Центр сертификатов доступа

Aladdin Enterprise Certificate Authority Certified Edition

Руководство оператора

Изделие	RU.АЛДЕ.03.01.020
Документ	RU.АЛДЕ.03.01.020 34 01
Версия	2.2.0
Листов	75
Дата	23.05.2025

АННОТАЦИЯ

Настоящий документ представляет собой руководство оператора программного средства «Центр сертификатов доступа Aladdin Enterprise Certificate Authority Certified Edition»[1].

Настоящий документ является эксплуатационным документом, содержащим описание действий оператора при работе с программным компонентом «Центр сертификации Aladdin Enterprise Certification Authority»[2], обеспечивающим управление жизненным циклом сертификатов субъектов.

Настоящий документ содержит сведения о назначении программы, условиях его применения, порядке действий оператора по работе с Aladdin eCA CE, сообщениях, выдаваемых оператору в процессе работы.

Настоящий документ соответствует требованиям к разработке эксплуатационной документации, определённым в методическом документе «Требования по безопасности информации, устанавливающие уровни доверия к средствам технической защиты информации и средствам обеспечения безопасности информационных технологий», утверждённого приказам ФСТЭК России от 02 июня 2020 г. №76 по 4 уровню доверия.

Таблица 1 – Соответствие документации требованиям доверия – раздел 16 «Требования к разработке эксплуатационной документации»

Требования доверия (16.1 Руководство пользователя должно содержать описание)	Раздел настоящего документа, в котором представлено свидетельство
режимов работы средства	раздел 2 «Условия выполнения программы»
принципов безопасной работы средств	раздел 2 «Условия выполнения программы»
функций и интерфейсов функций средства, доступных каждой роли пользователей	раздел 4 «Описание функций программы»
параметров (настроек) безопасности средства, доступных каждой роли пользователей, и их безопасных значений	раздел 3 «Выполнение программы»
типов событий безопасности, связанных с доступными пользователю функциями средства	раздел 5 «Сообщения оператору»
действий после сбоев и ошибок эксплуатации средства	раздел 5 «Сообщения оператору»

Перед эксплуатацией программы рекомендуется внимательно ознакомиться с настоящим руководством.

[1] Далее по документу – программа, программное средство, Aladdin eCA

[2]Далее по документы – программный компонент, Центр сертификации Aladdin Enterprise Certificate Authority, Центр сертификации Aladdin eCA

Содержание

1 НАЗНАЧЕНИЕ ПРОГРАММЫ

1.1 Область применения

Программное средство «Центр сертификатов доступа Aladdin Enterprise Certificate Authority Certified Edition» применяется как элемент систем защиты информации автоматизированных (информационных) систем и используется совместно с другими средствами защиты информации при идентификации и строгой аутентификации субъектов и объектов доступа[3] в автоматизированной (информационной) системе.

1.2 Функции программы

Программное средство «Центр сертификатов доступа Aladdin Enterprise Certificate Authority Certified Edition» реализует следующие функции, для выполнения которых оно предназначено в заданных условиях применения:

- формирование идентификационной информации, необходимой для выпуска сертификатов безопасности (цифровых сертификатов) пользователей и средств вычислительной техники (устройств) на основе данных, полученных при первичной идентификации непосредственно от пользователей и средств вычислительной техники (устройств) через заявку на выпуск сертификатов безопасности (цифровых сертификатов), либо полученных от доменной службы каталогов или уполномоченных пользователей;
- выпуск и обслуживание сертификатов безопасности (цифровых сертификатов) пользователей и средств вычислительной техники (устройств), в том числе:
  - создание ключевых пар (открытый и закрытый ключи) пользователей и средств вычислительной техники (устройств);
  - формирование сертификатов безопасности (цифровых сертификатов) для пользователей и средств вычислительной техники (устройств);
  - формирование заявок на выпуск сертификатов безопасности (цифровых сертификатов) для пользователей и средств вычислительной техники (устройств);
  - выдача сертификатов безопасности (цифровых сертификатов) для их использования владельцами;
  - централизованное автоматическое (автоматизированное) отслеживание актуальности (с уведомлением владельцев о сроках действия) сертификатов безопасности (цифровых сертификатов);
- выпуск и обслуживание сертификатов безопасности (цифровых сертификатов) центров сертификации инфраструктуры открытых ключей, в том числе:
  - создание, экспорт, импорт и удаление ключевой пары (открытый и закрытый ключи) центра сертификации (корневого и/или подчиненного);
  - создание, импорт, просмотр, экспорт и удаление корневого (самоподписанного) сертификата центра сертификации;
  - создание, просмотр, экспорт и удаление запроса на сертификат центра сертификации в вышестоящий центр сертификации;
  - создание на основании запроса, импорт, просмотр, экспорт, удаление и отзыв сертификата для подчиненного центра сертификации;

[3] Субъектами доступа могут являться как физические лица (пользователи), так и ресурсы автоматизированной информационной системы, а также вычислительные процессы, инициирующие получение и получающие доступ от имени пользователей, программ, средств вычислительной техники и других программно-аппаратных устройств информационно-телекоммуникационной инфраструктуры.

- приостановка и/или возобновление действия сертификатов безопасности (цифровых сертификатов) пользователей и средств вычислительной техники (устройств), в том числе:
  - блокирование, возобновление действия, отзыв и перевыпуск сертификатов безопасности (цифровых сертификатов);
  - формирование, экспорт и публикация списка отозванных сертификатов безопасности (цифровых сертификатов);

1.3 Уровень подготовки пользователя

Операторы Aladdin eCA CE должны иметь навыки в работе с применением технических средств уровня семейства операционных систем Windows и семейства операционных систем Linux.

2 УСЛОВИЯ ВЫПОЛНЕНИЯ ПРОГРАММЫ

2.1 Поддерживаемые браузеры

Работа с программным компонентом «Центр сертификатов доступа Aladdin Enterprise Certificate Authority Certified Edition» поддерживается через веб-браузеры операционных систем РЕД ОС, Astra Linux Special Edition и Альт.

2.2 Поддерживаемые ключевые носители

Поддерживаемые модели электронных ключей (ключевых носителей):

- JaCarta PKI;
- JaCarta PRO;
- JaCarta-2 PKI/ГОСТ;
- JaCarta-2 ГОСТ.

2.3 Режим функционирования программы

Центр сертификатов доступа Aladdin Enterprise Certificate Authority Certified Edition функционирует в следующих режимах:

- штатный режим, при котором программа должна исправно функционировать, обеспечивая возможность круглосуточного выполнение задач и функций в полном объёме;
- сервисный режим, необходимый для проведения обслуживания (обновления программы).

Основным режимом функционирования программного средства «Центр сертификатов доступа Aladdin Enterprise Certificate Authority Certified Edition» является штатный режим.

Аварийный режим работы, при отказах/сбоях серверного общесистемного и специального программного обеспечения и оборудования, не предусматривается.

2.4 Доступ к программе

Для получения доступа к программному компоненту «Центр сертификации Aladdin Enterprise Certification Authority» необходимо обратиться к уполномоченному лицу, исполняющему обязанности администратора Центра сертификации для:

- создания новой учётной записи с ролью «Оператор» и выпуска сертификата в контейнере p12 для созданной учётной записи оператора.
- передачи сертификата лицу, исполняющему обязанности «Оператора», в контейнере p12 с атрибутом безопасности (паролем от контейнера) для дальнейшей аутентификации на веб-сервере Центра сертификации.

2.5 Принципы безопасной работы программного средства

К основным принципам безопасной работы программного средства относятся:

- выполнение ограничений по эксплуатации программного средства, приведённых в разделе 2 «Условия выполнения программы» настоящего документа;
- контроль физической сохранности средств вычислительной техники с установленным Средством двухфакторной аутентификации;
- сохранение в секрете пароля (PIN-кода) пользователя;
- исключение доступа посторонних лиц к персональному идентификатору.

3 ВЫПОЛНЕНИЕ ПРОГРАММЫ

3.1 Запуск программы

- Запуск служб программного компонента осуществляет администратор Центра сертификации на сервере, где развёрнут Центр сертификации Aladdin Enterprise Certification Authority.
- Оператору предоставляется доступ к клиентской части посредством веб-интерфейса. Для запуска клиентской части Центра сертификации Aladdin Enterprise Certification Authority запустите браузер;
- Выберите сертификат доступа аутентифицирующегося пользователя (см. Рисунок 3);
- В адресную строку браузера введите IP-адрес или полное доменное имя сервера, выдавшего импортированный сертификат доступа, на котором произведена установка программного компонента «Центр сертификации Aladdin Enterprise Certification Authority». Например:

```
https://172.22.5.21
```

3.2 Доступ пользователей к программе

3.2.1 Аутентификация с использованием сертификата, перенесённого на жесткий диск

Полученный оператором контейнер сертификат доступа для аутентификации на веб-сервере Центра сертификации Aladdin Enterprise Certification Authority необходимо перенести любым удобным способом на жёсткий диск СВТ для его дальнейшей установки в хранилище сертификатов браузера для сохранения информации о доверенных сертификатах с целью успешного подключения к серверу на клиентской стороне.

Для установки сертификата в доверенное хранилище сертификатов вашего браузера выполните нижеописанные действия. Процесс установки сертификата доступа в доверенное хранилище рассмотрим на примере браузера Firefox:

- Откройте браузер Firefox – Настройки – Приватность и Защита – Сертификаты (см. Рисунок 1). Нажмите кнопку <Просмотр сертификатов>.

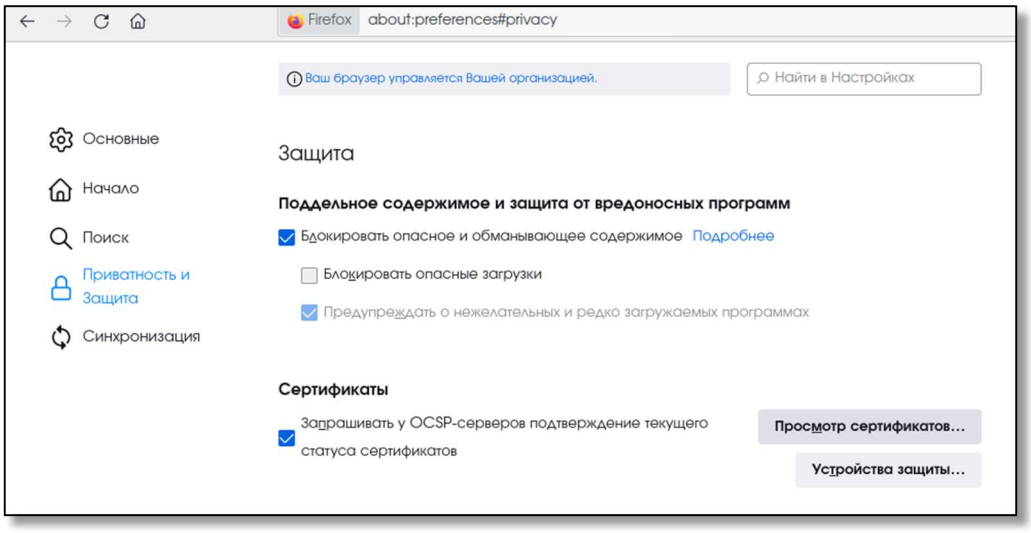


Рисунок 1 – Окно настроек браузера

- Выберите вкладку «Ваши сертификаты», в открывшейся вкладке нажмите кнопку <Импортировать> (см. Рисунок 2).

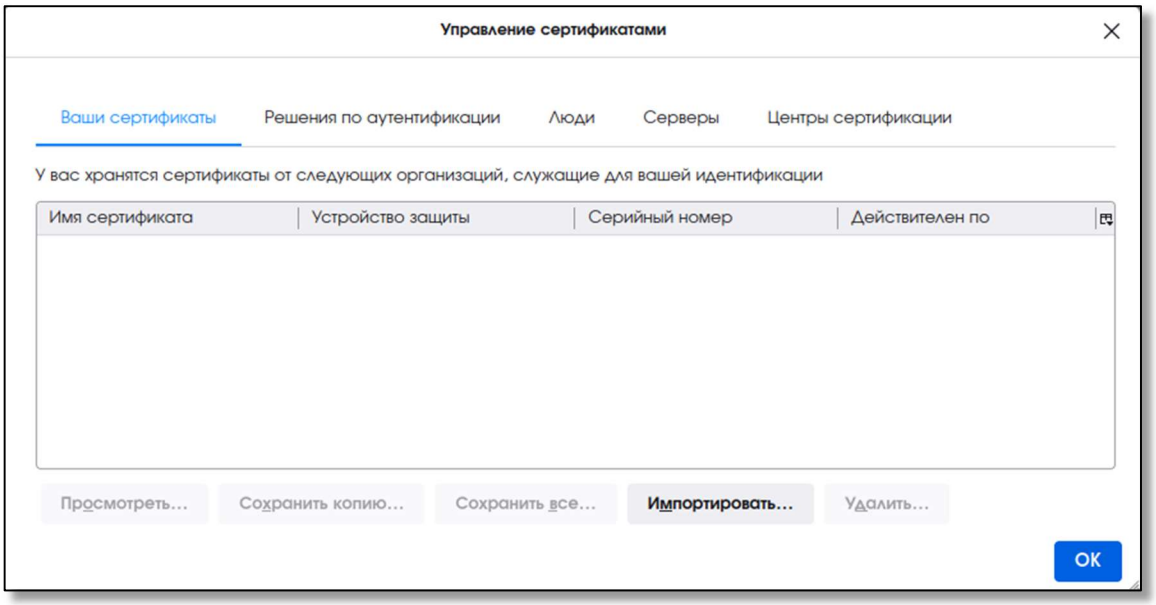


Рисунок 2 – Окно управления сертификатами

- Выберите контейнер .p12, содержащий закрытый ключ и сертификат доступа, перенесённый на жесткий диск, выпущенный для учётной записи пользователя (см. Рисунок 3).

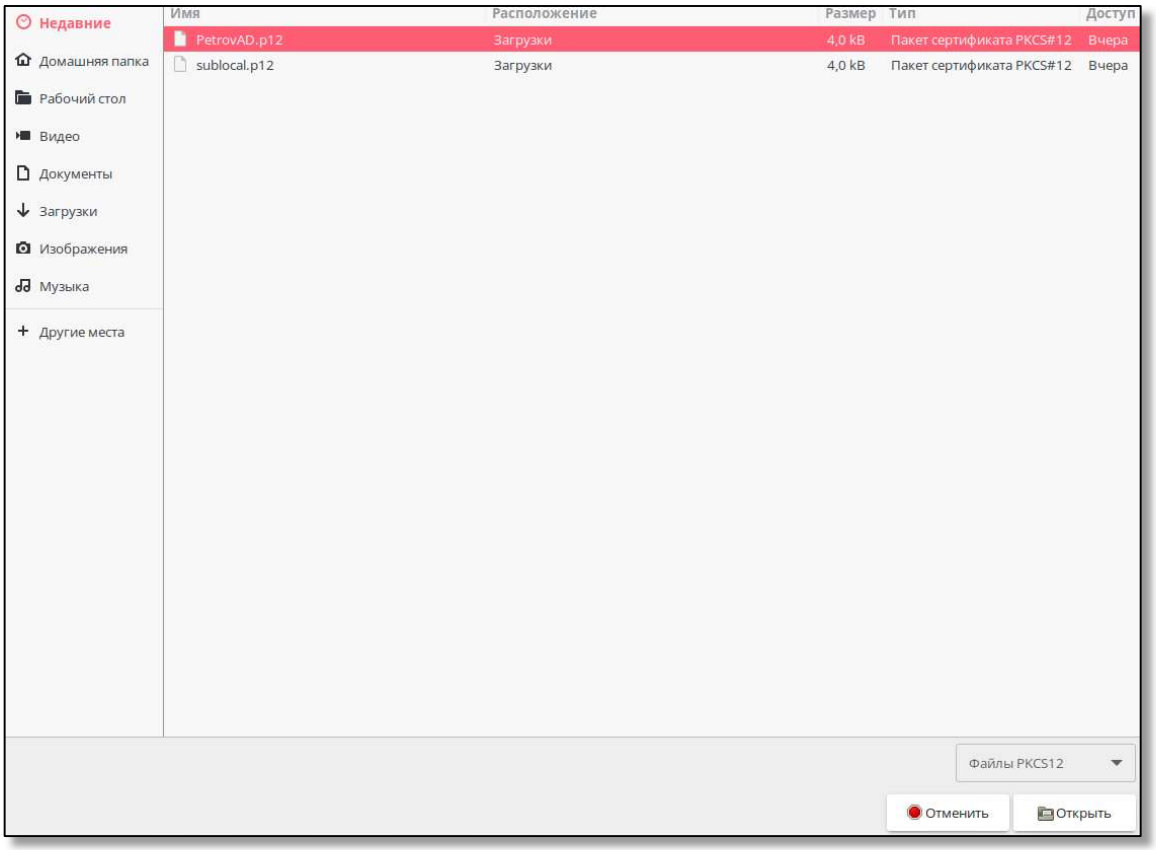


Рисунок 3 – Окно выбора импортируемого файла сертификата

- Введите пин-код загружаемого контейнера .p12 в открывшемся окне и нажмите кнопку <Ок> (см. Рисунок 4). Пин-код сертификата является атрибутом безопасности и должен быть передан администратором с контейнером закрытого ключа и сертификата.

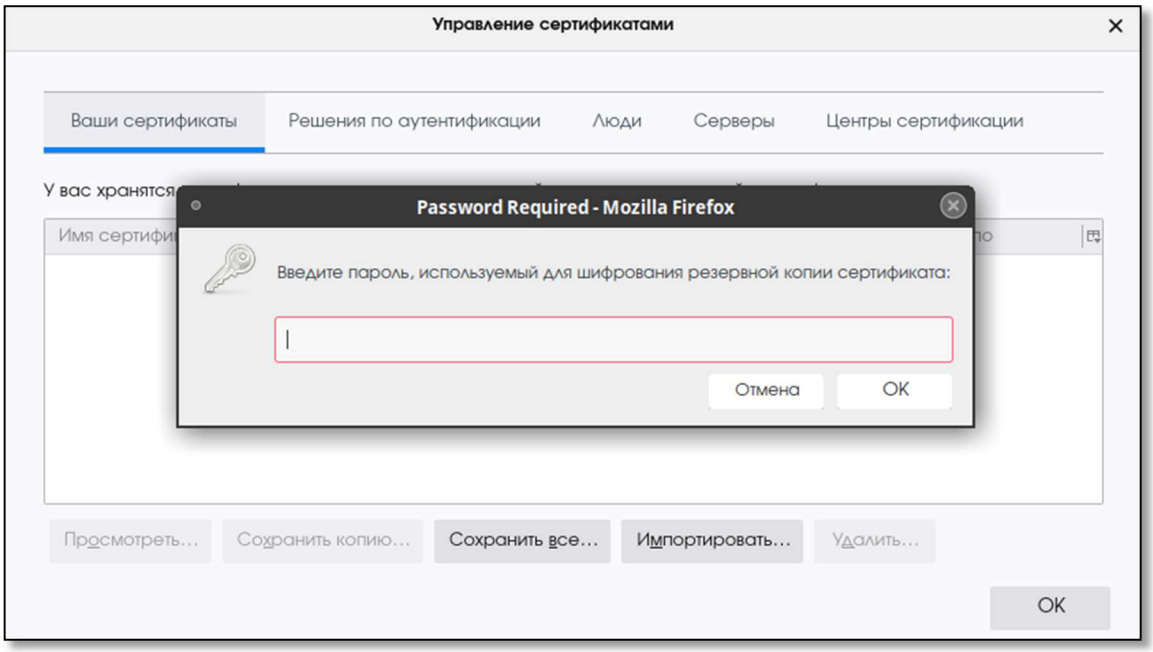


Рисунок 4 – Окно ввода пин-кода сертификата

- В таблице окна «Управление сертификатами» появится запись об импортированном сертификате (см. Рисунок 5). Нажмите кнопку <OK>.

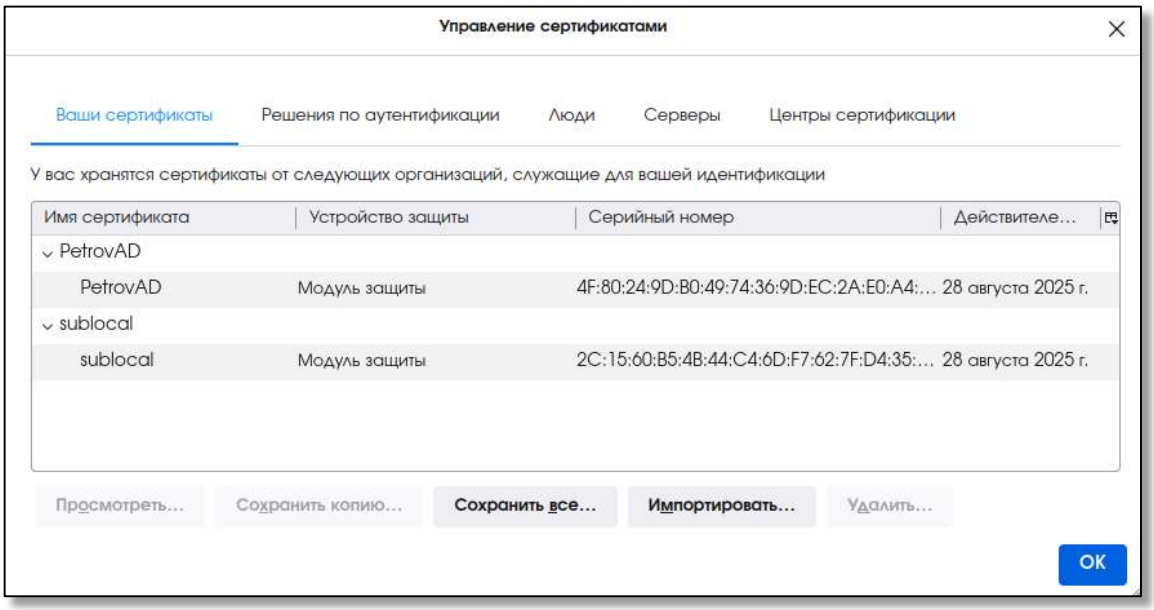


Рисунок 5 – Окно «Управление сертификатами»

- В адресную строку браузера введите ip-адрес или полное доменное имя сервера, выдавшего импортированный сертификат доступа, на котором произведена установка программного компонента «Центр сертификации Aladdin Enterprise Certification Authority».

Например:

```
https://sub02.presale.aeca
```

> **Для безопасного доверенного соединения при обращении к серверу Центра сертификации используйте доменное имя, указанное в атрибуте сертификата веб-сервера Subject alternative name (SAN) и соответственно указанное в конфигурационном файле `/etc/hosts/` сервера.**

- В открывшемся окне выберите сертификат для аутентификации на веб-сервере Центра сертификации Aladdin Enterprise Certification Authority (см. Рисунок 6). Нажмите кнопку <OK>.

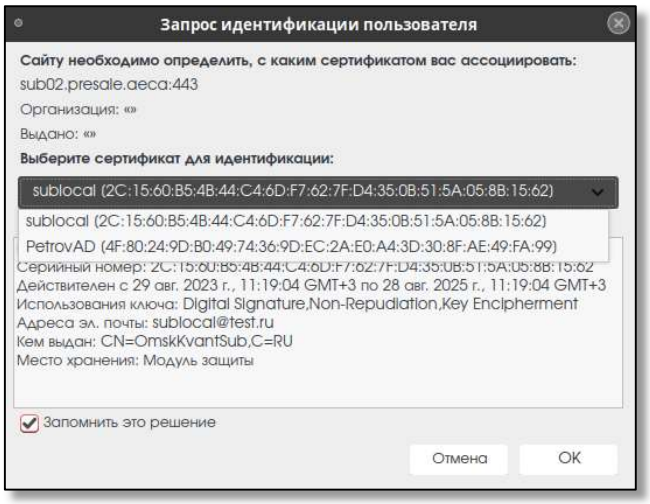


Рисунок 6 – Окно выбора сертификата для аутентификации

- Далее откроется страница с предупреждением системы безопасности (см. Рисунок 7). Нажмите кнопку <Дополнительно>.

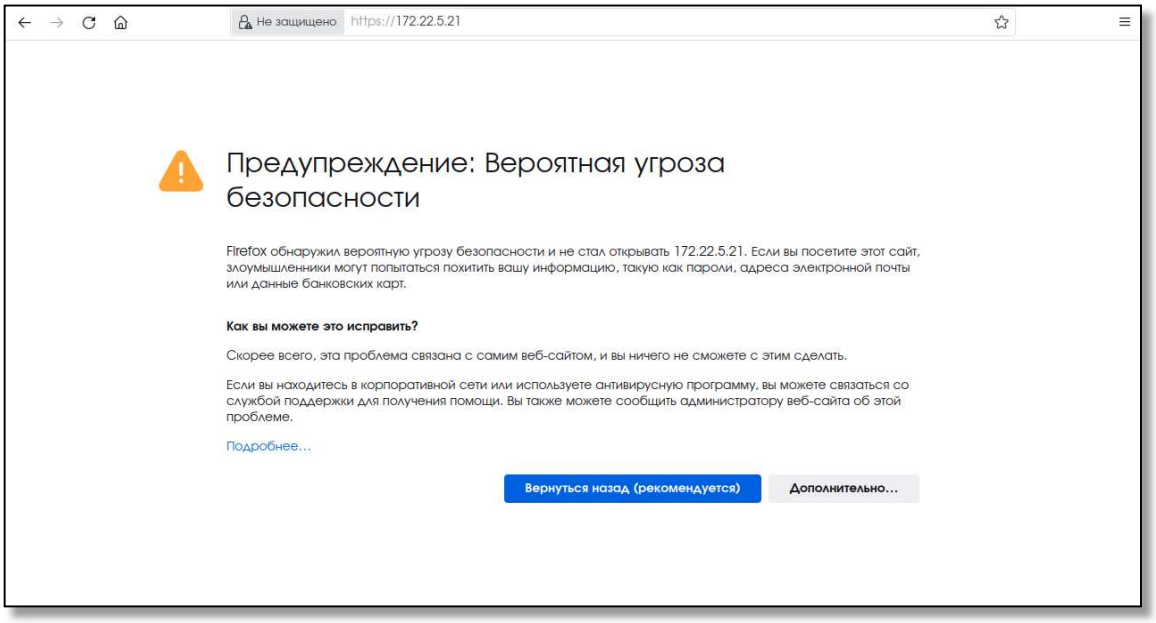


Рисунок 7 – Страница с предупреждением системы безопасности

- По нажатию кнопки <Дополнительно> на странице предупреждения системы безопасности осуществляется переход на страницу ошибки распознавания сертификата (см. Рисунок 8). Нужно принять риски, нажав кнопку <Принять риск и продолжить> на текущей странице.

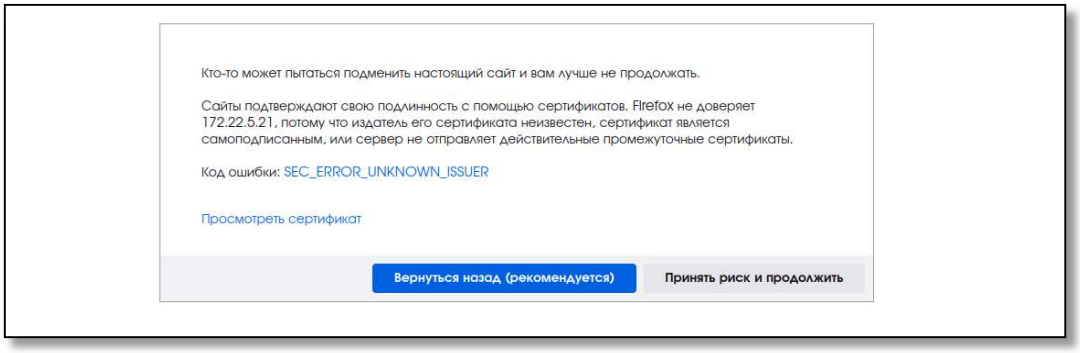


Рисунок 8 – Страница ошибки распознавания сертификата

- В случае отказа в доступе к веб-интерфейсу Центра сертификации Aladdin Enterprise Certification Authority Оператор будет уведомлен сообщением об ошибке. Возможные причины отказа:
  - сертификат доступа пользователя не импортирован в доверенное хранилище браузера;
  - отсутствие издателя сертификата доступа, импортированного в доверенное хранилище браузера, в списке разрешённых издателей веб-сервера;
  - остановка работы служб Центра сертификации на веб-сервере;
  - срок действия сертификата доступа истёк;
  - действия сертификата было приостановлено или сертификат отозван.

