



Центр сертификатов доступа

# Центр сертификатов доступа Aladdin Enterprise Certificate Authority Certified Edition

Руководство администратора. Часть 2. Функции управления  
Центра сертификации Aladdin Enterprise Certification Authority

Издание	RU.АЛДЕ.03.01.020
Документ	RU.АЛДЕ.03.01.020 32 01-2
Версия	2.2.0
Листов	271
Дата	23.05.2025

## Авторские права, товарные знаки, ограничения

Данный документ, включая подбор и расположение иллюстраций и материалов в нём, является объектом авторских прав и охраняется в соответствии с законодательством Российской Федерации. Обладателем исключительных авторских и имущественных прав является АО «Аладдин Р.Д.».

Использование этих материалов любым способом без письменного разрешения правообладателя запрещено и может повлечь ответственность, предусмотренную законодательством РФ. При перепечатке и использовании данных материалов либо любой их части ссылки на АО «Аладдин Р.Д.» обязательны.

Владельцем зарегистрированных товарных знаков "Аладдин", Aladdin, JaCarta, JMS, JAS, Secret Disk, SecurLogon, "Крипто БД", логотипов и правообладателем исключительных прав на их дизайн и использование, патентов на соответствующие продукты является АО «Аладдин Р.Д.».

Названия прочих технологий, продуктов, компаний, упоминающиеся в данном документе, могут являться товарными знаками своих законных владельцев.

### Ограничение ответственности

Информация, приведённая в данном документе, предназначена исключительно для ознакомления и не является исчерпывающей. Состав продуктов, компонент, их функции, характеристики, версии, доступность и пр. могут быть изменены АО «Аладдин Р.Д.» без предварительного уведомления.

АО «Аладдин Р.Д.» не гарантирует ни отсутствия ошибок в данном документе, ни того, что описанное программное обеспечение (ПО) не содержит дефектов, будет работать в произвольно выбранных условиях и при этом удовлетворять всем требованиям, которые могут быть к нему предъявлены.

АО «Аладдин Р.Д.» не гарантирует работоспособность нелегально полученного программного обеспечения. Нелегальное использование программного обеспечения и документации на него преследуется по закону

Все указанные данные о характеристиках продуктов основаны на международных или российских стандартах и результатах тестирования, полученных в независимых тестовых или сертификационных лабораториях, либо на принятых в компании методиках. В данном документе АО «Аладдин Р.Д.» не предоставляет никаких ни явных, ни подразумеваемых гарантий.

АО «Аладдин Р.Д.» НЕ НЕСЁТ ОТВЕТСТВЕННОСТИ (КАК В СИЛУ ДОГОВОРА, ГРАЖДАНСКОГО ПРАВОНАРУШЕНИЯ, ВКЛЮЧАЯ ХАЛАТНОСТЬ, ТАК И В ЛЮБОЙ ИНОЙ ФОРМЕ) ПЕРЕД ВАМИ ИЛИ ЛЮБОЙ ТРЕТЬЕЙ СТОРОНОЙ ЗА ЛЮБЫЕ ПОТЕРИ ИЛИ УБЫТКИ (ВКЛЮЧАЯ КОСВЕННЫЕ, ФАКТИЧЕСКИЕ ИЛИ ПОБОЧНЫЕ УБЫТКИ), ВКЛЮЧАЯ БЕЗ ОГРАНИЧЕНИЙ ЛЮБЫЕ ПОТЕРИ ИЛИ УБЫТКИ ПРИБЫЛЬНОСТИ БИЗНЕСА, ПОТЕРЮ ДОХОДНОСТИ ИЛИ РЕПУТАЦИИ, УТРАЧЕННУЮ ИЛИ ИСКАЖЁННУЮ ИНФОРМАЦИЮ ИЛИ ДОКУМЕНТАЦИЮ ВСЛЕДСТВИЕ ИСПОЛЬЗОВАНИЯ ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ И/ИЛИ ЛЮБОГО КОМПОНЕНТА ОПИСАННОГО ПРОДУКТА, ДАЖЕ ЕСЛИ АО «Аладдин Р.Д.» БЫЛО ПИСЬМЕННО УВЕДОМЛЕНО О ВОЗМОЖНОСТИ ПОДОБНЫХ УБЫТКОВ.

### Государственное регулирование и экспортный контроль

Описываемый в данном документе продукт (или продукты) может являться или содержать в себе средство криптографической защиты информации (СКЗИ), являющееся предметом экспортного контроля.

Вы соглашаетесь с тем, что продукт не будет поставляться, передаваться или экспортироваться в какую-либо страну, а также использоваться каким-либо противоречащим закону образом.

Вы гарантируете, что будете соблюдать накладываемые на экспорт и резкспорт продукта ограничения.

Сведения, приведённые в данном документе, актуальны на дату его публикации.

© АО «Аладдин Р.Д.», 1995–2025. Все права защищены

## Лицензионное соглашение

Пожалуйста, внимательно прочитайте данное лицензионное соглашение прежде, чем использовать содержимое данного комплекта и/или прежде, чем загружать или устанавливать программное обеспечение.

Все указания по использованию программного обеспечения, предоставляемые Закрытым акционерным обществом "Аладдин Р. Д." (или любым его дочерним предприятием – каждое из них упоминаемое как "компания"), подчиняются и будут подчиняться условиям, оговоренным в данном соглашении. Загружая данное программное обеспечение (как определено далее по тексту) и/или устанавливая данное программное обеспечение на Ваш компьютер и/или используя данное программное обеспечение иным способом, Вы принимаете данное соглашение и соглашаетесь с его условиями.

Если Вы не согласны с данным соглашением, не загружайте и/или не устанавливайте данное программное обеспечение и незамедлительно (не позднее 7 (семи) дней с даты ознакомления с настоящим текстом) верните этот продукт в АО «Аладдин Р.Д.», удалите данное программное обеспечение и все его части со своего компьютера и не используйте его никоим образом.

Настоящее лицензионное соглашение (далее "Соглашение") является договором, заключенным между Вами (физическим или юридическим лицом) – конечным пользователем (далее "Пользователь") – и АО «Аладдин Р.Д.» (далее "Компания") относительно передачи неисключительного права на использование настоящего программного обеспечения, являющегося интеллектуальной собственностью Компании.

### Права и собственность

ДАННОЕ СОГЛАШЕНИЕ НЕ ЯВЛЯЕТСЯ СОГЛАШЕНИЕМ О ПРОДАЖЕ.

Программное обеспечение, включая все переработки, исправления, модификации, дополнения, обновления и/или усовершенствования к нему (далее по всему тексту и любой его части определяемое как Программное обеспечение или ПО), и связанная с ним документация предназначена НЕ ДЛЯ ПРОДАЖИ и является и остаётся исключительной собственностью Компании.

Все права на интеллектуальную собственность (включая, без ограничений, авторские права, коммерческую тайну, товарные знаки, и т.д.), подтвержденные или включенные в приложенные/взаимосвязанные/имеющие отношение к данному руководству, данные, содержащиеся в нём, а также все права на ПО являются и будут являться собственностью исключительно Компании.

Данное соглашение не передаёт Вам права на Программное обеспечение, а лишь предоставляет ограниченное право на использование, которое подлежит отмене согласно условиям данного Соглашения. Ничто в данном Соглашении не подтверждает отказ Компании от прав на интеллектуальную собственность по какому бы то ни было законодательству.

### Лицензия

Компания настоящим предоставляет Вам, а Вы получаете индивидуальное, неисключительное и отзываемое ограниченное право на использование данного ПО только в форме исполняемого кода, как описано в прилагаемой к ПО технической/эксплуатационной документации, и только в соответствии с условиями данного

### Соглашения:

Вы можете установить ПО и использовать его на компьютерах, расположенных в пределах Вашего предприятия, как описано в соответствующей технической/эксплуатационной документации ПО и в настоящем соглашении.

Вы можете добавить/присоединить Программное обеспечение к программам для мобильных устройств с единственной целью, описанной в данном Соглашении. Принимая условия настоящего соглашения, Вы соглашаетесь:

- не использовать, не модифицировать и не выдавать сублицензии на данное Программное обеспечение и любое другое ПО Компании, за исключением явных разрешений в данном Соглашении;
- не модифицировать, не демонтировать, не декомпилировать, не реконструировать, не видоизменять и не расширять данное Программное обеспечение и не пытаться раскрыть (получить) исходные коды данного Программного обеспечения;
- не помещать данное Программное обеспечение на сервер с возможностью доступа к нему третьих лиц через открытую сеть;
- не использовать какие бы то ни было резервные или архивные копии данного Программного обеспечения (или позволять кому-либо ещё использовать такие копии) с любой иной целью, кроме замены его оригинального экземпляра в случае его разрушения или наличия дефектов.

### Требования к использованию

Программное обеспечение должно использоваться и обслуживаться строго в соответствии с описаниями и инструкциями Компании, приведёнными в данном и других документах Компании, в том числе на портале онлайн документации для разработчиков Компании (<http://developer.aladdin-rd.ru/>).

### Использование ПО

Пользователь вправе:

- воспроизводить ПО путём записи его в память электронно-вычислительных машин Пользователя, ограниченное правом инсталляции, копирования и запуска программ для ЭВМ;
- встраивать ПО любым способом в продукты и решения Пользователя;
- распространять ПО любым способом исключительно в составе продуктов и решений Пользователя.

При использовании и распространении ПО Пользователь обязан руководствоваться действующим законодательством Российской Федерации и международным законодательством, учитывая ограничения и дополнительные требования, которые могут возникать в связи с экспортом шифровальных (криптографических) средств с территории Российской Федерации и импортом таких средств в другие страны. В частности, ограничения и дополнительные требования могут возникать при распространении ПО через магазины приложений, содержащие различные приложения для мобильных устройств.

Условия использования, изложенные в настоящем соглашении, действуют в отношении всего содержимого ПО, в частности в отношении:

- дизайна (графики, расположения элементов оформления и т.п.);
- всех иных элементов, в том числе изображений, фонограмм, текстов.

Получаемые Пользователем неисключительные имущественные права не включают права на передачу третьим лицам каких-либо прав на встраивание, воспроизведение, распространение и использование программ для ЭВМ не в составе продуктов и решений Пользователя.

Компания сохраняет за собой все исключительные права на ПО и входящие в него компоненты, включая права на предоставление неисключительных и исключительных прав третьим лицам.

**Пользователь вправе осуществлять использование ПО в пределах, предусмотренных настоящим Соглашением, исключительно на территории Российской Федерации**

## Обслуживание и поддержка

Компания не несёт обязательств по предоставлению поддержки, обслуживания, модификации или выходу новых релизов ПО.

## Ограниченная гарантия

Компания гарантирует, что программное обеспечение с момента приобретения его Вами в течение 12 (двенадцати) месяцев будет функционировать в полном соответствии с его технической/эксплуатационной документацией, при условии, что ПО будет использоваться на компьютерном аппаратном обеспечении и с операционной системой, для которой оно было разработано.

## Отказ от гарантии

Компания не гарантирует, что программное обеспечение будет соответствовать Вашим желаниям и требованиям, или что его работа будет бесперебойной или безошибочной. В объёме, предусмотренном законодательством РФ, компания открыто отказывается от всех гарантий, не оговоренных здесь, от всех иных подразумеваемых гарантий. Ни один из дилеров, дистрибьюторов, продавцов, агентов или сотрудников компании не уполномочен производить модификации, расширения или дополнения к данной гарантии.

Если Вы произвели какие-либо модификации ПО или любой из его частей во время гарантийного периода, ПО подверглось повреждению, неосторожному или неправильному обращению, если Вы нарушили любое из условий настоящего Соглашения, то гарантия, упомянутая выше в разделе 5, будет немедленно прекращена.

Гарантия недействительна, если ПО используется в сочетании с иным аппаратным и/или программным обеспечением, отличным от описанных в технической/эксплуатационной документации, или используется на компьютере с любым установленным нелегальным программным обеспечением.

## Ограничение возмещения

В случае нарушения гарантии, оговоренной выше, Компания может по собственному усмотрению:

- заменить ПО, если это не противоречит вышеупомянутому ограничению гарантии;
- возместить стоимость, выплаченную Вами за ПО.

Гарантийные требования должны быть выставлены в письменном виде в течение гарантийного периода, но не позднее 7 (семи) дней с момента обнаружения дефекта, и содержать в себе подтверждения, удовлетворяющие Компанию. Всё ПО (все экземпляры, имеющиеся у Вас) должно быть возвращено Компании и отправлено возвращающей стороной с оплаченной стоимостью перевозки и, при необходимости, страховки. Экземпляры ПО должны быть отправлены с копией платёжных документов и накладных.

## Исключение косвенных убытков

Стороны признают, что Программное обеспечение не может быть полностью лишено ошибок. Компания не несёт ответственности (как в силу договора, гражданского правонарушения, включая халатность, так и в любой иной форме) перед Вами или любой третьей стороной за любые потери или убытки (включая косвенные, фактические, побочные или потенциальные убытки), включая, без ограничений, любые потери или убытки прибыльности бизнеса, потерю доходности или репутации, утраченную или искажённую информацию или документацию вследствие какого-либо использования данного программного обеспечения и/или любой компоненты данного ПО, даже если компания письменно уведомлена о возможности подобных убытков.

## Ограничение ответственности

В случае если, несмотря на условия данного соглашения, компания признана ответственной за убытки на основании каких-либо дефектов или несоответствия программного обеспечения Вашим ожиданиям, полная ответственность за каждый экземпляр дефектного программного обеспечения не будет превышать суммы, выплаченной вами АО «Аладдин Р.Д.» за это ПО.

## Прекращение действия соглашения

В случае невыполнения Вами условий данного Соглашения действие Вашей лицензии и настоящего Соглашения будет прекращено.

После прекращения действия данного Лицензионного соглашения:

- лицензия, предоставленная Вам данным Соглашением, прекращает своё действие, и Вы после её прекращения не сможете продолжать дальнейшее использование данного Программного обеспечения и других лицензионных Продуктов;
- вы немедленно вернёте в Компанию все экземпляры ПО и все копии такого и/или сотрёте/удалите любую информацию, содержащуюся в электронном виде.

## Применимое законодательство

Данное Соглашение должно быть истолковано и определено в соответствии с законодательством Российской Федерации (за исключением конфликта применения правовых норм), и только российский суд уполномочен осуществлять правосудие в любых конфликтах и спорах, вытекающих из данного Соглашения. Невозможность для любой из сторон воспользоваться любым из прав, предоставленных ей по данному Соглашению, или принять меры против другой стороны в случае любого нарушения своих обязательств по Соглашению не должно рассматриваться как отказ этой стороны от последующего понуждения к признанию своих прав или совершению последующих действий в случае дальнейших нарушений.

Государственное регулирование и экспортный контроль

Вы соглашаетесь с тем, что ПО не будет Вами поставляться, передаваться или экспортироваться в какую-либо страну, а также использоваться каким-либо противоречащим закону и условиям настоящего соглашения образом. ПО является предметом дополнительного экспортного контроля, относящегося к Вам или Вашей юрисдикции. Вы гарантируете, что будете соблюдать накладываемые ограничения на экспорт и резэкспорт ПО.

## Разное

Настоящее Соглашение представляет собой полное соглашение, относящееся к данной лицензии, и может быть изменено только посредством письменного соглашения, подписанного обеими сторонами. Если выполнение какого-либо условия настоящего Соглашения представляется невозможным, такое условие будет скорректировано только в пределах, обеспечивающих возможность выполнения данного условия.

Я ПРОЧИТАЛ И ПОНЯЛ НАСТОЯЩЕЕ ЛИЦЕНЗИОННОЕ СОГЛАШЕНИЕ И СОГЛАСЕН ВЫПОЛНЯТЬ ВСЕ ЕГО УСЛОВИЯ.

Я ПРИНИМАЮ ДАННОЕ ЛИЦЕНЗИОННОЕ СОГЛАШЕНИЕ ЦЕЛИКОМ.

ЕСЛИ Я НЕ ПРИНИМАЮ ЭТО ЛИЦЕНЗИОННОЕ СОГЛАШЕНИЕ ИЛИ ХОТЯ БЫ ОДИН ИЗ ЕГО ПУНКТОВ, ТО ДАННОЕ ЛИЦЕНЗИОННОЕ СОГЛАШЕНИЕ НЕ ВСТУПАЕТ В СИЛУ, И Я ОБЯЗУЮСЬ НЕ УСТАНАВЛИВАТЬ И НЕ ИСПОЛЬЗОВАТЬ ДАННОЕ ПРОГРАММНОЕ ОБЕСПЕЧЕНИЕ



## АННОТАЦИЯ

Настоящий документ представляет собой вторую часть руководства администратора программного средства «Центр сертификатов доступа Центр сертификатов доступа Aladdin Enterprise Certificate Authority Certified Edition»<sup>1</sup>.

Документ предназначен для администраторов программного средства «Центр сертификатов доступа Центр сертификатов доступа Aladdin Enterprise Certificate Authority Certified Edition», регламентирующих права доступа субъектов к объектам и введение ограничений на действия пользователей, а также на изменение условий эксплуатации, состава и конфигурации программных и программно-аппаратных средств.

Руководство определяет порядок настройки и администрирования программного средства «Центр сертификатов доступа Центр сертификатов доступа Aladdin Enterprise Certificate Authority Certified Edition». Перед эксплуатацией программного средства рекомендуется внимательно ознакомиться с настоящим руководством.

Характер изложения материала данного руководства предполагает, что вы знакомы с операционной системой семейства Linux, на которой работает программа и владеете базовыми навыками администрирования для работы в ней.

Настоящий документ ориентирован на администраторов безопасности, ответственных за установку, настройку и сопровождение систем безопасности организации.

Документ рекомендован как для последовательного, так и для выборочного изучения.

---

<sup>1</sup> Далее по документу – программа, программное средство, Aladdin eCA CE

## Содержание

<b>Аннотация</b> .....	5
1 Запуск программного компонента «Центр сертификации Aladdin Enterprise Certification Authority» .....	11
1.1 Проверка состояния сервера в терминале .....	11
1.2 Автоматический запуск программы .....	11
1.3 Запуск программы в терминале .....	11
1.4 Завершение работы программы в терминале .....	13
2 Лицензирование программы .....	14
2.1 Первичное лицензирование .....	14
2.2 Ограничение лицензии .....	17
2.3 Окончание срока действия лицензии .....	18
2.4 Продление срока действия лицензии .....	19
3 Начало работы с программой .....	21
3.1 Инициализация Центра сертификации с генерацией ключа .....	21
3.1.1 Инициализация Корневого Центра сертификации с генерацией ключа .....	21
3.1.2 Инициализация Подчиненного Центра сертификации с генерацией ключа .....	27
3.2 Инициализация Центра сертификации с импортом ключа .....	33
4 Доступ к программе .....	41
4.1 Аутентификация с использованием сертификата, перенесённого на жесткий диск .....	41
4.2 Аутентификация с использованием сертификата на ключевом носителе .....	45
4.2.1 Настройка CBT для двухфакторной аутентификации администратора по сертификату на ключевом носителе .....	45
4.2.1.1 Установка Единого Клиента JaCarta .....	45
4.2.1.2 Настройка браузера Firefox для РЕД ОС 7.3, Альт 8 СП релиз 10, Astra Linux Special Edition 1.7 .....	46
4.2.1.3 Настройка браузера Chromium для РЕД ОС 7.3 и Альт 8 СП релиз 10 .....	46
4.2.1.4 Настройка браузера Chromium для Astra Linux Special Edition 1.7 .....	47
4.2.2 Двухфакторная аутентификация администратора по сертификату на ключевом носителе .....	47
5 Безопасность соединения .....	49
5.1 Настройка доверенного соединения .....	49
6 Технологические составляющие программного компонента «Центр сертификации Aladdin Enterprise Certification Authority» .....	51
6.1 Назначение технологических составляющих .....	51
6.2 Установка и настройка технологических составляющих .....	51
6.3 Удаление технологических составляющих .....	52
6.4 Восстановление доступа к программному компоненту «Центр сертификации Aladdin Enterprise Certification Authority» в случае некорректного удаления технологических составляющих и/или блокировки доступа ...	52
7 Функции управления программным компонентом «Центр сертификации Aladdin Enterprise Certification Authority» .....	53
7.1 Верхняя панель «Центра сертификации Aladdin Enterprise Certification Authority» .....	53
7.2 Боковая панель «Центра сертификации» .....	54
7.3 Раздел «Центр сертификации» .....	57
7.3.1 Вкладка «Свои сертификаты» .....	57
7.3.1.1 Карточка сертификата ЦС .....	60
7.3.1.2 Создание Корневого Центра сертификации с генерацией ключа .....	64
7.3.1.3 Создание Подчиненного Центра сертификации с генерацией ключа .....	71
7.3.1.4 Создание Центра сертификации с импортом внешнего ключа .....	71
7.3.1.5 Скачивание запроса на сертификат для ЦС в состоянии «Запрос» .....	71

7.3.1.6	Импорт сертификата Подчиненного ЦС .....	72
7.3.1.7	Удаление Центра сертификации .....	74
7.3.1.8	Экспорт закрытого ключа Центра сертификации .....	76
7.3.1.9	Импорт закрытого ключа Центра сертификации .....	77
7.3.2	Вкладка «Сертификаты Подчиненных центров» .....	79
7.3.2.1	Карточка сертификата подчинённого ЦС .....	80
7.3.2.2	Подписание запроса на Корневом ЦС .....	81
7.4	Раздел «Сертификаты» .....	84
7.4.1	Выпуск сертификата .....	85
7.4.2	Поиск сертификатов .....	86
7.4.3	Сортировка сертификатов .....	86
7.4.4	Фильтрация сертификатов .....	87
7.4.4.1	Применение фильтров .....	87
7.4.4.2	Сброс применённых фильтров .....	87
7.4.5	Скачивание сертификатов .....	88
7.4.6	Статус сертификатов .....	88
7.4.7	Карточка сертификата .....	90
7.4.8	Экспорт списка выпущенных сертификатов .....	93
7.4.9	Массовые операции с сертификатами .....	94
7.5	Настройка уведомлений об истечении срока действия сертификата .....	97
7.5.1	Настройка параметров конфигурационного файла config.sh .....	97
7.5.2	Настройка шаблонов уведомлений об истечении срока действия сертификата .....	98
7.5.3	Настройка параметров почтового ящика пользователя .....	100
7.5.3.1	Настройка почтовой программы Яндекс.Почта .....	100
7.5.3.2	Настройка почтовой программы MS Exchange .....	102
7.6	Раздел «Учётные записи» .....	103
7.6.1	Создание учётной записи пользователя локального ресурса .....	104
7.6.2	Создание учетной записи для подключенного субъекта .....	105
7.6.3	Изменение статуса учётной записи .....	105
7.6.4	Редактирование учётной записи .....	105
7.6.5	Назначение прав оператору .....	106
7.6.6	Удаление учётной записи .....	106
7.6.7	Выпуск сертификата для учетной записи .....	106
7.7	Раздел «Правила доступа» .....	107
7.7.1	Создание правила доступа .....	108
7.7.2	Редактирование правила доступа .....	113
7.7.3	Удаление правила доступа .....	116
7.8	Раздел «Субъекты» .....	116
7.8.1	Просмотр субъектов ресурсных систем .....	118
7.8.2	Поиск субъектов .....	118
7.8.3	Сортировка субъектов .....	118
7.8.4	Карточка субъекта .....	119
7.8.4.1	Редактирование атрибутов субъекта .....	123
7.8.5	Субъекты локальной ресурсной системы .....	125
7.8.5.1	Создание нового субъекта локальной ресурсной системы .....	126
7.8.6	Субъекты внешнего ресурса .....	127
7.8.7	Создание сертификата для субъекта ресурсной системы .....	129

7.8.8 Создание учётной записи для субъекта.....	130
7.9 Раздел «Ресурсные системы».....	131
7.9.1 Регистрация точки подключения.....	132
7.9.2 Карточка ресурсной системы.....	137
7.9.3 Синхронизация ресурсных систем .....	139
7.9.3.1 Виды синхронизации ресурсных систем.....	139
7.9.3.2 Режимы синхронизации ресурсных систем.....	139
7.9.3.3 Полная синхронизация ресурсной системы в автоматизированном режиме .....	139
7.9.3.4 Частичная синхронизация точки подключения в автоматизированном режиме.....	140
7.9.4 Редактирование параметров точки подключения .....	140
7.9.5 Удаление зарегистрированной ресурсной системой.....	141
7.9.6 Удаление точки подключения к ресурсной системе .....	142
7.10 Раздел «Центры валидации».....	144
7.10.1 Настройка периодичности автоматического обновления CRL .....	144
7.10.2 Автоматизированная публикация списка отозванных сертификатов CRL .....	147
7.10.3 Экспорт актуального списка отозванных сертификатов CRL .....	147
7.10.4 Управление центрами валидации .....	149
7.10.4.1 Регистрация центра валидации.....	149
7.10.4.2 Подписание запроса OCSP-сервера .....	151
7.10.4.3 Просмотр карточки центра валидации.....	154
7.10.4.4 Удаление центра валидации.....	155
7.10.5 Управление точками распространения .....	155
7.10.5.1 Создание пользовательской точки распространения .....	157
7.10.5.2 Редактирование пользовательской точки распространения .....	159
7.10.5.3 Редактирование автоматической точки распространения .....	161
7.10.5.4 Удаление пользовательской точки распространения .....	161
7.10.5.5 Создание кластера точек распространения .....	162
7.10.5.6 Просмотр состава кластера точек распространения.....	164
7.10.5.7 Редактирование кластера точек распространения .....	164
7.10.5.8 Удаление кластера точек распространения .....	166
7.10.6 Управление службами OCSP.....	167
7.10.6.1 Создание пользовательской службы OCSP.....	168
7.10.6.2 Редактирование пользовательской службы OCSP.....	169
7.10.6.3 Редактирование автоматической службы OCSP .....	170
7.10.6.4 Удаление пользовательской службы OCSP.....	170
7.10.6.5 Создание кластера служб OCSP.....	171
7.10.6.6 Просмотр состава кластера служб OCSP .....	173
7.10.6.7 Редактирование кластера служб OCSP.....	174
7.10.6.8 Удаление кластера служб OCSP .....	175
7.10.7 Настройка технического решения «Центра валидации» .....	176
7.10.7.1 Настройка с использованием веб-сервера Nginx.....	176
7.10.7.2 Настройка с использованием веб-сервера Apache.....	180
7.10.8 Получение файлов CRL, Delta CRL и AIA .....	186
7.10.8.1 Получение файлов посредством запуска скрипта из состава программы .....	186
7.10.8.2 Получение файлов посредством использования методов REST API.....	186
7.10.9 Параметры точек распространения в сертификате .....	188
7.11 Раздел «Журнал событий» .....	189

7.11.1 Управление экранной таблицей.....	190
7.11.2 Выборка событий с помощью фильтров.....	190
7.11.3 Сортировка событий.....	191
7.11.4 Поиск событий.....	192
7.11.5 Карточка события.....	192
7.11.6 Копирование события в буфер обмена.....	193
7.11.7 Экспорт журнала событий.....	194
7.11.8 Архивирование и очистка журнала событий.....	204
7.12 Раздел «Шаблоны».....	204
7.12.1 Поиск шаблонов.....	206
7.12.2 Сортировка шаблонов.....	206
7.12.3 Карточка шаблона.....	206
7.12.3.1 Вкладка шаблона «Свойства».....	207
7.12.4 Вкладка шаблона «Расширения».....	208
7.12.4.1 Вкладка шаблона «Компоненты имени сертификата».....	209
7.12.5 Создание нового шаблона.....	209
7.12.5.1 Клонирование шаблона.....	210
7.12.6 Редактирование шаблона.....	210
7.12.6.1 Сохранение внесённых изменений в шаблон.....	215
7.12.7 Удаление шаблона.....	215
7.12.8 Массовая операция (удаления) с шаблонами.....	216
7.12.9 Шаблоны MSCS.....	217
7.12.9.1 Экспорт шаблонов из MSCS.....	217
7.12.9.2 Загрузка шаблона MSCS.....	218
7.12.10 Работа с шаблонами сертификатов.....	219
7.12.10.1 Идентификатор шаблона.....	219
7.12.11 Работа с идентификаторами расширенного использования ключа.....	220
7.12.11.1 Создание пользовательского идентификатора расширенного использования ключа.....	221
7.12.11.2 Удаление пользовательского идентификатора расширенного использования ключа.....	222
7.13 Раздел «Настройки».....	222
7.13.1 Установка сертификата веб-сервера.....	224
7.13.2 Разрешённые издатели.....	225
7.13.3 Добавление Syslog-сервера.....	225
7.13.4 Редактирование параметров Syslog-сервера.....	226
7.13.5 Удаление Syslog-сервера.....	227
8 Поиск и устранение неисправностей.....	228
Приложение 1. Создание сертификата для субъекта.....	232
1.1 Способы создания сертификатов.....	232
1.2 Параметры криптографии сертификатов учётных записей пользователей и Центров сертификации.....	233
1.3 Публикация сертификата в ресурсную систему.....	234
1.4 Создание сертификата с закрытым ключом PKCS#12.....	235
1.5 Создание сертификата субъекта по запросу.....	239
1.5.1 Создание сертификата субъекта по запросу в разделе «Сертификаты».....	239
1.5.2 Создание сертификата субъекта по запросу в разделе «Субъекты».....	249
1.6 Создание сертификата субъекта на ключевом носителе.....	253
1.6.1 Сообщения об ошибках при создании сертификата на ключевом носителе.....	256
Приложение 2. Описание полей предустановленных шаблонов сертификатов.....	258

Приложение 4. Правила валидации значений полей по умолчанию предустановленных шаблонов сертификатов .....	263
Приложение 5. Описание предустановленных идентификаторов расширенного использования ключа.....	265
Обозначения и сокращения.....	268
Термины и определения .....	269
Лист регистрации изменений.....	271

1 ЗАПУСК ПРОГРАММЫ

1.1 Проверка состояния сервера в терминале

Для проверки состояния сервера, на котором развёрнут программный компонент «Центр сертификации Aladdin Enterprise Certification Authority»<sup>2</sup> в терминале выполните команду с правами суперпользователя (root или sudo):

```

sudo systemctl status aeca-ca.service

```

Возможные варианты ответа: active (running) – сервер запущен, с перечислением модулей и их статуса (ожидание запуска, успешно запущен, не удалось запустить сервис) и inactive (dead) – сервер остановлен, с выводом информации о последних запущенных модулях.

1.2 Автоматический запуск программы

Программный компонент «Центр сертификации Aladdin Enterprise Certification Authority» запускается автоматически с запуском операционной системы, то есть в начале сеанса уполномоченного пользователя CBT, на котором развёрнут центр сертификации, обеспечивая автоматический запуск программного компонента.

1.3 Запуск программы в терминале

Для запуска программного компонента «Центр сертификации Aladdin Enterprise Certification Authority» в терминале выполните команду с правами суперпользователя (root или sudo):

```

sudo systemctl start aeca-ca.service

```

Модули программного компонента<sup>3</sup>, запускаемые поочерёдно, при выполнении команды приведены в таблице ниже (Таблица 1).

Таблица 1 – Модули программного компонента «Центр сертификации Aladdin eCA»

Порядок запуска	Исполняемый файл	Наименование	Назначение
1	logs-service.jar	Модуль журнала событий	Обеспечивает фиксацию событий в журнале и получение событий из журнала, просмотра и поиск записей журнала событий, экспорт и архивацию записей журнала событий
2	storage-service.jar	Модуль хранения данных	Обеспечивает хранение и управление файлами сертификатов
3	templates-service.jar	Модуль шаблонов	Обеспечивает просмотр, создание, редактирование и удаление шаблонов сертификатов
4	subjects-service.jar	Модуль работы с субъектами	Обеспечивает взаимодействие с группами безопасности и субъектами
5	license-service.jar	Модуль лицензирования	Обеспечивает управление лицензиями программы
6	export-service.jar	Модуль экспорта данных	Обеспечивает управление экспортом файлов программы

<sup>2</sup> Далее по документу – программный компонент, Центр сертификации Aladdin Enterprise Certification Authority, Центр сертификации Aladdin eCA

<sup>3</sup> Далее по документу - сервис

Порядок запуска	Исполняемый файл	Наименование	Назначение
7	security-service.jar	Модуль безопасности	Предназначен для идентификации и аутентификации пользователей программы, управления учетными записями пользователей программы, предоставления информации о пользователях программы.
8	ldap-service.jar	Модуль работы с LDAP	Обеспечивает взаимодействие с ресурсными системами и обеспечивает публикацию сертификатов в ресурсную систему, а также получение данных из ресурсной системы
9	event-delivery-service.jar	Модуль оповещения пользователей	Предназначен для оповещения посредством рассылки уведомлений по адресам электронной почты владельцев сертификатов
10	certificate-authority-service.jar	Модуль сертификатов	Обеспечивает создание сертификата, подпись сертификата (включая цепочки сертификатов), генерацию CRL, валидацию сертификата, взаимодействие уполномоченного пользователя с контейнерами и точками распространения.
11	publisher-service.jar	Модуль публикации	Обеспечивает обслуживание точек публикации CRL, Delta CRL и AIA
12	validation-authority-service.jar	Модуль валидации	Обеспечивает взаимодействия с точками распространения, а также для валидации сертификатов
13	external-integration-service.jar	Модуль внешних интеграций	Предназначен для предоставления пользователям или внешним системам доступа к программным интерфейсам (публичный API) программы, реализуемым другими модулями.
14	settings-service.jar	Модуль настроек	Обеспечивает управление жизненным циклом программы, её состоянием и параметрами (данные о продукте, конфигурация серверного сертификата SSL, разрешенные издатели сертификатов)
15	routes-service.jar	Модуль управления	Предоставляет пользовательские веб-интерфейсы, обеспечивает разграничение доступа на основе ролей пользователей
16	api-gateway-service.jar	Модуль проксирования	Предназначен для перенаправления поступающих в программу запросов в нужный сервис (на основании данных, указанных в URL запроса), а также для перенаправления запросов к модулю безопасности с целью аутентификации пользователя
17	x509-provider-service.jar	Модуль аутентификации по сертификату	Предназначен для аутентификации пользователей в программе по сертификату доступа.



## 1.4 Завершение работы программы в терминале

Для завершения работы программного компонента «Центр сертификации Aladdin Enterprise Certification Authority» в терминале ОС выполните команду с правами суперпользователя (root или sudo):

```
sudo systemctl stop aeca-ca.service
```

Программное средство при остановке отключает от веб-сервера свою конфигурацию. В результате отключения от веб-сервера конфигурации закрываются порты, используемые для доступа к программному средству (определяются параметрами «http\_port» и «http\_port» конфигурационного файла /opt/aecaCa/scripts/config.sh), если данные порты не используются иными программами.

## 2 ЛИЦЕНЗИРОВАНИЕ ПРОГРАММЫ

### 2.1 Первичное лицензирование

После установки программного компонента «Центр сертификации Aladdin Enterprise Certification Authority» в появившемся окне инициализации необходимо выбрать файл лицензии с расширением **.lic** (см. Рисунок 1).

Один экземпляр программной лицензии предназначен для работы одного экземпляра программного компонента «Центр сертификации Aladdin Enterprise Certification Authority».

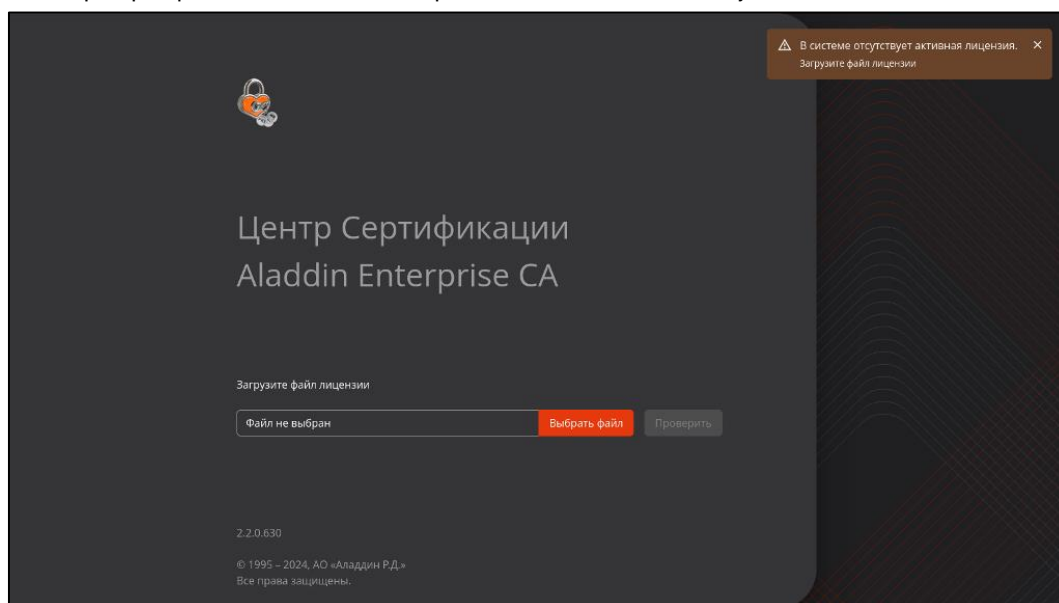


Рисунок 1 – Окно инициализации Центра сертификации. Шаг 1 – выбор лицензии

- Далее нажмите ставшую активной кнопку <Проверить> для проверки валидности файла лицензии (см. Рисунок 2).

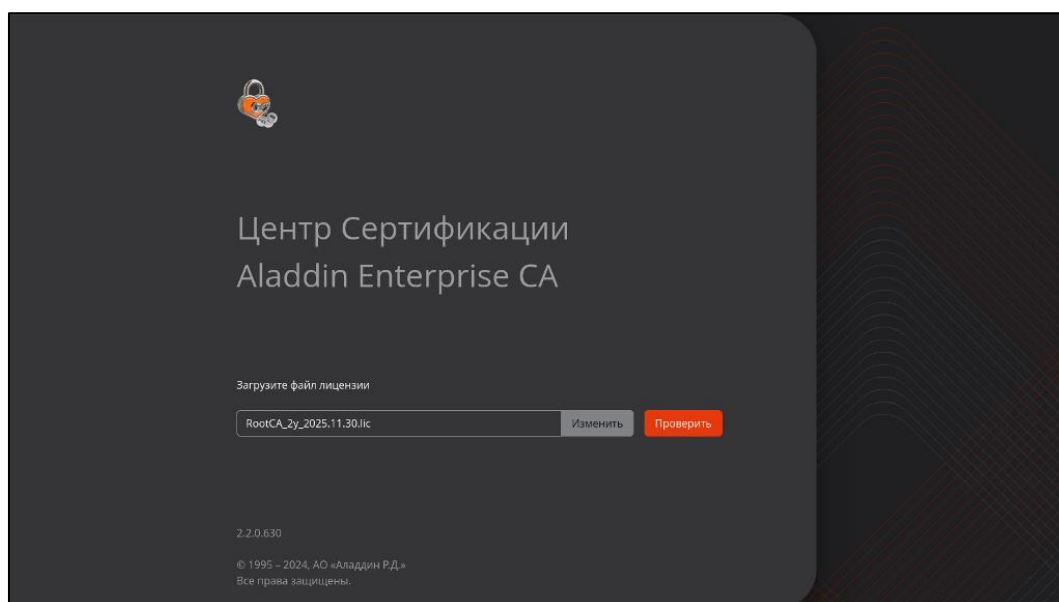


Рисунок 2 – Окно инициализации Центра сертификации. Шаг 1 – проверка лицензии

- При загрузке лицензии продукта проверяется подпись, срок и ключевые поля:

- при несовпадении ключевых полей – `productId` и `id` администратор будет уведомлён сообщением на экране «Данная лицензия не предназначена для продукта Aladdin Enterprise CA» (см. Рисунок 3);

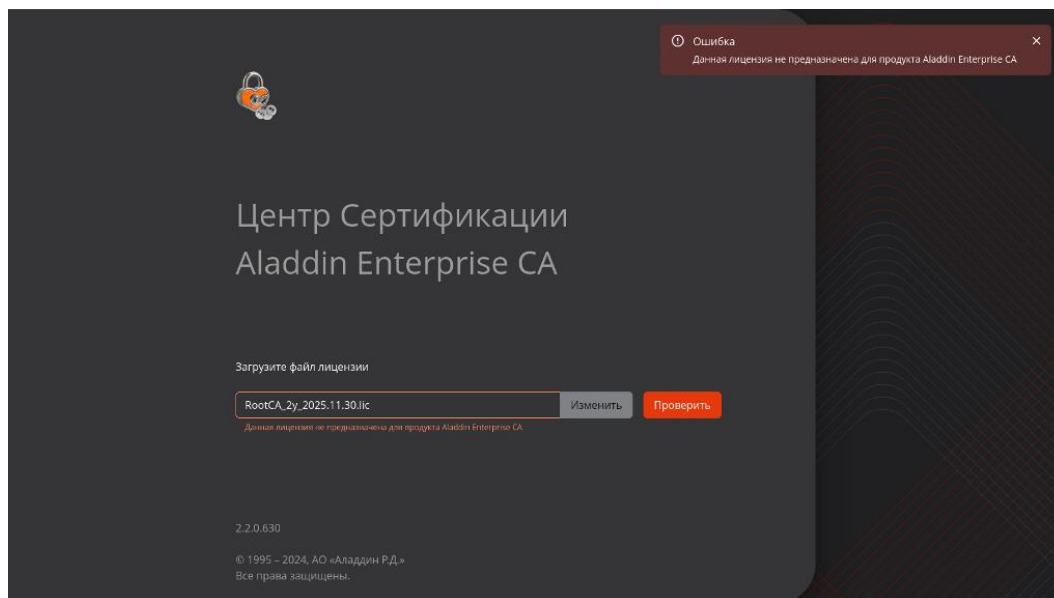


Рисунок 3 - Окно инициализации Центра сертификации. Проверка лицензии. Несовпадение полей

- при несовпадении подписи лицензии администратор будет уведомлён сообщением на экране «Подпись неверна» (см. Рисунок 4);

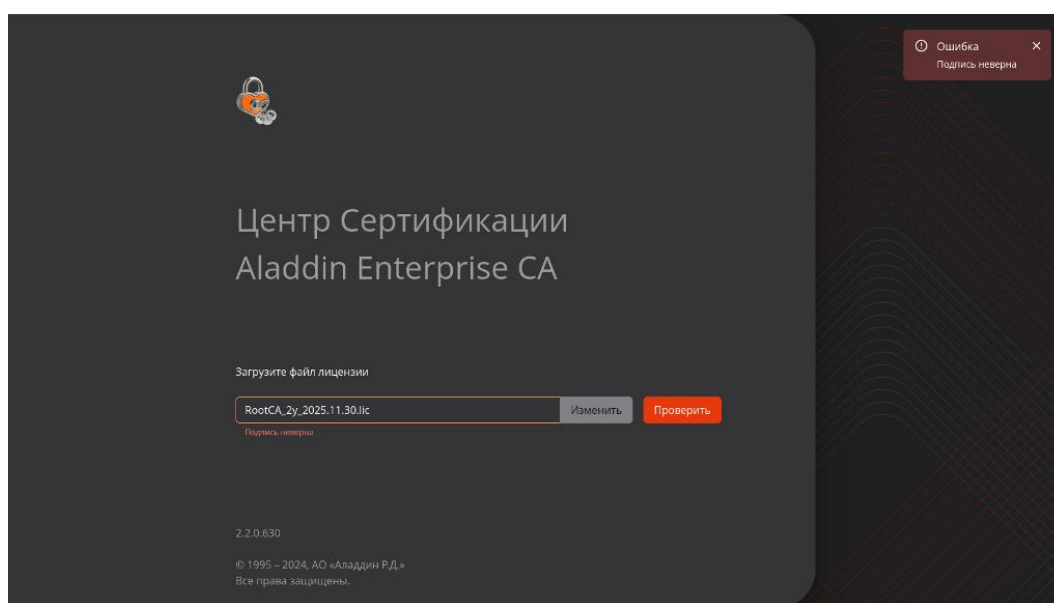


Рисунок 4 – Окно инициализации Центра сертификации. Лицензия предназначена для другого продукта

- при истечении срока действия лицензии администратор будет уведомлён сообщением на экране «Срок лицензии истёк» (см. Рисунок 5);

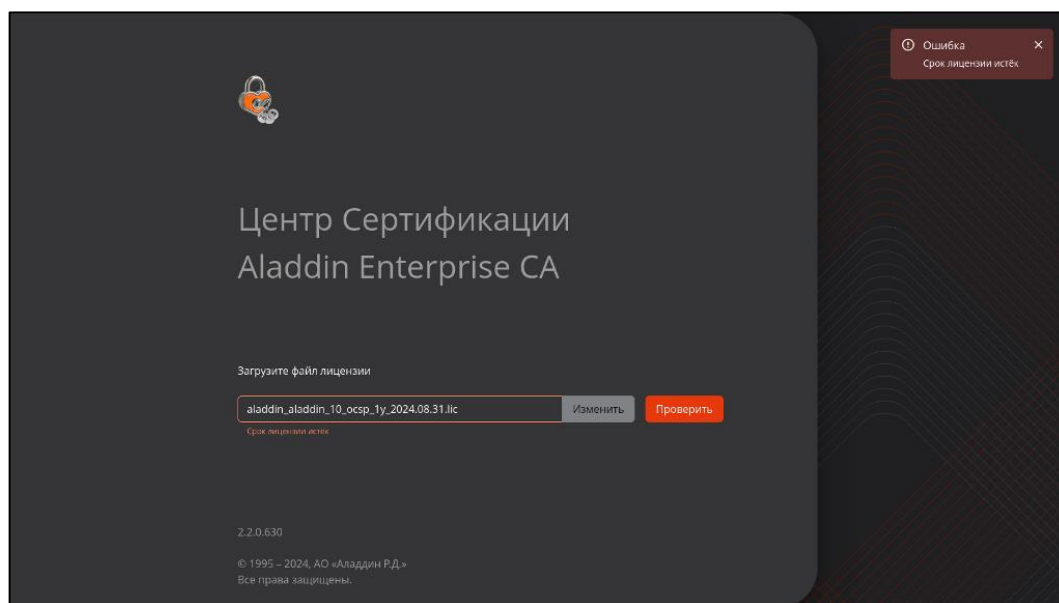


Рисунок 5 - Окно инициализации Центра сертификации. Срок лицензии истёк

- в случае ранее установленной лицензии на текущем рабочем месте и новой установке ПО Aladdin eCA администратор будет уведомлён сообщением на экране «В системе уже присутствует лицензия»;
- при невозможности чтения содержимого файла лицензии администратор будет уведомлён сообщением на экране «Некорректный файл».

Если лицензия продукта «Центр сертификации» Aladdin eCA успешно проходит проверку на валидность, то активируются кнопки <Сгенерировать ключ и создать центр сертификации> и <Импортировать ключ и создать центр сертификации> (см. Рисунок 6). Также на экране будут отображены параметры лицензии:

- перечень возможных типов центров сертификации в поле «Типы центров сертификации»;
- перечень доступных для выбора имён центра сертификации в поле «CN центра сертификации»
- перечень имен корневых центров сертификации в поле «CN корневого центра сертификации». Данное поле не отображается, если лицензия позволяет создать только корневой ЦС;
- максимальное количество субъектов с действующими сертификатами в поле «Субъекты с действующими сертификатами»;
- срок действия лицензии в поле «Действует до».

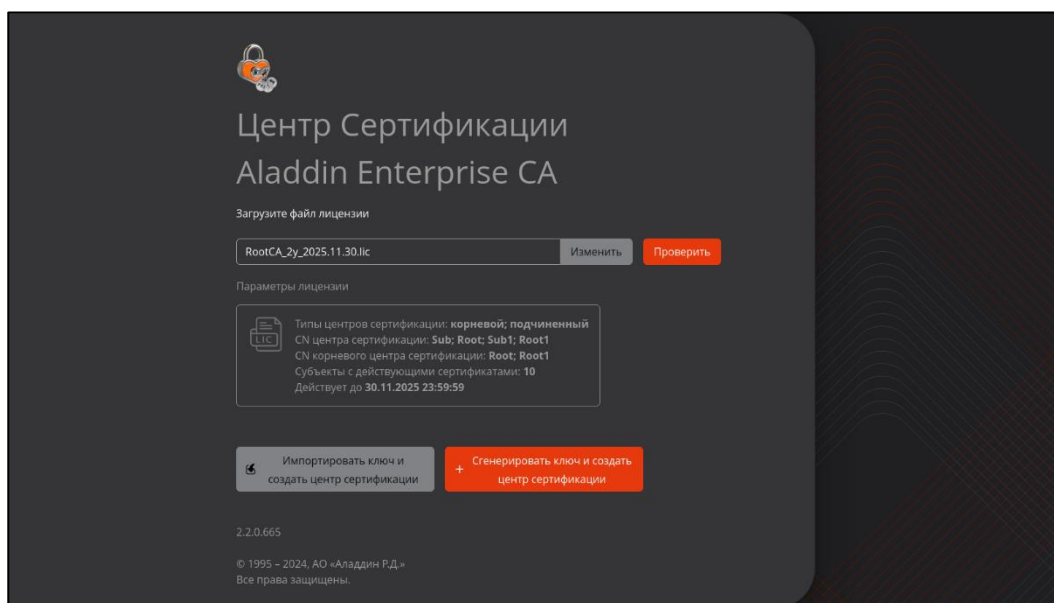


Рисунок 6 – Окно инициализации. Проверка на валидность файла лицензии прошла успешно

- Далее нажмите кнопку <Сгенерировать ключ и создать центр сертификации> для перехода к инициализации Центра сертификации с генерацией ключа (см. раздел 3.1).

Либо нажмите кнопку <Импортировать ключ и создать центр сертификации> для перехода к инициализации Центра сертификации с импортом ключа из контейнера PKCS#12 (см. раздел 3.2).

## 2.2 Ограничение лицензии

- Лицензию необходимо импортировать для каждого разворачиваемого Центра сертификации.
- Лицензия на право использования программы ограничивает типы центров сертификации (корневой или подчиненный), которые могут быть созданы.
- Лицензия на право использования программы ограничивает имена центров сертификации, которые могут быть указаны при создании центра сертификации определенного типа.
- Лицензия на право использования программы ограничивает максимальное количество субъектов, которые могут быть владельцами действующих сертификатов.
- Лицензия на право использования программы ограничена сроком действия.
- Сведения об установленной лицензии доступны для просмотра в окне «О программе» (см. Рисунок 7, Рисунок 8, Рисунок 9), вызываемом на верхней панели экранной формы Центра сертификации и содержащим следующие данные:
  - домен лицензии в поле «Лицензия»;
  - дата и время окончания срока действия лицензии в поле «Действует до»;
  - доступные для создания типы центров сертификации в поле «Типы центров сертификации».
 Если по лицензии доступно создание только одного типа ЦС, то поле называется «Тип центра сертификации» и имеет значение «корневой» или «подчиненный» в зависимости от параметров лицензии;
  - перечень доступных для выбора имен центра сертификации в поле «CN центра сертификации»;
  - перечень имен корневых центров сертификации в поле «CN корневого центра сертификации».
 Данное поле не отображается, если лицензия позволяет создание только корневого ЦС<sup>4</sup>.

<sup>4</sup> В данном случае перечень имен ЦС и имен корневых ЦС будет совпадать.

- текущее и предельное количество субъектов с действующими сертификатами в поле «Количество субъектов».

Aladdin Enterprise CA 2.2.0.630

Центр сертификации

+7 (495) 223-00-01, +7 (495) 988-46-40

www.aladdin-rd.ru

Лицензия

aladdin

Действует до: 31.08.2035 23:59:59

Типы центров сертификации: **корневой**

CN центра сертификации: CA\_INFORM

Количество субъектов: 39 / 1000

Импортировать лицензию

Данная программа защищена законом об авторских правах и международными соглашениями. Незаконное воспроизведение и/или распространение данной программы и/или любой её части влечёт гражданскую, административную и уголовную ответственность в соответствии с законодательством Российской Федерации.

© 1995 – 2024, АО «Аладдин Р.Д.».

Все права защищены.

Рисунок 7 – Окно «О программе» для лицензии на Корневой ЦС

Aladdin Enterprise CA 2.2.0.630

Центр сертификации

+7 (495) 223-00-01, +7 (495) 988-46-40

www.aladdin-rd.ru

Лицензия

aladdin

Действует до: 31.08.2025 23:59:59

Типы центров сертификации: **подчиненный**

CN центра сертификации: SUB\_CA\_INFORM

CN корневого центра сертификации: aladdin

Количество субъектов: 111 / 1000

Импортировать лицензию

Данная программа защищена законом об авторских правах и международными соглашениями. Незаконное воспроизведение и/или распространение данной программы и/или любой её части влечёт гражданскую, административную и уголовную ответственность в соответствии с законодательством Российской Федерации.

© 1995 – 2024, АО «Аладдин Р.Д.».

Все права защищены.

Рисунок 8 – Окно «О программе» для лицензии на Подчинённый ЦС

Aladdin Enterprise CA 2.2.0.665

Центр сертификации

+7 (495) 223-00-01, +7 (495) 988-46-40

www.aladdin-rd.ru

Лицензия

Не определено

Действует до: 07.01.2025 23:59:59

Типы центров сертификации: **подчиненный; корневой**

CN центра сертификации: Sub; Root; Sub1; Root1

CN корневого центра сертификации: Root; Root1

Количество субъектов: 1 / 10

Импортировать лицензию

Данная программа защищена законом об авторских правах и международными соглашениями. Незаконное воспроизведение и/или распространение данной программы и/или любой её части влечёт гражданскую, административную и уголовную ответственность в соответствии с законодательством Российской Федерации.

© 1995 – 2024, АО «Аладдин Р.Д.».

Все права защищены.

Рисунок 9 – Окно «О программе» для лицензии на оба типа ЦС

2.3 Окончание срока действия лицензии

- После истечения срока действия лицензии функция выпуска сертификатов субъектов станет недоступна. Кнопки <Создать сертификат> в разделах «Центр сертификации» и «Сертификаты», кнопка <Подписать запрос> в разделе «Центр сертификации» будут заблокированы. При наведении на заблокированные кнопки будет показано сообщение о причинах блокировки «Срок действия лицензии истёк» (см. Рисунок 10).

Центр сертификации Aladdin eCA

SUB\_CA\_INFORM NOT GOST INITIAL\_ADMIN\_100

Свои сертификаты Сертификаты подчиненных центров

Импортировать сертификат Добавить сертификат

Т...	Отобража...	Владелец	Действите...	Алгоритм кл...	Длина ключа	Состояние	Кол-во с...	Срок действия лицензии истек
▼	NOT GOST	SUB_CA_INFO...	08.08.2034 1...	RSA	2048	Активирован	42643	
▼	Testp1234	SUB_CA_INFO...	12.08.2034 1...	RSA	2048	Не активирован	8	
▼	TEST111	SUB_CA_INFO...	02.11.2034 1...	RSA	2048	Не активирован	0	
▼	test 3	SUB_CA_INFO...	07.08.2034 1...	RSA	2048	Не активирован	8	
▼	Testp123	SUB_CA_INFO...	12.08.2034 1...	RSA	2048	Не активирован	1	
▼	OCSP 1	SUB_CA_INFO...	11.10.2034 2...	RSA	2048	Не активирован	12	
	qweqweqwe	SUB_CA_INFO...	-	RSA	2048	Запрос	0	
	Test	SUB_CA_INFO...	-	RSA	2048	Запрос	0	
▼	hfh	SUB_CA_INFO...	14.08.2034 1...	GOST_R_34_1...	256	Не активирован	52	
▼	Центр серти...	SUB_CA_INFO...	11.10.2034 2...	RSA	2048	Не активирован	12	

Строк на странице 10 1-10 из 30

Рисунок 10 – Заблокированная кнопка <Создать сертификат> по истечении срока действия лицензии

## 2.4 Продление срока действия лицензии

- Для доступа к полному функционалу компонента «Центр сертификации Aladdin eCA» необходимо загрузить действительную лицензию, нажав кнопку <Импортировать лицензию> в окне «О программе» (см. Рисунок 7, Рисунок 8), расположенном на верхней панели экранной формы «Центра сертификации».
- В открывшемся окне импорта лицензии (см. Рисунок 11) будет доступна информация о текущей установленной лицензии.
- Выберите файл лицензии в формате `.lic`.

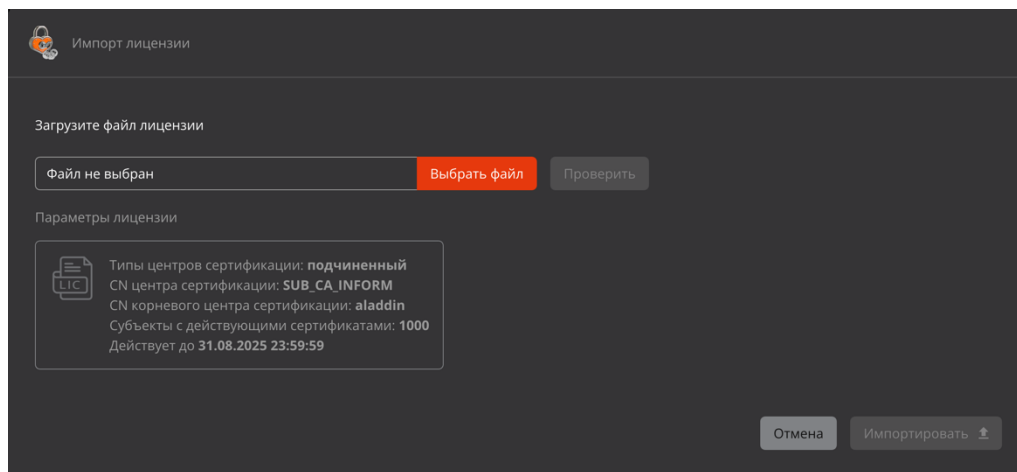


Рисунок 11 – Окно импорта лицензии

- После выбора файла лицензии нажмите ставшую активной кнопку <Проверить>. Происходит проверка цифровой подписи файла лицензии, срока действия лицензии и ключевых полей файла лицензии «productId» и «id».
- По результатам успешной проверки на валидность в текущем окне будут показаны параметры загружаемой лицензии:
  - перечень возможных типов центров сертификации в поле «Типы центров сертификации»;
  - перечень доступных для выбора имён центра сертификации в поле «CN центра сертификации»
  - перечень имен корневых центров сертификации в поле «CN корневого центра сертификации». Данное поле не отображается, если лицензия позволяет создать только корневой ЦС;
  - максимальное количество субъектов с действующими сертификатами в поле «Субъекты с действующими сертификатами»;
  - срок действия лицензии в поле «Действует до».

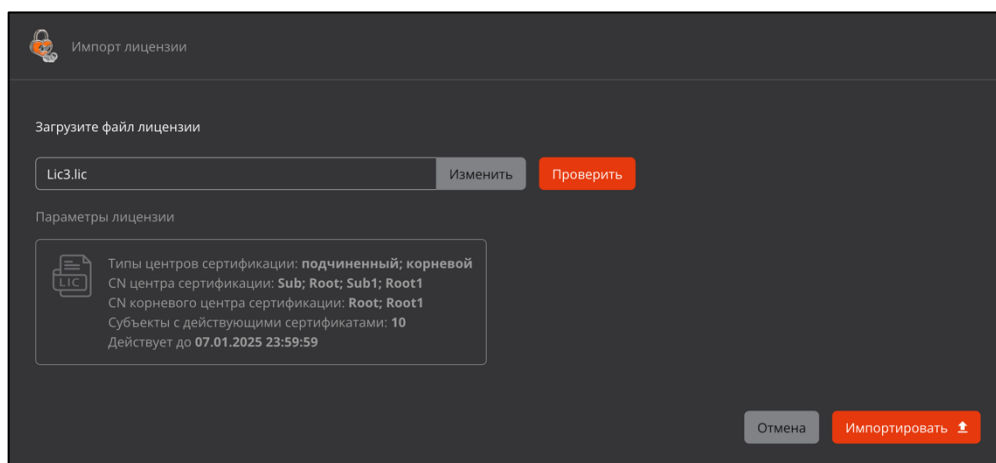


Рисунок 12 – Окно импорта лицензии после успешной проверки на валидность

- Нажмите кнопку <Импортировать> для установки лицензии.
- После успешного импорта лицензии будет:
  - выведено на экран уведомление об успешной установке лицензии «Успешно. Лицензия загружена»;
  - обновлены данные лицензии в поле «Действует до» окна «О программе»;
  - произведена запись в Журнал событий CAENV002.
- После успешной установки лицензии функционал программного средства доступен в полном объеме.
- При попытке импорта лицензии, в которой в перечень имен Центров сертификации не входят имена действующих<sup>5</sup> Центров сертификации (учитывается комбинация имени Центра сертификации и корневого Центра сертификации)<sup>6</sup>, генерируется сообщение об ошибке «В импортируемой лицензии отсутствует имя действующего центра сертификации».

<sup>5</sup> Имеющих статус «Активирован» или «Не активирован».

<sup>6</sup> Импортируемая лицензия позволяет повторно создать любой из действующих Центров сертификации.



## 3 НАЧАЛО РАБОТЫ С ПРОГРАММОЙ

После выбора лицензии (раздел 2.1) необходимо инициализировать Центр сертификации.

- Для инициализации ЦС с генерацией собственного ключа нажмите кнопку <Сгенерировать ключ и создать центр сертификации> и выполните инструкции из раздела 3.1.
- Для инициализации ЦС с импортом существующего ключа из контейнера PKCS#12 нажмите кнопку <Импортировать ключ и создать центр сертификации> и выполните инструкции из раздела 3.2.

### 3.1 Инициализация Центра сертификации с генерацией ключа

#### 3.1.1 Инициализация Корневого Центра сертификации с генерацией ключа

Для инициализации Корневого Центра сертификации с генерацией ключа выполните следующие шаги:

- Если в поле «Типы центров сертификации» указано значение «корневой, подчиненный», то отобразится модальное окно «Окно инициализации корневого центра сертификации. Шаг 1/4» с шагом выбора лицензии (см. Рисунок 13). Для инициализации Корневого Центра сертификации необходимо выбрать тип «Корневой» и нажать на кнопку <Продолжить>.

Если в поле «Типы центров сертификации» указано значение «корневой», то данный шаг пропускается.

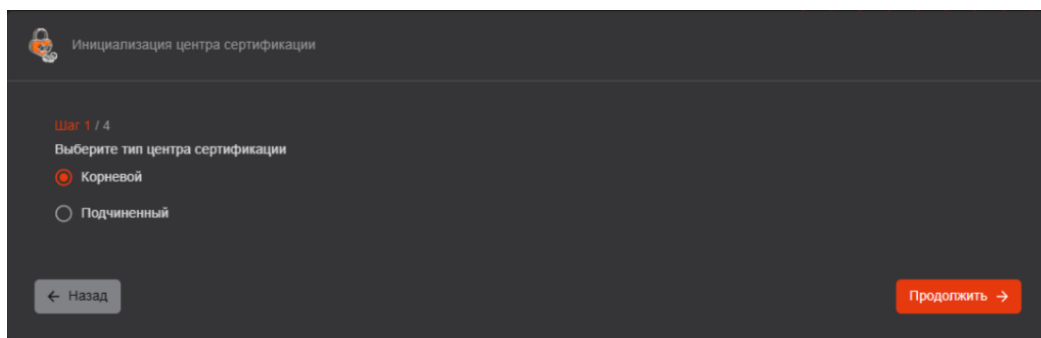


Рисунок 13 – Окно инициализации центра сертификации. Шаг 1/4 . Выбор типа центра сертификации

- На шаге 2/4 (см. Рисунок 14) заполните поля:
  - «Отображаемое имя» – введите имя создаваемого центра сертификации, которое будет отображаться в интерфейсе ЦС Aladdin eCA. Оно может содержать буквы латинского и/или кириллического алфавита, цифры от 0 до 9, символы таблицы ASCII, максимальная длина 200 символов;
  - «Имя центра сертификации» (Common Name) – выберите имя создаваемого корневого центра сертификации из перечня возможных имен в соответствии с параметрами лицензии;
  - «Суффикс различающегося имени» – укажите суффикс различающегося имени корневого сертификата (формат ввода суффикса приведен справа от поля). Ограничители ввода между параметрами – запятые и запятые с пробелами. Длина вводимого суффикса различающегося имени не должна превышать 250 байт. Ввод атрибутов возможен в любом порядке, но в сертификате порядок атрибутов будет установлен в соответствии с номерами пунктов в Таблица 2.

