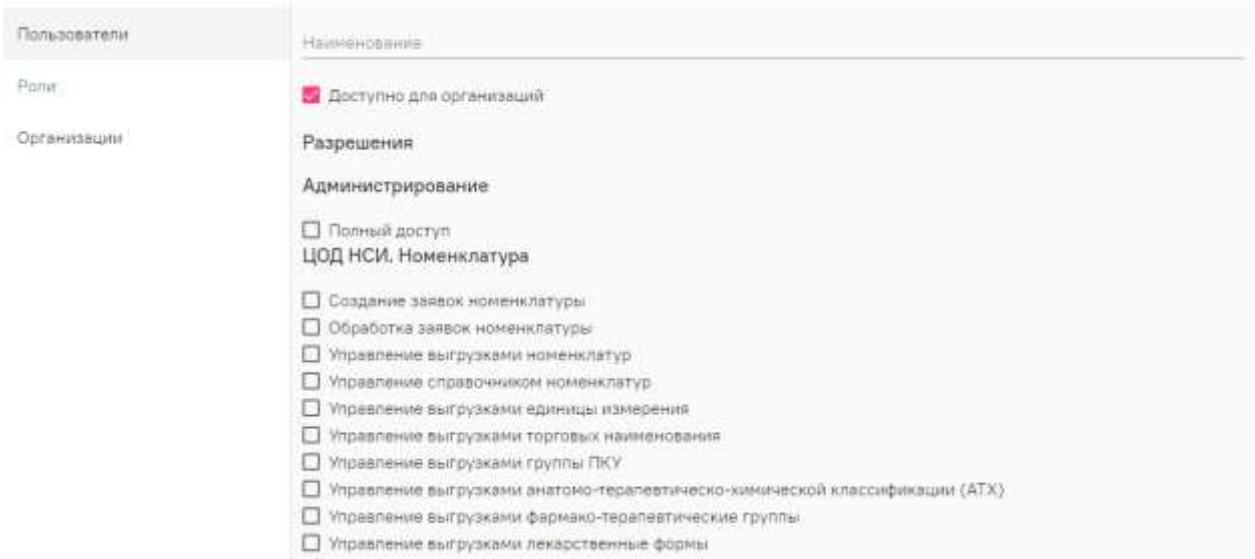

Рисунок 11. Список доступных разрешений при создании новой роли

На странице следует заполнить наименование роли и установить флажки рядом с теми разрешениями, которые будут предоставлены пользователю.

После сохранения изменений созданная роль появится в списке. Список ролей можно сортировать по наименованию (Рисунок 12).

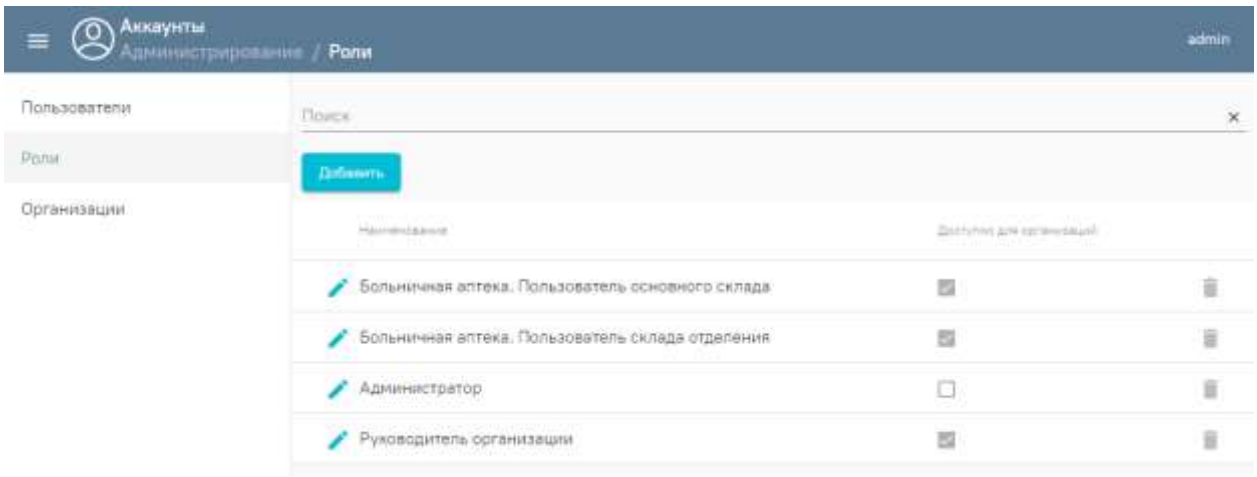

Рисунок 12. Список доступных ролей

2.2.3 Управление организациями

Раздел «Организации» предназначен для управления организациями в режиме администратора. Раздел доступен при наличии разрешений для управления аккаунтами или ролями, список таких разрешений см. в п. 2.2.1 и 2.2.2.

В зависимости от назначенных пользователю разрешений, на вкладке отображается список всех доступных медицинских организаций или только та организация, к которой принадлежит текущий пользователь. При отображении списка, для управления конкретной организацией необходимо открыть ее для редактирования.

2.2.3.1 Пользователи

Вкладка предназначена для управления пользователями организации. Подробнее о создании пользователя см. раздел «Пользователи». Для привязки пользователя к конкретной медицинской организации необходимо создать его именно через вкладку «Организации».

2.2.3.1.1 Вкладка «Хосты»

Для предоставления доступа пользователю к работе с хостом, необходимо добавить ранее созданный в сервисе хостов адрес подключения, выбрав его из предложенного списка (Рисунок 13). Подробнее о создании хоста см. в п. 3.1.

Рисунок 13. Вкладка «Хосты»

2.2.3.2 Роли

Вкладка предназначена для отображения доступных для организации ролей. Список содержит как базовые, недоступные для редактирования роли, так и персональные, созданные для текущей организации администратором МО. Подробнее о создании новой роли см. п. 2.2.2.

2.2.3.3 Сервисы подписи

Вкладка содержит список адресов сервисов подписи организации. После добавления адреса через вкладку «Сервисы подписи», созданная запись будет доступна для выбора при создании серверного сертификата для пользователя.

Подробнее о развертывании сервиса см. в п.5.1.

2.3. Настройки для отпуска Рецептов

Должен быть установлен:

1) Плагин КриптоПРО на рабочем месте фармацевта;
2) Клиентский сертификат на рабочем месте фармацевта.

У пользователя должны быть прописаны:

1) Роль - Льготная аптека. Фармацевт;
2) ФРМР. Должности;
3) СНИЛС.

Аккаунты

- Перейти в Профиль пользователя (Рисунок 14).

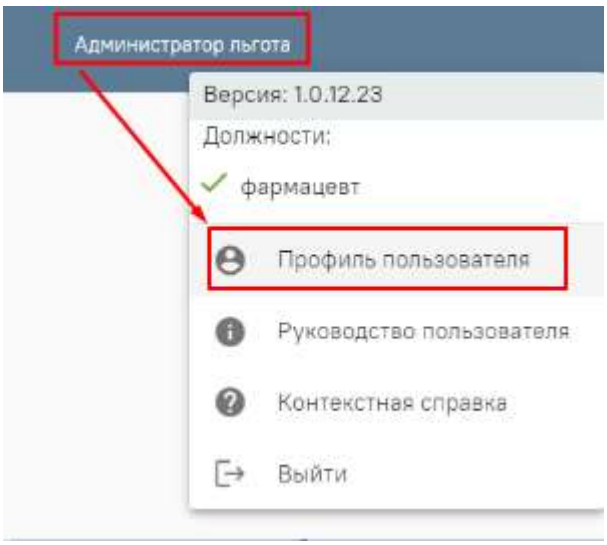

Рисунок 14. Профиль пользователя

- Администрирование (Рисунок 15) -> Пользователи - найти нужного пользователя и перейти к редактированию (Рисунок 16).