В случае отказа доступа обратитесь к Администратору Центра сертификации Aladdin Enterprise Certification Authority.

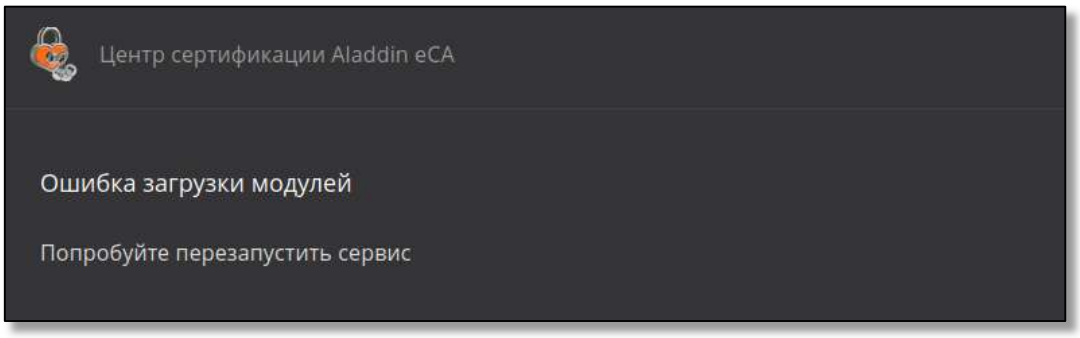


Рисунок 9 – Окно «Управление сертификатами»

- В случае успешной аутентификации пользователя будет сформировано защищённое соединение клиент – сервер и предоставлен доступ к веб-интерфейсу Центра сертификации Aladdin Enterprise Certification Authority.

3.2.2 Аутентификация с использованием сертификата на ключевом носителе

3.2.2.1 Первичная настройка СВТ для двухфакторной аутентификации оператора по сертификату на ключевом носителе

Для настройки сначала выполните установку Единого Клиента JaCarta (см. подраздел 3.2.2.2), а затем выполните настройку браузера (настройку Firefox см. в подразделе 3.2.2.3, настройку Chromium в зависимости от ОС см. в подразделах 3.2.2.3.1 и 3.2.2.4).

3.2.2.2 Установка Единого Клиента JaCarta

- Для поддержки ключевых носителей произведите установку Единого Клиента JaCarta, для этого:
  - Скопируйте на компьютер в одну папку файлы из дистрибутива для дальнейшей инсталляции:
    - install.sh;
    - jacartauc_*_ro_x64.rpm;
    - jcpkcs11-2_*_x64.rpm;
    - jcsecurbio_*_x64.rpm;
    - RPM-GPG-KEY-ALADDIN_RD-AO.public (Открытый ключ АО "Аладдин Р.Д.").
  - Под пользователем с правами администратора запустите эмулятор терминала.
  - В эмуляторе терминала прейдите в папку с дистрибутивами, выполнив команду:

```
cd …/…/…
```

  - Установите Единый Клиент JaCarta, выполнив команду:

```
bash install.sh
```

Подробное описание процедуры установки Единого Клиента JaCarta приведено в разделе 4 RU.АЛДЕ.03.01.013-01 32 01-2 «Единый Клиент JaCarta. Руководства администратора «Аладдин Р.Д.».

- Только для **ОС Astra Linux Special Edition 1.7** произведите подготовку операционной системы, установив дополнительную библиотеку службы сетевой безопасности, выполнив команду от имени текущего пользователя:

```
apt install libnss3-tools
```

Текущий локальный пользователь должен иметь права на файлы в папке ~/.pki/nssdb/.

- Рекомендуется очистить кэш браузера и ранее применённые решения по аутентификации в браузере (для браузера Firefox: Настройки -> Приватность и защита -> Сертификаты -> Просмотр сертификатов).

3.2.2.3 Настройка браузера Firefox для РЕД ОС, Альт 8 СП релиз 10, Astra Linux Special Edition

- Выполните настройку браузера **Firefox**, если подключение к серверу Центра сертификации Aladdin Enterprise Certification Authority будет выполнено в этом браузере:
  - откройте Настройки -> Приватность и защита -> Сертификаты -> Устройства защиты;
  - в диалоговом окне нажмите кнопка <Загрузить>;
  - в окне загрузки драйвера нажмите кнопку <Обзор> и выберите файл модуля `/lib64/libjcPKCS11-2.so` (см. Рисунок 10) и подтвердите загрузку модуля, нажав кнопку <OK>;

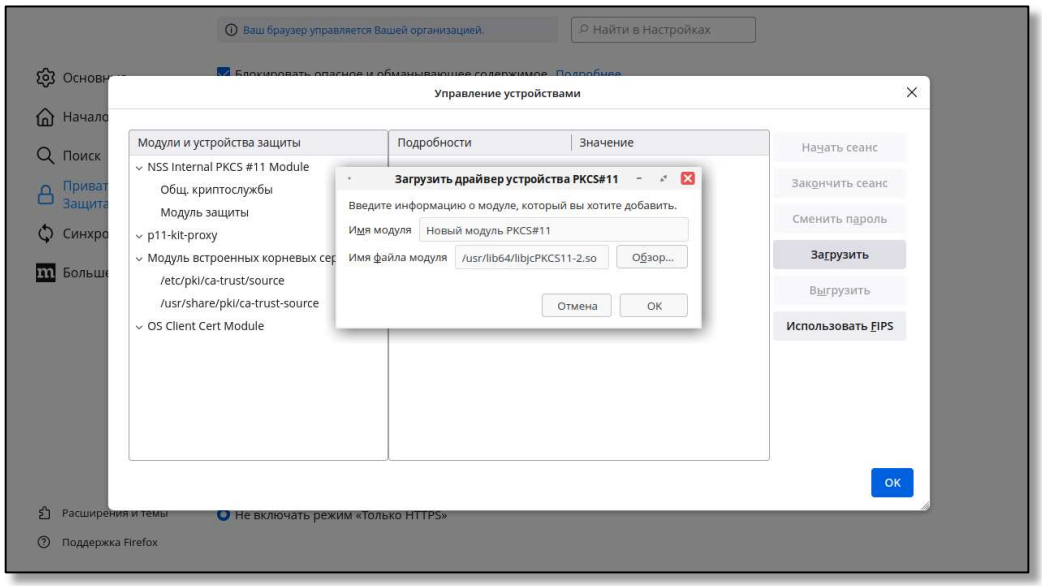


Рисунок 10 – Настройка браузера Firefox

  - перезапустите браузер.

3.2.2.3.1 Настройка браузера Chromium для РЕД ОС и Альт 8 СП релиз 10

- Выполните настройку браузера **Chromium**, если подключение к серверу Центра сертификации Aladdin Enterprise Certification Authority будет выполнено в этом браузере посредством **ОС РЕД ОС** или **Альт 8**:
  - удалите каталог локальной библиотеки сертификатов, выполнив команду:

```
rm -rf ~/.pki
```

  - создайте каталог локальной библиотеки сертификатов, выполнив команду под текущим пользователем:

```
mkdir ~/.pki/nssdb
```

– инициализируйте локальную библиотеку сертификатов, выполнив команду под текущим пользователем:

```
certutil --empty-password -d ~/.pki/nssdb -N
```

– подключите модуль к локальной библиотеке сертификатов `nssdb`, выполнив команду под текущим пользователем:

```
modutil -dbdir sql:.pki/nssdb/ -add "JaCarta" -libfile /usr/lib64/libjcPKCS11-2.so
```

– перезапустите браузер.

3.2.2.4 Настройка браузера Chromium для Astra Linux Special Edition

- Выполните настройку браузера **Chromium**, если подключение к серверу Центра сертификации Aladdin Enterprise Certification Authority будет выполнено в этом браузере посредством **Astra Linux Special Edition**:

– подключите модуль `nssdb` для работы с сертификатами, выполнив команду:

```
modutil -dbdir sql:.pki/nssdb/ -add "JaCarta" -libfile /lib/libjcPKCS11-2.so
```

– перезапустите браузер.

3.2.2.5 Двухфакторная аутентификации оператора по сертификату на ключевом носителе

- Полученный оператором ключевой носитель с записанным на нём сертификатом доступа для аутентификации на веб-сервере Центра сертификации Aladdin Enterprise Certification Authority необходимо подключить в USB-порт предварительного настроенного средства вычислительной техники – рабочего места оператора для его дальнейшей аутентификации с целью успешного подключения к серверу на клиентской стороне.
- Откройте браузер, для которого была выполнена первичная настройка двухфакторной аутентификации, и введите в адресную строку ip-адрес или полное доменное имя сервера, выдавшего импортированный сертификат доступа, на котором произведена установка программного компонента «Центр сертификации Aladdin Enterprise Certification Authority».

Например:

```
https://sub02.presale.aeca
```

- В появившемся окне введите PIN-код ключевого носителя.

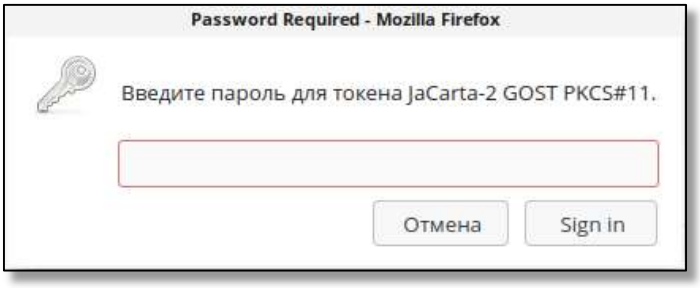


Рисунок 11 – Окно ввода PIN-кода ключевого носителя

- В появившемся окне выберите сертификат с подключенного ключевого носителя.

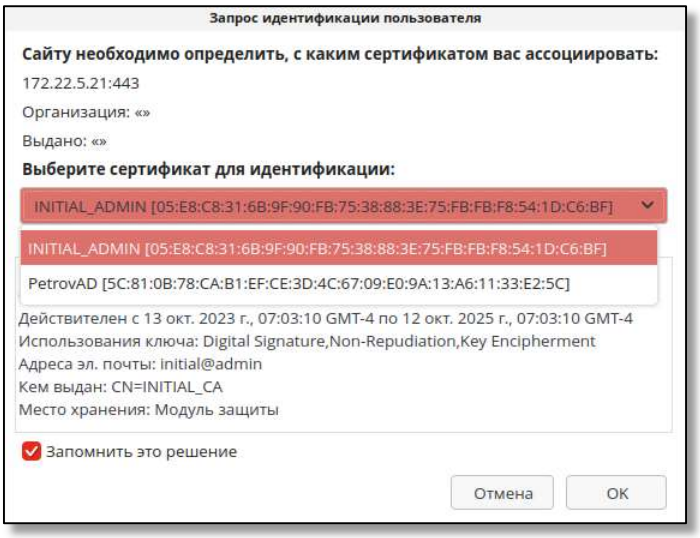


Рисунок 12 – Окно выбора сертификата пользователя для аутентификации на сервере

Время действия токена доступа – 3 минуты.

Время действия токена обновления – 24 часа, то есть по истечению времени действия токена обновления будет требоваться повторная аутентификация пользователя для доступа к серверу Центра сертификации.

4 ОПИСАНИЕ ФУНКЦИЙ ПРОГРАММЫ

4.1 Описание верхней панели «Центра сертификации»

Верхняя панель (см. Рисунок 13) Центра сертификации фиксирована и отображается на любом шаге или переходе между вкладками.

Рисунок 13 – Верхняя панель окна «Центра сертификации»

При наведении курсора на иконку панели всплывает соответствующее текстовое пояснение для каждого элемента.

Верхняя панель содержит следующие элементы:

- 

- тип активного ЦС (возможные варианты: Корневой или Подчиненный);

- 

- обозначение статуса ЦС.

  При отсутствии ошибок и предупреждений отображается активный статус:
  - активный  . При наведении курсора отображается всплывающее сообщение «Активный»;

  Индикатор «треугольник с восклицательным знаком» присутствует в следующих случаях:
  - истёк срок действия сертификата текущего активного ЦС  . При наведении курсора отображается всплывающее сообщение «Истек срок действия сертификата ЦС»;
  - истекает[4] срок действия сертификата текущего активного ЦС  . При наведении курсора отображается всплывающее сообщение «Истекает срок действия сертификата ЦС»;
  - закрытый ключ ЦС недоступен[5]  . При наведении курсора отображается всплывающее сообщение «Закрытый ключ центра сертификации недоступен».
  - истёк срок действия лицензии  . При наведении курсора отображается всплывающее сообщение «Истек срок действия лицензии»;
  - достигнуто лицензионное ограничение на количество

[4] До истечения остаётся менее 90 дней.

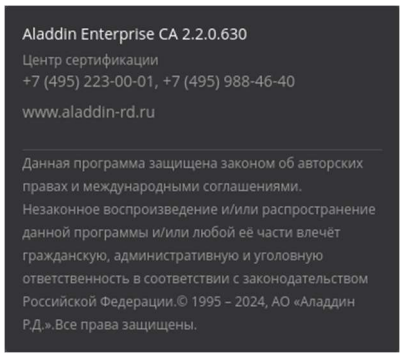
[5] При запуске серверного компонента Aladdin eCA не удалось получить закрытый ключ данного ЦС, что может быть обусловлено удалением или повреждением локально хранимого контейнера закрытого ключа либо отсутствием доступа к криптопровайдеру алгоритма, по которому была создана ключевая пара данного ЦС.

субъектов с действующими сертификатами  . При наведении курсора отображается всплывающее сообщение «Достигнуто предельное количество субъектов с действующими сертификатами по лицензии».

- 

- имя текущего активного ЦС. При наведении курсора всплывают заданные имя и значения суффикса различающегося имени ЦС;
- 

- отображаемое имя текущего активного ЦС;
- 

- текущая авторизация учётной записи пользователя;
- 

- сведения о текущей версии программного компонента, контактная информация разработчика.

4.2 Описание боковой панели «Центра сертификации»

В зависимости от ширины окна браузера боковая панель может:

- либо быть закрепленной и отображаться на любом шаге или переходе между разделами (при ширине окна браузера более или равной 1200px). При этом боковая панель отображается в полном (см. Рисунок 14) или компактном (см. Рисунок 15) виде. Выбор вида боковой панели происходит по нажатию кнопки  , расположенной внизу данной панели;
- либо быть скрытой и отображаться только после нажатия на кнопку  , которая отображается только в данном режиме (при ширине окна браузера менее 1200px).

Полный вид боковой панели при отсутствии у оператора доступа к шаблонам показан на Рисунок 14, компактный вид боковой панели при отсутствии у оператора доступа к шаблонам приведен на Рисунок 15. Выбор вида боковой панели происходит по нажатию кнопки  , расположенной внизу данной панели.

Рисунок 14 – Полный вид боковой панели (при отсутствии у оператора доступа к шаблонам)

Рисунок 15 – Компактный вид боковой панели (при отсутствии у оператора доступа к шаблонам)

Полный вид боковой панели при наличии у оператора доступа к шаблонам показан на Рисунок 14, компактный вид боковой панели при наличии у оператора доступа к шаблонам приведен на Рисунок 15.

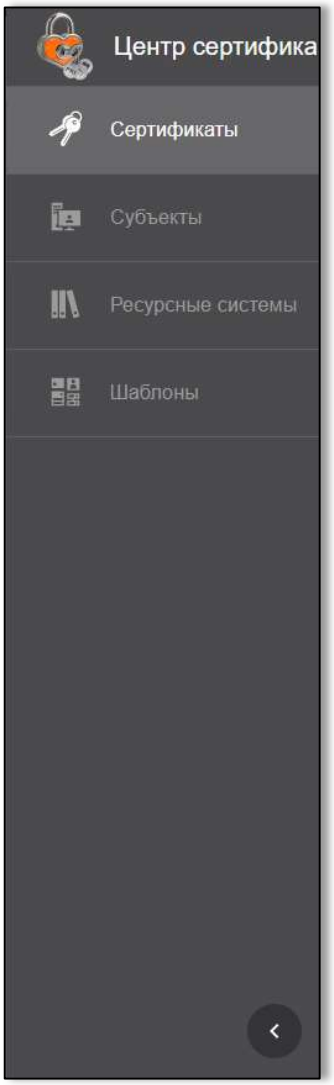


Рисунок 16 – Полный вид боковой панели (при наличии у оператора доступа к шаблонам)

Рисунок 17 – Компактный вид боковой панели (при наличии у оператора доступа к шаблонам)

Боковая панель состоит из разделов, определяющих соответствующие функции программы, доступные учётной записи с ролью «Оператор», и созданы для организации управления выпуском и жизненным циклом сертификатов доступа:

- Раздел «Сертификаты» – в данном разделе возможно:
  - посмотреть список всех выпущенных сертификатов субъектов, издателем которых является активный ЦС, с отображением статуса сертификата, срока действия, типа субъекта, имени субъекта и серийного номера сертификата;
  - произвести поиск выпущенных сертификатов по имени субъекта или серийному номеру;
  - отозвать или приостановить действие выпущенного сертификата субъекта;
  - посмотреть карточку выпущенного сертификата субъекта;
  - скачать сертификат субъекта в формате .pem;
  - скачать цепочку сертификатов;
  - скачать список выпущенных сертификатов в формате .csv;
  - применить массовые операции к выбранным сертификатам (отзыв, приостановка, возобновление);
- Раздел «Субъекты» – в данном разделе возможно:
  - произвести поиск субъекта по его имени (или части имени);

- обновить список групп и субъектов;
- посмотреть организационные группы субъектов локальной и подключенных ресурсных систем;
- посмотреть существующие субъекты;
- выпустить сертификат с закрытым ключом PKCS#12 для субъекта;
- выпустить сертификат на основании запроса для субъекта;
- выпустить сертификат на ключевом носителе для субъекта;
- посмотреть все выпущенные сертификаты для каждого субъекта;
- создать учётную запись для субъекта из группы «Users»;
- посмотреть карточку субъекта;
- опубликовать сертификат субъекта в ресурсную систему;

- Вкладка «Ресурсная система» – на данной вкладке возможно:
  - обновить список субъектов ресурсной системы и их данных в ручном режиме.
- Вкладка «Шаблоны», доступная оператору только при наличии у него доступа к шаблонам, – на данной вкладке возможно:
  - просмотреть шаблоны, доступные оператору для использования при создании сертификатов.

Далее в настоящем документе приводится полное описание доступных функций управления Центром сертификации для каждой вкладки.

4.3 Раздел «Сертификаты»

Раздел «Сертификаты» обеспечивает просмотр и управление сертификатами субъектов в соответствии с правами учётной записи пользователя. Авторизованному пользователю с ролью «Оператор» доступны только сертификаты тех субъектов, на которые ему прямо или косвенно[6] предоставлены полномочия в соответствии с текущими правилами доступа.

Переход на экран управления центра сертификации осуществляется по выбору раздела «Сертификаты» бокового меню, расположенного слева на главном экране (см. Рисунок 14).

На данном экране отображаются все созданные сертификаты субъектов (см. Рисунок 18).

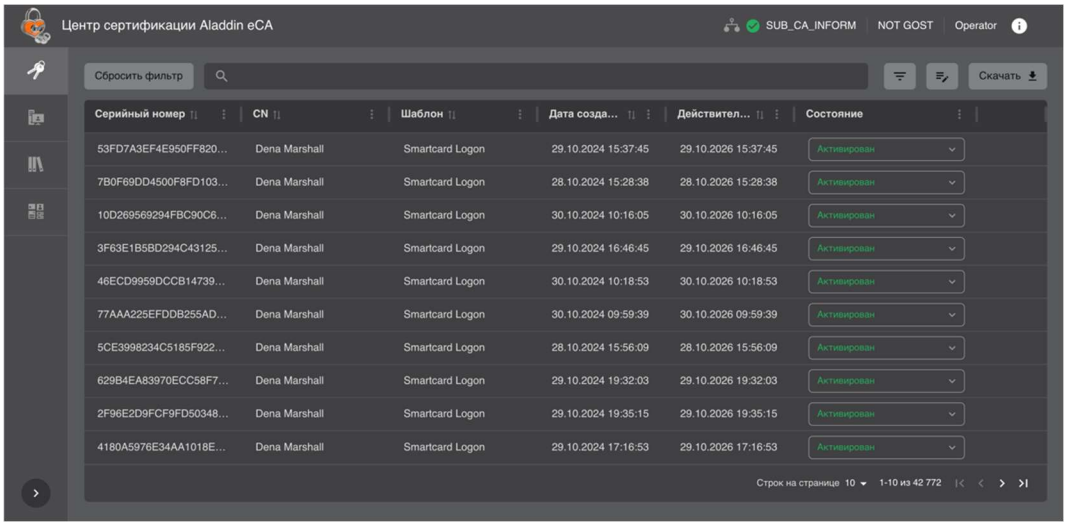


Рисунок 18 - Экран раздела меню «Сертификаты»

- На экране раздела «Сертификаты» отображены информационные элементы (табличные поля):

[6] Путем наследования от группы безопасности куда входит субъект, на основе которого создана учетная пользователя с ролью «Оператор».

- серийный номер сертификата;
- имя субъекта (CN);
- тип шаблона сертификата (шаблон);
- дата выпуска сертификата;
- дата срока окончания действия сертификата (действителен до);
- текущий статус сертификата (состояние).

- Доступны следующие операции по работе с сертификатами:
  - поиск выпущенных сертификатов;
  - сортировка сертификатов;
  - скачивание сертификатов;
  - изменение статуса сертификатов в формате .pem;
  - просмотр списка сертификатов с заданными критериями;
  - сброс всех применённых фильтров или выборочная отмена выбранного фильтра;
  - просмотр карточки сертификата;
  - экспорт списка выпущенных сертификатов с атрибутами;
  - массовые операции с выпущенными сертификатами.
- Все созданные сертификаты субъектов на экране раздела отображаются в виде таблицы с пагинацией.

4.3.1 Поиск сертификатов

Строка поиска (см. Рисунок 19) предназначена для поиска сертификатов по имени (поле Common Name), альтернативному имени субъекта (поле SubjectAltName) и серийному номеру сертификата (поле Serial Number). Поиск запускается автоматически при вводе искомого значения в строку поиска, результат поиска будет отражён на экранной таблице.

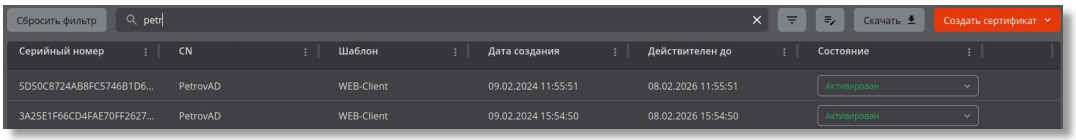


Рисунок 19 – Поисковая строка в разделе «Сертификаты»

- Для сброса результатов поиска и возврату к полному перечню сертификатов в экранной таблице удалите содержимое строки поиска.

4.3.2 Сортировка сертификатов

- Средства сортировки выпущенных сертификатов представлены элементами выбора направления сортировки в заголовке таблицы экранной формы (см. Рисунок 20):
  - «Серийный номер» – сортировка осуществляется в порядке возрастания или убывания значения;
  - «CN» – сортировка осуществляется в алфавитном порядке;
  - «Шаблон» – осуществляется группировка по типу шаблона;
  - «Дата создания», «Действителен до» – сортировка осуществляется в порядке возрастания или убывания значения даты.
- Сортировка происходит только по одному значению при нажатии на соответствующий заголовок таблицы. Активное значение, по которому выполнена фильтрация обозначен знаком с правой стороны от заголовка таблицы.

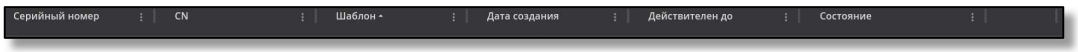


Рисунок 20 – Поля сортировки содержимого раздела «Сертификаты»

- Также отобразить в определённом порядке список сертификатов (отсортировать) в колонке возможно по нажатию кнопки  <Действия в колонке>, выбрав и нажав в раскрывшемся меню «Сортировать…» (см. Рисунок 22).

4.3.3 Фильтрация сертификатов

4.3.3.1 Применение фильтров

- Для выборочного просмотра сертификатов на экране раздела «Сертификаты» возможно применение фильтров. Для отображения параметров фильтрации для всех колонок таблицы нажмите кнопку <Фильтр>  , заголовки колонок экранной таблицы будут дополнены полями фильтра для каждой колонки (см. Рисунок 21):
  - шаблон. Выберите шаблоны сертификатов для отображения списка сертификатов, которые были выпущены на основании выбранных шаблонов;
  - дата создания. Выберите за какой период создания отобразить сертификаты на экране, введите дату с помощью клавиатуры или выберите в развернувшемся календаре;
  - действителен до. Выберите за какой период даты окончания действия отобразить сертификаты на экране, введите дату с помощью клавиатуры или выберите в развернувшемся календаре;
  - состояние. Выберите состояния сертификатов для отображения (активирован, приостановлен, отозван).

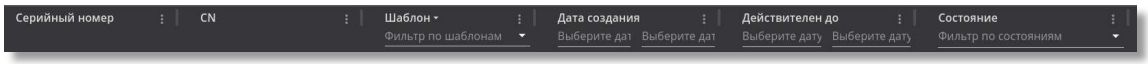


Рисунок 21 – Поля фильтра заголовков экранной таблицы

- Выберите одно или несколько значений фильтров, после выбора фильтр будет применён сразу автоматически.
- Повторное нажатие кнопки <Фильтр>  скроет поля выбора критериев фильтрации, но не отменяет применённые фильтры.
- Заголовки таблицы, для которых применён фильтр, будут отмечены знаком  .

4.3.3.2 Сброс применённых фильтров

- Для очистки применённых фильтров для каждого заголовка колонки:
  - нажмите кнопку  <Действия в колонке> и в раскрывшемся окне выберите пункт «Очистить фильтр» (см. Рисунок 22);

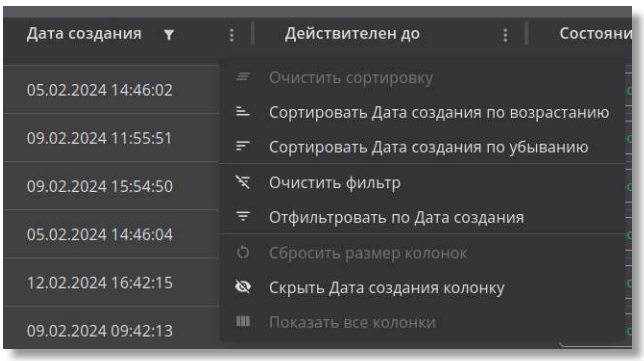
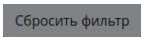


Рисунок 22 – Кнопка <Очистить> фильтр

- Для полной отмены всех применённых фильтров по всем колонкам воспользуйтесь кнопкой <Сбросить фильтр>  на экране раздела «Сертификаты».

4.3.4 Скачивание сертификатов

Для скачивания наведите указатель мыши на выбранный сертификат в экранной таблице, нажмите появившуюся кнопку  (см. Рисунок 18) и в раскрывшемся подменю выберите пункт <Скачать сертификат> или «Скачать цепочку» в формате .pem (см. Рисунок 23).