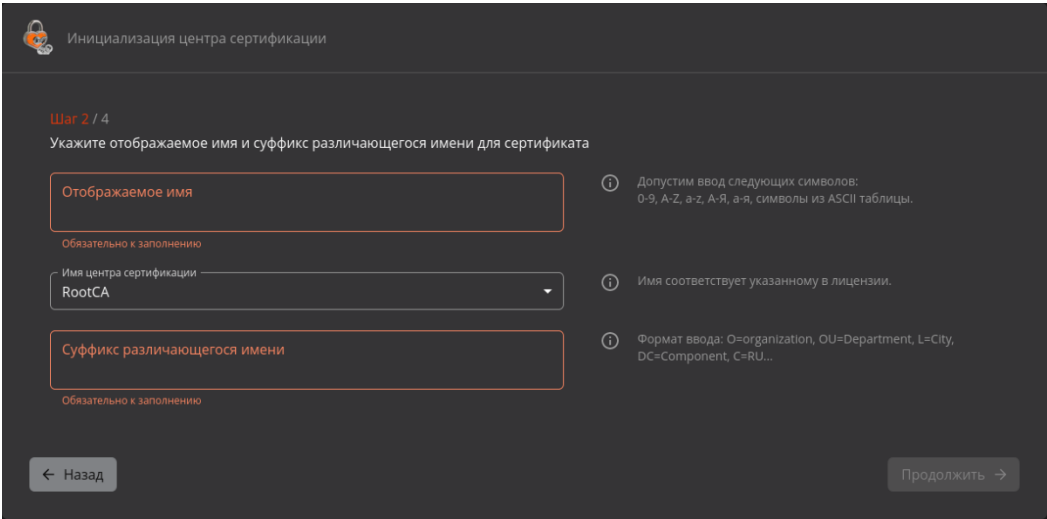


Рисунок 14 – Окно инициализации корневого центра сертификации. Шаг 2/4

Таблица 2 – Поддерживаемые атрибуты суффикса различающегося имени

№	Наименование атрибута	Описание атрибута
1	EMAILADDRESS=	E-mail address (адрес электронной почты) OID: 1.2.840.113549.1.9.1
2	CN=	Common name OID: 2.5.4.3
3	UID=	Unique Identifier (уникальный идентификатор) OID: 2.5.4.45
4	SERIALNUMBER=	Serial number (серийный номер) OID: 2.5.4.5
5	OU=	Organizational Unit (отдел (организации)) OID: 2.5.4.11
6	O=	Organization (организация) OID: 2.5.4.10
7	L=	Locality (район) OID: 2.5.4.7
8	ST=	State or Province (область, край, республика) OID: 2.5.4.8
9	C=	Country (страна, ввод осуществлять согласно регламенту ISO 3166) OID: 2.5.4.6
10	T=	Title (заглавие) OID: 2.5.4.12
11	SURNAME=	Surname (фамилия) OID: 2.5.4.4
12	STREET=	Street address (адрес – улица) OID: 2.5.4.9
13	INITIALS=	First name abbreviation (инициалы) OID: 2.5.4.43
14	GIVENNAME=	Given name (first name - имя) OID: 2.5.4.42
15	DC=	Domain Component (first) (первый доменный компонент, при повторном вводе – второй) OID: 0.9.2342.19200300.100.1.25
16	UNSTRUCTUREDADDRESS=	IP Address (IP-адрес) OID: 1.2.840.113549.1.9.8

№	Наименование атрибута	Описание атрибута
17	UNSTRUCTUREDNAME=	Domain name (доменное имя – FQDN) OID: 1.2.840.113549.1.9.2
18	POSTALCODE=	Postal code (почтовый индекс) OID: 2.5.4.17
19	BUSINESSCATEGORY=	Organization type (категория (тип) организации) OID: 2.5.4.15
20	TELEPHONENUMBER=	Telephone number (телефонный номер) OID: 2.5.4.20
21	PSEUDONYM=	Pseudonym (псевдоним) OID: 2.5.4.65
22	POSTALADDRESS=	Postal adress (почтовый адрес) OID: 2.5.4.16
23	NAME=	//Name (дополнительное имя) OID: 2.5.4.41
24	DN=	DN Qualifier (признак отличительного имени для идентификации субъекта) OID: 2.5.4.46
25	DESCRIPTION=	Description (краткое описание) OID: 2.5.4.13
26	INN=	ИНН (идентификационный номер налогоплательщика) OID: 1.2.643.3.131.1.1
27	OGRN=	ОГРН (основной государственный регистрационный номер) OID: 1.2.643.100.1
28	OGRNIP=	ОГРНИП (основной государственный регистрационный номер индивидуального предпринимателя) OID: 1.2.643.100.5
29	SNILS=	СНИЛС (Страховой номер индивидуального лицевого счёта) OID: 1.2.643.100.3
30	INNLE=	ИНН юридического лица OID: 1.2.643.100.4

После заполнения полей нажмите на кнопку <Продолжить> для перехода к следующему шагу.

- На шаге 3/4 необходимо определить, какой должен использоваться криптопровайдер для каждого алгоритма при создании сертификата центра сертификации и в последующих сценариях выпуска сертификатов субъектов. Для отключенных криптопровайдеров выбор алгоритма будет недоступен и при выпуске сертификатов, несмотря на допустимые значения в шаблонах. Для выбора криптопровайдеров заполните следующие поля (см. Рисунок 15):
  - «RSA» – поле выбора криптопровайдера для алгоритма RSA, допустимые варианты выбора:
    - Стандартный (по умолчанию);
    - КриптоПро CSP<sup>7</sup> (доступен только при наличии активного и подключенного криптопровайдера «КриптоПро CSP», работающего на сервере совместно с компонентом «Центр сертификации Aladdin eCA»);
    - Отключен.
  - «ECDSA» – поле выбора криптопровайдера для алгоритма ECDSA, допустимые варианты выбора:
    - Стандартный (по умолчанию);

<sup>7</sup> Подробная информация по настройке взаимодействия ПО «Центр сертификатов доступа Центр сертификатов доступа Aladdin Enterprise Certificate Authority Certified Edition» с криптопровайдером «КриптоПро CSP» описана в Приложении 5, «Руководства администратора. Установка и обслуживание Центра сертификации Aladdin Enterprise Certification Authority. «Центр сертификатов доступа Центр сертификатов доступа Aladdin Enterprise Certificate Authority Certified Edition». RU.АЛДЕ.03.01.020 32 01-1».

- Отключен.
- «ГОСТ Р 34.10-2012» – поле выбора криптопровайдера для алгоритма ГОСТ Р 34.10-2012, допустимые варианты выбора:
  - КриптоПро CSP (доступен только при наличии активного и подключенного криптопровайдера «КриптоПро CSP», работающего на сервере совместно с компонентом «Центр сертификации Aladdin eCA»);
  - Отключен (по умолчанию).

**На следующем шаге не будет доступен для выбора алгоритм ключа, для которого указано значение криптопровайдера «Отключен».**

**При отключении всех криптопровайдеров кнопка <Продолжить> не будет активирована и переход к следующему шагу будет невозможен.**

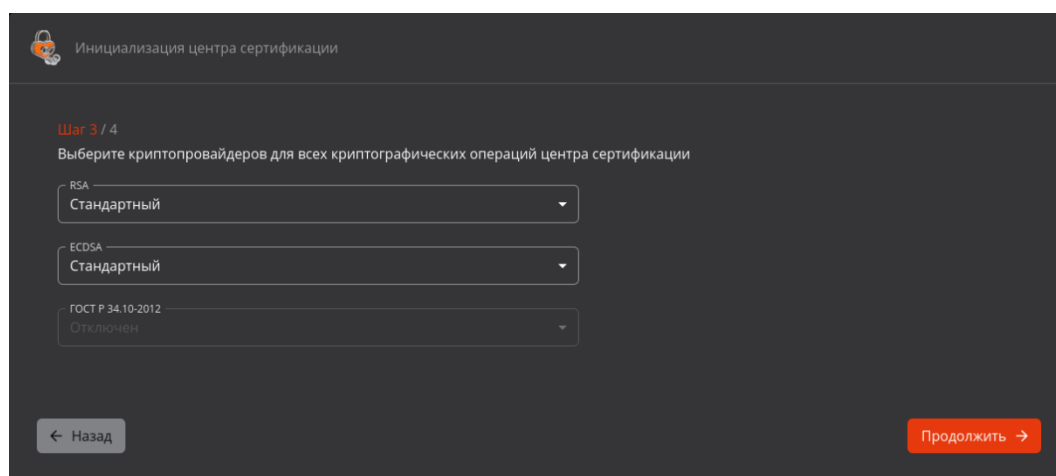


Рисунок 15 - Окно инициализации корневого центра сертификации. Шаг 3/4

После выбора криптопровайдеров нажмите кнопку <Продолжить> для перехода к следующему шагу.

- На шаге 4/4 необходимо указать срок действия сертификата ЦС и задать параметры криптографии (см. Рисунок 16). Заполните следующие поля:
  - «Срок действия сертификата» – срок действия Корневого сертификата (по умолчанию – 10 лет). Ввод осуществляется вручную или выбором даты окончания действия сертификата в открывшемся календаре. Максимальный срок действия сертификата определяется шаблоном «Root CA»<sup>8</sup>;
  - «Алгоритм ключа» (состав алгоритмов зависит от выбранных провайдеров):
    - RSA;
    - ECDSA;
    - ГОСТ Р 34.10-2012.
  - «Длина ключа»:
    - для RSA: 1024, 1536, 2048, 3072, 4096, 6144, 8192 (по умолчанию 4096);
    - для ECDSA: 256, 384, 521 (по умолчанию 384);
    - для ГОСТ Р 34.10-2012: 256, 512 (по умолчанию 512).
  - «Алгоритм хэш-суммы»:

<sup>8</sup> Про шаблон «Root CA» см. в Приложение 2. Описание полей предустановленных шаблонов сертификатов

- для алгоритма ключа RSA или ECDSA: SHA1, SHA256, SHA384, SHA512 (выбран по умолчанию);
- для алгоритма ключа ГОСТ Р 34.10-2012: ГОСТ Р 34.11-2012.
- «Место хранения закрытого ключа»:
  - Доступные варианты выбора, если криптопровайдером выбранного алгоритма ключа является КриптоПро CSP:
    - Локальное хранилище Aladdin eCA (выбрано по умолчанию, требует заранее подготовленной на БДЧ криптопровайдера КриптоПро CSP гаммы);
    - КриптоПро CSP (HDIMAGE);
    - КриптоПро HSM (доступно только при наличии подключения криптопровайдера КриптоПро CSP к ПАКМ «КриптоПро HSM», создаваемые на ПАКМ «КриптоПро HSM» закрытые ключи ЦС являются неэкспортируемыми).
  - В противном случае в данном поле указано неизменяемое значение «Локальное хранилище Aladdin eCA».
- Чек-бокс «Экспортируемый закрытый ключ». Если выбрано место хранения закрытого ключа «Локальное хранилище Aladdin eCA», данный чек-бокс включен по умолчанию и недоступен для изменения.

**При выпуске сертификата доступа Центра сертификации рекомендуется выбирать алгоритмы хэш-суммы SHA256, SHA384 или SHA512 (в случае если в качестве алгоритма ключа выбран RSA или ECDSA).**

**Криптографическая хэш-функция SHA1 не обеспечивает требуемой безопасности и может быть выбрана только при необходимости обеспечения совместимости.**

Рисунок 16 – Окно инициализации корневого центра сертификации. Шаг 4/4  
После задания значений нажать ставшую активной кнопку <Создать ЦС>.

- В случае неудачной попытки создания ЦС будет отображено сообщение об ошибке (см. Таблица 3).

Таблица 3 – Перечень сообщений в случае неудачной попытки создания ЦС

Текст ошибки	Причина																				
Ошибка. Некорректный компонент суффикса различающегося имени – <Имя компонента>	Ошибка ввода неизвестного имени компонента суффикса различающегося имени																				
Ошибка. Лицензионные ограничения не позволяют создать ЦС используя данное имя	Ошибка несоответствия значения в компоненте «CN» суффикса различающегося имени значению, указанному в лицензии																				
Ошибка. Произошла ошибка при создании ключевой пары для алгоритма «Название алгоритма».	Ошибка обращения к криптопровайдеру алгоритма генерации ключевой пары.																				
Ошибка. Ошибка атрибута attributeName: Значение не соответствует регулярному выражению: “regex”	<p>Ошибка валидации введенного значения атрибута различающегося имени<sup>9</sup>. Возможные значения переменной «attributeName» и соответствующие им значения переменной «regex» представлены в таблице ниже:</p> <table> <tr> <th>attributeName</th><th>regex</th></tr> <tr> <td>C</td><td>^[A-Za-z]{2}\$</td></tr> <tr> <td>DN</td><td>^[A-Za-z0-9'()+,\.\/:=? ]+\$</td></tr> <tr> <td>EMAILADDRESS</td><td>^[A-Za-zA-Яа-я0-9._-]+@[A-Za-zA-Яа-я0-9._-]+\$</td></tr> <tr> <td>SERIALNUMBER</td><td>^[A-Za-z0-9'()+,\.\/:=? ]+\$</td></tr> <tr> <td>INN</td><td>^\d{12}\$</td></tr> <tr> <td>OGRN</td><td>^\d{13}\$</td></tr> <tr> <td>OGRNIP</td><td>^\d{15}\$</td></tr> <tr> <td>SNILS</td><td>^\d{11}\$</td></tr> <tr> <td>INNLE</td><td>^\d{10}\$</td></tr> </table>	attributeName	regex	C	^[A-Za-z]{2}\$	DN	^[A-Za-z0-9'()+,\.\/:=? ]+\$	EMAILADDRESS	^[A-Za-zA-Яа-я0-9._-]+@[A-Za-zA-Яа-я0-9._-]+\$	SERIALNUMBER	^[A-Za-z0-9'()+,\.\/:=? ]+\$	INN	^\d{12}\$	OGRN	^\d{13}\$	OGRNIP	^\d{15}\$	SNILS	^\d{11}\$	INNLE	^\d{10}\$
attributeName	regex																				
C	^[A-Za-z]{2}\$																				
DN	^[A-Za-z0-9'()+,\.\/:=? ]+\$																				
EMAILADDRESS	^[A-Za-zA-Яа-я0-9._-]+@[A-Za-zA-Яа-я0-9._-]+\$																				
SERIALNUMBER	^[A-Za-z0-9'()+,\.\/:=? ]+\$																				
INN	^\d{12}\$																				
OGRN	^\d{13}\$																				
OGRNIP	^\d{15}\$																				
SNILS	^\d{11}\$																				
INNLE	^\d{10}\$																				
Ошибка при создании Центра сертификации. Неизвестная ошибка	Внутренняя ошибка ПО																				

- При успешном создании Корневого ЦС и завершении инициализации центра сертификации будет отображено соответствующее окно (см. Рисунок 17). В нём возможно:
  - скачать сертификат созданного Корневого ЦС;
  - скачать цепочку сертификатов в формате .pem;
  - или открыть страницу созданного Центра сертификации.

Также в результате успешного создания данного ЦС в контейнере закрытого ключа данного ЦС будут содержаться закрытый ключ данного ЦС и цепочка сертификатов данного ЦС<sup>10</sup>.

<sup>9</sup> Правила валидации значений атрибутов представлены в Приложение 4. Правила валидации значений полей по умолчанию предустановленных шаблонов сертификатов.

<sup>10</sup> Если местом хранения закрытого ключа ЦС является ПАКМ «КриптоПро HSM», то созданный закрытый ключ ЦС будет неэкспортируемым.

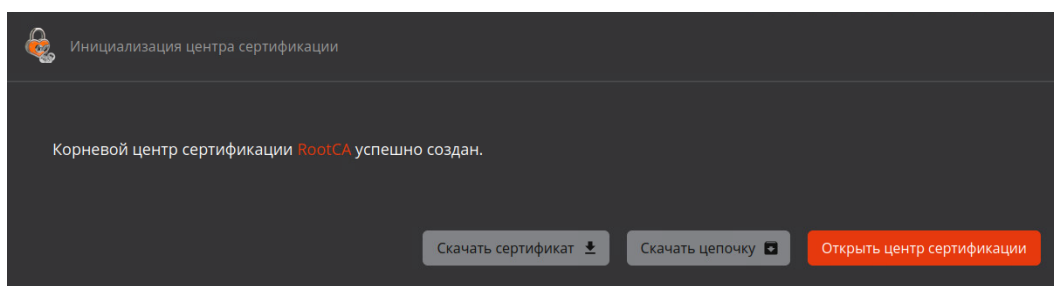


Рисунок 17 – Окно завершения инициализации корневого центра сертификации

### 3.1.2 Инициализация Подчиненного Центра сертификации с генерацией ключа

Для инициализации Подчиненного Центра сертификации с созданием ключа выполните следующие шаги:

- Если в поле «Типы центров сертификации» указано значение «корневой, подчиненный», то отобразится модальное окно «Окно инициализации корневого центра сертификации. Шаг 1/4» с шагом выбора лицензии (см. Рисунок 13). Для инициализации Подчиненного Центра сертификации необходимо выбрать тип «Подчиненный» и нажать на кнопку <Продолжить>.

Если в поле «Типы центров сертификации» указано значение «подчиненный», то данный шаг пропускается.

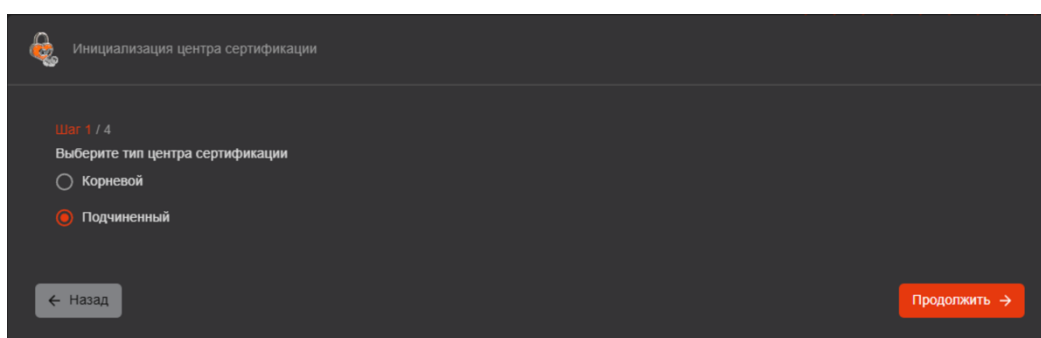


Рисунок 18 – Окно инициализации центра сертификации. Шаг 1/4 . Выбор типа центра сертификации

- На шаге 2/4 (см. Рисунок 19) заполните поля:
  - «Отображаемое имя» – введите имя создаваемого центра сертификации, которое будет отображаться в интерфейсе ЦС Aladdin eCA. Оно может содержать буквы латинского и/или кириллического алфавита, цифры от 0 до 9, символы таблицы ASCII, максимальная длина 200 символов;
  - «Имя центра сертификации» (Common Name) – выберите имя создаваемого подчиненного центра сертификации из перечня возможных имен в соответствии с параметрами лицензии;
  - «Суффикс различающегося имени» – укажите суффикс различающегося имени подчиненного ЦС (формат ввода суффикса приведен справа от поля). Ограничители ввода между параметрами – запятые и запятые с пробелами. Длина вводимого суффикса различающегося имени не должна превышать 250 байт. Ввод атрибутов возможен в любом порядке, но в сертификате порядок атрибутов будет установлен в соответствии с номерами пунктов в Таблица 4.

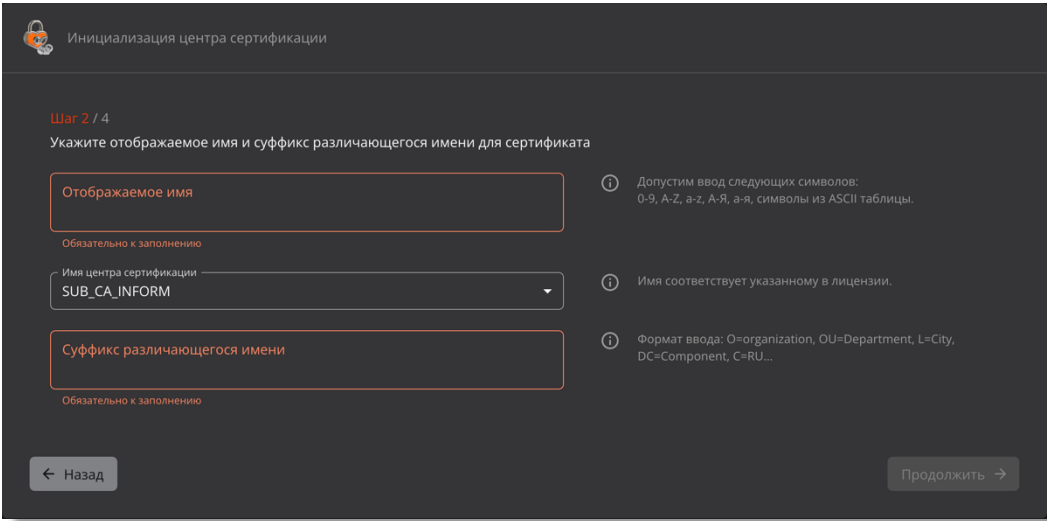


Рисунок 19 – Окно инициализации подчиненного центра сертификации. Шаг 2/4

Таблица 4 – Поддерживаемые атрибуты суффикса различающегося имени

№	Наименование атрибута	Описание атрибута
1	EMAILADDRESS=	E-mail address (адрес электронной почты) OID: 1.2.840.113549.1.9.1
2	CN=	Common name OID: 2.5.4.3
3	UID=	Unique Identifier (уникальный идентификатор) OID: 2.5.4.45
4	SERIALNUMBER=	Serial number (серийный номер) OID: 2.5.4.5
5	OU=	Organizational Unit (отдел (организации)) OID: 2.5.4.11
6	O=	Organization (организация) OID: 2.5.4.10
7	L=	Locality (район) OID: 2.5.4.7
8	ST=	State or Province (область, край, республика) OID: 2.5.4.8
9	C=	Country (страна, ввод осуществлять согласно регламенту ISO 3166) OID: 2.5.4.6
10	T=	Title (заглавие) OID: 2.5.4.12
11	SURNAME=	Surname (фамилия) OID: 2.5.4.4
12	STREET=	Street address (адрес – улица) OID: 2.5.4.9
13	INITIALS=	First name abbreviation (инициалы) OID: 2.5.4.43
14	GIVENNAME=	Given name (first name - имя) OID: 2.5.4.42
15	DC=	Domain Component (first) (первый доменный компонент, при повторном вводе – второй) OID: 0.9.2342.19200300.100.1.25
16	UNSTRUCTUREDADDRESS=	IP Address (IP-адрес) OID: 1.2.840.113549.1.9.8



№	Наименование атрибута	Описание атрибута
17	UNSTRUCTUREDNAME=	Domain name (доменное имя – FQDN) OID: 1.2.840.113549.1.9.2
18	POSTALCODE=	Postal code (почтовый индекс) OID: 2.5.4.17
19	BUSINESSCATEGORY=	Organization type (категория (тип) организации) OID: 2.5.4.15
20	TELEPHONENUMBER=	Telephone number (телефонный номер) OID: 2.5.4.20
21	PSEUDONYM=	Pseudonym (псевдоним) OID: 2.5.4.65
22	POSTALADDRESS=	Postal adress (почтовый адрес) OID: 2.5.4.16
23	NAME=	//Name (дополнительное имя) OID: 2.5.4.41
24	DN=	DN Qualifier (признак отличительного имени для идентификации субъекта) OID: 2.5.4.46
25	DESCRIPTION=	Description (краткое описание) OID: 2.5.4.13
26	INN=	ИНН (идентификационный номер налогоплательщика) OID: 1.2.643.3.131.1.1
27	OGRN=	ОГРН (основной государственный регистрационный номер) OID: 1.2.643.100.1
28	OGRNIP=	ОГРНИП (основной государственный регистрационный номер индивидуального предпринимателя) OID: 1.2.643.100.5
29	SNILS=	СНИЛС (Страховой номер индивидуального лицевого счёта) OID: 1.2.643.100.3
30	INNLE=	ИНН юридического лица OID: 1.2.643.100.4

После заполнения полей нажмите на кнопку <Продолжить> для перехода к следующему шагу.

- На шаге 3/4 необходимо определить, какой должен использоваться криптопровайдер для каждого алгоритма при создании сертификата центра сертификации и в последующих сценариях выпуска сертификатов субъектов. Для отключенных криптопровайдеров выбор алгоритма будет недоступен и при выпуске сертификатов, несмотря на допустимые значения в шаблонах. Для выбора криптопровайдеров заполните следующие поля (см. Рисунок 20):
  - «RSA» – поле выбора криптопровайдера для алгоритма RSA, допустимые варианты выбора:
    - Стандартный (по умолчанию);
    - КриптоПро CSP<sup>11</sup> (доступен только при наличии активного и подключенного криптопровайдера «КриптоПро CSP», работающего на сервере совместно с компонентом «Центр сертификации Aladdin eCA»);
    - Отключен.
  - «ECDSA» – поле выбора криптопровайдера для алгоритма ECDSA, допустимые варианты выбора:

<sup>11</sup> Подробная информация по настройке взаимодействия ПО «Центр сертификатов доступа Центр сертификатов доступа Aladdin Enterprise Certificate Authority Certified Edition» с криптопровайдером «КриптоПро CSP» описана в Приложении 5, «Руководства администратора. Установка и обслуживание Центра сертификации Aladdin Enterprise Certification Authority. «Центр сертификатов доступа Центр сертификатов доступа Aladdin Enterprise Certificate Authority Certified Edition». RU.АЛДЕ.03.01.020 32 01-1».

- Стандартный (по умолчанию);
- Отключен.
- «ГОСТ Р 34.10-2012» – поле выбора криптопровайдера для алгоритма ГОСТ Р 34.10-2012, допустимые варианты выбора:
  - КриптоПро CSP Ошибка! Закладка не определена. (доступен только при наличии активного и подключенного криптопровайдера «КриптоПро CSP», работающего на сервере совместно с компонентом «Центр сертификации Aladdin eCA»);
  - Отключен (по умолчанию).

**На следующем шаге не будет доступен для выбора алгоритм ключа, для которого указано значение криптопровайдера «Отключен».**

**При отключении всех криптопровайдеров кнопка <Продолжить> не будет активирована и переход к следующему шагу будет невозможен.**

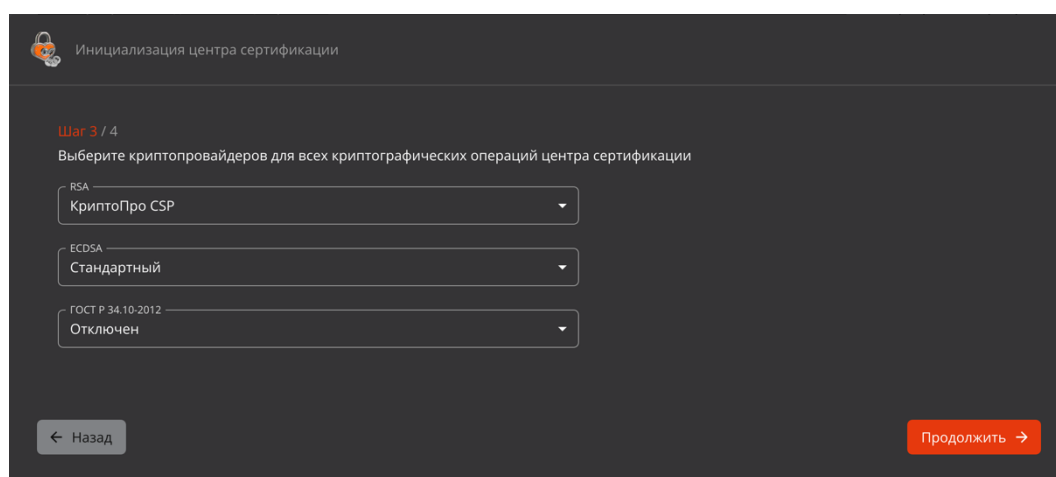


Рисунок 20 - Окно инициализации подчиненного центра сертификации. Шаг 2/3

После выбора криптопровайдера во всех полях нажмите ставшую активной кнопку <Продолжить>.

- На шаге 4/4 необходимо задать параметры криптографии (см. Рисунок 21):
  - «Алгоритм ключа» (состав алгоритмов зависит от выбранных провайдеров):
    - RSA;
    - ECDSA;
    - ГОСТ Р 34.10-2012.
  - «Длина ключа» (по умолчанию выбирается наименьшая доступная длина ключа для выбранного алгоритма):
    - для RSA: 1024, 1536, 2048, 3072, 4096, 6144, 8192 (по умолчанию 3072);
    - для ECDSA: 256, 384, 521 (по умолчанию 256);
    - для ГОСТ Р 34.10-2012: 256, 512 (по умолчанию 256).
  - «Алгоритм хэш-суммы»:
    - для алгоритма ключа RSA или ECDSA: SHA1, SHA256, SHA384 (выбран по умолчанию), SHA512;
    - для алгоритма ключа ГОСТ Р 34.10-2012: ГОСТ Р 34.11-2012.
  - «Место хранения закрытого ключа»:

- Доступные варианты выбора, если криптопровайдером выбранного алгоритма ключа является КриптоПро CSP:
  - Локальное хранилище Aladdin eCA (выбрано по умолчанию, требует заранее подготовленной на БДЧ криптопровайдера КриптоПро CSP гаммы);
  - КриптоПро CSP (HDIMAGE);
  - КриптоПро HSM (доступно только при наличии подключения криптопровайдера КриптоПро CSP к ПАКМ «КриптоПро HSM», создаваемые на ПАКМ «КриптоПро HSM» закрытые ключи ЦС являются неэкспортируемыми).
- В противном случае в данном поле указано неизменяемое значение «Локальное хранилище Aladdin eCA».
- Чек-бокс «Экспортируемый закрытый ключ». Если выбрано место хранения закрытого ключа «Локальное хранилище Aladdin eCA», данный чек-бокс включен по умолчанию и недоступен для изменения.

**При выпуске сертификата доступа Центра сертификации рекомендуется выбирать алгоритмы хэш-суммы SHA256, SHA384 или SHA512 (в случае если в качестве алгоритма ключа выбран RSA или ECDSA).**

**Криптографическая хэш-функция SHA1 не обеспечивает требуемой безопасности и может быть выбрана только при необходимости обеспечения совместимости.**

**Срок действия сертификата по умолчанию устанавливается равным сроку действия, заданному в шаблоне, используемом при выпуске сертификата (подписании запроса), но не превышает срок действия сертификата Корневого ЦС.**

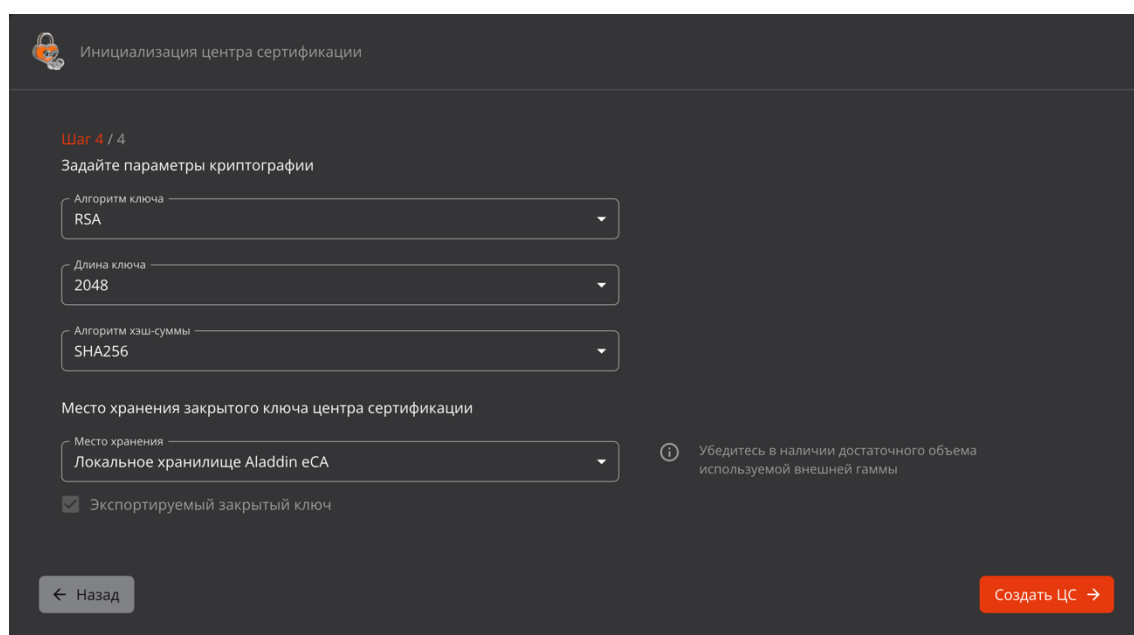


Рисунок 21 – Окно инициализации подчиненного центра сертификации. Шаг 4/4  
После задания значений нажать ставшую активной кнопку «Создать ЦС».

- В случае неудачной попытки создания ЦС будет отображено сообщение об ошибке (см. Таблица 5).

Таблица 5 – Перечень сообщений в случае неудачной попытки создания ЦС

Текст ошибки	Причина																				
Ошибка. Некорректный компонент суффикса различающегося имени – <Имя компонента>	Ошибка ввода неизвестного имени компонента суффикса различающегося имени																				
Ошибка. Лицензионные ограничения не позволяют создать ЦС используя данное имя	Ошибка несоответствия значения в компоненте «CN» суффикса различающегося имени значению, указанному в лицензии																				
Ошибка. Произошла ошибка при создании ключевой пары для алгоритма «Название алгоритма».	Ошибка обращения к криптопровайдеру алгоритма генерации ключевой пары.																				
Ошибка. Ошибка атрибута attributeName: Значение не соответствует регулярному выражению: «regex»	<p>Ошибка валидации введенного значения атрибута различающегося имени<sup>12</sup>. Возможные значения переменной «attributeName» и соответствующие им значения переменной «regex» представлены в таблице ниже:</p> <table border="1"> <thead> <tr> <th>attributeName</th><th>regex</th></tr> </thead> <tbody> <tr> <td>C</td><td>^[A-Za-z]{2}\$</td></tr> <tr> <td>DN</td><td>^[A-Za-z0-9''()+,\.\/:=? ]+\$</td></tr> <tr> <td>EMAILADDRESS</td><td>^[A-Za-zA-Яa-я0-9._-]+@[A-Za-zA-Яa-я0-9._-]+\$</td></tr> <tr> <td>SERIALNUMBER</td><td>^[A-Za-z0-9''()+,\.\/:=? ]+\$</td></tr> <tr> <td>INN</td><td>^\d{12}\$</td></tr> <tr> <td>OGRN</td><td>^\d{13}\$</td></tr> <tr> <td>OGRNIP</td><td>^\d{15}\$</td></tr> <tr> <td>SNILS</td><td>^\d{11}\$</td></tr> <tr> <td>INNLE</td><td>^\d{10}\$</td></tr> </tbody> </table>	attributeName	regex	C	^[A-Za-z]{2}\$	DN	^[A-Za-z0-9''()+,\.\/:=? ]+\$	EMAILADDRESS	^[A-Za-zA-Яa-я0-9._-]+@[A-Za-zA-Яa-я0-9._-]+\$	SERIALNUMBER	^[A-Za-z0-9''()+,\.\/:=? ]+\$	INN	^\d{12}\$	OGRN	^\d{13}\$	OGRNIP	^\d{15}\$	SNILS	^\d{11}\$	INNLE	^\d{10}\$
attributeName	regex																				
C	^[A-Za-z]{2}\$																				
DN	^[A-Za-z0-9''()+,\.\/:=? ]+\$																				
EMAILADDRESS	^[A-Za-zA-Яa-я0-9._-]+@[A-Za-zA-Яa-я0-9._-]+\$																				
SERIALNUMBER	^[A-Za-z0-9''()+,\.\/:=? ]+\$																				
INN	^\d{12}\$																				
OGRN	^\d{13}\$																				
OGRNIP	^\d{15}\$																				
SNILS	^\d{11}\$																				
INNLE	^\d{10}\$																				
Ошибка при создании Центра сертификации. Неизвестная ошибка	Внутренняя ошибка ПО																				

- При успешном создании Подчиненного ЦС и завершении инициализации центра сертификации будет отображено соответствующее окно (см. Рисунок 22). В нём возможно:
  - скачать запрос на сертификат созданного подчинённого ЦС;
  - импортировать цепочки сертификатов корневого ЦС после подписания запроса на сертификат подчиненного ЦС;
  - закрыть окно инициализации центра сертификации.

<sup>12</sup> Правила валидации значений атрибутов представлены в Приложение 4. Правила валидации значений полей по умолчанию предустановленных шаблонов сертификатов.

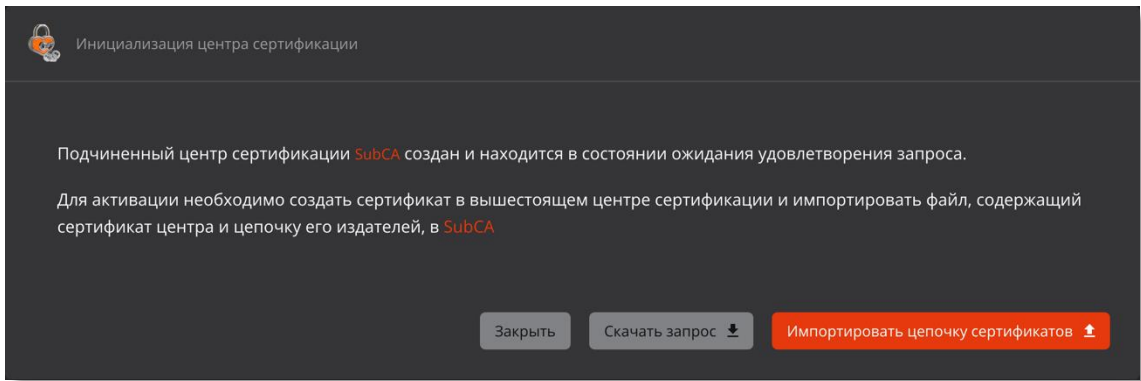


Рисунок 22 – Окно завершения инициализации подчиненного центра сертификации

- Скачайте созданный запрос на сертификат Подчиненного ЦС в формате `.csr`.
- На данном этапе Подчиненный ЦС создан, отображается на вкладке «Свои сертификаты» и имеет статус «Запрос» (см. Рисунок 23).
- Для перевода ЦС в состояние «Активирован»:
  - необходимо выполнить подписание запроса на Корневом ЦС (см. раздел 7.3.2.2);
  - и затем импорт подписанного сертификата Подчиненного ЦС (см. раздел 7.3.1.6).

До момента активации у Подчиненного ЦС в контейнере закрытого ключа содержится самоподписанный технологический сертификат, а после успешной активации в контейнере закрытого ключа Подчиненного ЦС будут содержаться закрытый ключ данного ЦС и цепочка сертификатов данного ЦС<sup>13</sup>.

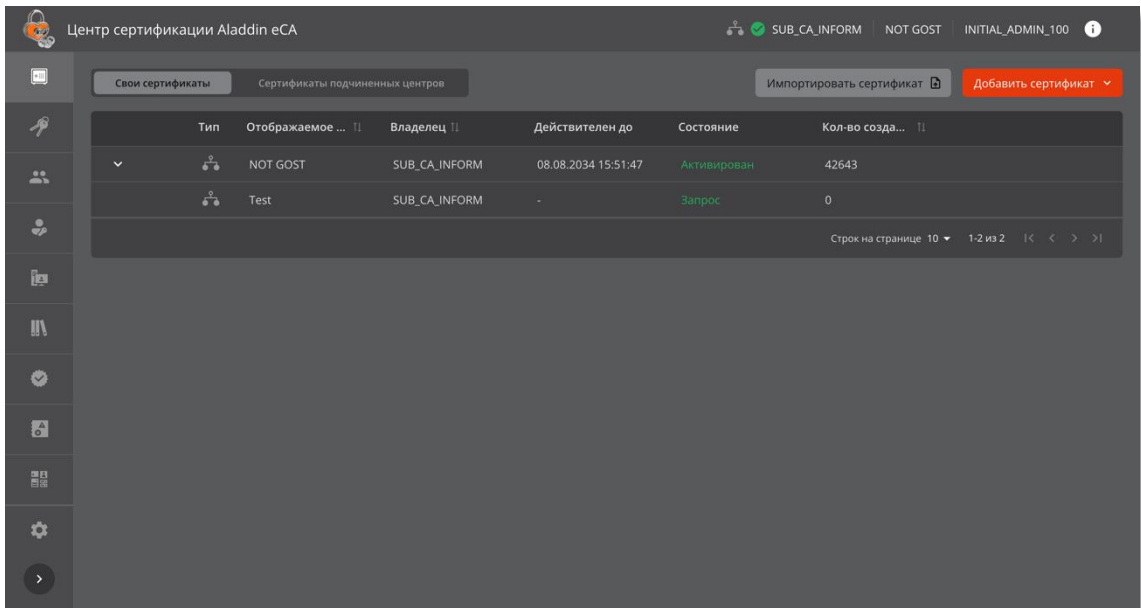


Рисунок 23 – Окно Центра сертификации. Подчинённый ЦС в состоянии «Запрос»

### 3.2 Инициализация Центра сертификации с импортом ключа

Для инициализации Центра сертификации с импортом внешнего ключа из контейнера PKCS#12 выполните следующие шаги:

<sup>13</sup> Если местом хранения закрытого ключа ЦС является ПАКМ «КриптоПро HSM», то созданный закрытый ключ ЦС будет неэкспортируемым.

- В появившемся модальном окне «Окно инициализации центра сертификации с импортом ключа. Шаг 1/3» (см. Рисунок 24) выберите файл контейнера ключей PKCS#12 и введите пароль от него.

**Программный компонент Aladdin eCA поддерживает следующие алгоритмы хэш-суммы ключа при импорте контейнера Корневого ЦС: SHA1, SHA256, SHA384, SHA512, SHA3-256, SHA3-384, SHA3-512, RSASSA-PSS.**

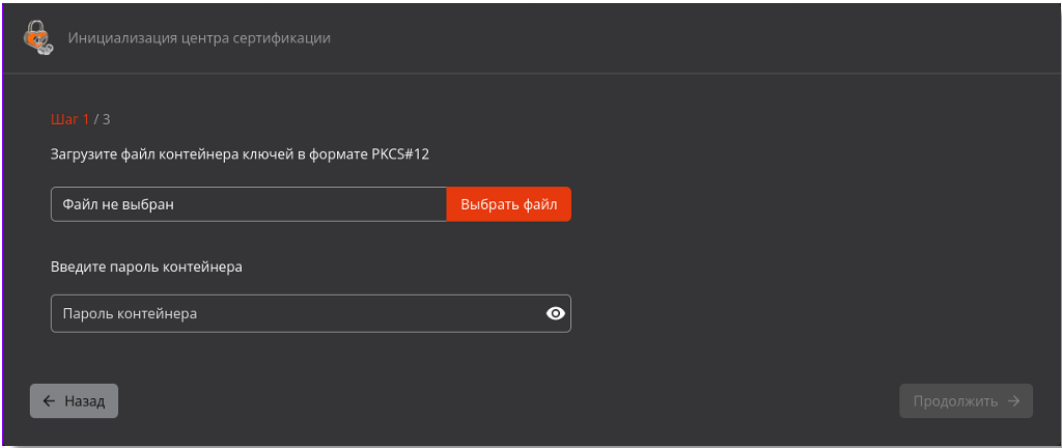


Рисунок 24 – Окно инициализации центра сертификации с импортом ключа. Шаг 1/3

- После выбора файла и ввода пароля необходимо нажать кнопку <Проверить>, которая появляется после их заполнения (см. Рисунок 25).

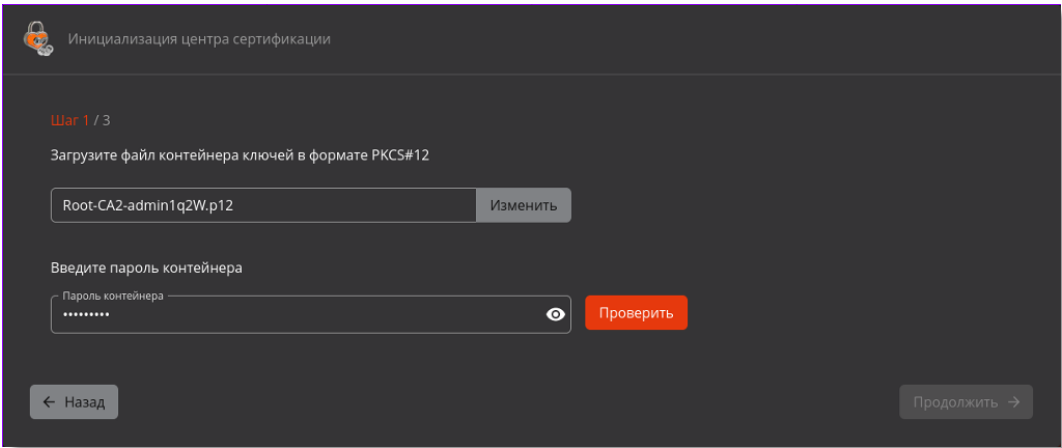


Рисунок 25 – Окно инициализации центра сертификации с импортом ключа. Шаг 1/3 – после заполнения полей

При нажатии на неё происходит проверка контейнера ключей PKCS#12. Если в результат проверки возникла ошибка, то в окне отображается соответствующее сообщение. Список возможных ошибок приведен в Таблица 6.

Таблица 6 – Возможные ошибки при проверке контейнера ключей PKCS#12

Ошибка	Причина
Формат файла	
Ошибка. Некорректный формат файла контейнера.	Формат файла контейнера не соответствует PKCS#12.
Ошибка. Неверный пароль контейнера.	Не удалось открыть контейнер с помощью указанного пароля.
Лицензионные ограничения	
Ошибка.	Тип ЦС из контейнера не входит в разрешенные типы ЦС из лицензии.

Лицензионные ограничения не позволяют создать <Тип ЦС> ЦС.	
Ошибка. Лицензионные ограничения не позволяют создать ЦС с именем <Имя ЦС>.	Указанное в контейнера «CN» суффикса различающегося имени значение не входит в перечень значений имени ЦС из лицензии.
Ошибка. Лицензионные ограничения не позволяют создать ЦС с издателем <Имя издателя>.	Указанный в контейнере имя издателя сертификата не входит в перечень значений имени корневых ЦС из лицензии.
<b>Сертификат</b>	
Ошибка. Срок действия сертификата истек.	Дата «Действителен до» сертификата из контейнера превышает текущую.
Ошибка. Срок действия сертификата <Имя> из цепочки истек.	Дата «Действителен до» сертификата из цепочки сертификатов контейнера превышает текущую. За исключение сертификата ЦС из контейнера – в этом случае отображается предыдущая ошибка (более конкретная).
Ошибка Сертификат не является сертификатом ЦС.	У сертификата в поле 2.5.29.19 «Basic Constraints» (Основные ограничения) не указано, что субъектом является ЦС.
<b>Параметры криптографии</b>	
Ошибка. Неподдерживаемый алгоритм ключа: <Алгоритм> <Длина ключа>.	Неподдерживаемый алгоритм ключа “значение” с длиной ключа “значение”;
Ошибка. Неподдерживаемый алгоритм хэш-суммы: <Алгоритм>.	Неподдерживаемый алгоритм хэш-суммы “значение”.
<b>Прочее</b>	
Ошибка. Неизвестная ошибка.	Внутренняя ошибка ПО.

- При корректности данных контейнера PKCS#12 в окне отобразится соответствующая информация, включающая (см. Рисунок 26):
  - Наименование издателя;
  - Наименование субъекта;
  - Срок действия сертификата;
  - Цепочку сертификатов;
  - Алгоритм ключа;
  - Длину ключа.

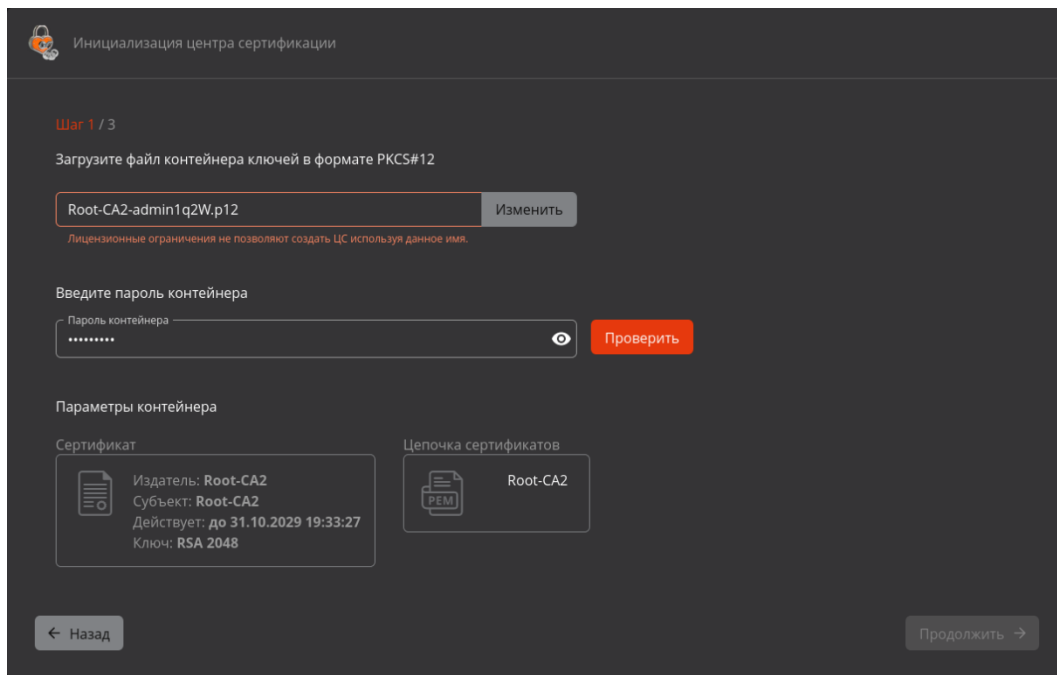


Рисунок 26 – Окно инициализации центра сертификации с импортом ключа. Шаг 1/3. Ошибка лицензионного ограничения

- При отсутствии ошибок становится доступной кнопка <Продолжить> (см. Рисунок 27).

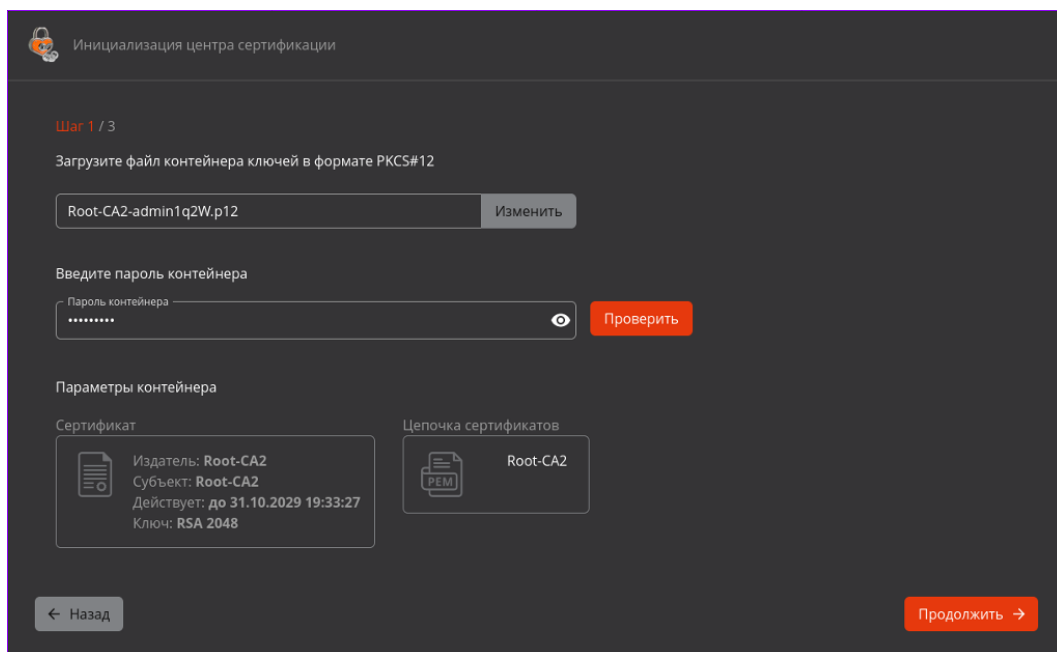


Рисунок 27 – Окно инициализации центра сертификации. Шаг 1/3. После успешной проверки  
Для перехода к следующему шагу нажмите кнопку <Продолжить>.

**Тип Центра сертификации (Корневой или Подчиненный) выбирается автоматически в соответствии с данными контейнера PKCS#12.**

- На шаге 2/3 заполните поля:



- «Отображаемое имя» – введите имя создаваемого центра сертификации, которое будет отображаться в интерфейсе ЦС Aladdin eCA. Оно может содержать буквы латинского и/или кириллического алфавита, цифры от 0 до 9, символы таблицы ASCII, максимальная длина 200 символов;
- «Место хранения закрытого ключа центра сертификации». Список вариантов мест хранения закрытого ключа зависит от:
  - алгоритма ключа, указанного в контейнере PKCS#12;
  - криптопровайдера закрытого ключа, определяемого при проверке контейнера PKCS#1214;
  - наличия активного криптопровайдера «КриптоПро CSP» на хосте ЦС Aladdin eCA;
  - наличия подключения криптопровайдера «КриптоПро CSP» к ПАКМ «КриптоПро HSM».

И представлен ниже (см. Таблица 7):

Таблица 7 – Варианты мест хранения закрытого ключа

Алгоритм ключа	Криптопровайдер ключа	Место хранения
RSA	Стандартный	<ul style="list-style-type: none"> <li>• Локальное хранилище Aladdin eCA</li> <li>• КриптоПро CSP (HDIMAGE) при наличии активного криптопровайдера «КриптоПро CSP» на хосте ЦС Aladdin eCA</li> <li>• КриптоПро HSM при активном криптопровайдере «КриптоПро CSP» на хосте ЦС Aladdin eCA и подключении криптопровайдера «КриптоПро CSP» к ПАКМ «КриптоПро HSM»</li> </ul>
RSA	КриптоПро CSP	<ul style="list-style-type: none"> <li>• КриптоПро CSP (HDIMAGE) при наличии активного криптопровайдера «КриптоПро CSP» на хосте ЦС Aladdin eCA</li> <li>• КриптоПро HSM при активном криптопровайдере «КриптоПро CSP» на хосте ЦС Aladdin eCA и подключении криптопровайдера «КриптоПро CSP» к ПАКМ «КриптоПро HSM»</li> </ul>
ECDSA	Стандартный	<ul style="list-style-type: none"> <li>• Локальное хранилище Aladdin eCA</li> </ul>
ГОСТ Р 34.11-2012	КриптоПро CSP	<ul style="list-style-type: none"> <li>• КриптоПро CSP (HDIMAGE) при наличии активного криптопровайдера «КриптоПро CSP» на хосте ЦС Aladdin eCA</li> <li>• КриптоПро HSM при активном криптопровайдере «КриптоПро CSP» на хосте ЦС Aladdin eCA и подключении криптопровайдера «КриптоПро CSP» к ПАКМ «КриптоПро HSM»</li> </ul>

<sup>14</sup> Данная зависимость обусловлена тем, что возможности работы с закрытым ключом в Java зависят от криптопровайдера, создавшего данный ключ. Например, при использовании криптопровайдера КриптоПро CSP работа происходит не с самим закрытым ключом, а с его дескриптором – и доступ к данным закрытого ключа отсутствует.

Возможно, результат дальнейших исследований покажет, как обойти это ограничение. И тогда необходимо будет обновить таблицу.

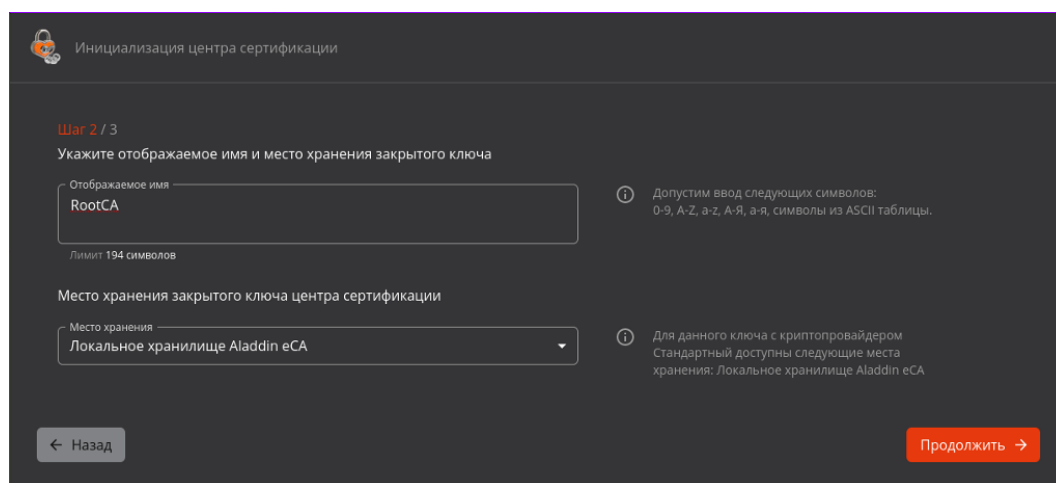


Рисунок 28 – Окно инициализации центра сертификации. Шаг 2/3

Для перехода к следующему шагу нажмите кнопку <Продолжить>.

- На шаге 3/3 выберите криптопровайдеры для всех криптографических операций центра сертификации. Для выбора криптопровайдеров заполните следующие поля (см. Рисунок 29 и Рисунок 30):
  - «RSA» – поле выбора криптопровайдера для алгоритма RSA, допустимые варианты выбора:
    - Стандартный (по умолчанию);
    - КриптоПро CSP<sup>15</sup> (доступен только при наличии активного и подключенного криптопровайдера «КриптоПро CSP», работающего на сервере совместно с компонентом «Центр сертификации Aladdin eCA»);
    - Отключен.
  - «ECDSA» – поле выбора криптопровайдера для алгоритма ECDSA, допустимые варианты выбора:
    - Стандартный (по умолчанию);
    - Отключен.
  - «ГОСТ Р 34.10-2012» – поле выбора криптопровайдера для алгоритма ГОСТ Р 34.10-2012, допустимые варианты выбора:
    - КриптоПро CSP (доступен только при наличии активного и подключенного криптопровайдера «КриптоПро CSP», работающего на сервере совместно с компонентом «Центр сертификации Aladdin eCA»);
    - Отключен (по умолчанию).
  - поле «Алгоритм хэш-суммы»:
    - Для корневого ЦС значение берется из контейнера PKCS#12 (см. Рисунок 29). При этом поле заблокировано. Поддерживаются следующие алгоритмы хэш-суммы ключа: SHA1, SHA256, SHA384, SHA512, SHA3-256, SHA3-384, SHA3-512, RSASSA-PSS.
    - Для подчиненного ЦС необходимо задать значение (см. Рисунок 30):

<sup>15</sup> Подробная информация по настройке взаимодействия ПО «Центр сертификатов доступа Центр сертификатов доступа Aladdin Enterprise Certificate Authority Certified Edition» с криптопровайдером «КриптоПро CSP» описана в Приложении 5, «Руководства администратора. Установка и обслуживание Центра сертификации Aladdin Enterprise Certification Authority. «Центр сертификатов доступа Центр сертификатов доступа Aladdin Enterprise Certificate Authority Certified Edition». RU.АЛДЕ.03.01.020 32 01-1».

- для алгоритма ключа RSA или ECDSA: SHA1, SHA256, SHA384 (выбран по умолчанию), SHA512;
- для алгоритма ключа ГОСТ Р 34.10-2012: ГОСТ Р 34.11-2012.

Рисунок 29 – Окно инициализации корневого центра сертификации. Шаг 3/3

Рисунок 30 – Окно инициализации подчиненного центра сертификации. Шаг 3/3

**При отключении всех криптопровайдеров кнопка <Продолжить> не будет активирована и переход к следующему шагу будет невозможен.**

После задания значений нажмите кнопку <Создать ЦС>.

- В результате успешного создания ЦС отобразится модальное окно с сообщением об успешном создании и активации ЦС (см. Рисунок 31 и Рисунок 32). В модальном окне есть следующие кнопки:
  - <Скачать сертификат> – при нажатии происходит скачивание сертификата созданного ЦС;
  - <Скачать цепочку сертификатов> – при нажатии происходит скачивание цепочки сертификатов созданного ЦС;

- <Открыть созданный центр сертификации> – при нажатии на кнопку происходит переход в раздел «Центр сертификации» с активной вкладкой «Свои сертификаты».

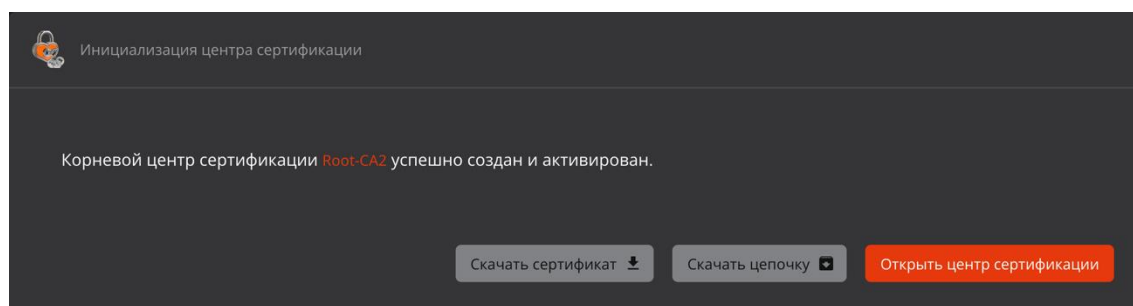


Рисунок 31 – Окно завершения инициализации корневого центра сертификации

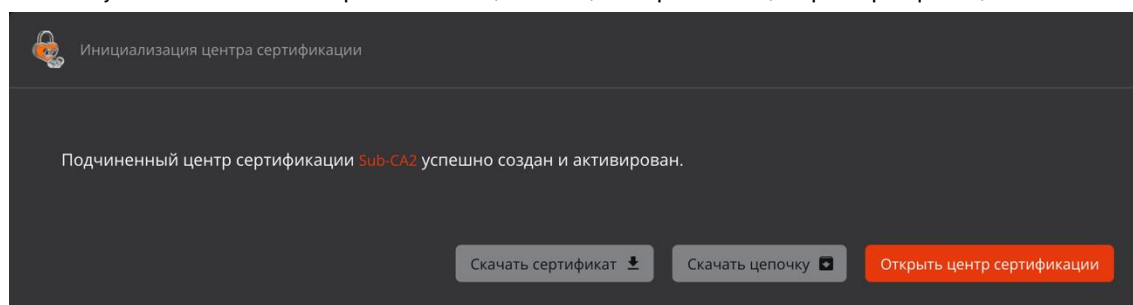


Рисунок 32 – Окно завершения инициализации подчиненного центра сертификации

## 4 ДОСТУП К ПРОГРАММЕ

Перед началом работы с Центром сертификации и доступа к ресурсам необходимо произвести двустороннюю HTTPS-аутентификацию пользователя для входа в учётную запись, когда веб-клиент проверяет сертификат веб-сервера и веб-сервер проверяет сертификат веб-клиента.

### 4.1 Аутентификация с использованием сертификата, перенесённого на жесткий диск

Полученный администратором контейнер сертификата доступа для аутентификации на веб-сервере Центра сертификации Aladdin Enterprise Certification Authority необходимо перенести любым удобным способом на жёсткий диск СBT 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 33). Нажмите кнопку <Просмотр сертификатов>.

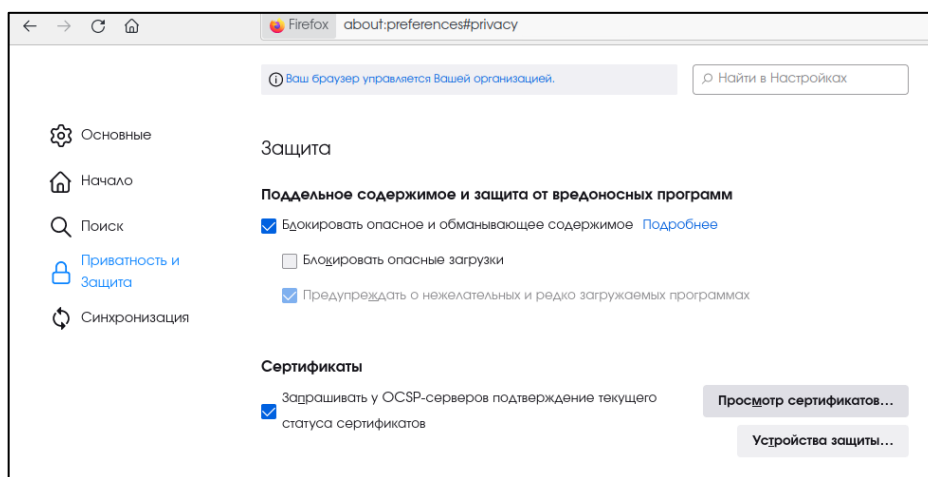


Рисунок 33 – Окно настроек браузера

- Выберите вкладку «Ваши сертификаты», в открывшейся вкладке нажмите кнопку <Импортировать> (см. Рисунок 34).

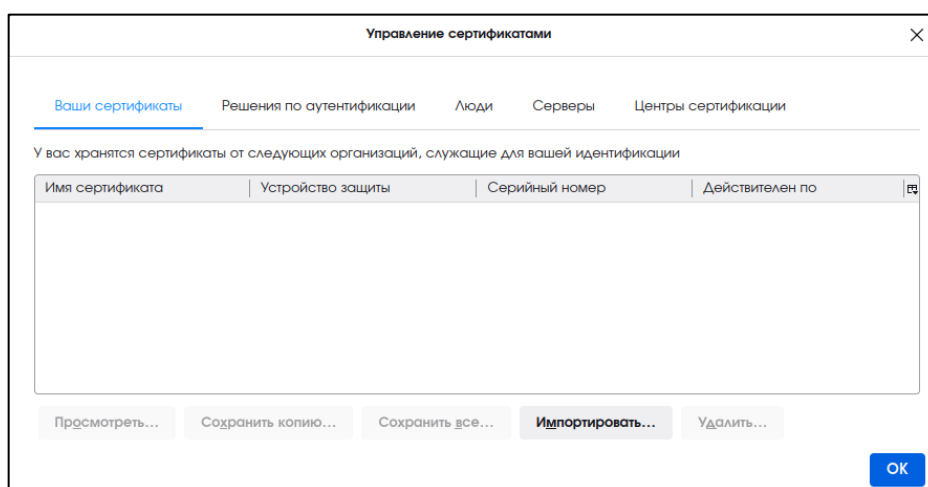


Рисунок 34 – Окно управления сертификатами

- Выберите контейнер .p12, содержащий закрытый ключ и сертификат доступа, перенесённый на жесткий диск, выпущенный для учётной записи пользователя (см. Рисунок 35).