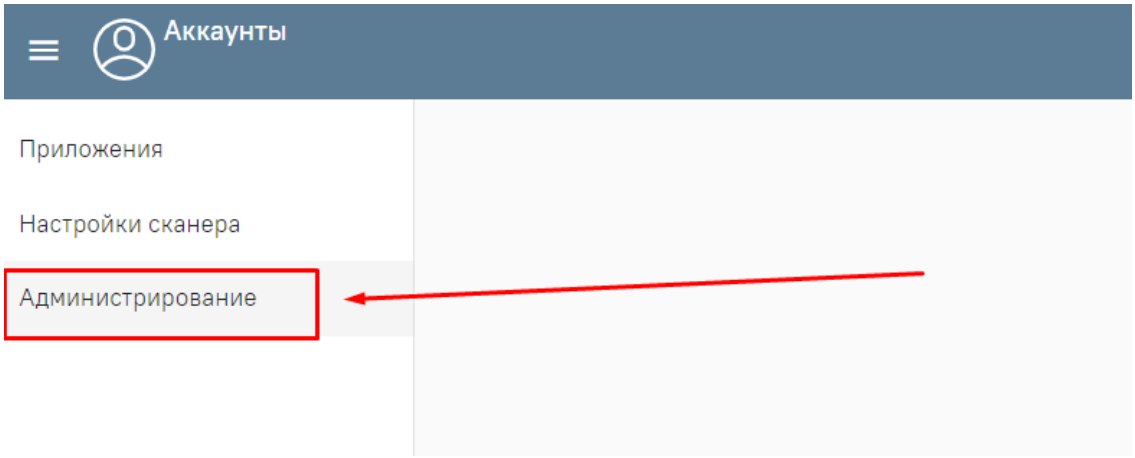

Рисунок 15. Вкладка «Администрирование»

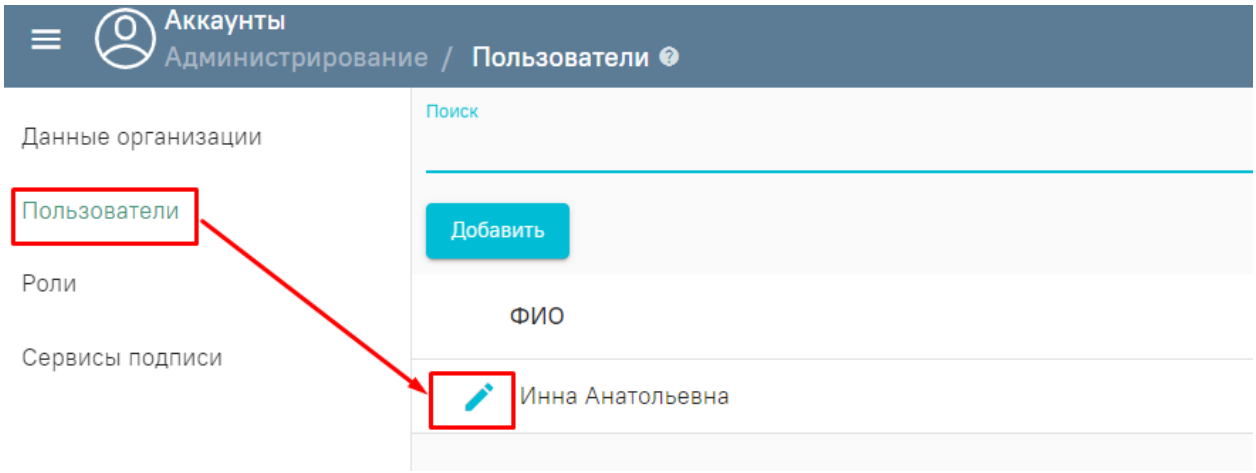

Рисунок 16. Вкладка «Пользователи»

- Сертификаты (Рисунок 17) -> Добавить «Тип-Клиентский», необходимо нажать на значок выбора сертификата справа от строки, где должен находиться номер сертификата,

откроется окно подтверждения доступа к сертификату (нажимаем «Да») (Рисунок 18).

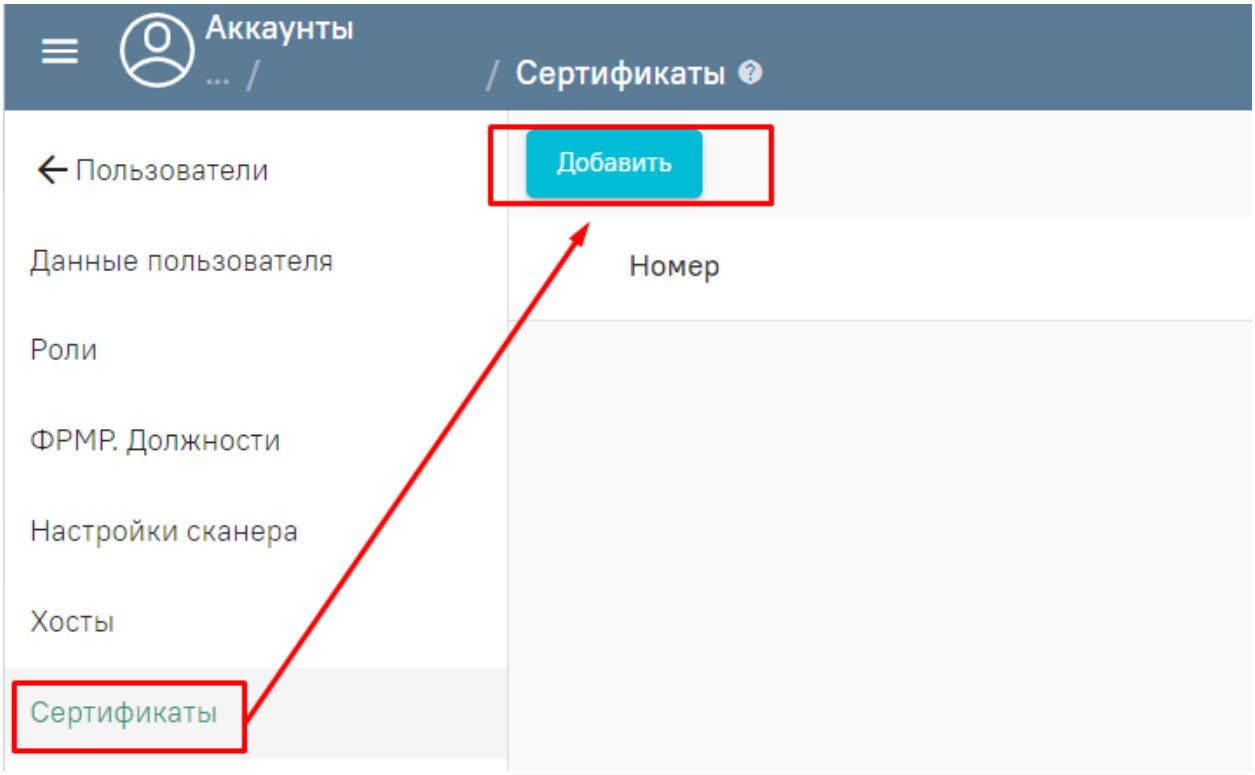

Рисунок 17. Форма добавления сертификата

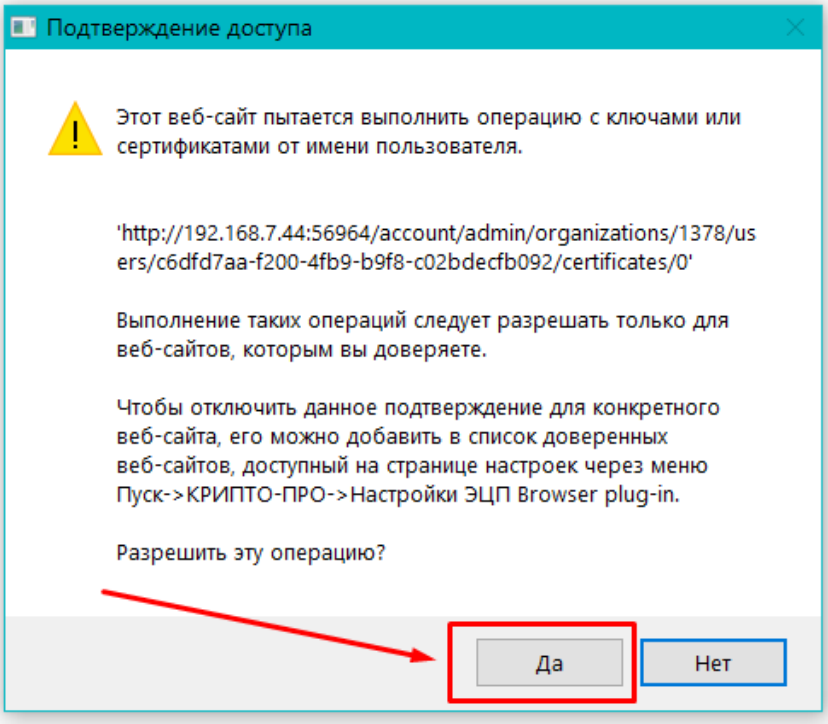

Рисунок 18. Форма подтверждения доступа

- В окне выбора сертификата выбрать наш клиентский сертификат (СНИЛС сертификата должен совпадать со СНИЛС прописанным у пользователя) (Рисунок 19).