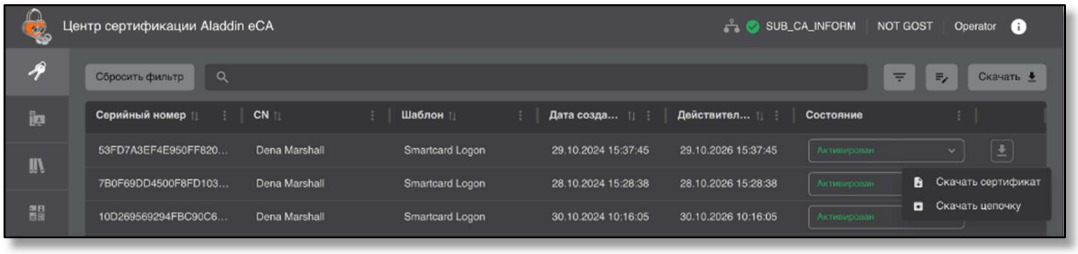


Рисунок 23 – Подменю «Скачать сертификат/цепочку»

4.3.5 Статус сертификатов

- Возможные варианты состояния и доступные действия над сертификатами в зависимости от состояния приведены в Таблица 2.

Таблица 2 – Доступные действия над сертификатами в зависимости от состояния

Состояние сертификата	Доступные действия		
	активация	приостановка	отзыв
активирован	☒	+	+
приостановлен	+	☒	+
отозван	☒	☒	☒

- Смена состояния сертификата производится посредством выбора нужного значения из выпадающего меню при выделении строки сертификата (см. Рисунок 24).

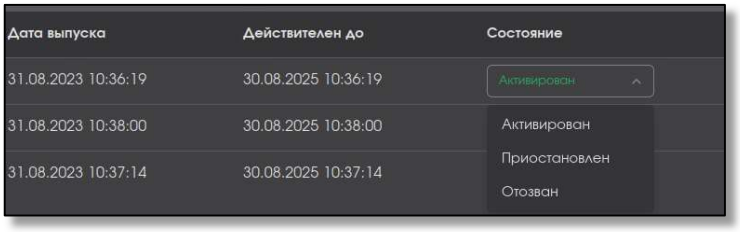


Рисунок 24 – Выпадающее меню смены состояния сертификата

- При смене состояния сертификата посредством радиокнопки появляется окно с запросом на подтверждение операции, в зависимости от типа операции предусмотрена различная активность для данного окна:
  - активация (см. Рисунок 25)

> **Если достигнуто предельное количество субъектов с действующими сертификатами в соответствии с лицензией, при попытке активации сертификата субъекта, у которого отсутствуют действующие сертификаты, будет отображаться сообщение об ошибке «Лицензионные ограничения не позволяют активировать данный сертификат. Достигнуто предельное количество субъектов с действующими сертификатами».**

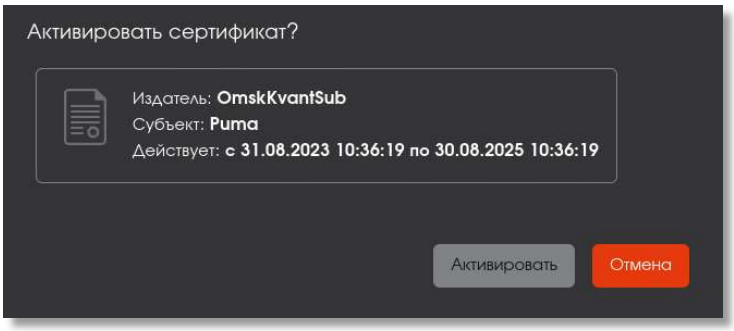


Рисунок 25 – Окно активации сертификата

– приостановка действия сертификата (см. Рисунок 26):

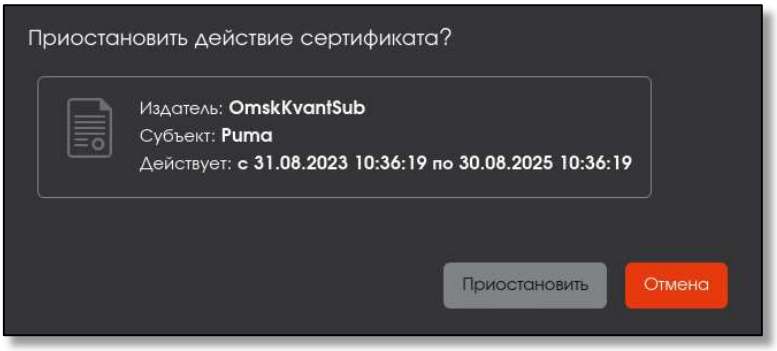


Рисунок 26 – Окно приостановки действия сертификата

– отзыв (см. Рисунок 27);

ВНИМАНИЕ! Данную операцию нельзя отменить.

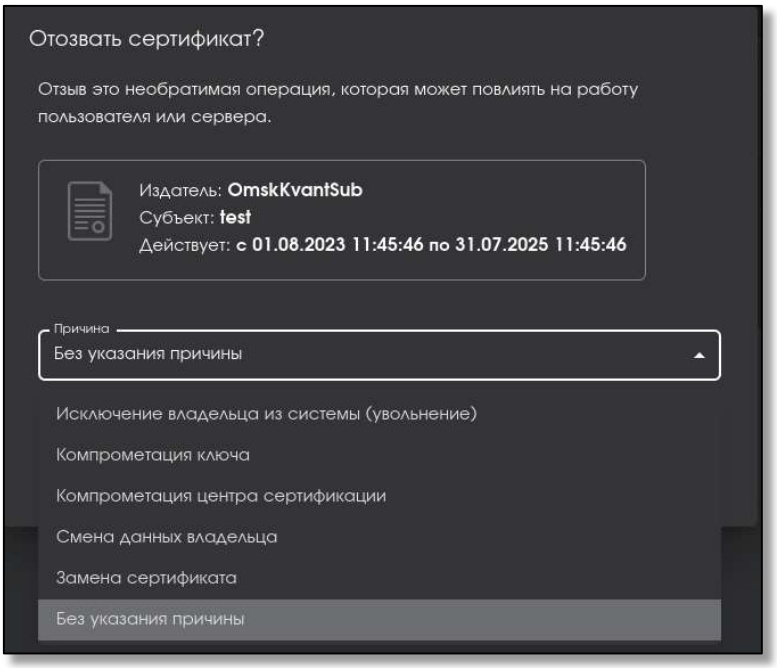


Рисунок 27 – Окно отзыва сертификата

Возможные причины отзыва (в соответствии с разделом 6.3.2 RFC5280):

– неиспользуемый (unused) – исключение владельца из системы/увольнение;
– принадлежность изменена (affiliation Changed) – смена данных владельца;
– приостановка полномочий владельца сертификата (certificateHold);
– компрометация ключа (keyCompromise);

- компрометация центра сертификации (cACompromise);
- заменен (сертификат) – заменен на иной сертификат;
- без указания причины (unspecified).

4.3.6 Карточка сертификата

- Просмотр данных сертификата возможен посредством страницы «Карточка сертификата».
- Переход к экрану «Карточка сертификата» (см. Рисунок 28) осуществляется при нажатии на строку сертификата таблицы главного экрана раздела «Сертификаты» (см. Рисунок 18).

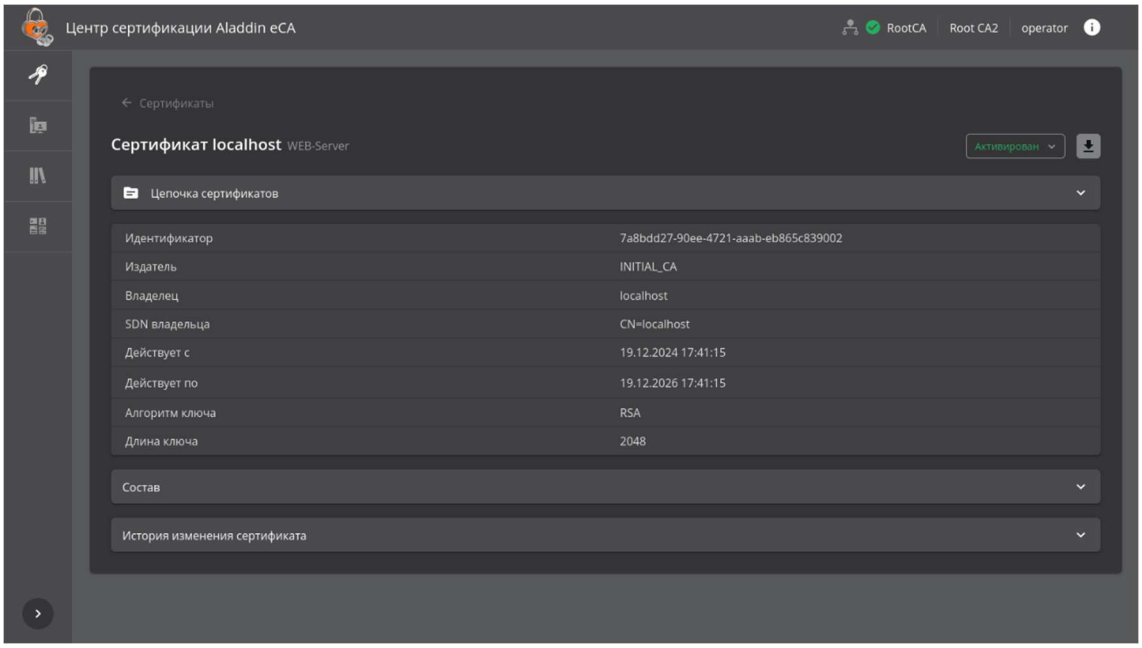


Рисунок 28 – Окно «Карточка сертификата»

- Оглавление карточки сертификата включает в себя (см. Рисунок 28):
  - тип (сертификат);
  - принадлежность (TestLocal);
  - шаблон сертификата (Web-Client).
- Для возврата на главный экран раздела «Сертификаты» проследовать по стрелке 

- Для изменения статуса сертификата выбрать из выпадающего списка действие 

в соответствие с Таблица 2.

> **Если достигнуто предельное количество субъектов с действующими сертификатами в соответствии с лицензией, при попытке активации сертификата субъекта, у которого отсутствуют действующие сертификаты, будет отображаться сообщение об ошибке «Лицензионные ограничения не позволяют активировать данный сертификат. Достигнуто предельное количество субъектов с действующими сертификатами».**

- Для скачивания сертификата наведите указатель мыши на кнопку  , во всплывающем меню выберите <Скачать сертификат> субъекта или <Скачать цепочку> сертификатов.
- В карточке сертификата отображаются следующие сведения:
  - идентификатор;
  - издатель;
  - владелец;
  - SDN владельца;

- срок действия («действует с», «действует по»);
- алгоритм ключа;
- длина ключа.

- Карточка сертификата содержит раскрывающиеся вкладки:
  - «Цепочка сертификатов». Раскройте вкладку, нажав в строке с именем вкладки символ . На раскрывшемся экране отображены все Центры сертификации, участвующие в построении цепочки сертификатов, начиная с Корневого ЦС, на основе которого строится цепочка доверия сертификатам, до конечного Центра сертификации, выдавшего текущий сертификат субъекта (см. Рисунок 29).

Рисунок 29 – Окно карточки сертификата. Вкладка «Цепочка сертификатов»

  - «Состав». Раскройте вкладку, нажав в строке с именем вкладки символ . На раскрывшемся экране отображены следующие поля (см. Рисунок 30):
    - серийный номер;
    - открытый ключ;
    - отпечаток;
    - версия;
    - параметр открытого ключа;
    - алгоритм цифровой подписи
    - основные ограничения;
    - использование ключа;
    - доступ информации о центре сертификации;
    - альтернативное имя субъекта;
    - идентификатор ключа центра;
    - идентификатор ключа субъекта;
    - расширенное использование ключа.

При переходе на выбранное поле, в правой части экрана будет отображена информация, соответствующая выделенному полю.

Рисунок 30 – Окно карточки сертификатов. Вкладка «Состав»

– «История изменения сертификата». Раскройте вкладку, нажав в строке с именем вкладки символ  . На данной вкладке зафиксирована информация о всех совершённых над сертификатом действиях в хронологическом порядке. На раскрывшемся экране отображены поля (см. Рисунок 31):

  - дата – дата совершенного действия;
  - пользователь – учётная запись, под которой было совершенно данное действие;
  - событие – действие, совершённое над сертификатом.

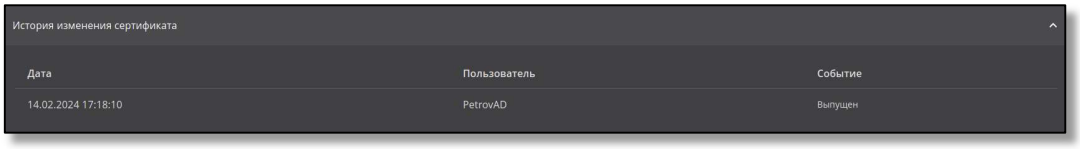
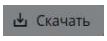


Рисунок 31 – Окно карточки сертификатов. Вкладка «История изменения сертификата»

- Выход из карточки сертификата осуществляется по кнопке <Возврат> и по кнопкам разделов на боковой панели.

4.3.7 Экспорт списка выпущенных сертификатов

- При использовании учётной записи «Оператор» в список .csv файла будут собраны только выпущенные сертификаты тех субъектов, права доступа на которые назначены данному оператору.
- Для выгрузки списка сертификатов нажмите кнопку 

<Скачать все сертификаты в формате CSV>. Происходит формирование списка сертификатов, по завершению действия и готовности к выгрузке списка сертификатов кнопка переходит в состояние 

. Нажмите кнопку <Скачать (готово)> для сохранения подготовленного списка сертификатов.
- Сохранение списка сертификатов в виде zip-архива происходит по выбранному пути в открывшемся окне сохранения файла (см. Рисунок 32).

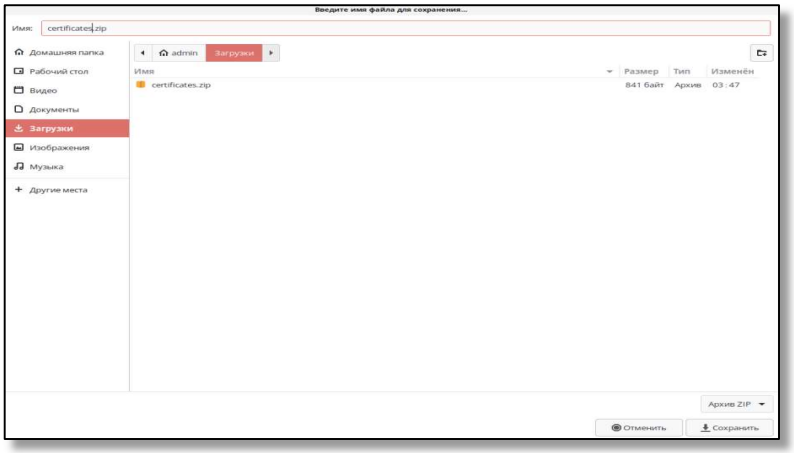
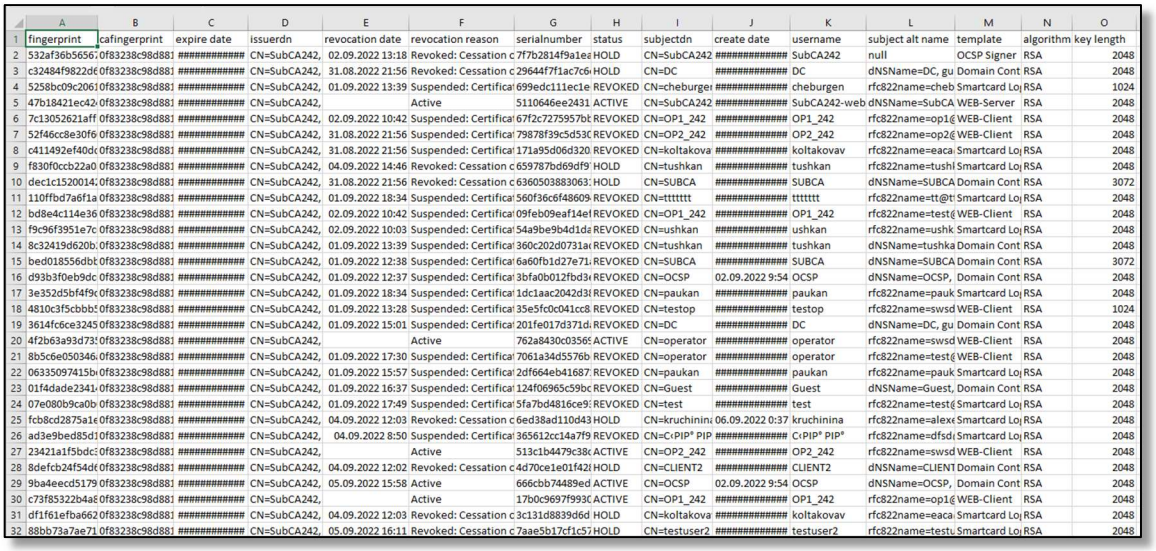


Рисунок 32 – Окно указания пути сохранения файла

- Выгруженный файл .csv представлен в текстовом формате для представления табличных данных, где строки текста содержат поля таблицы, разделённые запятыми. Сформированная таблица содержит следующие столбцы (см. Рисунок 33):

  – fingerprint – содержит уникальный числовой отпечаток сертификата;
  – cafingerprint – содержит уникальный числовой отпечаток сертификата центра, подписавшего сертификат;
  – expire date – содержит значение даты «годен до»;
  – issuerdn – содержит отличительное имя издателя;
  – revocation date – содержит дату отзыва;
  – revocation reason – содержит причину отзыва;

- serialnumber – содержит серийный номер сертификата;
- status – содержит текущий статус сертификата;
- subjectdn – содержит отличительное имя держателя сертификата;
- create date – содержит дату выпуска сертификата;
- username – содержит имя держателя сертификата;
- subject alt name – содержит дополнительные имена держателя;
- template – содержит наименование шаблона;
- algorithm – содержит обозначение алгоритма;
- key length – содержит длину ключа;
- history – содержит историю изменений сертификата в формате JSON.



	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O
1	fingerprint	cafingerprint	expire date	issuerdn	revocation date	revocation reason	serialnumber	status	subjectdn	create date	username	subject alt name	template	algorithm	key length
2	532af36b5656	0f83238c98d88	###########	CN=SubCA242,	02.09.2022 13:18	Revoked: Cessation c	7f7b2814f9a1ea	HOLD	CN=SubCA242	###########	SubCA242	null	OCSP Signer	RSA	2048
3	c32484f9822d6	0f83238c98d88	###########	CN=SubCA242,	31.08.2022 21:56	Revoked: Cessation c	29644f7f1ac7c6	HOLD	CN=DC	###########	DC	dNSName=DC, gu	Domain Cont	RSA	2048
4	5258bc09c2061	0f83238c98d88	###########	CN=SubCA242,	01.09.2022 13:39	Suspended: Certifica	699edc111ec1e	REVOKED	CN=cheburger	###########	cheburgen	rfc822name=cheb	Smartcard Lo	RSA	1024
5	47b18421ec42	0f83238c98d88	###########	CN=SubCA242,		Active	5110646ee2431	ACTIVE	CN=SubCA242	###########	SubCA242-web	dNSName=SubCA	WEB-Server	RSA	2048
6	7c13052621aff	0f83238c98d88	###########	CN=SubCA242,	02.09.2022 10:42	Suspended: Certifica	67f2c7275957bb	REVOKED	CN=OP1_242	###########	OP1_242	rfc822name=op1@	WEB-Client	RSA	2048
7	52f46cc8e30f6	0f83238c98d88	###########	CN=SubCA242,	31.08.2022 21:56	Suspended: Certifica	79878f39c5d53(	REVOKED	CN=OP2_242	###########	OP2_242	rfc822name=op2@	WEB-Client	RSA	2048
8	c411492ef40dc	0f83238c98d88	###########	CN=SubCA242,	31.08.2022 21:56	Suspended: Certifica	171a95d06d320	REVOKED	CN=koltakova	###########	koltakovav	rfc822name=eaca	Smartcard Lo	RSA	2048
9	f830f0ccb22a0	0f83238c98d88	###########	CN=SubCA242,	04.09.2022 14:46	Revoked: Cessation c	659787bd69df9	HOLD	CN=tushkan	###########	tushkan	rfc822name=tush	Smartcard Lo	RSA	2048
10	dec1c1520014	0f83238c98d88	###########	CN=SubCA242,	31.08.2022 21:56	Revoked: Cessation c	6360503883063	HOLD	CN=SUBCA	###########	SUBCA	dNSName=SUBCA	Domain Cont	RSA	3072
11	110ffbd7a6f1a	0f83238c98d88	###########	CN=SubCA242,	01.09.2022 18:34	Suspended: Certifica	560f36c6f48609	REVOKED	CN=ttttttt	###########	ttttttt	rfc822name=tt@t	Smartcard Lo	RSA	2048
12	bd8e4c114e36	0f83238c98d88	###########	CN=SubCA242,	02.09.2022 10:42	Suspended: Certifica	09feb09eaf14e(	REVOKED	CN=OP1_242	###########	OP1_242	rfc822name=test@	WEB-Client	RSA	2048
13	f9c96f3951e7c	0f83238c98d88	###########	CN=SubCA242,	02.09.2022 10:03	Suspended: Certifica	54a9be9b4d1da	REVOKED	CN=ushkan	###########	ushkan	rfc822name=ushk	Smartcard Lo	RSA	2048
14	8c32419d620b	0f83238c98d88	###########	CN=SubCA242,	01.09.2022 13:39	Suspended: Certifica	360c202d0731a(	REVOKED	CN=tushkan	###########	tushkan	dNSName=tushka	Domain Cont	RSA	2048
15	bed018556db8	0f83238c98d88	###########	CN=SubCA242,	01.09.2022 12:38	Suspended: Certifica	6a60fb1d27e71	REVOKED	CN=SUBCA	###########	SUBCA	dNSName=SUBCA	Domain Cont	RSA	3072
16	d93b3f0eb9dc	0f83238c98d88	###########	CN=SubCA242,	01.09.2022 12:37	Suspended: Certifica	3bfa0b012fbd3(	REVOKED	CN=OCSP	02.09.2022 9:54	OCSP	dNSName=OCSP,	Domain Cont	RSA	2048
17	3e352d5bf4f9c	0f83238c98d88	###########	CN=SubCA242,	01.09.2022 18:34	Suspended: Certifica	1dc1aac2042d3(	REVOKED	CN=paukan	###########	paukan	rfc822name=pauk	Smartcard Lo	RSA	2048
18	4810c3f5cbbb5	0f83238c98d88	###########	CN=SubCA242,	01.09.2022 13:28	Suspended: Certifica	35e5fc0c041cc8	REVOKED	CN=testop	###########	testop	rfc822name=swsd	WEB-Client	RSA	1024
19	3614fc6ce3245	0f83238c98d88	###########	CN=SubCA242,	01.09.2022 15:01	Suspended: Certifica	201fe017d371d(	REVOKED	CN=DC	###########	DC	dNSName=DC, gu	Domain Cont	RSA	2048
20	4f2b63a93d73!	0f83238c98d88	###########	CN=SubCA242,		Active	762a8430c0356!	ACTIVE	CN=operator	###########	operator	rfc822name=swsd	WEB-Client	RSA	2048
21	8b5c6e050346	0f83238c98d88	###########	CN=SubCA242,	01.09.2022 17:30	Suspended: Certifica	7061a34d5576b	REVOKED	CN=operator	###########	operator	rfc822name=test@	WEB-Client	RSA	2048
22	06335097415b	0f83238c98d88	###########	CN=SubCA242,	01.09.2022 15:57	Suspended: Certifica	2df664eb41687	REVOKED	CN=paukan	###########	paukan	rfc822name=pauk	Smartcard Lo	RSA	2048
23	01f4dade2341	0f83238c98d88	###########	CN=SubCA242,	01.09.2022 16:37	Suspended: Certifica	124f06965c59bc	REVOKED	CN=Guest	###########	Guest	dNSName=Guest,	Domain Cont	RSA	2048
24	07e080b9ca0b	0f83238c98d88	###########	CN=SubCA242,	01.09.2022 17:49	Suspended: Certifica	5fa7bd4816ce9!	REVOKED	CN=test	###########	test	rfc822name=test@	Smartcard Lo	RSA	2048
25	fcb8cd2875a1e	0f83238c98d88	###########	CN=SubCA242,	04.09.2022 12:03	Revoked: Cessation c	6ed38ad110d43	HOLD	CN=kruchinina	06.09.2022 0:37	kruchinina	rfc822name=alex	Smartcard Lo	RSA	2048
26	ad3e9bed85d1	0f83238c98d88	###########	CN=SubCA242,	04.09.2022 8:50	Suspended: Certifica	365612cc14a7f9	REVOKED	CN=Cr PIP° PIP	###########	Cr PIP° PIP°	rfc822name=dfsd	Smartcard Lo	RSA	2048
27	23421a1f5bdc:	0f83238c98d88	###########	CN=SubCA242,		Active	513c1b4479c38(	ACTIVE	CN=OP2_242	###########	OP2_242	rfc822name=swsd	WEB-Client	RSA	2048
28	8defcb24f54d(	0f83238c98d88	###########	CN=SubCA242,	04.09.2022 12:02	Revoked: Cessation c	4d70ce1e01f42(	HOLD	CN=CLIENT2	###########	CLIENT2	dNSName=CLIENT	Domain Cont	RSA	2048
29	9ba4eecd5179	0f83238c98d88	###########	CN=SubCA242,	05.09.2022 15:58	Active	666cbb74489ed	ACTIVE	CN=OCSP	02.09.2022 9:54	OCSP	dNSName=OCSP,	Domain Cont	RSA	2048
30	c73f85322b4a6	0f83238c98d88	###########	CN=SubCA242,		Active	17b0c9697f993(	ACTIVE	CN=OP1_242	###########	OP1_242	rfc822name=op1@	WEB-Client	RSA	2048
31	df1f61efba662	0f83238c98d88	###########	CN=SubCA242,	04.09.2022 12:03	Revoked: Cessation c	3c131d8839d6d	HOLD	CN=koltakova	###########	koltakovav	rfc822name=eaca	Smartcard Lo	RSA	2048
32	88bb73a7ae71	0f83238c98d88	###########	CN=SubCA242,	05.09.2022 16:11	Revoked: Cessation c	7aae5b17cf1c57	HOLD	CN=testuser2	###########	testuser2	rfc822name=testu	Smartcard Lo	RSA	2048

Рисунок 33 – Пример экспортированного файла списка выпущеных сертификатов.csv

4.3.8 Массовые операции с сертификатами

- Для массовой операции, применяемой к выбранному множеству сертификатов доступа, нажмите кнопку  <Массовые операции>, которая запускает окно выполнения массовой операции (см. Рисунок 34).

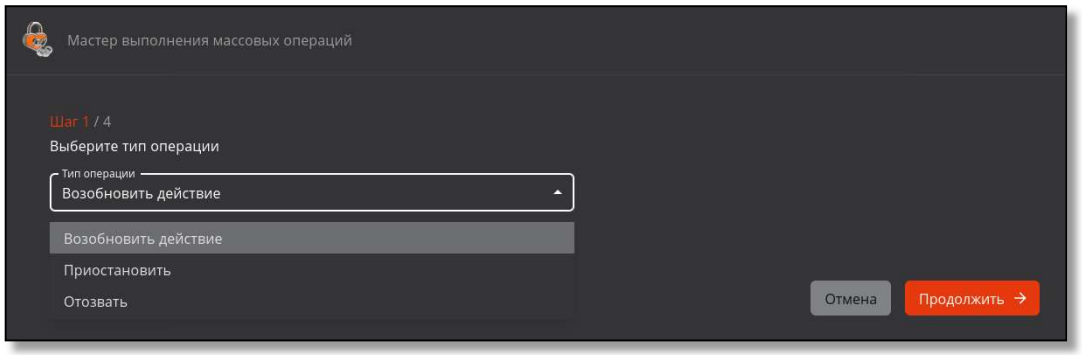


Рисунок 34 – Окно выполнения массовых операций. Шаг 1

- Выберите необходимую операцию из раскрывающегося списка. Доступны следующие типы операций:
  - возобновление действия;
  - приостановить;
  - отозвать.