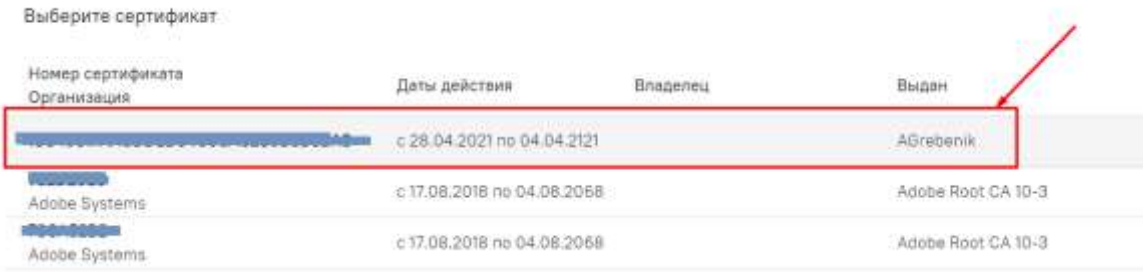

Рисунок 19. Окно выбора сертификата

- Доступ - Льготная аптека. Фармацевт (Рисунок 20).

- Нажимаем кнопку «Сохранить» (Рисунок 21).

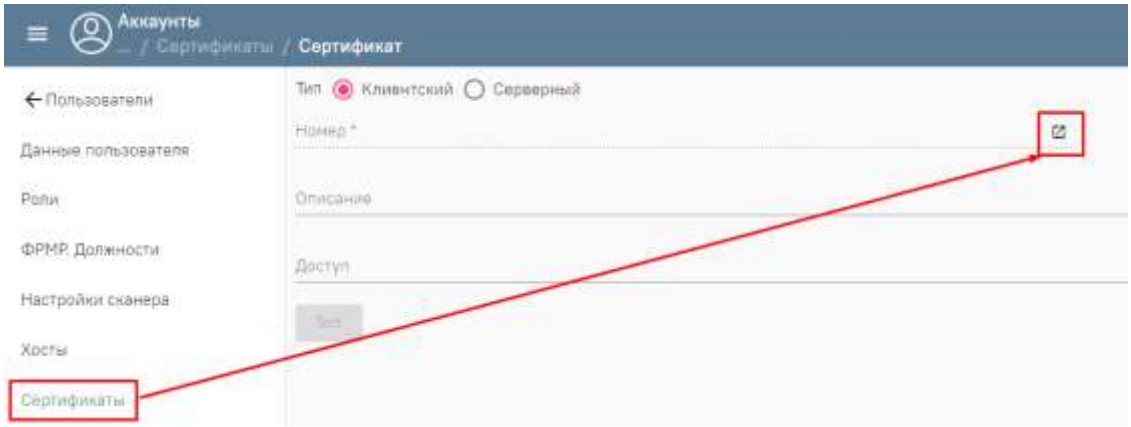

Рисунок 20. Форма доступа

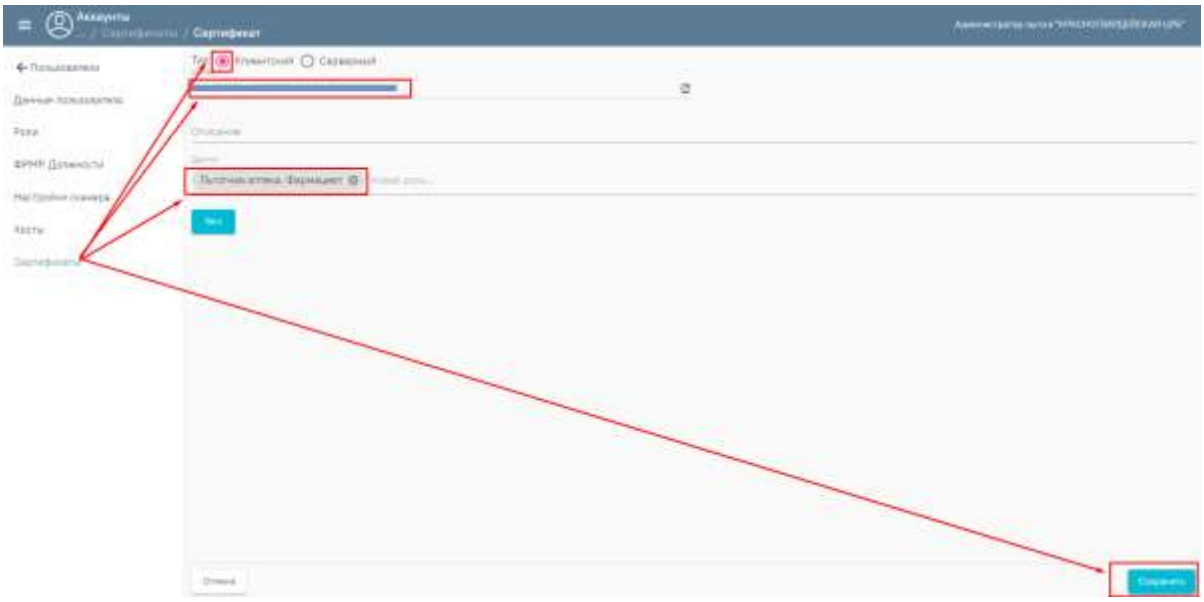

Рисунок 21. Вкладка «Сертификаты»

- Для проверки работоспособности сертификата нажимаем кнопку «Тест».

Аптека

- Администрирование (Рисунок 22) _ Настройки пользователя - найти нужного пользователя и перейти к редактированию (Рисунок 23).

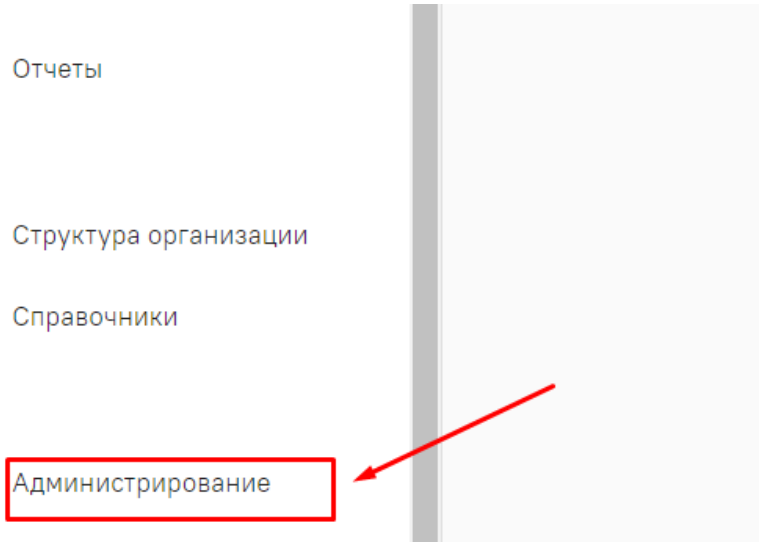

Рисунок 22. Вкладка «Администрирование»

Рисунок 23. Вкладка «Настройки пользователя»

- Настройки платформы ЭР - нажимаем на поле «Сертификат подписи организации» и выбираем сертификат организации и нажимаем кнопку «Сохранить» (Рисунок 24).

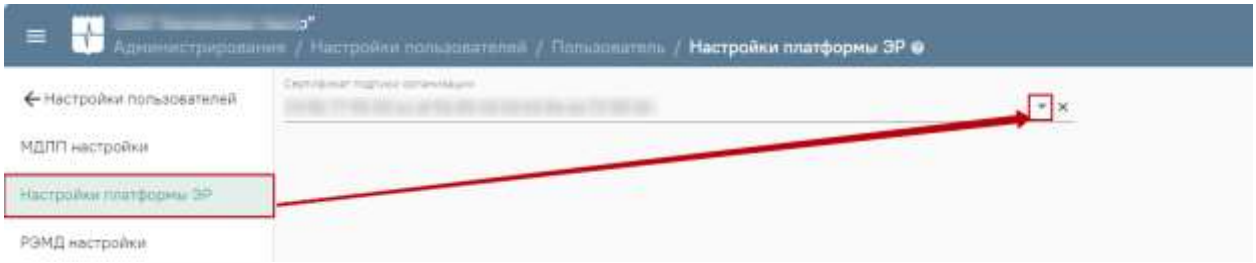

Рисунок 24. Вкладка «Настройки платформы ЭР»

- РЭМД настройки - нажимаем на поле «Сертификат подписи фармацевта» и выбираем сертификат пользователя и нажимаем кнопку «Сохранить» (Рисунок 25).