При выборе операции «Отозвать» дополнительно необходимо будет указать причину отзыва из выпадающего списка.

- Нажмите кнопку <Продолжить>.

- Далее необходимо осуществить поиск сертификатов по отличительному имени субъекта Subject Distinguished Names, для которых требуется применить выбранную операцию, в левом поле окна Шага 2 (см. Рисунок 35). Поиск сертификатов производится с учётом текущего статуса сертификата и выбранного типа операции на шаге 1. Например, при выборе типа операции «Возобновить» поиск осуществляется только среди сертификатов со статусом «Приостановлен», для которых допустимо выполнить данный тип операции.
- Выберите, найденные сертификаты, отметив их флажками .
- Перенесите отмеченные флажками сертификаты в правую часть окна, нажав кнопку , которая находится между правой и левой частью окна выполнения операции.

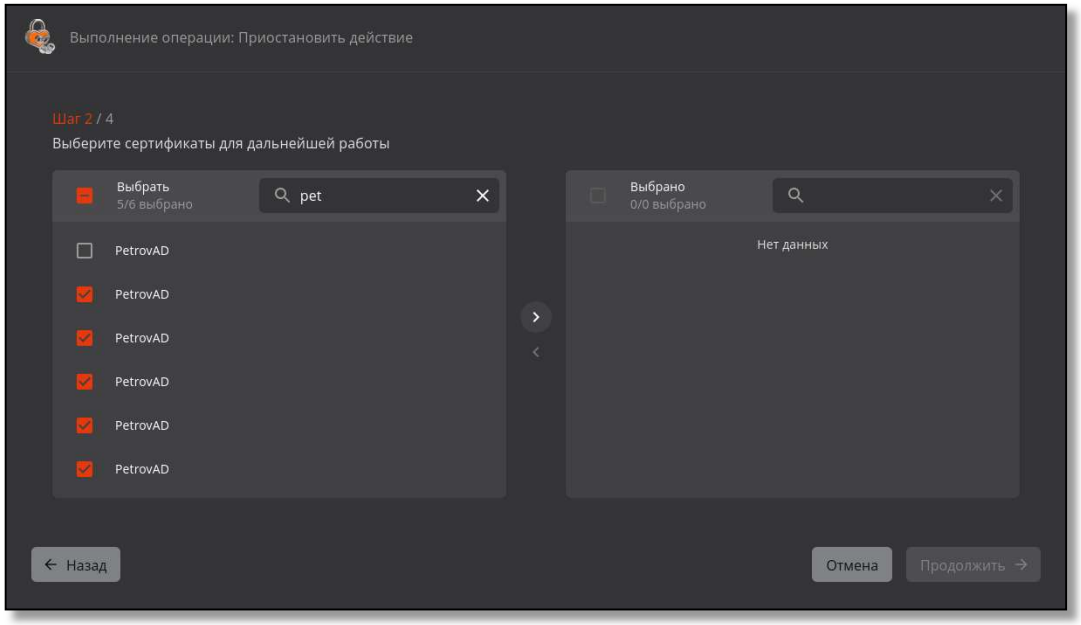


Рисунок 35 – Окно выполнения массовых операций. Шаг 2. Создание списка выбранных сертификатов

- В случае необходимости исключения из выбранных сертификатов, к которым будет применена массовая операция, отметьте флажками сертификата из списка в правой части окна, и нажмите кнопку .

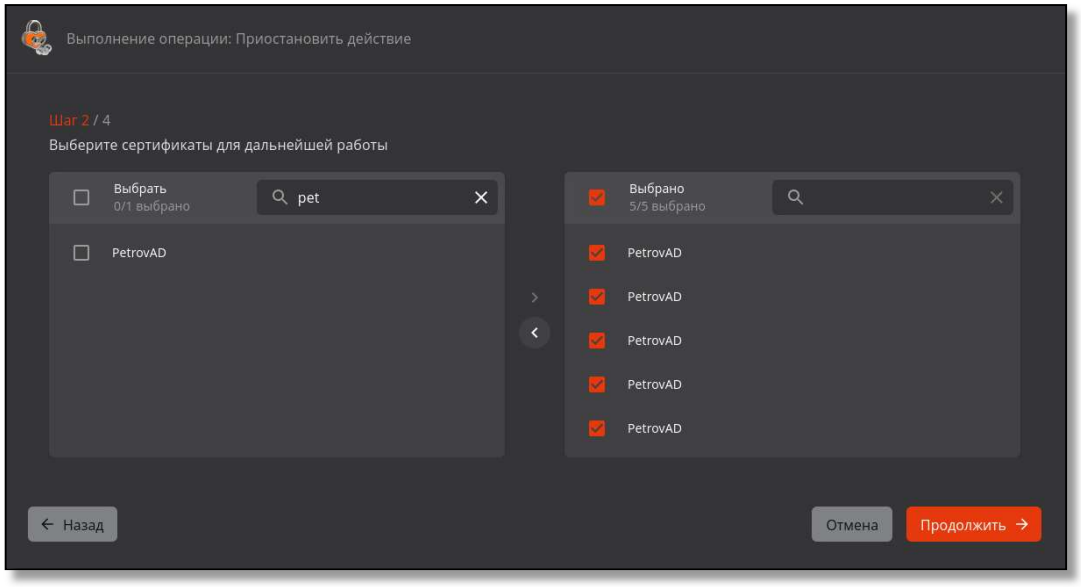


Рисунок 36 – Окно выполнения массовых операций. Шаг 2. Редактирование списка выбранных сертификатов

- Для перехода на следующий шаг нажмите кнопку <Продолжить>.
- В открывшемся окне подтвердите действие, нажав кнопку «Применить» (см. Рисунок 37).

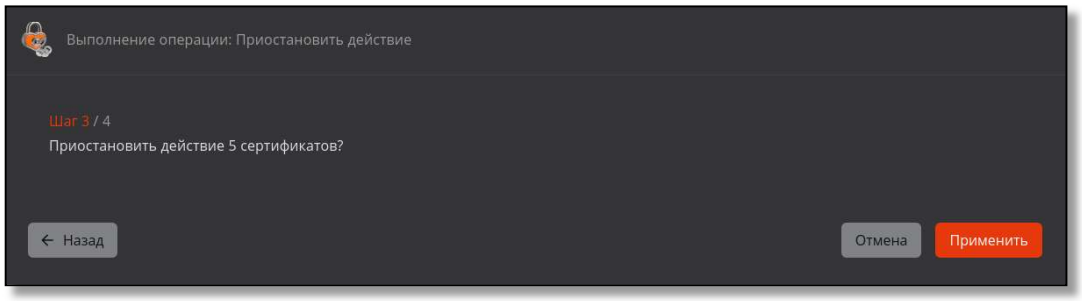


Рисунок 37 – Окно выполнения массовых операций. Шаг 3

- В случае успешного выполнения операции администратор будет уведомлён на шаге 4.

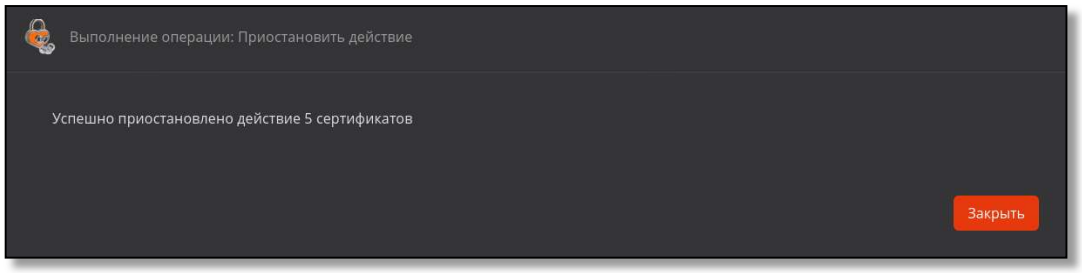


Рисунок 38 – Окно выполнения массовых операций. Шаг 4

Если выбранная на шаге 1 операция не может быть выполнена в связи с лицензионными ограничениями со всеми сертификатами, выбранными на шаге 2, то в данном окне отображается количество и перечень CN из сертификатов, для которых операция не была завершена успешно (см. Рисунок 39).

Рисунок 39 – Окно выполнения массовых операций. Шаг 4. Перечень сертификатов, для которых операция не была завершена успешно

4.4 Раздел «Субъекты»

Раздел «Субъекты» обеспечивает возможность просмотра субъектов подключенных служб каталога, выпуска сертификатов для субъектов. Для авторизованного пользователя с ролью «Оператор» в разделе «Субъекты» доступны только те субъекты, на которые ему прямо или косвенно[7] предоставлены полномочия в соответствии с текущими правилами доступа.

- Переход в раздел «Субъекты» осуществляется через боковое меню, расположенное слева на главном экране (см. Рисунок 40).
- После выбора источника в поле «Внешние ресурсные системы», субъекты будут отображены в виде списка в окне раздела «Субъекты (см. Рисунок 40).

[7] Путем наследования от группы безопасности, куда входит субъект, на основе которого создана учетная пользователя с ролью «Оператор».

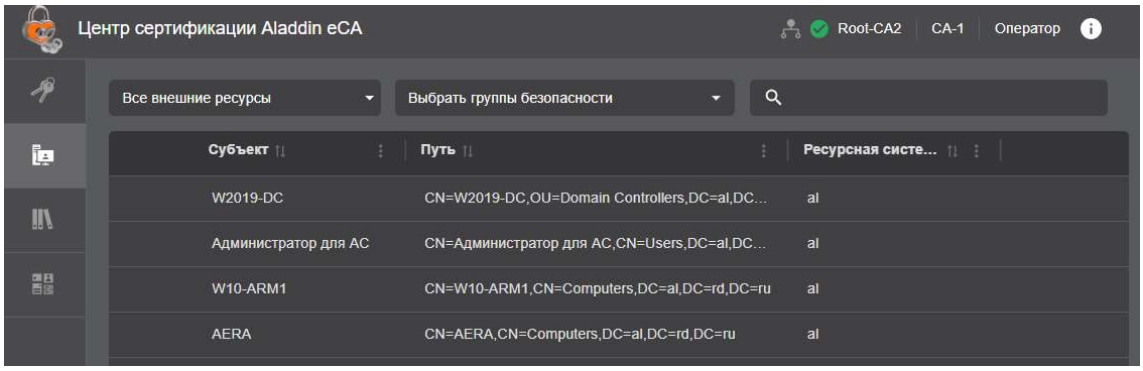


Рисунок 40 – Экран раздела меню «Субъекты». Подключенный ресурс

В разделе доступны следующие элементы:

- строка поиска субъекта. Поиск субъектов осуществляется по вхождению текста в атрибуты субъекта в его карточке и в путь субъекта.
- кнопка «Создать» для создания локального субъекта;
- поле выбора ресурсной системы с именами подключенных ресурсных систем. В данном поле присутствует возможность выбора всех внешних ресурсных систем (значение «Все внешние ресурсы») и локальной ресурсной системы (значение «Локальная ресурсная система»);
- поле выбора групп безопасности ресурсной системы. В данном поле отображаются только группы безопасности, в которых в ресурсной системе присутствуют субъекты. В данном поле присутствует возможность поиска групп безопасности, а также возможность указать значение «Без группы безопасности» для отображения субъектов, не входящих в группы безопасности;
- список субъектов, содержащий следующие поля:
  - пиктограмма «Сертификат» – отображается, если у субъекта имеются действующий сертификаты, при наведении курсора на пиктограмму отображается количество действующих сертификатов субъекта;
  - «Субъект» – значение атрибута «Common name» данного субъекта;
  - «Путь» – содержит отличительное имя субъекта в ресурсной системе;
  - «Ресурсная система» – содержит название ресурсной системы, которой принадлежит данный субъект.

В разделе «Субъекты» доступны следующие действия:

- просмотр субъектов подключенных ресурсных систем с выбором группы безопасности;
- просмотр субъектов локальной ресурсной системы;
- поиск субъекта;
- создание нового субъекта локальной ресурсной системы;
- редактирование значения атрибутов субъекта локальной ресурсной системы;
- просмотр карточки субъекта;
- просмотр списка сертификатов, выпущенных Центром сертификации для субъекта;
- управление статусом сертификатов, выпущенных Центром сертификации для субъекта;
- публикация сертификата субъекта в ресурсную систему;
- экспорт сертификата субъекта;
- создание сертификата для субъекта;
- создание учётной записи для субъекта.

- Идентификация локальных и подключенных субъектов в Центре сертификации осуществляется по атрибуту `UUID`.

4.4.1 Просмотр субъектов ресурсных систем

- Просмотр субъектов осуществляется посредством выбора источника:
  - все внешние ресурсы – подключенные службы каталогов, на субъекты которых назначены права авторизованному оператору;
  - локальный ресурс – появляется в случае, если назначены права хот бы на один субъект в локальной базе данных Центра сертификации;
  - внешний ресурс, отображаемое имя которого соответствует имени контроллера домена.
- В разделе «Субъекты» в верхней панели расположены элементы выбора ресурса и фильтрации (см. Рисунок 41):
  - поле «Ресурсная система», по нажатию на которое в выпадающем меню выберите локальную ресурсную систему, подключенный ресурс или все внешние ресурсы для отображения всех субъектов внешних ресурсных систем;
  - поле «Выбрать группу безопасности», для отображения на экране субъектов определенной группы нажмите на поле и в выпадающем меню выберите необходимую группу. В случае если группа безопасности не выбрана, то будут отображены все субъекты выбранного источника. Для локального ресурса группы безопасности отсутствуют. В списке «Выбрать группу безопасности» отображаются только те группы безопасности, которые содержат один или более субъектов. Группы безопасности, не имеющие членов, не будут показаны в списке и не доступны для выбора.

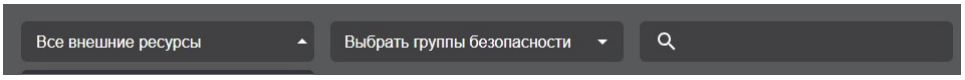


Рисунок 41 – Верхняя панель экранной формы вкладки «Субъекты»

4.4.2 Поиск субъектов

- В разделе «Субъекты» в верхней панели расположены элементы (см. Рисунок 41
  - поле поиска, в котором осуществляется поиск субъектов по компонентам SubjectDN и SubjectAltName в выбранной ресурсной системе. Для поиска начните ввод имени субъекта в строке, поиск начинается автоматически через 1 секунду после прекращения ввода с клавиатуры. Для сброса поиска и отображения всех субъектов выбранной ресурсной системы очистите строку поиска.

4.4.3 Сортировка субъектов

Средства сортировки субъектов выбранной ресурсной системы представлены элементами выбора направления сортировки в заголовке таблицы экранной формы (см. Рисунок 42):

- «Субъект» – сортировка осуществляется в алфавитном порядке;
- «Путь» – сортировка осуществляется в алфавитном порядке содержимого атрибута «Common Name»;
- «Ресурсная система» – сортировка осуществляется в алфавитном порядке.

Сортировка происходит только по одному значению при нажатии на соответствующий заголовок таблицы. Активное значение, по которому выполнена сортировка обозначено знаком ▲ с правой стороны от заголовка таблицы.

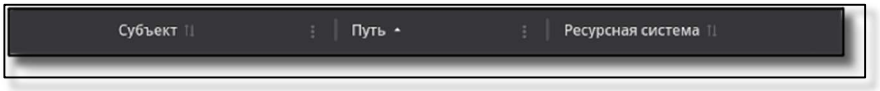


Рисунок 42 – Поля сортировки содержимого экрана раздела «Сертификаты»

4.4.4 Карточка субъекта

- Просмотра данных субъекта возможен посредством страницы «Карточка субъекта».
- Переход к экрану «Карточка субъекта» (см. Рисунок 43) осуществляется при нажатии на строку субъекта главного экрана раздела «Субъекты» (см. Рисунок 40).

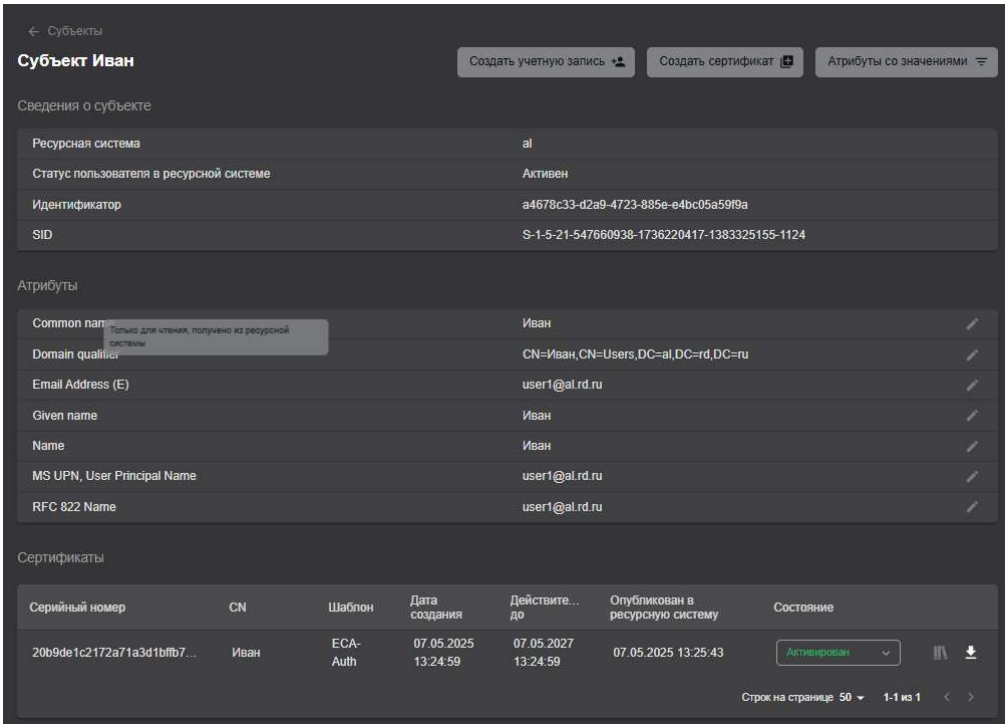
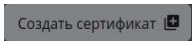


Рисунок 43 – Окно просмотра карточки субъекта (включено отображение «Атрибуты со значениями»)

- Карточка субъекта включает в себя следующие информационные поля:
  - сведения о субъекте:
    - из какой ресурсной системы получен субъект;
    - статус пользователя в ресурсной системе;
    - идентификатор UUID;
  - SID (идентифкатор безопасности)[8];
  - атрибуты SAN и SDN (см. Таблица 3);
  - сведения обо всех сертификатах субъекта, ранее выпущенных Центром сертификации:
    - серийный номер;
    - Common Name владельца сертификата;
    - шаблон;
    - дата создания;
    - дата окончания действия;
    - дата публикации в ресурсную систему;
    - состояние сертификата.
- Доступные действия в карточке субъекта:

[8] SID может быть получен для субъекта только из ресурсных систем MS AD, SambaDC, РЕД АДМ» и «Альт Домен». Для субъектов ресурсных систем FreeIPA и ALD PRO данный атрибут отсутствует.

- создать сертификат для выбранного субъекта с закрытым ключом, на основании запроса или на ключевом носителе по нажатию на кнопку <Создать сертификат> 

(см. п. 4.4.7, настоящего руководства);
- выбрать набор атрибутов SDN и SAN, отображаемых в карточке субъекта, в выпадающем меню (см. Рисунок 44);

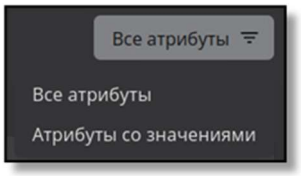


Рисунок 44 – Фильтрация отображаемых атрибутов в карточке субъекта

- опубликовать сертификат в ресурсную систему (только для подключенных субъектов). По нажатию на кнопку  происходит запись сертификата в формате LDIF в атрибут `userCertification` выбранного субъекта ресурсной системы, для которого выпущен сертификат. Если атрибут `userCertification` заполнен, то происходит перезапись содержимого;
- экспорт сертификата выбранного субъекта по указанному для сохранения файла по указанному пути по кнопке  <Скачать>;
- переход в карточку сертификата;
- изменить статус сертификатов, выпущенных для данного субъекта в поле сертификата «Состояние».

При активации сертификата учитывается ограничения лицензии: если в программе достигнуто максимальное количество субъектов с действующими сертификатами по лицензии, то активация сертификата в карточке субъекта доступна только при условии, что у данного субъекта есть действующие сертификаты, иначе при попытке активации сертификата отображается сообщение об ошибке «Лицензионные ограничения не позволяют активировать данный сертификат. Достигнуто предельное количество субъектов с действующими сертификатами»;

- редактировать значения в полях атрибутов (только для локальных субъектов).

Таблица 3 – Атрибуты субъекта

Атрибут	Возможные значения	Представление в API	Представление в клиентском компоненте
Сведения о субъекте			
Ресурсная система, к которой подключен субъект	Ресурсная система, к которой подключен субъект	resource: { id (UUID), commonName (string), name (string)}	Поле «Получен из ресурсной системы» в карточке субъекта Для локальных субъектов всегда отображается значение «Локальная ресурсная система».
Флаг подключения к РС	Субъект подключен к ресурсной системе (true)	"isConnected": true	Отображение субъекта в списке субъектов ресурсной системы, к которой он подключен.
	Локальный субъект (false)	" isConnected": false	Отображение субъекта в списке субъектов локальной ресурсной системы.
Флаг блокировки	Для подключенных к	"isBlocked"	Поле «Статус в ресурсной системе» в

Атрибут	Возможные значения	Представление в API	Представление в клиентском компоненте
в РС	РС субъектов: субъект заблокирован в РС (true) или субъект не заблокирован в РС (false)		карточке субъекта. Для локальных субъектов всегда отображается символ «-».
	Для локальных субъектов: всегда false		
UUID	string($uuid)	"id"	Поле «UUID» карточки субъекта
Расположение субъекта в структуре РС	Строка	"distinguishedName"	Поле «Путь» в списке субъектов в разделе «Субъекты»
Время обновления субъекта	Дата в формате ISO 8601	"updated"	-
Время создания субъекта	Дата в формате ISO 8601	"created"	-
SID[9]	Строка	"sid"	Поле «SID» карточки субъекта
Атрибуты SDN			
Common name	Список строк	"CN"	Поле «Common name» в карточке субъекта
Unique Identifier (UID)	Список строк	"UID"	Поле «Unique Identifier (UID)» в карточке субъекта
Email Address (E)	Список строк	"E"	Поле «Email Address (E)» в карточке субъекта
Email Address (Mail)	Список строк	"EMAILADDRESS"	Поле «Email Address (Mail)» в карточке субъекта
Mail	Список строк	"MAIL"	Поле «Mail» в карточке субъекта
Serial number	Список строк	"SN"	Поле «Serial number» в карточке субъекта
Given name	Список строк	"GIVENNAME"	Поле «Given name» в карточке субъекта
Initials	Список строк	"INITIALS"	Поле «Initials» в карточке субъекта
Surname	Список строк	"SURNAME"	Поле «Surname» в карточке субъекта
Organizational unit	Список строк	"OU"	Поле «Organizational unit» в карточке субъекта
Organization	Список строк	"O"	Поле «Organization» в карточке субъекта

[9] SID может быть получен для субъекта только из ресурсных систем MS AD, SambaDC, РЕД АДМ» и «Альт Домен».

Атрибут	Возможные значения	Представление в API	Представление в клиентском компоненте
Locality	Список строк	"L"	Поле «Locality» в карточке субъекта
State or province	Список строк	"ST"	Поле «State or province» в карточке субъекта
Domain component	Список строк	"DC"	Поле «Domain component» в карточке субъекта
Country	Список строк	"C"	Поле «Country» в карточке субъекта
Unstructured address	Список строк	"UNSTRUCTUREDADDRESS"	Поле «Unstructured address» в карточке субъекта
Unstructured name	Список строк	"UNSTRUCTUREDNAME"	Поле «Unstructured name» в карточке субъекта
Postalcode	Список строк	"POSTALCODE"	Поле «Postalcode» в карточке субъекта
Business category	Список строк	"BUSINESSCATEGORY"	Поле «Business category» в карточке субъекта
Telephone number	Список строк	"TELEPHONENUMBER"	Поле «Telephone number» в карточке субъекта
Pseudonym	Список строк	"PSEUDONYM"	Поле «Pseudonym» в карточке субъекта
Postal address	Список строк	"POSTALADDRESS"	Поле «Postal address» в карточке субъекта
Street	Список строк	"STREET"	Поле «Street» в карточке субъекта
Name	Список строк	"NAME"	Поле «Name» в карточке субъекта
Title	Список строк	"T"	Поле «Title» в карточке субъекта
Domain Qualifier	Список строк	"DN"	Поле «Domain Qualifier» в карточке субъекта
Description	Список строк	"DESCRIPTION"	Поле «Description» в карточке субъекта
ИНН	Список строк	"INN"	Поле «ИНН» в карточке субъекта
ОГРН	Список строк	"OGRN"	Поле «ОГРН» в карточке субъекта
ОГРНИП	Список строк	"OGRNIP"	Поле «ОГРНИП» в карточке субъекта
СНИЛС	Список строк	"SNILS"	Поле «СНИЛС» в карточке субъекта
ИНН ЮЛ	Список строк	"INNLE"	Поле «ИНН ЮЛ» в карточке субъекта
Атрибуты SAN			
MS GUID, Globally Unique Identifier	string($uuid)	"MS_GUID"	Поле «MS GUID, Globally Unique Identifier» в карточке субъекта
RFC 822 NAME	Список строк	"RFC822NAME"	Поле «RFC 822 NAME» в карточке субъекта
MS UPN, UserPrincipalName	Список строк	"MS_UPN"	Поле «MS UPN, UserPrincipalName» в карточке субъекта

Атрибут	Возможные значения	Представление в API	Представление в клиентском компоненте
DNS Name	Список строк	"DNS_NAME"	Поле «DNS Name» в карточке субъекта
IP address	Список строк	"IPADDRESS"	Поле «IP address» в карточке субъекта
Directory Name	Список строк	“DIRECTORY_NAME"	Поле «Directory Name» в карточке субъекта
Uniform resource identifier	Список строк	"UNIFORM_RESOURCE_ID"	Поле «Uniform resource identifier» в карточке субъекта
Registered identifier	Список строк	"REGISTERED_ID"	Поле «Registered identifier» в карточке субъекта
Kerberos KPN, Kerberos 5 Principal	Список строк	"KRB5PRINCIPAL"	Поле «Kerberos KPN, Kerberos 5 Principal» в карточке субъекта
Permanent identifier	Список строк	"PERMANENT_IDENTIFIER"	Поле «Permanent identifier» в карточке субъекта
Xmpp address	Список строк	"XMPP_ADDR"	Поле «Xmpp address» в карточке субъекта
Service Name	Список строк	"SRV_NAME"	Поле «Service Name» в карточке субъекта
Subject Identification Method	Список строк	"SUBJECT_IDENTIFICATION_METHOD"	Поле «Subject Identification Method» в карточке субъекта

- Выход из карточки субъекта осуществляется по кнопке <Возврат> ← Субъекты в раздел «Субъекты» и по кнопкам разделов боковой панели.