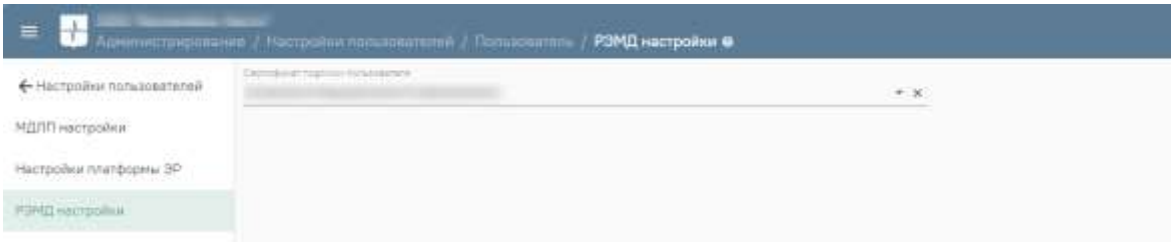

Рисунок 25. Вкладка «РЭМД настройки»

3. СЕРВИС ХОСТОВ

Сервис предназначен для создания хостов и выполнения их настройки.

Пользователь должен обладать следующими разрешениями:

- «Управление справочником хостов» – для управления хостами всех доступных организации.
- «Управление хостами своей организации» – для управления хостами той организации, к которой он прикреплен.

В рамках одного хоста (базы данных) могут храниться данные нескольких медицинских организаций с разграничением доступа между ними.

3.1 Хосты организации

Перед добавлением хоста пользователю необходимо развернуть базу данных с типом Postgres на сервере медицинской организации или ЦОД, а затем авторизоваться в сервисе хостов. Откроется форма со списком доступных медицинских организаций.

Доступный пользователю список организаций определяется наличием разрешения:

- «Управление справочником хостов» – во вкладке отобразится список всех доступных организаций;
- «Управление хостами своей организации» – на вкладке будет отражена только та организация, к которой прикреплена текущая учетная запись.

Для привязки хоста к конкретной организации необходимо открыть ее для редактирования.

Для добавления нового хоста необходимо указать сведения: наименование и краткое описание хоста, выбрать тип – Postgres, вид «Аптека» и ввести строку подключения из ЦОДа (Рисунок 26).

Пример строки подключения:

User ID=<userId>;Password=<password>;Host=127.0.0.1;Port=5432;Database=<dabaseName>;Integrated Security=true;Pooling=true;

Рисунок 26. Вкладка «Хосты»

Далее необходимо через сервис аккаунтов (*в режиме администрирования*) под руководителем организации добавить пользователей этой организации, которые будут работать в Системе, назначить им роли, дать разрешение для работы с хостом аптеки.

Видеоинструкция по работе с созданием профиля и сопоставление его со складом

4. СЕРВИС АПТЕКИ

Сервис предназначен для учета лекарственных средств, формирования отчетов, а также обмена с информационной системой МДЛП. Подробнее о работе с сервисом аптеки в режиме пользователя см. в разделе «Больничная аптека v2».

Перед началом работы в Системе необходимо выполнить действия по обновлению базы данных (доступны пользователю с разрешением «Администрирование») и загрузке справочников (доступны пользователю с разрешением «Управление справочниками»).

В случае первоначального заполнения базы необходимо обновить БД, а затем при загрузке данных справочников нажать кнопку «Полная загрузка».

4.1 Загрузка справочников

Справочники раздела «Справочники» разделены на 4 группы: «Организации», «Номенклатура», «Контрагенты» и «Финансы», они распределены между базами данных ЦОДа и ведутся на региональном уровне.

В данном разделе можно просмотреть, какие пакеты с обновлениями справочников ещё не были загружены в Систему и загрузить недостающие. Для просмотра данных, содержащихся в справочнике, следует нажать на кнопку рядом с выбранным справочником.

Для загрузки справочной информации следует в разделе «Справочники» нажать кнопку «Загрузка». Откроется новое окно со списком всех доступных справочников с указанием последней загруженной версии.

Например, если в базе данных сервиса Аптеки нет необходимого пакета данных для справочника, но он есть в базе данных ЦОД, следует загрузить его в сервис.

В случае первоначальной загрузки данных необходимо нажать кнопку «Полная загрузка», будет загружен пакет обновлений с последней версией.

Кнопка «Инкрементная загрузка» позволяет загрузить не весь справочник, а только новые или измененные данные с момента прошлой загрузки.

Для управления справочниками пользователь должен обладать разрешениями из групп:

- «ЦОД НСИ. Номенклатура»
- «ЦОД НСИ. Организации»
- «ЦОД НСИ. Контрагенты»
- «ЦОД НСИ. Финансы»

Если данное условие выполнено, администратору следует перейти в одноименный сервис.

4.2 Обновление структуры БД

Сервисы Аптеки работают с базами данных определенной структуры. Для приведения БД аптеки к спецификации сервисов необходимо выполнить «Обновление структуры БД»:

- Региональному администратору. Войти в сервис аптеки с разрешением «Вход в хосты организаций», пункт бокового меню «Хосты», выбрать необходимые и нажать «Обновить».
- Администратору МО. Войти в сервис аптеки с разрешением «Вход в хосты своей организации», пункт «Администрирование/Обновление БД» и нажать «Обновить».

5. МАРКИРОВКА

5.1 Настройка сервиса подписи для МДЛП

5.1.1 Установка CryptoProCSP

1. Установите CryptoProCSP на компьютере с «ТМ:Аптека». При использовании VipNetCSP наблюдается нестабильная работа с МДЛП.

2. Установите сертификат, который имеет доступ в личный кабинет МДЛП, у пользователя данного сертификата должны быть права для работы с функционалом МДЛП. Сертификат должен быть установлен под пользователем, который будет указан в пуле приложений IIS.

3. Сертификат в крипто про должен быть установлен в реестр

4. У сертификата должен быть сохранен пароль

5.1.2 Включение IIS

1. Убедитесь, что компонент уже не включен. Зайдите на сервер аптеки.

Откройте IIS (нажмите **win+r** введите **inetmgr**). Если открылось окно IIS, то он

установлен.

2. Если IIS не установлен, его необходимо установить.

Подробное описание установки IIS представлено по ссылке https://professorweb.ru/my/ASP_NET/sites/level3/3_1.php

5.1.3 Установка .Net Framework 4.5.2

Установка через «программы и компоненты» или отдельно скачанный файл.

5.1.4 Развертывание сервиса подписи

1. Скопируйте сервис подписи на сервер, например, в папку c:/inetpub/fss.

2. Добавьте веб-сайт. Укажите: имя сайта - Fss, Физический путь – путь папки с сервисом (c:/inetpub/fss), Порт – любой свободный, например, 89 (Рисунок 27).