4.4.4.1 Редактирование атрибутов субъекта

- Для субъектов локальной ресурсной системы доступно редактирование всех атрибутов SDN и SAN.
- Для субъектов подключенной ресурсной системы редактирование атрибутов SDN или SAN, значения которых получены Центром сертификации из ресурсной системы, недоступно. Все остальные атрибуты SDN или SAN доступны для редактирования.
- Для субъектов любой ресурсной системы редактирование сведений о субъектах в их карточках (поля «Получен из ресурсной системы», «Статус в ресурсной системе», «UUID») недоступны для редактирования.
- При вводе/редактировании значений атрибутов, указанных в Таблица 4, осуществляется валидация. Для всех остальных атрибутов субъекта валидация отсутствует.

Таблица 4 – Допустимые значения атрибутов

Атрибут	Правило валидации
Country	Допустимые символы: "A"-"Z", "a"-"z". Длина значения должна составлять 2 символа.
Domain qualifier	Допустимые символы: "A"-"Z", "a"-"z", "0"-"9", "'", "(", ")", "+", ",", "-", ".", "/", ":", "=", "?", пробел.
Email Address (E)	Допустимые символы: "A"-"Z", "a"-"z", "А"-"Я", "а"-"я", "0"-"9", ".", "@", "_", "-". Формат значения: "text@text".
Serial number	Допустимые символы: "A"-"Z", "a"-"z", "0"-"9", "'", "(", ")", "+", ",", "-", ".", "/", ":", "=", "?", пробел.
RFC 822 Name	Допустимые символы: "A"-"Z", "a"-"z", "0"-"9", ".", "@", "_", "-". Если необходимо использовать кириллицу, то кириллицу необходимо преобразовать в латиницу с помощью Punycode (подробнее см. RFC 3492) и ввести полученное значение в поле. При этом преобразовывать можно только доменную часть. Формат значения: "text@text".

Атрибут	Правило валидации
DNS Name	Допустимые символы: "A"-"Z", "a"-"z", "0"-"9", "-", ".", "*". Если необходимо использовать кириллицу, то кириллицу необходимо преобразовать в латиницу с помощью Punycode (подробнее см. RFC 3492) и ввести полученное значение в поле.
IP address	Допустимые символы: "A"-"F", "a"-"f", "0"-"9", ".", ":". Формат значения: IPv4-адрес или IPv6-адрес.
Directory Name	Формат значения: последовательность идентификаторов относительных отличительных имен (RDN) и их значений, отделенных запятой или запятой с пробелом (например, O=organization, OU=Department, L=City, DC=Component, C=RU...). Допускается использование следующих идентификаторов RDN: EMAILADDRESS, CN, UID, SERIALNUMBER, OU, O, L, ST, C, T, SURNAME, STREET, INITIALS, GIVENNAME, DC, UNSTRUCTUREDADDRESS, UNSTRUCTUREDNAME, POSTALCODE, BUSINESSCATEGORY, TELEPHONENUMBER, PSEUDONYM, POSTALADDRESS, NAME, DN, DESCRIPTION. В качестве идентификатора RDN допускается указание OID (формат OID должен соответствовать рекомендации ITU X.660).
Registered Identifier (OID)	Допустимые символы: "0"-"9", ".". Формат значения: OID в соответствии с рекомендацией ITU X.660.
MS UPN, User Principal Name	Допустимые символы: "A"-"Z", "a"-"z", "А"-"Я", "а"-"я", "ё", "Ё", "0"-"9", ".", "@", "_", "-", "/". Формат значения: "text@text".
MS GUID, Globally Unique Identifier	Допустимые символы: "A"-"F", "a"-"f", "0"-"9". Длина значения должна составлять 32 символа.
Kerberos KPN, Kerberos 5 Principal Name	Допустимые символы: "A"-"Z", "a"-"z", "А"-"Я", "а"-"я", "ё", "Ё", "0"-"9", ".", "@", "_", "-", "/". Формат значения: "text@text".
Permanent Identifier	Формат значения: "value/OID", где "value" – любая последовательность символов, а "OID" – OID в соответствии с рекомендацией ITU X.660. Допускается отсутствие значения "text", например, "/1.2.2.3.4.5".
Xmpp address	Допустимые символы: "A"-"Z", "a"-"z", "А"-"Я", "а"-"я", "ё", "Ё", "0"-"9", ".", "@", "_", "-", "/". Формат значения: "text@text".
Subject Identification Method	Формат значения: "OID::text::text", где "OID" – OID в соответствии с рекомендацией ITU X.660, а "text" – любая последовательность символов.
ИНН	Допустимые символы: "0"-"9". Длина значения должна составлять 12 символов.
ОГРН	Допустимые символы: "0"-"9". Длина значения должна составлять 13 символов.
ОГРНИП	Допустимые символы: "0"-"9". Длина значения должна составлять 15 символов.
СНИЛС	Допустимые символы: "0"-"9". Длина значения должна составлять 11 символов.
ИНН ЮЛ	Допустимые символы: "0"-"9". Длина значения должна составлять 10 символов.

- Для редактирования значения атрибута в карточке субъекта нажмите кнопку <Редактировать>  , в открывшемся окне введите новое значение атрибута в соответствующем поле, в соответствии с условиями валидации (см. Рисунок 45).
  - Для добавления значения атрибута (будет указано в поле атрибута через запятую) нажмите кнопку <Добавить значение +>;
  - Для удаления значения атрибута нажмите кнопку <Удалить значение атрибута>  . При этом у атрибута «Common name» нельзя удалить последнее значение;
  - Для сохранения результата нажмите кнопку <Сохранить>;
  - Для выхода из режима редактирования без сохранения изменений или нажмите кнопку <Закрыть>.

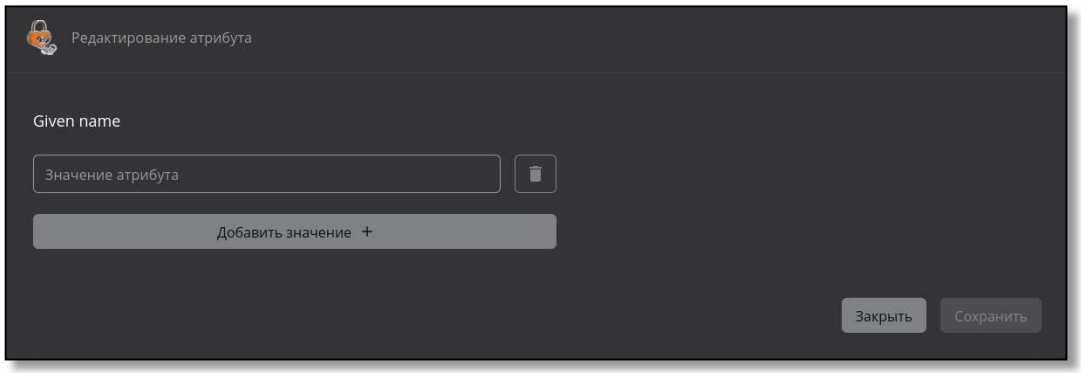


Рисунок 45 – Окно редактирования значения атрибута в карточке субъекта

4.4.5 Субъекты локальной ресурсной системы

- Локальную базу субъектов формируют:
  - субъекты, созданные Администратором путём вызова метода API;
  - субъекты отключенной ресурсной системы (удалённой ранее зарегистрированной ресурсной системы), атрибут субъекта «isBlocked» принимает значение «false». В случае повторного подключения ресурсной системы связи субъектов с группами будут восстановлены, обновлены атрибуты в соответствии с данными из ресурсной системы;
  - субъекты, загруженные в базу данных Aladdin eCA при подключении ресурсной системы, но отсутствующие в списке субъектов, полученном по результатам выполнения полной синхронизации ресурсной системы. Атрибут субъекта «isBlocked» принимает значение «false».
- Локальный субъект отключенной ресурсной системы при подключении ресурсной системы, где существует данный субъект, будет перенесён из базы локальной ресурсной системы (атрибут субъекта «isConnected» примет значение «true»). При этом будет выполнено обновление атрибутов субъекта в соответствии с его атрибутами из ресурсной системы, остальные текущие атрибуты (то есть те, которые не были получены из ресурсной системы) не изменятся. Проверка субъектов осуществляется по атрибуту «id».

4.4.6 Субъекты внешнего ресурса

- Внешний (подключенный) ресурс формируется в результате регистрации службы каталогов доменных служб Samba DC, РЕД АДМ, ALD PRO, FreeIPA, MS Active Directory или Альт Домен.
- Подключенный ресурс будет отображен только после регистрации ресурсной системы на вкладке «Ресурсная система».
- Обновление списков и данных субъектов ресурсной системы происходит по правилам, приведённым в пункте 4.5.1 настоящего руководства.
- После подключения внешней ресурсной системы, обновления и выбора источника в поле «Ресурсная система», субъекты будут отображены в виде списка в окне вкладки «Субъекты». Возможно настроить отображение определенной группы безопасности или вывести полный список, упорядочив субъекты в алфавитном порядке по имени (CommonName) (см. Рисунок 40).

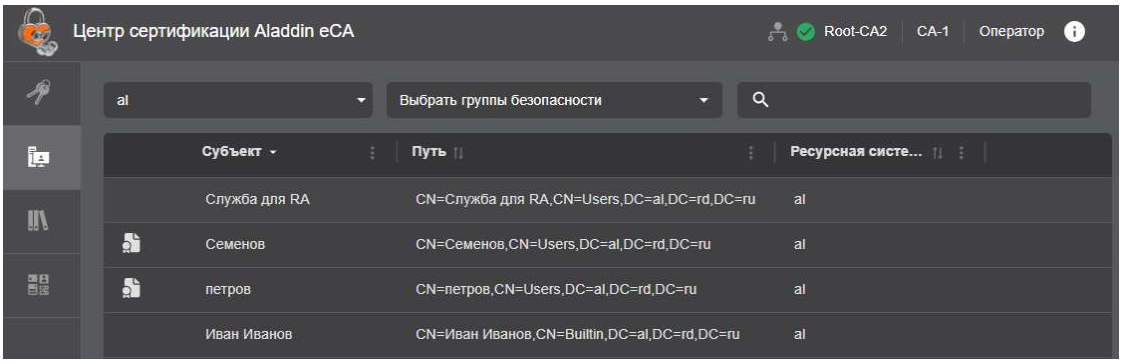


Рисунок 46 – Экран раздела меню «Субъекты». Подключенный ресурс

- Загрузка данных осуществляется из всей ресурсной системы, начиная с точки подключения, указанной в настройках подключения Корневого каталога.
- Для каждого загруженного пользователя и компьютера будет создан субъект и подгружены все поля, относящиеся к SubjectDN и SubjectAltName. Преобразование содержимого записи LDAP в поля базы субъектов ресурсной системы происходит в соответствии с Таблица 9.

Таблица 5 – Преобразование данных субъектов ресурсной системы

Атрибут субъекта Aladdin eCA	**Поле в базах Samba DC, MS AD, РЕД АДМ, Альт Домен для типов субъектов**		**Поле в базах ALD PRO, FreeIPA для типов субъектов**		
	Пользователь	**Компьютер**	**Пользователь**	**Компьютер**	**Сервис**
Id	ObjectGUID	ObjectGUID	ipaUniquelD	ipaUniquelD	ipaUniquelD
Common name	cn	cn	cn	cn	krbPrincipalName
			uid		
Initials	-	-	initials	-	-
Surname	sn	-	sn	-	-
Given Name	givenName	-	givenName	-	-
Organization	-	-	krbPrincipalName	krbPrincipalName	krbPrincipalName
Name	name	name	-	serverHostName	-
MS GUID	-	ObjectGUID	-	-	-
Domain Qualifier	distigushedName	distigushedName	entrydn	entrydn	
Description	description	-	-	-	-
DNS Name	-	dNSHostName	-	fqdn	-
Email Address (Mail)	mail	-	mail	-	-
	userPrincipalName		krbPrincipalName	krbPrincipalName	
RFC 822 NAME	mail	-	mail	-	krbPrincipalName
	userPrincipalName		krbPrincipalName	krbPrincipalName	
MS UPN	userPrincipalName	-	krbPrincipalName	krbPrincipalName	krbPrincipalName
Unique Identifier (UID)	-	-	uid	-	-
Kerberos KPN, Kerberos 5 Principal	-	-	-	krbPrincipalName	-

SID	objectSid	objectSid	-	-	-

- Если данные поля отсутствуют в описании субъекта в подключенном домене, то в шаблоне при выпуске сертификата соответствующие поля заполняются пустыми значениями.
- Идентификация подключенных субъектов в Центре сертификации осуществляется по атрибуту `UUID`.

4.4.7 Создание сертификата для субъекта ресурсной системы

Создание сертификата для локального субъекта доступно авторизованному пользователю с ролью «Оператор», которому в соответствии с правилами доступа предоставлены полномочия на доступ к субъектам локальной ресурсной системы. Создание сертификата для подключенного к ресурсной системе субъекта доступно авторизованному пользователю с ролью «Оператор», которому в соответствии с правилами доступа предоставлены полномочия на доступ к субъектам группы безопасности ресурсной системы, куда входит данный субъект.

- Выберите субъект, для которого необходимо создать сертификат, нажмите появившуюся кнопку <Создать сертификат> и выберите способ создания из выпадающего списка (см. Рисунок 47).

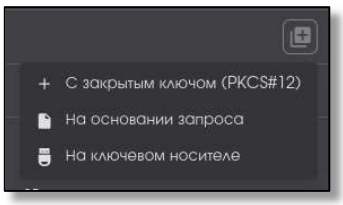


Рисунок 47 - Окно выпуска сертификата для субъекта ресурсной системы

4.4.7.1 Создание сертификата с закрытым ключом pkcs#12

- В открывшемся окне создания сертификата (см. Рисунок 48) выберите шаблон создаваемого сертификата из выпадающего списка. В выпадающем списке будут присутствовать только те шаблоны, на использование которых данному оператору предоставлен доступ администратором путем создания правил доступа. Описание полей для шаблонов по умолчанию приведено в Приложение 1. Описание полей по умолчанию предустановленных шаблонов сертификатов. После выбора шаблона в окне отображается информация о центре сертификации, в котором будет выпущен сертификат. Центр сертификации, в котором будет выпущен сертификат, определяется при создании шаблона. Если в шаблоне в качестве центра сертификации выбрано значение «Любой», то выпуск сертификатов по данному шаблону доступен в любом центре сертификации. При этом для выпуска сертификатов будет использован активный в данный момент центр сертификации.

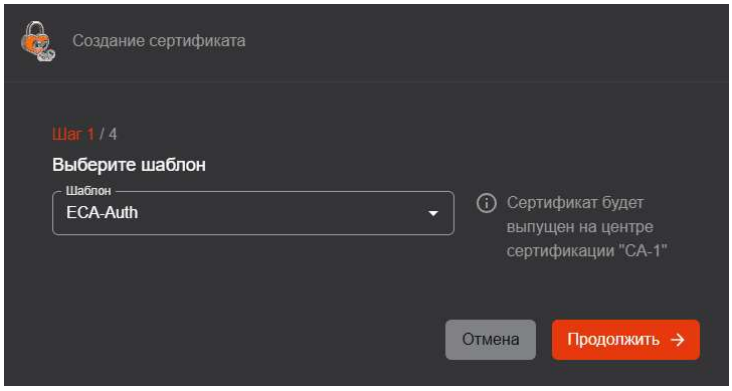


Рисунок 48 – Окно создания сертификата PKCS#12. Шаг 1. Выбор шаблона

- Нажмите ставшую активной кнопку <Продолжить> для перехода к следующему шагу.
- Значение атрибутов заполняется автоматически в соответствии с данными в карточке субъекта (см. п. 4.4.4 настоящего руководства) и изменению не подлежит (подробное описание полей предустановленных шаблонов см. в Приложение 1. Описание полей по умолчанию предустановленных шаблонов сертификатов).

В случае если в атрибуте указано несколько значений, в выпадающем меню будет предложен выбор значения из существующих или возможно добавление значения атрибута по нажатию кнопки <Добавить> справа от соответствующего поля (если атрибут содержит несколько значений, то при наведении мышки на кнопку <Добавить>, она становиться активной – красного цвета). Также дополнительно добавленное значение атрибута можно удалить по кнопке справа от соответствующего поля атрибута (см. Рисунок 49).

- Если данные атрибутов отсутствуют, то необходимо ввести значения в соответствующие поля в карточке субъекта (см. п. 4.4.4.1 настоящего руководства).
- Необязательные поля могут оставаться незаполненными.
- Нажмите ставшую активной кнопку <Продолжить> для перехода к следующему шагу.

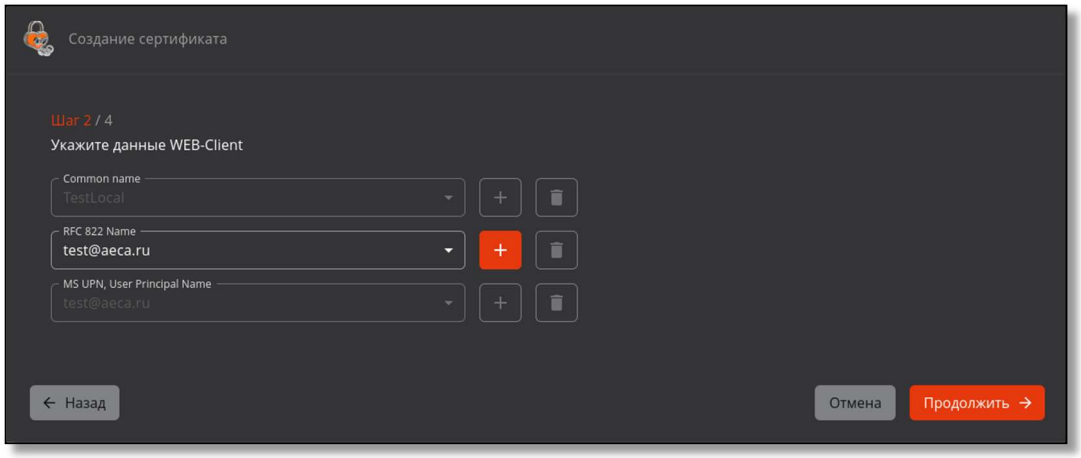


Рисунок 49 – Окно создания сертификата PKCS#12. Шаг 2. Атрибуты сертификата

- Далее администратору необходимо создать пароль с подтверждением для ключевого контейнера (см. Рисунок 50). Правила ввода пароля:
  - для просмотра вводимых символов необходимо нажать кнопку на текущей строке;
  - пароль должен содержать не менее 8 символов с использованием цифр, заглавных и прописных букв, ввод осуществляется на латинице;
  - если в пароле используются запрещенные символы, то рамка поля ввода приобретает красный цвет;
  - если пароли не совпадают, то рамка поля подтверждения окрашивается в красный цвет.

Кнопка <Продолжить> доступна только после ввода и верного повторения пароля в соответствии с правилами ввода.

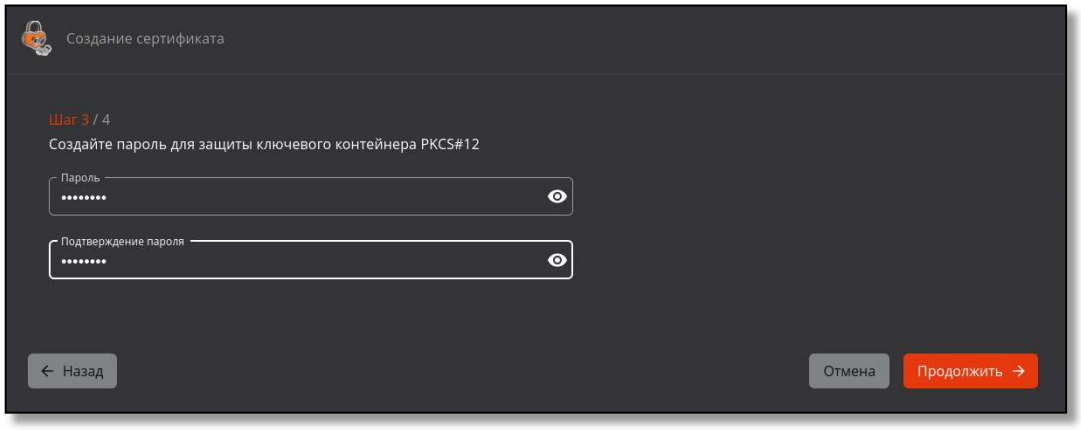


Рисунок 50 – Окно создания сертификата PKCS#12. Шаг 3. Задание пароля контейнера сертификата

- В следующем окне требуется определить параметры шифрования (см. Рисунок 51):
  - алгоритм ключа;

– длину ключа.

Доступные алгоритмы определяются выбранным шаблоном (если криптопровайдер алгоритма не заявлен в шаблоне, его выбор будет недоступен), а также зависят от криптопровайдеров центра сертификации, указанного в выбранном шаблоне (если в шаблоне в качестве центр сертификации установлено значение «любой», доступные алгоритмы будут зависеть от криптопровайдеров активного центра сертификации).

- После выбора алгоритма нажмите кнопку <Создать сертификат>.

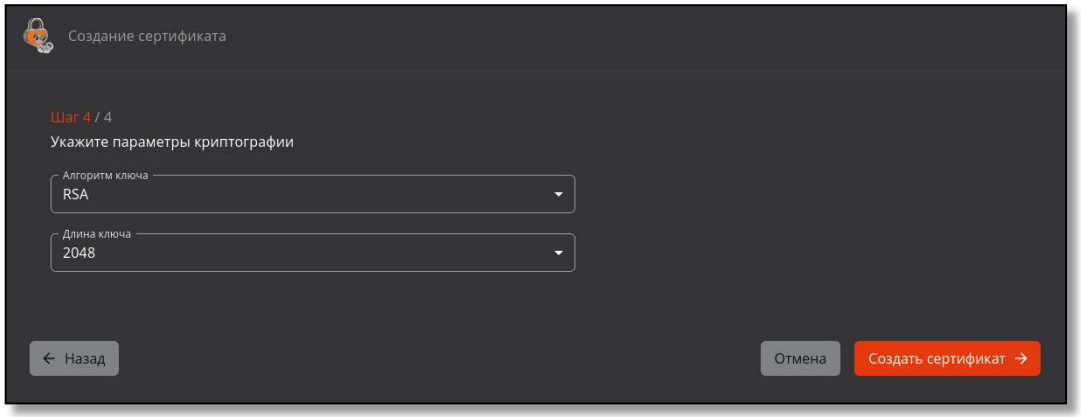


Рисунок 51 - Окно создания сертификата PKCS#12. Шаг 4. Выбор параметров криптографии

- Далее по нажатию кнопки <Создать сертификат> открывается финальное окно создания сертификата и отображается краткая информация о созданном сертификате (см. Рисунок 58).

Внимание! Только в данном окне возможно скачать сертификат и закрытый ключ в контейнере pkcs#12, после закрытия окна скачать сертификат возможно только в формате .pem.

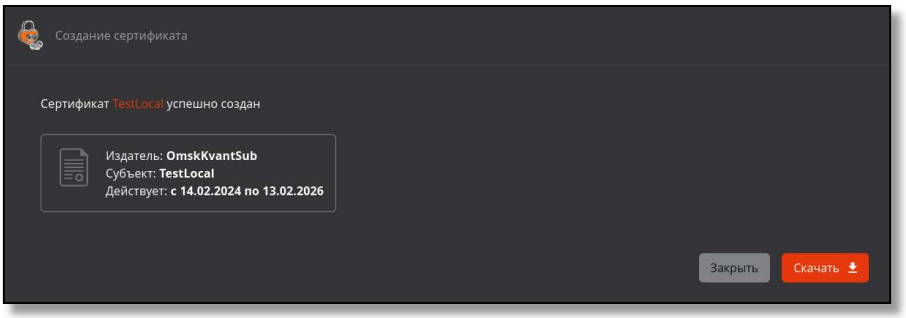


Рисунок 52 – Окно по результату успешного завершения создания сертификата PKCS#12

- При успешном создании сертификата и выполнении всех условий ниже происходит его публикация в ресурсную систему:

  – сертификат был создан для субъекта, подключенного к ресурсной системе;
  – сертификат создан по шаблону, в котором включена публикация сертификата в ресурсную систему.

  В случае успешной публикации сертификата в ресурсную систему отобразится всплывающее сообщение «Сертификат успешно опубликован в ресурсную систему».
  В случае ошибки публикации сертификата в ресурсную систему отобразится всплывающее сообщение «Ошибка публикации сертификата в ресурсную систему», также сертификат будет помечен, как требующий публикации. И при включенной настройке автопубликации будет произведена попытка его публикации в соответствии с расписанием.

4.4.7.2 Создание сертификата субъекта по запросу

- Предварительные условия выполнения сценария:
  - файл-запрос для субъекта должен быть подготовлен заранее на стороннем ЦС (например, при помощи ПО «Единый клиент JaCarta»);
  - расширение файл-запроса должно быть `***.csr` или `***.pem`;
  - файл-запрос должен быть сформирован с учетом известных данных выбранного шаблона компонента «Центр сертификации Aladdin Enterprise Certification Authority». Например, для использования шаблона «Domain Controller» в запросе должны быть указаны параметры DNS Name и MS GUID;
  - по файлу-запроса ранее не был выпущен сертификат.
- В открывшемся окне (см. Рисунок 53) необходимо выбрать и загрузить файл-запрос, а также выбрать шаблон сертификата в соответствии с запросом (предполагается, что оператор заранее знает какой шаблон необходимо выбрать). В списке шаблонов будут присутствовать только те шаблоны, на использование которых данному оператору предоставлен доступ администратором путем создания правил доступа. По файлу запроса возможен только одноразовый выпуск сертификата. После выбора шаблона в окне отображается информация о центре сертификации, в котором будет выпущен сертификат. Центр сертификации, в котором будет выпущен сертификат, определяется при создании шаблона. Если в шаблоне в качестве центра сертификации выбрано значение «Любой», то выпуск сертификатов по данному шаблону доступен в любом центре сертификации. При этом для выпуска сертификатов будет использован активный в данный момент центр сертификации.
- При необходимости, возможно перезагрузить файл-запрос в мастере создания сертификата без сброса текущего прогресса по кнопке <Изменить>.

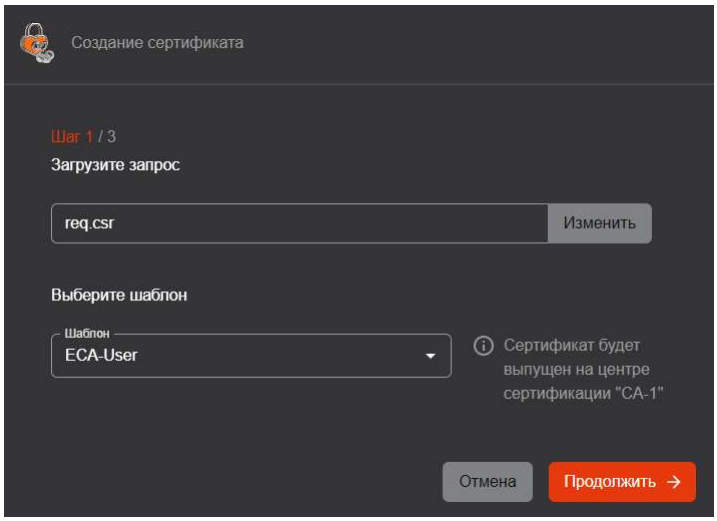


Рисунок 53 – Окно создания сертификата по запросу. Шаг 1. Загрузка запроса и выбор шаблона

- После загрузки файла запроса и выбора шаблона нажмите активировавшуюся кнопку <Продолжить>.
- Программа проверяет запрос на соответствие полей запроса на сертификат и атрибутов субъекта по правилам, приведённым в Таблица 6. Проверка является регистронезависимой.