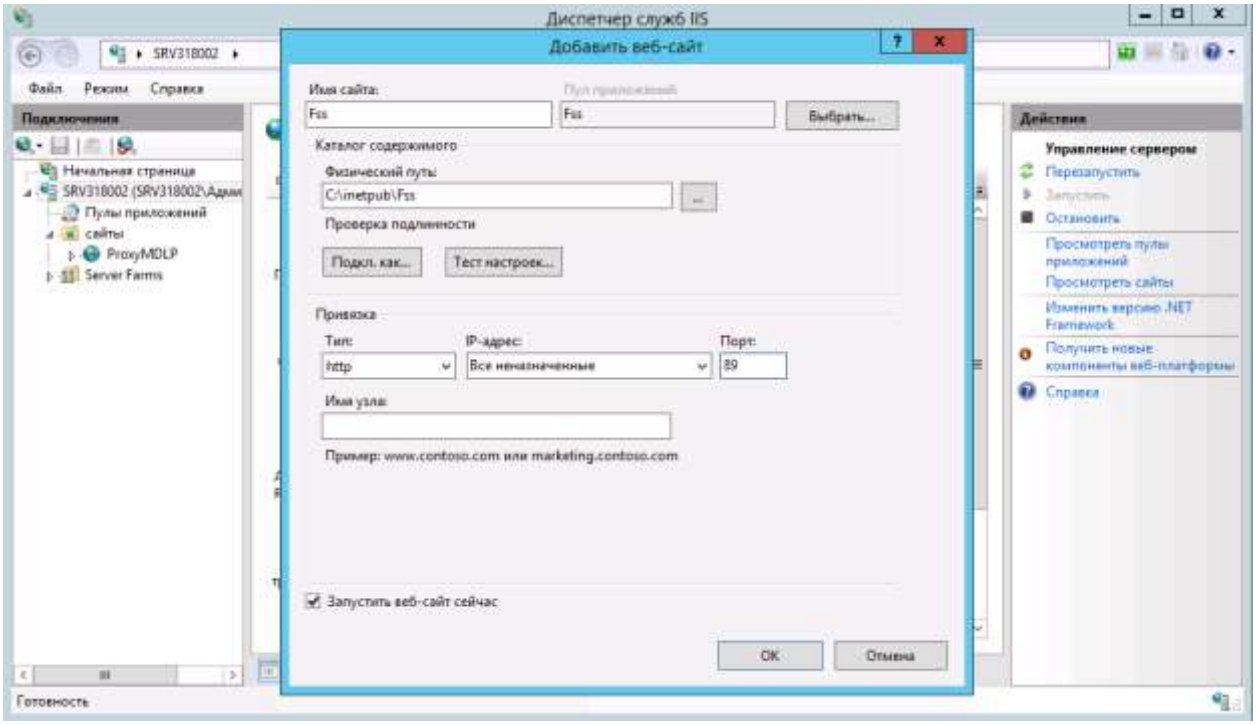

Рисунок 27. Добавление веб-сайта

3. Зайдите в «Пулы приложений», найдите пул «Fss». Зайдите в «Основные настройки» и выберите версию среды v.4. Затем зайдите в дополнительные параметры, пункт «Удостоверение», выберите «Особая учетная запись» и нажмите «Установить». Введите имя пользователя и пароль, которому доступны сертификаты на компьютере сервера.

5.1.5 Установка настроек

1. Внесение настройки сервиса подписи

1. Зайдите на сервер. Откройте IIS (нажмите **win+r** введите **inetmgr**). Перейдите на сайт сервиса подписи (Рисунок 28).

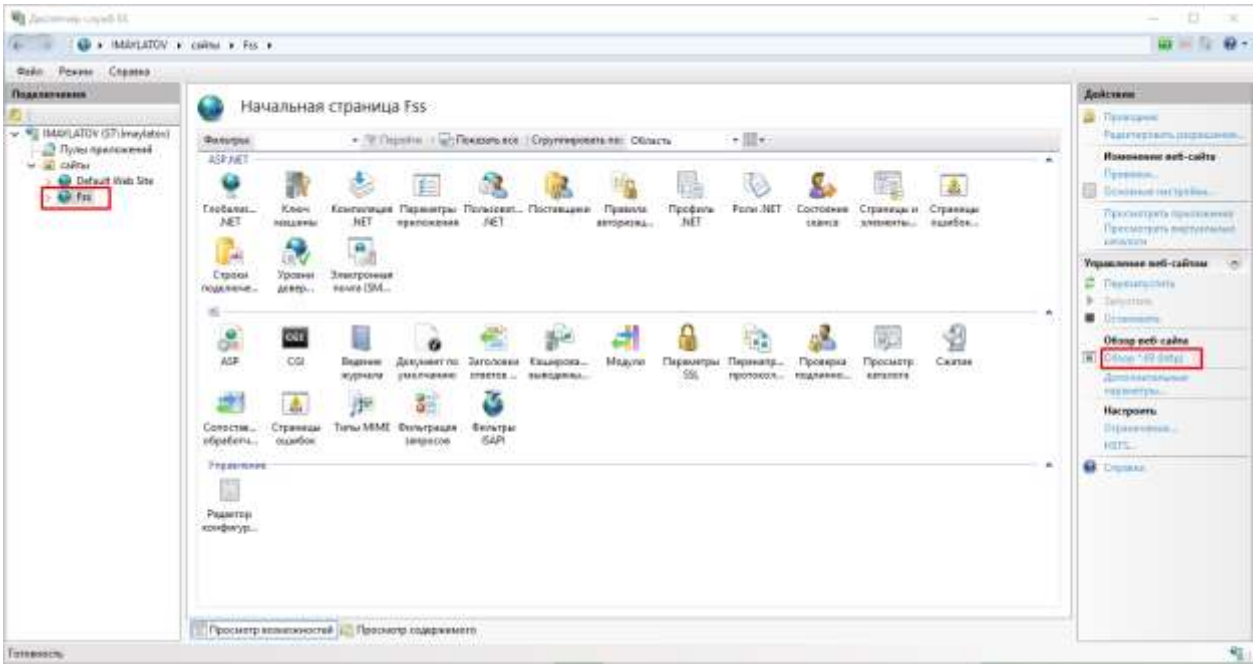

Рисунок 28. Переход на сайт сервиса подписи

2. Вместо localhost используйте ip-адрес сервера, например, http://192.168.7.170:89/ (**должен быть указать ip адрес защищенной сети).** Запомните адрес.

3. В сервисе Аккаунтов модуля «Аптека»/account пункт меню «Администрирование» – «Организации» найдите нужную организацию, нажмите «Редактировать». Далее пункт меню «Сервисы подписи» – «Добавить». В поле «Адрес» внесите адрес сервиса подписи. Нажмите кнопку «Сохранить» внизу страницы (Рисунок 29).

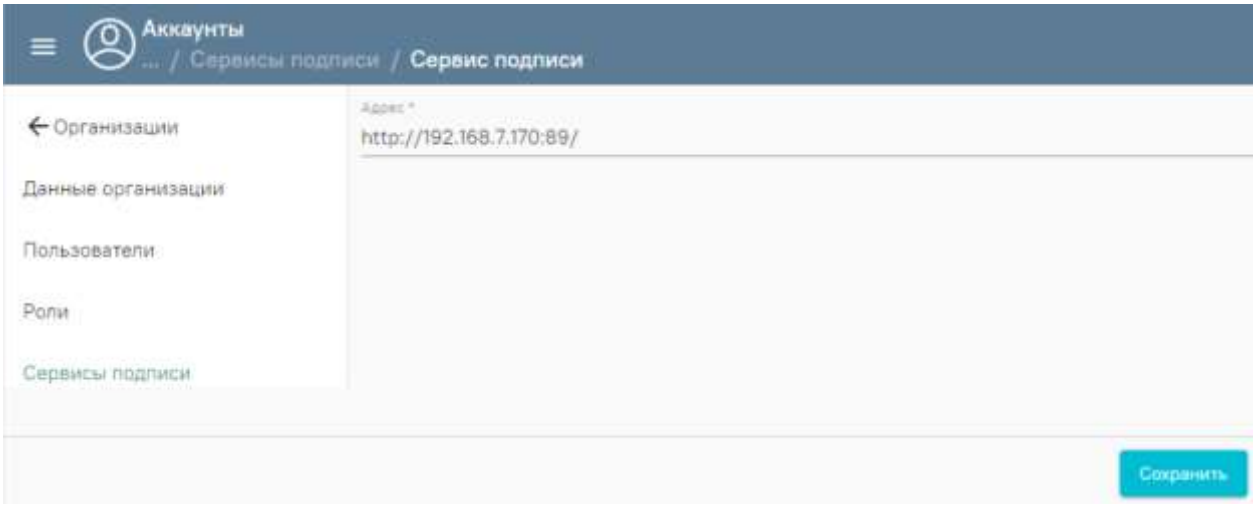

Рисунок 29. Настройка «Сервис подписи»

2. Внесение настройки «Сертификаты»

1. Получение номера сертификата**.** Зайдите на сервер. Откройте консоль управления (нажмите **win+r** введите **mmc**). Пункт меню «Файл» – «Добавить или удалить оснастку». Добавьте пункт «Сертификаты» – «Моей учетной записи пользователя», нажмите «Готово». В появившемся списке выберите «Сертификаты» – «Личное» –

«Сертификаты» (Рисунок 30).