Таблица 6 – Соответствие полей запроса шаблону выпускаемого сертификата

Поле в шаблоне	Значение поля в запросе	Атрибут субъекта АЕСА	Возможность создания сертификата	Поле в сертификате	Возможные ошибки*
Правила проверки соответствия SDN полей					
Есть, обязательное	Есть	Нет	Нет	-	1) Ошибка №2, если значение в запросе не проходит валидацию по шаблону

Поле в шаблоне	Значение поля в запросе	Атрибут субъекта АЕСА	Возможность создания сертификата	Поле в сертификате	Возможные ошибки*
					2) Ошибка №4
Есть, обязательное	Нет	Нет	Нет	-	Ошибка №1
Есть, обязательное	Есть	Есть	Да	Присутствует	1) Ошибка №2, если значение в запросе не проходит валидацию по шаблону 2) Ошибка №4, если значение в запросе не соответствует значению атрибута субъекта
Есть, обязательное	Нет	Есть	Нет	-	Ошибка №1
Есть, необязательное	Есть	Нет	Нет	-	1) Ошибка №2, если значение в запросе не проходит валидацию по шаблону 2) Ошибка №4
Есть, необязательное	Нет	Нет	Да	Отсутствует	-
Есть, необязательное	Есть	Есть	Да	Присутствует	1) Ошибка №2, если значение в запросе не проходит валидацию по шаблону 2) Ошибка №4, если значение в запросе не соответствует значению атрибута
Есть, необязательное	Нет	Есть	Да	Отсутствует	-
Нет	Есть	Нет	Нет	-	Ошибка №3
Нет	Нет	Нет	Да	Отсутствует	-
Нет	Есть	Есть	Нет	-	Ошибка №3
Нет	Нет	Есть	Да	Отсутствует	-
Правила проверки соответствия SAN полей					
Есть, обязательное	Есть	Нет	Нет	-	1) Ошибка №2, если значение в запросе не проходит валидацию по шаблону 2) Ошибка №4
Есть, обязательное	Нет	Нет	Нет	-	Ошибка №1
Есть, обязательное	Есть	Есть	Да	Присутствует	1) Ошибка 2, если значение в запросе не проходит валидацию по шаблону 2) Ошибка 4, если значение в запросе не соответствует значению атрибута субъекта Исправление указанных ошибок доступно на этапе переопределения значений для полей SAN, указанных в шаблоне.
Есть, обязательное	Нет	Есть	Да	Присутствует	Ошибка №1 Исправление указанной ошибки доступно на этапе переопределения SAN (путем выбора значения для поля из атрибута субъекта).
Есть, необязательное	Есть	Нет	Да	Отсутствует	1) Ошибка №2, если значение в запросе не проходит валидацию по шаблону 2) Ошибка №4

Поле в шаблоне	Значение поля в запросе	Атрибут субъекта АЕСА	Возможность создания сертификата	Поле в сертификате	Возможные ошибки*
Есть, необязательное	Нет	Нет	Да	Отсутствует	-
Есть, необязательное	Есть	Есть	Да	Присутствует, если поле не было удалено на этапе переопределения значений для полей SAN, указанных в шаблоне или Отсутствует, если поле было удалено на этапе переопределения значений для полей SAN, указанных в шаблоне	1) Ошибка №2, если значение в запросе не проходит валидацию по шаблону 2) Ошибка 4, если значение в запросе не соответствует значению атрибута
Есть, необязательное	Нет	Есть	Да	Присутствует, если поле не было удалено на этапе переопределения значений для полей SAN, указанных в шаблоне или Отсутствует, если поле было удалено на этапе переопределения значений для полей SAN, указанных в шаблоне	-
Нет	Есть	Нет	Да	Отсутствует	Ошибка №3
Нет	Нет	Нет	Да	Отсутствует	-
Нет	Есть	Есть	Да	Отсутствует	Ошибка №3
Нет	Нет	Есть	Да	Отсутствует	-

- Если во время обработки запроса произошла ошибка, в окне результата обработки запроса отображаются сообщения об ошибках в полях запроса, где они были обнаружены, с цветовой (красной) индикацией и предупреждающей иконкой (см. Рисунок 54 и Рисунок 55).

- В случае выявления ошибки в запросе на сертификат доступа для субъекта возможны следующие сообщения:
  - «Отсутствует обязательное поле» (ошибка №1)[10];
  - «Значение в поле не соответствует регулярному выражению: \"%s\"", где \"%s\» (ошибка №2)[11];
  - «Поле отсутствует в шаблоне» (ошибка №3);
  - «Значение в поле не соответствует значению атрибута субъекта» (ошибка №4).

Если создание сертификата невозможно, то существует две возможности:
- вернуться на предыдущий шаг и сменить шаблон на подходящий;
- пересоздать файл-запрос с учетом выявленных при сверке ошибок и перезагрузить файл-запрос, вернувшись на предыдущие шаги по нажатию кнопки <Назад>.

[10] Описание полей предустановленных шаблонов см. в Приложение 1. Описание полей по умолчанию предустановленных шаблонов сертификатов.

[11] Правила валидации значений полей предустановленных шаблонов см. в Приложение 2. Правила валидации значений полей по умолчанию предустановленных шаблонов сертификатов.

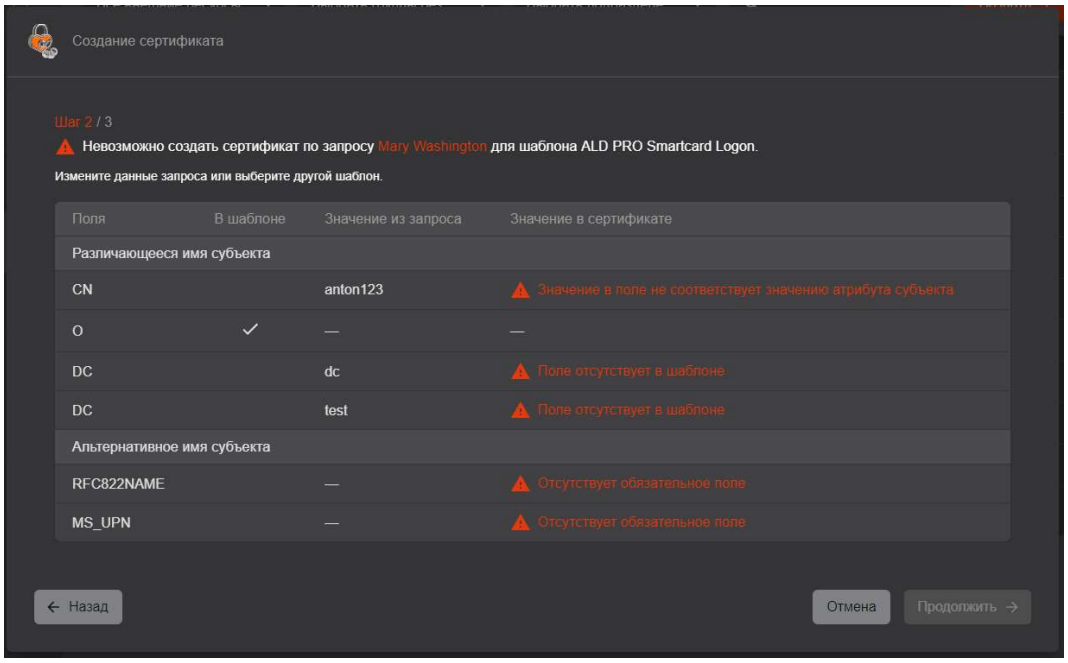


Рисунок 54 – Окно создания сертификата по запросу. Шаг 2. Результат обработки запроса с ошибкой в поле различающегося имени субъекта

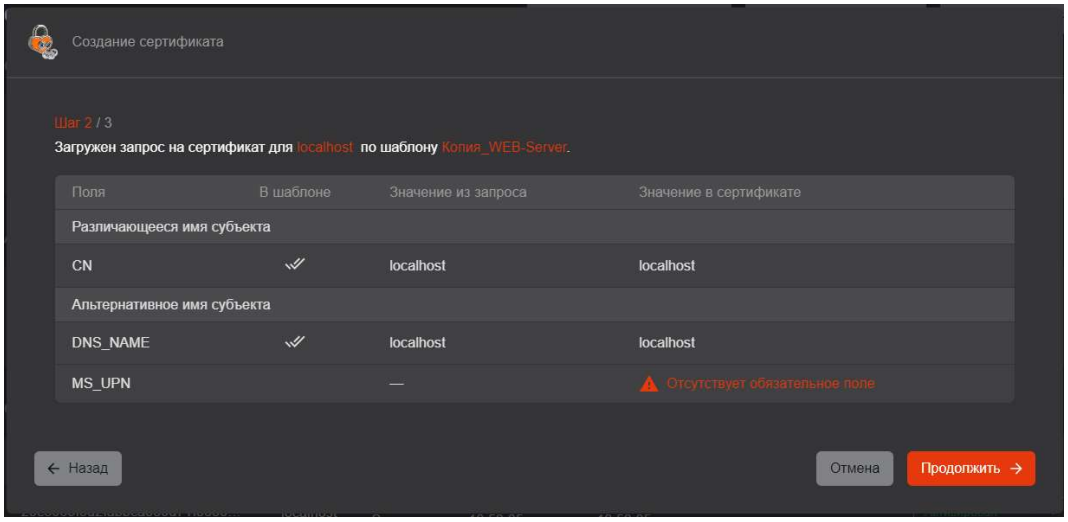


Рисунок 55 – Окно создания сертификата по запросу. Шаг 2. Результат обработки запроса с ошибками в полях альтернативного имени субъекта

- В результате успешной обработки запроса на сертификат субъекта на следующем шаге отображаются (см. Рисунок 56):
  - таблица, содержащая:
    - перечень полей, заданных в шаблоне (в столбце «Поля»);
    - пиктограммы, отображающие обязательные и необязательные поля шаблона (в столбце «В шаблоне»). Пиктограмма «Галка» ✓ указывает на необязательность поля, а пиктограмма «Двойная галка» ✓✓ указывает на обязательность поля;
    - значения для полей, заданных шаблоном, полученные из запроса на сертификат (в столбце «Значение из запроса»);
    - значения, которые будут указаны в полях создаваемого сертификата (в столбце «Значение в сертификате»).
  - данные таблицы разделена на две основные части:

- различающееся имя субъекта (Subject DN);
- дополнительное имя субъекта (Subject AltName).

– кнопка <Продолжить> для перехода к следующему шагу;

– кнопка <Назад> для возврата к предыдущему шагу;

– кнопка <Отмена> для завершения работы мастера создания сертификата без сохранения результатов.

- В случае, если в файле-запросе существуют дополнительные поля субъектных идентификаторов, отсутствующие в текущей реализации[12], то они идентифицируются по параметру OID.

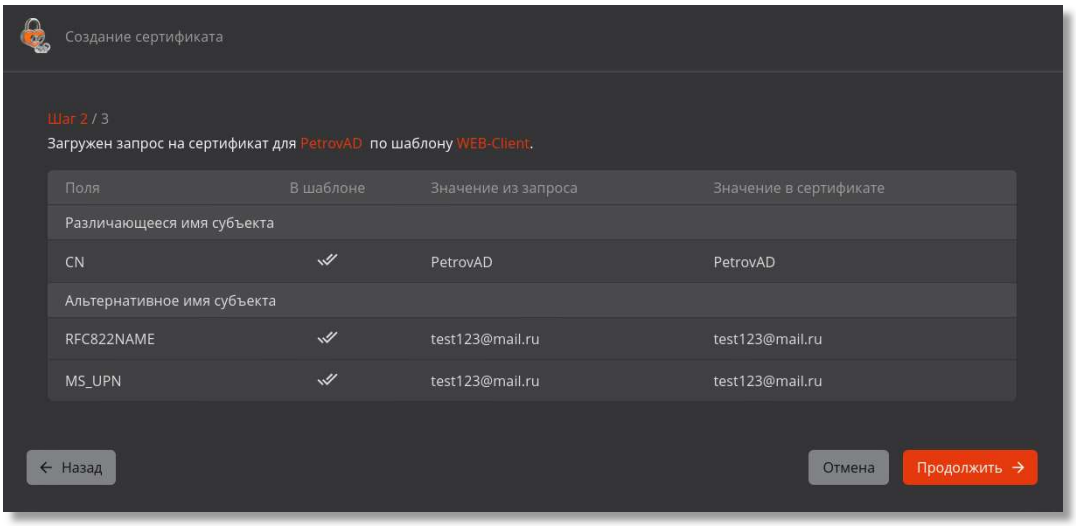


Рисунок 56 – Окно создания сертификата по запросу. Шаг 2. Результат успешной обработки запроса

- После успешной загрузки файла запроса нажмите кнопку <Продолжить> для продолжения процедуры выпуска сертификата для субъекта, кнопку <Отмена> для прекращения процедуры выпуска сертификата или кнопку <Назад> для возврата на предыдущий шаг.

- В окне следующего шага указаны атрибуты в соответствии с шаблоном сертификата (подробное описание полей предустановленных шаблонов см. в Приложение 1. Описание полей по умолчанию предустановленных шаблонов сертификатов). Значение атрибутов заполняется автоматически в соответствии с данными в карточке субъекта (см. п. 4.4.4 настоящего руководства) и изменению не подлежит. В случае если в атрибуте указано несколько значений, в выпадающем меню будет предложен выбор значения из существующих или возможно добавление значения атрибута по нажатию кнопки <Добавить> справа от соответствующего поля (если атрибут содержит несколько значений, то при наведении мышки на кнопку <Добавить>, она становиться активной – красного цвета). Также дополнительно добавленное значение атрибута можно удалить по кнопке справа от соответствующего поля атрибута (см. Рисунок 57).

- Перечень доступных для выбора значений в полях SAN включает в себя:
  – значения соответствующего полю атрибута субъекта;
  – значения данного поля из запроса, если у субъекта в соответствующем атрибуте есть аналогичное значение, отличающееся от значения в запросе только регистрами символов (такие значения отмечены пиктограммой «Запрос»).

- При отсутствии доступных для указания значений в поле обязательного атрибута будет отображаться ошибка «У субъекта отсутствует указанный атрибут».

[12] Для справки – https://www.alvestrand.no/objectid/2.5.4.html, раздел Subdirectory references.

- Необязательные поля могут оставаться незаполненными.

Рисунок 57 – Окно создания сертификата на основании запроса. Шаг 3. Атрибуты сертификата

- Далее по нажатию кнопки <Создать сертификат> открывается финальное окно создания сертификата и отображается краткая информация о созданном сертификате (см. Рисунок 58). У созданного сертификата значения в полях SDN соответствуют значениям в соответствующих полях SDN запроса, на основе которого был создан сертификат.

- При попытке повторного создания сертификата на основании одного запроса на данном шаге отображается ошибка.

Внимание! Только в данном окне возможно скачать сертификат и закрытый ключ в контейнере pkcs#12, после закрытия окна скачать сертификат возможно только в формате .pem.

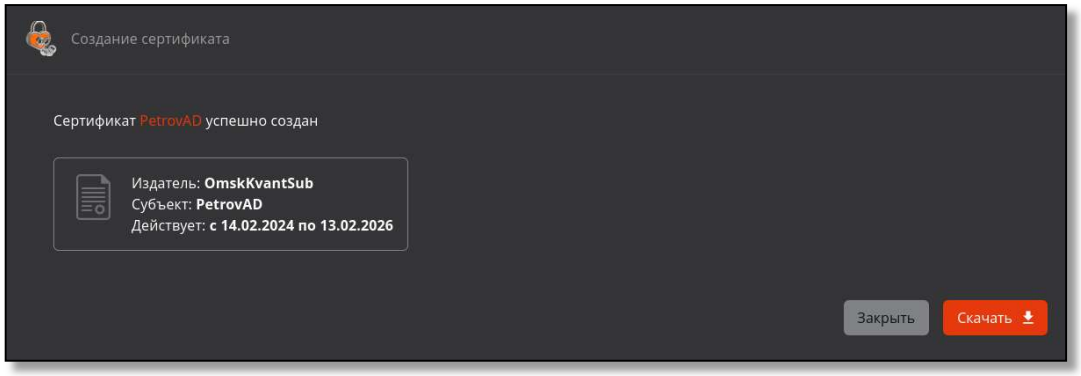


Рисунок 58 – Окно создания сертификата по запросу. Информирование об успешном создании сертификата

- При успешном создании сертификата и выполнении всех условий ниже происходит его публикация в ресурсную систему:

  – сертификат был создан для субъекта, подключенного к ресурсной системе;
  – сертификат создан по шаблону, в котором включена публикация сертификата в ресурсную систему.

  В случае успешной публикации сертификата в ресурсную систему отобразится всплывающее сообщение «Сертификат успешно опубликован в ресурсную систему».
  В случае ошибки публикации сертификата в ресурсную систему отобразится всплывающее сообщение «Ошибка публикации сертификата в ресурсную систему», также сертификат будет помечен, как требующий публикации. И при включенной настройке автопубликации будет произведена попытка его публикации в соответствии с расписанием.

4.4.7.3 Создание сертификата субъекта на ключевом носителе

Предварительные условия выполнения сценария:

- Убедитесь, что поддерживаемый электронный ключ присоединен к АРМ выпускающего Центра сертификации;
- Убедитесь, что на сервере выпускающего Центра сертификации установлено ПО JC-WebClient версии 4.3.2 или 4.3.3 для дальнейшей работы с ключевыми носителями из браузера.
- Нажатие кнопки <Создать (Выпустить) сертификат> - «на ключевом носителе» стартует сценарий по созданию сертификата на ключевом носителе.
- В случае если электронный ключ успешно подключен, в открывшемся окне (см. **Ошибка! Источник ссылки не найден.**) необходимо выбрать ключевой носитель из выпадающего списка в поле «Устройство», ввести PIN-код пользователя ключевого носителя и указать шаблон для выпуска сертификата. В списке шаблонов будут присутствовать только те шаблоны, на использование которых данному оператору предоставлен доступ администратором путем создания правил доступа. После выбора шаблона в окне отображается информация о центре сертификации, в котором будет выпущен сертификат. Центр сертификации, в котором будет выпущен сертификат, определяется при создании шаблона. Если в шаблоне в качестве центра сертификации выбрано значение «Любой», то выпуск сертификатов по данному шаблону доступен в любом центре сертификации. При этом для выпуска сертификатов будет использован активный в данный момент центр сертификации.
- Переход на следующий шаг осуществляется по ставшей активной кнопке <Продолжить> в случае ввода корректного PIN-кода электронного ключа и заполнении всех полей.

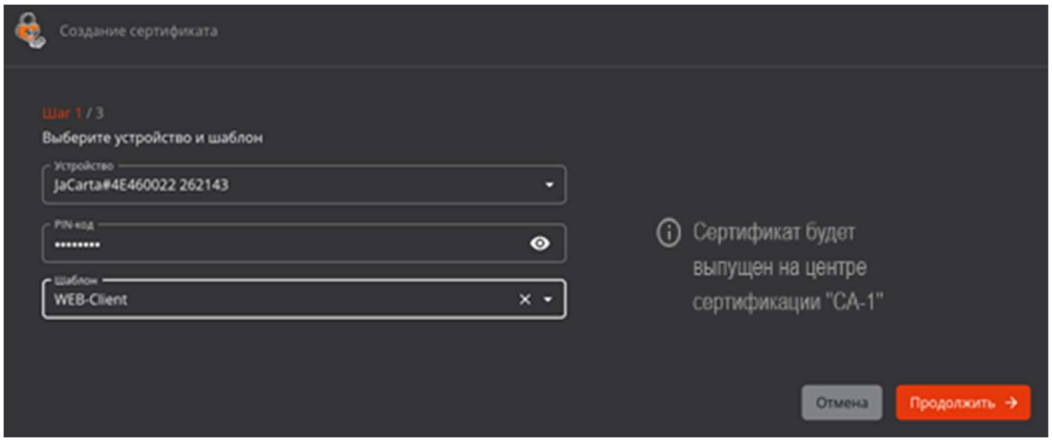


Рисунок 59 – Окно создания сертификата на электронном ключе. Шаг 1

- В окне Шага 2 указаны атрибуты в соответствии с выбранным (на предыдущем шаге) шаблоном сертификата (подробное описание полей предустановленных шаблонов см. в Приложение 1. Описание полей по умолчанию предустановленных шаблонов сертификатов). Значение атрибутов заполняется автоматически в соответствии с данными в карточке субъекта (см. п. 4.4.4 настоящего руководства) и изменению не подлежит. В случае если в атрибуте указано несколько значений, в выпадающем меню будет предложен выбор значения из существующих или возможно добавление значения атрибута по нажатию кнопки <Добавить> + справа от соответствующего поля (если атрибут содержит несколько значений, то при наведении мышки на кнопку <Добавить>, она становиться активной – красного цвета). Также дополнительно добавленное значение атрибута можно удалить по кнопке справа от соответствующего поля атрибута (см. **Ошибка! Источник ссылки не найден.**).
- Необязательные поля могут оставаться незаполненными.

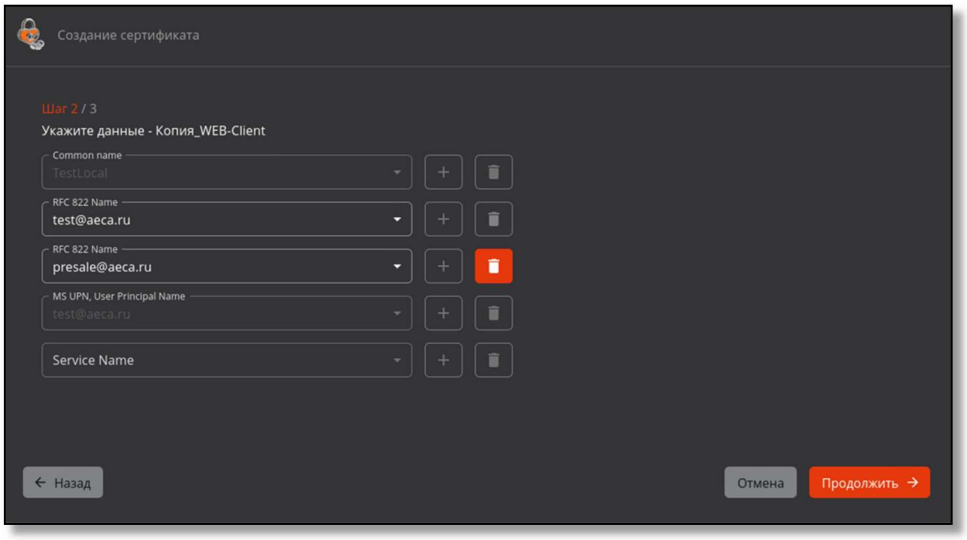


Рисунок 60 – Окно создания сертификата на электронном ключе. Шаг 2

- Далее необходимо выбрать параметры криптографии (см. **Ошибка! Источник ссылки не найден.**):
  - выберите алгоритм генерации ключевой пары из раскрывающегося списка. Список алгоритмов ключа определяется шаблоном. При этом алгоритмы, для которых на активном центре сертификации отключен криптопровайдер, не будут отображены в списке. По умолчанию указан первый алгоритм из списка в используемом шаблоне, для которого не отключен криптопровайдер;
  - выберите длину ключа из раскрывающегося списка. Минимальная доступная для выбора длина ключа определяется выбранным шаблоном. По умолчанию указана минимальная длина ключа по шаблону;
  - после выбора алгоритма нажмите кнопку <Создать сертификат>.

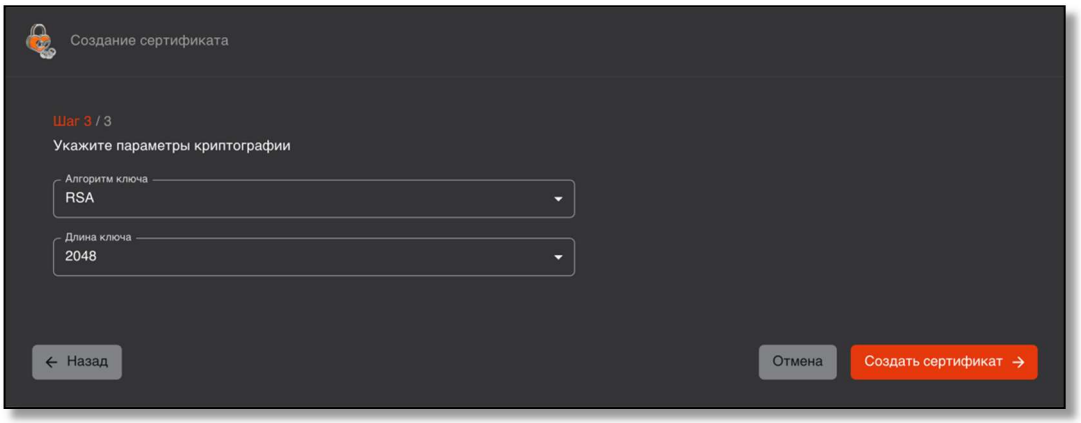


Рисунок 61 – Окно создания сертификата на электронном ключе. Шаг 3

- Далее осуществляются все необходимые операции для выпуска и записи сертификата на ключевой носитель:
  - генерация ключевой пары на основе данных заполненного шаблона сертификата на предыдущем шаге;
  - генерация запроса на основе данных заполненного шаблона сертификата на предыдущем шаге;
  - выпуск сертификата;
  - запись сертификата на ключевой носитель.
- Процессы выполняются автоматически и после завершения процессов станут доступны кнопки <Скачать сертификат> и <Скачать цепочку сертификатов> (см. **Ошибка! Источник ссылки не найден.**).

Внимание! Сертификат и закрытый ключ в контейнере pkcs#12 возможно скачать только в последнем окне выпуска сертификата «об успешном создании сертификата» по нажатию на кнопку <Скачать>. Далее, после закрытия окна, скачивание выпущенного сертификата для субъекта в разделе «Сертификаты» доступно только в формате .pem!

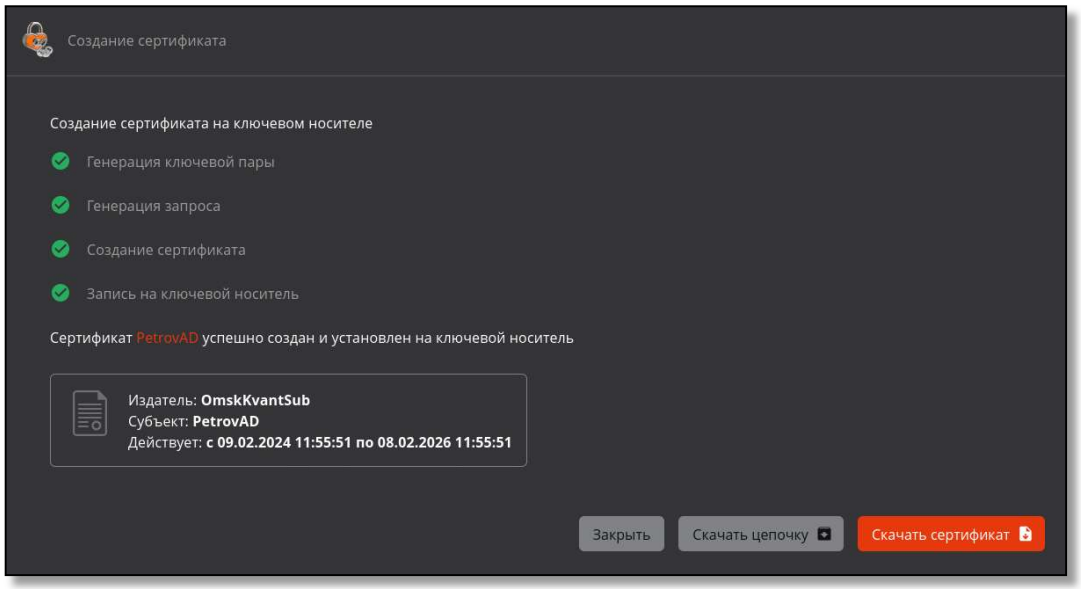


Рисунок 62 – Окно успешного создания сертификата субъекта на электронном ключе

сертификата

- При успешном создании сертификата и выполнении всех условий ниже происходит его публикация в ресурсную систему:
  - сертификат был создан для субъекта, подключенного к ресурсной системе;
  - сертификат создан по шаблону, в котором включена публикация сертификата в ресурсную систему.

  В случае успешной публикации сертификата в ресурсную систему отобразится всплывающее сообщение «Сертификат успешно опубликован в ресурсную систему».

  В случае ошибки публикации сертификата в ресурсную систему отобразится всплывающее сообщение «Ошибка публикации сертификата в ресурсную систему», также сертификат будет помечен, как требующий публикации. И при включенной настройке автопубликации будет произведена попытка его публикации в соответствии с расписанием.

4.5 Раздел «Ресурсные системы»

Раздел «Ресурсные системы» обеспечивает получение данных субъектов с целью упрощенного выпуска сертификатов субъектам служб каталогов Linux и Microsoft, а также централизованную публикацию выпущенных сертификатов в карточку субъекта службы каталогов. Для авторизованного пользователя с ролью «Оператор» в списке присутствуют только те ресурсные системы, на субъекты которых ему прямо или косвенно[13] предоставлены полномочия в соответствии с текущими правилами доступа.

Переход в раздел «Ресурсные системы» осуществляется через боковое меню, расположенное слева на главном экране (см. Рисунок 63).

- На основном экране «Ресурсной системы» отображены информационные поля (см. Рисунок 63):
  - имя домена – домен подключенной ресурсной системы;

[13] Путем наследования от группы безопасности, куда входит субъект, на основе которого создана учетная пользователя с ролью «Оператор».

- последнее обновление – отображается дата и время последней синхронизации базы субъектов источника с базой данных программного компонента;
- статус –статус ресурсной системы, который назначается в соответствии с критериями, приведенными в таблице ниже;;

Таблица 7 – Статусы ресурсной системы и критерии их присвоения

Статус ресурсной системы	Критерии присвоения статуса ресурсной системе
Ожидание обработки	Все точки подключения к данной ресурсной системе ожидают первой синхронизации (при регистрации ресурсной системы)
Успешно	Все точки подключения к ресурсной системе успешно синхронизированы
В процессе	Какая-либо точка подключения к ресурсной системе находится в процессе синхронизации или удаления
Ошибка	У ресурсной системы нет точек, находящихся в процессе синхронизации, и есть хотя бы одна точка, синхронизация которой завершена с ошибкой

- субъекты – показывает количество загруженных субъектов из источника;
-  - пиктограмма «Очередь» показывает, что ресурсной системе назначена задача, которая поставлена в очередь, так как в данный момент выполняется другая задача.

  Назначение ресурсной системе новой задачи с постановкой в очередь сопровождается уведомительным сообщением «Успешно. Задача поставлена в очередь».

  Повторно назначить ресурсной системе задачу, уже находящуюся в очереди, невозможно. Данное действие сопровождается уведомительным сообщением «Ошибка. Задача уже находится в очереди».

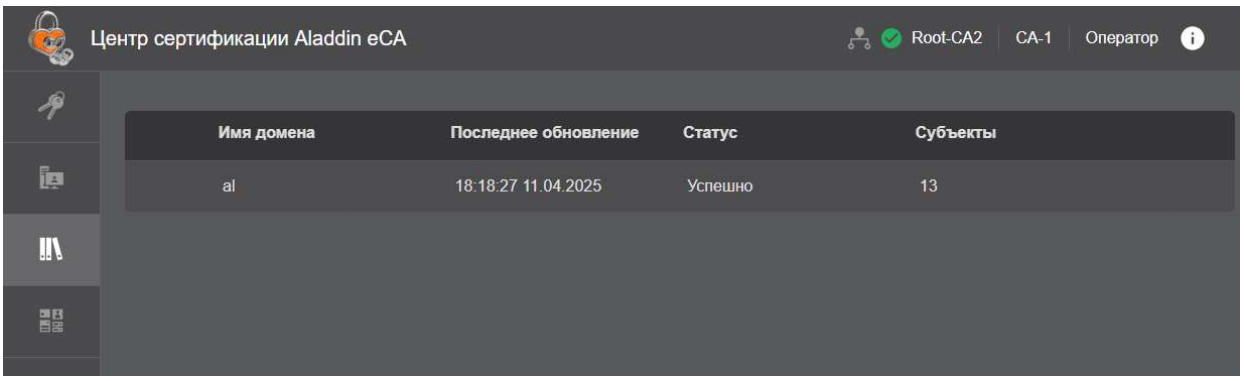


Рисунок 63 – Экран раздела «Ресурсная система»

- Центр сертификации Aladdin Enterprise Certification Authority позволяет загрузить из нескольких ресурсных систем Samba DC, РЕД АДМ, MS AD, FreeIPAALD PRO или Альт Домен:
  - список субъектов (пользователей, компьютеров и сервисов (только для ALD PRO и FreeIPA)), их атрибуты и сертификаты;
  - список и состав групп безопасности.
- В разделе «Ресурсные системы» доступны следующие возможности:
  - переход в карточку ресурсной системы (см. п. 4.5.1);
  - запуск полной синхронизации ресурсной системы (см. п. 4.5.2.3).

4.5.1 Карточка ресурсной системы

Просмотр информации о ресурсной системе возможен посредством окна «Карточка ресурсной системы».

- Переход к «Карточке ресурсной системы» (см. Рисунок 64) осуществляется при нажатии на строку ресурсной системы в разделе «Ресурсные системы» (см. Рисунок 63).

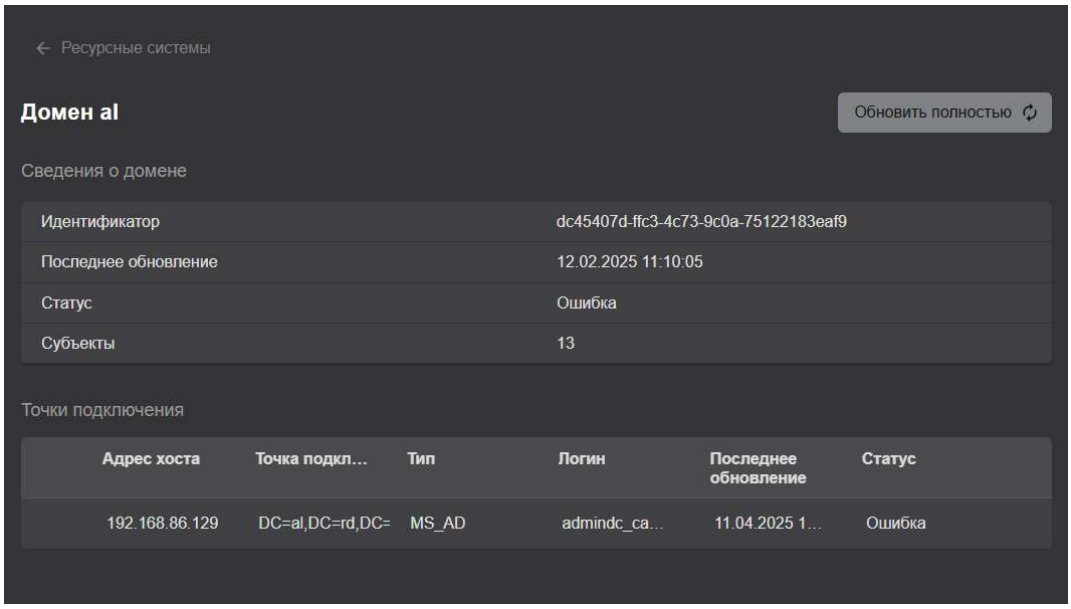


Рисунок 64 – Окно «Ресурсная система»

- Карточка ресурсной системы включает в себя следующую информацию:
  - Заголовок с именем домена в формате «Домен DomainName», где «DomainName» – имя домена;
  - Подраздел «Сведения о домене», включающий в себя таблицу со следующими полями:
    - «Идентификатор». В данном поле указан идентификатор ресурсной системы;
    - «Последнее обновление». В данном поле указаны дата и время последней попытки полной синхронизации ресурсной системы;
    - «Статус». Статус ресурсной системы, который назначается в соответствии с критериями, приведенными в таблице выше (Таблица 7);
    - «Субъекты». В данном поле указано количество субъектов, полученных из ресурсной системы.
  - Подраздел «Точки подключения», содержащий таблицу со списком точек подключения к данной ресурсной системе, которая включает в себя поля:
    - «Адрес хоста» - полное доменное имя или IP-адрес точки подключения ресурсной системы;
    - «Точка подключения» – Base DN, который содержит в своем DN объекты, получаемые из точки подключения; указывается при регистрации точки подключения в формате Distinguished Name;
    - «Тип» – значение из списка: SambaDC, ALD PRO, MS AD, FreeIPA, RED ADM или Альт Домен. Указывается при регистрации точки подключения;
    - «Логин» – логин уполномоченного пользователя контроллера домена, указанный при регистрации точки подключения);
    - «Последнее обновление» – дата последней успешной полной синхронизации точки подключения;
    - «Статус» – статус точки подключения, который назначается в соответствии с критериями, приведенными в таблице ниже;

Таблица 8 – Статусы точки подключения и критерии их присвоения

Статус точки подключения	Критерии присвоения статуса точке подключения

Статус точки подключения	Критерии присвоения статуса точке подключения
Ожидание обработки	Точка подключения ресурсной системы ожидает первой синхронизации (при регистрации ресурсной системы)
Успешно	Точка подключения к ресурсной системе успешно синхронизирована
В процессе	Точка подключения к ресурсной системе находится в процессе синхронизации или удаления
Ошибка	Последняя синхронизация точки подключения завершена с ошибкой

- Доступные действия в карточке ресурсной системы:
  - запуск полной синхронизации ресурсной системы (см. п. 4.5.2);
  - запуск частичной синхронизации точки подключения (см. п. 4.5.2.3).

4.5.2 Синхронизация ресурсных систем

4.5.2.1 Виды синхронизации ресурсных систем

Программный компонент «Центр сертификации Aladdin Enterprise Certification Authority» поддерживает следующие виды синхронизации:

- полная. Синхронизация выполняется из точки подключения к ресурсной системе всех данных – списка субъектов (пользователей, компьютеров и сервисов (только для ALD PRO и FreeIPA), их атрибуты и сертификаты, список и состав групп безопасности).

  При запуске полной синхронизации нескольких точек подключения процесс выполняется поочерёдно. Статус ресурсной системы, обновление которой выполняется, будет отображен как «В процессе».
  По результатам обновления ресурсной системы будут:
  - обновлены дата и время в поле «Последнее обновление» экранной формы «Ресурсная система»;
  - в поле «Статус» экранной формы «Ресурсная система» будет отображён результат синхронизации «Успешно» или «Ошибка»;
  - выведено всплывающее сообщение по результату синхронизации «Успешно» или «Ошибка».
- частичная. При частичной синхронизации выполняется обновление всех данных, полученных при полной синхронизации, за исключением сведений об удалении субъектов, организационных групп и групп безопасности из ресурсной системы.

Субъекты ресурсной системы, которые не могут быть синхронизированы, будут отсутствовать в списке субъектов данной ресурсной системы. Ошибка синхронизации для каждого субъекта ресурсной системы будет зафиксирована в Журнале событий с кодом CAENV090.

4.5.2.2 Режимы обновления ресурсной системы

- Автоматическая частичная и полная синхронизация всех зарегистрированных точек подключения к ресурсным системам выполняется по расписанию в соответствии с заданным CRON-выражением администратором.
- Ручной запуск полной синхронизации ресурсной системы (см. п. 4.5.2.3);
- Ручной запуск частичной синхронизации точки подключения (см. п. 4.5.2.4);
- В результате обновления ресурсной системы состав объектов будет синхронизирован:
  - переименованы существующие объекты;
  - изменены существующие связи (включения в группы и т.д.);

– обновлён список субъектов (добавлены новые группы и объекты, удалены субъекты).

- Для каждого загруженного пользователя и компьютера будет создан субъект и подгружены все поля, относящиеся к SubjectDN и SubjectAltName. Преобразование содержимого записи LDAP в поля базы субъектов ресурсной системы происходит в соответствии с Таблица 9. Если данные поля отсутствуют в описании субъекта в подключенном домене, то в шаблоне при выпуске сертификата соответствующие поля заполняются пустыми значениями.

Таблица 9 – Преобразование данных субъектов ресурсной системы

Атрибут субъекта АЕСА-CA	**Поле в MS AD, SambaDC, RED ADM, Альт Домен**		**Поле в ALD PRO, FreeIPA**		
	Тип субъекта		**Тип субъекта**		
	Пользователь	**Компьютер**	**Пользователь**	**Компьютер**	**Сервис**
Id	ObjectGUID	ObjectGUID	ipaUniqueID	ipaUniqueID	ipaUniqueID
Common name	cn	cn	cn	cn	krbPrincipalName
			uid		
Initials	-	-	initials	-	-
Surname	sn	-	sn	-	-
Given Name	givenName	-	givenName	-	-
Organization	-	-	krbPrincipalName	krbPrincipalName	krbPrincipalName
Name	name	name	-	serverHostName	-
MS GUID	-	ObjectGUID	-	-	-
Domain Qualifier	distigushedName	distigushedName	entrydn	entrydn	entrydn
Description	description	-	-	-	-
DNS Name	-	dNSHostName	-	fqdn	-
Email Address (Mail)	mail	-	mail	-	-
	userPrincipalName	-	krbPrincipalName	krbPrincipalName	krbPrincipalName
RFC 822 NAME	mail	-	mail	-	-
	userPrincipalName	-	krbPrincipalName	krbPrincipalName	krbPrincipalName
MS UPN	userPrincipalName	-	krbPrincipalName	krbPrincipalName	krbPrincipalName
Unique Identifier (UID)	-	-	uid	-	-
Kerberos KPN, Kerberos 5 Principal	-	-	-	krbPrincipalName	-

4.5.2.3 Ручной запуск полной синхронизации ресурсной системы

Запуск полной синхронизации ресурсной системы может осуществляться путем нажатия на кнопку <Обновить> для ресурсной системы в разделе «Ресурсные системы» (см. Рисунок 65) или путем нажатия на кнопку <Обновить полностью> в карточке ресурсной системы (см. Рисунок 65). Ресурсная система, для которой выполняется полная синхронизация, имеет статус «В процессе».

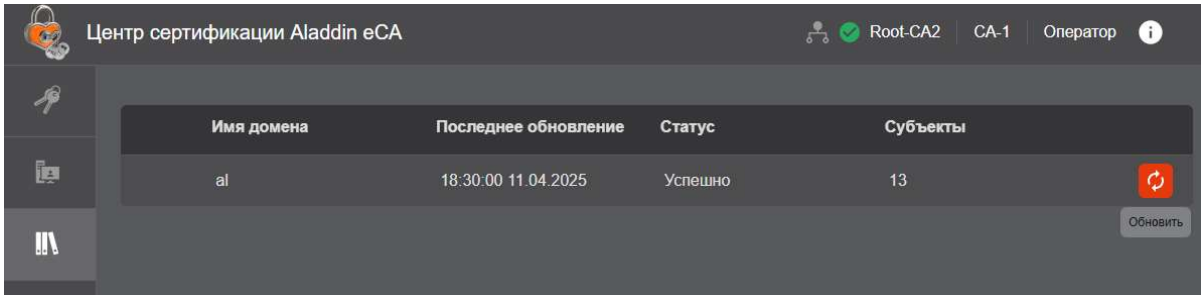


Рисунок 65 – Запуск полной синхронизации ресурсной системы из раздела «Ресурсные системы»

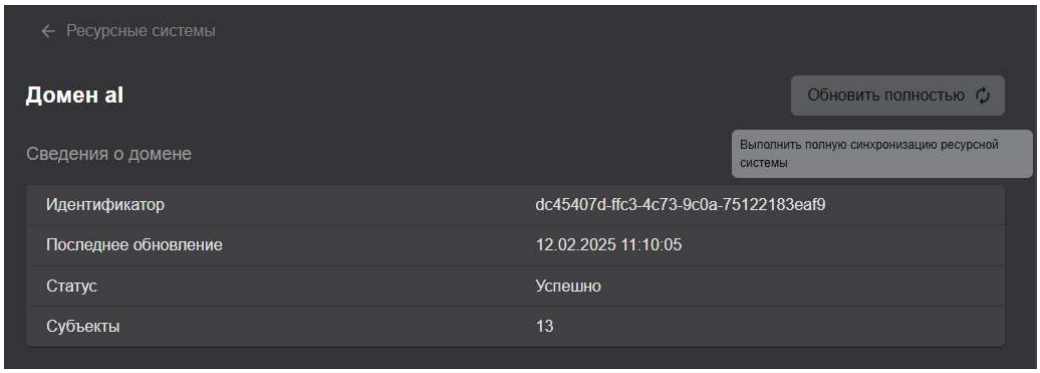


Рисунок 66 – Запуск полной синхронизации ресурсной системы из карточки ресурсной системы

4.5.2.4 Ручной запуск частичной синхронизации точки подключения

Запуск частичной синхронизации точки подключения осуществляться путем нажатия на кнопку <Обновить> для точки подключения в карточке ресурсной системы (см. Рисунок 67).

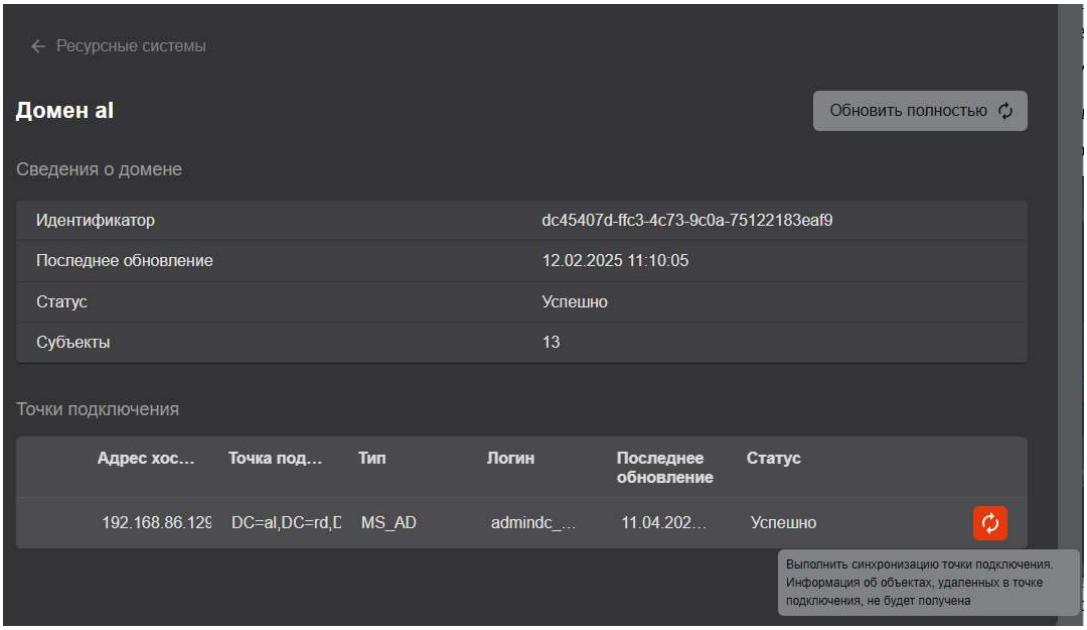


Рисунок 67 – Запуск частичной синхронизации точки подключения

4.6 Раздел «Шаблоны»

Раздел «Шаблоны» позволяет операторам просматривать шаблоны, доступ к которым им предоставлен в соответствии с текущими правилами доступа.

- Переход в раздел «Шаблоны» (см. Рисунок 68) осуществляется через боковое меню, расположенное слева на экране (см. Рисунок 16).

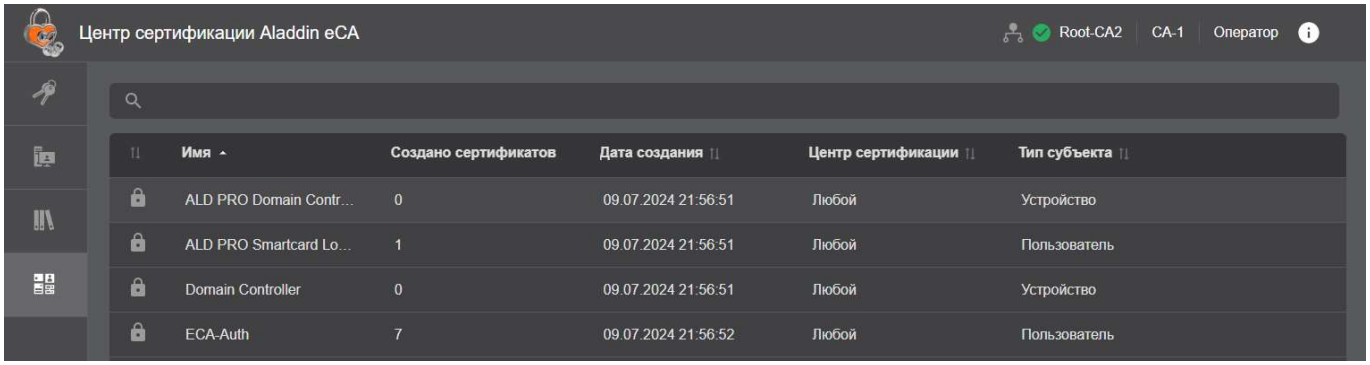


Рисунок 68 – Раздел «Шаблоны»

- На экранной таблице раздела «Шаблоны» отображены следующие колонки:
  - условное обозначение вида шаблона:
    - – предустановленные по умолчанию шаблоны, созданные в момент установки Центра сертификации Aladdin eCA. Данный вид шаблонов не подлежит редактированию;
    - – клонированные шаблоны для редактирования с целью создания нового шаблона с заданными параметрами;
    - – импортированные шаблоны (например, из MS CS).
  - имя – содержит название шаблона;
  - создано сертификатов – количество сертификатов, выпущенных по данному шаблону, владельцами которых являются субъекты, на управление которыми данному оператору назначены полномочия;
  - дата создания – дата создания (клонирования) шаблона;
  - центр сертификации – центр сертификации, в котором будет выполняться выпуск сертификатов по данному шаблону. Если в данном параметре шаблона указано значение «Любой», то выпуск сертификатов по данному шаблону доступен в любом центре сертификации. При этом для выпуска сертификатов будет использоваться активный в данный момент центр сертификации. Для предустановленных шаблонов данный параметр всегда имеет значение «Любой»;

    Внимание! При обновлении ПО с версии 2.1 до версии 2.2 всем шаблонам для параметра «Центр сертификации» устанавливается значение «Любой».

  - тип субъекта – определяет тип субъекта, для которого предназначен данный шаблон (корневой Центр сертификации, подчинённый Центр сертификации, устройство, пользователь).

    Внимание! При обновлении ПО с версии 2.1 до версии 2.2 ранее применяемый для шаблонов параметр «Тип сертификата» преобразовывается в параметр «Тип субъекта» по следующим правилам. Шаблон с типом сертификата «Корневой» принимает значение для типа субъекта «Корневой ЦС». Шаблон с типом сертификата «Подчиненный» принимает значение для типа субъекта «Подчиненный ЦС». Шаблон с типом сертификата «Пользовательский» принимает значение для типа субъекта «Пользователь» (за исключением шаблонов по умолчанию «ВЕБ-Server», «ECA-ВЕБ-Server», «OCSP Signer», «Domain Controller», «ALD PRO Domain Controller», «SCEP Management», для которых устанавливается заначение типа субъекта «Устройство»).

- Действия доступные над всеми видами шаблонов для операторов:
  - просмотр полного списка доступных шаблонов или по результатам поиска;

– просмотр параметров шаблона в его карточке.

- Все шаблоны на экране раздела отображаются в виде таблицы с пагинацией.

4.6.1 Поиск шаблонов

Строка поиска (см. Рисунок 69) предназначена для поиска шаблонов в экранной таблице по содержимому колонки «Имя». Поиск запускается автоматически при вводе искомого значения в строку поиска, результат поиска будет отражён на экранной таблице.

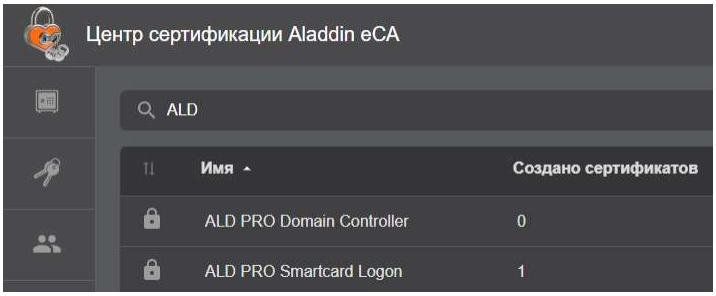


Рисунок 69 – Поисковая строка в разделе «Шаблоны»

- Для сброса результатов поиска и возврату к полному перечню шаблонов в экранной таблице удалите содержимое строки поиска.

4.6.2 Сортировка шаблонов

- Средство сортировки списка шаблонов представлено элементом выбора направления сортировки в заголовках колонок экранной таблицы (см. Рисунок 68) – полями «Имя» (сортировка в алфавитном порядке), «Дата создания» (сортировка в порядке убывания/возрастания), «Тип субъекта» (упорядочивание по типу субъекта в алфавитном порядке), по виду шаблона (предустановленный, импортированный, клонированный), «Центр сертификации» (упорядочивание по названию центра сертификации в алфавитном порядке).
- Сортировка происходит только по одному значению при нажатии на соответствующий заголовок колонки таблицы.
- Активное поле таблицы, по которому выполнена сортировка, обозначено знаком с правой стороны от заголовка таблицы.
- Для сброса сортировки в колонке несколько раз нажмите на заголовке колонки, для которой применена сортировка.

4.6.3 Карточка шаблона

- Для просмотра карточки шаблона необходимо щёлкнуть левой кнопкой мыши на нужном шаблоне на главном экране вкладки «Шаблоны».

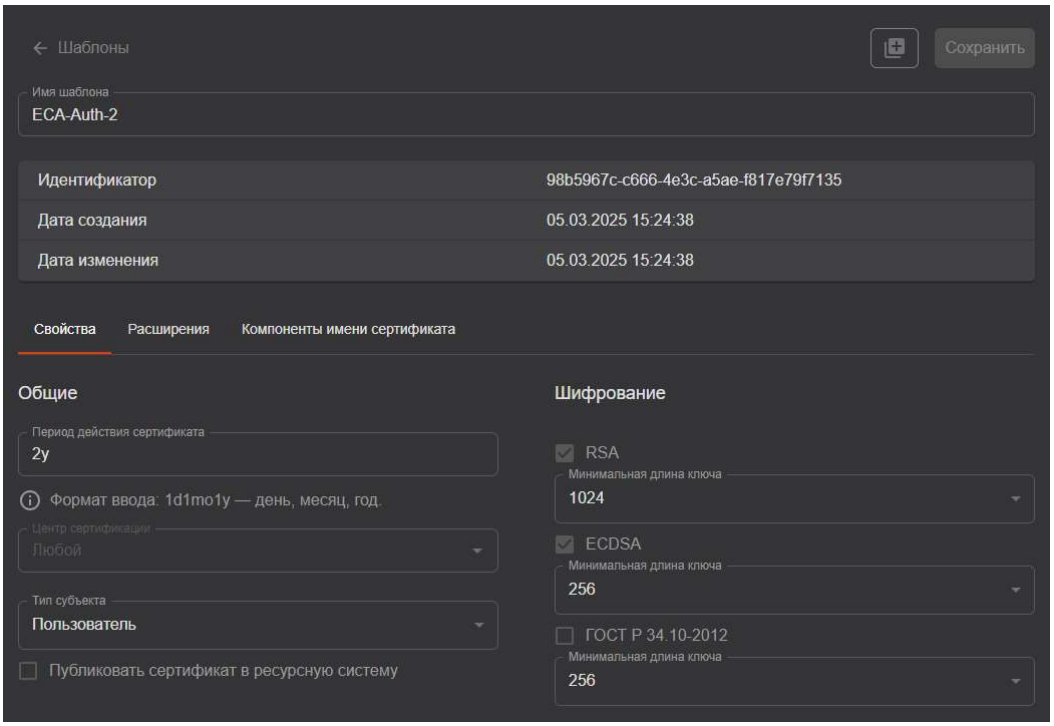


Рисунок 70 – Окно карточки шаблона

- В открывшемся окне оператору доступны:
  - поле «Имя шаблона»;
  - поле «Идентификатор», содержащее постоянный идентификатор шаблона;
  - поле «Дата создания шаблона»;
  - поле «Дата изменения шаблона»;
  - информация о шаблоне, сформированная в виде вкладок «Свойства», «Расширения», «Компоненты имени субъекта».