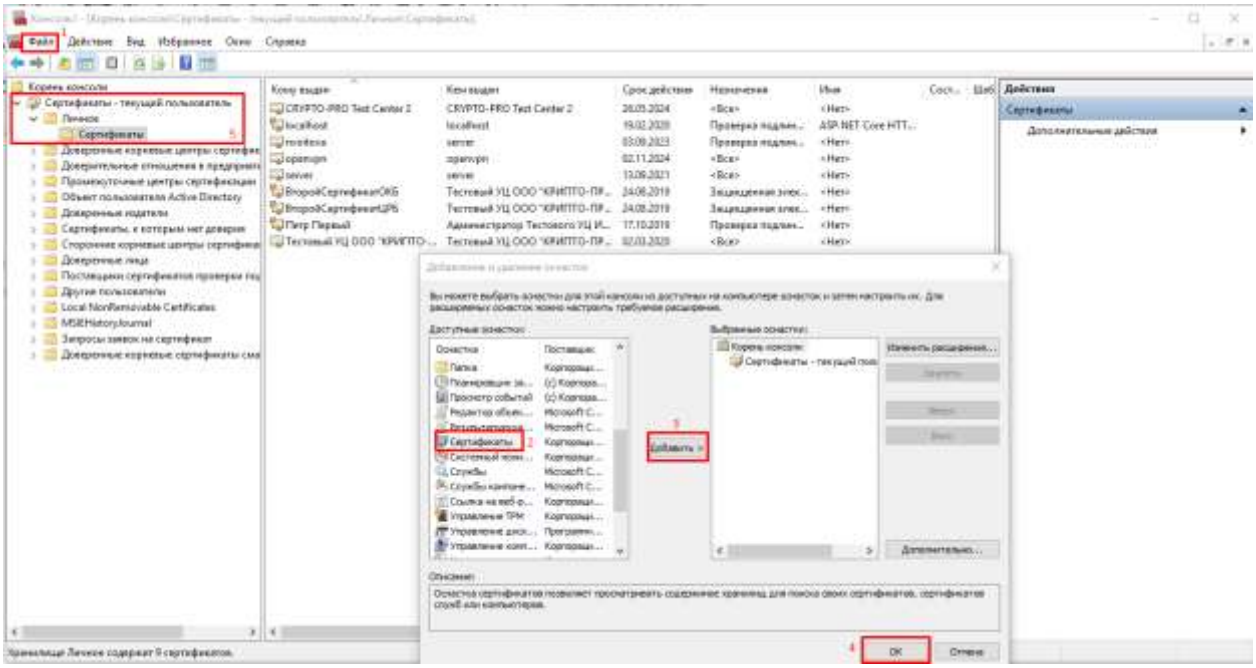

Рисунок 30. Выбор сертификата

2. В появившемся списке выберите нужный сертификат и зайдите в его свойства (двойной щелчок мыши). Перейдите на вкладку «Состав», выберите пункт «Серийный номер» списка. Запомните его (Рисунок 31).

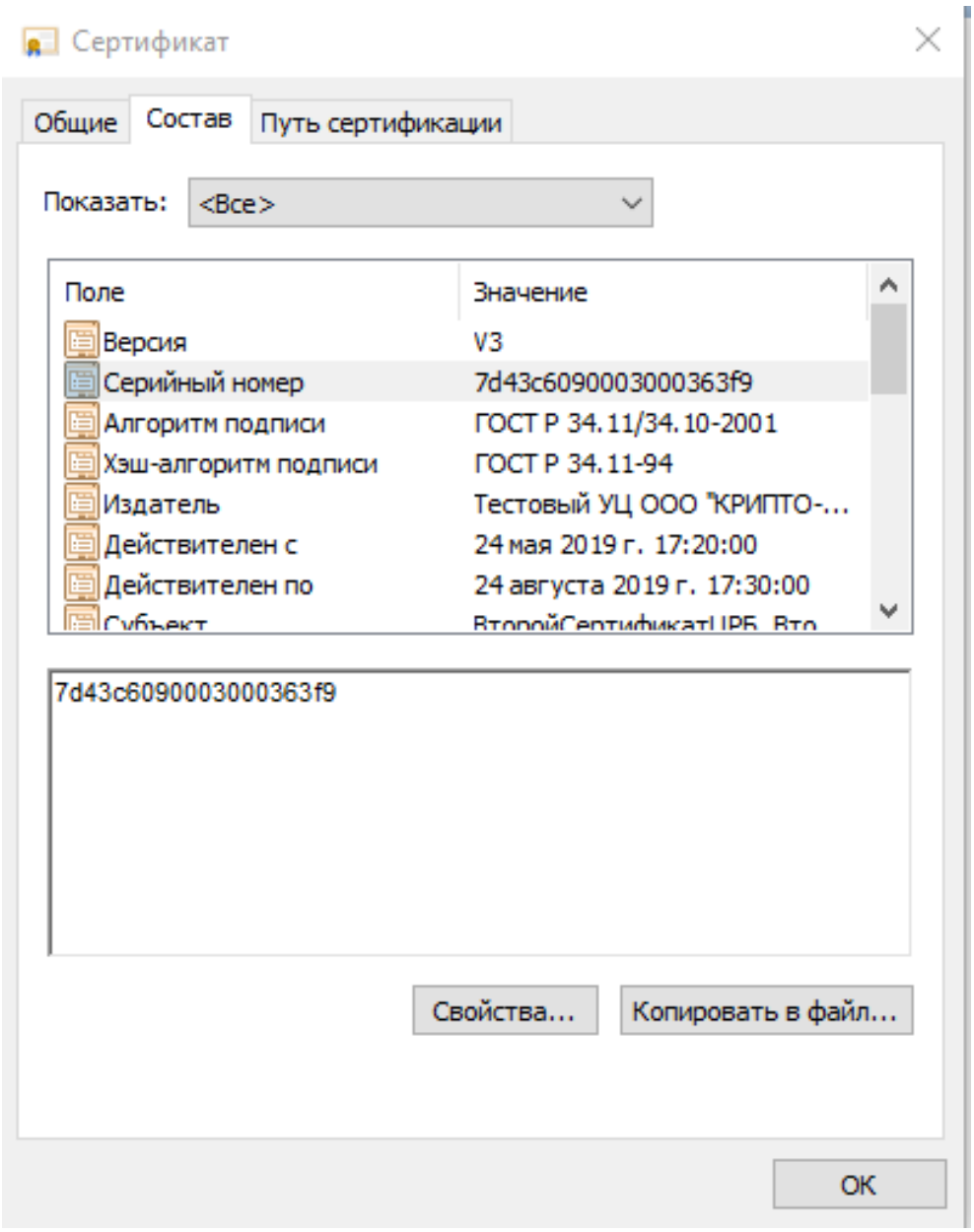

Рисунок 31. Получение номера сертификата

3. В сервисе Аккаунтов модуля «Аптека» /account пункт меню «Администрирование» – «Организации» найдите нужную организацию, нажмите «Редактировать». Перейдите в раздел «Пользователи». Откройте на редактирование пользователя с ролью «Руководитель организации». Перейдите в раздел «Сертификаты». Нажмите «Добавить» (Рисунок 32).

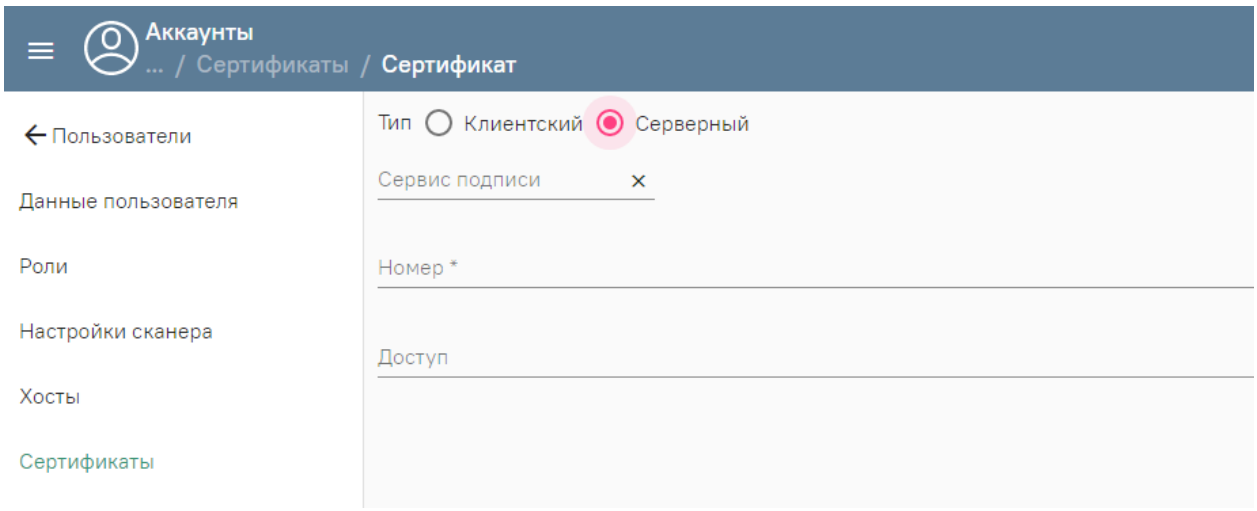

Рисунок 32. Настройка «Сертификаты»

Выберите «Тип»:

- «Клиентский» – в случае, если сертификат установлен на рабочем месте пользователя.
- «Серверный» – в случае, если сертификат установлен на сервере медицинской организации или ЦОД.