4.6.3.1 Вкладка шаблона «Свойства»

На вкладке шаблона «Свойства» для просмотра доступны поля (см. Рисунок 71):

- общие:
  - поле «Период действия сертификата». Формат значения в поле: 1d,1m,1y - час, день, месяц, год;
  - чек-бокс «Публиковать сертификат в ресурсную систему».
  - поле «Центр сертификации» - центр сертификации, в котором возможен выпуск сертификатов по данному шаблону;
  - поле «Тип субъекта» - определяет тип субъекта, для которого предназначен данный шаблон (корневой Центр сертификации, подчинённый Центр сертификации, устройство, пользователь).
- шифрование:
  - RSA;
  - ECDSA;
  - ГОСТ Р 34.10-2012.

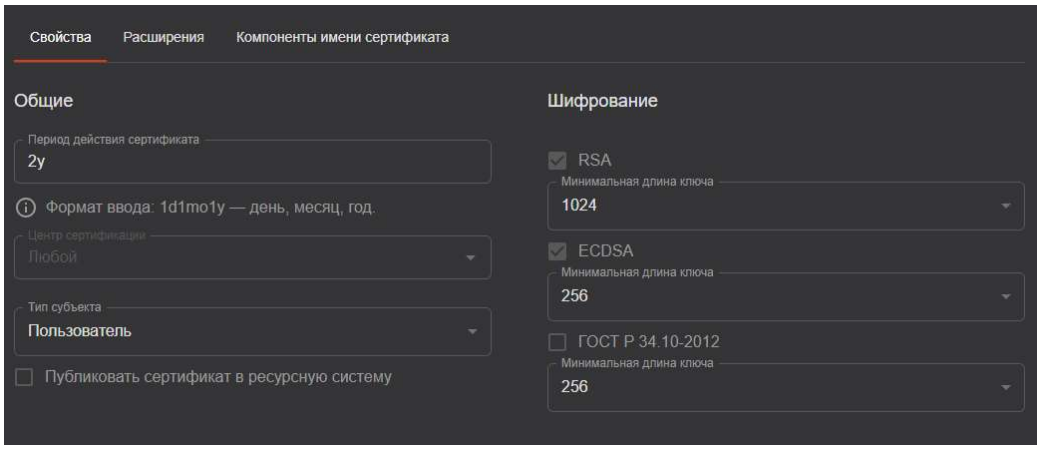


Рисунок 71 – Вкладка «Свойства» шаблона сертификата

4.6.3.2 Вкладка шаблона «Расширения»

На вкладке шаблона «Расширения» для просмотра доступны (см. Рисунок 72):

- поле «Использование ключа»;
- поле «Расширенное использование ключа»;
- OID политики сертификата;
- чек-бокс «Считать это расширение критическим» для списка «Использование ключа»;
- чек-бокс «Считать это расширение критическим» для списка «Расширенное использование ключа».

чек-бокс «Включить SID субъекта в сертификат». При включенной опции в поле сертификата субъекта с OID 1.3.6.1.4.1.311.25.2 будет записан его SID (при наличие данного атрибута у субъекта). SID может быть получен только для субъектов ресурсных систем MS AD, SambaDC, РЕД АДМ и Альт Домен.

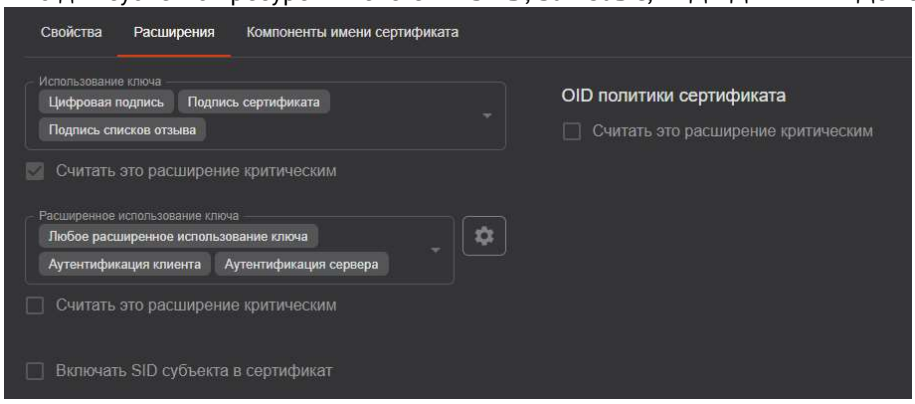


Рисунок 72 – Вкладка «Расширения» шаблона сертификата

4.6.3.3 Вкладка шаблона «Компоненты имени сертификата»

На вкладке шаблона «Компоненты имени сертификата» для просмотра доступны (см. Рисунок 73):

- отличительное имя субъекта;
- альтернативное имя субъекта.

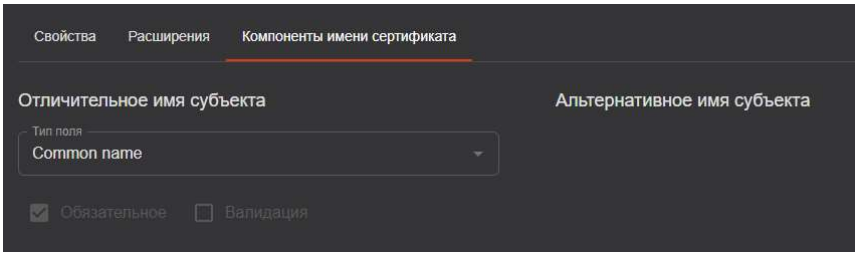


Рисунок 73 – Вкладка «Компоненты имени сертификата» шаблона сертификата

5 СООБЩЕНИЯ ОПЕРАТОРУ

Сообщения оператору представляют собой текст сообщения в модальном окне под полем ввода пароля или пин-кода, которое появляется по центру текущего окна входа в систему и сообщает об ошибке или обязательном действии, которое не выполнено. Список всех возможных сообщения для оператора приведён в Таблица 10.

Таблица 10 – Оповещения программы

№ п/п	Сообщение об ошибке/ уведомление	Описание	Действие оператора
1	Не задано обязательное поле	Сообщение об ошибке при выпуске сертификата по запросу. В загружаемом запросе отсутствует поле, которое является обязательным в выбранном шаблоне	Вернуться на предыдущий шаг и сменить шаблон на подходящий или Пересоздать файл-запрос с учетом выявленных при сверке ошибок и перезагрузить файл-запрос, вернувшись на предыдущие шаги по нажатию кнопки <Назад>
2	Поле не соответствует формату, указанному в шаблоне	Сообщение об ошибке при выпуске сертификата по запросу. Загружаемый запрос содержит поле, которое отсутствует в выбранном шаблоне	
3	Для работы с ключевым носителем должно быть установлено ПО JC-WebClient. Установите необходимое ПО и перезапустите мастер выпуска сертификатов	Сообщение об ошибке при выпуске сертификата на ключевом носителе ПО JC-WebClient предварительно не установлено	Для выпуска сертификата на электронном ключе установить ПО JC-WebClient версии 4.3.2 или 4.3.3
4	Нет доступных устройств. Подключите устройство и перезапустите мастер создания сертификата	Сообщение об ошибке при выпуске сертификата на ключевом носителе Электронный носитель не подключен	Для выпуска сертификата на электронном ключе подсоедините ключевой носитель к USB-порту и запустите мастер создания сертификатов
5	Алгоритм не поддерживается выбранной моделью ключевого носителя	Сообщение об ошибке при выпуске сертификата на ключевом носителе Выбранный для выпуска сертификата алгоритм не поддерживается выбранной моделью ключевого носителя	Для выпуска сертификата на электронном ключе выберите поддерживаемый ключевой носитель, присоедините ключевой носитель к USB-порту и запустите мастер создания сертификатов
6	Синхронизация запущена	Уведомление о успешном запуске обновления ресурсной системы	—

7	Ресурс с указанным идентификатором не найден	Ошибка при запуске обновления ресурсной системы	Выбрать актуальную ресурсную систему
№ п/п	Сообщение об ошибке/ уведомление	Описание	Действие оператора
8	Не удалось найти объект сущности по идентификатору: ${id}	Сообщение об ошибке при выпуске сертификата	Выбрать актуальный и активный субъект
9	[Ошибка публикации] Невозможно опубликовать сертификат в ресурсную систему. Связь между сертификатом и субъектом не обнаружена.	Сообщение об ошибке при выпуске сертификата. Сертификат невозможно опубликовать в ресурсную систему	Обратиться к администратору домена
10	Не должны присутствовать одновременно параметры SubjectId и UserId.	Сообщение об ошибке при выпуске сертификата. Ошибка присутствия одновременно параметров субъекта и юзера	Выбрать только одни параметры
11	Ошибка получения шаблона	Сообщение об ошибке при выпуске сертификата. Ошибка при выборе шаблона	Выбрать актуальный и активный шаблон
12	Время действия активной лицензии истекло	Сообщение об ошибке при приостановке, отзыве и активации сертификата.	Использовать актуальную лицензию
Примечание: в случае возникновения ошибок, связанных с работой JC-WebClient, администратор будет уведомлён сообщением, согласно описанию ошибки в документации JC-WebClient SDK: https://developer.aladdin-rd.ru/archive/jc-webclient/4.0.0/api/addendum/errors.html https://developer.aladdin-rd.ru/archive/jc-webclient/3.1.1/api/addendum.html			

ПРИЛОЖЕНИЕ 1. ОПИСАНИЕ ПОЛЕЙ ПО УМОЛЧАНИЮ ПРЕДУСТАНОВЛЕННЫХ ШАБЛОНОВ СЕРТИФИКАТОВ

Имя шаблона	Идентификатор	Период действия сертификата	Публиковать сертификат в ресурсную систему	Шифрование		Использование ключа		Расширенное использование ключа		Компоненты имени сертификата					
										Отличительное имя субъекта			Альтернативное имя субъекта		
				Алгоритм	Минимальная длина ключа	Значения	Крит.	Значения	Крит.	Поле	Обязат.	Валидац.	Поле	Обязат.	Валидац.
ECA-Auth	8ecba810-7f48-4c4e-b803-99a97146e2ba	2y	-	RSA ECDSA ГОСТ Р 34.10-2012	1024 256 Выключен	- Цифровая подпись - Подтверждение подлинности - Шифрование ключей	+	- Аутентификация клиента - Защита электронной почты	-	Common name	+	+	-		
ECA-User	e97d92b1-2e6e-4ed2-943f-6508113feac6	2y	-	RSA ECDSA ГОСТ Р 34.10-2012	1024 256 256	- Цифровая подпись - Подтверждение подлинности - Шифрование ключей - Шифрование данных	+	- Аутентификация клиента - Защита электронной почты - Вход с MS смарт-картой	-	Common name[14]	+	+	-		
ECA-WEB-Server	076f61dc-5ff4-43cc-8cf9-6b833adf1092	2y	-	RSA	1024	- Цифровая подпись	+	- Аутентификация сервера	-	Common name	+	+	DNS name	+	+

[14] Имя пользователя.

				ECDSA	256	- Шифрование ключей									
				ГОСТ Р 34.10-2012	256										
Domain Controller	bf2dac0a-f05f-49dd-95b4-e50691489b6a	2y	-	RSA	1024	- Цифровая подпись - Подтверждение подлинности - Шифрование ключей	+	- Аутентификация клиента - Центр распространения ключей Kerberos - SSH сервер	-	Common name[15]	+	+	DNS name[16]	+	+
				ECDSA	256								MS GUID[17]	+	+
				ГОСТ Р 34.10-2012	Выключен										
Smartcard Logon	aa03e458-50cd-46b8-82cd-d5612ed3b647	2y	-	RSA	1024	- Цифровая подпись	+	- Аутентификация клиента	-	Common name[18]	+	+	MS UPN[19]	+	+
				ECDSA	256								RFC 822 Name[20]	+	+

[15] Имя контроллера домена.

[16] FQDN – полное доменное имя вашего сервера.

[17] Глобальный уникальный идентификатор контроллера домена, данные должны быть получены из контроллера домена

Для получения значения идентификатора в среде РЕД ОС выполните команду: `samba-tool computer show <hostname> | grep objectGUID`

Для получения значения идентификатора в среде Astra Linux Special Edition выполните команду: `ipa host-show <hostname> --all | grep ipauniqueid`, где `hostname` – короткое имя контроллера домена.

[18] Имя пользователя.

[19] Имя входа пользователя в формате e-mail адреса.

[20] Почтовый адрес пользователя, может совпадать с MS UPN.

				ГОСТ Р 34.10-2012	Выключен	- Подтверждение подлинности - Шифрование ключей - Шифрование данных		- Защита электронной почты - Вход с MS смарт-картой							
WEB-Client	059a38f5-f345-4275-b79f-e7e6cc3cbb68	2y	-	RSA	1024	- Цифровая подпись - Подтверждение подлинности - Шифрование ключей	+	- Аутентификация клиента - Защита электронной почты	-	Common name[21]	+	+	MS UPN[22]	+	+
				ECDSA	256								RFC 822 Name[23]	+	+
				ГОСТ Р 34.10-2012	Выключен										
WEB-Server	08c66f99-218a-46ef-bdee-6a2b3b26a4f1	2y	-	RSA	1024	- Цифровая подпись	+	Аутентификация сервера	-	Common name[24]	+	+	DNS name[25]	+	+
				ECDSA	256										

[21] Имя web-клиента.

[22] Имя входа пользователя в формате e-mail адреса.

[23] Почтовый адрес пользователя, может совпадать с MS UPN.

[24] Имя web-сервера.

[25] FQDN – полное доменное имя вашего сервера.

				ГОСТ Р 34.10-2012	Выключен	- Шифрование ключей									
S/MIME	0c234243-18cf-4c05-b699-537731b2436f	2y	-	RSA ECDSA ГОСТ Р 34.10-2012	1024 256 Выключен	- Цифровая подпись - Подтверждение подлинности - Шифрование ключей - Шифрование данных	+	- Аутентификация клиента - Защита электронной почты - Вход с MS смарт-картой	-	Common name[26]	+	+	RFC 822 Name[27]	+	+
ALD PRO Domain Controller	11ec34a4-d03e-4059-92f0-9c09b08bffea	2y	-	RSA ECDSA ГОСТ Р 34.10-2012	1024 256 Выключен	- Цифровая подпись - Подтверждение подлинности - Шифрование ключей - Шифрование данных	+	- Центр распространения ключей Kerberos - Аутентификация сервера	-	Common name[28] Organization[30]	+ -	+ +	MS UPN[29] Kerberos KPN[31]	+ +	+ +
ALD PRO	18d9bd4e-6f15-423f-	2y	-	RSA	1024	- Цифровая	+	- Аутентификация	-	Common name[32]	+	+	MS UPN[33]	+	+

[26] Имя пользователя.

[27] почтовый адрес пользователя, может совпадать с MS UPN

[28] Имя контроллера домена ALD PRO.

[29] Данные в формате «krbtgt/полное имя домена@полное имя домена».

[30] Организация.

[31] Данные в формате «krbtgt/полное имя домена@полное имя домена».

[32] Имя пользователя ALD PRO.

[33] Имя входа пользователя в формате e-mail адреса.

Smartcard Logon	8137-ac8416ad6874			ECDSA ГОСТ Р 34.10-2012	256 Выключен	подпись - Подтверждение подлинности - Шифрование ключей - Шифрование данных		клиента - Центр распространения ключей Kerberos - Аутентификация сервера		Organization[34]	-	+	RFC 822 Name[35]	+	+
OCSP Signer	aac2e49b-9c8e-4869-80c1-eef526ba75ab	2y	-	RSA ECDSA ГОСТ Р 34.10-2012	1024 256 Выключен	Цифровая подпись	+	OCSP подписант	-	Common name	+	+	-		
Root CA	9129245a-eaad-4ebc-a2a4-8845ac0336fb	7d24y	-	RSA ECDSA ГОСТ Р 34.10-2012	1024 256 256	- Цифровая подпись - Подпись сертификата - Подпись списка отзыва	+	- Любое расширенное использование ключа - Аутентификация клиента - Аутентификация сервера	-	Common name	+	+	RFC 822 Name	-	+
										Unique Identifier (UID)	-	+	DNS name	-	+
										Given name	-	+	MS UPN	-	+
										Initials	-	+	MS GUID	-	+
										Surname	-	+	IP address	-	+
										Organizational unit	-	+	Directory Name	-	+
										Locality	-	+	Uniform resource identifier	-	+
										State or province	-	+	Registered Identifier (OID)	-	+
										Domain component	-	+	Permanent identifier	-	+
										Country	-	+	Xmpp address	-	+
										Postal code	-	+	Service Name	-	+
										Business category	-	+	Subject Identification Method	-	+
										Telephone number	-	+	Kerberos KPN	-	+
										Pseudonym	-	+			
										Postal address	-	+			
										Street	-	+			
										Name	-	+			
										Title	-	+			
										Domain qualifier	-	+			

[34] Организация.

[35] Почтовый адрес пользователя, может совпадать с MS UPN.

										Description	-	+			
										Unstructured address	-	+			
										Unstructured name	-	+			
										Email Address (E)	-	+			
										Serial number	-	+			
										Organization	-	+			
										ИНН	-	+			
										ОГРН	-	+			
										ОГРНИП	-	+			
										СНИЛС	-	+			
										ИНН ЮЛ	-	+			
Sub CA	af3b0355-1798-4c64-98f7-a9c70407db1c	7d24y	-	RSA	1024	- Цифровая подпись - Подпись сертификата - Подпись списка отзыва	+	- Любое расширенное использование ключа - Аутентификация клиента - Аутентификация сервера	-	Common name	+	+	RFC 822 Name	-	+
				ECDSA	256					Unique Identifier (UID)	-	+	DNS name	-	+
				ГОСТ Р 34.10-2012	256					Given name	-	+	MS UPN	-	+
										Initials	-	+	MS GUID	-	+
										Surname	-	+	IP address	-	+
										Organizational unit	-	+	Directory Name	-	+
										Locality	-	+	Uniform resource identifier	-	+
										State or province	-	+	Registered Identifier (OID)	-	+
										Domain component	-	+	Permanent identifier	-	+
										Country	-	+	Xmpp address	-	+
										Postal code	-	+	Service Name	-	+
										Business category	-	+	Subject Identification Method	-	+
										Telephone number	-	+	Kerberos KPN	-	+
										Pseudonym	-	+			
										Postal address	-	+			
										Street	-	+			
										Name	-	+			
										Title	-	+			
										Domain qualifier	-	+			
										Description	-	+			

										Unstructured address	-	+			
										Unstructured name	-	+			
										Email Address (E)	-	+			
										Serial number	-	+			
										Organization	-	+			
										ИНН	-	+			
										ОГРН	-	+			
										ОГРНИП	-	+			
										СНИЛС	-	+			
										ИНН ЮЛ	-	+			
SCEP Management	3e5df3d4-683c-4252-b862-467589c2225b	25y	-	RSA	1024	- Цифровая подпись - Шифрование ключей - Шифрование данных	+	-	-	Common name	+	-	-		
				ECDSA	256										
				ГОСТ Р 34.10-2012	256										

ПРИЛОЖЕНИЕ 2. ПРАВИЛА ВАЛИДАЦИИ ЗНАЧЕНИЙ ПОЛЕЙ ПО УМОЛЧАНИЮ ПРЕДУСТАНОВЛЕННЫХ ШАБЛОНОВ СЕРТИФИКАТОВ

Поле	Правило валидации
Поля SDN	
Country	Допустимые символы: "A"-"Z", "a"-"z". Длина значения должна составлять 2 символа.
Domain qualifier	Допустимые символы: "A"-"Z", "a"-"z", "0"-"9", "'", "(", ")", "+", ",", "-", ".", "/", ":", "=", "?", пробел.
Email Address (E)	Допустимые символы: "A"-"Z", "a"-"z", "А"-"Я", "а"-"я", "0"-"9", ".", "@", "_", "-". Формат значения: "text@text".
Serial number	Допустимые символы: "A"-"Z", "a"-"z", "0"-"9", "'", "(", ")", "+", ",", "-", ".", "/", ":", "=", "?", пробел.
ИНН	Допустимые символы: "0"-"9". Длина значения должна составлять 12 символов.
ОГРН	Допустимые символы: "0"-"9". Длина значения должна составлять 13 символов.
ОГРНИП	Допустимые символы: "0"-"9". Длина значения должна составлять 15 символов.
СНИЛС	Допустимые символы: "0"-"9". Длина значения должна составлять 11 символов.
ИНН ЮЛ	Допустимые символы: "0"-"9". Длина значения должна составлять 10 символов.
Поля SAN	
RFC 822 Name	Допустимые символы: "A"-"Z", "a"-"z", "0"-"9", ".", "@", "_", "-". Формат значения: "text@text". Пример заполнения: “ivanova@example.com”.
DNS Name	Допустимые символы: "A"-"Z", "a"-"z", "0"-"9", "-", ".", "*". Пример значения: “dc1.presale.aeca”.
IP address	Допустимые символы: "A"-"F", "a"-"f", "0"-"9", ".", ":".

Поле	Правило валидации
	Формат значения: IPv4-адрес или IPv6-адрес.
Directory Name	Формат значения: последовательность идентификаторов относительных отличительных имен (RDN) и их значений, отделенных запятой или запятой с пробелом (например, O=organization, OU=Department, L=City, DC=Component, C=RU...). Допускается использование следующих идентификаторов RDN: EMAILADDRESS, CN, UID, SERIALNUMBER, OU, O, L, ST, C, T, SURNAME, STREET, INITIALS, GIVENNAME, DC, UNSTRUCTUREDADDRESS, UNSTRUCTUREDNAME, POSTALCODE, BUSINESSCATEGORY, TELEPHONENUMBER, PSEUDONYM, POSTALADDRESS, NAME, DN, DESCRIPTION. В качестве идентификатора RDN допускается указание OID (формат OID должен соответствовать рекомендации ITU X.660).
Registered Identifier (OID)	Допустимые символы: "0"-"9", ".". Формат значения: OID в соответствии с рекомендацией ITU X.660.
MS UPN, User Principal Name	Допустимые символы: "A"-"Z", "a"-"z", "А"-"Я", "а"-"я", "ё", "Ё", "0"-"9", ".", "@", "_", "-", "/". Формат значения: "text@text".Пример заполнения: “krbtgt/ald.pro@ald.pro”.
MS GUID, Globally Unique Identifier	Допустимые символы: "A"-"F", "a"-"f", "0"-"9". Длина значения должна составлять 32 символа. Пример значения: “92625ee510e248479554779d1f43f751”.
Kerberos KPN, Kerberos 5 Principal Name	Допустимые символы: "A"-"Z", "a"-"z", "А"-"Я", "а"-"я", "ё", "Ё", "0"-"9", ".", "@", "_", "-", "/". Формат значения: "text@text". Пример заполнения: “krbtgt/ald.pro@ald.pro”.
Permanent Identifier	Формат значения: "value/OID", где "value" – любая последовательность символов, а "OID" – OID в соответствии с рекомендацией ITU X.660. Допускается отсутствие значения "text", например, "/1.2.2.3.4.5".
Xmpp address	Допустимые символы: "A"-"Z", "a"-"z", "А"-"Я", "а"-"я", "ё", "Ё", "0"-"9", ".", "@", "_", "-", "/". Формат значения: "text@text".
Subject Identification Method	Формат значения: "OID::text::text", где "OID" – OID в соответствии с рекомендацией ITU X.660, а "text" – любая последовательность символов.

ТЕРМИНЫ И ОПРЕДЕЛЕНИЯ

Администратор безопасности (администратор) – сотрудник (специалист), ответственный за приёмку и ввод в эксплуатацию изделия, а также роль в центре сертификации, которой доступны функции локального администрирования. Физическое лицо (уполномоченный пользователь), имеющее роль «Администратора», должно быть указано в организационно-распорядительных документах организации, эксплуатирующей ПО.

Аутентификация – действия по проверке подлинности идентификатора пользователя. Под аутентификацией понимается ввод пароля или PIN-кода на средстве вычислительной техники в открытом контуре, а также процессы, реализующие проверку этих данных.

Ключевой носитель – это сущность в центре сертификации, соответствующая физическому токену, программному или аппаратному модулю безопасности Hardware Security Module (HSM). С помощью крипто-токена ЦС осуществляет хранение ключей и выполнение криптографических операций.

Оператор – сотрудник (специалист) или система (приложение, сервис) и соответствующая роль в центре сертификации, отвечающая за управление жизненным циклом сертификатов субъектов.

Сертификат – выпущенный центром сертификации цифровой документ в форматах x509v3 или другом поддерживаемом формате, подтверждающий принадлежность владельцу закрытого ключа или каких-либо атрибутов и предназначенный для аутентификации в информационной системе.

Субъект – пользователь информационной системы или устройство (сервер, шлюз, маршрутизатор). Субъекту для строгой аутентификации в информационной системе в центре сертификации выдается сертификат. Синоним – конечная сущность (end entity).

Токен доступа – это уникальная последовательность символов (букв, цифр и символов), основанная на формате JSON. Токен доступа используется для передачи данных для аутентификации в клиент-серверных приложениях. Токены создаются сервером, подписываются секретным ключом и передаются клиенту, который в дальнейшем использует данный токен для подтверждения своей личности.

Токен обновления – это уникальная последовательность символов (букв, цифр и символов), основанная на формате JSON. Токен обновления выдается сервером в результате успешной аутентификации и используется для получения нового токена доступа и обновления токена обновления.

Центр сертификации – комплекс средств, задача которых заключается в обеспечении жизненного цикла сертификатов пользователей и устройств информационной системы, а также в создании инфраструктуры для обеспечения процессов идентификации и строгой аутентификации в информационной системе. Программный компонент «Центр сертификации» является частью Центра сертификатов доступа Aladdin Enterprise Certificate Authority Certified Edition.

Шаблон субъекта – шаблон, на основании которого необходимо создавать субъекты. Шаблон определяет свойства субъекта (subject name, alternative name), свойства сертификата (криптографию, срок действия, назначение, политики и проч.), а также инфраструктурные характеристики (реквизиты для доставки сертификатов, возможности отзыва, хранения и проч.).

ОБОЗНАЧЕНИЯ И СОКРАЩЕНИЯ

ОС	–	Операционная система
ПО	–	Программное обеспечение
СВТ	–	Средство вычислительной техники
СУБД	–	Система управления базами данных
УЦ	–	Удостоверяющий центр
ЦС	–	Центр сертификатов
Aladdin eCA CE	–	Центр сертификатов доступа Aladdin Enterprise Certificate Authority Certified Edition
CRL	–	Certificate Revocation List
AIA	–	Authority Information Access
URL	–	Uniform Resource Locator

ЛИСТ РЕГИСТРАЦИИ ИЗМЕНЕНИЙ

Изм.	Номера листов (страниц)				Всего листов (страниц) в документе	Номер документа	Входящий номер сопроводительного документа и дата	Подпись	Дата
	измененных	замененных	новых	аннулированных					