«Сервис подписи» – доступен только при выборе типа «серверный», выберите из списка адрес сервиса подписи.

«Номер» – укажите номер сертификата, указывается без пробелов.

«Доступ» – указываются роли пользователей, для которых будет доступно использование сертификата (т.е. пользователь разрешает работать со своим сертификатом пользователям, у которых есть указанные роли).

Нажмите «Сохранить» внизу страницы.

4. Проверку настроек сервиса подписи можно произвести в модуле «Аптека» – «администрирование» – «Настройки пользователей». Необходимо открыть пользователя на редактирование и перейти в «МДЛП настройки», далее нажать кнопку «ТЕСТ».

5.2 Настройка TLS/SSL соединения для МДЛП

1. Установите сертификаты удостоверяющего центра в доверенные корневого центра локального компьютера:

- crypto.cer
- minkom.cer

2. Добавьте запись DisableClientExtendedMasterSecret (dword) в реестре HKLM\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL со значением 1 (Рисунок 33).

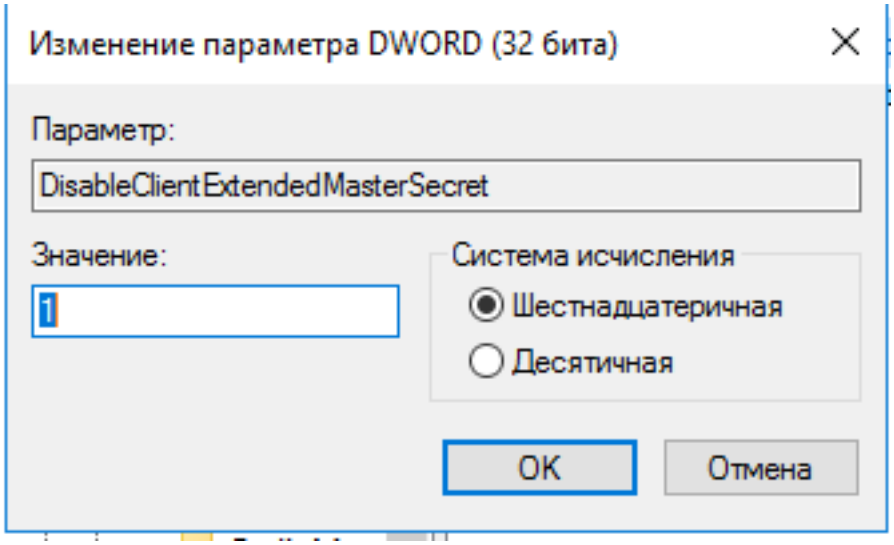

Рисунок 33. Изменение параметра DWORD

4. Для взаимодействия с МДЛП должны быть открыты порты (Информация от СТП «Честного знака»): 21301, 21401, 443, 8080, 48484, 80.

5. Должны быть открыты порты сервиса подписи.

5.3 Настройка параметров подключения к МДЛП

1. Зайдите в личный кабинет МДЛП. **Продуктивный контур** https://mdlp.crpt.ru/index.html#/auth/signin.

2. Перейдите в пункт «Администрирование» – «Учетные системы». Запомните содержимое полей «Идентификатор клиента» и «Секретный код». Если учетной системы нет, то добавьте ее по кнопке «Добавить учетную систему». Введите название и нажмите «Зарегистрировать» (Рисунок 34).

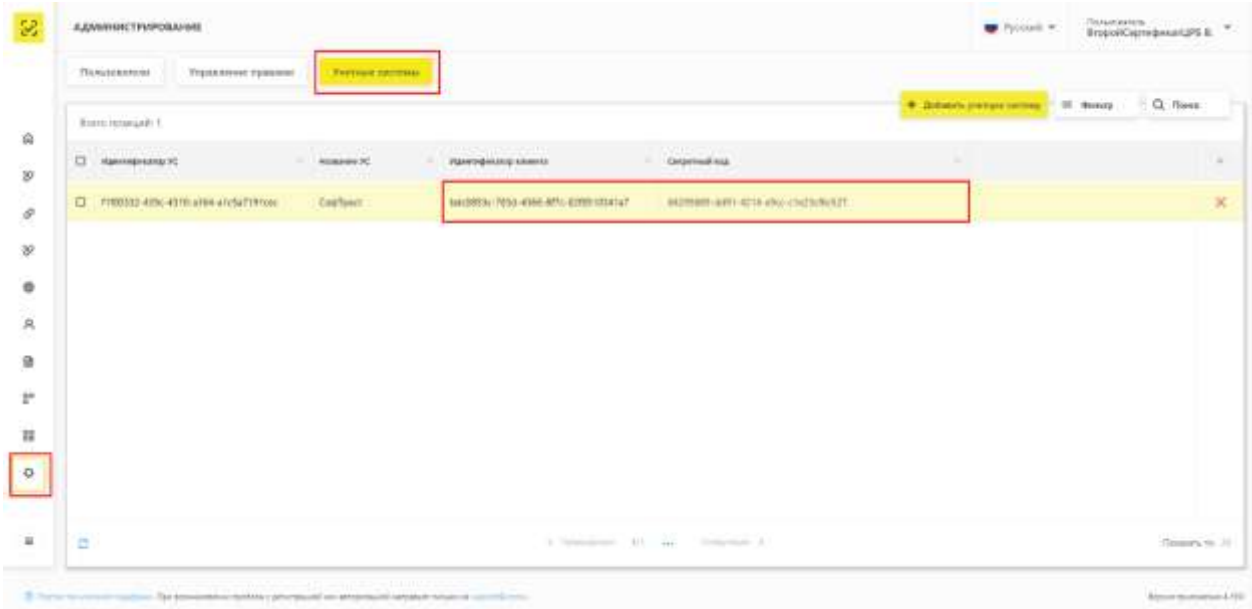

Рисунок 34. Вкладка «Учетные системы»

3. В модуле «Аптека» перейдите в пункт «Администрирование» – «МДЛП

настройки» и добавьте следующие настройки (Рисунок 35):

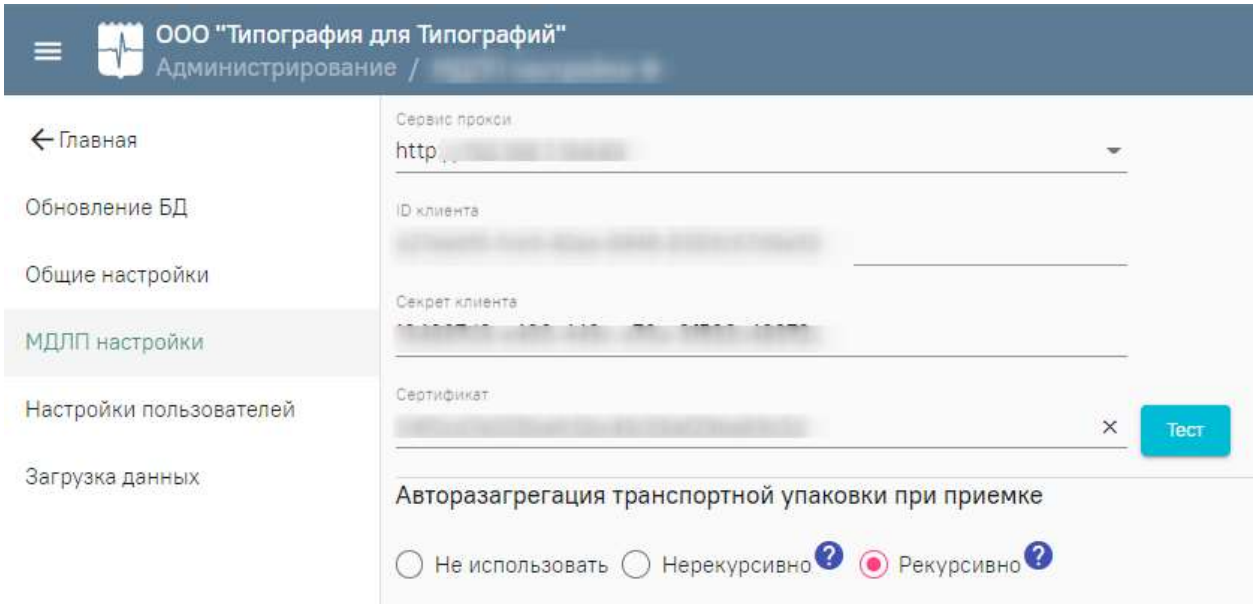

Рисунок 35. Настройки МДЛП

«Сервис прокси» – выбирается из списка, список состоит из адресов сервиса подписи.

«ID клиента» – Идентификатор клиента (п.2).

«Secret клиента» – Секретный код (п.2).

«Сертификат» – выбирается из списка, список состоит из сертификатов.

4. Проверку настроек можно произвести, нажав кнопку «ТЕСТ».

5.4 Настройка Регистратора выбытия (РВ)

Регистратор выбытия (РВ) – устройство для фиксации факта выдачи лекарства по льготным рецептам и вывода лекарств из оборота для оказания медицинской помощи.

Настройка РВ производится на вкладке «Регистраторы выбытия» раздела «Структура организации»:

1. Просмотрите документацию к РВ и переключите его в сетевой режим.

2. Проверьте доступность РВ: он должен находится в одной сети с рабочим местом пользователя. Так как вызовы к РВ будут проходить напрямую из браузера, необходимо убедиться, что запрос к устройству прошел успешно. Для этого откройте командную строку и выполните команду: **ping <ip адрес РВ>.** В случае ошибки проверьте настройки сети – возможно VipNet блокирует отправку, и нужно добавить соответствующее правило.

3. В сервисе аптеки на вкладке «Регистраторы выбытия» выберите «Добавить» или отредактируйте уже созданный РВ. На экране отобразится следующая форма (Рисунок 36):

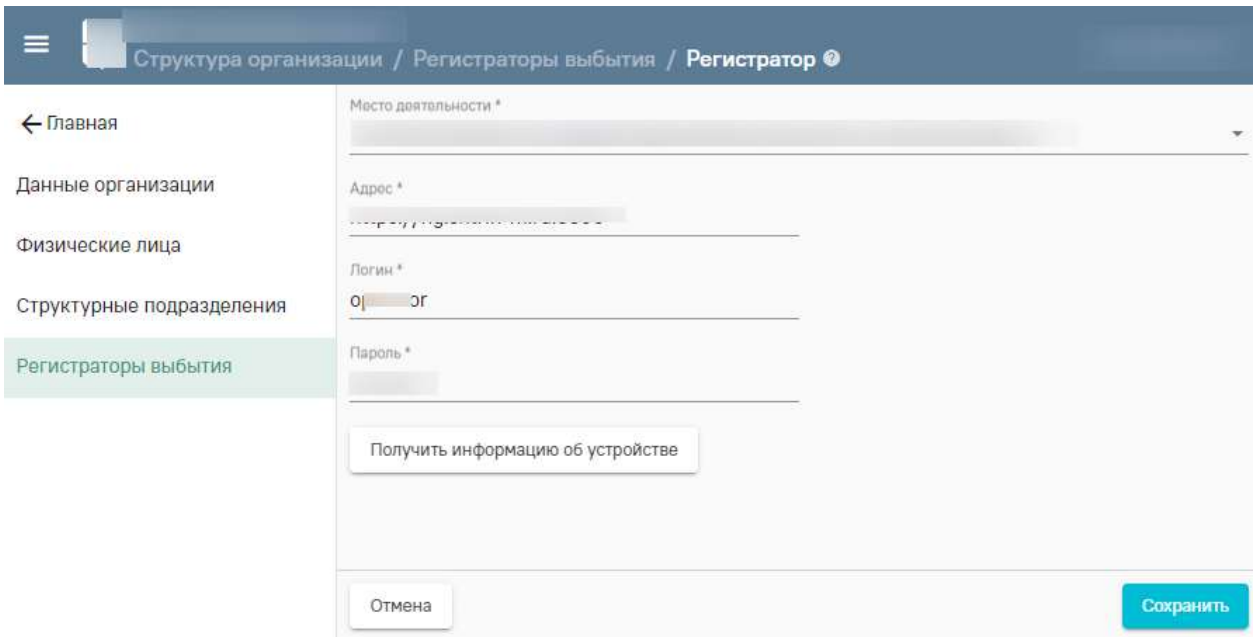

Рисунок 36. Добавление настройки «Регистратор выбытия»

4. Введите настройки РВ и нажмите «Сохранить» (Таблица 1).

Таблица 1. Настройки РВ

Наименование настройки	РВ Штрих 	РВ Атол 	Пример
Адрес	https://<ip **регистратора выбытия>:8080**	https://<ip **регистратора выбытия>:8443**	https://192.168.0.1:8080
Логин	**operator**	**user2**	
Пароль	**123456**	**qwE123xx**	
Место деятельности	**Указывается место деятельности, которое указано у склада.**	**Указывается место деятельности, которое указано у склада.**	

5. Нажмите «Получить информацию об устройстве». Если вы получили информацию, то настройка РВ выполнена. В противном случае проверьте правильность внесения настроек и доступность РВ через ping.

5.5 Загрузка МД организации

Для загрузки мест деятельности организации необходимо зайти в раздел «Справочники» -> «Контрагенты». В данном справочнике выполнить поиск нужной организации, после нажать кнопку для редактирования данных.

Слева в меню необходимо выбрать раздел «Места деятельности». При помощи кнопки «Загрузить» загрузить нужные адреса мест деятельности предварительно отметив их галочкой (Рисунок 37).

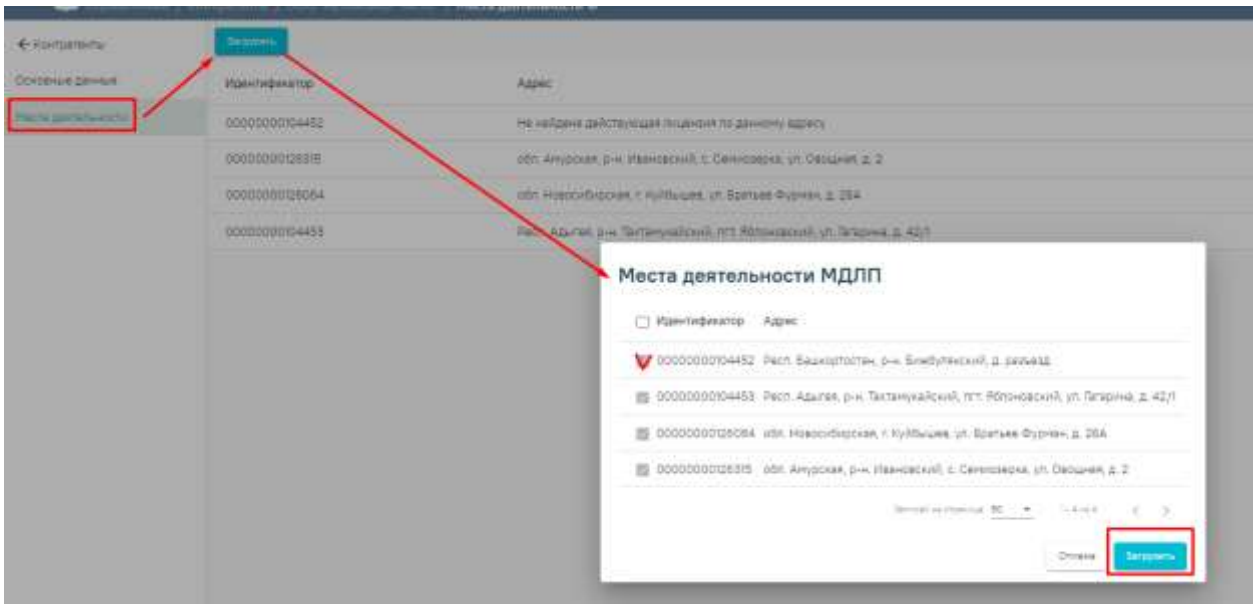

Рисунок 37. Форма «Места деятельности»