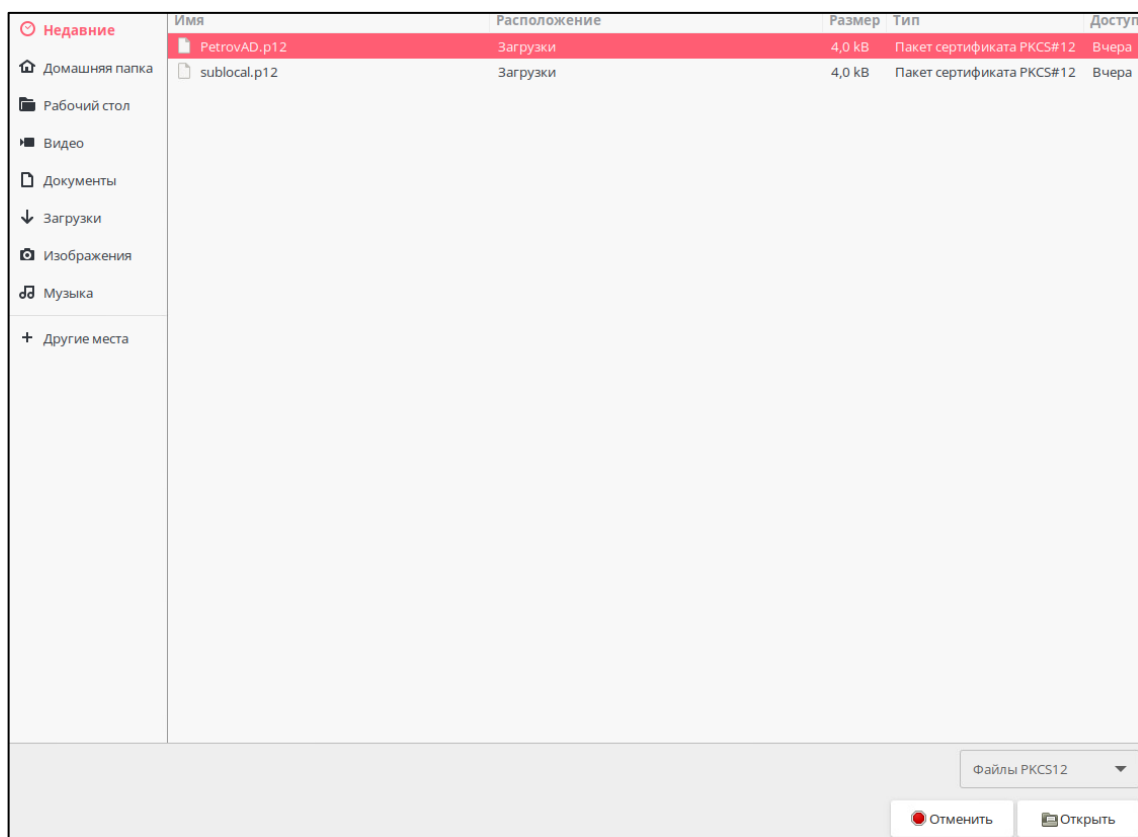


Рисунок 35 – Окно выбора импортируемого файла сертификата

- Введите PIN-код загружаемого контейнера .p12 в открывшемся окне и нажмите кнопку <Ок> (см. Рисунок 36). PIN-код сертификата является атрибутом безопасности и должен быть передан администратором с контейнером закрытого ключа и сертификата.

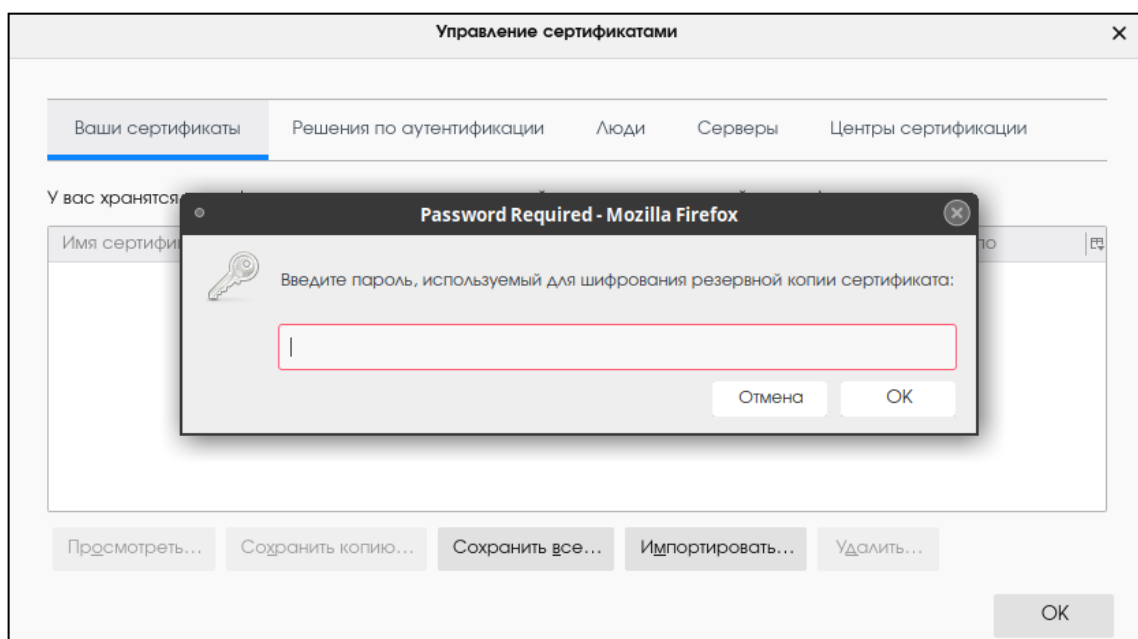


Рисунок 36 – Окно ввода PIN-кода сертификата

- В таблице окна «Управление сертификатами» появится запись об импортированном сертификате (см. Рисунок 37). Нажмите кнопку <OK>.

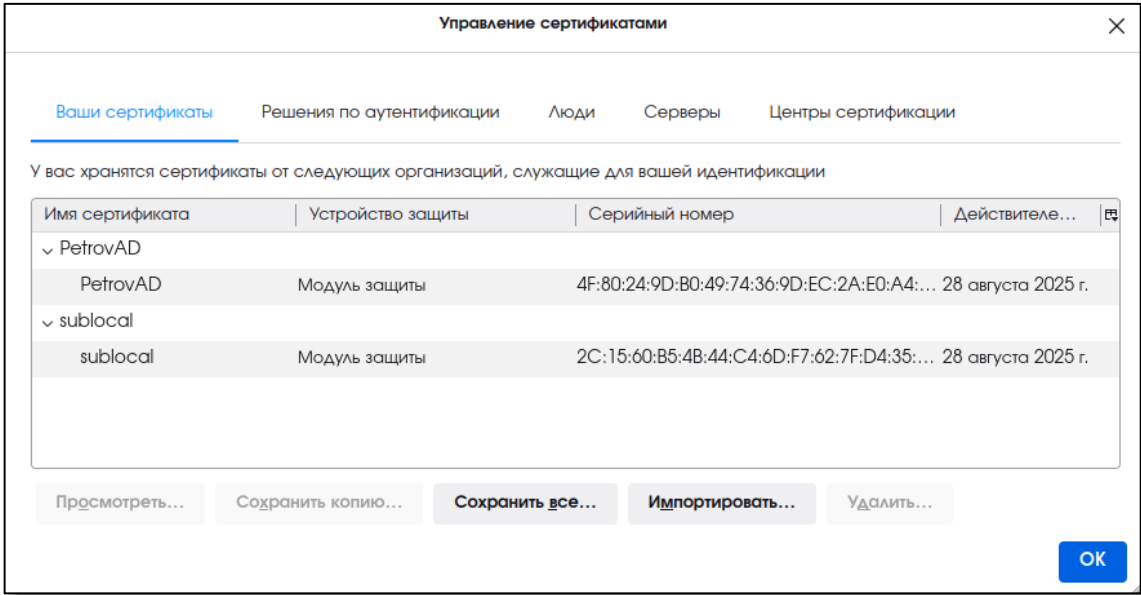


Рисунок 37 – Окно «Управление сертификатами»

- 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://172.22.5.21`

- В открывшемся окне выберите сертификат для аутентификации на веб-сервере Центра сертификации Aladdin Enterprise Certification Authority (см. Рисунок 38). Нажмите кнопку <OK>.

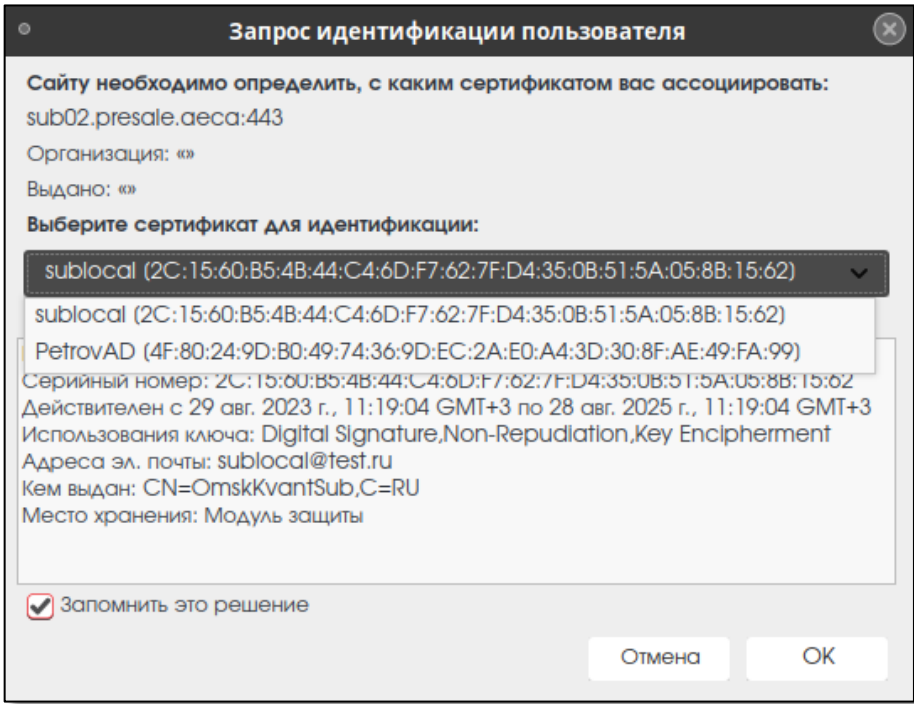


Рисунок 38 – Окно выбора сертификата для аутентификации

- Далее откроется страница с предупреждением системы безопасности (см. Рисунок 39). Нажмите кнопку <Дополнительно>.

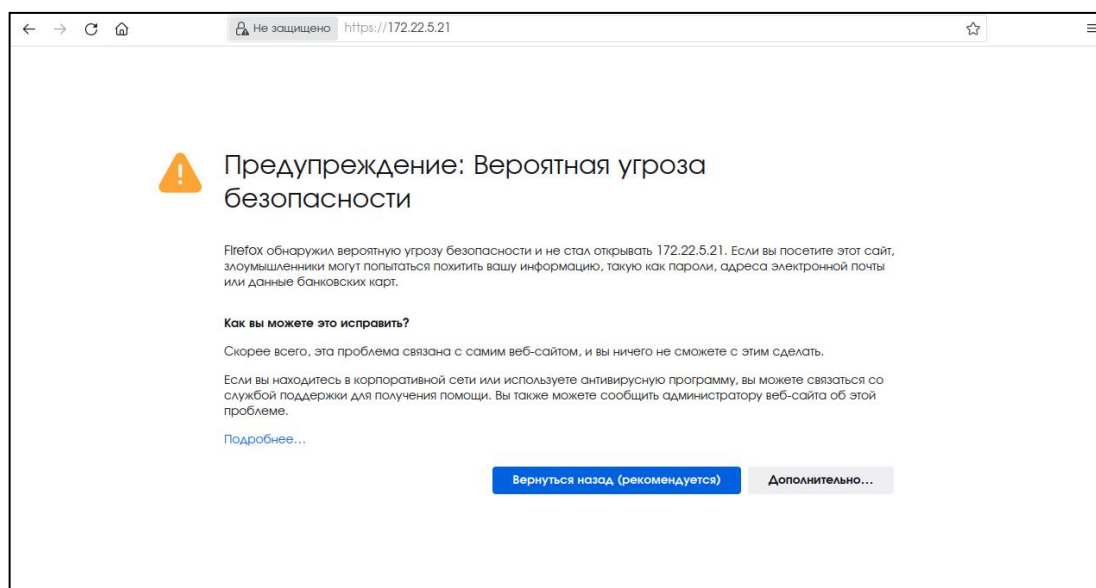


Рисунок 39 – Страница с предупреждением системы безопасности

- По нажатию кнопки <Дополнительно> на странице предупреждения системы безопасности осуществляется переход на страницу ошибки распознавания сертификата (см. Рисунок 40). Нужно принять риски, нажав кнопку <Принять риск и продолжить> на текущей странице.

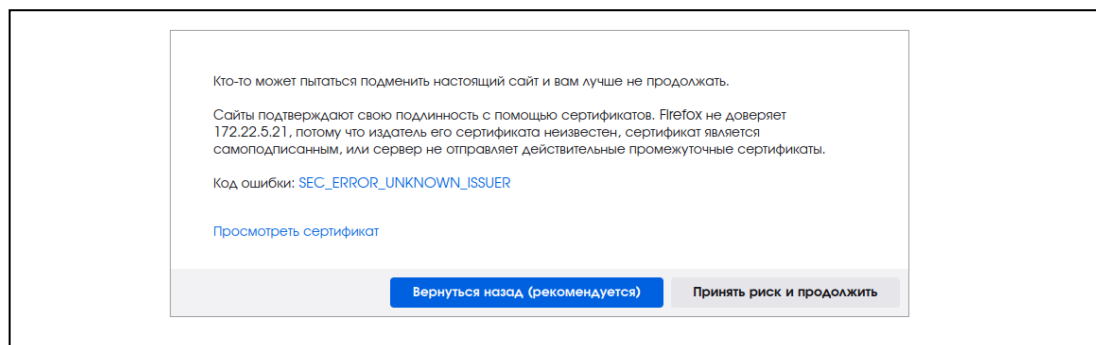


Рисунок 40 – Страница ошибки распознавания сертификата

- 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.



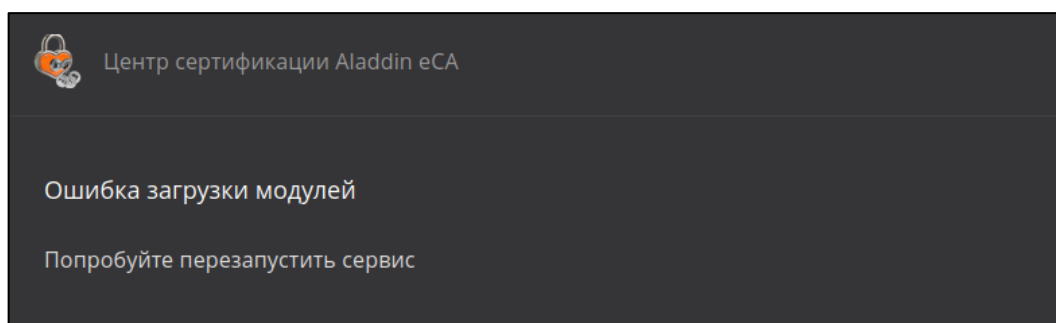


Рисунок 41 – Окно «Управление сертификатами»

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

## 4.2 Аутентификация с использованием сертификата на ключевом носителе

### 4.2.1 Настройка СВТ для двухфакторной аутентификации администратора по сертификату на ключевом носителе

Для настройки сначала выполните установку Единого Клиента JaCarta (см. подраздел 4.2.1), а затем выполните настройку браузера (настройку Firefox см. в подразделе 4.2.1.2, настройку Chromium в зависимости от ОС см. в подразделах 4.2.1.3 и 4.2.1.4).

#### 4.2.1.1 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 перейдите 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 к 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).

#### 4.2.1.2 Настройка браузера Firefox для РЕД ОС 7.3, Альт 8 СП релиз 10, Astra Linux Special Edition 1.7

- 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 `libjcpkcs11-2.so`<sup>16</sup> (см. Рисунок 42) и подтвердите загрузку модуля, нажав кнопку <ОК>;

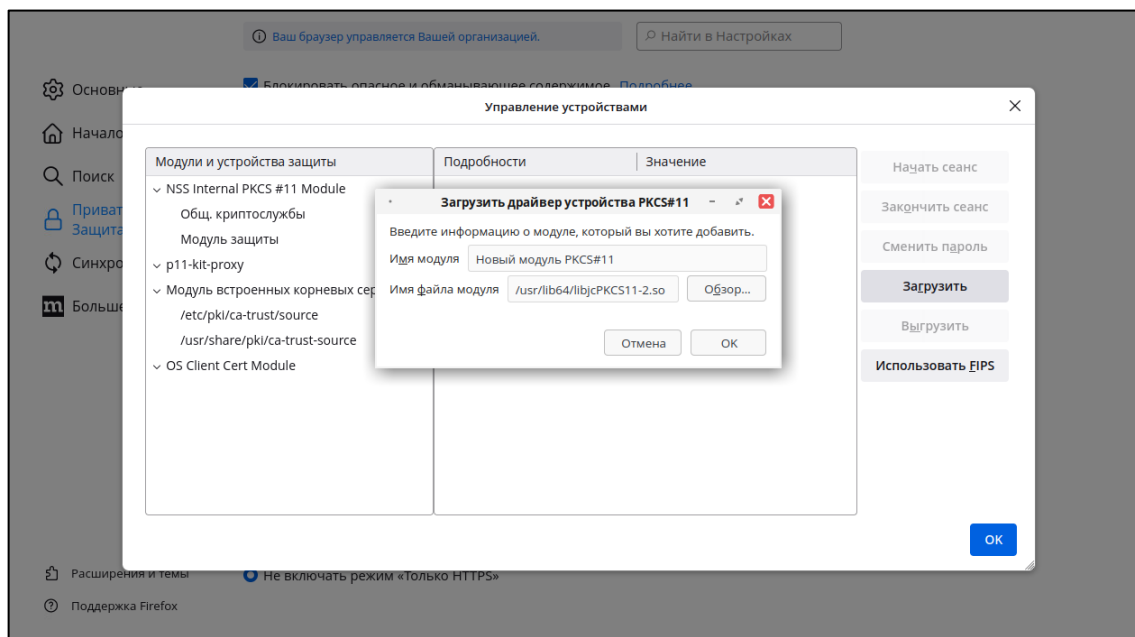


Рисунок 42 – Настройка браузера Firefox

- перезапустите браузер.

#### 4.2.1.3 Настройка браузера Chromium для РЕД ОС 7.3 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 7.3** или **Альт 8 СП, релиз 10**:
  - 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:

<sup>16</sup> Файл модуля `libjcpkcs11-2.so` создается при успешной установке Единого Клиента JaCarta (описание установки было выше в 4.2.1). В зависимости от операционной системы файл модуля может находиться в каталогах `/lib`, `/usr/lib`, `/lib64`, `/usr/lib64`. Для поиска можно использовать команду: `find {/lib,/usr/lib,/lib64,/usr/lib64} -name libjcpkcs11-2.so`. В примере файл модуля находится в каталоге `/usr/lib64` (Рисунок 42).

```
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.

#### 4.2.1.4 Настройка браузера Chromium для Astra Linux Special Edition 1.7

- Выполните настройку браузера **Chromium**, если подключение к серверу Центра сертификации Aladdin Enterprise Certification Authority будет выполнено в этом браузере посредством **Astra Linux Special Edition 1.7**:

- подключите модуль **nssdb** для работы с сертификатами, выполнив команду:

```
modutil -dbdir sql:.pki/nssdb/ -add "JaCarta" -libfile /lib/libjcpkcs11-2.so
```

- перезапустите браузер.

#### 4.2.2 Двухфакторная аутентификация администратора 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/администратора для его дальнейшей аутентификации с целью успешного подключения к серверу на клиентской стороне.
- Откройте браузер, для которого была выполнена первичная настройка двухфакторной аутентификации (согласно раздел 4.2.1 настоящего руководства), и введите в адресную строку ip-адрес или полное доменное имя сервера (в зависимости от SAN, указанного в сертификате веб-сервера), выдавшего импортированный сертификат доступа, на котором произведена установка программного компонента «Центр сертификации Aladdin Enterprise Certification Authority».

Например:

```
https://172.22.5.21
```

- В появившемся окне введите PIN-код ключевого носителя.

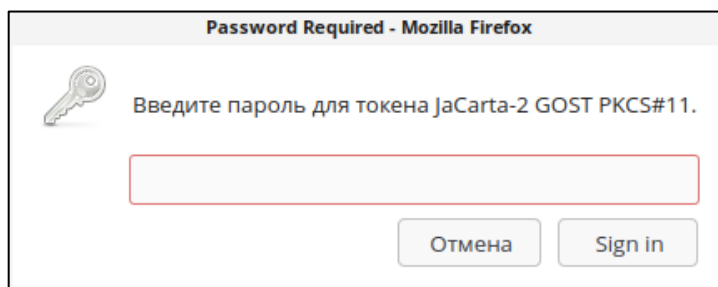


Рисунок 43 – Окно ввода PIN-кода ключевого носителя

- В появившемся окне выберите сертификат с подключенного ключевого носителя.

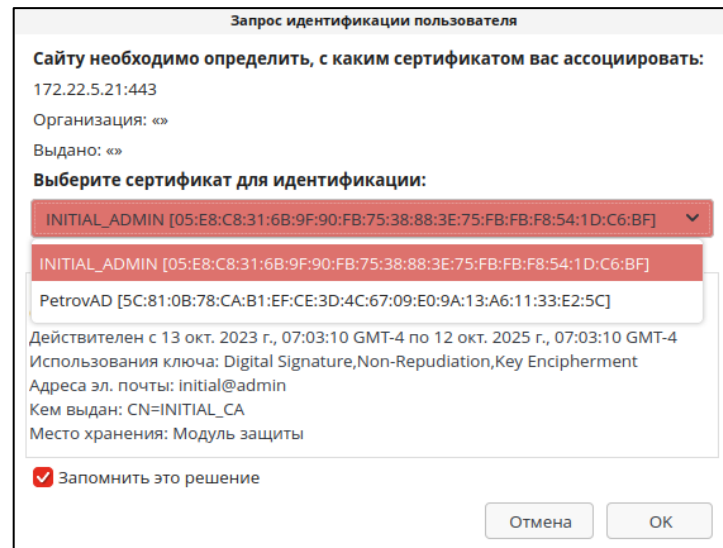


Рисунок 44 – Окно выбора сертификата пользователя для аутентификации на сервере

**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.**

## 5 БЕЗОПАСНОСТЬ СОЕДИНЕНИЯ

Подключение клиента к серверу Центра сертификации выполняется по протоколу TLS, который предоставляет зашифрованный обмен данными и проверку подлинности конечной точки.

Протокол TLS позволяет авторизованным пользователям (администраторам/операторам) клиентской части программы проходить проверку подлинности серверов Центров сертификации, к которым они подключаются. При подключении по протоколу TLS клиент запрашивает действительный сертификат у сервера. Common Name сертификата или значение записи DNS name в разделе Subject Alternative Name должно соответствовать имени веб-сервера. Результатом установки соединения является доверенное подключение и защищенный обмен трафиком между клиентом (авторизованным пользователем) и сервером.

### 5.1 Настройка доверенного соединения

Для настройки доверенного соединения:

- Подготовьте сертификаты Центров сертификации, на основе которых строится цепочка доверия сертификатам, или цепочку сертификатов Центра сертификации, с которым требуется установить безопасное соединение (см. пункт 7.3.1.1 настоящего руководства).
- Установите сертификаты Центров сертификации цепочки доверия в доверенное хранилище браузера. Процесс установки сертификатов рассмотрим на примере браузера Firefox:
  - Откройте браузер Firefox – Настройки – Приватность и Защита – Сертификаты (см. Рисунок 45). Нажмите кнопку <Просмотр сертификатов>.

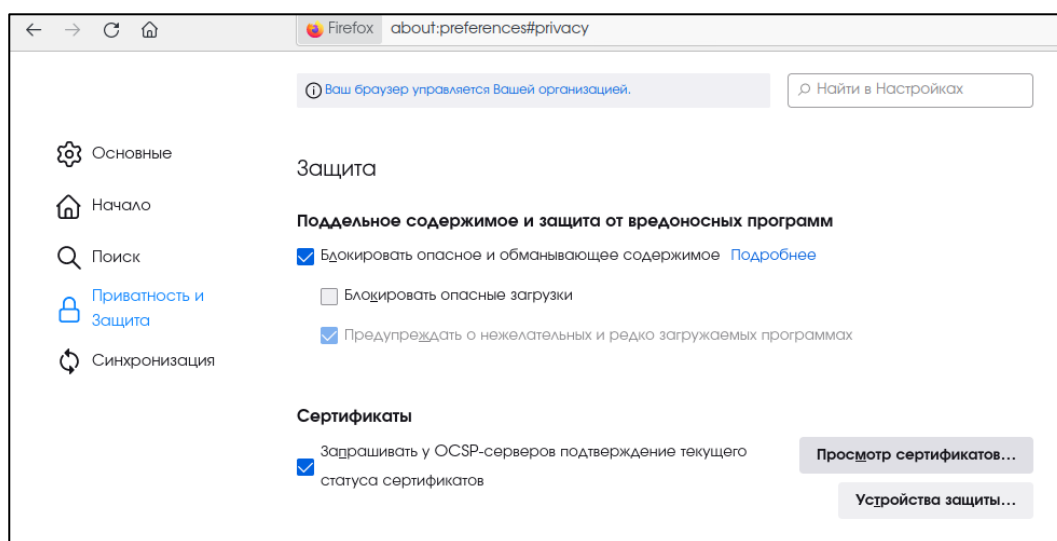


Рисунок 45 – Окно настроек браузера

- Выберите вкладку «Центры сертификации», в открывшейся вкладке нажмите кнопку <Импортировать> и выберите предварительно подготовленный сертификат Центра сертификации, проставьте флажки в чек-боксах «Доверять при идентификации веб-сайтов» и «Доверять при идентификации пользователей электронной почты». Поочерёдно импортируйте все сертификаты Центров сертификации, участвующие в построении цепочки доверия (см. Рисунок 46) или импортируйте цепочку сертификатов.

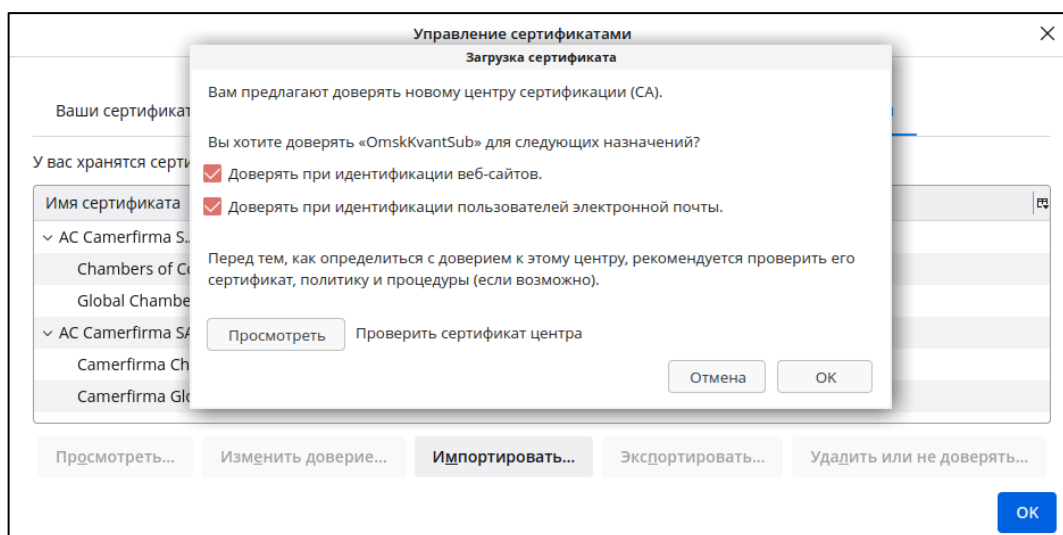


Рисунок 46 – Окно управления сертификатами

- Выпустите (см. пункт 7.4.1 настоящего руководства) для локального субъекта веб-сервера и установите сертификат веб-сервера (см. пункт 7.13.1 настоящего руководства), если это не сделано ранее.
- Перезапустите браузер.
- Для безопасного доверенного соединения при обращении к серверу Центра сертификации используйте доменное имя (см. Рисунок 47), указанное в атрибуте сертификата веб-сервера Subject alternative name (SAN) (см. Рисунок 48) и соответственно указанное в конфигурационном файле `/etc/hosts/` сервера.

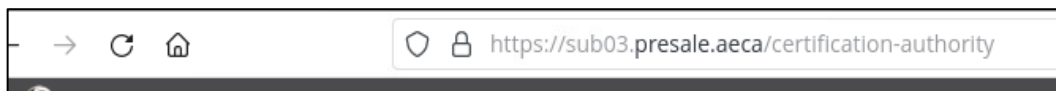


Рисунок 47 – Адресная строка в браузере

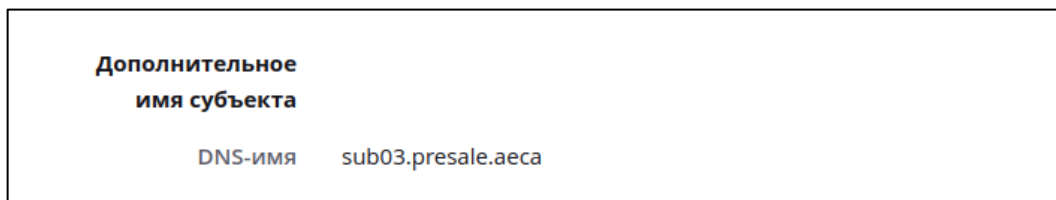


Рисунок 48 – Сертификат веб-сервера

## 6 ТЕХНОЛОГИЧЕСКИЕ СОСТАВЛЯЮЩИЕ ПРОГРАММЫ

### 6.1 Назначение технологических составляющих

Технологические составляющие программного компонента «Центр сертификации Aladdin Enterprise Certification Authority» создаются автоматически, с целью первичного запуска программного компонента «Центр сертификации Aladdin Enterprise Certification Authority».

### 6.2 Установка и настройка технологических составляющих

- Перед установкой программного компонента «Центр сертификации Aladdin Enterprise Certification Authority» возможно задать в файле конфигурации `/opt/aecaCa/scripts/config.sh` переменные окружения, используемые сервисом «settings-service» (см. Руководство администратора. Часть 1. Установка):
  - параметры технологического Центра сертификации;
  - криптографические параметры сертификата технологического ЦС;
  - задание параметров учётной записи;
  - криптографические параметры сертификата учётной записи администратора;
  - криптографические параметры сертификата Веб-сервера.
- В процессе установки программного компонента «Центр сертификации Aladdin Enterprise Certification Authority» будут автоматически созданы технологические компоненты:
  - технологический Центр сертификации «INITIAL\_CA» (по умолчанию);
  - локальные субъекты (локальный субъект веб-сервера и учётная запись администратора инициализации).
- Для технологических компонентов автоматически создаются:
  - учётная запись администратора инициализации «INITIAL\_ADMIN» (по умолчанию);
  - сертификат технологического Центра сертификации «INITIAL\_CA» (по умолчанию) со сроком действия 24 года;
  - сертификат учётной записи администратора «INITIAL\_ADMIN» (по умолчанию) со сроком действия 2 года;
  - сертификат веб-сервера со сроком действия 2 года.
- После завершения развёртывания программного компонента «Центр сертификации Aladdin Enterprise Certification Authority» в каталоге `/opt/aecaCa/dist/certificates/account/INITIAL_ADMIN.p12` будет размещён сертификат администратора инициализации INITIAL\_ADMIN.p12, необходимый для дальнейшей аутентификации на веб-сервере. PIN-код сертификата администратора, заданный по умолчанию в конфигурационном файле `config.sh`, «INITIAL».
- Первичная авторизация в открывшемся интерфейсе установленного программного компонента «Центр сертификации Aladdin Enterprise Certification Authority» по умолчанию выполняется под учётной записью «INITIAL\_ADMIN» с правами администратора.
- В открывшемся интерфейсе программного средства «Центр сертификации Aladdin Enterprise Certification Authority» отображены:
  - Сертификат технологического Центра сертификации в разделе «Центр сертификации» на вкладке «Свои сертификаты».

- Учётная запись «INITIAL\_ADMIN» в разделе «Учётные записи». Технологическая учётная запись имеет неограниченные права;
- Субъекты локальной ресурсной системы в разделе «Субъекты»;
- Веб-сервер и Издатель в разделе «Настройка».

### 6.3 Удаление технологических составляющих

**Внимание! Нарушение нижеприведённого порядка удаления технологических составляющих, созданных при развёртывании Центра сертификации, может привести к ошибкам и/или полному блокированию доступа к программному компоненту «Центр сертификации Aladdin Enterprise Certification Authority».**

Для удаления технологических составляющих, необходимых для первичного запуска программного компонента «Центр сертификации Aladdin Enterprise Certification Authority», после развёртывания Центра сертификации и загрузки лицензии, выполните следующие действия:

- 1) Выпустите и импортируйте сертификат для созданного подчинённого Центра сертификации в состоянии «Запрос» (согласно пунктам о и 7.3.1.6 настоящего руководства).
- 2) Удостоверьтесь в том, что созданный Центр сертификации активирован.
- 3) Создайте учётную запись с ролью «Администратор» (см. пункт 7.6.1 настоящего руководства).
- 4) Выпустите сертификат для созданной учётной записи (см. пункт 7.6.7 настоящего руководства).
- 5) Выполните аутентификацию по выпущенному сертификату учётной записи (см. раздел 7.3.1.7 Руководства администратора. Часть 1. Установка).
- 6) Выключите проверку издателя технологического Центра сертификации (см. пункт 7.13 настоящего руководства).
- 7) Выпустите сертификат веб-сервера, сохранив контейнер с ключевой парой (сертификат и закрытый ключ) в формате PKCS#12 (см. пункт 7.4.1 настоящего руководства).
- 8) Выполните смену ключей веб-сервера в целях безопасности (см. пункт 7.13.1 настоящего руководства).
- 9) Удалите технологический Центр сертификации (см. пункт 7.3.1.7 настоящего руководства).

### 6.4 Восстановление доступа к программе в случае некорректного удаления технологических составляющих и/или блокировки доступа

В случае блокировки доступа к программному компоненту «Центр сертификации Aladdin Enterprise Certification Authority», возникшей в результате некорректного удаления технологических составляющих, восстановление доступа возможно произвести двумя способами:

- восстановление из резервной копии (см. раздел 9 Руководства администратора. Часть 1. Установка и обслуживание Центра сертификации Aladdin Enterprise Certification Authority);
- восстановление технологических составляющих (см. раздел 10 Руководства администратора. Часть 1. Установка и обслуживание Центра сертификации Aladdin Enterprise Certification Authority).



## 7 ФУНКЦИИ УПРАВЛЕНИЯ ПРОГРАММЫ

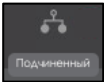
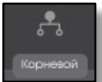
### 7.1 Верхняя панель «Центра сертификации Aladdin Enterprise Certification Authority»


Верхняя панель (см. Рисунок 49) Центра сертификации фиксирована и отображается на любом шаге или переходе между разделами.



Рисунок 49 – Верхняя панель окна «Центра сертификации»


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

- 








- 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»;

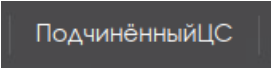

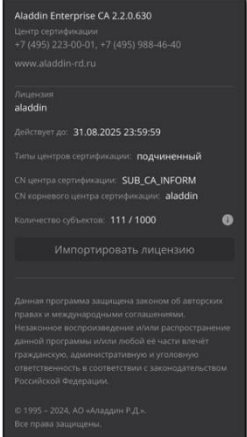
Индикатор «треугольник с восклицательным знаком» присутствует в следующих случаях:

  - истёк срок действия сертификата текущего активного ЦС . При наведении курсора отображается всплывающее сообщение «Истек срок действия сертификата ЦС»;
  - истекает<sup>17</sup> срок действия сертификата текущего активного ЦС . При наведении курсора отображается всплывающее сообщение «Истекает срок действия сертификата ЦС»;
  - закрытый ключ ЦС недоступен<sup>18</sup> . 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 субъектов с действующими сертификатами . При наведении курсора отображается всплывающее сообщение «Достигнуто предельное количество субъектов с действующими сертификатами по лицензии».
- 

- имя текущего активного ЦС, заданное в применённой лицензии (не изменяемое). При наведении курсора всплывают заданные имя и значения суффикса различающегося имени ЦС;



<sup>17</sup> До истечения остаётся менее 90 дней.

<sup>18</sup> 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.

-  - отображаемое имя текущего активного ЦС (задаётся при первичной активации лицензии);
-  - текущая авторизация учётной записи пользователя;
-  - сведения о текущей версии программного компонента, контактная информация разработчика, информация о лицензии.  
По нажатию на кнопку <Импортировать лицензию> возможно загрузить обновление лицензии.

## 7.2 Боковая панель «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 50) или компактном (см. Рисунок 51) 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).

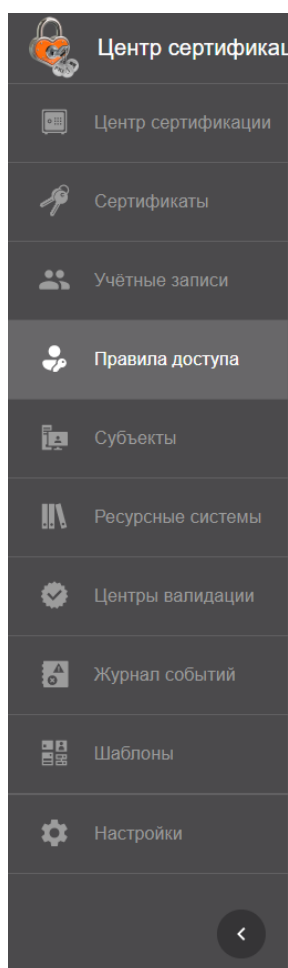


Рисунок 50 – Полный вид боковой панели



Рисунок 51 – Компактный вид боковой панели

Боковая панель состоит из разделов, определяющих соответствующие функции «Центра сертификации Aladdin eCA», и создана для организации управления Центром сертификации:

- Раздел «Центр сертификации» – в данном разделе возможно:
  - выпустить сертификат Центра сертификации;
  - подписать запрос на выпуск сертификата Подчиненного Центра сертификации;
  - скачать цепочку сертификатов активного Центра сертификации;
  - скачать сертификат Корневого и Подчиненного ЦС в формате .pem;
  - отозвать сертификат Подчиненного ЦС;
  - посмотреть карточку Центра сертификации;
- Раздел «Сертификаты» – в данном разделе возможно:
  - выпустить сертификат с закрытым ключом PKCS#12 для субъекта;
  - выпустить сертификат на основании запроса для субъекта;
  - выпустить сертификат на ключевом носителе для субъекта;
  - посмотреть список всех выпущенных сертификатов субъектов, выпущенных активным ЦС, с отображением статуса сертификата, срока действия, типа субъекта, имени субъекта и серийного номера сертификата;
  - произвести поиск выпущенных сертификатов по имени субъекта;
  - отозвать или приостановить действие выпущенного сертификата субъекта;

- посмотреть карточку выпущенного сертификата субъекта;
- скачать сертификат субъекта в формате .pem;
- скачать цепочку сертификатов;
- скачать текущий CRL;
- скачать список всех выпущенных сертификатов в формате .csv;
- применить массовые операции к выбранным сертификатам (отзыв, приостановка, возобновление);
- Раздел «Учетные записи» – в данном разделе возможно:
  - создать новую учетную запись;
  - отредактировать существующую учетную запись;
  - заблокировать или активировать существующую учетную запись;
  - задать группы, на которые предоставляются права для управления сертификатами субъектов, для учетной записи, выполняющей роль «Оператор»;
  - выпустить сертификат для пользователя учётной записи;
- Раздел «Правила доступа» – в данном разделе возможно:
  - просмотреть существующие правила доступа;
  - создать новое правило доступа;
  - отредактировать правило доступа;
  - удалить правило доступа.
- Раздел «Субъекты» – в данном разделе возможно:
  - произвести поиск субъекта по его имени (или части имени);
  - обновить список групп и субъектов;
  - посмотреть существующие субъекты;
  - создать новый локальный субъект;
  - выпустить сертификат с закрытым ключом PKCS#12 для субъекта;
  - выпустить сертификат по запросу 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;
- Раздел «Ресурсная система» – в данном разделе возможно:
  - подключить ресурсную систему для управления сертификатами доменных пользователей и других субъектов;
  - обновить список субъектов ресурсной системы и их данных в ручном режиме.
- Раздел «Центры валидации» – в данном разделе возможно:
  - настроить параметры рассылки CRL/Delta CRL;
  - скачать CRL;
  - обновить CRL по нажатию кнопки;
  - просмотреть список уже зарегистрированных Центров валидации;
  - зарегистрировать сторонние Центры валидации;
  - создать Центр валидации Aladdin Enterprise Certificate Authority;

- объединить точки распространения или службы OCSP в кластер;
- Раздел «Журнал событий» – в данном разделе возможно:
  - посмотреть в интерактивном режиме полный или выборочный (с применением фильтров) журнал событий;
  - скачать журнал событий в формате .csv по выбранным параметрам экспорта.
- Раздел «Шаблоны» – в данном разделе отображены предустановленные шаблоны сертификатов. Возможно выполнение следующих операций с шаблонами сертификатов:
  - клонирование;
  - редактирование загруженных и созданных шаблонов сертификатов;
  - удаление шаблонов (кроме предустановленных);
  - отображение списка шаблонов;
  - загрузка шаблонов сертификатов MSCS.
- Раздел «Настройки» – в данном разделе производится:
  - настройка аутентификации при подключении к веб-серверу;
  - замена сертификата текущего веб-сервера;
  - управление списком подключенных Syslog-серверов.

Далее в настоящем документе приводится полное описание доступных функций управления Центром сертификации для каждого раздела.

## 7.3 Раздел «Центр сертификации»

Переход на экран управления центра сертификации осуществляется по выбору раздела «Центр сертификации» бокового меню, расположенного слева на главном экране (см. Рисунок 50).

Раздел «Центр сертификации» управления центром сертификации в правом поле экрана содержит вкладки «Свои сертификаты» (управление собственными Корневыми и Подчиненными центрами сертификации) и «Сертификаты подчиненных центров» (работа с Подчиненными центрами сертификации нижнего уровня).

Данный раздел доступен только пользователю с ролью «Администратор».

### 7.3.1 Вкладка «Свои сертификаты»

Вид раздела «Центр сертификации» – вкладка «Свои сертификаты» показан на рисунке ниже (Рисунок 52).

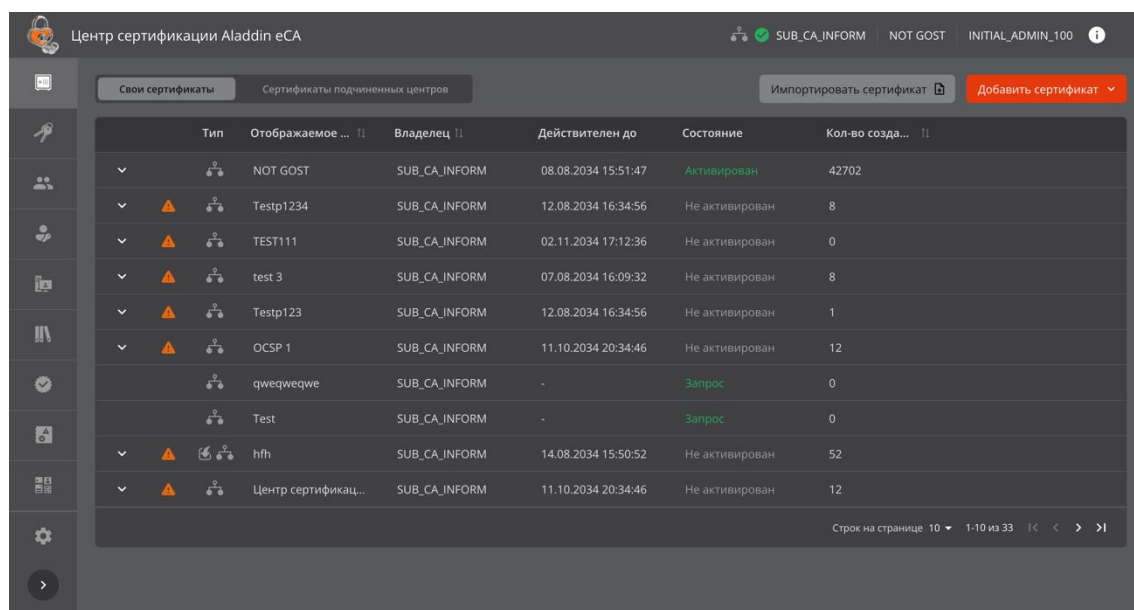


Рисунок 52 - Экран раздела "Центр сертификации" – вкладка «Свои сертификаты»

- На данной вкладке после инициализации отображены сертификат технологического центра сертификации, создаваемый по умолчанию при установке Центра сертификации Aladdin eCA, и сертификат центра сертификации, созданный при инициализации.
- Сертификаты центров сертификации в формате `.pem` хранятся в базе данных (имя базы данных по умолчанию, конфигурация базы данных указана в файле `/opt/aecaCa/scripts/config.sh`).
- Открытый и закрытый ключи центров сертификации хранятся в контейнере PKCS#12 по умолчанию в каталоге `/opt/aeca/cryptotoken`, если не изменена конфигурация развёртывания в конфигурационном файле `/opt/aecaCa/scripts/config.sh`.
- Пароль контейнера PKCS#12 хранится в базе данных в зашифрованном по алгоритму AES256 виде (имя базы данных по умолчанию, конфигурация базы данных указана в файле `/opt/aecaCa/scripts/config.sh`).
- Для сертификата центра сертификации из категории «Свои сертификаты», имеющего статус «активный», доступны настройки, в том числе создание и перенастройка сервисов публикации CRL DP и службы OCSP в разделе «Центры валидации».
- Таблица на вкладке «Свои сертификаты» содержит следующие поля:
  - индикатор «Обратить внимание на ЦС» – отображается только при наличии проблем у данного центра сертификации. Подробнее см. в таблице ниже (Таблица 8);
  - тип – тип центра сертификации:
    - – для корневого ЦС;
    - – для подчиненного ЦС;

Если центр сертификации был создан с импортом ключа из контейнера PKCS#12, то поле содержит иконку-префикс – «Импортированный» тип ключа.

- отображаемое имя;
- владелец;
- действителен до – срок действия сертификата (дата и время):







- если до истечения срока действия остается менее 90 дней, то цвет значения – оранжевый и рядом отображается индикатор , при наведении курсора отображается всплывающая подсказка «Осталось менее 90 дней до истечения»;
- для сертификатов с истекшим сроком действия цвет значения – красный и рядом отображается индикатор , при наведении курсора отображается всплывающая подсказка «Сертификат истек».
- алгоритм ключа;
- длина ключа;
- состояние – состояние центра сертификации:
  - активирован;
  - запрос;
  - отозван;
  - истёк срок;
  - не активирован.
- количество созданных – количество созданных сертификатов доступа независимо от статуса сертификатов.

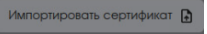

Таблица 8 – Причины отображения индикатора «Обратить внимание на ЦС»


Тип	Причина отображения
 Ошибка	Если истёк срок действия сертификата центра сертификации. При наведении курсора на индикатор отображается всплывающее сообщение «Истек срок действия сертификата ЦС»
 Ошибка	Если закрытый ключ центра сертификации недоступен. При запуске серверного компонента Центра сертификации Aladdin eCA не удалось получить закрытый ключ данного центра сертификации, 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 центра сертификации.
 Ошибка	Если закрытый ключ центра сертификации находится в состоянии «Ключ экспортирован». При наведении курсора на индикатор отображается всплывающее сообщение «Закрытый ключ центра сертификации недоступен».
 Ошибка	Если до истечения срока действия сертификата центра сертификации остается менее 90 дней. При наведении курсора на индикатор отображается всплывающее сообщение «Истекает срок действия сертификата ЦС».

- Для управления центрами сертификации администратору доступны действия, приведённые в таблице ниже (Таблица 9).

Таблица 9 – Возможные операции, совершаемые над ЦС на вкладке «Свои сертификаты»

Операция	ЦС в состоянии «Запрос»	ЦС в состоянии «Активирован»	ЦС в состоянии «Не активирован»	Необходимое действие для выполнения операции
Скачать сертификат	-	+	+	Выделить сертификат и нажать кнопку  «Скачать»
Скачать цепочку сертификатов	-	+	+	
Скачать список отозванных сертификатов	-	+	+	

Операция	ЦС в состоянии «Запрос»	ЦС в состоянии «Активирован»	ЦС в состоянии «Не активирован»	Необходимое действие для выполнения операции
Скачать запрос на сертификат	+	-	-	
Удалить центр сертификации	+	-	+	Выделить сертификат и нажать кнопку  <Удалить>
Импортировать сертификат	+	-	-	Выделить сертификат и нажать кнопку  <Загрузить> или кнопку 
Просмотр цепочки сертификатов	-	+	-	Выделить сертификат и нажать кнопку  в строке слева от имени сертификата
Просмотр карточки сертификата	-	+	+	Нажать на строку сертификата в экранной таблице
Смена состояния (активировать)	-	-	+	выделить сертификат и нажать кнопку  <Активировать> в строке экранной таблицы или карточке сертификата <sup>19</sup>

- Технологический центр сертификации может быть удалён после выпуска и загрузки нового сертификата для текущего сервера (см. подраздел 6.3 настоящего руководства).
- На вкладке «Свои сертификаты» по нажатию на кнопку  доступны функции добавления нового сертификата Центра сертификации, созданного при инициализации на основании текущей лицензии. Добавленный сертификат может служить заменой текущего активного центра сертификации в случае компрометации его закрытого ключа.
  - Для добавления сертификата центра сертификации с созданием ключа выберите опцию «Создать ключ» (подробнее см. раздел 7.3.1.2);
  - Для добавления сертификата ЦС с импортом внешнего ключа из контейнера PKCS#12 выберите опцию «Импорт внешнего ключа» (подробнее см. раздел 7.3.1.2).

### 7.3.1.1 Карточка сертификата ЦС

- Переход к экрану «Карточка сертификата ЦС» осуществляется при нажатии на строку сертификата таблицы на вкладке «Свои сертификаты» в состоянии «Активирован» или «Не активирован» (см. Рисунок 53 и Рисунок 54).
- В карточке активного ЦС доступны следующие действия (см. Рисунок 53):
  - выгрузить сертификат, цепочку сертификатов или текущий список отозванных сертификатов по нажатию кнопки <Скачать>;
  - удалить Центр сертификации по нажатию кнопки <Удалить>.

<sup>19</sup> При успешной активации центра сертификации в журнале событий регистрируется запись с кодом CAENV008.



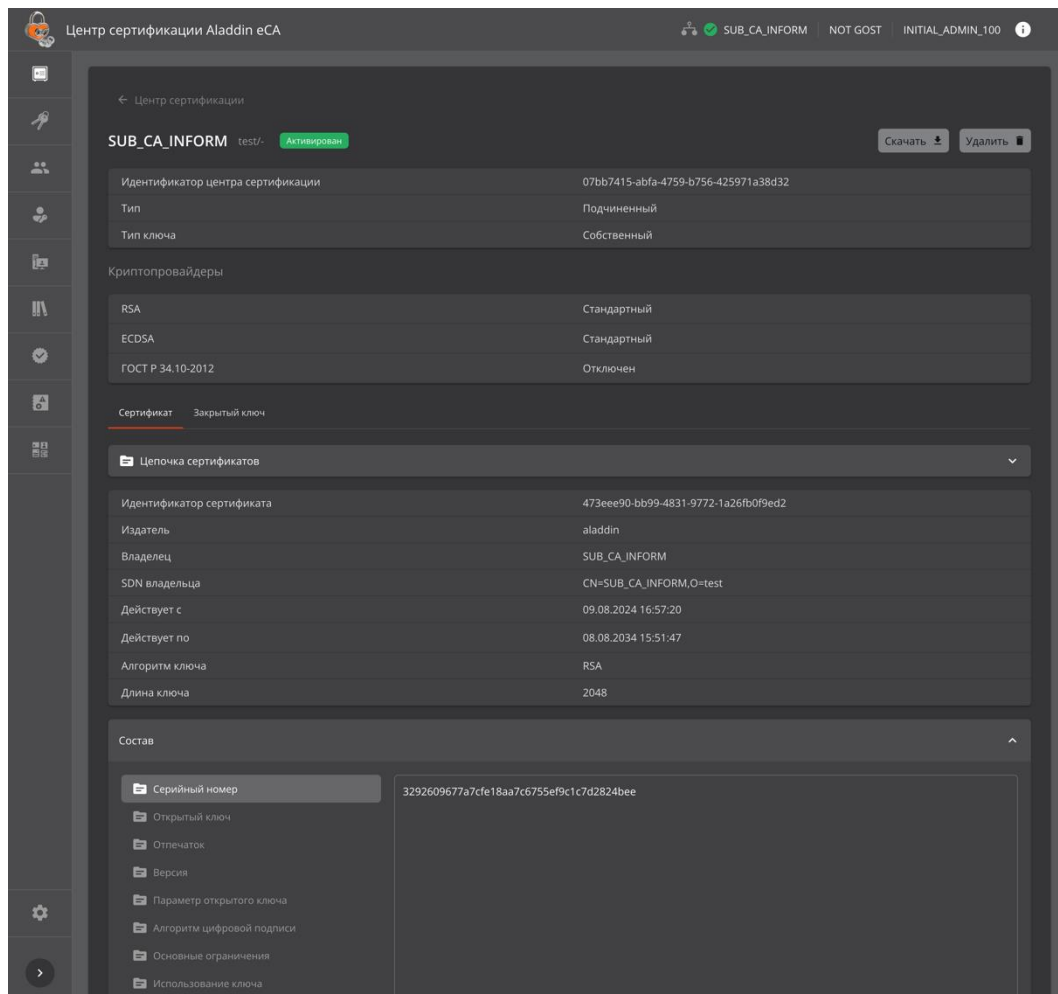


Рисунок 53 – Карточка центра сертификации в состоянии «Активирован»

- В карточке неактивного центра сертификации доступны следующие действия (Рисунок 54):
  - выгрузить сертификат, цепочку сертификатов или текущий список отозванных сертификатов по нажатию кнопки <Скачать>;
  - удалить центр сертификации по нажатию кнопки <Удалить>;
  - активировать центр сертификации<sup>20</sup>.

<sup>20</sup> При успешной активации центра сертификации будет произведена запись события CAENV008 в Журнал событий.

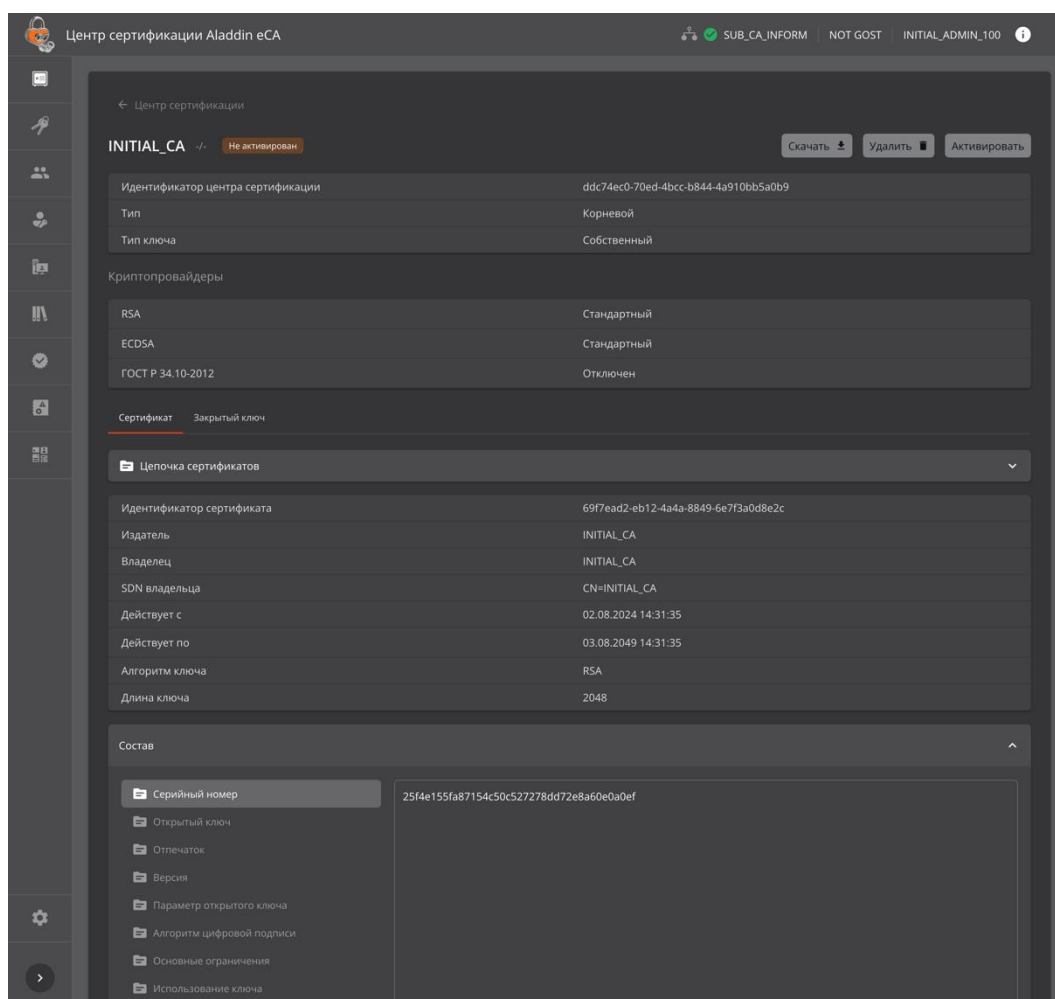




Рисунок 54 – Карточка центра в состоянии «Не активирован»

- В карточке центра сертификации отображаются следующие сведения:
  - В заголовке карточки:
    - Отображаемое имя центра сертификации;
    - Состояние центра сертификации;
    - Индикатор «Обратить внимание на ЦС» – отображается только при наличии проблем у данного центра сертификации (Таблица 8).
  - идентификатор центра сертификации;
  - тип - тип центра сертификации (корневой или подчиненный);
  - тип ключа:
    - собственный – ключевая пара была создана при инициализации центра сертификации;
    - импортированный – ключевая пара была импортирована из контейнера PKCS#12;
  - Подраздел «Криптопровайдеры», отображающий выбранных при создании данного центра сертификации криптопровайдеров алгоритмов. В случае, если криптопровайдер недоступен, слева от его названия отображается индикация «треугольник с восклицательным знаком», при наведении на которую отображается всплывающее сообщение «Криптопровайдер недоступен»;
  - Вкладка «Сертификат», содержащая:
    - Раскрывающийся список (дерево) «Цепочка сертификатов»;

- Сведения о сертификате центра сертификации в табличной форме, содержащие следующие строки в формате «ключ – значение»:
  - Идентификатор сертификата (значение в данном поле соответствует идентификатору сертификата данного центра сертификации);
  - Издатель (поле «Issuer» сертификата);
  - Владелец (атрибут «CN» из поля «Subject» сертификата);
  - SDN издателя (значение поля «Subject» сертификата);
  - Действует с (атрибут «Not Before» из поля «Validity» сертификата);
  - Действует по (атрибут «Not After» из поля «Validity» сертификата):
    - если до истечения остается менее 90 дней, то цвет значения – оранжевый и рядом отображается индикатор , при наведении курсора отображается всплывающая подсказка «Осталось менее 90 дней до истечения»;
    - для истекших сертификатов цвет значения – красный и рядом отображается индикатор , при наведении курсора отображается всплывающая подсказка «Сертификат истек».
  - Алгоритм ключа (атрибут «Public Key Algorithm» из поля «Subject Public Key Info» сертификата);
  - Длина ключа (атрибут «Public Key Algorithm» из поля «Subject Public Key Info» сертификата);
- Раскрывающийся список «Состав», содержащий следующую информацию о полях сертификата ЦС:
  - Серийный номер (поле «Serial Number» сертификата);
  - Открытый ключ (поле «Subject Public Key Info»);
  - Отпечаток (вычисляемое значение, отсутствует в сертификате);
  - Версия (поле «Version» сертификата);
  - Параметр открытого ключа (всегда «X509»);
  - Алгоритм цифровой подписи (поле «Signature Algorithm»);
  - Основные ограничения (поле «X509v3 Basic Constraints»);
  - Использование ключа (поле «X509v3 Key Usage» сертификата);
  - Доступ к информации о центре сертификации (поле «Authority Information Access»);
  - Альтернативное имя субъекта (поле «X509v3 Subject Alternative Name» сертификата);
  - Идентификатор ключа центра (поле «X509v3 Authority Key Identifier» сертификата);
  - Идентификатор ключа субъекта (поле «X509v3 Subject Key Identifier» сертификата);
  - Расширенное использование ключа (поле «X509v3 Extended Key Usage» сертификата).
- Вкладка «Закрытый ключ», содержащая:
  - Кнопку для экспорта/импорта закрытого ключа ЦС;
    - Для центра сертификации в состоянии «Не активирован» кнопка называется <Экспортировать ключ>, если в поле «Состояние» на вкладке «Закрытый ключ» указано значение «Доступен» и в поле «Экспорт ключа» указано значение «Разрешен»;

- Для центра сертификации с состоянием закрытого ключа «Ключ экспортирован» кнопка называется <Импортировать ключ>.
- Иначе кнопка для экспорта/импорта закрытого ключа ЦС не отображается на вкладке «Закрытый ключ».
- Алгоритм ключа - название алгоритма ключевой пары центра сертификации;
- Длина ключа - длина закрытого ключа центра сертификации;
- Место хранения - место хранения закрытого ключа центра сертификации:
  - Локальное хранилище Aladdin eCA;
  - КриптоПро CSP (HDIMAGE);
  - КриптоПро HSM

Для центра сертификации с состоянием закрытого ключа «Ключ экспортирован» в данном поле указан прочерк (символ «-»).


- Экспорт ключа – возможность экспорта закрытого ключа центра сертификации:
  - Разрешен;
  - Запрещен.

Для центра сертификации в состоянии «Ключ экспортирован» в данном поле прочерк (символ «-»).

- Состояние - состояние закрытого ключа центра сертификации:
  - Доступен;
  - Недоступен;
  - Экспортирован.

### 7.3.1.2 Создание Корневого Центра сертификации с генерацией ключа

Предварительно для создания Корневого ЦС необходимо использование лицензии на Корневой ЦС. Новый Корневой ЦС будет создаваться на основании текущей лицензии. Для создания Корневого ЦС следует выполнить шаги ниже.

- На вкладке «Свои сертификаты» нажмите кнопку  <Добавить сертификат> и в выпадающем списке выберите опцию «Создать ключ».
- Если текущая лицензия позволяет создание корневого и подчиненного ЦС, то отобразится модальное окно «Окно инициализации корневого центра сертификации. Шаг 1/5» с шагом выбора лицензии (см. Рисунок 55). Для инициализации Корневого Центра сертификации необходимо выбрать тип «Корневой» и нажать на кнопку <Продолжить>.

Если в поле «Типы центров сертификации» указано значение «корневой», то данный шаг пропускается.

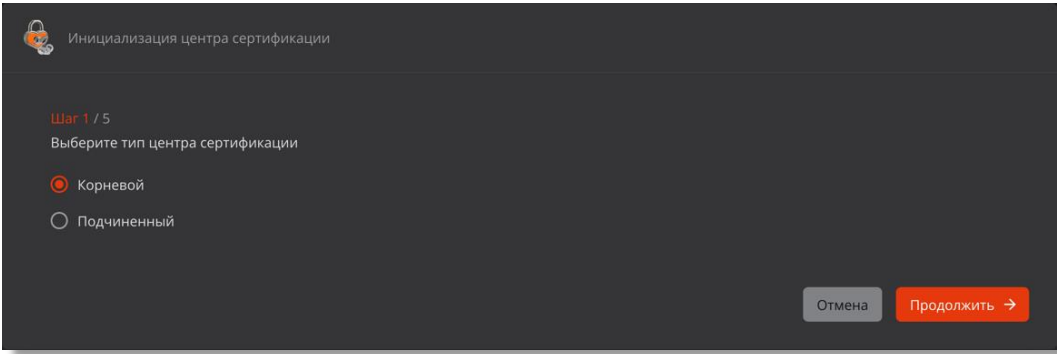


Рисунок 55 – Окно инициализации центра сертификации. Шаг 1/5 . Выбор типа центра сертификации

- На шаге 2/5 (см. Рисунок 56) заполните поля:
  - «Отображаемое имя» – введите имя создаваемого центра сертификации, которое будет отображаться в интерфейсе ЦС Aladdin eCA. Оно может содержать буквы латинского и/или кириллического алфавита, цифры от 0 до 9, символы таблицы ASCII, максимальная длина 200 символов;
  - «Имя центра сертификации» (Common Name) – выберите имя создаваемого корневого центра сертификации из перечня возможных имен в соответствии с параметрами лицензии;
  - «Суффикс различающегося имени» – укажите суффикс различающегося имени корневого сертификата (формат ввода суффикса приведен справа от поля). Ограничители ввода между параметрами – запятые и запятые с пробелами. Длина вводимого суффикса различающегося имени не должна превышать 250 байт. Ввод атрибутов возможен в любом порядке, но в сертификате порядок атрибутов будет установлен в соответствии с номерами пунктов в Таблица 10.

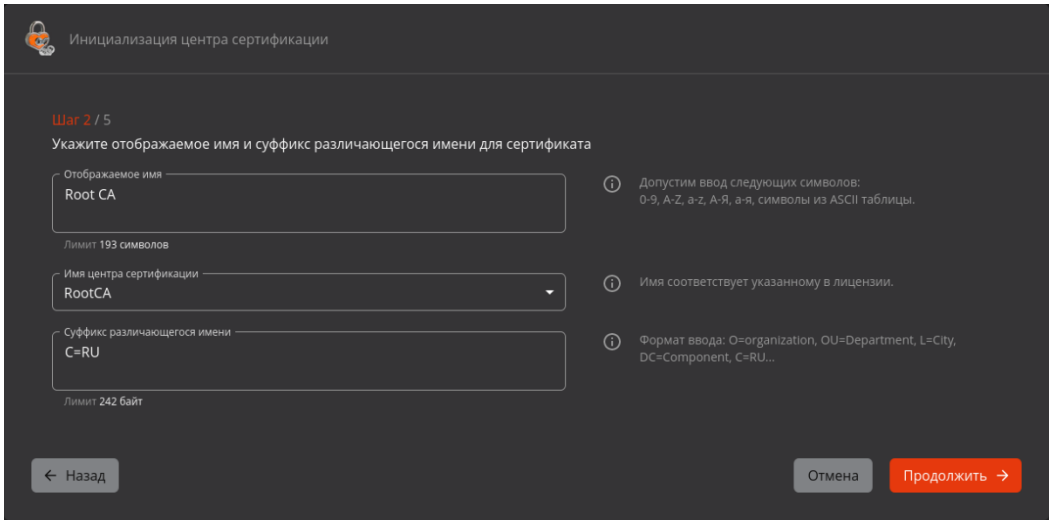


Рисунок 56 – Окно инициализации корневого центра сертификации. Шаг 2/5

Таблица 10 – Поддерживаемые атрибуты суффикса различающегося имени

№	Наименование атрибута	Описание атрибута
1	EMAILADDRESS=	E-mail address (адрес электронной почты) OID: 1.2.840.113549.1.9.1
2	CN=	Common name OID: 2.5.4.3
3	UID=	Unique Identifier (уникальный идентификатор) OID: 2.5.4.45
4	SERIALNUMBER=	Serial number (серийный номер) OID: 2.5.4.5

№	Наименование атрибута	Описание атрибута
5	OU=	Organizational Unit (отдел (организации)) OID: 2.5.4.11
6	O=	Organization (организация) OID: 2.5.4.10
7	L=	Locality (район) OID: 2.5.4.7
8	ST=	State or Province (область, край, республика) OID: 2.5.4.8
9	C=	Country (страна, ввод осуществлять согласно регламенту ISO 3166) OID: 2.5.4.6
10	T=	Title (заглавие) OID: 2.5.4.12
11	SURNAME=	Surname (фамилия) OID: 2.5.4.4
12	STREET=	Street address (адрес – улица) OID: 2.5.4.9
13	INITIALS=	First name abbreviation (инициалы) OID: 2.5.4.43
14	GIVENNAME=	Given name (first name - имя) OID: 2.5.4.42
15	DC=	Domain Component (first) (первый доменный компонент, при повторном вводе – второй) OID: 0.9.2342.19200300.100.1.25
16	UNSTRUCTUREDADDRESS=	IP Address (IP-адрес) OID: 1.2.840.113549.1.9.8
17	UNSTRUCTUREDNAME=	Domain name (доменное имя – FQDN) OID: 1.2.840.113549.1.9.2
18	POSTALCODE=	Postal code (почтовый индекс) OID: 2.5.4.17
19	BUSINESSCATEGORY=	Organization type (категория (тип) организации) OID: 2.5.4.15
20	TELEPHONENUMBER=	Telephone number (телефонный номер) OID: 2.5.4.20
21	PSEUDONYM=	Pseudonym (псевдоним) OID: 2.5.4.65
22	POSTALADDRESS=	Postal address (почтовый адрес) OID: 2.5.4.16
23	NAME=	//Name (дополнительное имя) OID: 2.5.4.41
24	DN=	DN Qualifier (признак отличительного имени для идентификации субъекта) OID: 2.5.4.46
25	DESCRIPTION=	Description (краткое описание) OID: 2.5.4.13
26	INN=	ИНН (идентификационный номер налогоплательщика) OID: 1.2.643.3.131.1.1
27	OGRN=	ОГРН (основной государственный регистрационный номер) OID: 1.2.643.100.1
28	OGRNIP=	ОГРНИП (основной государственный регистрационный номер индивидуального предпринимателя) OID: 1.2.643.100.5

№	Наименование атрибута	Описание атрибута
29	SNILS=	СНИЛС (Страховой номер индивидуального лицевого счёта) OID: 1.2.643.100.3
30	INNLE=	ИНН юридического лица OID: 1.2.643.100.4

После заполнения полей нажмите на кнопку <Продолжить> для перехода к следующему шагу.

- На шаге 3/5 необходимо определить, какой должен использоваться криптопровайдер для каждого алгоритма при создании сертификата центра сертификации и в последующих сценариях выпуска сертификатов субъектов. Для отключенных криптопровайдеров выбор алгоритма будет недоступен и при выпуске сертификатов, несмотря на допустимые значения в шаблонах. Для выбора криптопровайдеров заполните следующие поля (см. Рисунок 57):
  - «RSA» – поле выбора криптопровайдера для алгоритма RSA, допустимые варианты выбора:
    - Стандартный (по умолчанию);
    - КриптоПро CSP<sup>21</sup> (доступен только при наличии активного и подключенного криптопровайдера «КриптоПро CSP», работающего на сервере совместно с компонентом «Центр сертификации Aladdin eCA»);
    - Отключен.
  - «ECDSA» – поле выбора криптопровайдера для алгоритма ECDSA, допустимые варианты выбора:
    - Стандартный (по умолчанию);
    - Отключен.
  - «ГОСТ Р 34.10-2012» – поле выбора криптопровайдера для алгоритма ГОСТ Р 34.10-2012, допустимые варианты выбора:
    - КриптоПро CSP<sup>Ошибка! Закладка не определена.</sup> (доступен только при наличии активного и подключенного криптопровайдера «КриптоПро CSP», работающего на сервере совместно с компонентом «Центр сертификации Aladdin eCA»);
    - Отключен (по умолчанию).

**На следующем шаге не будет доступен для выбора алгоритм ключа, для которого указано значение криптопровайдера «Отключен».**

**При отключении всех криптопровайдеров кнопка <Продолжить> не будет активирована и переход к следующему шагу будет невозможен.**

<sup>21</sup> Подробная информация по настройке взаимодействия ПО «Центр сертификатов доступа Центр сертификатов доступа Aladdin Enterprise Certificate Authority Certified Edition» с криптопровайдером «КриптоПро CSP» описана в Приложении 5, «Руководства администратора. Установка и обслуживание Центра сертификации Aladdin Enterprise Certification Authority. «Центр сертификатов доступа Центр сертификатов доступа Aladdin Enterprise Certificate Authority Certified Edition». RU.АЛДЕ.03.01.020 32 01-1».

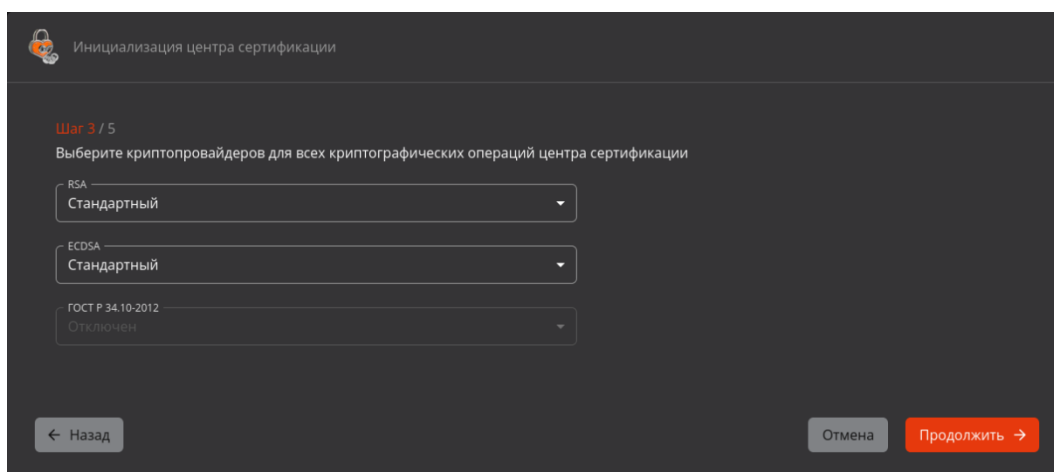


Рисунок 57 - Окно инициализации корневого центра сертификации. Шаг 3/5

После выбора криптопровайдеров нажмите кнопку <Продолжить> для перехода к следующему шагу.

- На шаге 4/5 необходимо выбрать шаблон сертификата Корневого ЦС. В списке шаблонов отображаются все имеющиеся в программе шаблоны с типом «Корневой» (см. Рисунок 58).

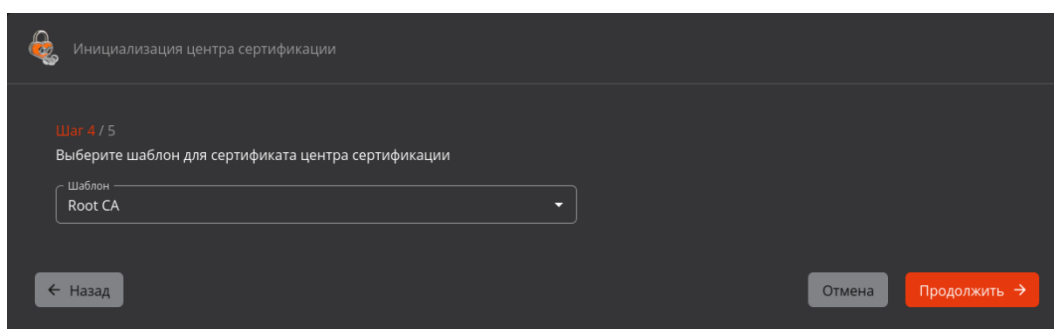


Рисунок 58 - Окно инициализации корневого центра сертификации. Шаг 4/5

После выбора шаблона нажмите кнопку <Продолжить> для перехода к следующему шагу.

- На шаге 5/5 необходимо указать срок действия сертификата ЦС и задать параметры криптографии (см. Рисунок 59). Заполните следующие поля:
  - «Срок действия сертификата» – срок действия Корневого сертификата (по умолчанию – 15 лет). Ввод осуществляется вручную или выбором даты окончания действия сертификата в открывшемся календаре. Максимальный срок действия сертификата определяется шаблоном, выбранным на предыдущем шаге;
  - «Алгоритм ключа» (состав алгоритмов зависит от выбранных провайдеров и шаблоном, выбранным на предыдущем шаге):
    - RSA;
    - ECDSA;
    - ГОСТ Р 34.10-2012.
  - «Длина ключа» (доступные значения определяются шаблоном, выбранным на предыдущем шаге):
    - для RSA: 1024, 1536, 2048, 3072, 4096, 6144, 8192 (по умолчанию 4096);
    - для ECDSA: 256, 384, 521 (по умолчанию 384);
    - для ГОСТ Р 34.10-2012: 256, 512 (по умолчанию 512).
  - «Алгоритм хэш-суммы»:



- для алгоритма ключа RSA или ECDSA: SHA1, SHA256, SHA384, SHA512 (выбран по умолчанию);
- для алгоритма ключа ГОСТ Р 34.10-2012: ГОСТ Р 34.11-2012.
- «Место хранения закрытого ключа»:
  - Доступные варианты выбора, если криптопровайдером выбранного алгоритма ключа является КриптоПро CSP:
    - Локальное хранилище Aladdin eCA (выбрано по умолчанию, требует заранее подготовленной на БДЧ криптопровайдера КриптоПро CSP гаммы);
    - КриптоПро CSP (HDIMAGE);
    - КриптоПро HSM (доступно только при наличии подключения криптопровайдера КриптоПро CSP к ПАКМ «КриптоПро HSM», создаваемые на ПАКМ «КриптоПро HSM» закрытые ключи ЦС являются неэкспортируемыми).
  - В противном случае в данном поле указано неизменяемое значение «Локальное хранилище Aladdin eCA».
- Чек-бокс «Экспортируемый закрытый ключ». Если выбрано место хранения закрытого ключа «Локальное хранилище Aladdin eCA», данный чек-бокс включен по умолчанию и недоступен для изменения.

**При выпуске сертификата доступа Центра сертификации рекомендуется выбирать алгоритмы хэш-суммы SHA256, SHA384 или SHA512 (в случае если в качестве алгоритма ключа выбран RSA или ECDSA).**

**Криптографическая хэш-функция SHA1 не обеспечивает требуемой безопасности и может быть выбрана только при необходимости обеспечения совместимости.**

Рисунок 59 – Окно инициализации корневого центра сертификации. Шаг 5/5  
После задания значений нажмите ставшую активной кнопку «Создать ЦС».

- В случае неудачной попытки создания ЦС будет отображено сообщение об ошибке (см. Таблица 11).

Таблица 11 – Перечень сообщений в случае неудачной попытки создания ЦС

Текст ошибки	Причина																				
Ошибка. Некорректный компонент суффикса различающегося имени – <Имя компонента>	Ошибка ввода неизвестного имени компонента суффикса различающегося имени																				
Ошибка. Лицензионные ограничения не позволяют создать ЦС используя данное имя	Ошибка несоответствия значения в компоненте «CN» суффикса различающегося имени значению, указанному в лицензии																				
Ошибка. Произошла ошибка при создании ключевой пары для алгоритма «Название алгоритма».	Ошибка обращения к криптопровайдеру алгоритма генерации ключевой пары.																				
Ошибка. Ошибка атрибута attributeName: Значение не соответствует регулярному выражению: «regex»	<p>Ошибка валидации введенного значения атрибута различающегося имени<sup>22</sup>. Возможные значения переменной «attributeName» и соответствующие им значения переменной «regex» представлены в таблице ниже:</p> <table> <tr> <th>attributeName</th><th>regex</th></tr> <tr> <td>C</td><td>^[A-Za-z]{2}\$</td></tr> <tr> <td>DN</td><td>^[A-Za-z0-9"()+,\.V:=? ]+\$</td></tr> <tr> <td>EMAILADDRESS</td><td>^[A-Za-zA-Яa-я0-9._-]+@[A-Za-zA-Яa-я0-9._-]+\$</td></tr> <tr> <td>SERIALNUMBER</td><td>^[A-Za-z0-9"()+,\.V:=? ]+\$</td></tr> <tr> <td>INN</td><td>^\d{12}\$</td></tr> <tr> <td>OGRN</td><td>^\d{13}\$</td></tr> <tr> <td>OGRNIP</td><td>^\d{15}\$</td></tr> <tr> <td>SNILS</td><td>^\d{11}\$</td></tr> <tr> <td>INNLE</td><td>^\d{10}\$</td></tr> </table>	attributeName	regex	C	^[A-Za-z]{2}\$	DN	^[A-Za-z0-9"()+,\.V:=? ]+\$	EMAILADDRESS	^[A-Za-zA-Яa-я0-9._-]+@[A-Za-zA-Яa-я0-9._-]+\$	SERIALNUMBER	^[A-Za-z0-9"()+,\.V:=? ]+\$	INN	^\d{12}\$	OGRN	^\d{13}\$	OGRNIP	^\d{15}\$	SNILS	^\d{11}\$	INNLE	^\d{10}\$
attributeName	regex																				
C	^[A-Za-z]{2}\$																				
DN	^[A-Za-z0-9"()+,\.V:=? ]+\$																				
EMAILADDRESS	^[A-Za-zA-Яa-я0-9._-]+@[A-Za-zA-Яa-я0-9._-]+\$																				
SERIALNUMBER	^[A-Za-z0-9"()+,\.V:=? ]+\$																				
INN	^\d{12}\$																				
OGRN	^\d{13}\$																				
OGRNIP	^\d{15}\$																				
SNILS	^\d{11}\$																				
INNLE	^\d{10}\$																				
Ошибка при создании Центра сертификации. Неизвестная ошибка	Внутренняя ошибка ПО																				

- При успешном создании Корневого ЦС и завершении инициализации центра сертификации будет отображено соответствующее окно (см. Рисунок 60). В нём возможно:
  - скачать сертификат созданного Корневого ЦС;
  - скачать цепочку сертификатов в формате .pem;
  - или открыть страницу созданного Центра сертификации.

Также в результате успешного создания данного ЦС в контейнере закрытого ключа данного ЦС будут содержаться закрытый ключ данного ЦС и цепочка сертификатов данного ЦС<sup>23</sup>.

<sup>22</sup> Правила валидации значений атрибутов представлены в Приложение 4. Правила валидации значений полей по умолчанию предустановленных шаблонов сертификатов.

<sup>23</sup> Если местом хранения закрытого ключа ЦС является ПАКМ «КриптоПро HSM, то созданный закрытый ключ ЦС будет неэкспортируемым.

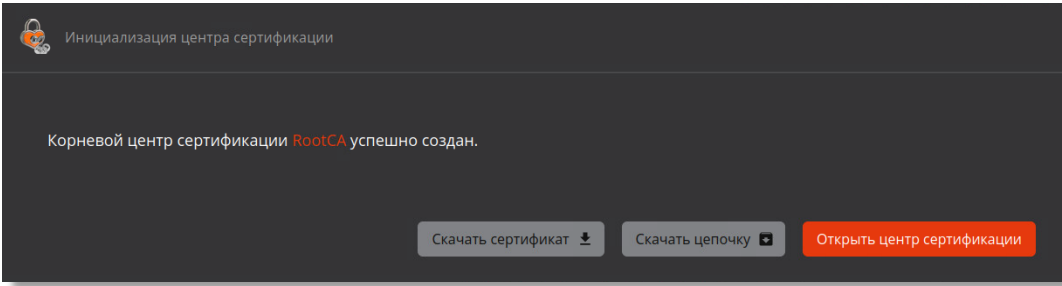




Рисунок 60 – Окно завершения инициализации корневого центра сертификации

7.3.1.3 Создание Подчиненного Центра сертификации с генерацией ключа

- Для создания Центра сертификации на вкладке «Свои сертификаты» нажмите кнопку  <Добавить сертификат>.
- После этого в выпадающем списке выберите опцию «Создать ключ» для создания ЦС с генерацией собственного ключа – дальнейшие шаги создания ЦС описаны в разделе 3.1.2 при создании сертификата подчиненного ЦС;
- Новый Центр сертификации будет создан на основании текущей лицензии.

7.3.1.4 Создание Центра сертификации с импортом внешнего ключа

- Для создания Центра сертификации на вкладке «Свои сертификаты» нажмите кнопку  <Добавить сертификат>.
- После этого в выпадающем списке выберите опцию «Импорт внешнего ключа» для создания ЦС с генерацией собственного ключа – дальнейшие шаги создания ЦС описаны в разделе 3.2.
- Новый Центр сертификации будет создан на основании текущей лицензии.

7.3.1.5 Скачивание запроса на сертификат для ЦС в состоянии «Запрос»

В случае, если запрос на сертификат Подчинённого ЦС по каким-либо причинам не был скачан в окне мастера инициализации, следует:

- На вкладке «Свои сертификаты» выбрать созданный Подчиненный ЦС в состоянии «Запрос» (см. Рисунок 61).

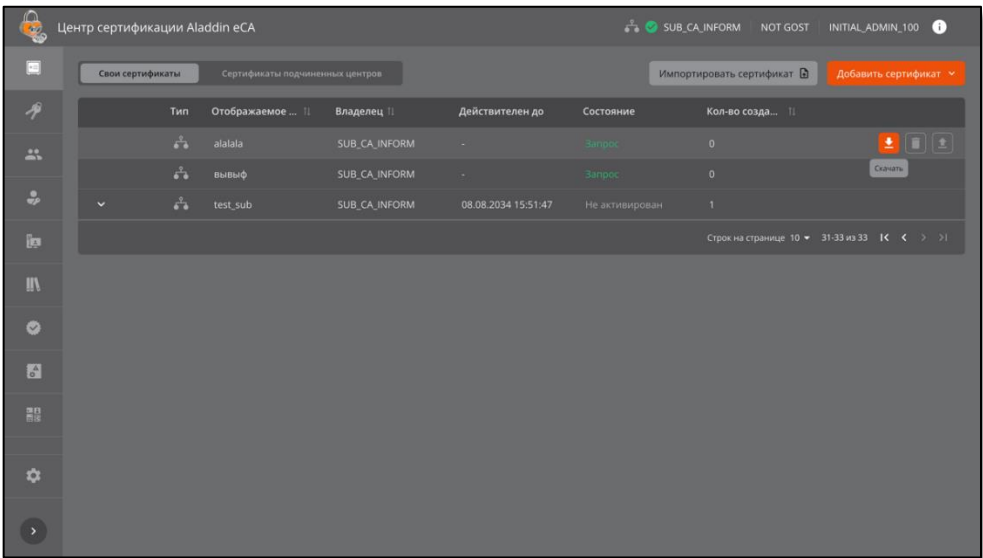



Рисунок 61 – Окно скачивания запроса на сертификат для Подчинённого ЦС

- Нажать появившуюся в строке выбранного ЦС кнопку  и скачать запрос в формате `.csr`.



- Далее следует подписать скачанный запрос на Корневом Центре сертификации согласно пункту 7.3.2.2 настоящего руководства администратора.

### 7.3.1.6 Импорт сертификата Подчиненного ЦС

**ВНИМАНИЕ!** Сценарий является контекстным и используется только для ЦС со статусом «Запрос».

**В случае загрузки цепочки сертификатов, содержащей сертификат с хэш-алгоритмом подписи ГОСТ Р 34.11-2012, на хосте подчиненного Центра сертификации должен быть установлен и подключен к программе криптопровайдер «КриптоПро CSP».**

После подписания запроса на сертификат на Корневом центре сертификации необходимо импортировать цепочку сертификатов для Подчинённого центра сертификации в состоянии «Запрос».

- На вкладке «Свои сертификаты» выбрать Подчиненный ЦС в состоянии «Запрос», по запросу которого был сформирован сертификат и цепочка сертификатов в формате `.pem` или `.p7b` в разделе 7.3.1.5 данного руководства. Нажать кнопку  «Загрузить» (см. Рисунок 61) или кнопку  «Импортировать сертификат» на вкладке «Свои сертификаты» для выбора цепочки сертификатов и автоматического сопоставления соответствия запросу Центра сертификации с целью удовлетворения запроса и активации Центра сертификации.
- Далее в появившемся окне импорта цепочки сертификатов (см. Рисунок 62) выбрать скачанный ранее файл цепочки сертификата для загрузки в формате `.pem` или `.p7b`. Нажать кнопку «Загрузить», активированную после выбора файла цепочки сертификатов.

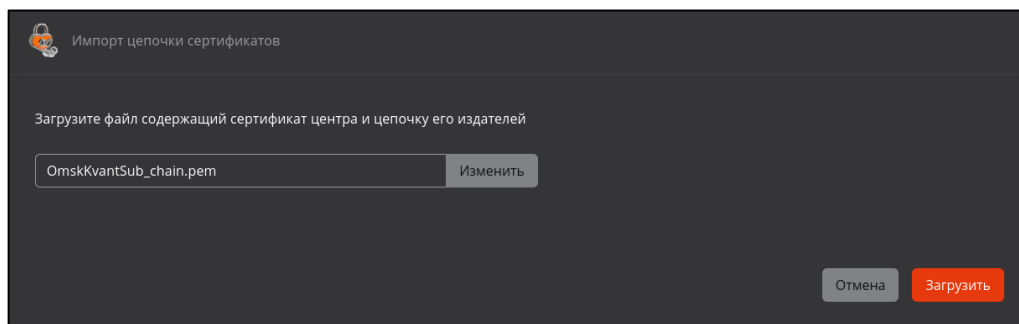


Рисунок 62 - Окно импорта цепочки сертификатов

- В процессе загрузки будет осуществлена проверка загружаемого сертификата, а именно:
  - имени подчиненного ЦС, указанного в импортируемом сертификате (компонент «Common name» в поле «Subject») на соответствие имени, указанному в лицензии подчиненного ЦС;
  - имени корневого ЦС, указанного в его сертификате (компонент «Common name» в поле «Subject») на соответствие имени корневого ЦС, указанному в лицензии;
  - соответствия порядка расположения компонентов SDN в поле «Subject» в сертификате подчиненного ЦС порядку, указанному в Таблица 2;
  - соответствие структуры сертификата стандарту X.509;
  - срока действия всех сертификатов в составе цепочки;
  - аутентичность цепочки (проверка осуществляется криптографическими методами);
  - соответствие открытого ключа в сертификате закрытому ключу в Подчинённом Центре сертификации.
- В запросах на сертификат и сертификатах Центров сертификации, создаваемых Aladdin eCA компоненты SDN в поле «Subject» расположены в следующем порядке:
  - 1) EMAILADDRESS;

- 2) CN;
- 3) UID;
- 4) SERIALNUMBER;
- 5) OU;
- 6) O;
- 7) L;
- 8) ST;
- 9) DC;
- 10) C;
- 11) T;
- 12) SURNAME;
- 13) STREET;
- 14) INITIALS;
- 15) GIVENNAME;
- 16) UNSTRUCTUREDADDRESS;
- 17) UNSTRUCTUREDNAME;
- 18) POSTALCODE;
- 19) BUSINESSCATEGORY;
- 20) TELEPHONENUMBER;
- 21) PSEUDONYM;
- 22) POSTALADDRESS;
- 23) NAME;
- 24) DN;
- 25) DESCRIPTION;
- 26) INN;
- 27) OGRN;
- 28) OGRNIP;
- 29) SNILS;
- 30) INNLE.

- В случае несоответствия каких-либо параметров импортируемого сертификата (цепочки сертификатов) администратор будет уведомлён сообщением об ошибке импорта сертификата Подчинённого ЦС (см. Таблица 12), а в Журнал событий будет произведена запись события CAENV013.

Таблица 12 – Перечень сообщений в случае неудачной попытки импорта сертификата подчинённого ЦС

Текст ошибки	Причина
Ошибка. Недействительный сертификат.	Ошибка истечения срока действия сертификата, входящего в состав цепочки.
Ошибка. Проверка публичного ключа сертификата не удалась.	Ошибка прохождения проверки соответствия открытого ключа закрытому ключу.
Ошибка. Имя подчиненного ЦС, указанное в сертификате, не соответствует лицензии.	Ошибка несоответствия имени подчиненного ЦС, указанного в его сертификате (компонент «Common name» в поле «Subject» сертификата подчиненного ЦС) имени (перечню имен), указанному в лицензии.
Ошибка. Имя корневого ЦС, указанное в сертификате, не соответствует лицензии.	Ошибка несоответствия имени корневого ЦС, указанного в его сертификате (компонент «Common name» в поле

	«Subject» сертификата корневого ЦС) имени (перечню имен) корневого ЦС, указанному в лицензии.
Ошибка. Сертификат ЦС содержит некорректный порядок компонентов суффикса различающегося имени.	Сертификат ЦС содержит некорректный порядок компонентов суффикса различающегося имени.
Ошибка. Загружаемая цепочка сертификатов содержит сертификат (CN="CN сертификата"), не являющийся сертификатом ЦС	Указанный в ошибке сертификат из цепочки не является сертификатом ЦС (флаг <code>isCA=false</code> , а должен быть <code>isCA=true</code> ).
Ошибка. Неизвестная ошибка.	Внутренняя ошибка ПО.

- После успешной загрузки цепочки сертификатов открывается окно с уведомлением об успешной загрузке сертификата (см. Рисунок 63) и отображается следующая информация о сертификате ЦС: издатель, субъект, срок действия сертификата. Также в результате успешной загрузки цепочки сертификатов в контейнере закрытого ключа данного ЦС будут содержаться закрытый ключ данного ЦС и цепочка сертификатов данного ЦС<sup>24</sup>. В Журнал событий производится запись события CAENV012.

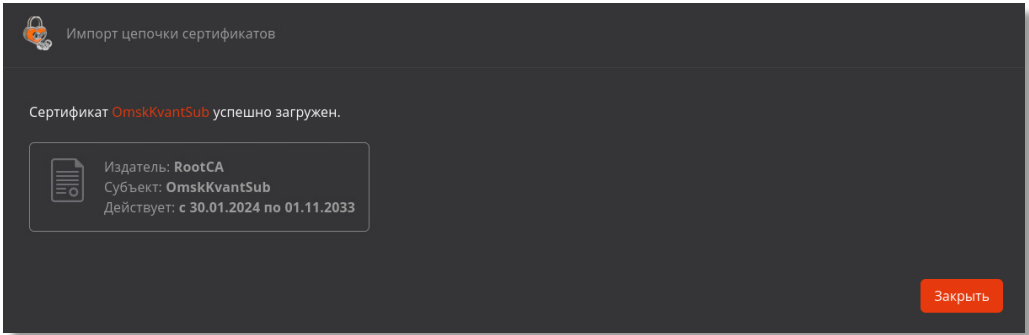


Рисунок 63 – Окно уведомления об успешном загрузке сертификата

- По нажатию на кнопку <Закрыть> в последнем окне импорта цепочки сертификатов:
  - сертификат присваивается Подчиненному ЦС;
  - работа мастера импорта цепочки сертификатов завершается;
  - ЦС автоматически активируется.

7.3.1.7 Удаление Центра сертификации

- Условия удаления центра сертификации:
  - удаляемый центр сертификации находится в состоянии «Не активирован» (см. Рисунок 64);

▼	SubCA	OmskKvantSub	01.11.2033 18:18:21	RSA	2048	Не активирован	7
---	-------	--------------	---------------------	-----	------	----------------	---



Рисунок 64 – Раздел «Центр сертификации» – Вкладка «Свои сертификаты» – Состояние удаляемого ЦС

- выключена проверка издателя – удаляемого центр сертификации (см. Рисунок 65, подраздел 7.13.2 настоящего руководства).

<sup>24</sup> Если местом хранения закрытого ключа центра сертификации является ПАКМ «КриптоПро HSM», то созданный закрытый ключ центра сертификации будет неэкспортируемым.

Разрешенные издатели			
Отображаемое имя	Издатель	Действителен до	Проверка издателя
Sub03	OmskKvantSub	01.11.2033 18:18:21	<input checked="" type="checkbox"/>
SubCA	OmskKvantSub	01.11.2033 18:18:21	<input type="checkbox"/>
INITIAL_CA	INITIAL_CA	13.01.2048 18:50:57	<input checked="" type="checkbox"/>

Рисунок 65 – Раздел «Настройки – Поле «Разрешённые издатели» - Выключение издателя из разрешённых

- Для удаления Центра сертификации, наведите указатель мыши на строку с выбранным ЦС и нажмите кнопку  или откройте карточку выбранного ЦС и нажмите кнопку .
- В появившемся окне подтверждения внимательно ознакомьтесь с рекомендациями (см. Рисунок 66).

**Внимание! После удаления Центра сертификации будут также удалены:**

- запись о центре сертификации, сертификат и закрытый ключ выбранного ЦС;
- все выпущенные сертификаты субъектов;
- субъекты локальной ресурсной системы;
- привязку сертификатов к учётным записям Aladdin eCA;
- шаблоны сертификатов, в которых в качестве издателя указан удаляемый центр сертификации;
- настроенные Центры валидации Aladdin eCA CA.

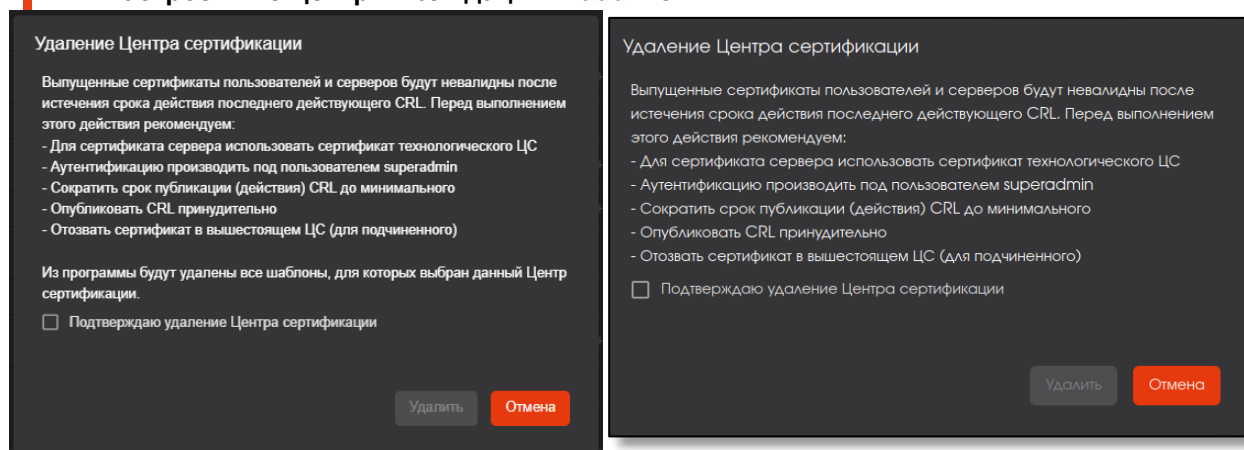


Рисунок 66 – Окно подтверждения удаления Центра сертификации

- Сертификаты, ранее выпущенные удалённым ЦС, будут действительны до следующего запланированного обновления списка отозванных сертификатов.
- Центр валидации, ранее зарегистрированный удалённым ЦС, необходимо самостоятельно удалить на сервере отзыва.
- Для подтверждения удаления ЦС установите флаг в чек-боксе «Подтверждаю удаление Центра сертификации» и нажмите ставшую активной кнопку «Удалить». Для прерывания процесса удаления ЦС нажмите кнопку «Отмена».
- В результате удаления центра сертификации в журнал событий будут зарегистрированы записи с кодами:
  - CAENV059;
  - CAENV038 (изменение списка издателей);
  - CAENV060.
- При попытке удаления активного или разрешённого издателя ЦС будет выведено сообщение (см. Рисунок 67).

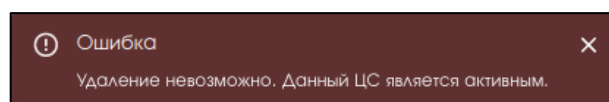


Рисунок 67 – Уведомление об ошибке при попытке удаления активного или разрешённого издателя ЦС

### 7.3.1.8 Экспорт закрытого ключа Центра сертификации

Экспорт закрытого ключа ЦС доступен только для ЦС с состоянием «Не активирован» и с разрешенным экспортом закрытого ключа. Для выполнения экспорта выполните следующие шаги:

- В разделе «Центр сертификации» перейти на вкладку «Свои сертификаты», затем перейдите в карточку ЦС с состоянием «Не активирован» и с разрешенным экспортом закрытого ключа.
- В открывшейся карточке ЦС перейдите на вкладку «Закрытый ключ». На данной вкладке нажмите на кнопку «Экспортировать ключ» (см. Рисунок 68).

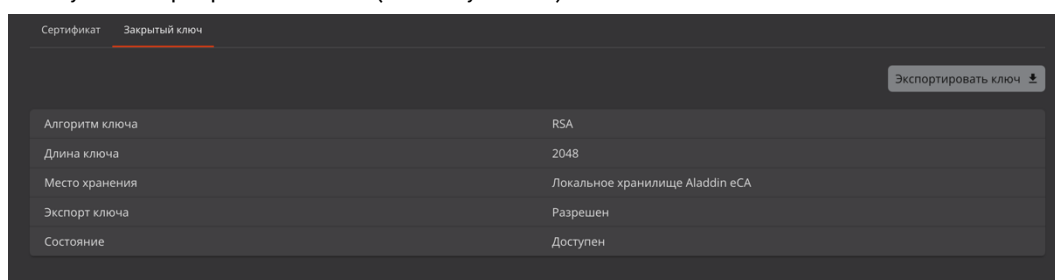


Рисунок 68 – Вкладка «Закрытый ключ» с возможностью экспорта закрытого ключа

- В отобразившемся окне «Экспорт закрытого ключа центра сертификации» задайте пароль для защиты контейнера PKCS#12, в который будем записан закрытый ключ данного ЦС, и подтвердить введенный пароль (см. Рисунок 69).

Пароль должен содержать не менее 8 (восьми) символов с использованием цифр, заглавных и прописных букв, ввод осуществляется на латинице.

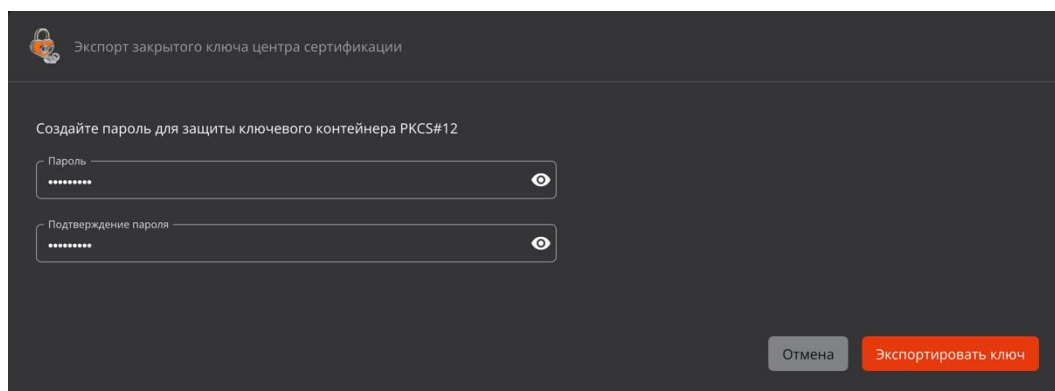


Рисунок 69 – Создание пароля для контейнера PKCS#12 при экспорте закрытого ключа

- Для экспорта ключа нажмите на кнопку «Экспортировать ключ».
- После этого в окне «Экспорт закрытого ключа центра сертификации» будет отображен текст «Закрытый ключ центра сертификации `Имя\_ЦС` успешно экспортирован» (см. Рисунок 70).

И будет доступно скачивание контейнера PKCS#12, содержащего экспортированный закрытый ключ ЦС, путем нажатия на кнопку «Скачать», а также закрытие данного окна путем нажатия на кнопку «Закрыть».

Для скачивания контейнера PKCS#12 нажмите на кнопку «Скачать».

**Внимание! После закрытия данного окна скачивание контейнера PKCS#12, содержащего экспортированный закрытый ключ ЦС, будет недоступно.**



**В случае утери экспортированного контейнера закрытого ключа его восстановление будет невозможно.**

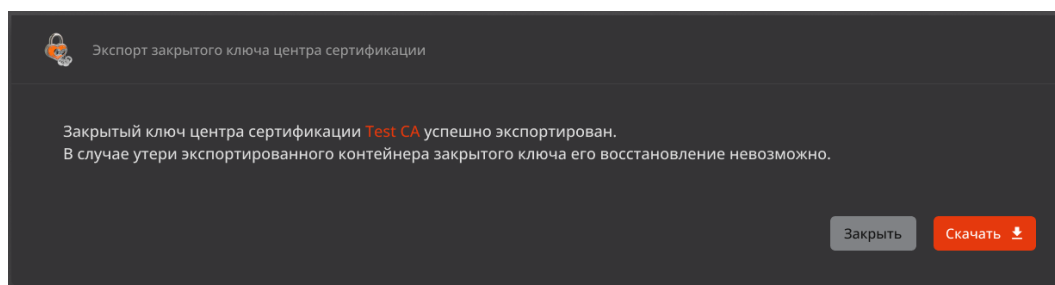


Рисунок 70 – Окно с успешным результатом экспорта закрытого ключа ЦС

- В результате выполнения экспорта закрытого ключа ЦС:
  - Закрытый ключ ЦС будет удален из места хранения, определенного при создании данного ЦС;
  - ЦС, ключ которого был экспортирован, перейдет в состояние «Ключ экспортирован»;
  - В журнале событий будет зафиксировано событие с кодом CAENV103. При каждом скачивании контейнера PKCS#12 в окне «Экспорт закрытого ключа центра сертификации» в журнале событий будет зафиксировано событие с кодом CAENV105.

### 7.3.1.9 Импорт закрытого ключа Центра сертификации

Импорт закрытого ключа ЦС доступен только для ЦС с экспортированным ранее закрытым ключом. Для выполнения импорта выполните следующие шаги:

- В разделе «Центр сертификации» перейдите на вкладку «Свои сертификаты», затем в карточку ЦС с состоянием «Ключ экспортирован».
- В открывшейся карточке ЦС перейдите на вкладку «Закрытый ключ». В данной вкладке нажмите на кнопку «Импортировать ключ» (см. Рисунок 71).

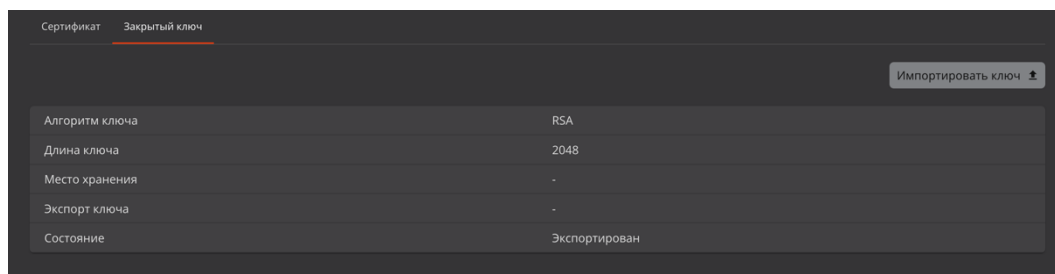


Рисунок 71 – Вкладка «Закрытый ключ» с возможностью импорта закрытого ключа

- В отобразившемся окне «Импорт закрытого ключа центра сертификации» на шаге 1 необходимо выбрать место хранения для закрытого ключа ЦС (см. Рисунок 72).

Доступные варианты выбора, если криптопровайдером алгоритма ключа ЦС является «КриптоПро CSP»:

- «Локальное хранилище Aladdin eCA»;
- «КриптоПро CSP (HDIMAGE)»;
- «КриптоПро HSM» (только при наличии подключения криптопровайдера «КриптоПро CSP» к ПАКМ «КриптоПро HSM»).

Иначе в данном поле будет указано «Локальное хранилище Aladdin eCA».

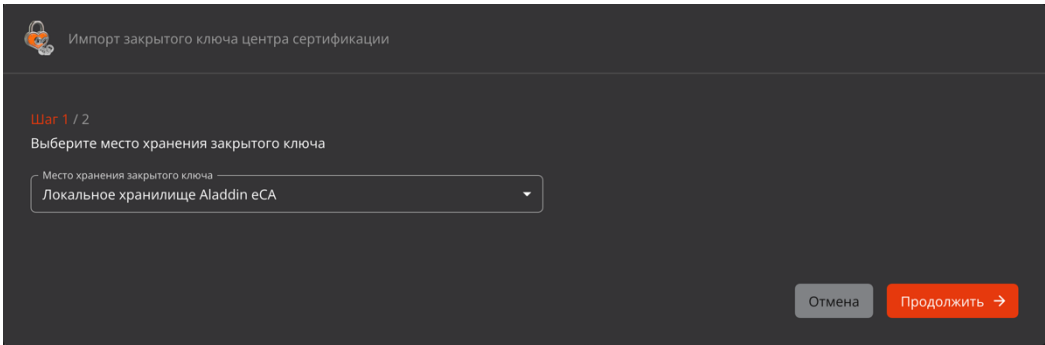


Рисунок 72 – Окно «Импорт закрытого ключа центра сертификации». Шаг 1/2

- Для перехода к следующему шагу нажмите на кнопку <Продолжить>.
- На шаге 2 загрузите файл контейнера закрытого ключа и введите пароль от него (см. Рисунок 73). Допустимое расширение для загружаемых файлов – .p12. При загрузке файла с иным расширением в поле загрузки файла будет отображено сообщение об ошибке «Некорректный формат файла».

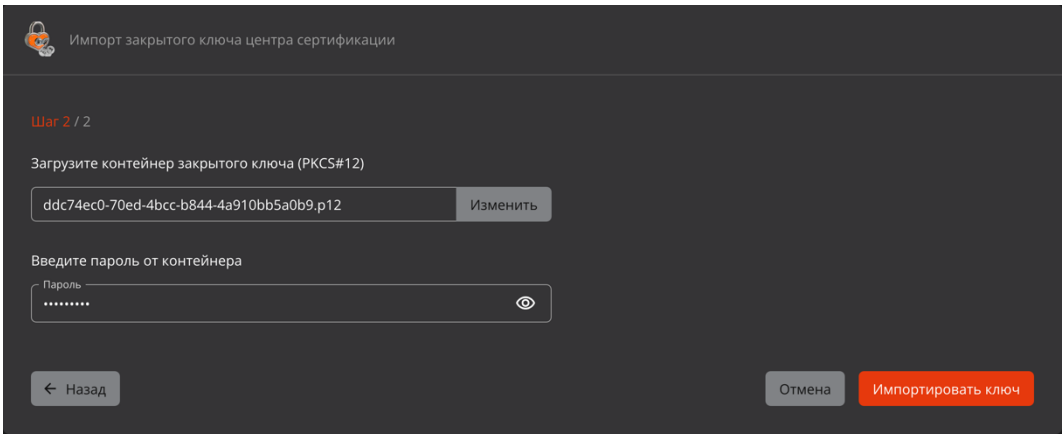


Рисунок 73 – Окно «Импорт закрытого ключа центра сертификации». Шаг 2/2

- После загрузки файла контейнера закрытого ключа и ввода пароля от него нажмите на кнопку <Импортировать ключ>.
- В случае неудачной попытки импорта закрытого ключа будет отображено сообщение об ошибке (см. Таблица 13).

Таблица 13 – Перечень сообщений в случае неудачной попытки импорта закрытого ключа ЦС

Текст ошибки	Причина
Неверный пароль	Указание неверного пароля от контейнера закрытого ключа ЦС
Закрытый ключ не соответствует открытому ключу ЦС	При попытке импорта закрытого ключа, не соответствующего открытому ключу данного ЦС
Цепочка сертификатов в импортируемом контейнере не соответствует цепочке сертификатов ЦС	При попытке импорта контейнера закрытого ключа, цепочка сертификатов в котором не соответствует цепочке сертификатов данного ЦС

- При отсутствии ошибок при импорте закрытого ключа в окне «Импорт закрытого ключа центра сертификации» будет отображен текст «Закрытый ключ центра сертификации `Имя\_ЦС` успешно импортирован.» (см. Рисунок 74).  
В окне «Импорт закрытого ключа центра сертификации» будет доступно закрытие данного окна путем нажатия на кнопку <Закрыть>.

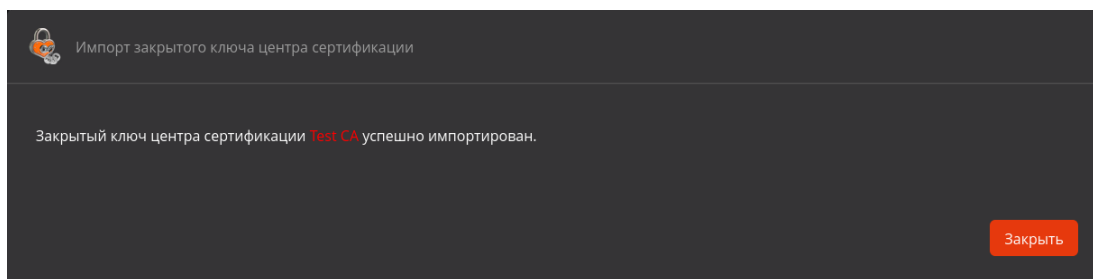


Рисунок 74 – Окно с успешным результатом импорта закрытого ключа ЦС

- В результате выполнения импорта закрытого ключа ЦС:
  - Закрытый ключ ЦС будет помещен в хранилище, выбранное на шаге 1 окна «Импорт закрытого ключа центра сертификации»;
  - ЦС, ключ которого был импортирован, перейдет в состояние «Не активирован»;
  - В журнале событий будет зафиксировано событие с кодом CAENV107.

### 7.3.2 Вкладка «Сертификаты Подчиненных центров»

- Вкладка «Сертификаты Подчиненных центров» (см. Рисунок 75) предназначена для работы с Сертификатами Подчиненных ЦС. В списке сертификатов подчиненных ЦС отображаются только сертификаты, выпущенные активным центром сертификации.
- Варианты состояния и возможных операций над сертификатами из категории «Сертификаты Подчиненных центров» с учетом наведенного указателя мыши и без приведены в Таблица 14.
- Нажатие на кнопку <Подписать запрос> запускает сценарий подписи запроса Подчиненного ЦС из категории «Сертификаты Подчиненных центров».

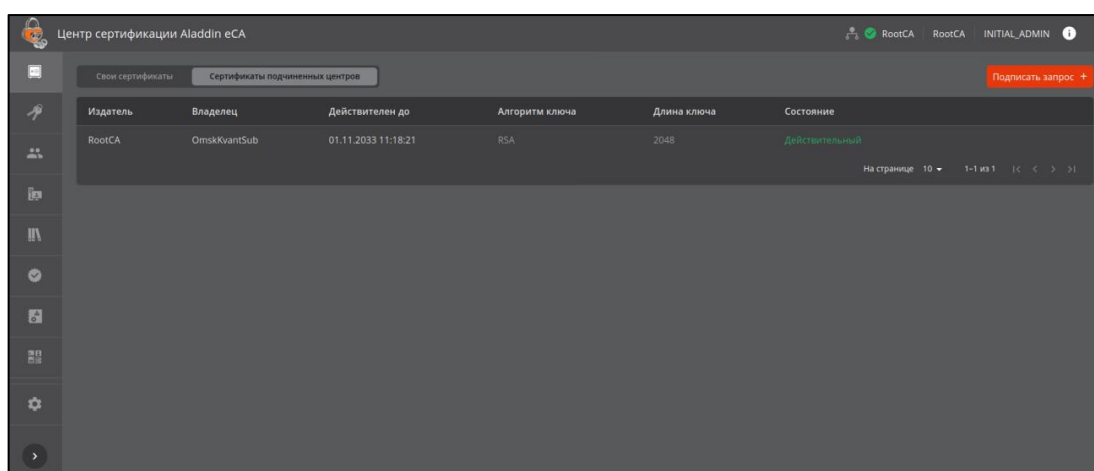


Рисунок 75 - Экран «Сертификаты Подчиненных центров»

- Информационные элементы экрана «Сертификаты Подчиненных центров» – неуправляемые табличные поля:
  - издатель;
  - владелец;
  - действителен до (дата);
  - алгоритм ключа;
  - длина ключа;
  - состояние (варианты состояний: действительный, отозван, истёк срок).

- Управляемые поля. В соответствии с состоянием Подчиненного сертификата при помощи кнопок управления, расположенных на табличных полях, возможны действия, приведенные в Таблица 14.

Таблица 14 – Действия над сертификатами Подчиненных центров

Состояние сертификата	Функции управления сертификатами		
	скачать	удалить	отозвать
действительный	+	✕	+
отозван	+	✕	✕
истек срок	+	+	✕

- Функции управления Подчиненными сертификатами:
  - скачать – скачивание сертификата (без подтверждения);
  - удалить – удаление сертификата с подтверждением;
  - отозвать – отзыв сертификата с подтверждением.

### 7.3.2.1 Карточка сертификата подчинённого ЦС

- Переход к экрану «Карточка сертификата ЦС» осуществляется при нажатии на строку сертификата таблицы на вкладке «Свои сертификаты» (см. Рисунок 53).

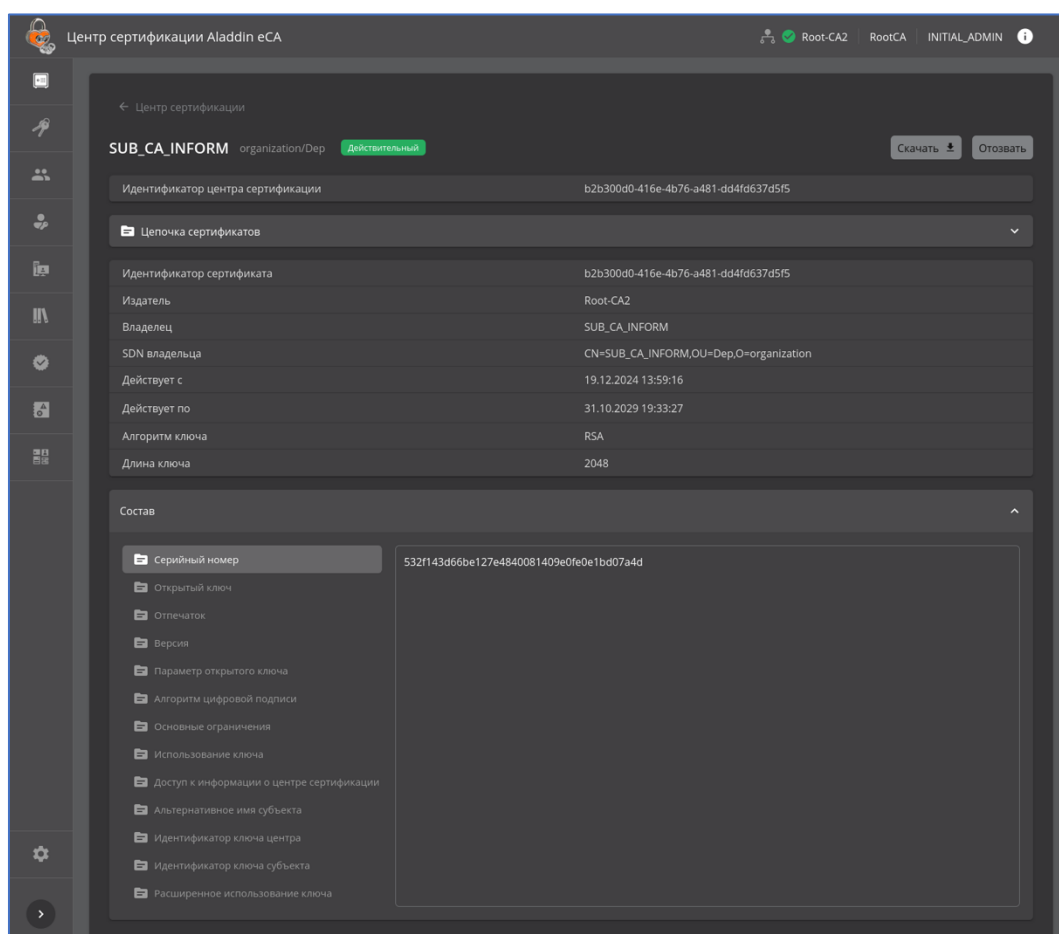


Рисунок 76 – Экран карточки сертификата Подчинённого ЦС в состоянии «Действительный»

- Доступные действия в карточке сертификата ЦС со статусом «Действительный» возможно:
  - выгрузить сертификат по нажатию кнопки <Скачать>
  - отозвать сертификат ЦС по нажатию кнопки <Отозвать>.

Набор кнопок в карточке ЦС в зависимости от статуса сертификата ЦС соответствует приведённым действиям в Таблица 14.

- В карточке Центра сертификации отображаются следующие сведения:
  - идентификатор центра сертификации;
  - цепочка сертификатов;
  - идентификатор сертификата;
  - издатель;
  - владелец;
  - SDN владельца;
  - срок действия («действует с», «действует по»);
  - алгоритм ключа;
  - длина ключа;
  - состав:
    - серийный номер (поле «Serial Number» сертификата);
    - открытый ключ (поле «Subject Public Key Info»);
    - отпечаток (вычисляемое значение, отсутствует в сертификате);
    - версия (поле «Version»);
    - параметры открытого ключа (всегда «X509»);
    - алгоритм цифровой подписи (поле «Signature Algorithm»);
    - основные ограничения (поле «X509v3 Basic Constraints»);
    - использование ключа (поле «X509v3 Key Usage» сертификата);
    - доступ к информации о центре сертификации (поле «Authority Information Access»);
    - альтернативное имя субъекта (поле «X509v3 Subject Alternative Name» сертификата);
    - идентификатор ключа центра (поле «X509v3 Authority Key Identifier» сертификата);
    - идентификатор ключа субъекта (поле «X509v3 Subject Key Identifier» сертификата);
    - расширенное использование ключа (поле «X509v3 Extended Key Usage» сертификата).

### 7.3.2.2 Подписание запроса на Корневом ЦС

- После предварительного скачивания запроса на сертификат Подчинённого ЦС и переноса его на Корневой ЦС выполните подписание согласно нижеприведённой инструкции.
- При активном Корневом ЦС, от имени которого будет выдан сертификат, на вкладке «Сертификаты Подчинённых центров» нажать кнопку <Подписать запрос> (см. Рисунок 77)

**Внимание! Подписание файл-запроса и выдача подписанного сертификата производится от ЦС в состоянии «Активирован» на вкладке «Сертификаты подчинённых центров». Запрос на сертификат Подчинённого ЦС может быть подписан только один раз Корневым ЦС.**

**Выпускаемые сертификаты подчинённых центров сертификации должны подписываться с использованием алгоритма хэш-суммы центра сертификации, на котором подписывается запрос, вне зависимости от указанного в запросе алгоритма хэш-суммы.**

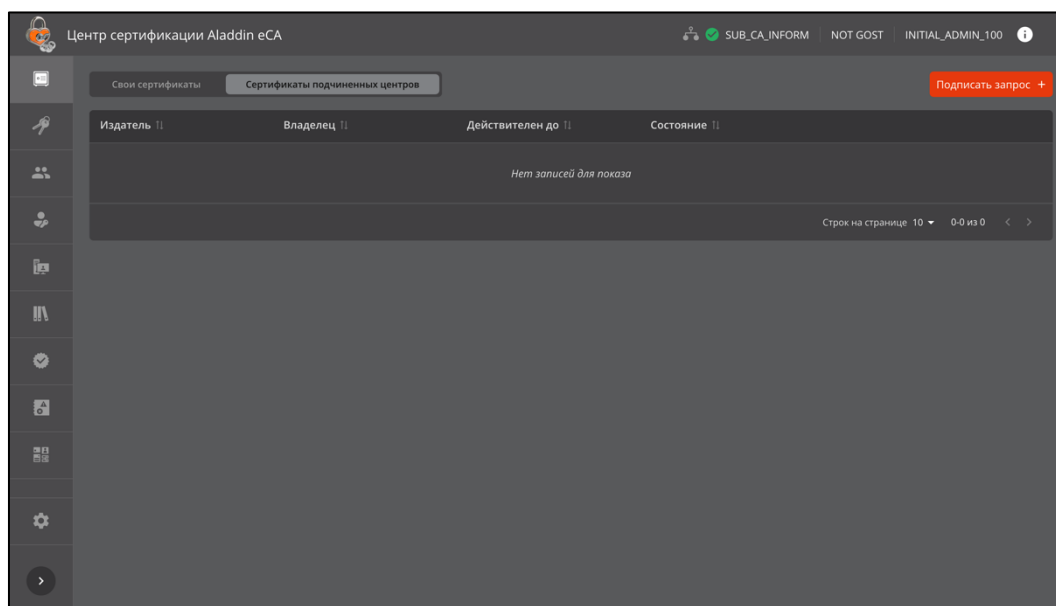


Рисунок 77 – Окно «Сертификаты Подчиненных ЦС»

- Далее загрузите запрос в формате `.csr`, скачанный на шаге 7.3.1.5, нажав кнопку <Выбрать файл> (см. Рисунок 78).
- Выберите шаблон сертификата Подчинённого центра сертификации (например, предварительно подготовленный шаблон путём редактирования клонированного предустановленного шаблона Подчинённого центра сертификации в разделе «Шаблоны»).

Срок действия сертификата Подчиненного ЦС определяется шаблоном «Sub CA»<sup>25</sup>, но не превышает срок действия сертификата Корневого ЦС.

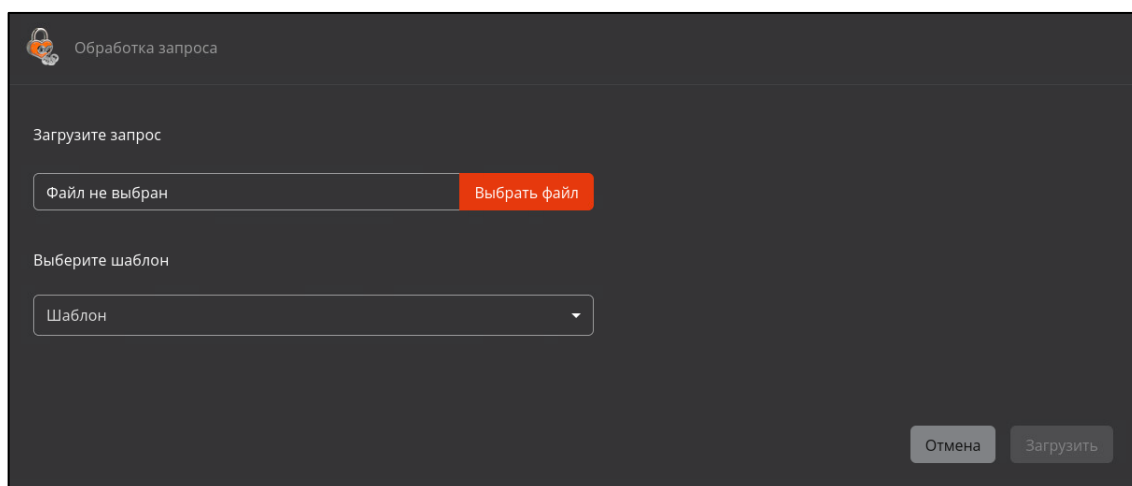


Рисунок 78 – Окно выбора файла запроса

На текущем шаге, после выбора файла запроса, возможно изменить выбор, нажав кнопку <Изменить> (см. Рисунок 79).

- Нажмите ставшую активной кнопку <Загрузить> (см. Рисунок 79).

<sup>25</sup> Про шаблон «Sub CA» см. в Приложение 2. Описание полей предустановленных шаблонов сертификатов

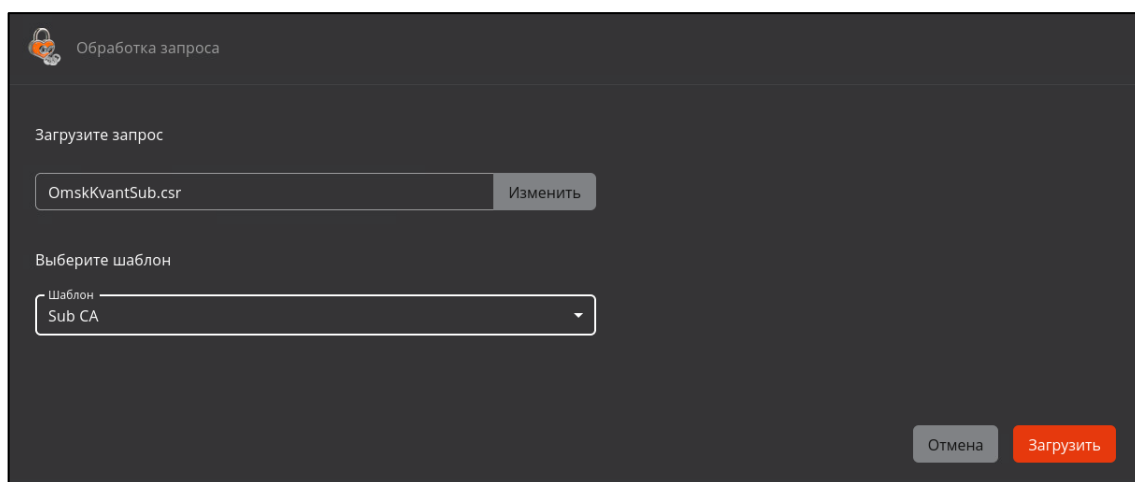


Рисунок 79 – Окно загрузки файла запроса

- При нажатии кнопки <Загрузить> происходит загрузка файл запроса в Корневой ЦС (текущий активный Корневой ЦС из категории «Свои сертификаты»). Далее администратор видит уведомление о том, что сертификат Подчиненного ЦС успешно сформирован и подписан Корневым ЦС (см. Рисунок 80).

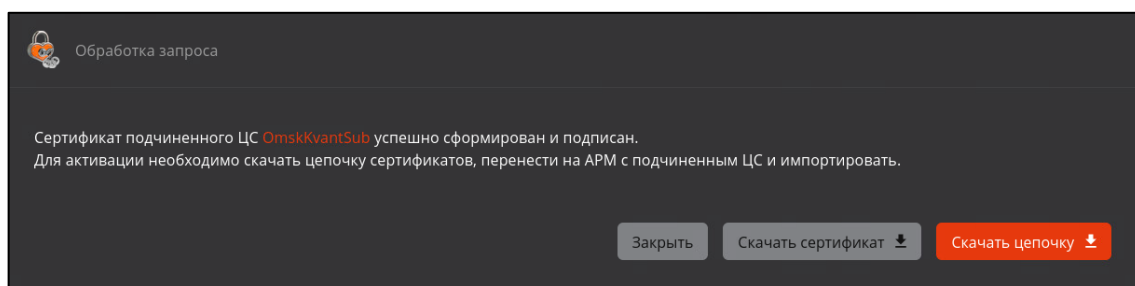


Рисунок 80 – Окно успешного формирования и подписи сертификата

- В случае если на основании загруженного запроса ранее был выпущен сертификат Подчинённого ЦС администратор будет уведомлён сообщением (см. Рисунок 81).

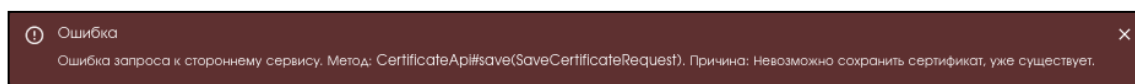



Рисунок 81 – Уведомление о том, что по загруженному запросу ранее выпущен сертификат

- Необходимо скачать цепочку сертификатов ЦС в формате `.pem`, нажав кнопку <Скачать цепочку сертификатов>, в окне «Обработка запроса» на данном шаге для дальнейшего импорта на Подчинённом центре сертификации.
- Скачать сформированный и подписанный сертификат, а также цепочку сертификатов можно позднее, открыв вкладку «Сертификаты Подчиненных центров», выбрав нужный сертификат и нажав появившуюся кнопку  для скачивания сертификата или цепочки сертификатов, выбрав соответствующий пункт в раскрывшемся меню (см. Рисунок 82).

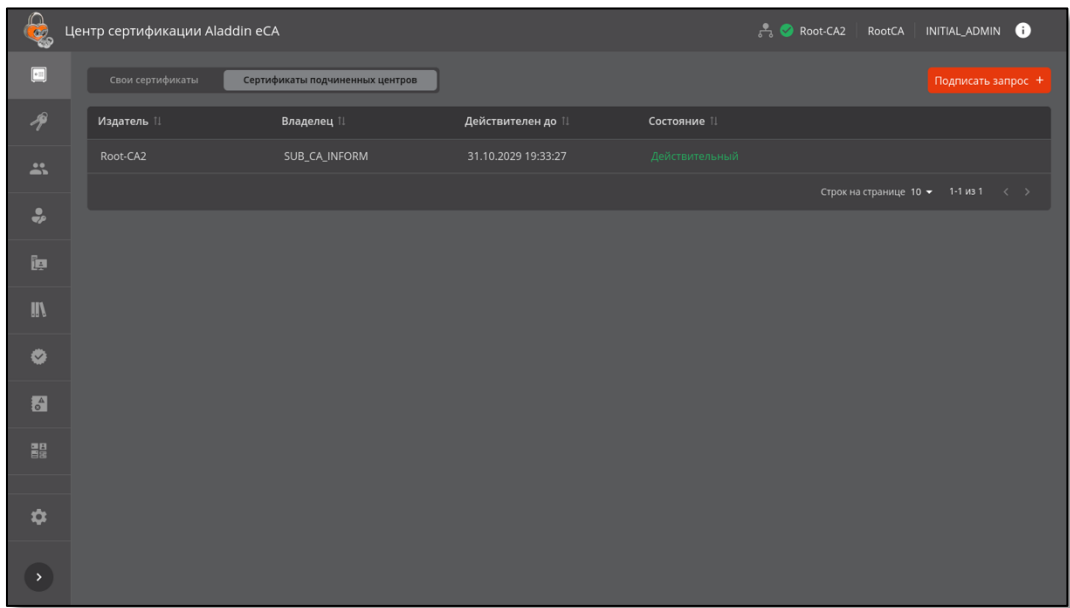


Рисунок 82 – Окно вкладки «Сертификаты Подчиненных центров» с выбранным сертификатом

- Далее перенесите сертификат на Подчинённый ЦС и выполните импорт цепочки сертификатов согласно пункту 7.3.1.6 настоящего руководства.

7.4 Раздел «Сертификаты»

Раздел «Сертификаты» обеспечивает просмотр и управление сертификатами субъектов в соответствии с правами учётной записи пользователя. Пользователю с ролью «Администратор» доступен просмотр и управление всеми сертификатами без ограничений по субъектам. Пользователю с ролью «Оператор» доступен просмотр и управление сертификатами субъектов, права на которые предоставлены для учётной записи.

Переход на экран управления центра сертификации осуществляется по выбору раздела «Сертификаты» бокового меню, расположенного слева на главном экране (см. Рисунок 50).

На данном экране отображаются все созданные сертификаты пользователей, контроллеров домена, веб-серверов.

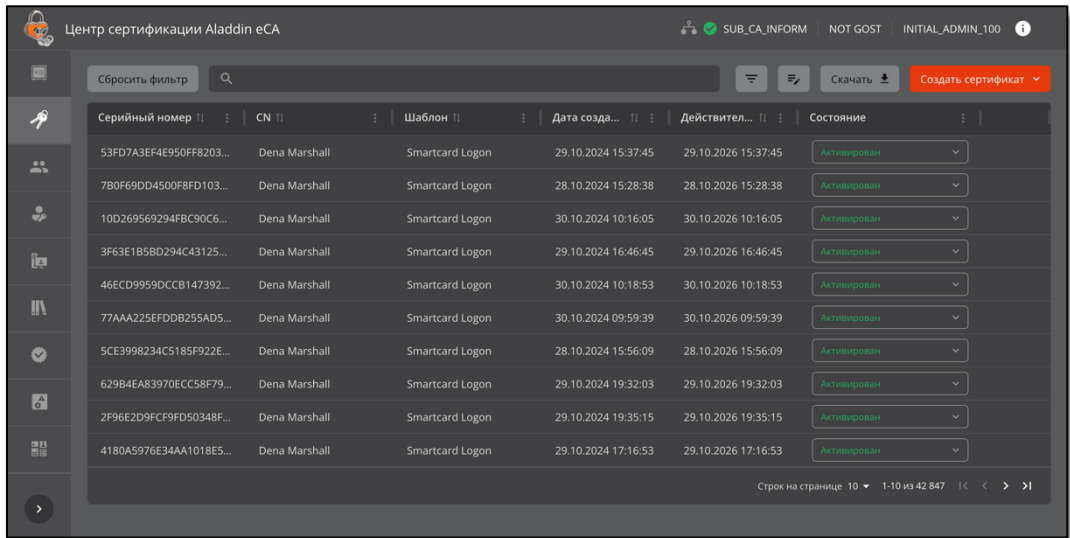


Рисунок 83 - Экран раздела меню «Сертификаты»

- На экране раздела «Сертификаты» отображены информационные элементы (табличные поля):
  - 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:
  - выпуск нового сертификата;
  - поиск выпущенных сертификатов;
  - сортировка сертификатов;
  - просмотр списка сертификатов с заданными критериями;
  - сброс всех применённых фильтров или выборочная отмена выбранного фильтра;
  - скачивание сертификатов в формате `.pem`;
  - скачивание цепочки сертификатов;
  - изменение статуса сертификатов;
  - просмотр карточки сертификата;
  - экспорт списка всех выпущенных сертификатов с атрибутами;
  - массовые операции с выпущенными сертификатами.
- Все созданные сертификаты (в формате `.pem`) и закрытые ключи (в формате PKCS#12) субъектов будут сохранены в базе данных (имя базы данных по умолчанию, конфигурация базы данных указана в файле `/opt/aecaCa/scripts/config.sh`).
- Все созданные сертификаты субъектов на экране раздела отображаются в виде таблицы с пагинацией.
- Скачивание контейнера PKCS#12, содержащего закрытый ключ и сертификат, доступна только в окне по завершению создания сертификата.

**Выпуск сертификатов для субъектов, не имеющих действующие сертификаты, доступен только при условии, что лицензионное ограничение на количество субъектов, владеющих действующими сертификатами, не достигнуто. В случае, если субъект уже является владельцем действующего сертификата, количество сертификатов, которое может быть создано для данного субъекта, не ограничено.**

#### 7.4.1 Выпуск сертификата

- Для выпуска сертификата для существующего или нового субъекта нажмите кнопку <Создать сертификат> и выберите способ создания из выпадающего списка (см. Рисунок 84):
  - с закрытым ключом (PKCS# 12);
  - на основании запроса;
  - на ключевом носителе.
- Более подробно процедура выпуска сертификата приведена в «Приложение 1. Создание сертификата для субъекта».

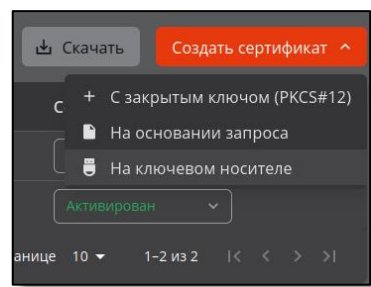


Рисунок 84 – Выпуск сертификата в разделе «Сертификаты»

7.4.2 Поиск сертификатов

Строка поиска (см. Рисунок 85) 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.

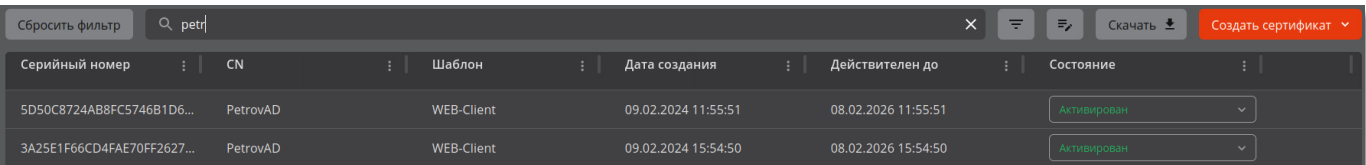


Рисунок 85 – Поисковая строка в разделе «Сертификаты»

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

7.4.3 Сортировка сертификатов

- Средства сортировки выпущенных сертификатов представлены элементами выбора направления сортировки в заголовке таблицы экранной формы (см. Рисунок 86):
  - «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.

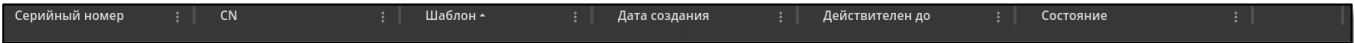



Рисунок 86 – Поля сортировки содержимого раздела «Сертификаты»

- Также отобразить в определённом порядке список сертификатов (отсортировать) в колонке возможно по нажатиию кнопки <Действия в колонке>, выбрав и нажав в раскрывшемся меню «Сортировать...» (см. Рисунок 88).

## 7.4.4 Фильтрация сертификатов

### 7.4.4.1 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 87):
  - 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).

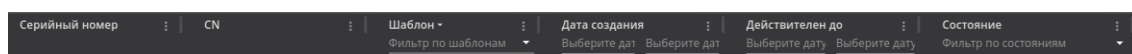





Рисунок 87 – Поля фильтра заголовков экранной таблицы

- 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 .

### 7.4.4.2 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 88);

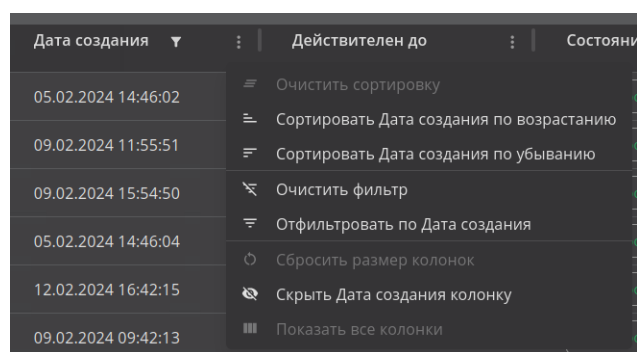
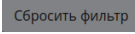



Рисунок 88 – Кнопка <Очистить> фильтр

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

7.4.5 Скачивание сертификатов

Для скачивания наведите указатель мыши на выбранный сертификат в экранной таблице, нажмите появившуюся кнопку  (см. Рисунок 83) и в раскрывшемся подменю выберите пункт <Скачать сертификат> или <Скачать цепочку> в формате .pem (см. Рисунок 89).

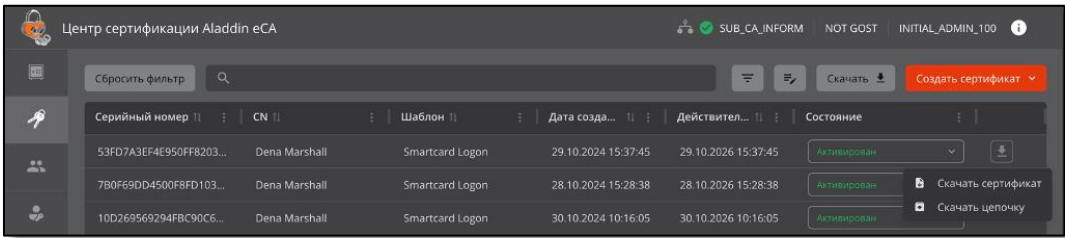


Рисунок 89 – Подменю «Скачать сертификат/цепочку»

7.4.6 Статус сертификатов

- Возможные варианты состояния и доступные действия над сертификатами в зависимости от состояния приведены в Таблица 15.

Таблица 15 – 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 90).

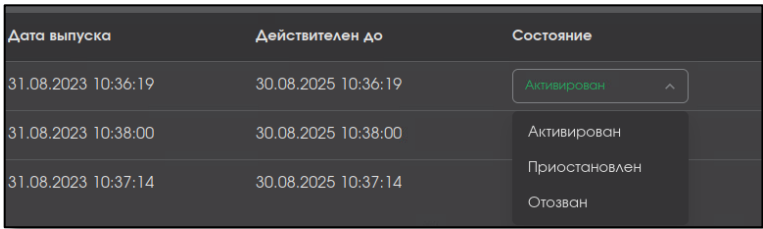


Рисунок 90 – Выпадающее меню смены состояния сертификата

- 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 91)

**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».**

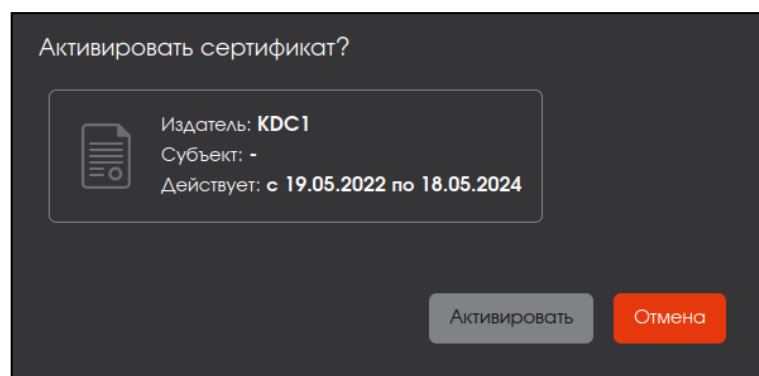


Рисунок 91 – Окно активации сертификата

- отзыв (см. Рисунок 92);

**ВНИМАНИЕ! Данную операцию нельзя отменить.**

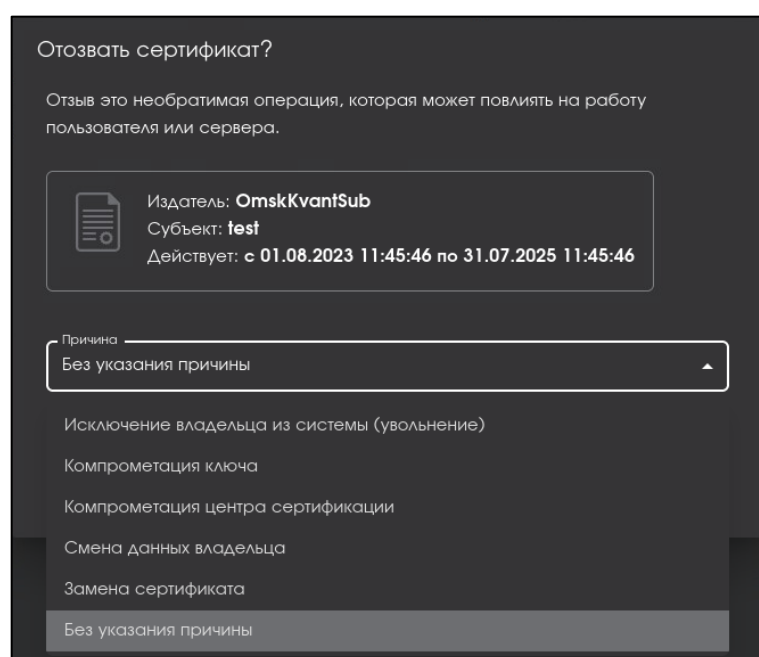


Рисунок 92 – Окно отзыва сертификата

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;
- компрометация ключа (keyCompromise);
- компрометация центра сертификации (cACompromise);
- заменен (сертификат) – заменен на иной сертификат;
- без указания причины (unspecified).
- Приостановка действия сертификата (см. Рисунок 93):

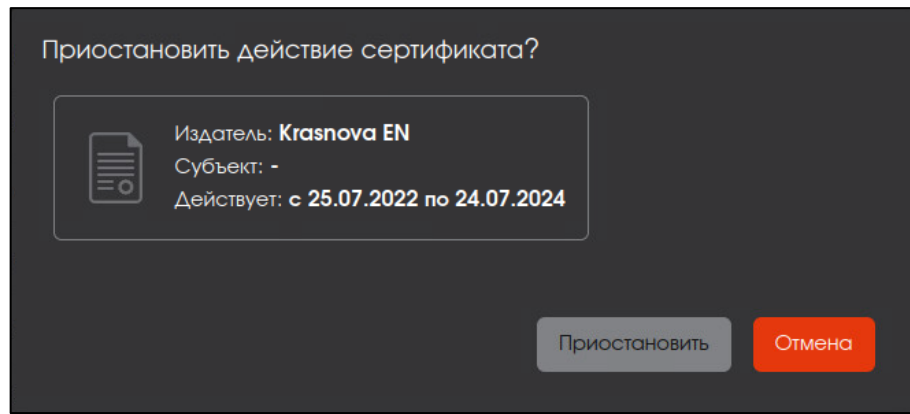
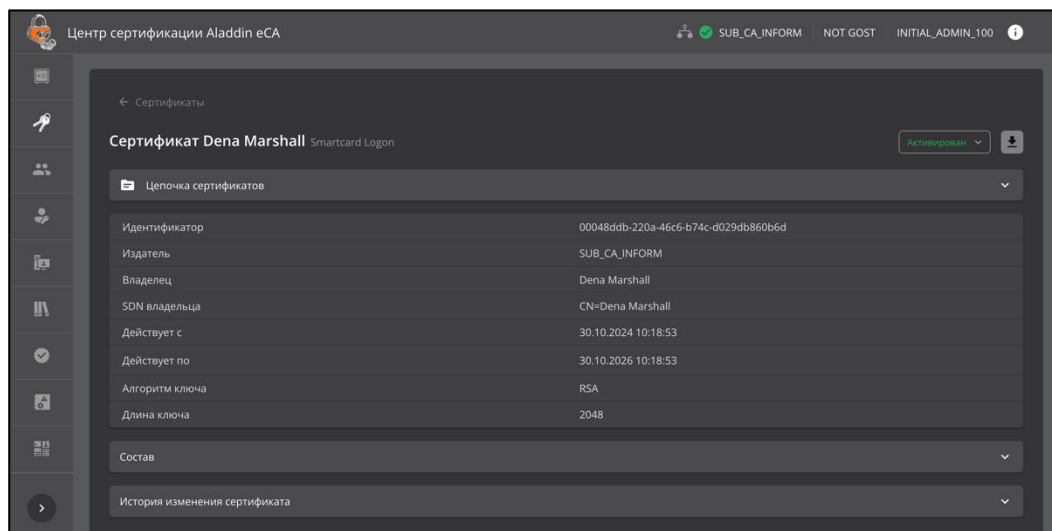


Рисунок 93 – Окно приостановки действия сертификата

#### 7.4.7 Карточка сертификата

- Просмотр данных сертификата возможен посредством страницы «Карточка сертификата».
- Переход к экрану «Карточка сертификата» (см.



- Рисунок 94) осуществляется при нажатии на строку сертификата таблицы главного экрана раздела «Сертификаты» (см. Рисунок 83).

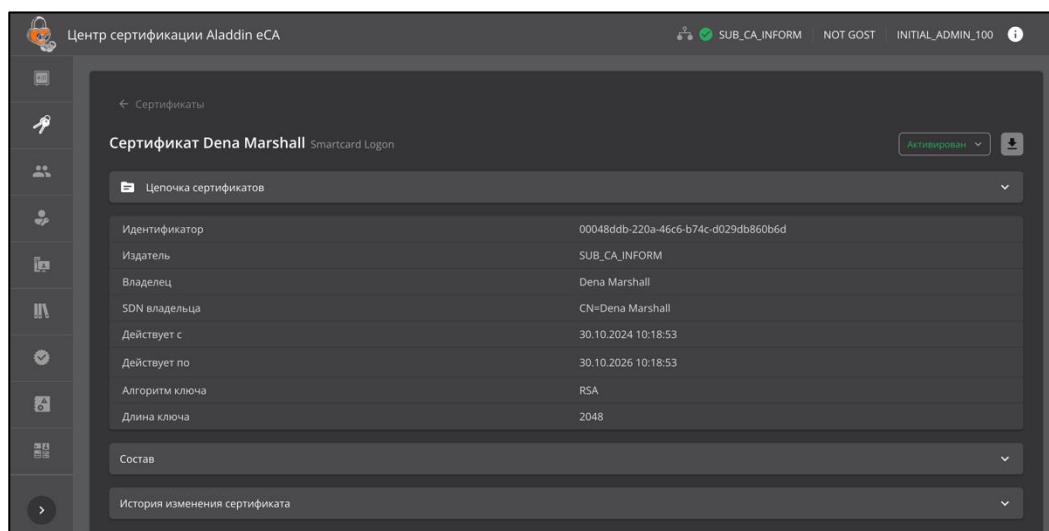



Рисунок 94 – Окно «Карточка сертификата»

- Оглавление карточки сертификата включает в себя:
  - тип-сертификата;
  - принадлежность;
  - тип субъекта.
- Для возврата на главный экран раздела «Сертификаты» проследовать по стрелке .
- Для изменения статуса сертификата выбрать из выпадающего списка действие в соответствии с Таблица 15.

**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 подменю, 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 95).



Рисунок 95 – Окно карточки сертификата. Подменю «Цепочка сертификатов»

- «Состав». Раскройте вкладку, нажав в строке с именем вкладки символ . На раскрывшемся экране отображены следующие поля (см. Рисунок 96):
  - 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.

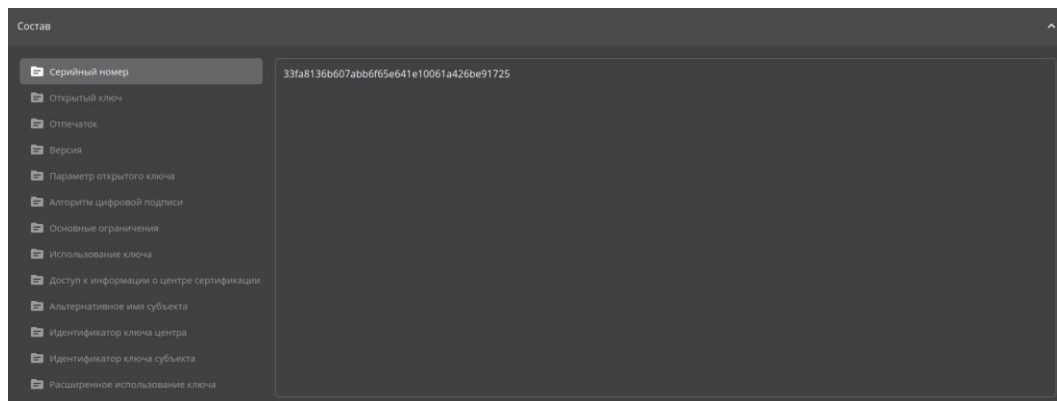



Рисунок 96 – Окно карточки сертификатов. Вкладка «Состав»

- «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 97):
  - дата – дата совершенного действия;
  - пользователь – учётная запись, под которой было совершено данное действие;
  - событие – действие, совершённое над сертификатом.



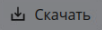
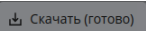
История изменения сертификата

Дата	Пользователь	Событие
01.08.2023 11:45:45	INITIAL_ADMIN	Выпущен
01.08.2023 11:51:58	INITIAL_ADMIN	Приостановлен Приостановка полномочий владельца
01.08.2023 12:00:12	INITIAL_ADMIN	Активирован Удален из CRL

Рисунок 97 – Окно карточки сертификатов. Вкладка «История изменения сертификата»

- Выход из карточки сертификата осуществляется по кнопке <Возврат> и по кнопкам вкладки главного меню.

#### 7.4.8 Экспорт списка выпущенных сертификатов

- При использовании учётной записи с ролью «Администратор» можно сохранить полный список всех выпущенных сертификатов в виде .csv файла.
- 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 98).

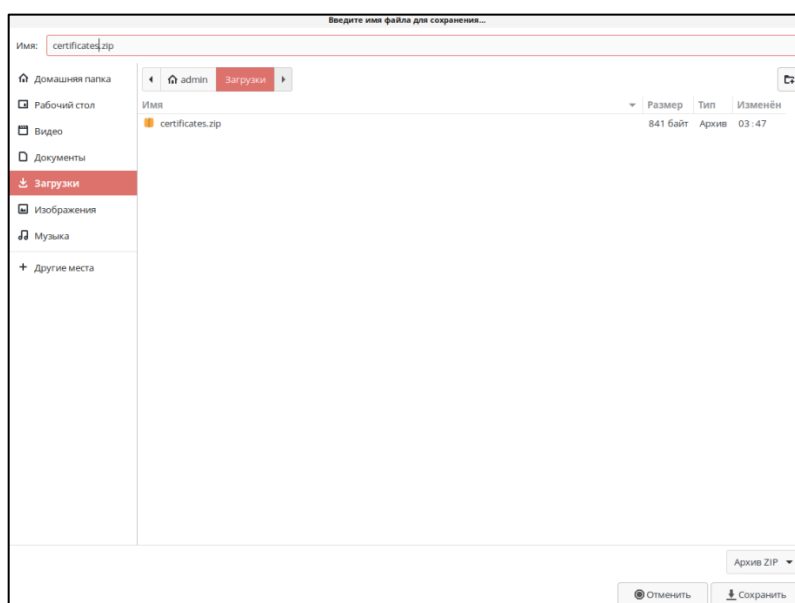


Рисунок 98 – Окно указания пути сохранения файла


- Выгруженный файл .csv (заархивированный при выгрузке) представлен в текстовом формате для представления табличных данных, где строки текста содержат поля таблицы, разделённые запятыми. Сформированная таблица содержит следующие столбцы (см. Рисунок 99):
  - fingerprint – содержит уникальный числовой отпечаток сертификата;
  - safingerprint – 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	cafingerpint	expire date	issuerdn	revocation date	revocation reason	serialnumber	status	subjectdn	create date	username	subject alt name	template	algorithm	key length	
2	532af36b5656;0f83238c98d881	#####	CN=SubCA242,	02.09.2022 13:18	Revoked: Cessation c 77b2814f9a1ee	HOLD	CN=SubCA242	#####	SubCA242	#####	SubCA242	null	OCSP Signer	RSA	2048	
3	c32484f9822dc0f83238c98d881	#####	CN=SubCA242,	31.08.2022 21:56	Revoked: Cessation c 29644f71ac7c6	HOLD	CN=DC	#####	DC	#####	DC	dNSName=DC, gu Domain Cont	RSA	#####	2048	
4	5258bc09c20610f83238c98d881	#####	CN=SubCA242,	01.09.2022 13:39	Suspended: Certificat 699edc111ec1e	REVOKED	CN=cheburgen	#####	cheburgen	#####	cheburgen	rfc822name=cheb Smartcard Lo	RSA	#####	1024	
5	47b18421ec4d0f83238c98d881	#####	CN=SubCA242,	Active	5110646ee2431	ACTIVE	CN=SubCA242	#####	SubCA242	#####	SubCA242	web dNSName=SubCA WEB-Server	RSA	#####	2048	
6	7c13052621aff0f83238c98d881	#####	CN=SubCA242,	02.09.2022 10:42	Suspended: Certificat 67f2c7275957b6	REVOKED	CN=OP1_242	#####	OP1_242	#####	OP1_242	rfc822name=op1 WEB-Client	RSA	#####	2048	
7	52746cc8e30f6f83238c98d881	#####	CN=SubCA242,	31.08.2022 21:56	Suspended: Certificat 79878f39c5d53c	REVOKED	CN=OP2_242	#####	OP2_242	#####	OP2_242	rfc822name=op2 WEB-Client	RSA	#####	2048	
8	c411492ef40dc0f83238c98d881	#####	CN=SubCA242,	31.08.2022 21:56	Suspended: Certificat 171a95d06d320	REVOKED	CN=koltakova	#####	koltakova	#####	koltakovav	rfc822name=eaca Smartcard Lo	RSA	#####	2048	
9	f830f0cb22a0f83238c98d881	#####	CN=SubCA242,	04.09.2022 14:46	Revoked: Cessation c 659787bd69d9f	HOLD	CN=tushkan	#####	tushkan	#####	tushkan	rfc822name=tush Smartcard Lo	RSA	#####	2048	
10	dec1c1520014f83238c98d881	#####	CN=SubCA242,	31.08.2022 21:56	Revoked: Cessation c 6360503883063	HOLD	CN=SUBCA	#####	SUBCA	#####	SUBCA	dNSName=SUBCA Domain Cont	RSA	#####	3072	
11	110ffbd7a6f1af83238c98d881	#####	CN=SubCA242,	01.09.2022 18:34	Suspended: Certificat 560f36c6f48609	REVOKED	CN=ttttttt	#####	ttttttt	#####	ttttttt	rfc822name=tt@t Smartcard Lo	RSA	#####	2048	
12	bd8e4c114e36f83238c98d881	#####	CN=SubCA242,	02.09.2022 10:42	Suspended: Certificat 09feb9eaf14ef	REVOKED	CN=OP1_242	#####	OP1_242	#####	OP1_242	rfc822name=test WEB-Client	RSA	#####	2048	
13	f9c9f3951e7cf83238c98d881	#####	CN=SubCA242,	02.09.2022 10:03	Suspended: Certificat 54a9be9b4d1da	REVOKED	CN=ushkan	#####	ushkan	#####	ushkan	rfc822name=ushk Smartcard Lo	RSA	#####	2048	
14	8c324192620bf83238c98d881	#####	CN=SubCA242,	01.09.2022 13:39	Suspended: Certificat 360c202d0731a	REVOKED	CN=tushkan	#####	tushkan	#####	tushkan	dNSName=tushka Domain Cont	RSA	#####	2048	
15	be0d18556dbtf83238c98d881	#####	CN=SubCA242,	01.09.2022 12:38	Suspended: Certificat 6a60fb1d27e71	REVOKED	CN=SUBCA	#####	SUBCA	#####	SUBCA	dNSName=SUBCA Domain Cont	RSA	#####	3072	
16	d93b3f0eb9dc0f83238c98d881	#####	CN=SubCA242,	01.09.2022 12:37	Suspended: Certificat 3bfa0b12f2f3d	REVOKED	CN=OCSP	#####	OCSP	02.09.2022 9:54	OCSP	dNSName=OCSP, Domain Cont	RSA	#####	2048	
17	3e352d5bf49cf83238c98d881	#####	CN=SubCA242,	01.09.2022 18:34	Suspended: Certificat 1dc1aac2042d3d	REVOKED	CN=paukan	#####	paukan	#####	paukan	rfc822name=pauk Smartcard Lo	RSA	#####	2048	
18	4810c3f5cbbbf83238c98d881	#####	CN=SubCA242,	01.09.2022 13:28	Suspended: Certificat 35e3f0c041cc8	REVOKED	CN=testop	#####	testop	#####	testop	rfc822name=swsd WEB-Client	RSA	#####	1024	
19	3614f6c6c3245f83238c98d881	#####	CN=SubCA242,	01.09.2022 15:01	Suspended: Certificat 201fe017d371d	REVOKED	CN=DC	#####	DC	#####	DC	dNSName=DC, gu Domain Cont	RSA	#####	2048	
20	472b6a99d373f83238c98d881	#####	CN=SubCA242,	Active	762a8430c03565	ACTIVE	CN=operator	#####	operator	#####	operator	rfc822name=swsd WEB-Client	RSA	#####	2048	
21	8b5c6e050346f83238c98d881	#####	CN=SubCA242,	01.09.2022 17:30	Suspended: Certificat 7061a34d5576b	REVOKED	CN=operator	#####	operator	#####	operator	rfc822name=test WEB-Client	RSA	#####	2048	
22	06335097415bf83238c98d881	#####	CN=SubCA242,	01.09.2022 15:57	Suspended: Certificat 2df664eb41687	REVOKED	CN=paukan	#####	paukan	#####	paukan	rfc822name=pauk Smartcard Lo	RSA	#####	2048	
23	01f4dade2341f83238c98d881	#####	CN=SubCA242,	01.09.2022 16:37	Suspended: Certificat 124f0965c59bc	REVOKED	CN=Guest	#####	Guest	#####	Guest	dNSName=Guest, Domain Cont	RSA	#####	2048	
24	07e0809ca0bf83238c98d881	#####	CN=SubCA242,	01.09.2022 17:49	Suspended: Certificat 5fa7b4816ce9f	REVOKED	CN=test	#####	test	#####	test	rfc822name=test Smartcard Lo	RSA	#####	2048	
25	fc8bcd2875a1ef83238c98d881	#####	CN=SubCA242,	04.09.2022 12:03	Revoked: Cessation c 6ed38ad110d43	HOLD	CN=kruchinina	#####	kruchinina	05.09.2022 0:37	kruchinina	rfc822name=alexe Smartcard Lo	RSA	#####	2048	
26	ad3e9bed85d1f83238c98d881	#####	CN=SubCA242,	04.09.2022 8:50	Suspended: Certificat 365612cc14a7f9	REVOKED	CN=CPIP* PIP	#####	CPIP* PIP	#####	CPIP* PIP	rfc822name=dfsd Smartcard Lo	RSA	#####	2048	
27	23421a1f5bdc0f83238c98d881	#####	CN=SubCA242,	Active	513c1b4479c38c	ACTIVE	CN=OP2_242	#####	OP2_242	#####	OP2_242	rfc822name=swsd WEB-Client	RSA	#####	2048	
28	8defcb24f54df83238c98d881	#####	CN=SubCA242,	04.09.2022 12:02	Revoked: Cessation c 4d70ce1e01f42f	HOLD	CN=CLIENT2	#####	CLIENT2	#####	CLIENT2	dNSName=CLIENT1 Domain Cont	RSA	#####	2048	
29	9ba4eecd5179f83238c98d881	#####	CN=SubCA242,	05.09.2022 15:58	Active	666bb74489ed	ACTIVE	CN=OCSP	#####	OCSP	02.09.2022 9:54	OCSP	dNSName=OCSP, Domain Cont	RSA	#####	2048
30	c7f385322b4aef83238c98d881	#####	CN=SubCA242,	Active	17b0c96979939c	ACTIVE	CN=OP1_242	#####	OP1_242	#####	OP1_242	rfc822name=op1 WEB-Client	RSA	#####	2048	
31	df1f61efba662f83238c98d881	#####	CN=SubCA242,	04.09.2022 12:03	Revoked: Cessation c 3c131d883996d	HOLD	CN=koltakova	#####	koltakovav	#####	koltakovav	rfc822name=eaca Smartcard Lo	RSA	#####	2048	
32	88bb73a7ae71f83238c98d881	#####	CN=SubCA242,	05.09.2022 16:11	Revoked: Cessation c 7a9e5b17cf1c57	HOLD	CN=testuser2	#####	testuser2	#####	testuser2	rfc822name=testu Smartcard Lo	RSA	#####	2048	

Рисунок 99 – Пример экспортированного файла списка выпущенных сертификатов.csv

## 7.4.9 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 100).



Мастер выполнения массовых операций

Шаг 1 / 4

Выберите тип операции

Тип операции

Возобновить действие

Приостановить

Отозвать

Отмена Продолжить →

Рисунок 100 – 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».
- На следующем шаге, до применения поиска в левом столбце окна будут отображены первые 100 сертификатов с соответствующим статусом (в зависимости от выбранной операции на шаге 1) в алфавитном порядке по атрибуту Common Name. В случае, если найдено более 100 сертификатов соответствующего выбранной операции статуса, то требуется уточнить параметры поиска сертификатов.

Также возможно осуществить поиск сертификатов по отличительному имени субъекта Subject Distinguished Names, для которых требуется применить выбранную операцию, в левом столбце окна Шага 2 (см. Рисунок 101). Поиск сертификатов производится с учётом текущего статуса сертификата и выбранного типа операции на шаге 1, отображается не более 100 результатов поиска, для выбора более 100 сертификатов требуется уточнить и повторить поиск.

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.

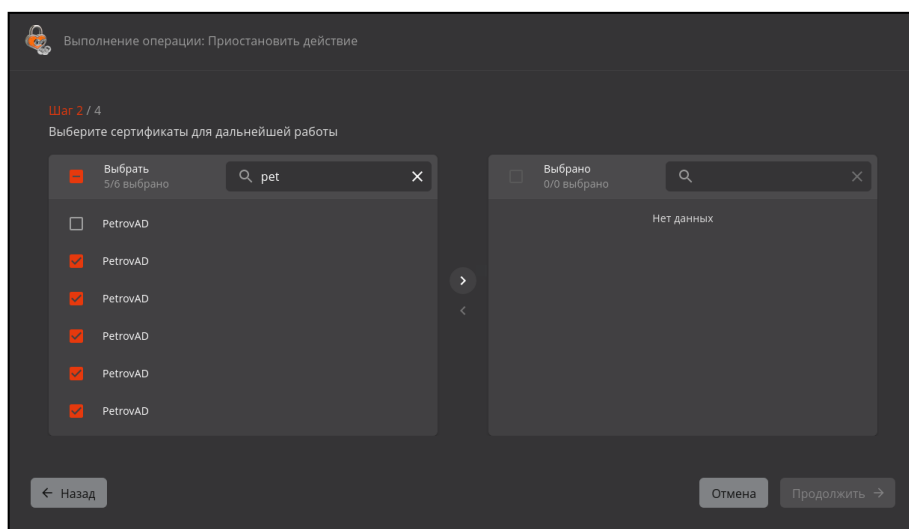



Рисунок 101 – Окно выполнения массовых операций. Шаг 2. Создание списка выбранных сертификатов

- 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 .

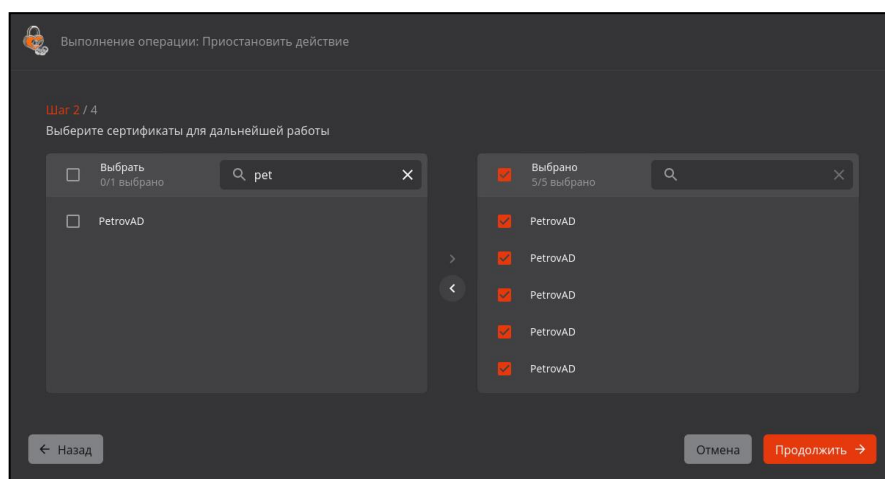


Рисунок 102 – Окно выполнения массовых операций. Шаг 2. Редактирование списка выбранных сертификатов

- Для перехода на следующий шаг нажмите кнопку <Продолжить>.
- В открывшемся окне подтвердите действие, нажав кнопку «Применить» (см. Рисунок 103).

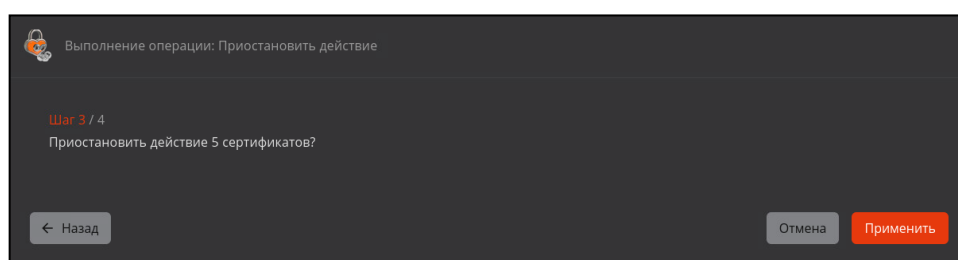


Рисунок 103 – Окно выполнения массовых операций. Шаг 3

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

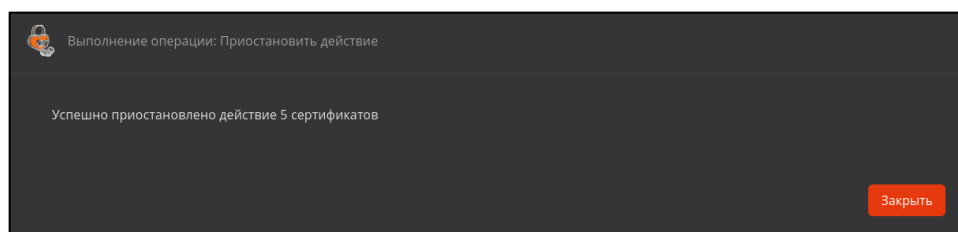


Рисунок 104 – Окно выполнения массовых операций. Шаг 4

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 105).

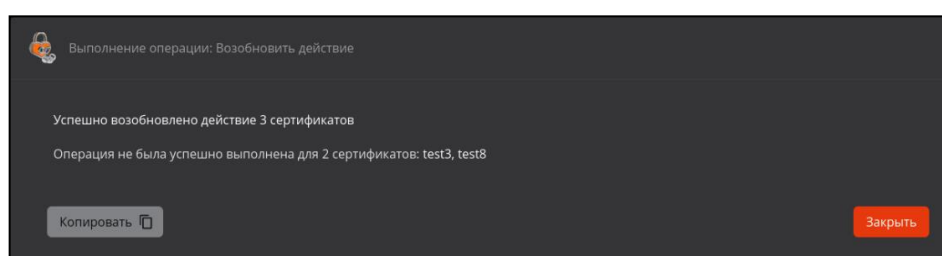


Рисунок 105 – Окно выполнения массовых операций. Шаг 4. Перечень сертификатов, для которых операция не была завершена успешно

## 7.5 Настройка уведомлений об истечении срока действия сертификата

Программный компонент «Центр сертификации Aladdin eCA» поддерживает возможность уведомления пользователей по электронной почте об истечении срока действия сертификатов.

- Отправка уведомлений об истечении срока действия сертификата фиксируется в Журнале событий с кодом CAENV054 «отправка уведомления на почту». События сохраняются в таблицу базы данных «аесаса» (имя базы данных по умолчанию, конфигурация базы данных указана в файле /opt/aecaCa/scripts/config.sh), схема базы данных «delivery», таблица «delivery\_log».
- При использовании настроек по умолчанию программа однократно отправит электронные письма с уведомлением по следующему расписанию:
  - 30 дней до истечения срока;
  - 7 дней до истечения срока;
  - 1 день до истечения срока.
- По умолчанию эти уведомления будут отправлены по электронной почте, указанной в атрибуте «msUPN» доменного пользователя, срок действия сертификата которого истекает.
- Условия выполнения уведомления об истечении срока действия сертификата субъекта:
  - статус сертификата, срок которого истекает – активный;
  - для субъекта, сертификат которого истекает, определен адрес электронной почты в поле «msUPN»;
  - произведена настройка параметров конфигурационного файла /opt/aecaCa/dist/environment/event-delivery.env. Настройка данного файла осуществляется посредством настройки конфигурационного файла /opt/aecaCa/scripts/config.sh, почтовой программы и успешного обновления программного средства;
  - создан и настроен хотя бы один шаблон уведомлений.

### 7.5.1 Настройка параметров конфигурационного файла config.sh

- Отредактируйте конфигурационный файл config.sh, размещенный по адресу /opt/aecaCa/scripts/config.sh, выполнив команду:

```
sudo nano /opt/aecaCa/scripts/config.sh
```

- Блок настройки уведомлений об истечении срока действия сертификата конфигурационного файла /opt/aecaCa/scripts/config.sh и описание настроек приведены в Таблица 16.

Таблица 16 – Переменные окружения, используемые сервисом event-delivery-service, файла config.sh

Параметр	Значение параметра по умолчанию	Описание
<b>Переменные окружения, используемые event-delivery-service</b>		
email_host	127.0.0.1	укажите ip-адрес почтового сервера
email_port	25	укажите порт почтового сервера
email_login	aeca	укажите логин пользователя, под которым производится авторизация в почтовом сервере
email_password	aeca	введите пароль пользователя, под которым производится авторизация в почтовом сервере

Параметр	Значение параметра по умолчанию	Описание
email_from	no_reply@aeca.ru	укажите адрес почты, с которой будет производиться рассылка уведомлений
email_schedule	'0 0 12 * * *'	укажите период проверки в виде CRON-выражения, по которому будет выполняться проверка сроков действия сертификатов и рассылка уведомлений (по умолчанию - каждый день в полдень (12:00))
email_enabled	true	Флаг отправки почтовых уведомлений, если выкл. то сообщения не отправляются, но помечаются, как отправленные
email_protocol	smtp	Протокол подключения к почтовому серверу
email_smtp_auth	false	Флаг: использование SMTP-авторизации
email_start_tls	false	Флаг: использование директивы start tls при подключении к почтовому серверу

- Для применения внесенных настроек следует запустить сценарий обновления, выполнив команду:

```
sudo bash /opt/aecaCa/scripts/install.sh
```

Установщик обнаружит установленную версию программного компонента и предложит выбрать необходимое действие в интерактивном режиме, для запуска процесса обновления введите в терминале цифру «2». По окончании процесса обновления программы выполненные настройки конфигурационного файла будут применены.

### 7.5.2 Настройка шаблонов уведомлений об истечении срока действия сертификата

- В базе данных в таблице «delivery.delivery\_template» хранится набор шаблонов рассылки уведомлений.
- Каждый шаблон определяет следующие параметры отправки уведомления:
  - наименование шаблона;
  - признак необходимости запуска выполнения действий по этому шаблону;
  - отслеживание времени окончания срока действия сертификата, для отправки уведомлений в установленный в шаблоне срок.
  - тему письма, указанную при отправке уведомления.
- По умолчанию созданы шаблоны, описанные в Таблица 17.

Таблица 17 – Шаблоны, настроенные по умолчанию

ID	Наименование шаблона	Признак запуска	Время, отслеживаемое до окончания действия сертификата, мс	Тема отправляемого письма
1	30 дней	ACTIVE	2592000000	Срок действия Вашего сертификата истекает через 30 дней
2	7 дней	ACTIVE	604800000	Срок действия Вашего сертификата истекает через 7 дней
3	1 день	ACTIVE	86400000	Рассылка об истечении срока действия сертификата через 1 день

- Уведомление формируется по следующим правилам:
  - тема письма в соответствии с указанной в шаблоне;
  - текст письма в соответствии с данными сертификата. Текст письма имеет формат, приведенный в листинге:

```
Здравствуйте, {certificate.username}!
Время действия сертификата истекает {certificate.expire_date}

Фингерпринт сертификата: {certificate.fingerprint}
Серийный номер сертификата: {certificate.serial_number}
```

- Для просмотра списка существующих шаблонов уведомлений выполните команду:

```
sh /opt/aecaCa/scripts/email_config.sh -list
```

- Отредактируйте существующий шаблон при необходимости, выполнив команду:

```
sh /opt/aecaCa/scripts/email_config.sh -edit <id> <name> <subject> <interval>
<status>
```

где:

`id` - идентификатор существующего шаблона;  
`template_name` - название шаблона;  
`subject` - тема сообщения;  
`interval` - время до окончания срока действия сертификата в мс;  
`status` - статус рассылки (ACTIVE, INACTIVE).

Пример редактирования шаблона уведомления:

```
bash /opt/aecaCa/scripts/email_config.sh -edit 4 "2 часа" "Истекает через 2 часа"
7200000 INACTIVE
```

- Для создания нового шаблона уведомлений выполните команду:

```
sh /opt/aecaCa/scripts/email_config.sh -new <name> <subject> <interval> <status>
```

где:

`id` - идентификатор существующего шаблона;  
`name` - название шаблона;  
`subject` - тема сообщения;  
`interval` - время до окончания срока действия сертификата в мс;  
`status` - статус рассылки (ACTIVE, INACTIVE).

- Пример создания нового шаблона уведомлений:

```
./email_config.sh -new "1 час" "Истекает через час" 3600000 INACTIVE
INSERT 0 1
```

id	template_name	subject	interval	status
1	30 дней	Срок истекает через 30 дней.	2592000000	ACTIVE
2	7 дней	Срок истекает через 7 дней.	604800000	ACTIVE
3	1 день	Срок истекает через 1 день.	86400000	ACTIVE
4	1 час	Истекает через час	3600000	INACTIVE

(4 строки)

- Для применения внесенных настроек следует перезапустить сервис, выполнив команду:

```
sudo systemctl restart aeca-ca.service
```

### 7.5.3 Настройка параметров почтового ящика пользователя

- Указанный в шаблоне почтовый ящик пользователя, должен иметь следующие настройки:
  - разрешен доступ к почтовому ящику с помощью почтовых клиентов;
  - отключить автоматическое удаление писем, помеченных в IMAP как удалённые;
  - разрешить доступ по протоколу POP3.

#### 7.5.3.1 Настройка почтовой программы Яндекс.Почта

- Настройка почтовой программы показана на примере настройки Яндекс.Почта (см. Рисунок 106).

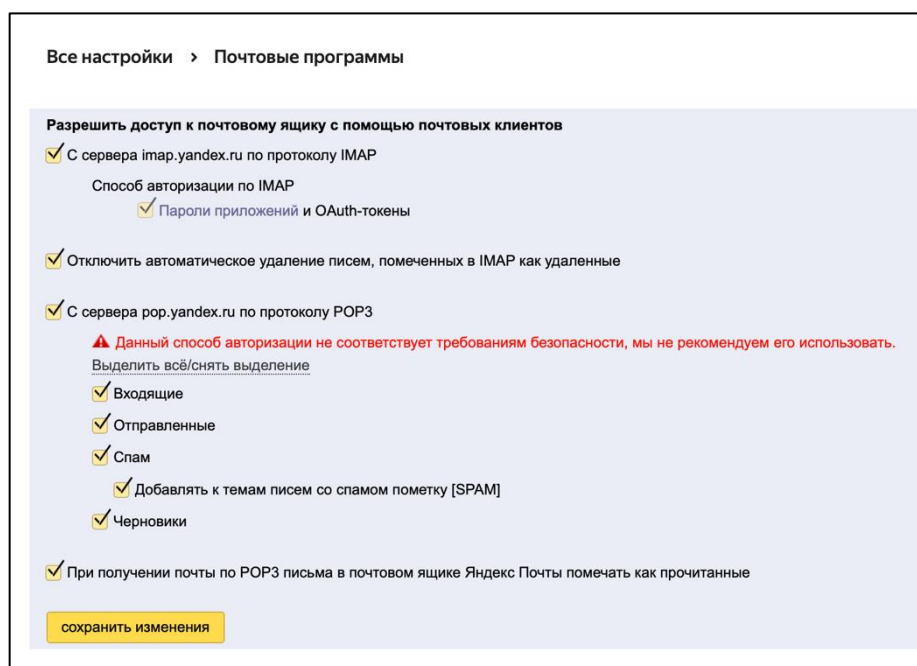


Рисунок 106 – Настройки почтового ящика Яндекс.Почта для получения уведомления об истечении срока сертификата

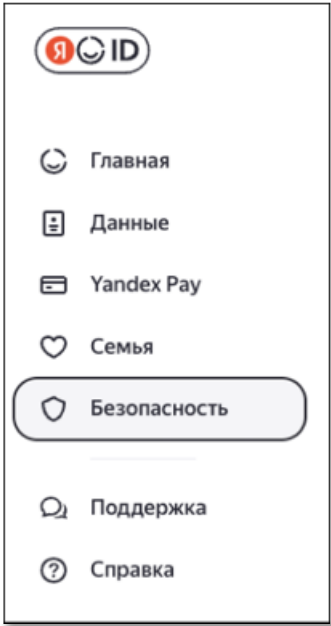
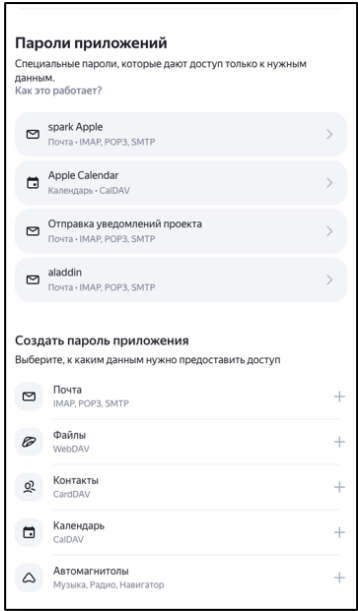
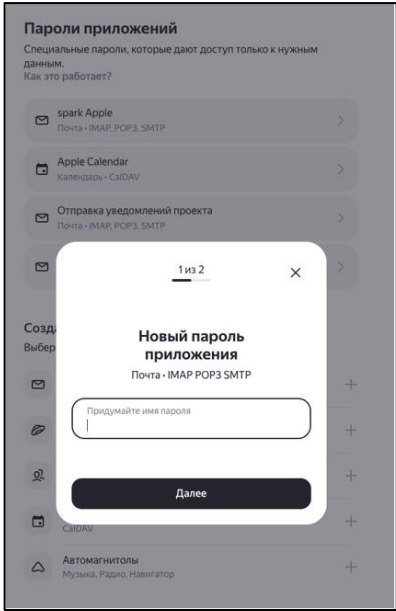
1. В настройках аккаунта Яндекс.Почты выберите пункт меню «Безопасность» (см. Рисунок 264).

2. Перейдите в раздел «Доступ к вашим данным» (см. Рисунок 108).



Рисунок 108 – Подраздел «Доступ к вашим данным» аккаунта почтового ящика Yandex



<div data-bbox="317 212 649 835"></div> <div data-bbox="210 853 770 925"><p>Рисунок 107 – Раздел «Безопасность» аккаунта почтового ящика Yandex</p></div>	
<div data-bbox="188 958 813 1043"><p>3 • Перейдите в подраздел «Пароли приложений» (см. Рисунок 109)</p></div> <div data-bbox="304 1057 663 1666"></div> <div data-bbox="201 1684 780 1756"><p>Рисунок 109 – Подраздел «Пароли приложений» аккаунта почтового ящика Yandex</p></div>	<div data-bbox="866 958 1505 1043"><p>4 • Перейдите в подраздел «Почта», «Создать пароль приложения» (см. Рисунок 110)</p></div> <div data-bbox="965 1057 1362 1666"></div> <div data-bbox="906 1684 1439 1722"><p>Рисунок 110 – Создание пароля приложения</p></div>
<div data-bbox="188 1787 798 1897"><p>5 Новый пароль необходимо сохранить. При потере восстановление невозможно. Возможен сброс и создание нового.</p></div>	<div data-bbox="866 1787 1468 1897"><p>6 Данный пароль необходимо внести в конфигурационный файл <code>config.sh</code> в параметр <code>email_password</code></p></div>

### 7.5.3.2 Настройка почтовой программы MS Exchange

- Настройка почтовой программы показана на примере настройки MS Exchange (см. Рисунок 111). Убедитесь, что настроен протокол SMTP в настройках MS Exchange.

**При настройке протокола SMTP почтового ящика по умолчанию должен быть выбран 587 порт.**

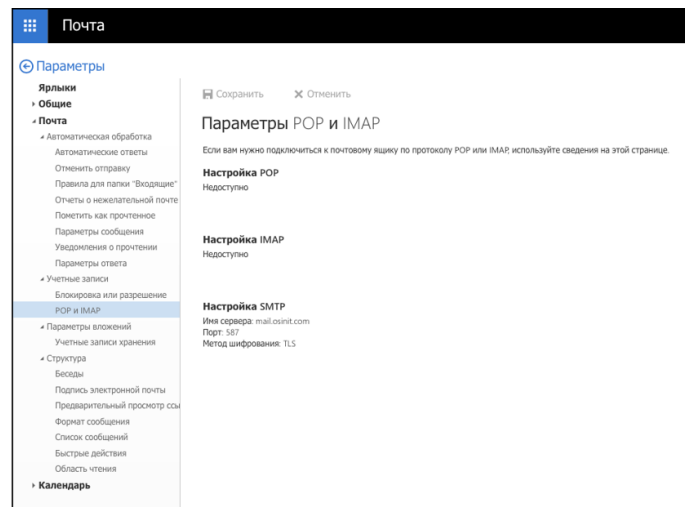


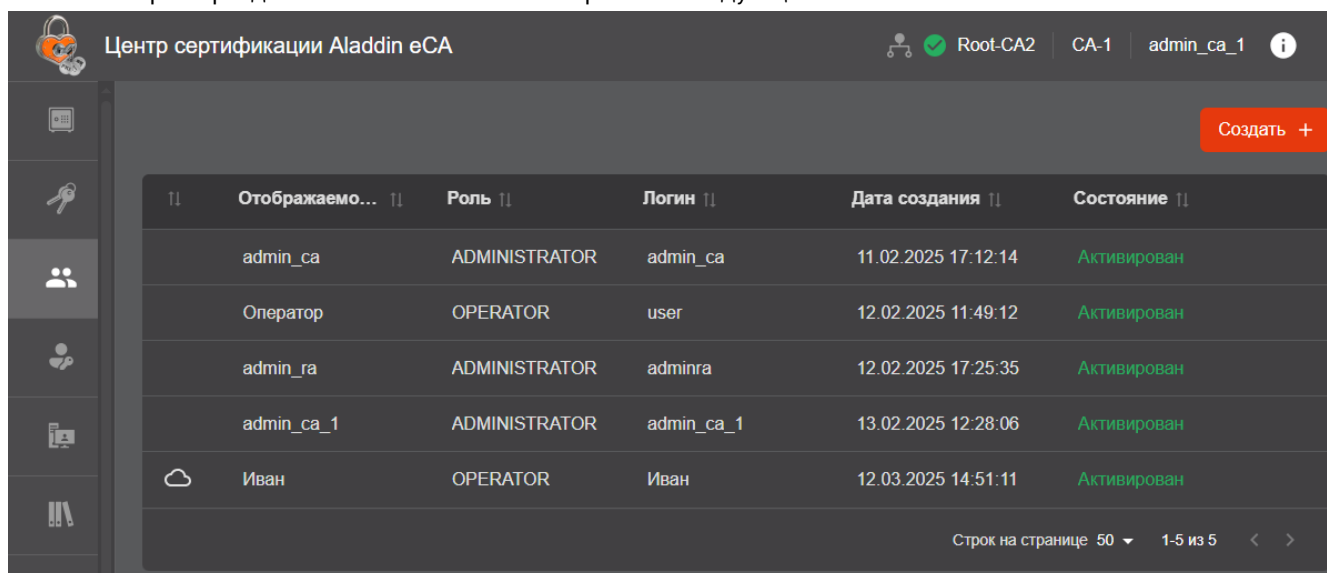
Рисунок 111 – Настройки почтового ящика MS Exchange для получения уведомления об истечении срока сертификата

## 7.6 Раздел «Учётные записи»

Раздел «Учётные записи» обеспечивает возможности управления доступом к интерфейсам управления на основе ролей, а также управление данными и ограничениями данных.

Переход к разделу «Учётные записи» осуществляется по выбору раздела «Учётные записи» бокового меню, расположенного слева на главном экране (см. Рисунок 112).

На экране раздела «Учётные записи» отображены следующие поля:





Отображаемо...	Роль	Логин	Дата создания	Состояние
admin_ca	ADMINISTRATOR	admin_ca	11.02.2025 17:12:14	Активирован
Оператор	OPERATOR	user	12.02.2025 11:49:12	Активирован
admin_ra	ADMINISTRATOR	adminra	12.02.2025 17:25:35	Активирован
admin_ca_1	ADMINISTRATOR	admin_ca_1	13.02.2025 12:28:06	Активирован
 Иван	OPERATOR	Иван	12.03.2025 14:51:11	Активирован

Рисунок 112 – Экран раздела меню «Учётные записи»

-  – соответствующий символ обозначает, что данная учётная запись создана для субъекта внешней (подключенной) ресурсной системы;
- отображаемое имя – идентифицирует владельца учетной записи, соответствует полю «Отображаемое имя» в окне создания учётной записи;
- роль – указывает набор дискретных прав. Возможные роли:
  - Оператор – обладает правами на работу с субъектами группы, над которой он может осуществлять свои ролевые права, и принадлежащими им сертификатами (выпуск, отзыв, приостановка и возобновление сертификата), имеет полномочия запуска обновления списка субъектов. Таким образом оператору доступны следующие разделы:
    - «Сертификаты», где доступны сертификаты субъектов, на которые оператору предоставлены права в соответствии с правилами доступа.
    - «Субъекты», где доступны субъекты ресурсных систем, на которые оператору предоставлены права в соответствии с правилами доступа, и принадлежащим им сертификатам, без прочих ограничений.
    - «Ресурсные системы», где доступен запуск синхронизации субъектов ресурсной системы, на которую оператору предоставлены права в соответствии с правилами доступа.
    - «Шаблоны», где доступен просмотр шаблонов, на которые оператору предоставлены права в соответствии с правилами доступа.
  - Администратор – обладает неограниченными возможностями, в том числе имеет доступ к управлению учетными записями и может делегировать полномочия Оператору на просмотр и использование шаблонов при создании сертификатов для субъектов, а также на работу с субъектами групп безопасности ресурсных систем;

- логин – показывает параметр учетной записи для авторизации, содержит Common Name субъекта. Логины учетных записей должны быть уникальными;
- дата создания – показывает дату создания учётной записи;
- состояние – отображает состояние учётной записи (активирован или заблокирован).

Вход под учётной записью пользователя на сервер осуществляется при помощи сертификата, выпущенного с использованием шаблона «Web-client». Подробнее о настройке аутентификации для входа в учётную запись см. раздел 4 настоящего руководства.

В программе отслеживается и фиксируются дата и время последней активности пользователей. Операциями, обновляющими запись о последней активности пользователя, являются:


- успешная аутентификация, включая аутентификацию в Центре регистрации Aladdin eRA;
- успешное обновление маркера доступа, включая его обновление в Центре регистрации Aladdin eRA.

Центр сертификации Aladdin eCA автоматически блокирует учетные записи пользователей с ролью «Оператор», период пассивности которых превысил значение, указанное в параметре `block_inactive_account_delay`<sup>26</sup> конфигурационного файла. Запуск проверки периода неактивности и блокировка соответствующих учетных записей пользователей с ролью «Оператор» выполняются по расписанию в соответствии со значением параметра `block_inactive_account_cron`<sup>27</sup> конфигурационного файла.

**При обновлении ПО с версии 2.1 на 2.2 для всех существующих в программе на момент обновления учетных записей в качестве даты и времени последней активности в базу данных записывается дата и время выполнения обновления.**

#### 7.6.1 Создание учётной записи пользователя локального ресурса

Порядок создания учетной записи для пользователя Центра сертификации Aladdin eCA:

- На панели слева выберите раздел «Учетные записи» .
- Нажмите кнопку **Создать +** (см. Рисунок 112).
- В открывшемся окне выполните следующие действия (см. Рисунок 113):
  - выберите роль учетной записи;
  - укажите имя, которое отображается на верхней панели веб-интерфейса после авторизации пользователя;
  - логин – имя учетной записи (данные для поля «Common Name» при выпуске сертификата пользователя).

**ВНИМАНИЕ! Логины (имена) учетных записей должны быть уникальными.**

<sup>26</sup> По умолчанию в данном параметре указано значение «0», обозначающее отсутствие ограничения на неактивность пользователей.

<sup>27</sup> По умолчанию – каждую полночь.

Рисунок 113 – Окно создания новой учётной записи локального пользователя

- Нажмите кнопку **Создать**.
- Для созданной учетной записи пользователя с ролью «Оператор» создайте правила доступа шаблонам и субъектам (см. подраздел 7.6.5).
- Для созданной учетной записи Администратора настройка прав не требуется, так как ограничений для этой роли не будет.

### 7.6.2 Создание учетной записи для подключенного субъекта

Для создания учётной записи доменного пользователя перейдите в раздел «Субъекты» Центра сертификации и создайте учётную запись в соответствии с разделом 7.8.8 настоящего руководства.

### 7.6.3 Изменение статуса учётной записи

При наведении курсора на строку с данными выбранной учётной записи отображаются инструменты управления учетной записью (возможность управления статусом текущей учётной записи) (см. Рисунок 114):

- по нажатию кнопки <Заблокировать> **Заблокировать** возможно приостановить действие активной выбранной учётной записи или
- по нажатию кнопки <Активировать> **Активировать** действие заблокированной ранее учётной записи будет возобновлено.

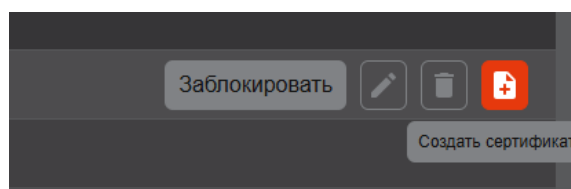


Рисунок 114 – Доступные действия над учетными записями

### 7.6.4 Редактирование учётной записи

- По нажатию на кнопку <Редактировать> **Редактировать** (в строке учётной записи) открывается карточка учётной записи, содержащая следующие поля (см. Рисунок 115):
  - редактируемый выбор назначенной роли;
  - редактируемое отображаемое имя (ФИО);

- таблицу с параметрами сертификатов («CN», «Дата создания», «Действителен до» и «Состояние»), которые привязаны к учетной записи. У каждого сертификата редактируемый статус (доступные действия приведены в Таблица 15), а также кнопку скачивания сертификата в формате .pem.
- Переход в карточку связанного сертификата возможен по нажатию на строку выбранного сертификата в карточке учётной записи.

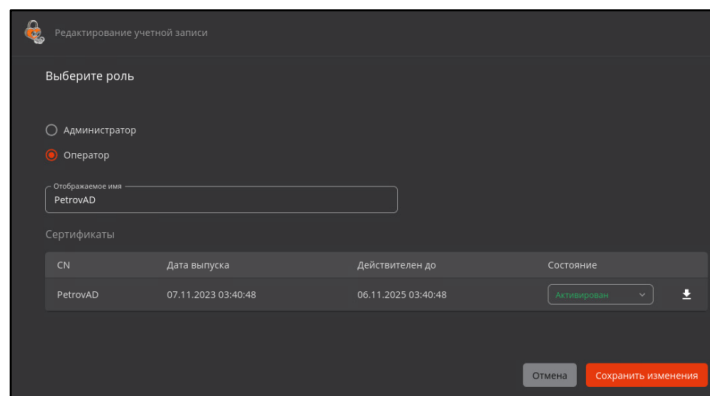



Рисунок 115 – Окно редактирование учётной записи

- Карточка учётной записи, которая в текущий момент авторизована, доступна только для просмотра.

#### 7.6.5 Назначение прав оператору

Для назначения прав оператору перейдите в раздел «Правила доступа» Центра сертификации и произведите назначение прав в соответствии с разделом 7.7 настоящего руководства.

#### 7.6.6 Удаление учётной записи

- По нажатию на кнопку <Удалить>  (в строке учётной записи) открывается окно подтверждения удаления учётной записи (см. Рисунок 116)

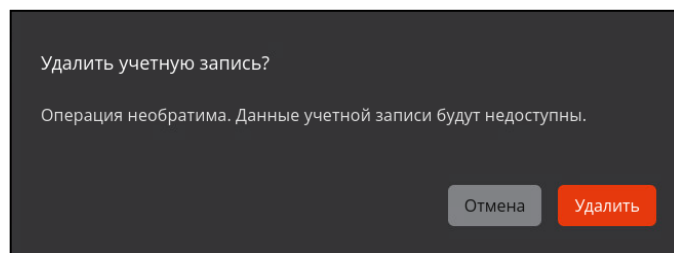



Рисунок 116 – Окно подтверждения удаления учётной записи

- После подтверждения действия нажатием кнопки <Удалить> администратор будет уведомлён всплывающим сообщением «Пользователь успешно удалён!».

#### 7.6.7 Выпуск сертификата для учетной записи

- По нажатию на кнопку <Создать сертификат>  (в строке учётной записи) в выпадающем меню выберите способ выпуска (см. Рисунок 117):
  - с закрытым ключом;
  - на ключевом носителе.
- Сертификат будет создан с использованием внутреннего шаблона ECA-Auth. Значение поля «Common Name», будет заполнено автоматически и соответствовать логину учетной записи, для которой выпускается сертификат.

- Более подробно процедура выпуска сертификата приведена в «Приложение 1. Создание сертификата для субъекта».

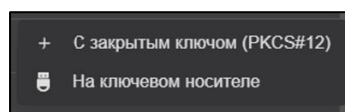


Рисунок 117 – Раздел «Учетные записи». Кнопка выпуска сертификата

## 7.7 Раздел «Правила доступа»

Раздел «Правила доступа» обеспечивает возможность предоставления пользователям с ролью «Оператор», а также группам безопасности зарегистрированных ресурсных систем<sup>28</sup> доступа на:

- просмотр и редактирование субъектов, создание, управление статусом и публикацию их сертификатов;
- просмотр и использование шаблонов при создании сертификатов для субъектов.

Оператору при отсутствии правил доступа, по которым ему прямо или косвенно (через наследование от группы безопасности, в которую входит субъект, на основе которого была создана учетная запись данного оператора) предоставлен доступ к шаблонам, будет недоступен просмотр и использование при создании сертификатов всех существующих в программе шаблонов.

Переход в раздел «Правила доступа» осуществляется через боковое меню, расположенное слева на главном экране (см. Рисунок 50).

В данном разделе отображаются все существующие правила доступа (см. Рисунок 118).

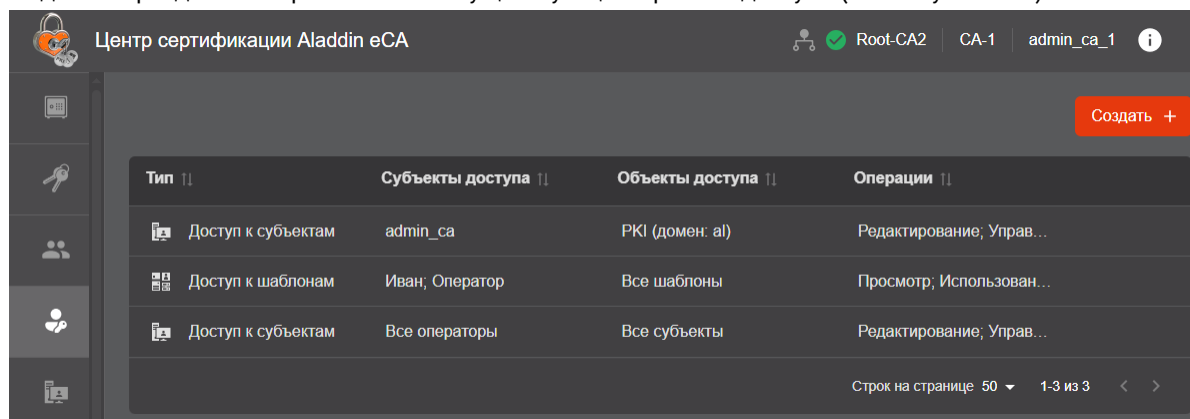


Рисунок 118 - Экран раздела меню «Правила доступа»

- На экране раздела «Правила доступа» отображены информационные элементы (табличные поля):
  - поле «Тип», отображающее тип правила доступа. Допустимые варианты значений в данном поле:
    - Доступ к шаблонам;
    - Доступ к субъектам.
  - поле «Субъекты доступа», содержащее перечень пользователей с ролью «Оператор», а также групп безопасности зарегистрированных ресурсных систем, которым предоставлен доступ в соответствии с правилом;
  - поле «Объекты доступа», содержащее перечень объектов доступа в соответствии с данным правилом. Объектами доступа в зависимости от типа правила могут являться шаблоны или группы безопасности;

<sup>28</sup> Назначение правил доступа группам безопасности зарегистрированных ресурсных систем предназначено обеспечивать возможность для наследования данных правил операторами, учетные записи которых созданы на основе субъектов данных групп безопасности.

- поле «Операции», содержащее печенье допустимых операций, которые могут выполнять субъекты доступа с объектами доступа.
- Доступны следующие операции по работе с правилами доступа:
  - просмотр списка правил доступа;
  - создание нового правила доступа;
  - редактирование правила доступа;
  - удаление правила доступа.

**При обновлении Aladdin eCA CE с версии 2.1 на версию 2.2 в правилах доступа субъекты или объекты доступа, являющиеся подразделениями зарегистрированных ресурсных систем, будут удалены. Если в правиле доступа все субъекты или объекты доступа являются подразделениями зарегистрированных ресурсных систем, то такое правило будет удалено.**

**При обновлении Aladdin eCA CE с версии 2.1 на версию 2.2 субъекты локальной ресурсной системы перестают быть членами подразделения «Local» (данное подразделение использовалось в правилах доступа для выдачи полномочий на локальную ресурсную систему). Все субъекты локальной ресурсной системы становятся членами группы «Локальные субъекты».**

#### 7.7.1 Создание правила доступа

- По нажатию кнопки «Создать +» на главном экране раздела «Правила доступа» происходит запуск сценария создания правила доступа.
- В открывшемся окне «Создание правила доступа» на шаге 1 выберите тип правила доступа из следующих вариантов (см. Рисунок 119):
  - Доступ к шаблонам (выбран по умолчанию);
  - Доступ к субъектам.

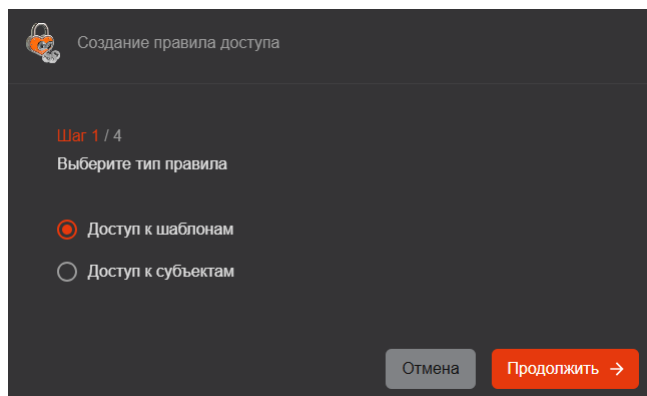


Рисунок 119 – Шаг 1 окна «Создание правила доступа»

- На шаге 2 окна «Создание правила доступа» выберите субъекты доступа. Допустимые варианты выбора субъектов доступа:



- выбор перечня субъектов доступа вручную при включении режима «Выбрать операторов или группы» (см. Рисунок 120). При выборе данного режима доступен выбор типа субъектов доступа (оператор или группа) для отображения. В поле «Выбрать» необходимо выбрать субъекты доступа, при необходимости воспользовавшись поиском, затем перенести их в поле «Выбрано» путем нажатия на стрелку вправо. В поле «Выбрано» будут присутствовать все ранее добавленные в него субъекты доступа вне зависимости от того, какой тип для отображения субъектов доступа выбран для поля «Выбрать». Для исключения субъектов доступа из поля «Выбрано» необходимо выделить их и перенести обратно в поле «Выбрать» путем нажатия на стрелку влево. В случае, если в поле «Выбрано» не добавлен ни один субъект доступа, переход на следующий шаг недоступен;

Рисунок 120 – Шаг 2 окна «Создание правила доступа» при выборе режима «Выбрать операторов или группы»

- выбор всех операторов или групп при включении режима «Все операторы» (см. Рисунок 121). При выборе данного режима субъектами доступа будут являться все пользователи с ролью «Оператор», а также все группы безопасности зарегистрированных ресурсных систем (в том числе те, которые будут созданы или получены из ресурсной системы позднее). В данном режиме указание отдельных операторов или групп на данном шаге недоступно.

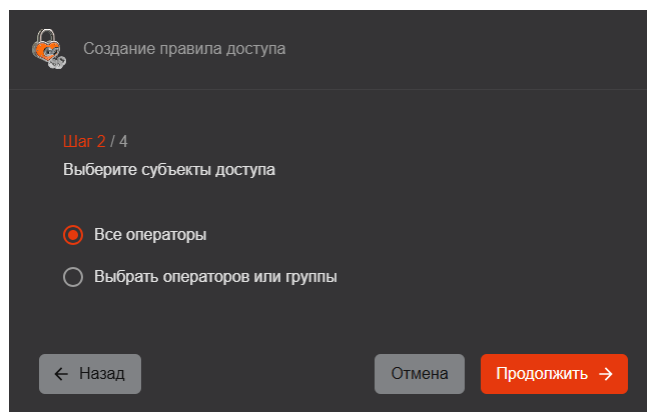


Рисунок 121 – Шаг 2 окна «Создание правила доступа» при выборе режима «Все операторы»

- Переход на следующий шаг осуществляется по ставшей активной кнопке <Продолжить> после выбора субъектов доступа.
- В окне «Создание правила доступа» на шаге 3 выберите объекты доступа.
- Если на шаге 1 был выбран тип «Доступ к шаблонам», то необходимо выбрать шаблоны, на просмотр и использование которых необходимо предоставить полномочия. Допустимые варианты выбора объектов доступа:
  - выбор шаблонов вручную при включении режима «Выбрать шаблоны» (см. Рисунок 122). В поле «Выбрать» необходимо выбрать шаблоны, при необходимости воспользовавшись поиском, затем перенести их в поле «Выбрано» путем нажатия на стрелку вправо. Для исключения шаблонов из поля «Выбрано» необходимо выделить их и перенести обратно в поле «Выбрать» путем нажатия на стрелку влево. В случае, если в поле «Выбрано» не добавлен ни один шаблон, переход на следующий шаг недоступен;
  - выбор всех шаблонов при включении режима «Все шаблоны» (см. Рисунок 123). При выборе данного режима объектами доступа будут являться все шаблоны (в том числе те, которые будут созданы позднее). При выборе режима «Все шаблоны» указание отдельных шаблонов на данном шаге будет недоступно.

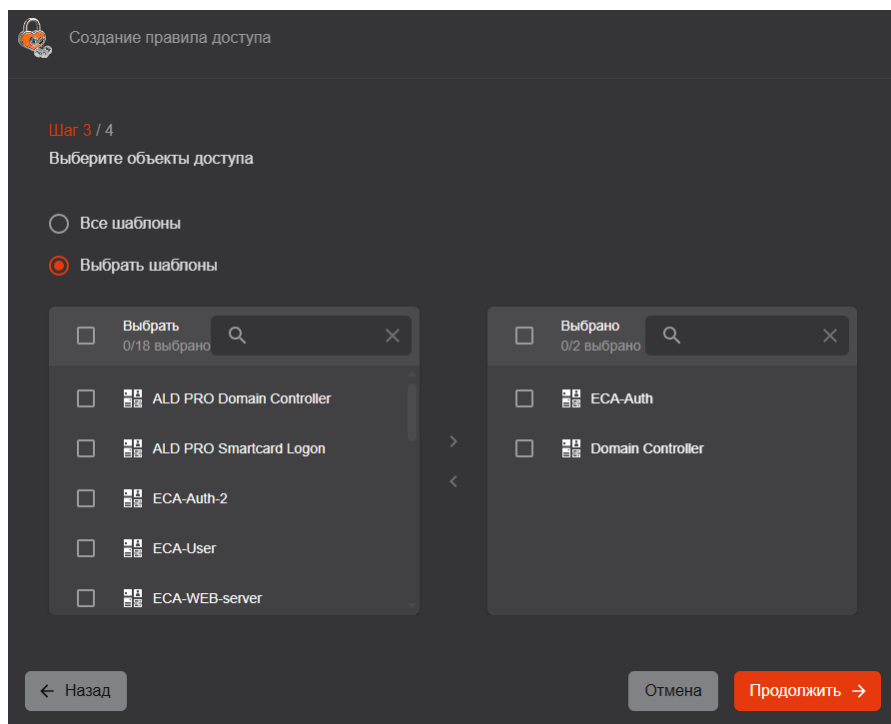


Рисунок 122 – Шаг 3 окна «Создание правила доступа» при выборе режима «Выбрать шаблоны»

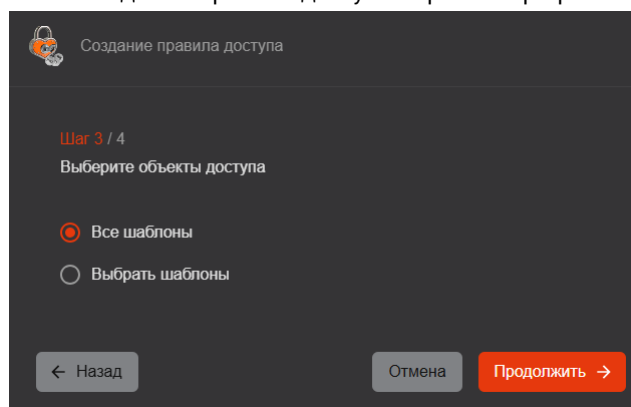


Рисунок 123 – Шаг 3 окна «Создание правила доступа» при выборе режима «Все шаблоны»

- Если на шаге 1 был выбран тип «Доступ к субъектам», то необходимо выбрать субъекты, на просмотр и использование которых необходимо предоставить полномочия. Допустимые варианты выбора объектов доступа:
  - выбор субъектов вручную при включении режима «Выбрать группы» (см. Рисунок 124). В поле «Домен» необходимо выбрать ресурсную систему. В поле «Выбрать» необходимо выбрать группы безопасности, при необходимости воспользовавшись поиском, затем перенести их в поле «Выбрано» путем нажатия на стрелку вправо. Для исключения групп безопасности из поля «Выбрано» необходимо выделить их и перенести обратно в поле «Выбрать» путем нажатия на стрелку влево. В случае, если в поле «Выбрано» не добавлены ни одна группа безопасности или ни один оператор, переход на следующий шаг недоступен;
  - выбор всех субъектов при включении режима «Все субъекты» (см. Рисунок 125). При выборе данного режима объектами доступа будут являться все субъекты зарегистрированных ресурсных систем (в том числе те, которые будут созданы позднее). При выборе режима «Все субъекты» указание отдельных групп безопасности зарегистрированных ресурсных систем на данном шаге будет недоступно.

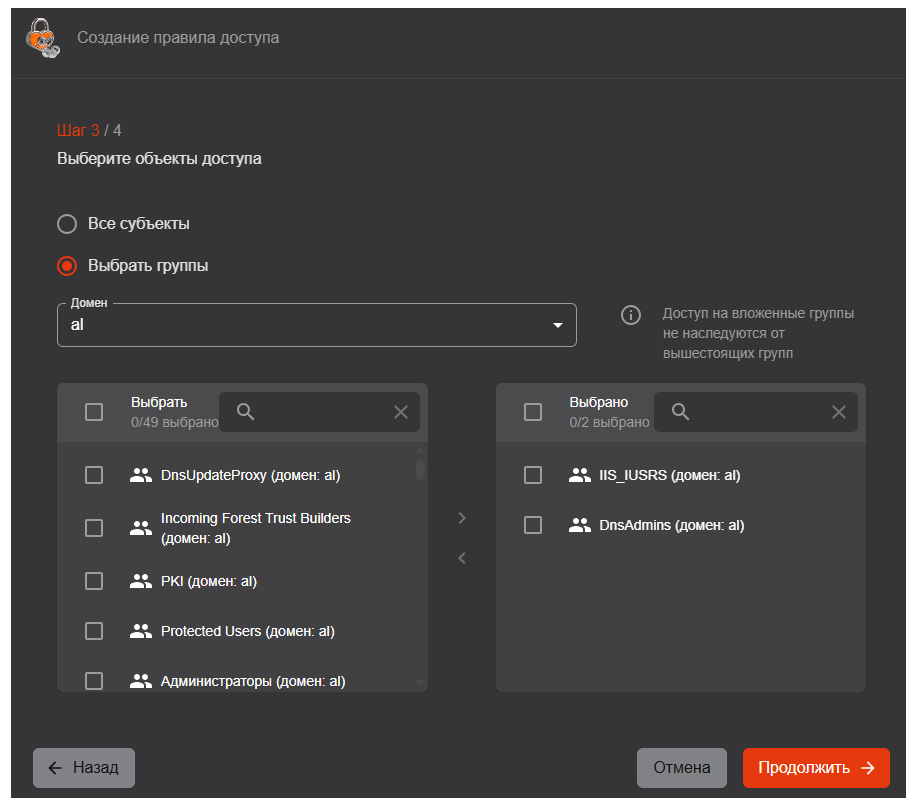


Рисунок 124 – Шаг 3 окна «Создание правила доступа» при выборе режима «Выбрать группы»

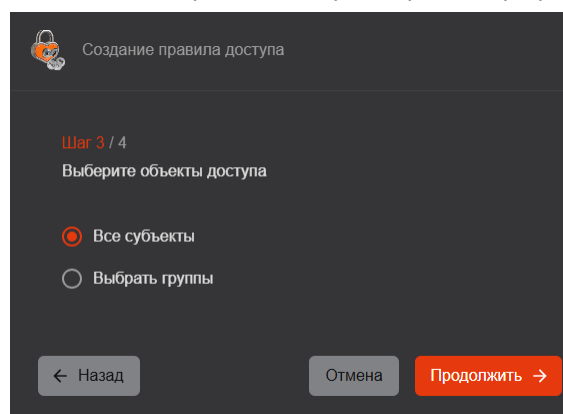


Рисунок 125 – Шаг 3 окна «Создание правила доступа» при выборе режима «Все субъекты»

- Переход на следующий шаг осуществляется по ставшей активной кнопке <Продолжить> после выбора объектов доступа.
- На шаге 4 окна «Создание правила доступа» будет отображена информация о создаваемом правиле доступа, включающая в себя: тип правила, перечень выбранных ранее субъектов доступа и объектов доступа и операции (см. Рисунок 126).

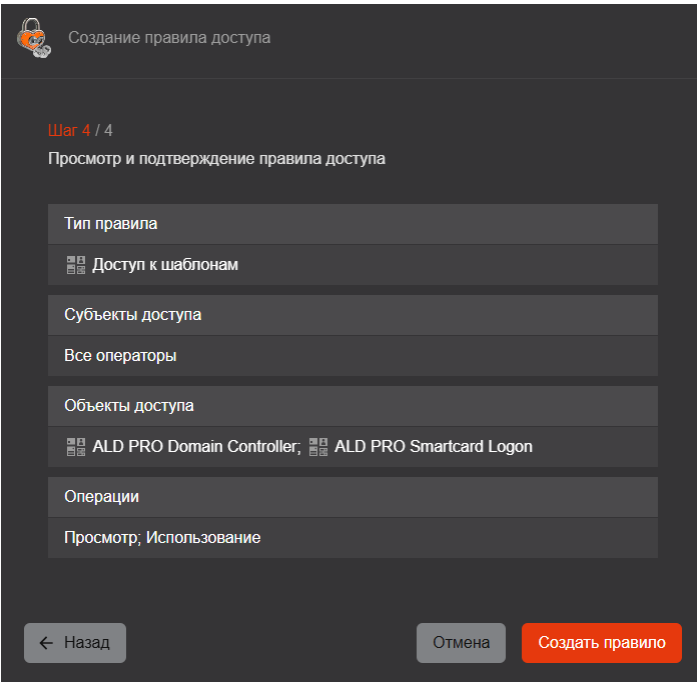



Рисунок 126 – Шаг 4 окна «Создание правила доступа» - «Просмотр и подтверждение правила доступа»

- После нажатия на кнопку «Создать правило» созданное правило будет отображаться в списке правил доступа. После добавления правила доступа субъектам доступа, выбранным на шаге 1 данного сценария, при создании сертификатов для субъектов ресурсных систем будет доступно использование шаблонов, выбранных на шаге 2 данного сценария.

7.7.2 Редактирование правила доступа

После создания правила доступа, при наведении курсора на строку добавленного правила доступа появляется возможность его редактирования – при нажатии на кнопку <Редактировать>  (см. Рисунок 127) открывается окно «Редактирование правила доступа» для редактирования перечня субъектов доступа и объектов доступа, указанных при создании правила доступа (см. Рисунок 128, Рисунок 129, Рисунок 130, Рисунок 131). Управление составом субъектов доступа и объектов доступа в правиле доступа при его редактировании осуществляется аналогично их выбору при создании правила доступа.

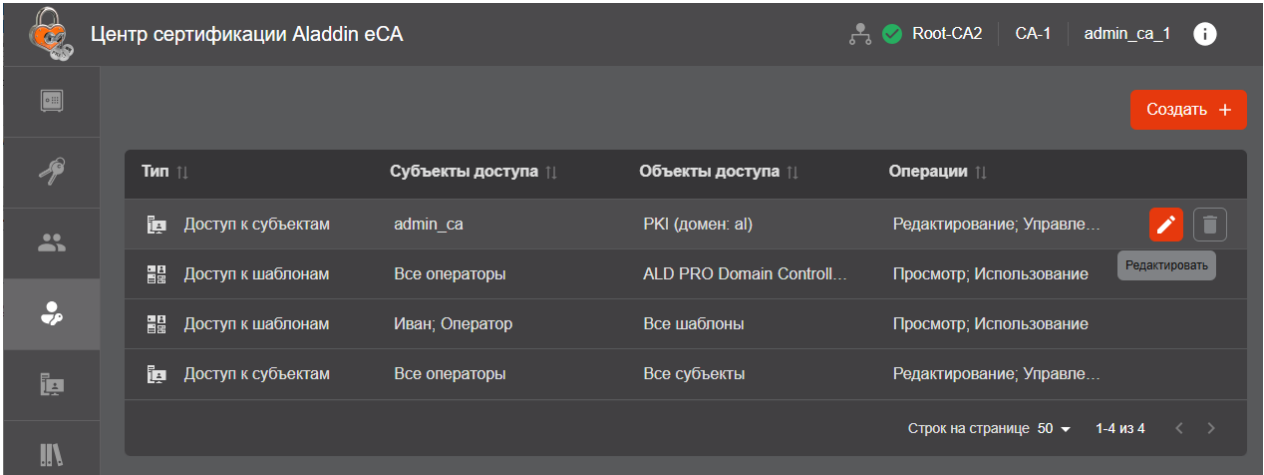


Рисунок 127 – Кнопка редактирования правила доступа

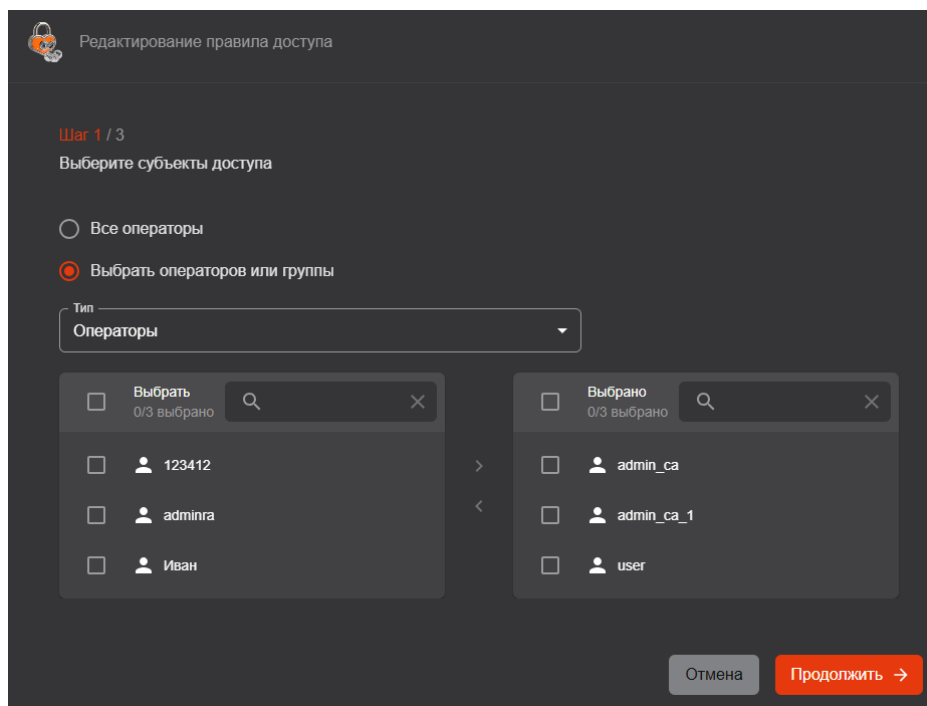


Рисунок 128 – Окно «Редактирование правила доступа», шаг 1

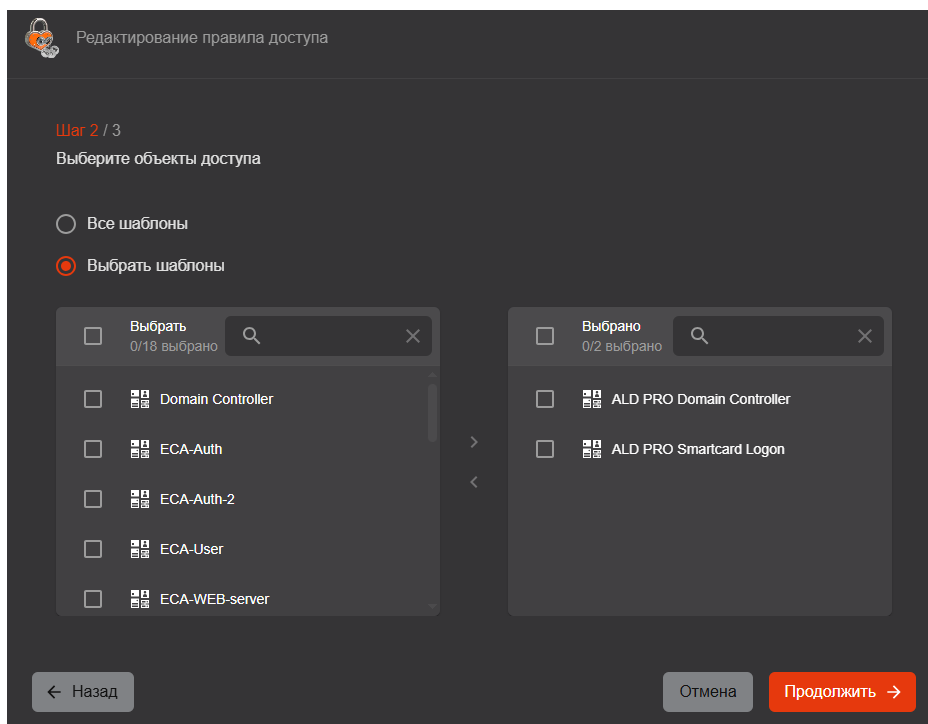


Рисунок 129 – Окно «Редактирование правила доступа», шаг 2, тип правила – «Доступ к шаблонам»

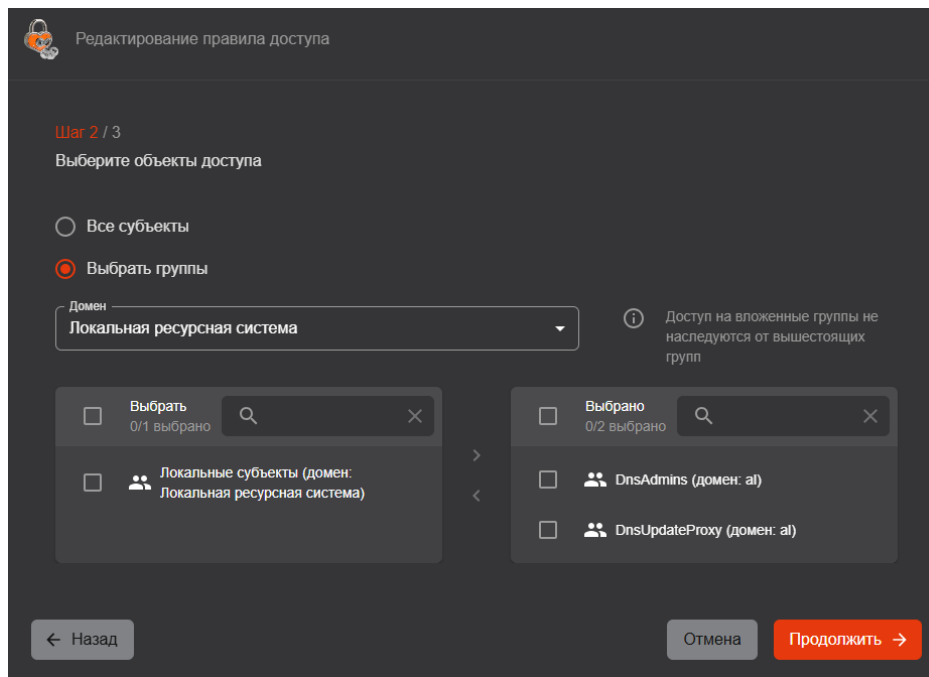


Рисунок 130 – Окно «Редактирование правила доступа», шаг 2, тип правила – «Доступ к группам»

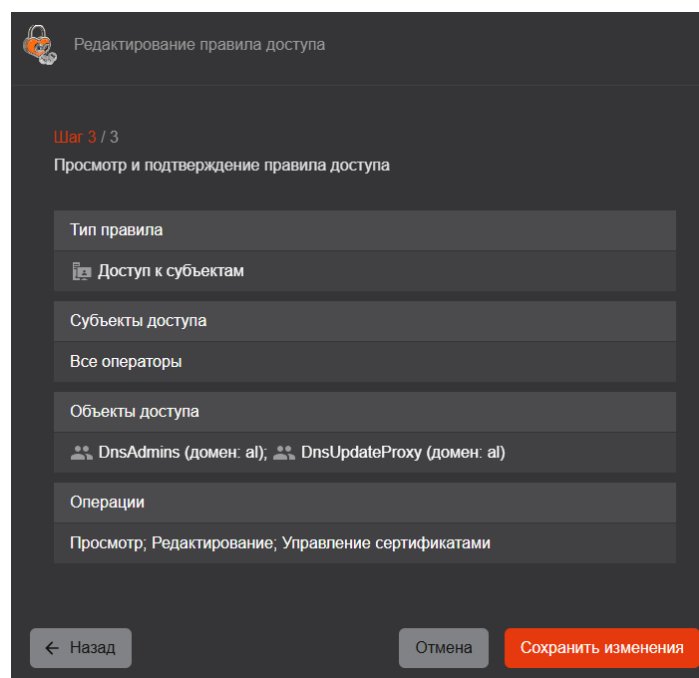



Рисунок 131 – Окно «Редактирование правила доступа», шаг 3

- Изменение типа правила доступа недоступно.
- При редактировании правила доступа исключение всех субъектов доступа или объектов доступа из правила доступа недоступно.
- После нажатия на кнопку «Сохранить изменения» правило доступа будет изменено.

7.7.3 Удаление правила доступа

- После добавления правила доступа, при наведении курсора на строку добавленного правила доступа появляется возможность его удаления – при нажатии на кнопку <Удалить>  (см. Рисунок 132) на экран будет выведено окно подтверждения выбранного действия (см. Рисунок 133).

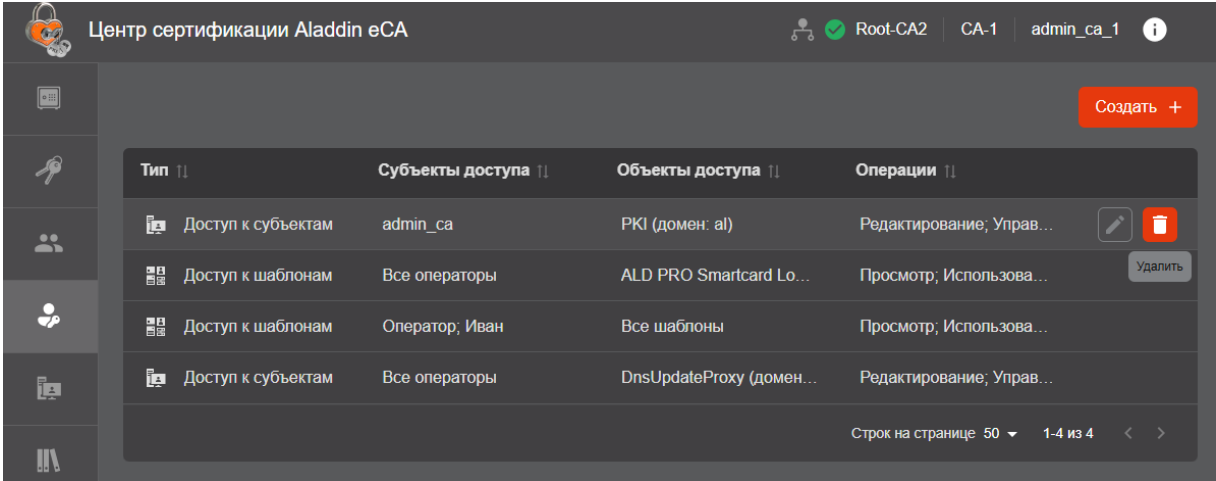


Рисунок 132 – Кнопка удаления правила доступа

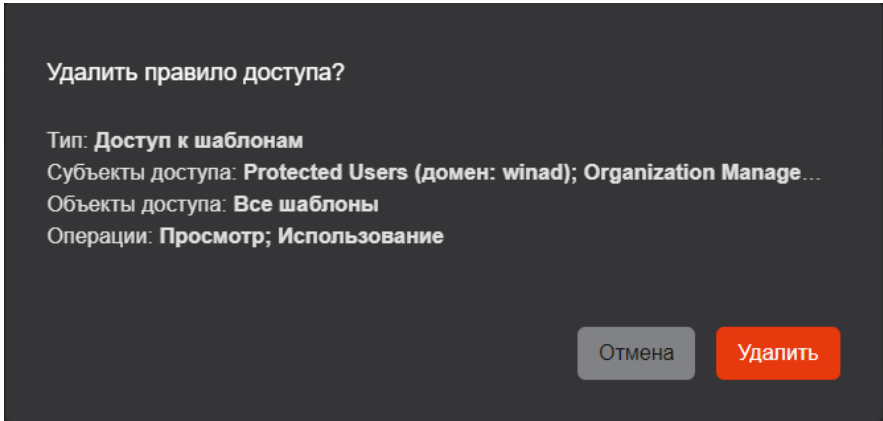


Рисунок 133 – Окно удаления правила доступа

- В результате удаления правила доступа субъекты доступа, указанные в правиле доступа, потеряют доступ на просмотр и использование шаблонов, указанных в объектах доступа данного правила.

7.8 Раздел «Субъекты»

Раздел «Субъекты» обеспечивает возможность просмотра субъектов подключенных и удалённых ресурсных систем, выпуска сертификатов для субъектов и создание учётных записей для субъектов типа «Пользователь».

Пользователю с ролью «Администратор» доступен просмотр и управление всеми субъектами всех ресурсных систем без ограничений, создание нового локального субъекта.

Пользователю с ролью «Оператор» доступен просмотр карточки субъекта, выпуск сертификата и создание учётных записей для субъектов, права на которые предоставлены учётной записи. Пользователю с ролью «Оператор» невозможно назначить доступ к локальной базе субъектов.

Переход в раздел «Субъекты» осуществляется через боковое меню, расположенное слева на главном экране (см. Рисунок 134).



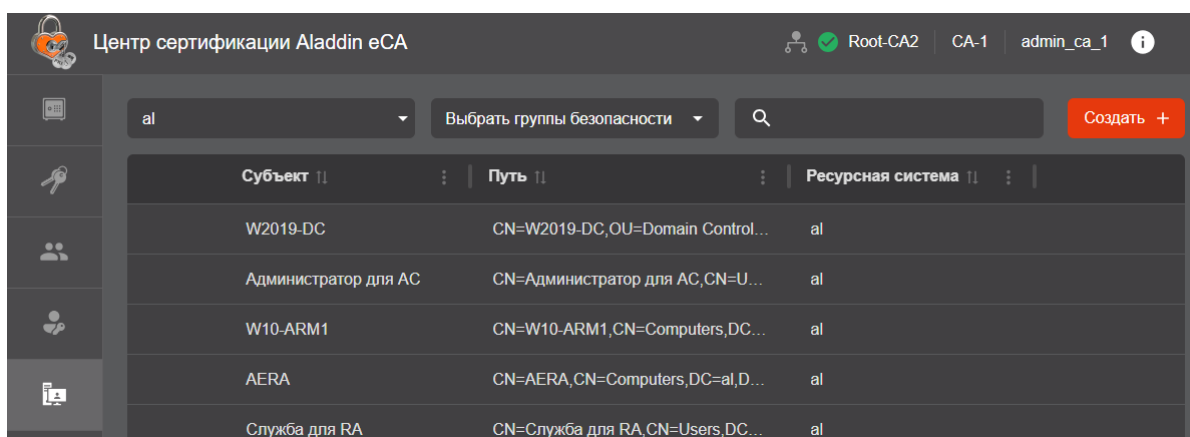


Рисунок 134 – Экран раздела «Субъекты»

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 действующие 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**.

### 7.8.1 Просмотр субъектов ресурсных систем

- Просмотр субъектов осуществляется посредством выбора источника:
  - все внешние ресурсы – подключенные службы каталогов;
  - локальный ресурс – появляется в случае, если в локальной базе данных Центра сертификации присутствует хотя бы один субъект;
  - внешний ресурс, отображаемое имя которого соответствует имени контроллера домена.
- В разделе «Субъекты» в верхней панели расположены элементы выбора ресурса и фильтрации (см. Рисунок 135):
  - 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 группы 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;

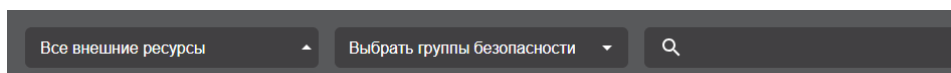


Рисунок 135 – Верхняя панель экранной формы вкладки «Субъекты»

### 7.8.2 Поиск субъектов

- В разделе «Субъекты» в верхней панели расположен элемент поиска (см. Рисунок 135). Поле поиска предназначено для поиска 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.

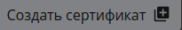
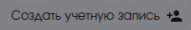
### 7.8.3 Сортировка субъектов

- Средства сортировки субъектов выбранной ресурсной системы представлены элементами выбора направления сортировки в заголовке таблицы экранной формы (см. Рисунок 136):
  - «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 136 – Поля сортировки содержимого экрана раздела «Субъекты»

#### 7.8.4 Карточка субъекта

- Просмотр данных субъекта возможен посредством страницы «Карточка субъекта».
- Переход к экрану «Карточка субъекта» (см. Рисунок 138) осуществляется при нажатии на строку субъекта главного экрана раздела «Субъекты» (см. Рисунок 134).
- 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 (идентификатор безопасности)<sup>29</sup>;
  - атрибуты SAN и SDN (см. Таблица 18);
  - 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:
  - создать сертификат для выбранного субъекта с закрытым ключом, на основании запроса или на ключевом носителе по нажатию на кнопку <Создать сертификат>  (см. раздел 7.8.7, настоящего руководства);
  - создание учётной записи для текущего субъекта по нажатию на кнопку . Только для субъекта типа «Пользователь»;
  - выбрать набор атрибутов SDN и SAN, отображаемых в карточке субъекта, в выпадающем меню (см. Рисунок 137);

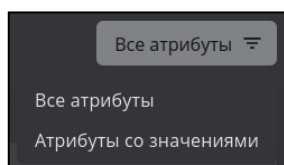




Рисунок 137 – Фильтрация отображаемых атрибутов в карточке субъекта

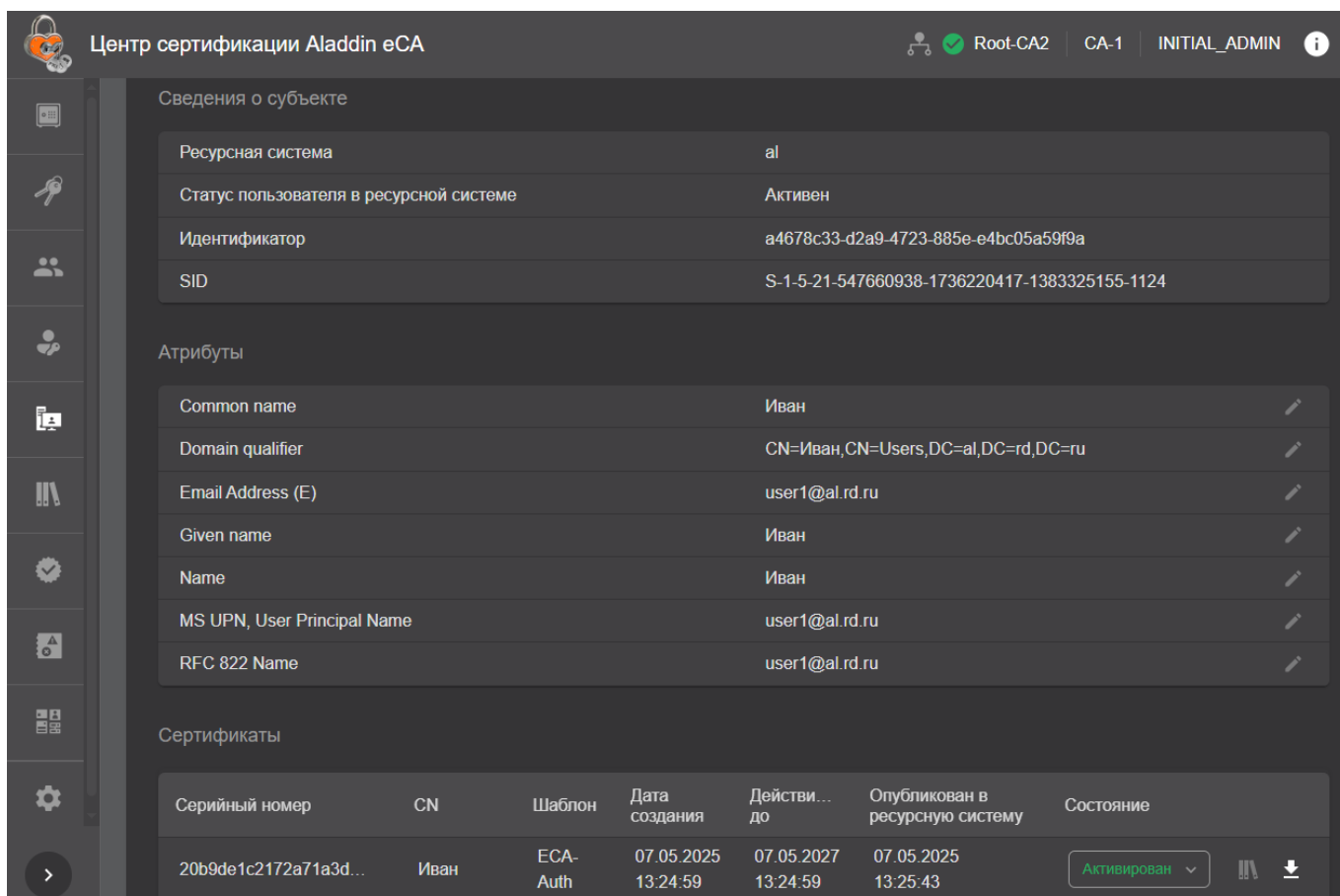
- опубликовать сертификат в ресурсную систему (только для подключенных субъектов). По нажатию на кнопку  происходит запись сертификата в формате LDIF в атрибут `userCertification` выбранного субъекта ресурсной системы, для которого выпущен сертификат. Если атрибут `userCertification` заполнен, то происходит перезапись содержимого;

<sup>29</sup> 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.

- 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 соответствии с Таблица 15 в поле сертификата «Состояние».

**При активации сертификата учитываются 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).










Центр сертификации Aladdin eCA

Root-CA2 CA-1 INITIAL\_ADMIN

Сведения о субъекте

Ресурсная система	al
Статус пользователя в ресурсной системе	Активен
Идентификатор	a4678c33-d2a9-4723-885e-e4bc05a59f9a
SID	S-1-5-21-547660938-1736220417-1383325155-1124

Атрибуты

Common name	Иван	
Domain qualifier	CN=Иван,CN=Users,DC=al,DC=rd,DC=ru	
Email Address (E)	user1@al.rd.ru	
Given name	Иван	
Name	Иван	
MS UPN, User Principal Name	user1@al.rd.ru	
RFC 822 Name	user1@al.rd.ru	

Сертификаты




Серийный номер	CN	Шаблон	Дата создания	Действи... до	Опубликован в ресурсную систему	Состояние
20b9de1c2172a71a3d...	Иван	ECA-Auth	07.05.2025 13:24:59	07.05.2027 13:24:59	07.05.2025 13:25:43	Активирован   

Рисунок 138 – Окно просмотра карточки подключенного субъекта (включено отображение «Атрибуты со значениями»)


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

Таблица 18 – Атрибуты субъекта

Атрибут	Возможные значения	Представление в API	Представление в клиентском компоненте
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 в РС	Для подключенных к РС субъектов: субъект заблокирован в РС (true) или субъект не заблокирован в РС (false)	"isBlocked"	Поле «Статус в ресурсной системе» в карточке субъекта. Для локальных субъектов всегда отображается символ «-».
	Для локальных субъектов: всегда false		
Идентификатор	string(\$uuid)	"id"	Поле «Идентификатор» 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 <sup>30</sup>	Строка	"sid"	Поле «SID» карточки субъекта
<b>Атрибуты SDN</b>			
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 (Mail)	Список строк	"EMAILADDRESS"	Поле «Email Address (EI)» в карточке субъекта

<sup>30</sup> 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
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
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 «Postal code» 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

Атрибут	Возможные значения	Представление в API	Представление в клиентском компоненте
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
<b>Атрибуты SAN</b>			
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
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

#### 7.8.4.1 Редактирование атрибутов субъекта



- Для субъектов локальной ресурсной системы доступно редактирование всех атрибутов SDN и SAN.

- Таблица 19 – Допустимые значения атрибутов

АО «Аладдин Р.Д.», 1995–2025 г.      Руководство администратора. Часть 2. Функции управления Центра сертификации Aladdin Enterprise Certification Authority  
Стр. 124 / 271



Атрибут	Правило валидации
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 139).
  - 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 <Заккрыть>.
- При синхронизации отредактированное поле атрибута будет заменено значением соответствующего атрибута субъекта синхронизированной ресурсной системы, если оно заполнено для этого доменного субъекта в ресурсной системе!

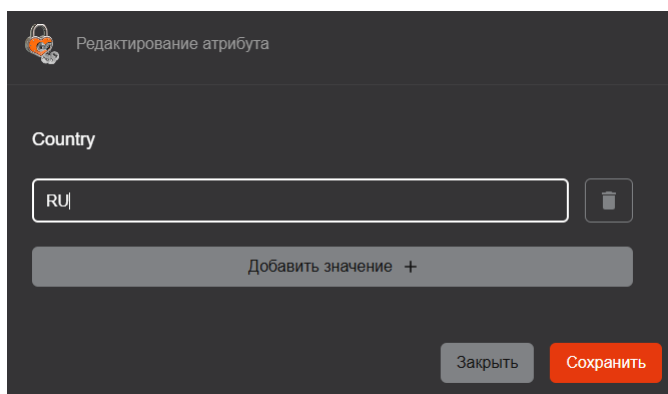


Рисунок 139 – Окно редактирования значения атрибута в карточке субъекта

### 7.8.5 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»;
  - субъект веб-сервера, автоматически созданный при развёртывании Центра сертификации, с параметрами, указанными в конфигурационном файле `/opt/aecaCa/scripts/config.sh`:
    - параметр `hostname` задаёт значение атрибутов «Common name» и «DNS Name» локального субъекта;

- параметры `initial_server_key_algorithm` и `initial_server_key_bits` задают значения криптографических параметров сертификата веб-сервера;
  - параметр `initial_server_password` задаёт значение пароля контейнера сертификата веб-сервера.
- 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 (см. Таблица 20), остальные текущие атрибуты (то есть те, которые не были получены из ресурсной системы) не изменятся.
- Проверка субъектов осуществляется по атрибуту «id».

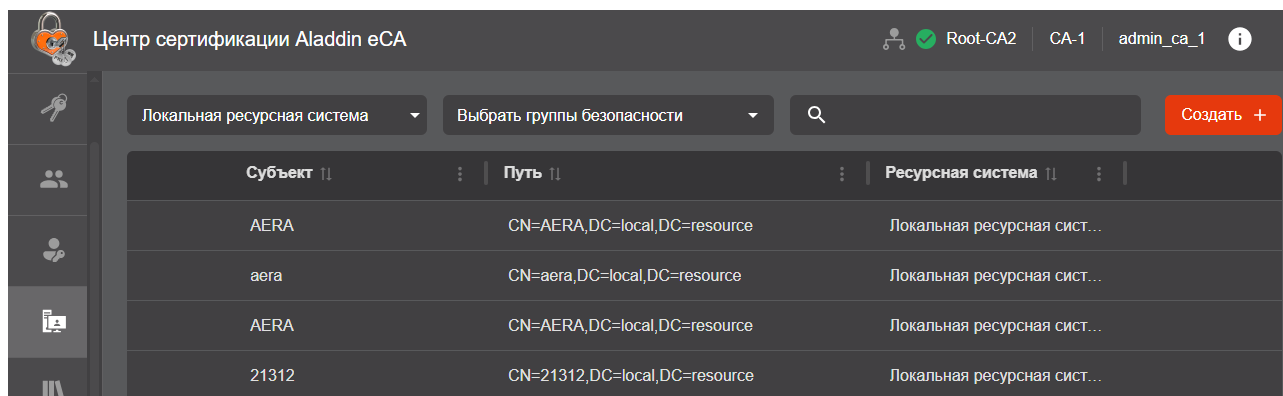


Рисунок 140 – Экран раздела меню «Субъекты». Локальный ресурс

#### 7.8.5.1 Создание нового субъекта локальной ресурсной системы

- Доступно только пользователю с ролью «Администратор».
- Для создания нового локального субъекта нажмите кнопку «Создать» (см. Рисунок 140), в открывшемся окне (см. Рисунок 141) введите имя создаваемого субъекта (CN), добавьте необходимые атрибуты и задайте им значения.

Для добавления атрибута нажмите кнопку «Добавить атрибут +» и выберите атрибут в списке возможных атрибутов SDN и SAN (см. Рисунок 142). При необходимости воспользуйтесь поиском и прокруткой списка.

Полный список доступных атрибутов приведён в Таблица 18.

Далее укажите значения выбранным атрибутам или удалите атрибуты, нажав кнопку «Удалить» (см. Рисунок 143). При отсутствии значения в поле «Common name» или несоответствии введенного значения допустимому формату создание субъекта запрещено.

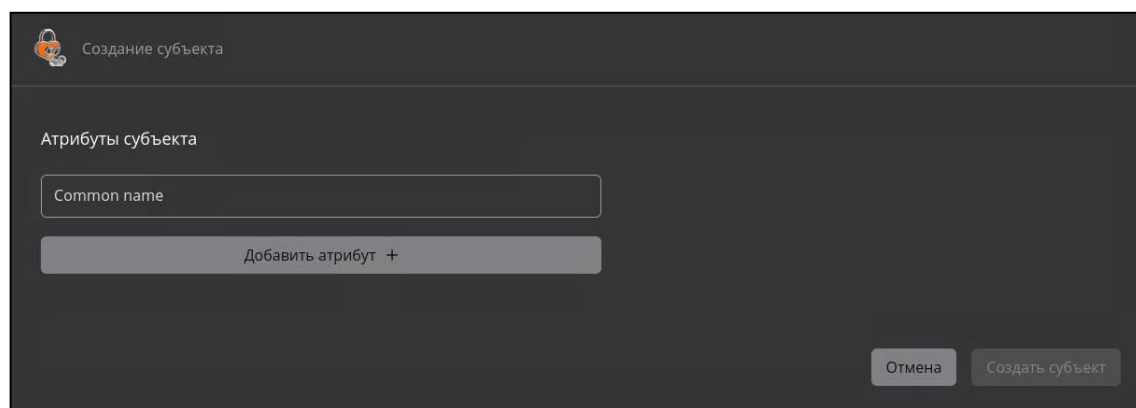


Рисунок 141 – Создание субъекта

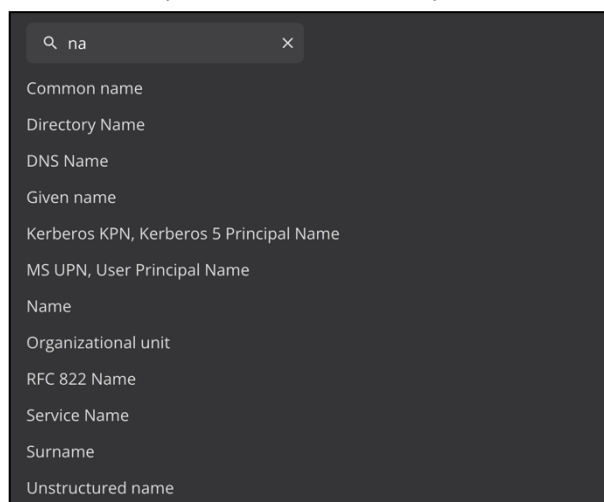


Рисунок 142 – Добавление атрибута субъекта

- После корректного заполнения всех выбранных полей атрибутов будет доступно создание субъекта по нажатию на кнопку <Создать субъект> (см. Рисунок 143).

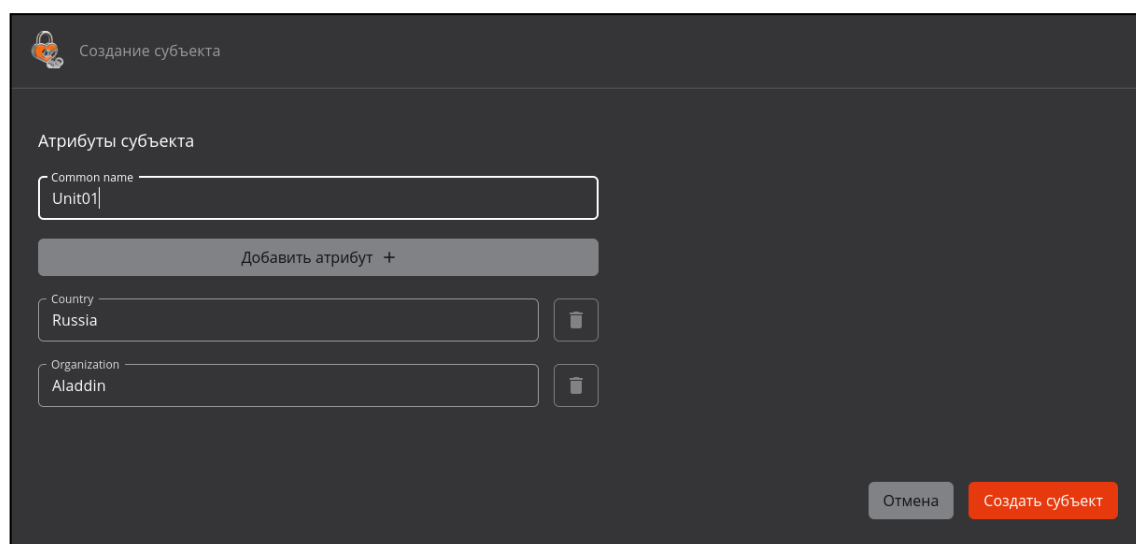


Рисунок 143 – Создание субъекта. Заполнение полей

- При создании локального субъекта Центр сертификации автоматически назначает новому субъекту идентификатор (UUID).
- В результате создания субъекта администратор будет уведомлён всплывающим сообщением об успешном создании субъекта.

#### 7.8.6 Субъекты внешнего ресурса

- Внешний (подключенный) ресурс формируется в результате регистрации службы каталогов доменных служб Samba DC, РЕД АДМ, ALD PRO, FreeIPA, Альт Домен или MS Active Directory.
- Подключенный ресурс будет отображен только после регистрации ресурсной системы на вкладке «Ресурсная система» (см. пункт 7.9.1 настоящего руководства).
- Обновление списков и данных субъектов ресурсной системы происходит по правилам, приведённым в пункте 7.9.3 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 144).

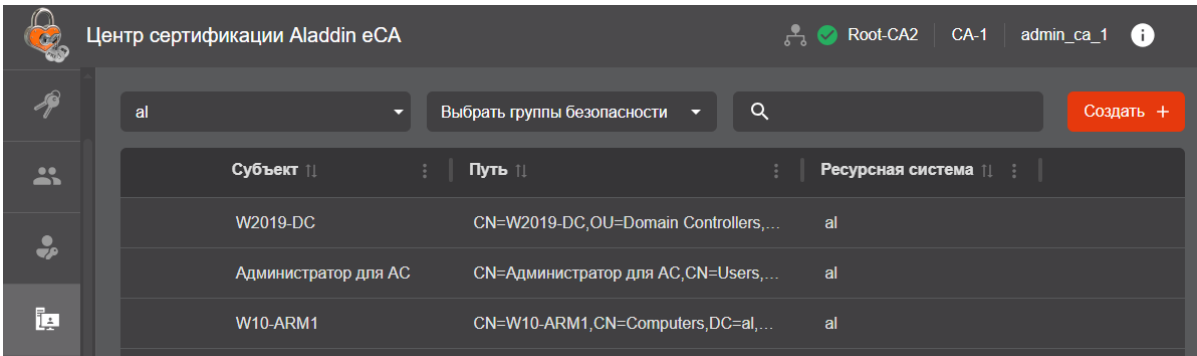


Рисунок 144 – Экран раздела меню «Субъекты». Подключенный ресурс

- 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 20.


Таблица 20 – 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	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	
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

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
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 `Id`.

### 7.8.7 Создание сертификата для субъекта ресурсной системы

- Выберите субъект, для которого необходимо создать сертификат, нажмите появившуюся кнопку  <Создать сертификат> и выберите способ создания из выпадающего списка (см. Рисунок 145):
  - с закрытым ключом (см. Приложение 1. Создание сертификата для субъекта);
  - на основании запроса (см. Приложение 1. Создание сертификата для субъекта);
  - на ключевом носителе (см. Приложение 1. Создание сертификата для субъекта).

При выпуске сертификата значения полей шаблона заполняются автоматически соответственно атрибутам, указанным для субъекта в ресурсной системе. Если атрибут отсутствует в карточке доменного субъекта, то необходимо отредактировать его значение в карточке субъекта Центра сертификации.

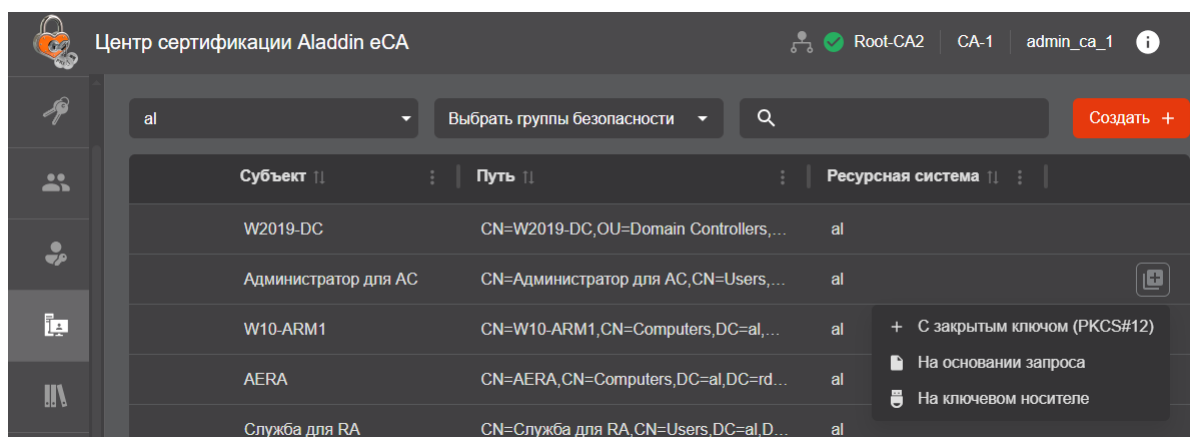


Рисунок 145 - Окно выпуска сертификата для субъекта ресурсной системы

- При выпуске сертификатов для субъектов внешних (подключенных) ресурсных систем возможно публиковать сертификат в формате LDIF в атрибут `userCertification` субъекта ресурсной системы (путём добавления, а не перезаписи атрибута), проставив флаг в чек-боксе «Публиковать сертификат в ресурсную систему» окна выпуска сертификата. По умолчанию флаг выполнения публикации сертификата включен.
- После выбора шаблона субъекта ресурсной системы на следующем шаге поля автоматически заполняются данными субъекта в соответствии с Таблица 20.
- Если значения атрибутов отсутствуют, то необходимо их ввести в соответствующие поля в карточке субъекта.

- Более подробно процедура выпуска сертификата приведена в «Приложение 1. Создание сертификата для субъекта».

### 7.8.8 Создание учётной записи для субъекта

- Выберите субъект локальной или подключенной ресурсной системы, для которого необходимо создать учетную запись и нажмите кнопку в строке выбранного пользователя <Создать учетную запись> (см. Рисунок 146).

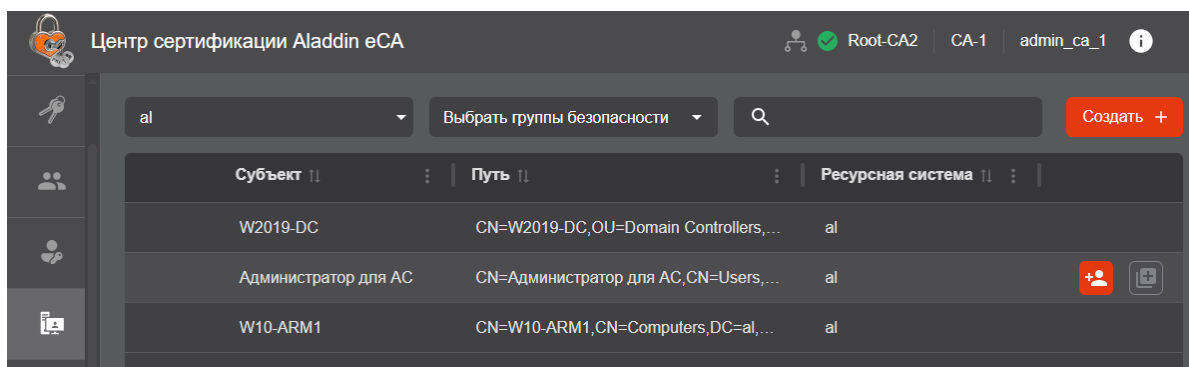


Рисунок 146 – Выбор субъекта для создания учётной записи

- В открывшемся окне создания новой учетной записи (см. Рисунок 147) поле «Отображаемое имя» автоматически заполнено данными атрибута «Common Name» субъекта, но доступно для редактирования, и соответствует полю «ФИО» в разделе «Учётные записи». Поле «Логин» не отображается в окне создания новой учётной записи и заполняется по умолчанию в соответствии со значением атрибута «Common Name» выбранного субъекта.
- Выберите роль, применяемую к создаваемой учетной записи.
- Нажмите кнопку <Создать> для создания учетной записи для субъекта.

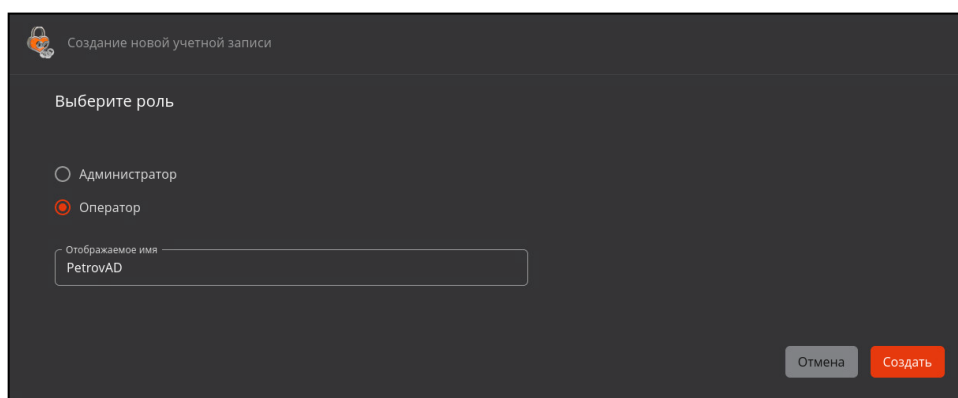


Рисунок 147 – Окно создания новой учётной записи

- Для созданной учетной записи с ролью «Оператор» произведите настройку прав доступа к группам и объектам ресурсной системы в соответствии с пунктом 7.6.5 настоящего руководства<sup>31</sup>.

**ВНИМАНИЕ! Логины (имена) учетных записей должны быть уникальными.**

<sup>31</sup> Учетные записи, созданные на основе субъектов, наследуют полномочия в соответствии с правилами доступа на просмотр и использование шаблонов и полномочия на доступ к субъектам ресурсных систем от групп безопасности, в которые входит субъект, связанный с данной учетной записью.

## 7.9 Раздел «Ресурсные системы»

Раздел «Ресурсные системы» обеспечивает получение данных субъектов с целью упрощенного выпуска сертификатов субъектам поддерживаемых служб каталогов Linux и Microsoft (далее – ресурсные системы), а также централизованную публикацию выпущенных сертификатов в карточку субъекта службы каталогов.


Каждая ресурсная система, зарегистрированная в Центре сертификации Aladdin eCA, может иметь несколько точек подключения.

Переход в раздел «Ресурсные системы» осуществляется через боковое меню, расположенное слева на главном экране (см. Рисунок 148).

- На основном экране раздела «Ресурсные системы» отображены следующие информационные поля (см. Рисунок 148):
  - имя домена – домен подключенной ресурсной системы;
  - последнее обновление – дата и время последней синхронизации с базой субъектов ресурсной системы;
  - статус – статус ресурсной системы, который назначается в соответствии с критериями, приведенными в таблице ниже (Таблица 21);

Таблица 21 – 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 – количество субъектов, загруженных из ресурсной системы;
-  - пиктограмма «Очередь» показывает, что ресурсной системе назначена задача, которая поставлена в очередь, так как в данный момент выполняется другая задача.

Ресурсным системам возможно назначить выполнение следующих задач:

- полная синхронизация ресурсной системы (см. раздел 7.9.3.3);
- частичная синхронизация ресурсной системы (синхронизация точки подключения ресурсной системы) (см. раздел 7.9.3.4);
- удаление зарегистрированной ресурсной системы (см. раздел 7.9.5);
- удаление точки подключения зарегистрированной ресурсной системы (см. раздел 7.9.6).

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».

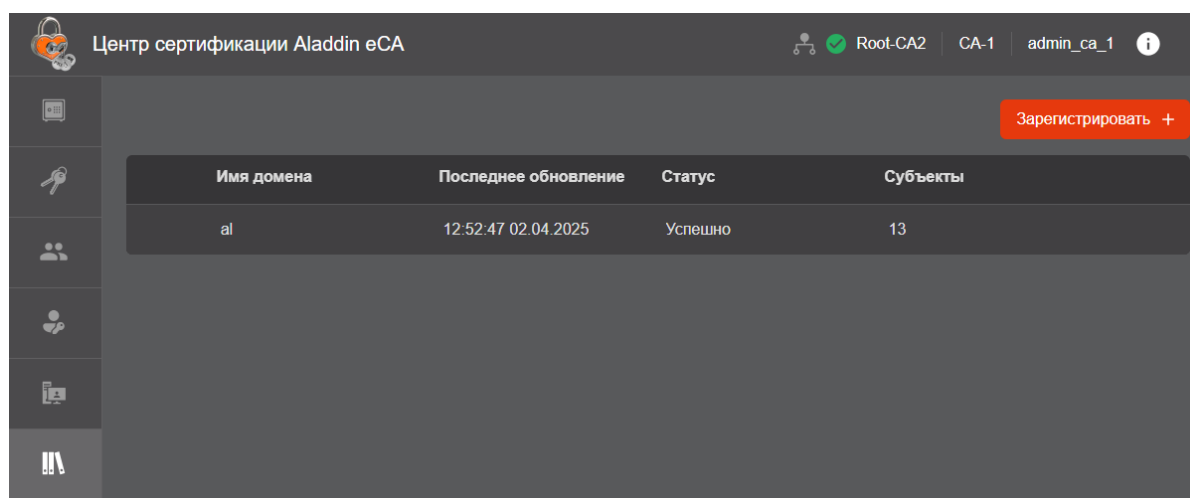


Рисунок 148 – Экран раздела «Ресурсные системы»

- Центр сертификации Aladdin eCA позволяет взаимодействовать с несколькими ресурсными системами: Samba DC, РЕД АДМ, MS AD, FreeIPA, ALD PRO и Альт Домен:
  - список субъектов (пользователей, компьютеров и сервисов (только для ALD PRO и FreeIPA)), их атрибуты и сертификаты;
  - список и состав групп безопасности.
- Идентификация загружаемых субъектов ресурсной системы производится по их атрибуту «id».
- В разделе «Ресурсные системы» доступны следующие возможности:
  - регистрация (подключение) ресурсной системы для выпуска сертификатов и учётных записей субъектам служб каталогов (см. раздел 7.9.1);
  - переход в карточку ресурсной системы (см. раздел 7.9.2);
  - запуск полной синхронизации ресурсной системы (см. раздел 7.9.3.3);
  - удаление зарегистрированной ресурсной системы (см. раздел 7.9.5).

### 7.9.1 Регистрация точки подключения

- Для подключения ресурсной системы ALD PRO или FreeIPA к Центру сертификации Aladdin eCA необходимо предварительно создать роль на контроллере домена ALD Pro/FreeIPA. Для этого на контроллере домена ALD Pro или FreeIPA выполните следующие команды с правами суперпользователя:

```
ipa permission-add "eCA - Reader" --right={read,search} --bindtype=permission --
attrs=*

ipa permission-add "eCA - Manage certificate" --right=write --bindtype=permission --
attrs=usercertificate

ipa privilege-add "eCA - Integrations privilege" --desc="Привилегии для интеграции с
eCA"

ipa privilege-add-permission "eCA - Integrations privilege" --permissions="eCA -
Reader" --permissions="eCA - Manage certificate"

ipa role-add "eCA - Integrations" --desc="Роль для интеграции с eCA"

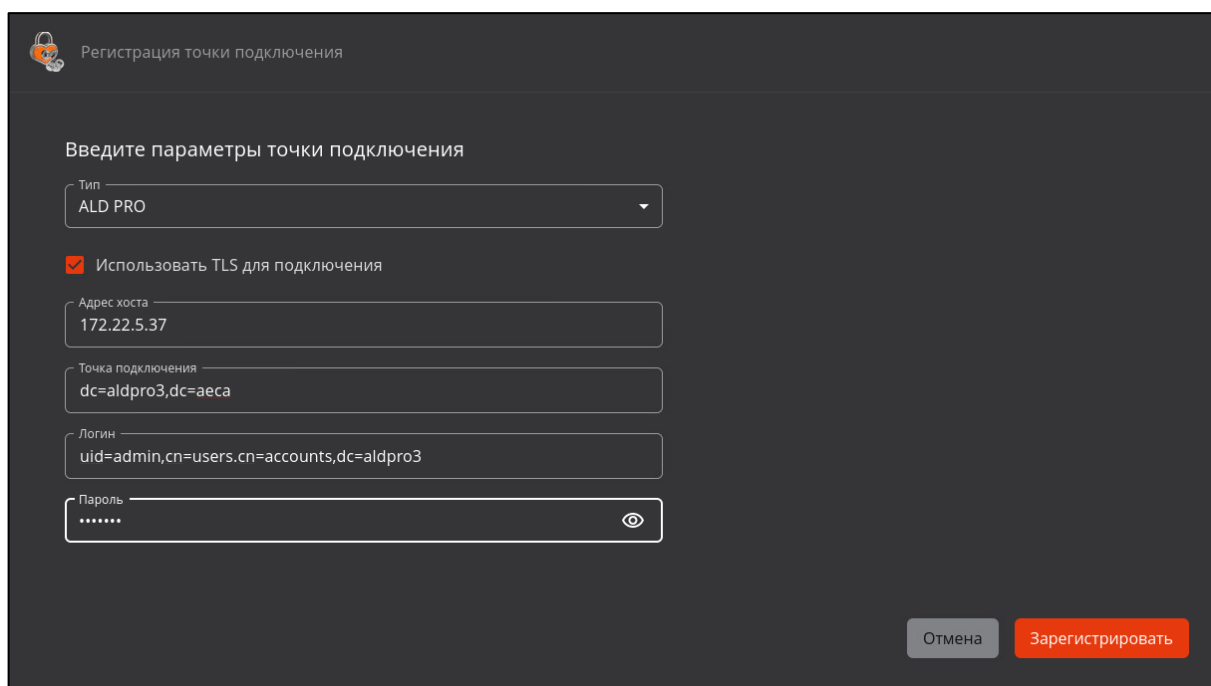
ipa role-add-privilege "eCA - Integrations" --privileges="eCA - Integrations
privilege"
```



```
ipa role-add-member "eCA - Integrations" --users=<Имя пользователя>
```

Для успешной публикации сертификатов в ресурсную систему ALD Pro или FreeIPA требуется подключение к ресурсной системе от имени пользователя с минимальным набором полномочий:

- наличие роли «Service Role» для подключения к ресурсной системе;
- наличие роли «helpdesk» или роли «User Administrator» для публикации сертификатов пользователей;
- наличие роли «Enrollment Administrator» для публикации сертификатов контроллеров домена.
- Для подключения к ресурсной системе Samba DC, Альт Домен, РЕД АДМ или MS AD необходимо создать учетную запись на контроллере домена с правами, позволяющими получить данные (наличие ролей «Domain Users» и «Cert Publishers» для публикации сертификатов пользователей).
- Запуск сценария регистрации точки подключения происходит по нажатию кнопки <Зарегистрировать +> на главном экране управления «Ресурсной системы» или по нажатию кнопки <Добавить +> в карточке ресурсной системы в подразделе «Точки подключения».
- В открывшемся окне заполните следующие поля:
  - тип – выберите в списке тип подключаемой ресурсной системы: Samba DC, Альт Домен, ALD PRO, MS AD, FreeIPA, РЕД АДМ;
  - чек-бокс «Использовать TLS для подключения» – выберите тип соединения. По умолчанию чек-бокс для соединения по протоколу TLS всегда включен. В случае использования незащищенного соединения снимите отметку чек-бокса;
  - адрес хоста – укажите полное доменное имя или IP-адрес точки подключения ресурсной системы;
  - точка подключения – укажите точку подключения в формате:  
`DC={первое доменное имя},DC={второе доменное имя}` и т.д.;
  - логин – укажите имя учетной записи администратора контроллера домена:
    - для Samba DC, Альт Домен, РЕД АДМ и MS AD имя учетной записи администратора указывается в формате RFC822Name;
    - для ALD PRO и FreeIPA имя учетной записи администратора указывается в формате Distinguished Names.
  - пароль – укажите пароль учетной записи администратора контроллера домена.  
Пароль хранится в базе данных в зашифрованном по алгоритму AES256 виде (конфигурация базы данных указана в конфигурационном файле `/opt/aecaCa/scripts/config.sh`).
- Примеры заполненных полей при подключении ресурсной системы для разных типов источников приведены на соответствующих рисунках (см. Рисунок 149, Рисунок 150, Рисунок 151, Рисунок 152, Рисунок 153, Рисунок 154).
- После заполнения всех полей нажмите кнопку <Зарегистрировать>. В результате успешной регистрации ресурсной системы будет выведено соответствующее уведомительное сообщение.



Регистрация точки подключения

Введите параметры точки подключения

Тип  
ALD PRO

☒ Использовать TLS для подключения

Адрес хоста  
172.22.5.37

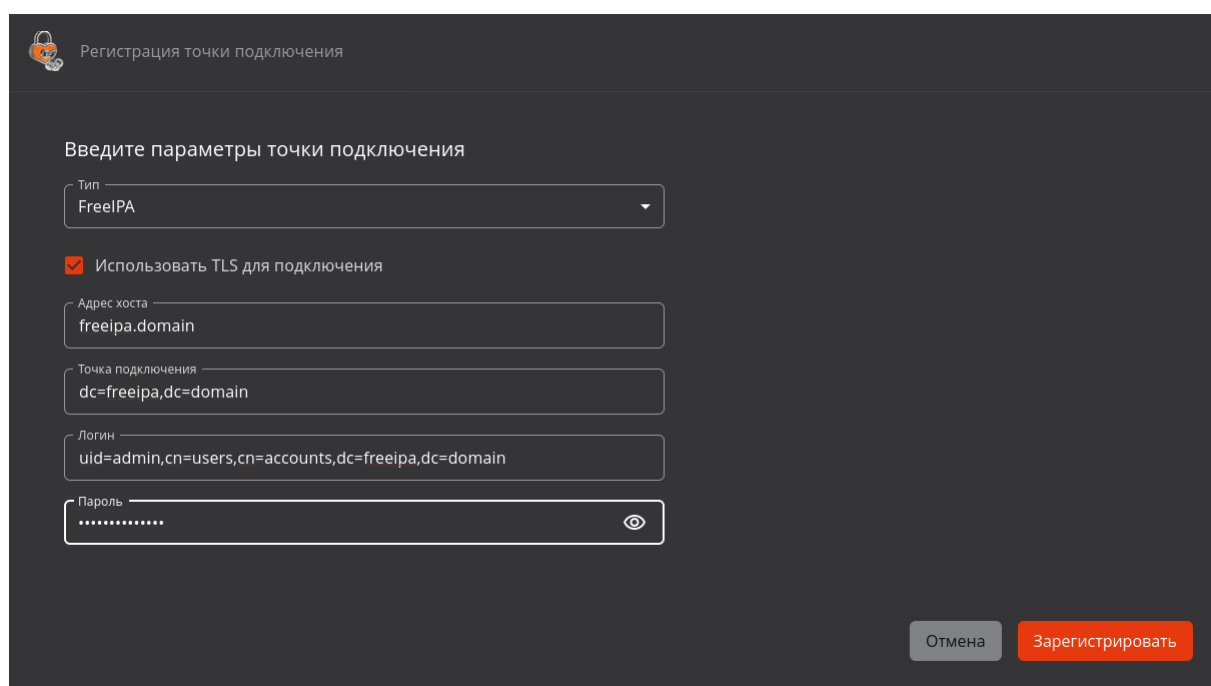
Точка подключения  
dc=aldpro3,dc=aeca

Логин  
uid=admin,cn=users,cn=accounts,dc=aldpro3

Пароль  
.....

Отмена Зарегистрировать

Рисунок 149 – Пример регистрации ресурсной системы ALD PRO



Регистрация точки подключения

Введите параметры точки подключения

Тип  
FreeIPA

☒ Использовать TLS для подключения

Адрес хоста  
freeipa.domain

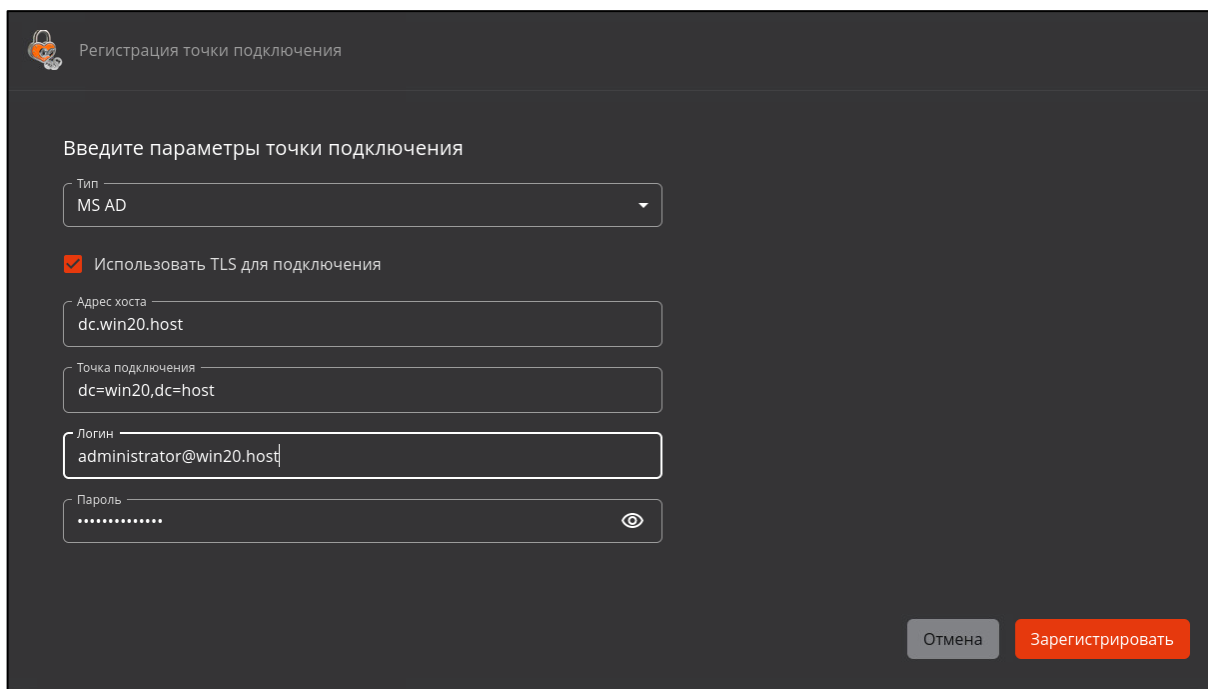
Точка подключения  
dc=freeipa,dc=domain

Логин  
uid=admin,cn=users,cn=accounts,dc=freeipa,dc=domain

Пароль  
.....

Отмена Зарегистрировать

Рисунок 150 – Пример регистрации ресурсной системы FreeIPA



Регистрация точки подключения

Введите параметры точки подключения

Тип  
MS AD

☒ Использовать TLS для подключения

Адрес хоста  
dc.win20.host

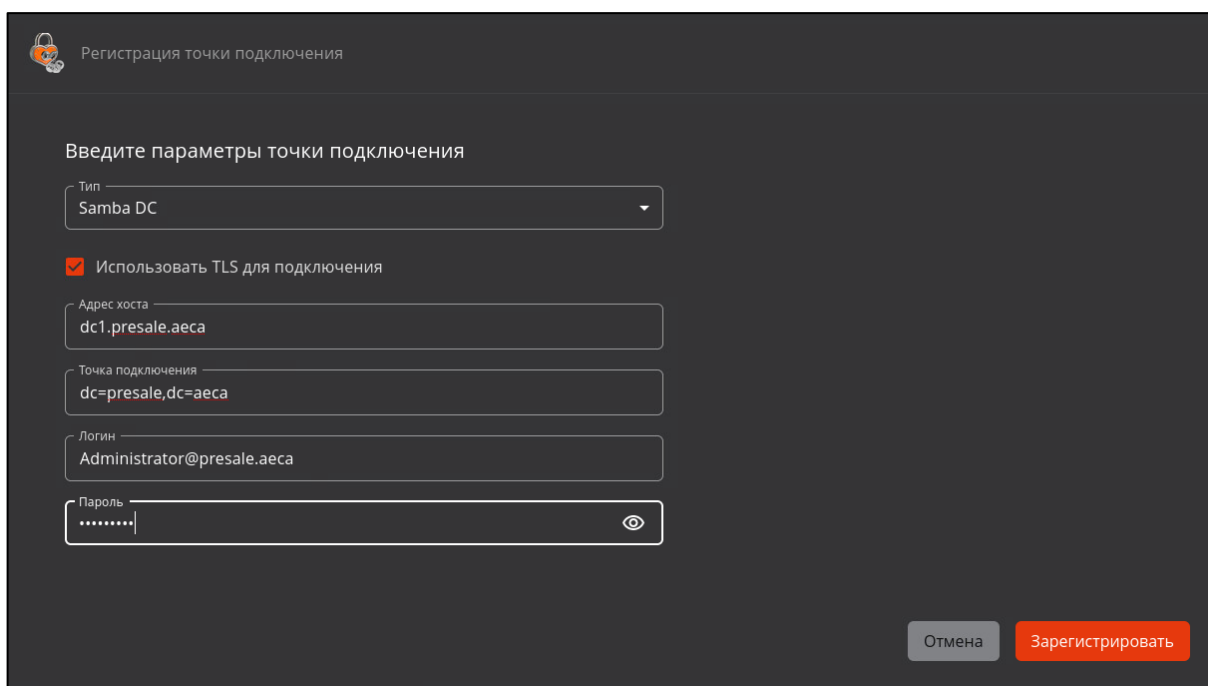
Точка подключения  
dc=win20,dc=host

Логин  
administrator@win20.host

Пароль  
.....

Отмена Зарегистрировать

Рисунок 151 – Пример регистрации ресурсной системы MS AD



Регистрация точки подключения

Введите параметры точки подключения

Тип  
Samba DC

☒ Использовать TLS для подключения

Адрес хоста  
dc1.presale.aeca

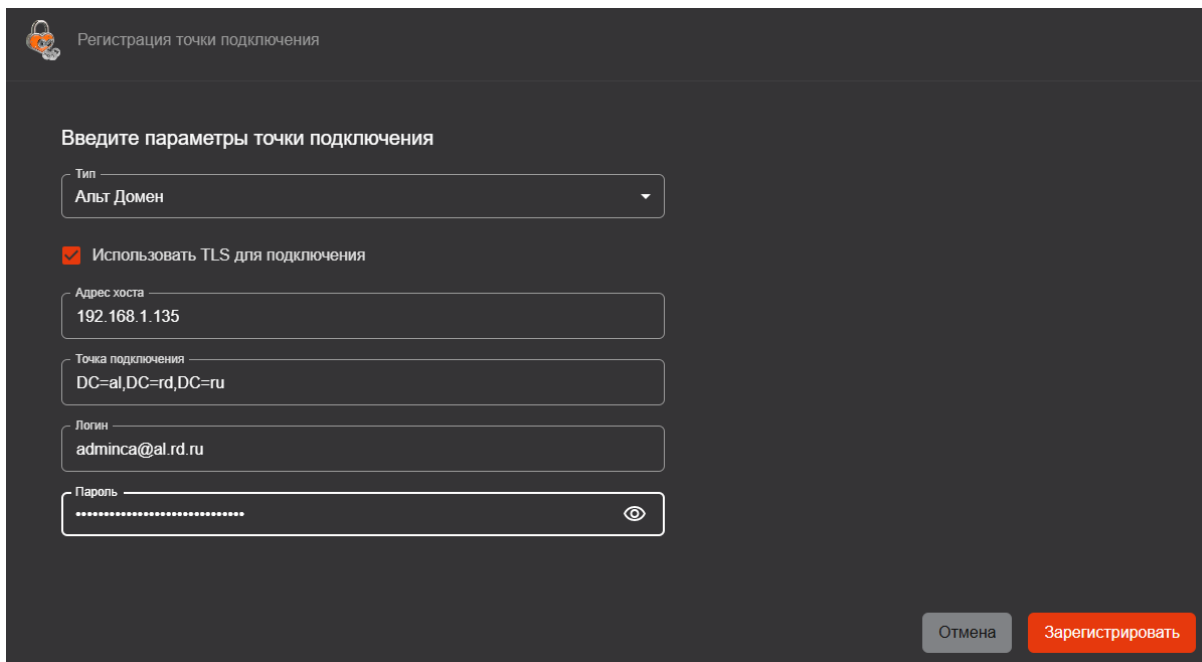
Точка подключения  
dc=presale,dc=aeca

Логин  
Administrator@presale.aeca

Пароль  
.....

Отмена Зарегистрировать

Рисунок 152 – Пример регистрации ресурсной системы Samba DC



Регистрация точки подключения

Введите параметры точки подключения

Тип  
Альт Домен

☒ Использовать TLS для подключения

Адрес хоста  
192.168.1.135

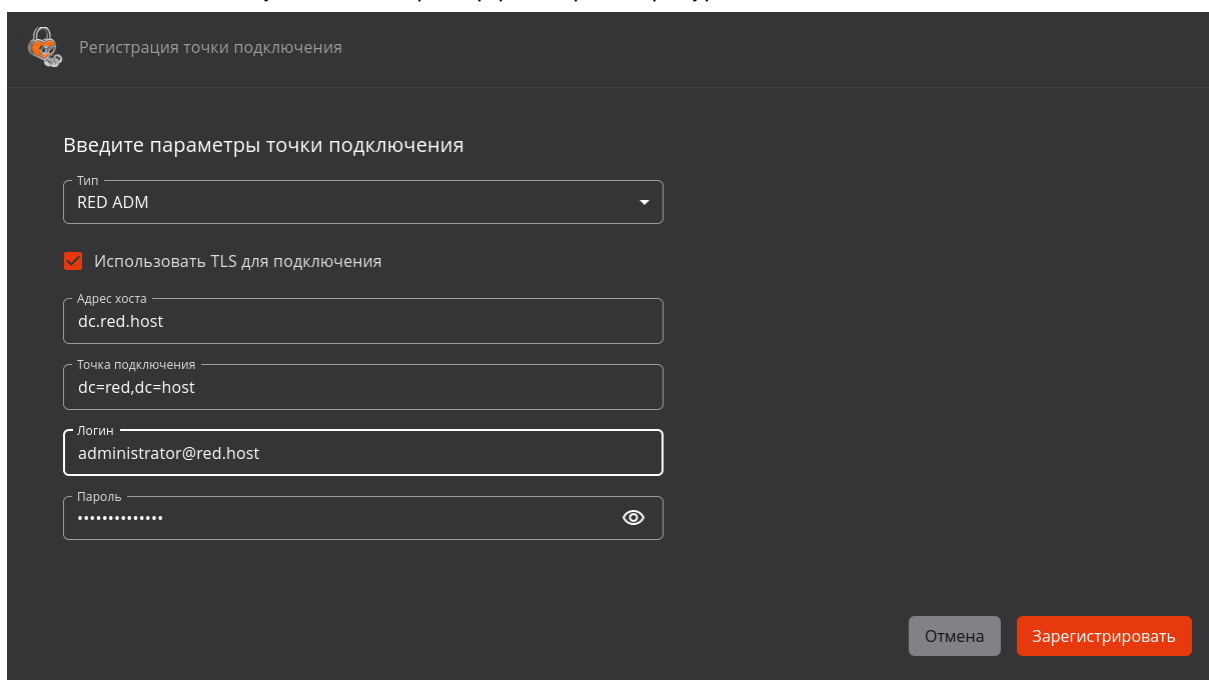
Точка подключения  
DC=al,DC=rd,DC=ru

Логин  
adminca@al.rd.ru

Пароль  
.....

Отмена Зарегистрировать

Рисунок 153 – Пример регистрации ресурсной системы Альт Домен



Регистрация точки подключения

Введите параметры точки подключения

Тип  
RED ADM

☒ Использовать TLS для подключения

Адрес хоста  
dc.red.host

Точка подключения  
dc=red,dc=host

Логин  
administrator@red.host

Пароль  
.....

Отмена Зарегистрировать

Рисунок 154 – Пример регистрации ресурсной системы РЕД АДМ

- При регистрации ресурсной системы могут возникать следующие ошибки:
  - сообщение «Ошибка LDAP аутентификации: Неправильный логин или пароль» – при вводе неверных данных учётной записи администратора домена;
  - сообщение об ошибке подключения по заданному URL (адресу хоста);
  - сообщение об ошибке при установлении TLS-соединения;
  - сообщение об ошибке при наличии уже зарегистрированной ресурсной системы с указанными данными;
  - сообщение «Ошибка подключения к ресурсной системе» при возникновении других ошибок подключения к ресурсной системе.

- Если регистрация точки подключения выполнялась из карточки ресурсной системы и в результате успешной регистрации было определено, что точка подключения принадлежит иной ресурсной системе, после нажатия на кнопку «Зарегистрировать» отображается модальное окно с информацией о принадлежности регистрируемой точки подключения другой ресурсной системе (см. Рисунок 155).

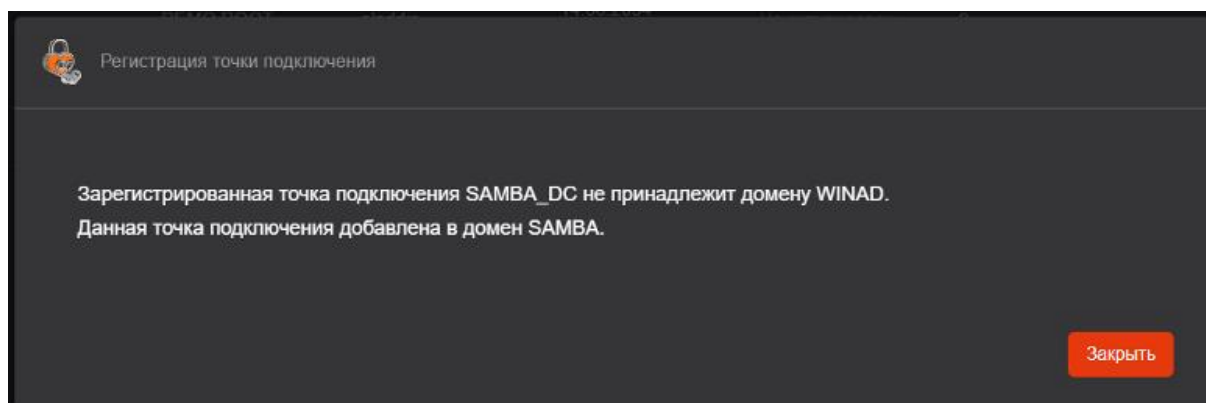


Рисунок 155 – Модальное окно с информацией о принадлежности регистрируемой точки подключения другой ресурсной системе

- При успешном подключении к ресурсной системе будет выполнена полная синхронизация данных из точки подключения, указанной при регистрации Base DN (dc=...).

### 7.9.2 Карточка ресурсной системы

Просмотр информации о ресурсной системе возможен в ее карточке. Переход к «Карточке ресурсной системы» (см. Рисунок 156) осуществляется при нажатии на строку ресурсной системы в разделе «Ресурсные системы» (см. Рисунок 148).

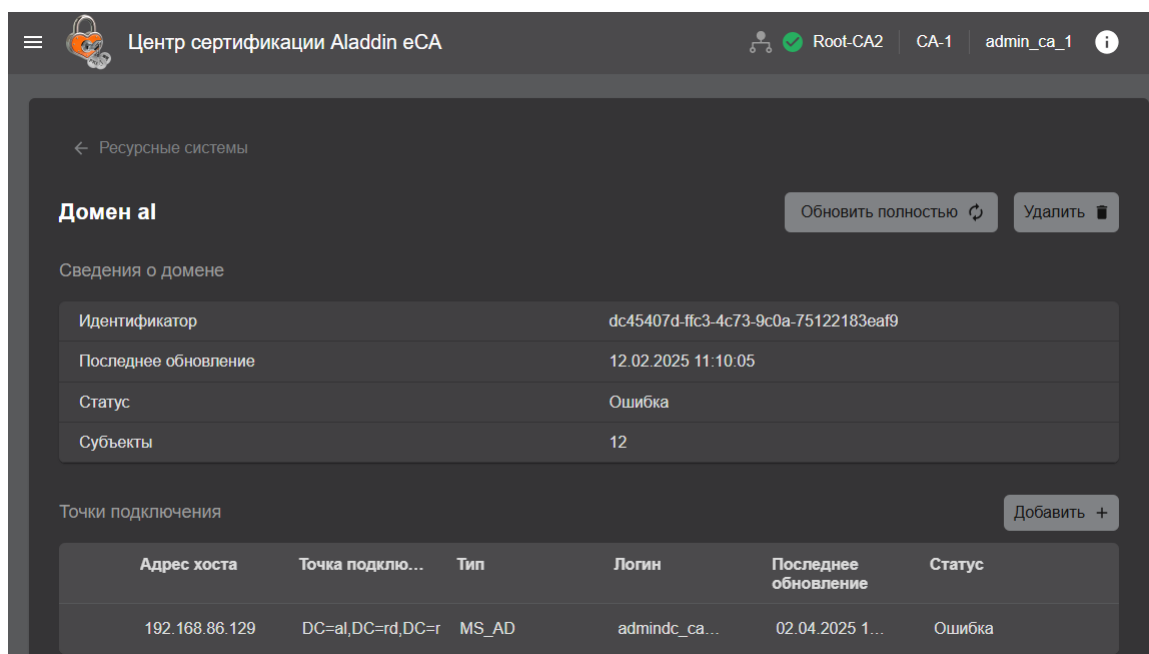


Рисунок 156 – Карточка ресурсной системы


В карточке ресурсной системы представлена следующая информация:

- имя домена;
- уникальный идентификатор ресурсной системы;
- дата и время последней попытки полной синхронизации ресурсной системы;

- статус ресурсной системы, который назначается в соответствии с критериями, приведенными в таблице выше (Таблица 21);
- количество субъектов, полученных из ресурсной системы.
- информация о точках подключения ресурсной систем:
  - адрес хоста - полное доменное имя или IP-адрес точки подключения ресурсной системы;
  - точка подключения – Base DN (Distinguished Name) уникальный идентификатор корневого объекта в LDAP-каталоге, который содержит в своем DN-объекты, получаемые из точки подключения;
  - тип – тип ресурсной системы: SambaDC, Альт домен, ALD PRO, MS\_AD, FreeIPA, RED ADM.
  - логин (имя) учетной записи администратора контроллера домена;
  - дата и время последней попытки синхронизации точки подключения;
  - статус точки подключения, который назначается в соответствии с критериями, приведенными в таблице ниже (Таблица 22);

Таблица 22 – Статусы точки подключения и критерии их присвоения

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

-  - пиктограмма «Очередь» показывает, что точке подключения ресурсной системы назначена задача, которая поставлена в очередь, так как в данный момент выполняется другая задача.

Точкам подключения ресурсных систем возможно назначить выполнение следующих задач:

- частичная синхронизация ресурсной системы (синхронизация точки подключения ресурсной системы) (см. раздел 7.9.3.4);
- удаление точки подключения зарегистрированной ресурсной системы (см. раздел 7.9.6).

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

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

- В карточке ресурсной системы доступны следующие действия:
  - запуск полной синхронизации ресурсной системы (см. раздел 7.9.3.3);
  - удаление зарегистрированной ресурсной системы (см. раздел 7.9.5);
  - регистрация новой точки подключения к ресурсной системе (см. раздел 7.9.1);
  - запуск частичной синхронизации точки подключения (см. раздел 7.9.3.4);
  - изменение параметров, указанные при регистрации точки подключения (см. раздел 7.9.4);
  - удаление точки подключения (см. раздел 7.9.6).

## 7.9.3 Синхронизация ресурсных систем

### 7.9.3.1 Виды синхронизации ресурсных систем

Центр сертификации Aladdin eCA поддерживает следующие виды синхронизации:

- Полная.  
Синхронизация списка субъектов (пользователей, компьютеров и сервисов (только для ALD PRO и FreeIPA), их атрибуты и сертификаты, список и состав групп безопасности) выполняется из всех точек подключения к ресурсной системе.
- Частичная.  
При частичной синхронизации выполняется синхронизация всех данных выбранных точек подключения к ресурсной системе, полученных при полной синхронизации, за исключением сведений об удалении субъектов 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.**

Синхронизация ресурсной системы производится постранично<sup>32</sup>. При этом максимально возможное количество объектов, получаемых при выполнении одного запроса, задаётся в параметре `ldap_partition_size` в конфигурационном файле `/opt/aecaCa/scripts/config.sh`.

### 7.9.3.2 Режимы синхронизации ресурсных систем

- Автоматический режим синхронизации.  
В данном режиме синхронизация всех зарегистрированных точек подключения к ресурсным системам выполняется по расписанию в соответствии с CRON-выражением, указанным в конфигурационном файле `/opt/aecaCa/scripts/config.sh`:
  - для задания расписания полной синхронизации укажите значение CRON-выражения для параметра `ldap_synch_resource` (значение по умолчанию '0 0 0 \* \* \*' – запуск полной синхронизации каждую полночь);
  - для задания расписания частичной синхронизации укажите значение CRON-выражения для параметра `ldap_synch_connection_point` (значение по умолчанию '0 \*/30 \* \* \* \*' – запуск частичной синхронизации каждые полчаса).
- Автоматизированный режим синхронизации.  
В данном режиме запуск синхронизации выполняется по команде пользователя с ролью «Администратор»:
  - запуск полной синхронизации выбранных ресурсных систем (см. раздел 7.9.3.3).
  - запуск частичной синхронизации выбранных точек подключения к ресурсным системам (см. раздел 7.9.3.4)

### 7.9.3.3 Полная синхронизация ресурсной системы в автоматизированном режиме

Запуск полной синхронизации ресурсной системы может осуществляться путем нажатия на кнопку «Обновить» для ресурсной системы в разделе «Ресурсные системы» (см. Рисунок 157) или путем нажатия на кнопку «Обновить полностью» в карточке ресурсной системы (см. Рисунок 156).

<sup>32</sup> Центр сертификации Aladdin eCA получает данные из ресурсной системы частями, выполняя несколько запросов с ограничением на максимальное количество выдаваемых объектов вместо одного запроса на выгрузку сразу всех данных.

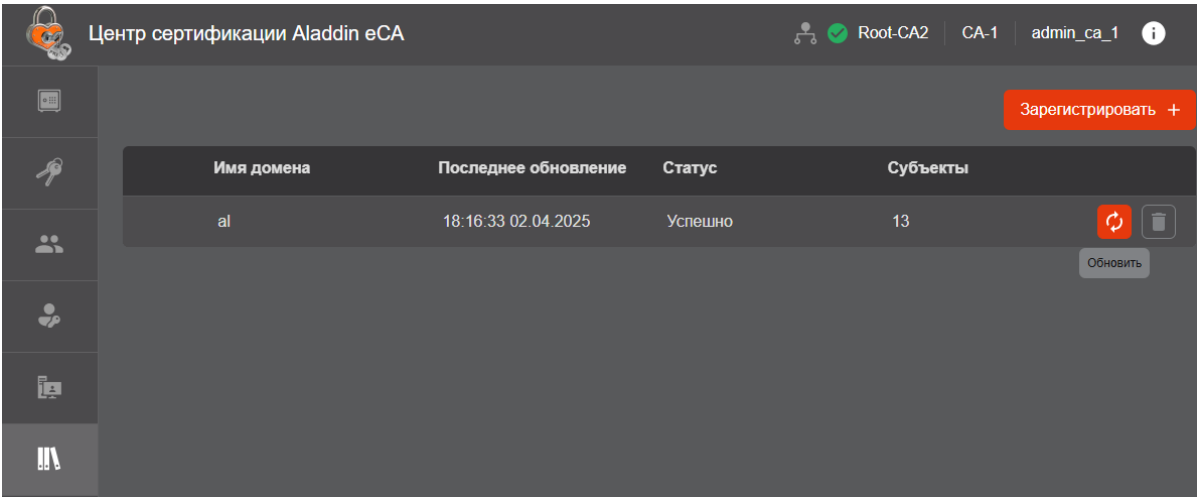


Рисунок 157 – Запуск полной синхронизации ресурсной системы из раздела «Ресурсные системы»

7.9.3.4 Частичная синхронизация точки подключения в автоматизированном режиме

Запуск частичной синхронизации точки подключения осуществляется путем нажатия на кнопку <Обновить> для выбранной точки подключения в карточке ресурсной системы (см. Рисунок 158).

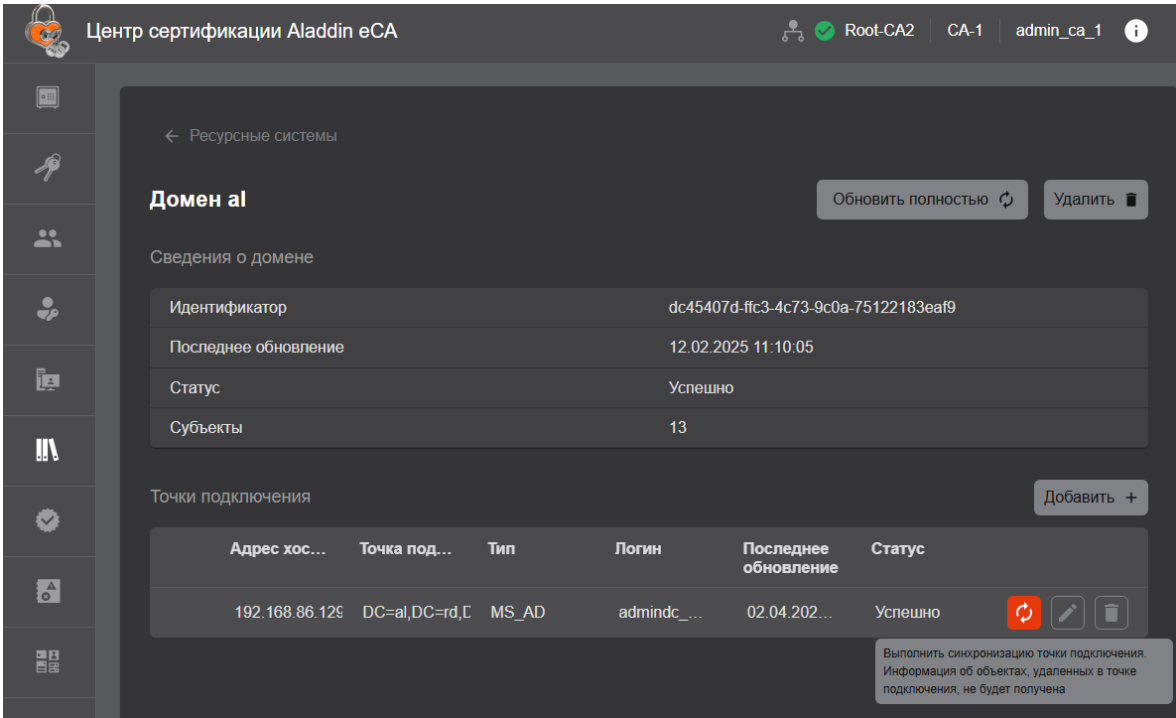



Рисунок 158 – Запуск частичной синхронизации точки подключения

7.9.4 Редактирование параметров точки подключения

- Для редактирования параметров точки подключения необходимо в карточке ресурсной системы нажать на кнопку <Редактировать>  около точки подключения (см. Рисунок 159).



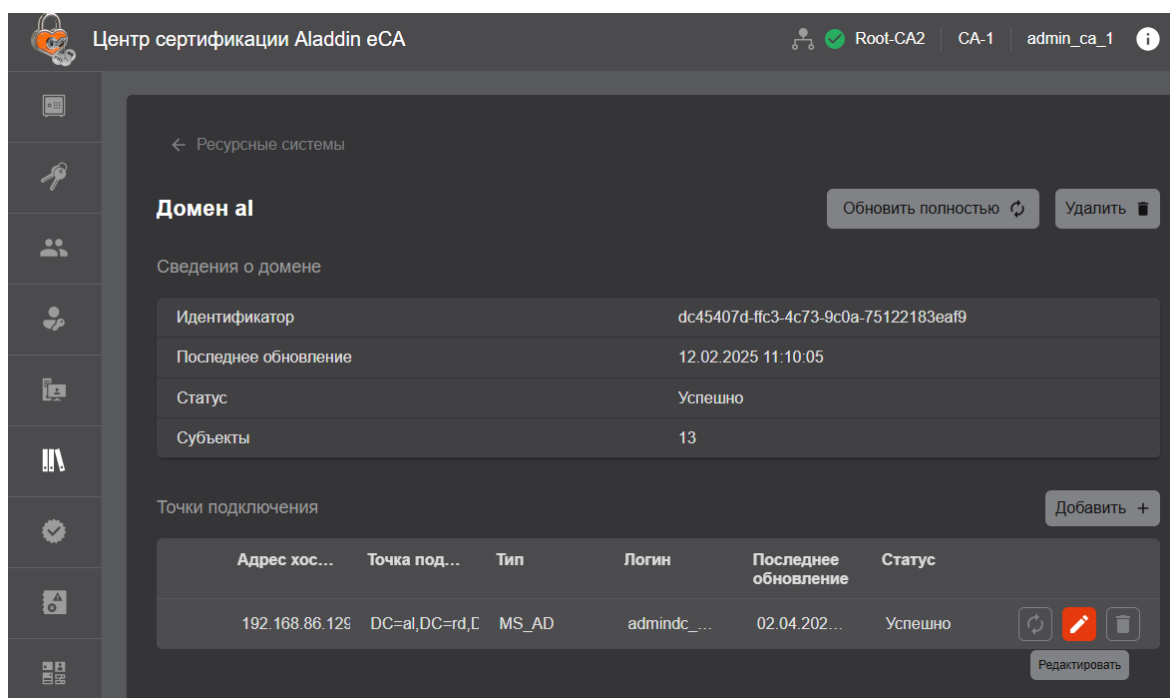


Рисунок 159 – Окно раздела «Ресурсная система». Кнопка редактирования РС

- После этого открывается окно для редактирования полей, заполненных при создании точки подключения. Тип подключаемого ресурса изменить невозможно (см. Рисунок 160).

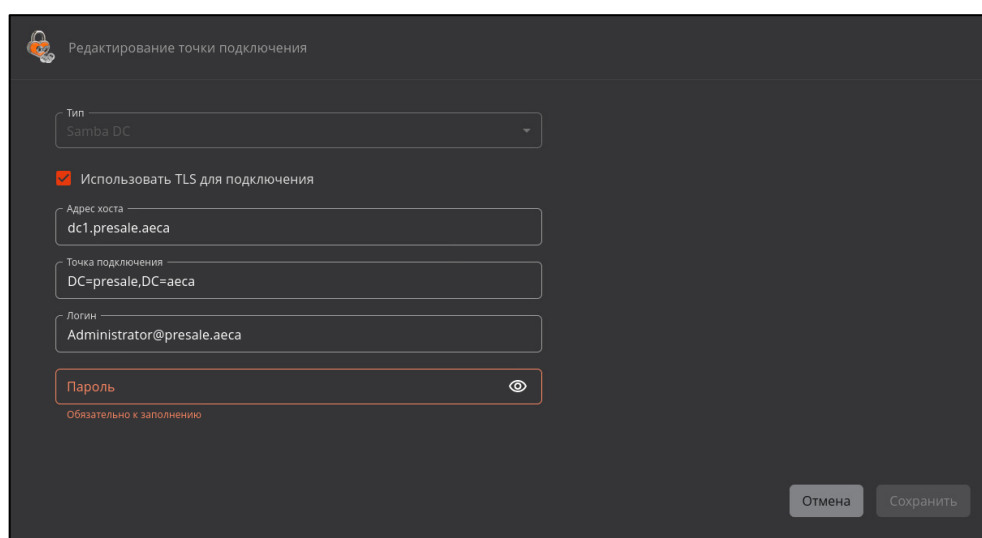


Рисунок 160 – Окно редактирования подключения к РС

- Для сохранения и применения параметров необходимо нажать кнопку <Сохранить>.

### 7.9.5 Удаление зарегистрированной ресурсной системой

- Удаление ресурсной системы может осуществляться путем нажатия на кнопку <Удалить> для ресурсной системы в разделе «Ресурсные системы» (см. Рисунок 161) или путем нажатия на кнопку <Удалить> в карточке ресурсной системы (см. Рисунок 156). **Ошибка! Источник ссылки не найден.**

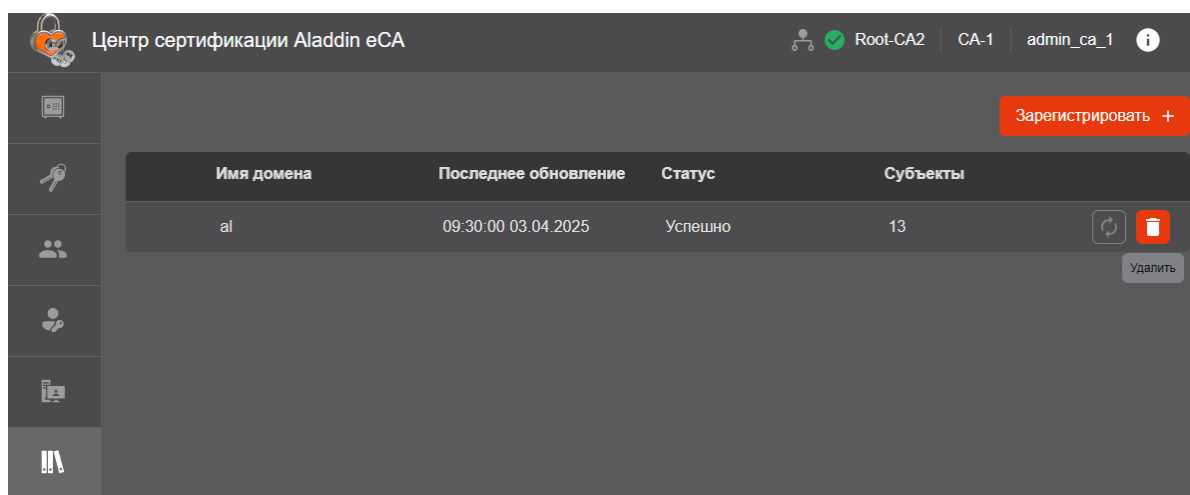


Рисунок 161 – Удаление ресурсной системы из раздела «Ресурсные системы»

- После этого отобразится окно подтверждения выбранного действия (см. Рисунок 162).

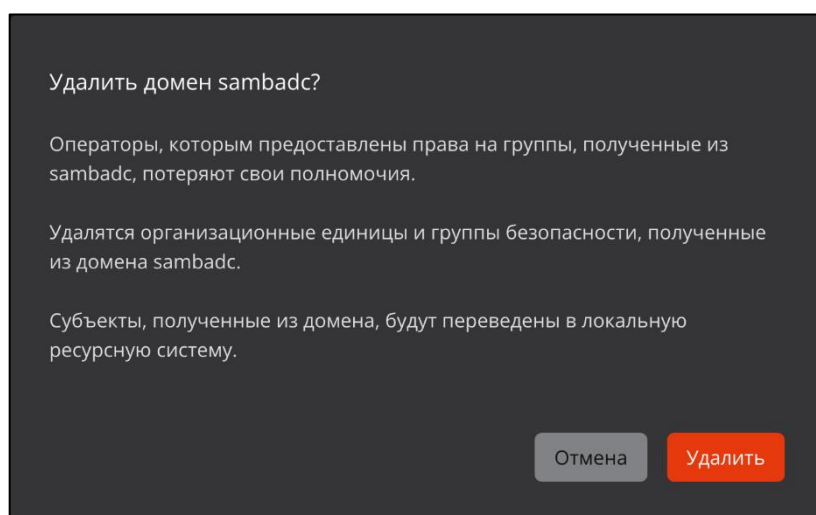


Рисунок 162 – Окно подтверждения удаления ресурсной системы

- Для удаления нажмите на кнопку <Удалить>.
- В результате удаления ресурсной системы:
  - все субъекты, полученные из этой ресурсной системы, будут переведены в локальную ресурсную систему;
  - будут удалены группы безопасности, полученные из этой ресурсной системы;
  - операторы, которым были предоставлены права на группы, полученные из этой ресурсной системы, потеряют свои полномочия.

#### 7.9.6 Удаление точки подключения к ресурсной системе

- Удаление точки подключения осуществляется путем нажатия на кнопку <Удалить> для точки подключения в карточке ресурсной системы (см. Рисунок 163).

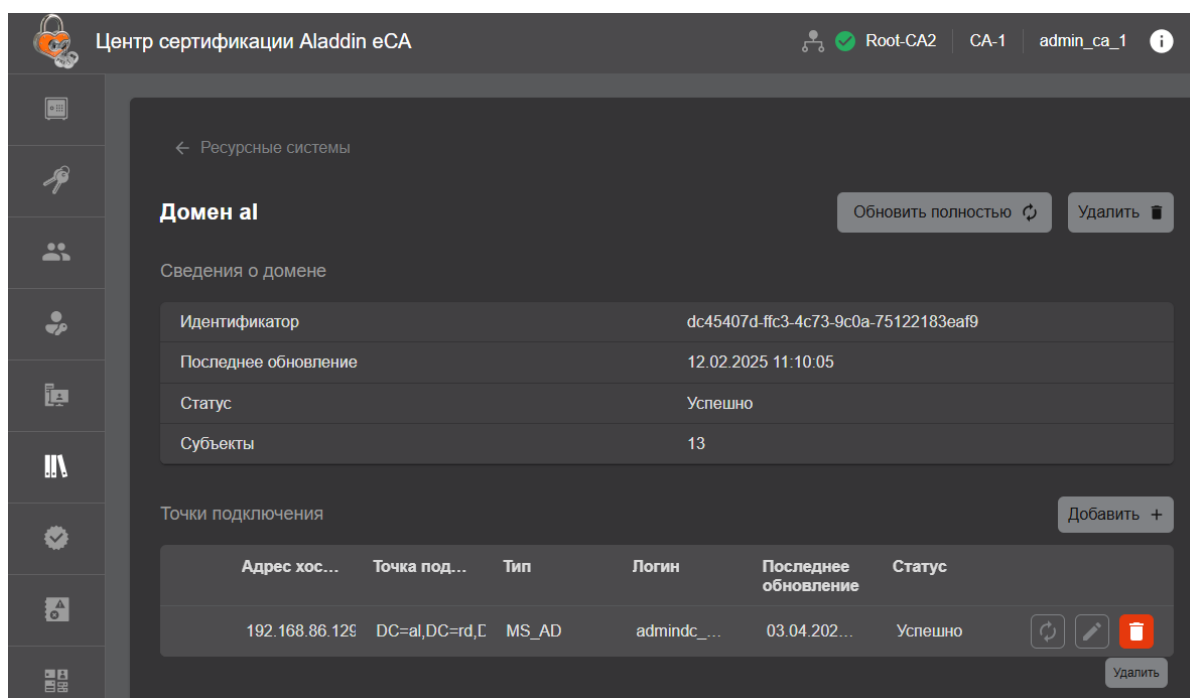


Рисунок 163 – Удаление ресурсной системы из карточки ресурсной системы

- После этого отобразится окно подтверждения выбранного действия (см. Рисунок 164).

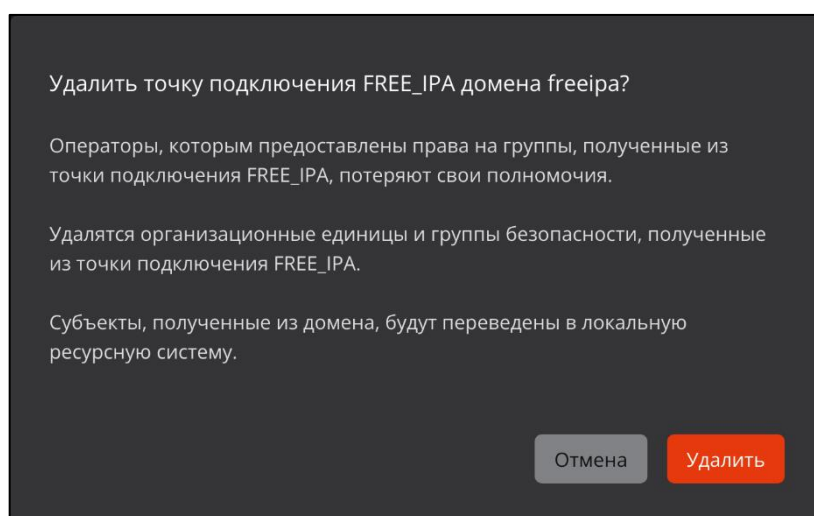


Рисунок 164 – Окно подтверждения удаления точки подключения

- Для удаления нажмите на кнопку <Удалить>.
- В результате удаления точки подключения:
  - все субъекты, полученные из этой точки подключения, будут переведены в локальную ресурсную систему;
  - будут удалены и группы безопасности, полученные из этой точки подключения;
  - операторы, которым были предоставлены права на группы, полученные из этой точки подключения, потеряют свои полномочия.

## 7.10 Раздел «Центры валидации»

Переход в раздел «Центры валидации» выполняется через боковое меню, расположенное слева на главном экране (см. Рисунок 165). Данный раздел доступен только для пользователя с ролью «Администратор».

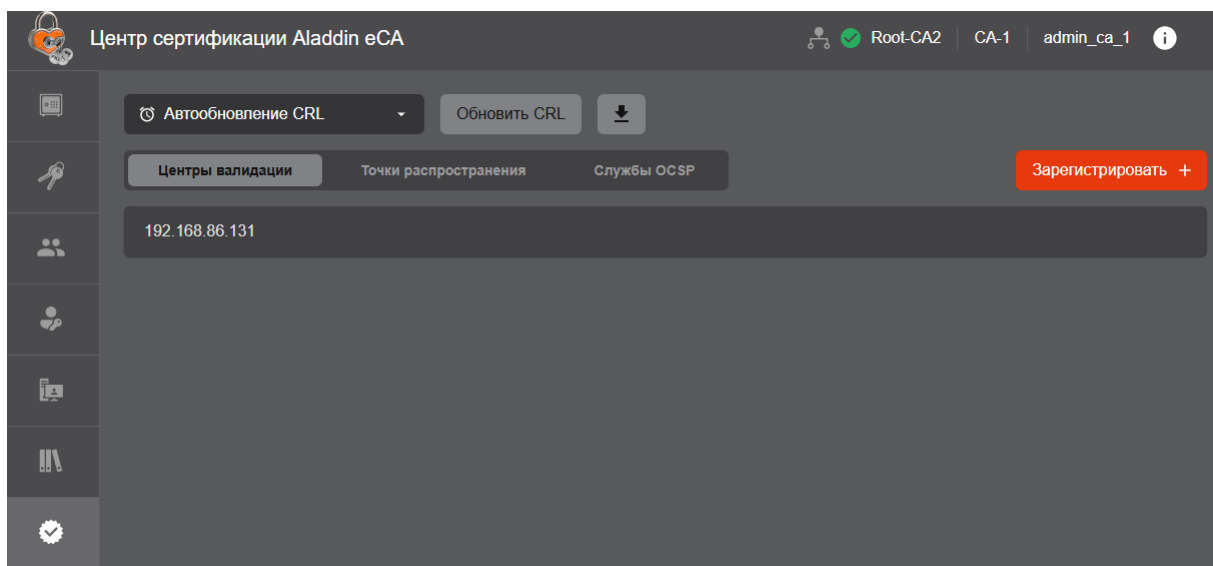


Рисунок 165 – Экран раздела «Центр валидации»

Раздел «Центры валидации» предназначен для выполнения следующих сценариев:

- Автоматизированная публикация списков отозванных сертификатов CRL по команде уполномоченного пользователя.
- Регистрация центров валидации.
- Настройка параметров центров валидации.
- Удаление центров валидации.
- Настройка периода автоматического обновления точек публикации CRL и срока действия перекрытия Delta CRL для активного центра сертификации.
- Экспорт актуального списка отозванных сертификатов CRL.
- Экспорт сертификата текущего издающего центра сертификации.
- Создание пользовательских точек распространения CRL, Delta CRL и AIA.
- Публикация CRL, Delta CRL и AIA в LDAP-каталог точек распространения ресурсных систем.
- Просмотр служб OCSP, зарегистрированных центров валидации.
- Создание пользовательской службы OCSP.

### 7.10.1 Настройка периодичности автоматического обновления CRL

Чтобы настроить периодичность автоматического обновления CRL и формирования Delta CRL, на верхней панели раздела «Центр валидации» раскройте список <Автообновление CRL> (см. Рисунок 166).

В раскрывшемся информационном блоке представлена следующая информация:

- Текущий период обновления публикации CRL и срок действия перекрытия CRL (CRL overlap).
- Дата и время последней публикации CRL.
- Дата и время следующей публикации CRL.
- Текущий период обновления публикации Delta CRL;
- Статус настройки автоматической генерации и публикации Delta CRL при изменении статусов сертификатов.

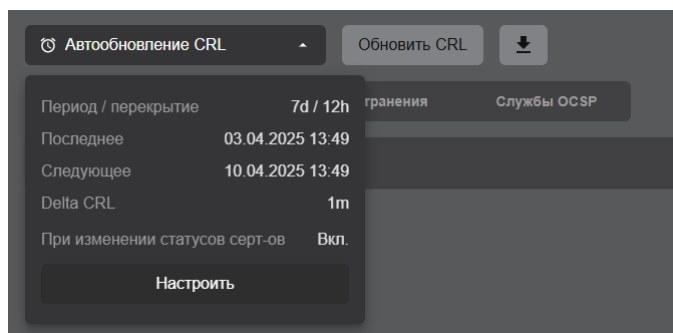


Рисунок 166 – Просмотр настроек автоматического обновления CRL

**ВНИМАНИЕ!** При изменении периодичности автоматического обновления CRL и формирования Delta CRL точки публикации активного центра сертификации перенастраивается время публикации всех списков CRL текущего центра сертификации. Время публикации CRL синхронизировано при настройке периода публикации, при создании нового сервиса публикации, при публикации по команде (включая REST API) и одинаково для всех точек публикации текущего центра сертификации.

- В раскрывшемся информационном блоке нажмите кнопку <Настроить> (см. Рисунок 166).
- В открывшемся окне выполните настройку следующих параметров автоматического обновления CRL (см. Рисунок 167):
  - Период обновления (публикации) CRL (crlperiod) (формат ввода: 1m, 1h, 1d, 1mo, 1y – минута, час, день, месяц, год).
  - Срок действия перекрытия CRL (crlOverlapTime) – временной отрезок до истечения срока действия текущего CRL, за который будет публиковаться новый CRL (формат ввода: 1m, 1h, 1d, 1mo, 1y – минута, час, день, месяц, год).
  - Для включения режима генерации и рассылки Delta CRL установите флажок «Рассылать Delta CRL».
  - Период обновления Delta CRL (deltacrlperiod) – время между публикациями Delta CRL. При вводе значения, превышающего заданный период обновления CRL, будет выведено предупреждение и до ввода корректного значения сохранить настройки будет невозможно.

Для включения режима автоматической генерации и публикации CRL (Delta CRL) при изменении статусов (отзыве/приостановке/возобновлении действия) сертификатов установите флажок «Генерировать и публиковать новый CRL при изменении статусов сертификатов» или «Генерировать и публиковать новый Delta CRL при изменении статусов сертификатов» (при включенной рассылке Delta CRL).

**Внимание!** Период публикации CRL должен быть больше периода публикации Delta CRL. Период публикации DeltaCRL может быть не задан, тогда Delta CRL не публикуется.

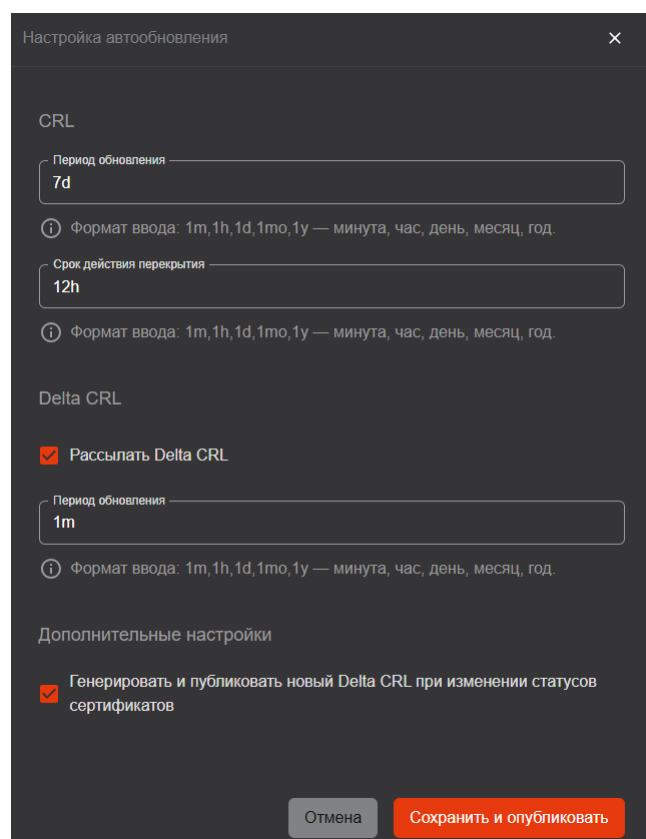


Рисунок 167 – Настройка автоматического обновления CRL

- Значения периодов обновления публикаций CRL и Delta CRL следует выбирать исходя из интенсивности обновления списка сертификатов в конкретных условиях эксплуатации.
- Значение срока действия перекрытия стоит выбирать исходя из следующих рекомендации:
  - Срок действия перекрытия (crlOverlapTime) должен составлять 1/10 от значения периода обновления публикаций CRL (crlperiod), но не более 12 часов. При этом должны выполняться две рекомендации, приведенные ниже.
  - Срок действия перекрытия (crlOverlapTime) не должен быть больше периода обновления Delta CRL (deltaCrlperiod), если выполняется следующее условие, приведенное ниже.
  - Срок действия перекрытия (crlOverlapTime) не должен быть меньше 1/5 от интервала рассинхронизации времени в сети (обычная рассинхронизация составляет не более 10 мин).
- Файлы CRL содержат следующие данные, указывающие на время действия списка отозванных сертификатов:
  - <Last Update> – дата и время вступления в силу CRL (момент начала действия).
  - <Next Update> – дата и время следующего обновления CRL (момент истечения срока действия CRL, когда CRL становится недействительным для проверки).
- При планировании срока действия CRL необходимо учитывать время следующей публикации <Next Publish> (момент выпуска центром сертификации нового CRL).
- Между настроенными значениями и значениями, которые указываются в файле CRL (Delta CRL) и выводятся в интерфейсе пользователя, должна быть следующая связь:
  - для CRL:
    - <Last Update> = <Время создания CRL>
    - <Next Publish> = <Last Update> + <crlperiod>

- $\langle \text{Next Update} \rangle = \langle \text{Next Publish} \rangle + \langle \text{crlOverlapTime} \rangle$
- для Delta CRL:
  - $\langle \text{Last Update} \rangle = \langle \text{время создания Delta CRL} \rangle$
  - $\langle \text{Next Publish} \rangle = \langle \text{Last Update} \rangle + \langle \text{deltacrlperiod} \rangle$
  - $\langle \text{Next Update} \rangle = \langle \text{Next Publish} \rangle$
- При каждой новой генерации CRL увеличивается значение номера версии (CRLNumber).
- При каждой новой генерации Delta CRL увеличивается значение CRLNumber индикатора (DeltaCRLIndicator) и соответствует тому CRL, для которого указана разница.
- Служба CRL DP начинает распространять CRL и Delta CRL с большим номером (версии и индикатора) сразу после его поступления и проверки подписи издателя.
- Если рассылка Delta CRL выключена, но на вкладке «Точки распространения» зарегистрированы точки распространения данного типа, то они не будут попадать в создаваемые сертификаты. В этом случае точки распространения будут отмечены восклицательным знаком в треугольнике, с отображением всплывающего сообщения «Точки распространения Delta CRL не будут попадать в создаваемые сертификаты, так как рассылка Delta CRL выключена (см.

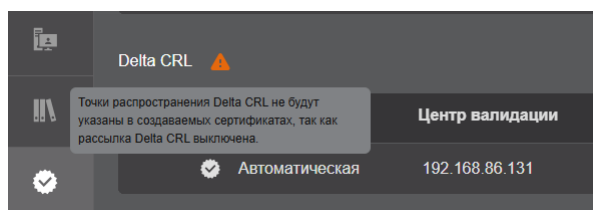


Рисунок 168 – Индикация точки распространения Delta CRL при выключенной рассылке Delta CRL

### 7.10.2 Автоматизированная публикация списка отозванных сертификатов CRL

Список отозванных сертификатов может быть обновлен внепланово по команде уполномоченного пользователя с ролью «Администратор». Для этого на верхней панели вкладки «Центры валидации» раздела «Центры валидации» нажмите кнопку «Обновить CRL» (см. Рисунок 169). При этом таймер автоматической публикации CRL сбрасывается, и начинается новый отсчет времени публикации.

Все сгенерированные списки отозванных сертификатов в формате .crl будут сохранены в базе данных (конфигурация базы данных указана в файле `/opt/aecaCa/scripts/config.sh`).

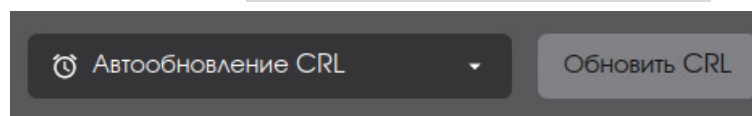



Рисунок 169 – Обновление CRL по команде администратора

### 7.10.3 Экспорт актуального списка отозванных сертификатов CRL

Для загрузки списка отозванных сертификатов CRL выполните следующие действия:

- На верхней панели вкладки «Центры валидации» раздела «Центры валидации» нажмите кнопку «Скачать CRL» .
- В открывшемся окне в зависимости от текущего состояния Центра сертификации Aladdin eCA выполните одно из следующих действий:
  - Если в Центре сертификации Aladdin eCA не зарегистрирован ни один центр валидации и CRL ранее не публиковался, то опубликуйте и загрузите новый CRL (см. Рисунок 170). Для этого в соответствующем поле укажите срок действия CRL и нажмите кнопку «Сгенерировать и скачать».

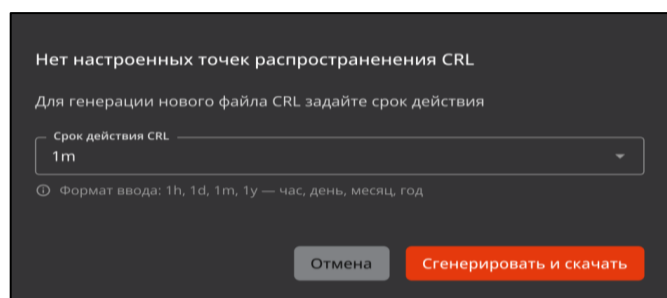


Рисунок 170 – Публикация и выгрузка нового CRL

- Если в Центре сертификации Aladdin eCA не зарегистрирован ни один центр валидации, а CRL ранее публиковался, то выполните одно из следующих действий (см. Рисунок 171):
  - Выгрузите последний опубликованный CRL. Для этого установите переключатель в положение «Скачать последний» и нажмите кнопку «Скачать».
  - Опубликуйте и выгрузите новый CRL. Для этого установите переключатель в положение «Сгенерировать новый», в соответствующем поле укажите срок действия CRL и нажмите кнопку «Сгенерировать и скачать».

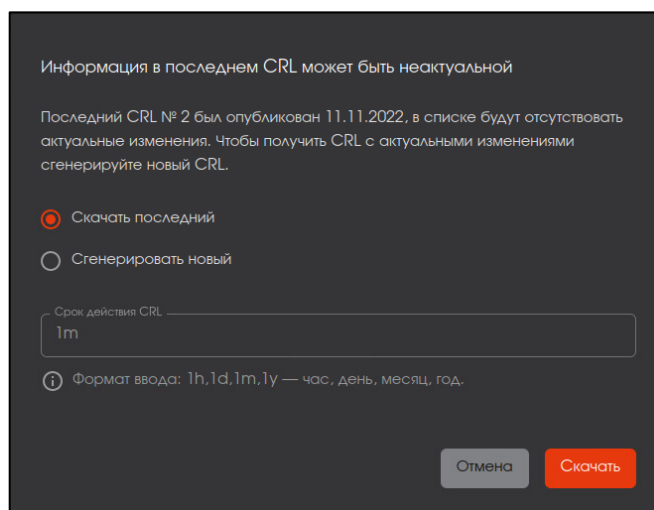


Рисунок 171 – Выгрузка последнего опубликованного CRL

- Если в Центре сертификации Aladdin eCA зарегистрирован хотя бы один центр валидации, скачайте последний опубликованный CRL, нажав кнопку «Скачать последний» (см. Рисунок 172).

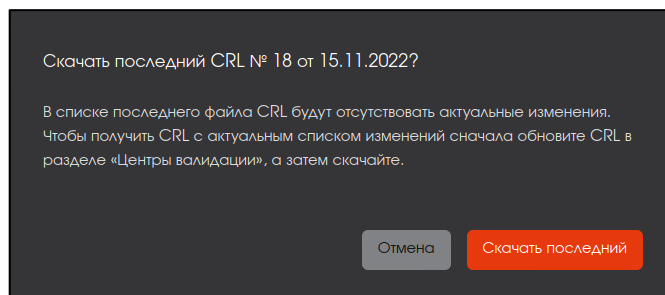


Рисунок 172 – Выгрузка последнего опубликованного CRL

**Время в экспортированном CRL указано в формате GMT+0.**



#### 7.10.4 Управление центрами валидации

Возможно создание нескольких записей для разных центров валидации, включающих точки распространения списков отозванных сертификатов (CRL DP) и информации о центре сертификации (AIA).



##### 7.10.4.1 Регистрация центра валидации

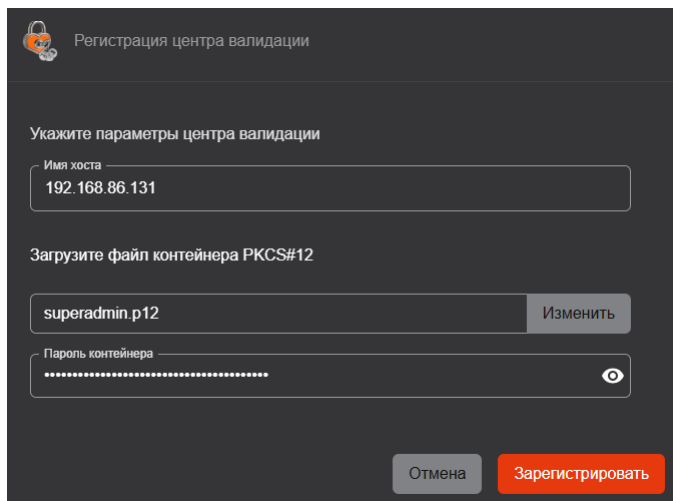
Процесс регистрации центра валидации заключается в активации служб AIA, CRL DP и OCSP.

Перед регистрацией центра валидации выполните следующие действия:

- Разверните программный комплекс «Центр валидации Aladdin Enterprise Certificate Authority» согласно документу «Центр сертификатов доступа Aladdin Enterprise Certificate Authority Certified Edition. Руководство администратора. Часть 3. Центр валидации Aladdin Enterprise Certification Authority».
- Выгрузите сертификат учётной записи пользователя с ролью «Администратор» центра валидации (контейнер PKCS#12, по умолчанию имя файла – superadmin.p12). Пароль к контейнеру находится в файле «generated\_passwords.txt».
- Перенесите подготовленные данные на компьютер, с которого выполняется подключение к веб-интерфейсу Центра сертификации Aladdin eCA.
- Настройте автоматическое обновление CRL (см. раздел 7.10.1).
- Опубликуйте CRL в автоматизированном режиме (см. раздел 7.10.2).

Для регистрации центра валидации выполните следующие действия:

- Перейдите на вкладку «Центры валидации» раздела «Центры валидации» и нажмите кнопку  .
- В открывшемся окне (см. Рисунок 173) укажите параметры центра валидации:
  - В поле «Имя хоста» укажите IP-адрес или полное доменное имя компьютера с установленным Центром валидации Aladdin eCA.
  - Нажмите кнопку <Выбрать файл> и укажите путь к контейнеру PKCS#12 (superadmin.p12) с сертификатом учетной записи с ролью «Администратор» Центра валидации Aladdin eCA.
  - В поле «Пароль контейнера» введите пароль к контейнеру PKCS#12 (пароль будет размещен в базе данных в зашифрованном по алгоритму AES256 виде).
- Нажмите кнопку  .



Регистрация центра валидации

Укажите параметры центра валидации

Имя хоста  
192.168.86.131

Загрузите файл контейнера PKCS#12

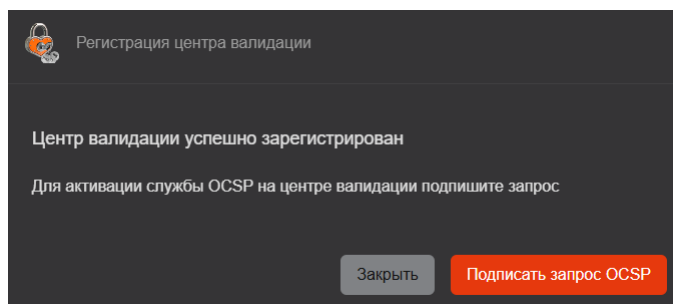
superadmin.p12 Изменить

Пароль контейнера  
..... 👁

Отмена Зарегистрировать

Рисунок 173 – Регистрация центра валидации

- На последнем шаге в открывшемся окне отображается информация об успешной регистрации центра валидации (см. Рисунок 174).



Регистрация центра валидации

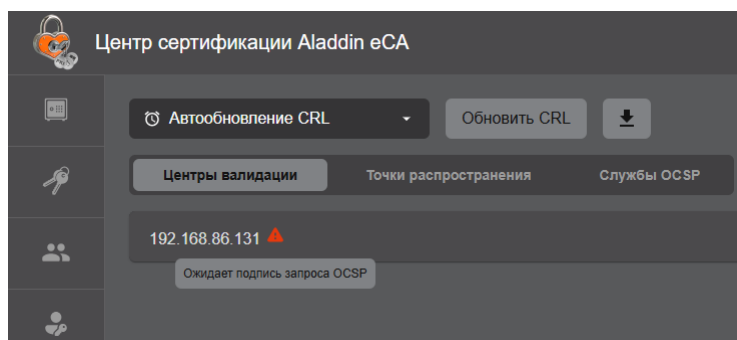
Центр валидации успешно зарегистрирован

Для активации службы OSCP на центре валидации подпишите запрос

Закреть Подписать запрос OSCP

Рисунок 174 – Завершение регистрации центра валидации

- В текущем окне вы можете перейти к процессу подписания запроса OSCP, нажав кнопку <Подписать запрос OSCP>, или выполнить данное действия позже из карточки центра валидации (см. раздел 7.10.4.2).
- Если запрос OSCP не подписан на этапе регистрации центра валидации, то центру валидации назначается статус «Ожидает подпись запроса OSCP» (см. Рисунок 175).



Центр сертификации Aladdin eCA

Автообновление CRL Обновить CRL 📄

Центры валидации Точки распространения Службы OSCP

192.168.86.131	Ожидает подпись запроса OSCP
----------------	------------------------------

Рисунок 175 – Центр валидации в статусе «Ожидает подпись запроса OSCP»

Схема взаимодействия Центра сертификации Aladdin eCA и Центра валидации Aladdin eCA после инициализации служб CRL DP, AIA и OSCP представлена на рисунке ниже (см. Рисунок 176).

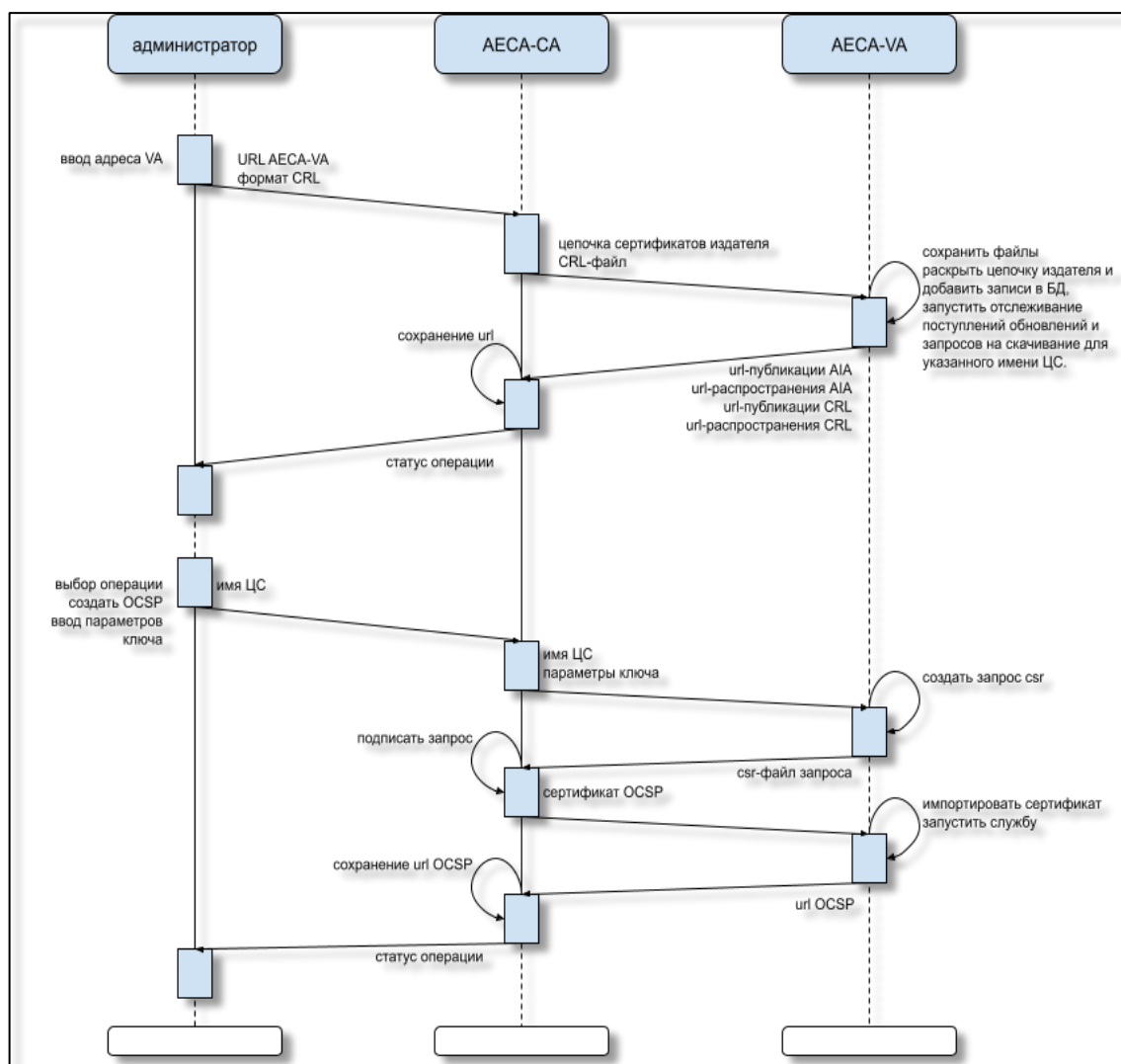


Рисунок 176 – Схема взаимодействия ПО «Центр сертификации» и ПО «Центр валидации»

#### 7.10.4.2 Подписание запроса OSCP-сервера

**Внимание! Перед активацией службы OSCP необходимо настроить автообновление CRL.**

Для активации службы подпишите запрос OSCP-сервера:

- Если вы не начали процесс подписания запроса OSCP на этапе регистрации центра валидации, откройте его карточку (см. раздел 7.10.4.3) и в разделе «OCSP» нажмите кнопку **Подписать запрос +**.
- В открывшемся окне (см. Рисунок 177) с помощью флажков выберите дополнительные расширения OSCP (по умолчанию рекомендовано выбрать все расширения) и нажмите кнопку <Продолжить>:
  - <Статус неизвестных сертификатов GOOD (рекомендуется)> – расширение определяет, что для любого сертификата, не указанного в CRL, ответ сервера «good», а если не удалось установить статус сертификата (серверу не известен издатель) – ответ «unknown (off)».
  - <Включать цепочку сертификатов в ответ (рекомендуется)> и <Включать сертификат подписи в ответ (рекомендуется)> – расширения определяют соответственно включать или не включать цепочку сертификатов и сертификат подписи (сертификат OSCP) в ответ сервера.

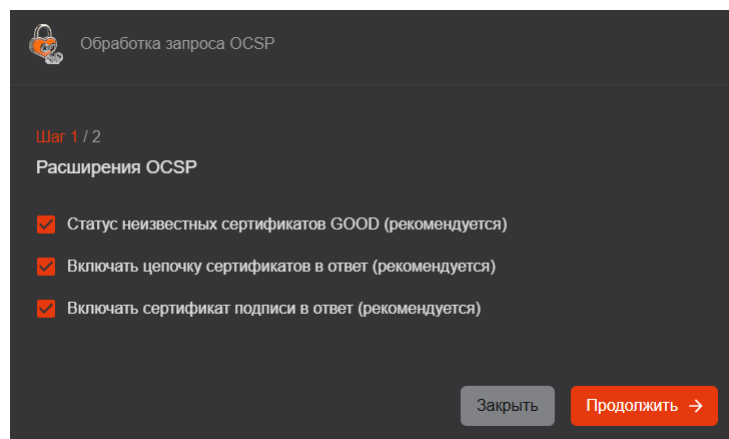


Рисунок 177 –Выбор расширений OCSP. Шаг 1

- В открывшемся окне (см. Рисунок 178) укажите параметры криптографии:

- Алгоритм ключа:

- RSA\_1024;
- RSA\_2048 (выбран по умолчанию);
- RSA\_4096;
- ECDSA\_224;
- ECDSA\_256;
- ECDSA\_384;
- ECDSA\_521;

- Алгоритм хэш-суммы:

- MD5\_WITH\_RSA;
- SHA1\_WITH\_RSA;
- SHA256\_WITH\_RSA (выбран по умолчанию);
- SHA384\_WITH\_RSA;
- SHA512\_WITH\_RSA;
- SHA3\_256\_WITH\_RSA;
- SHA3\_384\_WITH\_RSA;
- SHA3\_512\_WITH\_RSA;
- SHA1\_WITH\_ECDSA;
- SHA256\_WITH\_ECDSA;
- SHA384\_WITH\_ECDSA;
- SHA512\_WITH\_ECDSA;
- SHA3\_256\_WITH\_ECDSA;
- SHA3\_384\_WITH\_ECDSA;
- SHA3\_512\_WITH\_ECDSA.

**Внимание! Необходимо выбирать алгоритм хэш-суммы, содержащий название выбранного алгоритма ключа в своем названии. Например, при выборе алгоритма ключа RSA\_1024 необходимо выбирать алгоритм хэш-суммы из вариантов MD5\_WITH\_RSA, SHA1\_WITH\_RSA, SHA256\_WITH\_RSA и т.п.**

- Для завершения процесса подписи запроса OCSP нажмите кнопку <Подписать и запустить>.

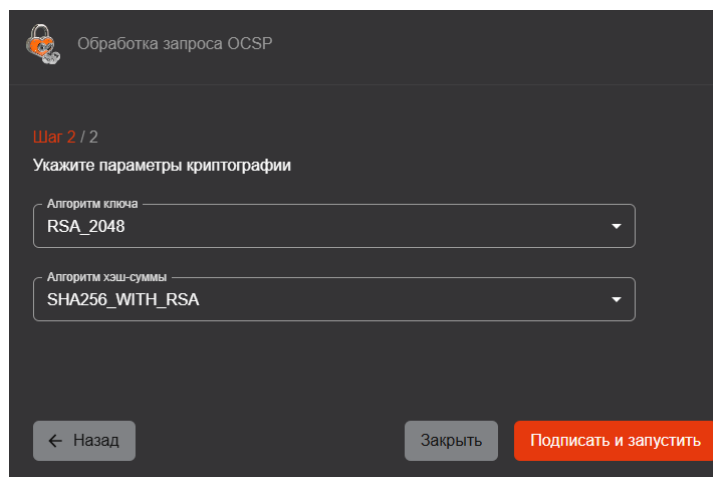


Рисунок 178 – Выбор параметров криптографи при обработке запроса OCSP. Шаг 2

- В открывшемся окне с сообщением об успешной активации службы OCSP нажмите кнопку <Заккрыть> (см. Рисунок 179).

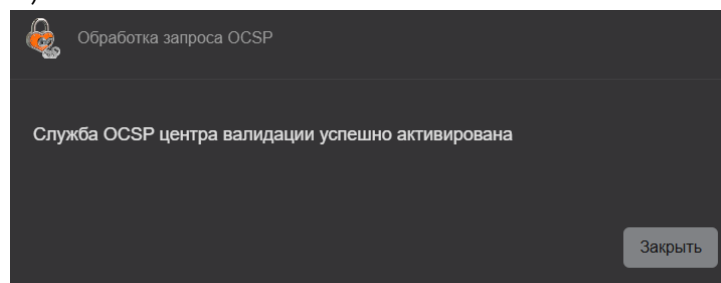


Рисунок 179 – Служба OCSP успешно запущена

**Внимание! В случае ошибки активации службы OCSP будет выведено сообщение «Ошибка подписания запроса и запуска сервиса. Проверьте подключение и работоспособность ЦВ. Сравните атрибуты имени субъекта с зарегистрированными сервисами ЦВ. Атрибуты не должны совпадать».**

**Возможные причины ошибки:**

- Центр валидации недоступен.
- Некорректный выбор комбинации алгоритма ключа и алгоритма хэш-суммы.
- Наличие в центре валидации активированной службы OCSP, у которой в сертификате указан аналогичный SDN (отличительное имя субъекта) издателя.

В результате выполненных действий будет выпущен сертификат OCSP-сервера сроком действия на 2 года. Просмотр карточки и выгрузка сертификата доступны на вкладке «Сертификаты». После подписания запроса OCSP-сервера на выпуск сертификата центр валидации переходит в состояние «Запущен» (см. Рисунок 180).

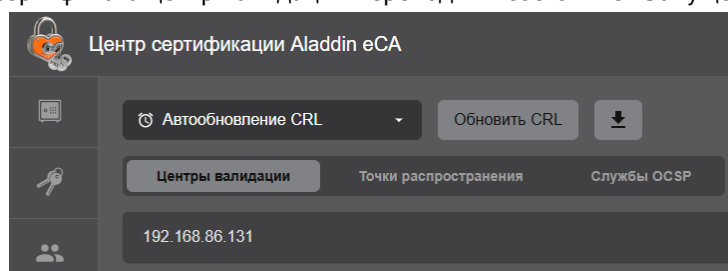


Рисунок 180 – Центр валидации в состоянии «Запущен»

### 7.10.4.3 Просмотр карточки центра валидации

Для просмотра карточки зарегистрированного центра валидации (см. Рисунок 181) перейдите на вкладку «Центры валидации» раздела «Центры валидации» и щелкните в списке строку с выбранным центром валидации.

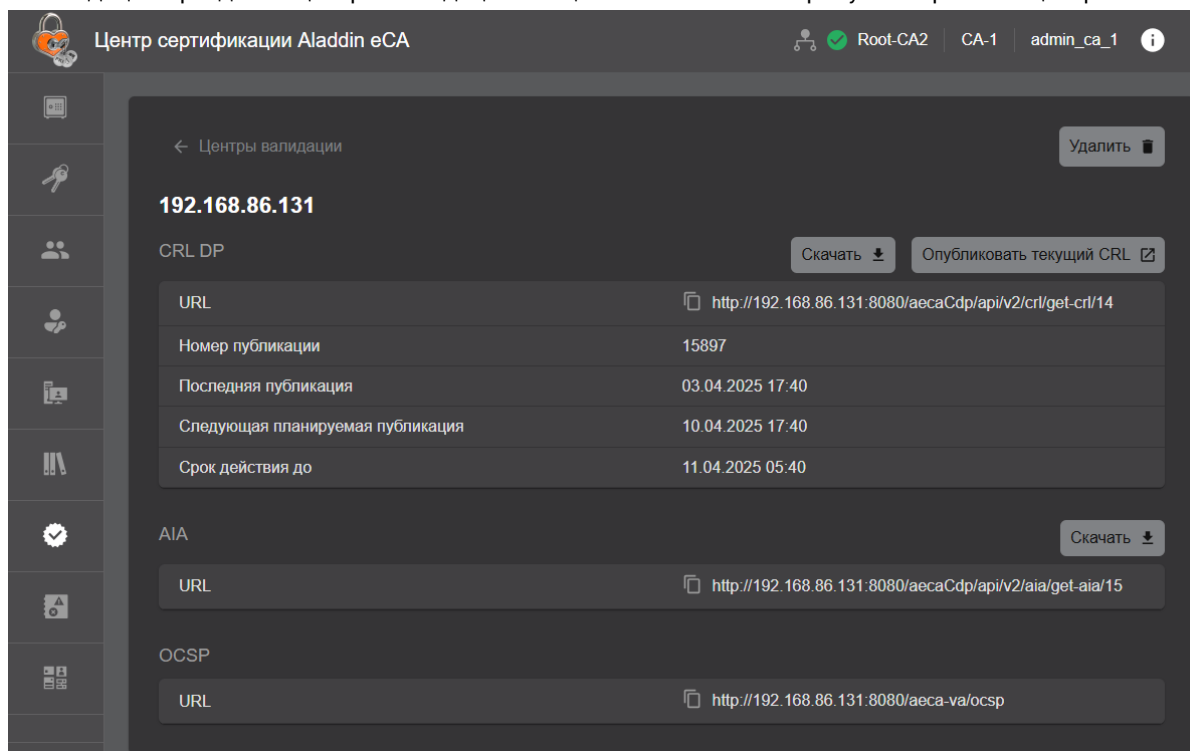





Рисунок 181 – Карточка зарегистрированного центра валидации

После регистрации центра валидации создаются службы CRL DP и AIA, а в карточке центра валидации появляются их адреса



В карточке центра валидации доступны следующие операции и информация:

- Удаление центра валидации (см. раздел 7.10.4.4).
- Для службы CRL DP:
  - Выгрузка списка отозванных сертификатов CRL. Для этого нажмите кнопку <Скачать>.
  - Публикация последнего сгенерированного CRL в Центре валидации Aladdin eCA. Для этого нажмите кнопку <Опубликовать текущий CRL>.
  - Просмотр URL выгрузки CRL. URL будет включаться в выпускаемые сертификаты (см. 7.10.9). Чтобы скопировать URL в буфер обмена, щелкните рядом с адресом CRL DP значок .
  - Просмотр порядкового номера публикации CRL.
  - Просмотр даты и времени последней публикации CRL.
  - Просмотр даты и времени следующей публикации CRL.
  - Просмотр даты и времени окончания срока действия CRL.
- Для службы AIA:
  - Выгрузка опубликованного сертификата текущего издающего центра сертификации. Для этого нажмите кнопку <Скачать>;
  - Просмотр URL выгрузки сертификата издателя. URL будет включаться в выпускаемые сертификаты (см. раздел 7.10.9). Чтобы скопировать URL в буфер обмена, щелкните рядом с адресом AIA значок .

- Для службы OCSP – просмотр URL OCSP-сервера. URL будет включаться в выпускаемые сертификаты (см. раздел 7.10.9). Чтобы скопировать URL в буфер обмена, щелкните рядом с адресом OCSP значок .

#### 7.10.4.4 Удаление центра валидации

Для удаления зарегистрированного центра валидации выполните следующие действия:

- Перейдите на вкладку «Центры валидации» раздела «Центры валидации».
- Наведите указателем мыши на выбранный центр валидации в списке и нажмите кнопку  <Удалить> или откройте карточку центра валидации (см. раздел 7.10.4.3, Рисунок 181) и нажмите кнопку  **Удалить**.

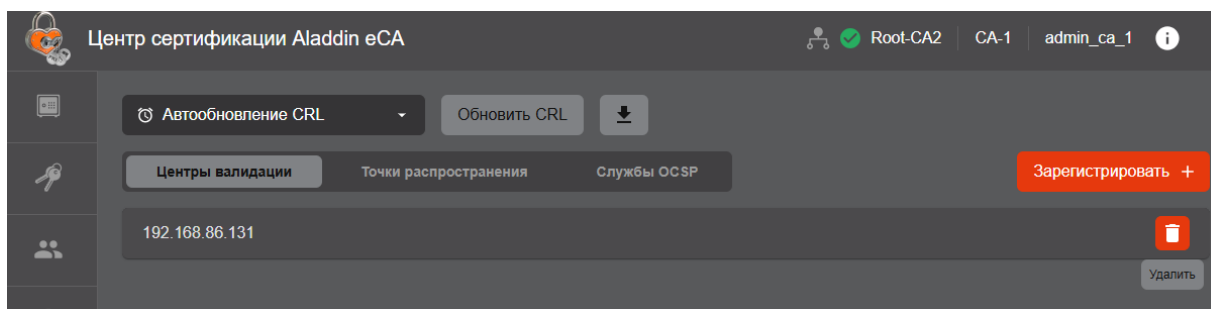


Рисунок 182 – Удаление центра валидации

- В открывшемся окне (см. Рисунок 183) подтвердите удаление, нажав кнопку <Удалить>.

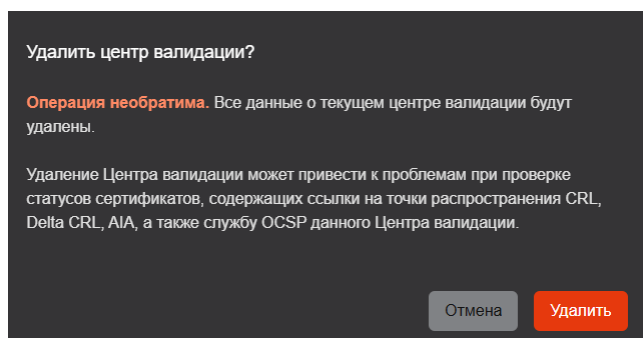




Рисунок 183 – Подтверждение удаления центра валидации

#### 7.10.5 Управление точками распространения

- Вкладка «Точки распространения» раздела «Центры валидации» предназначена для:
  - Просмотра URL точек распространения CRL, Delta CRL и AIA, зарегистрированных Центров валидации Aladdin eCA, образующих **автоматические точки распространения**. Данные точки распространения обозначены в списках значком  (поле «Тип»).
  - Регистрации, редактирования и удаления внешних точек распространения CRL, Delta CRL и AIA, образующих **пользовательские точки распространения**. Данные точки распространения обозначены в списках значком  (поле «Тип»);
  - Управления режимом публикации CRL, Delta CRL и AIA в LDAP-каталог ресурсных систем (доменные службы каталогов) пользовательских точек распространения.
  - Управления записью точек распространения в выпускаемые сертификаты.
  - Управления приоритетами точек распространения. Приоритет определяет очерёдность записи URL точек распространения в сертификаты субъектов (см. раздел 7.10.9).
  - Объединения точек распространения в кластеры (по типу) для проксирования доступа к ним с целью распределения нагрузки.

- Точки распространения сгруппированы по типу распространяемых данных (CRL, Delta CRL или AIA) и представлены на вкладке «Точки распространения» списками в табличном виде (см. Рисунок 184):
  - Тип – тип точки распространения (автоматическая или пользовательская).
  - Центр валидации – IP-адрес или полное доменное имя компьютера с установленным Центром валидации Aladdin eCA (только для автоматических точек распространения).
  - URL – адрес сервера точки распространения.
  - Приоритет – числовое значение от 0 до 1000.

Точки распространения располагаются в списках в порядке убывания назначенного им приоритета. Если приоритеты точек распространения совпадают, то выше в списке будет располагаться точка, в параметры которой изменения были внесены позднее (в том числе и дата создания).

  - Дата изменения – дата и время последнего редактирования параметров точки распространения (изменение URL и приоритета, а также состава кластера для точки распространения).
  - Публикация – статус последней публикации в точку распространения («Ошибка» или «Успешно»). Если для пользовательской точки распространения не включен режим публикации CRL, Delta CRL или AIA в LDAP-каталоге ресурсной системы (доменной службе каталогов), то точке назначается статус публикации «Выключена».
  - Дата публикации – дату и время последней попытки публикации данных в точку распространения.
  - Переключатель, позволяющий управлять записью точки распространения в выпускаемые сертификаты. При выключенном переключателе запись точек распространения в сертификаты не выполняется.

CRL							
Тип	Центр валида...	URL	Приоритет	Дата изменения	Публикация	Дата публика...	Запись в серти...
—	—	https://aeca/va...	15	07.05.2025 16...	Ошибка	20.05.2025 11:...	<input type="checkbox"/>
🕒	aeva	http://aeva:808...	0	07.05.2025 16...	Ошибка	20.05.2025 11:...	<input checked="" type="checkbox"/>
Delta CRL							
Тип	Центр валида...	URL	Приоритет	Дата изменения	Публикация	Дата публика...	Запись в серти...
—	—	https://aeca/va...	100	07.05.2025 16...	Выключена	—	<input type="checkbox"/>
🕒	aeva	http://aeva:808...	0	07.05.2025 16...	Успешно	20.05.2025 11:...	<input checked="" type="checkbox"/>
AIA							
Тип	Центр валида...	URL	Приоритет	Дата изменения	Публикация	Дата публика...	Запись в серти...
—	—	123123	123	07.05.2025 16...	Выключена	—	<input type="checkbox"/>
🕒	aeva	http://aeva:808...	0	07.05.2025 16...	Успешно	07.05.2025 16...	<input checked="" type="checkbox"/>

Рисунок 184 – Просмотр списков точек распространения

Управление точками распространения включает следующие действия:

- Создание (регистрация) новой точки распространения.
- Редактирование точки распространения.
- Удаление созданной точки распространения.
- Управление записью точек распространения в выпускаемые сертификаты.



- Объединение точек распространения в кластер.

#### 7.10.5.1 Создание пользовательской точки распространения

Пользовательские точки предназначены для распространения:

- Списка отзыва сертификатов (CRL).
- Разностного списка отзыва сертификатов (Delta CRL).
- Сертификатов издающих центров сертификации (AIA).

В Центре сертификации Aladdin eCA для пользовательских точек распространения реализована возможность публикации распространяемых данных в LDAP-каталоги ресурсных систем (доменных служб каталогов): Samba DC, Альт Домен, ALD PRO, MS AD, FreeIPA, РЕД АДМ. При включении режима публикации для точки распространения необходимо указать реквизиты подключения к LDAP-каталогу:

- IP-адрес или полное доменное имя контроллера домена.
- Имя и пароль учетной записи администратора домена.

Для доменов Samba DC, Альт Домен, РЕД АДМ и MS AD имя учетной записи указывается в формате RFC822Name, для ALD PRO и FreeIPA – в формате Distinguished Names.

**Внимание! Успешная публикация в ALD PRO или FreeIPA возможна только при наличии у администратора домена ролей «Service Role» и «Enrollment Administrator». Успешная публикация в Samba DC, РЕД АДМ, Альт Домен или MS AD возможна только при наличии у администратора домена ролей «Domain Users» и «Cert Publishers».**

- URL – путь к объекту в LDAP-каталоге для публикации распространяемых данных.

Пример URL для точки распространения CRL:

```
ldap:///CN=SUB_CA_INFORM,CN=SUB_CA_INFORM,CN=CDP,CN=Public Key Services,CN=Services,
CN=Configuration,DC=<1 компонент доменного имени>,...,DC=<последний компонент доменного имени>?certificateRevocationList?base?objectClass=cRLDistributionPoint
```

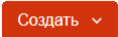
Пример URL для точки распространения Delta CRL:

```
ldap:///CN=SUB_CA_INFORM,CN=SUB_CA_INFORM,CN=CDP,CN=Public Key Services,CN=Services,
CN=Configuration,DC=<1 компонент доменного имени>,...,DC=<последний компонент доменного имени>?deltaRevocationList?base?objectClass=cRLDistributionPoint
```

Пример URL для точки распространения сертификатов издающих центров сертификации (AIA):

```
ldap:///CN=SUB_CA_INFORM,CN=AIA,CN=Public Key Services,CN=Services,
CN=Configuration, DC=<1 компонент доменного имени>,...,DC=<последний компонент доменного имени>?cACertificate?base?objectClass=certificationAuthority
```

Порядок создания пользовательской точки распространения:

- Перейдите на вкладку «Точки распространения» раздела «Центры валидации».
- Нажмите кнопку  и выберите в списке «Пользовательская».
- В открывшемся окне (см. Рисунок 185) выполните следующие действия:
  - В списке «Тип распространяемых данных» выберите тип распространяемых данных (CRL, DELTA, AIA).
  - Чтобы включить режим публикации распространяемых данных в LDAP-каталог ресурсной системы (доменной службы каталогов), установите флажок:
    - <Публиковать CRL в точку распространения> - при создании точки распространения CRL.
    - <Публиковать Delta CRL в точку распространения> - при создании точки распространения Delta CRL.

- <Публиковать AIA в точку распространения> - при создании точки распространения сертификатов издающих центров сертификации.

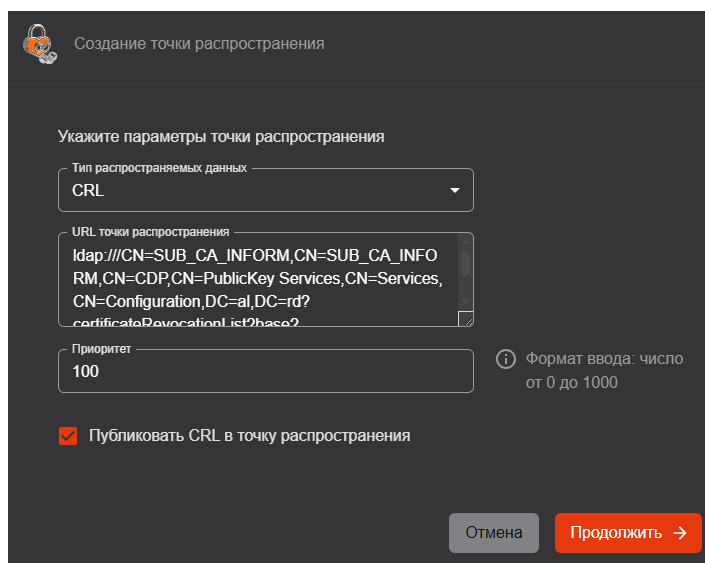


Рисунок 185 – Создание точки распространения

- в поле «URL» укажите URL точки распространения.  
При указании URL возможны следующие сообщения об ошибках:
  - «Указан URL существующей точки распространения» - введенный URL совпадает с URL ранее зарегистрированной точки распространения (любого типа).
  - «Некорректный ввод» - введенный URL содержит один или несколько пробелов.

Если вы создаете точку распространения с возможностью публикации распространяемых данных в LDAP-каталог ресурсной системы, укажите в поле «URL» путь к объекту в LDAP-каталоге для публикации распространяемых данных.

- В поле «Приоритет» укажите приоритет точки распространения (числовое значение от 0 до 1000).  
Точки распространения располагаются в списке в порядке убывания назначенного им приоритета. Если приоритеты точек распространения совпадают, то выше в списке будет располагаться точка, в параметры которой изменения были внесены позднее, начиная с момента ее создания.
- Если вы создаете точку распространения без возможности публикации распространяемых данных, нажмите кнопку <Создать>. В результате будет создана пользовательская точка распространения.
- Если вы создаете точку распространения с возможностью публикации распространяемых данных, нажмите кнопку <Продолжить>.
- В открывшемся окне (см. Рисунок 186) выполните следующие действия:
  - В списке «Тип домена» выберите тип доменной службы каталогов ресурсной системы (Samba DC, Альт Домен, ALD PRO, MS AD, FreeIPA, РЕД АДМ).
  - В поле «Адрес хоста» укажите IP-адрес или полное доменное имя контроллера домена.
  - В полях «Логин» и «Пароль» укажите соответственно имя и пароль учетной записи администратора контроллера домена.
  - Чтобы установить TLS-соединение с контроллером домена для распространения данных, установите флажок «Использовать TLS для подключения». По умолчанию использование протокола TLS для соединения с контроллером домена включено.
  - Нажмите кнопку <Создать>.

Создание точки распространения

Укажите параметры публикации

Протокол

LDAP

URL публикации

ldap:///CN=SUB\_CA\_INFORM,CN=SUB\_CA\_INFORM,CN=CDP,CN=PublicKey Services,CN=Services,CN=Configuration,DC=al,DC=rd?certificateRevocationList?base?objectClass=CRLDistributionPoint

Тип домена

MS AD

Адрес хоста

192.168.23.131

Логин

admindc@al.rd

Пароль

.....

☒

Использовать TLS для подключения

← Назад

Отмена

Создать

Рисунок 186 – Указание параметров публикации для точки распространения

7.10.5.2 Редактирование пользовательской точки распространения

Порядок редактирования пользовательской точки распространения:

- Перейдите на вкладку «Точки распространения» раздела «Центры валидации».
- Наведите указателем мыши на выбранную службу в списке и нажмите кнопку <Редактировать> (см. Рисунок 187).

Центр сертификации Aladdin eCA

Root-CA2

CA-1

INITIAL\_ADMIN

Автообновление CRL

Обновить CRL

Центры валидации

Точки распространения

Службы OCSP

Создать

▼

CRL

Тип	Центр валида...	URL	Приоритет	Дата изменения	Публикация	Дата публика...	Запись в серти...
	—	https://aeca/va...	15	07.05.2025 16...	Ошибка	20.05.2025 11:...	
	aeca	http://aeca:808...	0	07.05.2025 16...	Ошибка	20.05.2025 11:...	

Рисунок 187 – Инициализация процесса редактирования пользовательской точки распространения

- В открывшемся окне (см. Рисунок 188) выполните следующие действия:
  - При необходимости в соответствующих полях измените URL и приоритет точки распространения (описание и правила заполнения полей см. в разделе 7.10.5.1).
  - Если режим публикации распространяемых данных в LDAP-каталог ресурсной системы выключен, а вы не хотите его включать, то нажмите кнопку <Сохранить изменения> для завершения процесса редактирования.

- Если режим публикации распространяемых данных в LDAP-каталог ресурсной системы включен, а вы хотите его выключить, снимите флажок <Публиковать CRL в точку распространения> (при редактировании точки распространения CRL), <Публиковать Delta CRL в точку распространения> (при редактировании точки распространения Delta CRL), <Публиковать AIA в точку распространения> (при редактировании точки распространения сертификатов издающих центров сертификации) и нажмите кнопку <Сохранить изменения> для завершения процесса редактирования.
- Если режим публикации распространяемых данных в LDAP-каталог ресурсной системы включен, а вы не хотите его выключать, то нажмите кнопку <Продолжить> для изменения параметров публикации точки распространения.
- Если режим публикации распространяемых данных в LDAP-каталог ресурсной системы выключен, а вы хотите его включить, установите флажок <Публиковать CRL в точку распространения> (при редактировании точки распространения CRL), <Публиковать Delta CRL в точку распространения> (при редактировании точки распространения Delta CRL), <Публиковать AIA в точку распространения> (при редактировании точки распространения сертификатов издающих центров сертификации) и нажмите кнопку <Продолжить> для указания параметров публикации точки распространения.

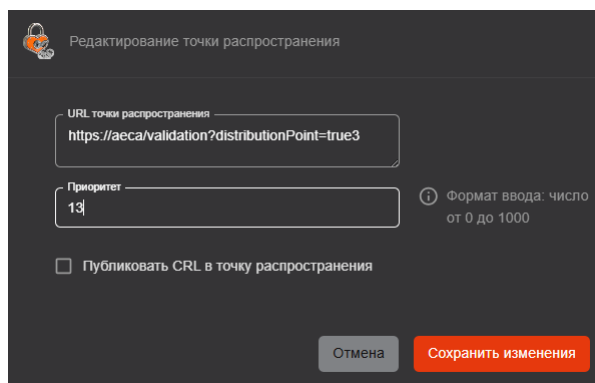


Рисунок 188 – Редактирование пользовательской точки распространения

- В открывшемся окне (см. Рисунок 189) выберите тип доменной службы, укажите адрес контроллера домена, имя и пароль учетной записи администратора контроллера домена (описание и правила заполнения полей см. в разделе 7.10.5.1) и нажмите кнопку <Сохранить изменения>.

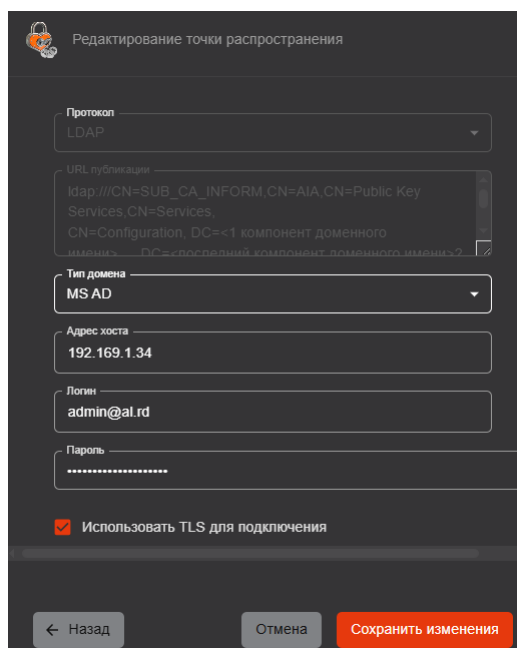



Рисунок 189 – Редактирование параметров публикации пользовательской точки распространения

7.10.5.3 Редактирование автоматической точки распространения

Для редактирования параметров автоматической точки распространения выполните следующие действия:

- Перейдите на вкладку «Точки распространения» раздела «Центры валидации».
- Наведите указателем мыши на выбранную автоматическую точку распространения в списке и нажмите кнопку  «Редактировать» (см. Рисунок 187).
- В открывшемся окне (см. Рисунок 190) в соответствующем поле измените приоритет автоматической точки распространения (описание и правила заполнения полей см. в разделе в разделе 7.10.5.1). После этого нажмите кнопку «Продолжить».

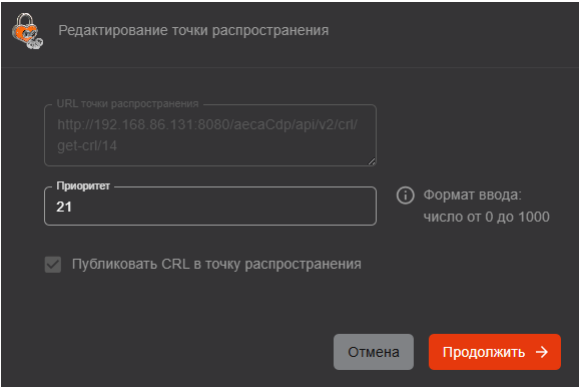


Рисунок 190 – Редактирование автоматической точки распространения

- В открывшемся окне (см. Рисунок 191) нажмите кнопку «Сохранить изменения».

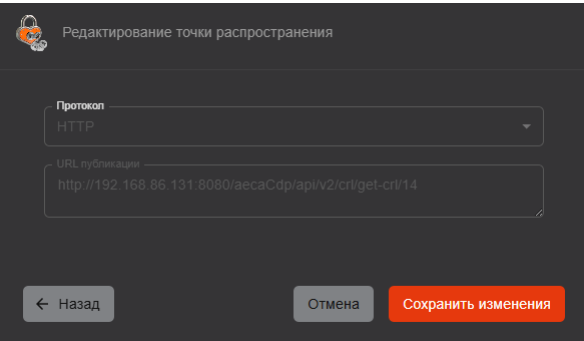



Рисунок 191 – Редактирование автоматической точки распространения

7.10.5.4 Удаление пользовательской точки распространения

Для удаления пользовательской точки распространения выполните следующие действия:

- Перейдите на вкладку «Точки распространения» раздела «Центры валидации».
- Наведите указателем мыши на выбранную автоматическую точку распространения в списке и нажмите кнопку  «Удалить» (см. Рисунок 192).

CRL






▼	Тип	Центр валид...	URL	Приоритет	Дата изменен...	Публикация	Дата публика...	Запись в серти...	
		—	https://aeca/v...	15	07.05.2025 1...	Ошибка	20.05.2025 1...	<input type="checkbox"/>	  
		aeva	http://aeva:80...	0	07.05.2025 1...	Ошибка	20.05.2025 1...	<input checked="" type="checkbox"/>	<div>Удалить</div>

Рисунок 192 –Инициализация процесса удаления точки распространения

- В открывшемся окне (см. Рисунок 193) подтвердите удаление точки распространения, нажав кнопку <Удалить>.

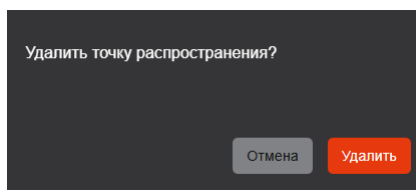


Рисунок 193 – Подтверждение удаления пользовательской точки распространения

#### 7.10.5.5 Создание кластера точек распространения

Объединения точек распространения в кластеры может потребоваться для проксирования доступа к ним с целью распределения нагрузки.

Кластер может быть организован только из точек распространения одного типа (CRL, DeltaCRL или AIA). Кластер может быть организован как из автоматических, так и из пользовательских точек распространения.

Создание кластера возможно двумя способами:

- Путем создания нового кластера и добавления в него уже существующих точек распространения.
- Путем создания кластера на базе ранее созданной точки распространения.

Порядок создания нового кластера и добавления в него ранее зарегистрированных точек распространения:

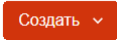
- Перейдите на вкладку «Точки распространения» раздела «Центры валидации».
  - Нажмите кнопку  и выберите в списке «Кластер».
  - В открывшемся окне (см. Рисунок 194) выполните следующие действия:
    - В списке «Тип» выберите тип объединяемых в кластер точек распространения:
      - CRL – для распространения списка отозванных сертификатов.
      - Delta CRL – для распространения разностного списка отозванных сертификатов.
      - AIA – для распространения сертификатов издающих центров сертификации.
    - В поле «URL» укажите URL балансировщика нагрузки. При указании URL возможны следующие сообщения об ошибках:
      - «Указан URL существующей точки распространения» - введенный URL совпадает с URL ранее зарегистрированной точки распространения.
      - «Некорректный ввод» - введенный URL содержит один и несколько пробелов.
    - В поле «Приоритет» укажите приоритет кластера (числовое значение от 0 до 1000).
- Кластеры и точки распространения располагаются в списках в порядке убывания назначенного им приоритета. Если приоритеты кластеров и/или точек распространения совпадают, то выше в списке будет располагаться кластер и/или точка, в параметры которых изменения были внесены позднее (в том числе и дата создания).
- Нажмите кнопку <Продолжить>.

Рисунок 194 – Создание кластера точек распространения. Шаг 1

- В открывшемся окне (см. Рисунок 195) выполните следующие действия:
  - В списке «Выбрать» с помощью флажков выберите URL точек распространения, которые необходимо объединить в кластер, и щелкните значок ➔. В результате выбранные точки распространения будут перемещены в список «Выбрано».
  - Чтобы изменить список точек распространения, объединяемых в кластер, в списке «Выбрано» с помощью флажков выберите URL точек распространения, исключаемых из кластера, и щелкните значок ⬅. В результате выбранные точки распространения будут перемещены в список «Выбрать».
  - Чтобы найти точки распространения в списках, используйте поля поиска.
  - Нажмите кнопку <Создать кластер>.

Рисунок 195 – Создание кластера точек распространения. Шаг 2

В результате будет создан кластер точек распространения в соответствии с назначенным приоритетом. Порядок создания кластера на основе существующей пользовательской точки распространения:

- Перейдите на вкладку «Точки распространения» раздела «Центры валидации».
- Выделите выбранную пользовательскую точку распространения в списке и нажмите кнопку <Создать кластер> (см. Рисунок 196).

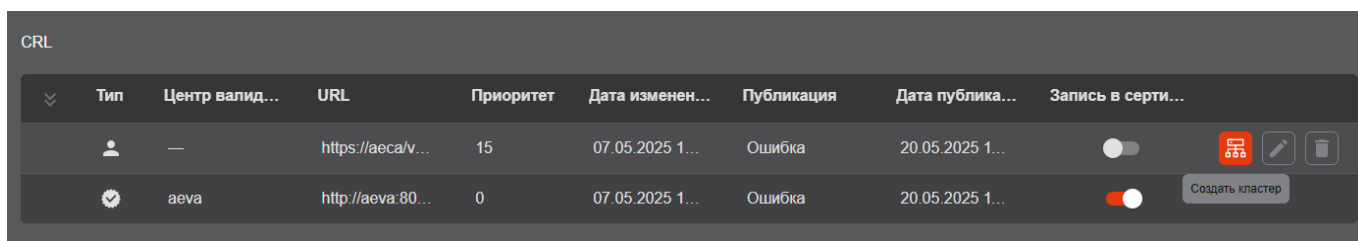


Рисунок 196 – Создание кластера на основе зарегистрированной точки распространения

- В открывшемся окне (см. Рисунок 195) выполните следующие действия:
  - В списке «Выбрать» с помощью флажков выберите URL точек распространения, которые необходимо объединить в кластер, и щелкните значок . В результате выбранные точки распространения будут перемещены в список «Выбрано».
  - Чтобы изменить список точек распространения, объединяемых в кластер, в списке «Выбрано» с помощью флажков выберите URL точек распространения, исключаемых из кластера, и щелкните значок .
  - Чтобы найти точки распространения в списках, используйте поля поиска.
  - Нажмите кнопку «Создать кластер».

В результате будет создан кластер с URL и приоритетом пользовательской точки распространения, на основе которой он был создан.

#### 7.10.5.6 Просмотр состава кластера точек распространения

Для просмотра точек распространения, объединённых в кластер, выполните следующие действия:

- Перейдите на вкладку «Точки распространения» раздела «Центры валидации».
- Раскройте состав кластер в списке. Для этого в строке выбранного кластера щелкните значок (см Рисунок 197).

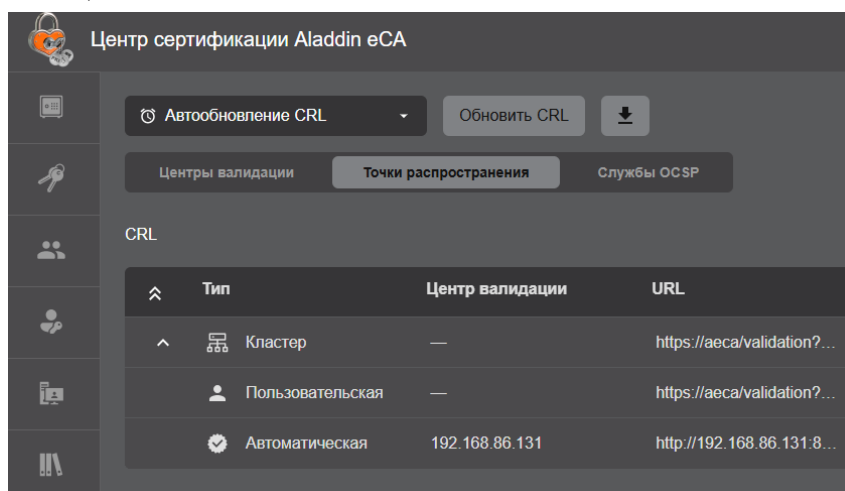


Рисунок 197 –Просмотр состава кластера точек распространения


- Чтобы скрыть состав кластера, щелкните значок .

#### 7.10.5.7 Редактирование кластера точек распространения

Для редактирования состава кластера точек распространения выполните следующие действия:

- Перейдите на вкладку «Точки распространения» раздела «Центры валидации».



- Наведите указателем мыши на выбранный кластер в списке и нажмите кнопку  «Редактировать кластер» (см. Рисунок 198).

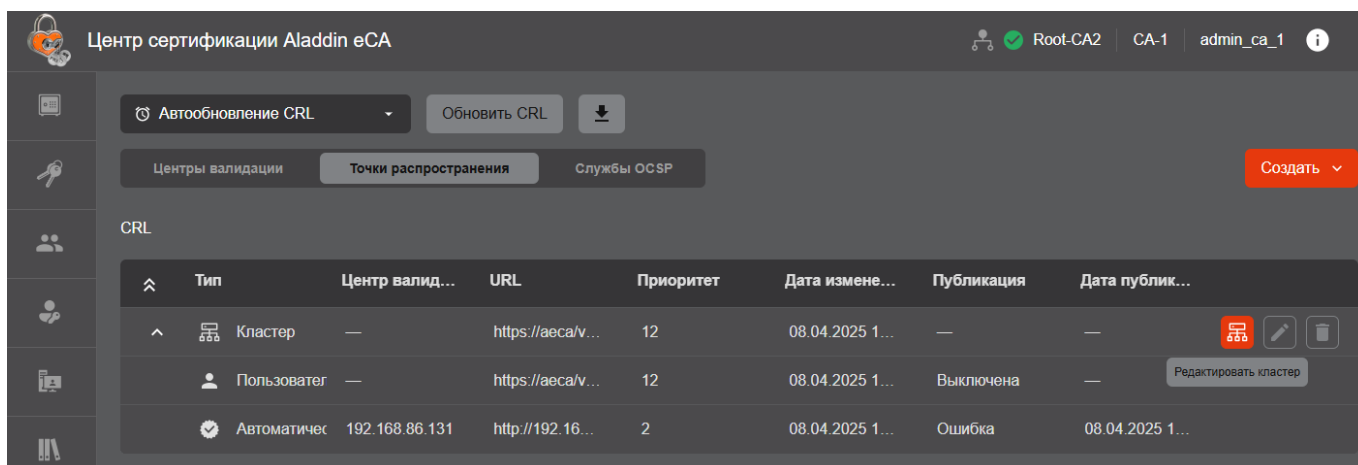




Рисунок 198 – Инициализация процесса редактирования кластера

- В открывшемся окне управления кластером (см. Рисунок 199) измените состав кластера и нажмите кнопку «Сохранить изменения».

В списке «Выбрать» с помощью флажков выберите URL точек распространения, которые необходимо добавить в кластер, и щелкните значок . В результате выбранные точки распространения будут перемещены в список «Выбрано». Чтобы исключить точки распространения из кластера, выберите в списке «Выбрано» с помощью флажков URL точек распространения и щелкните значок . Чтобы найти точки распространения в списках, используйте поля поиска.

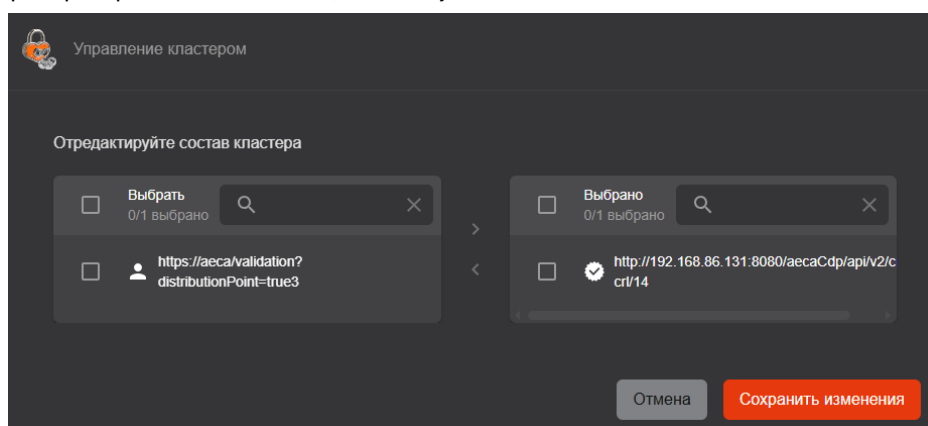



Рисунок 199 – Редактирование состава кластера

Для редактирования параметров кластера выполните следующие действия:

- Перейдите на вкладку «Точки распространения» раздела «Центры валидации».
- Наведите указателем мыши на выбранный кластер в списке и нажмите кнопку  «Редактировать» (см. Рисунок 200).

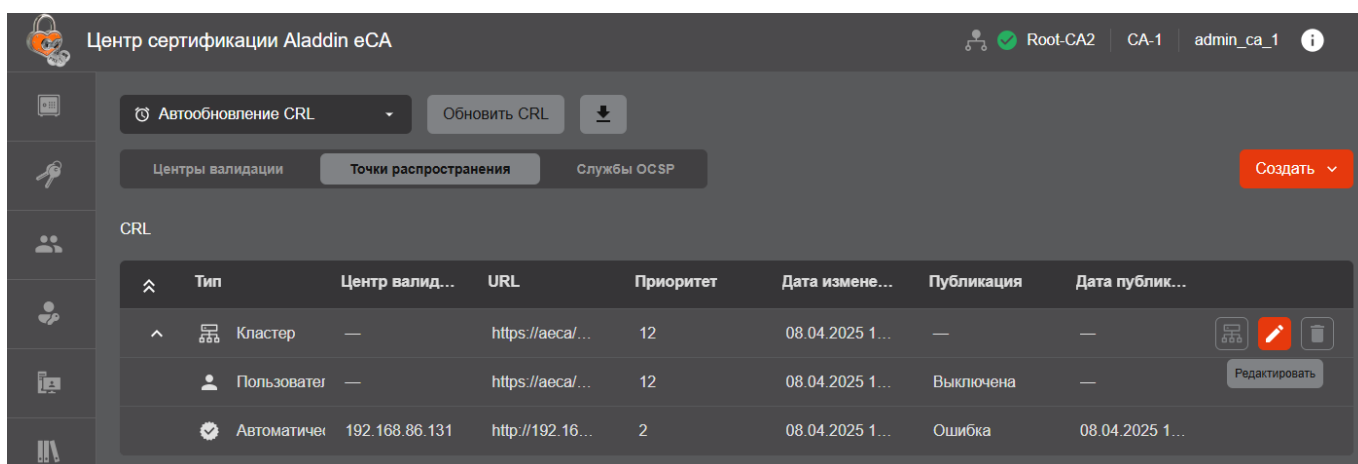


Рисунок 200 – Инициализация процесса редактирования параметров кластера

- В открывшемся окне (см. Рисунок 201) в соответствующих полях измените URL, приоритет кластера точек распространения и нажмите кнопку <Сохранить изменения> (описание и правила заполнения полей см. в разделе 0).

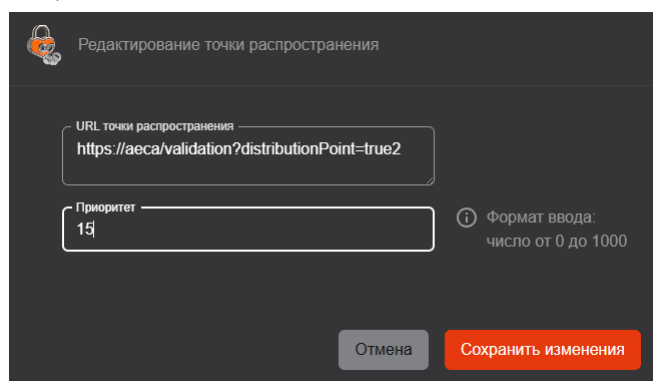



Рисунок 201 – Редактирования кластера точек распространения

#### 7.10.5.8 Удаление кластера точек распространения

Для удаления кластера точек распространения выполните следующие действия:

- Перейдите на вкладку «Точки распространения» раздела «Центры валидации».
- Наведите указателем мыши на выбранный кластер в списке и нажмите кнопку  <Удалить> (см. Рисунок 202).

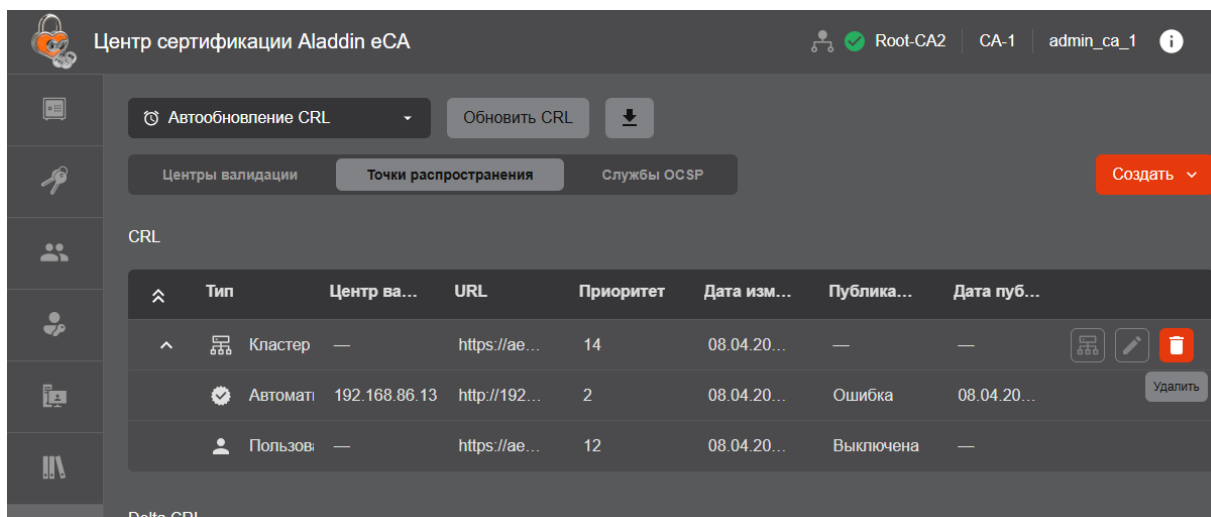


Рисунок 202 – Инициализация процесса удаления кластера

- В открывшемся окне (см. Рисунок 203) подтвердите удаление, нажав кнопку <Удалить>.

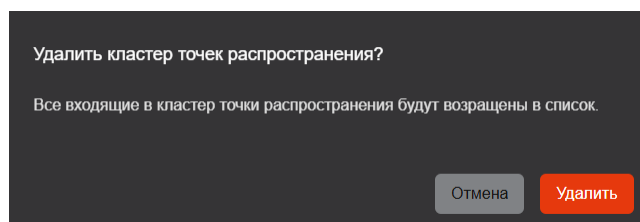




Рисунок 203 – Подтверждение удаления кластера

В результате кластер точек распространения будет удален. При этом точки распространения, входившие в кластер, будут исключены из него и доступны в списке точек распространения.

#### 7.10.6 Управление службами OCSP

Вкладка «Службы OCSP» раздела «Центры валидации» предназначена для:

- Просмотра URL служб OCSP, зарегистрированных Центров валидации Aladdin eCA, образующих **автоматические службы**. Данные службы обозначены в списке значком  (поле «Тип»).
- Регистрации сторонних служб OCSP, существующих или развертываемых на серверах в информационной системе, образующих **пользовательские службы**. Данные службы обозначены в списке значком  (поле «Тип»).
- Управления приоритетом служб OCSP. Приоритет определяет очередность записи URL служб OCSP в сертификаты субъектов (см. раздел 7.10.9).
- Управления записью служб OCSP в выпускаемые сертификаты. Объединение служб OCSP в кластеры для проксирования доступа к ним с целью распределения нагрузки.

Информация о службах OSCP представлена на вкладке «Службы OSCP» раздела «Центры валидации» (см.

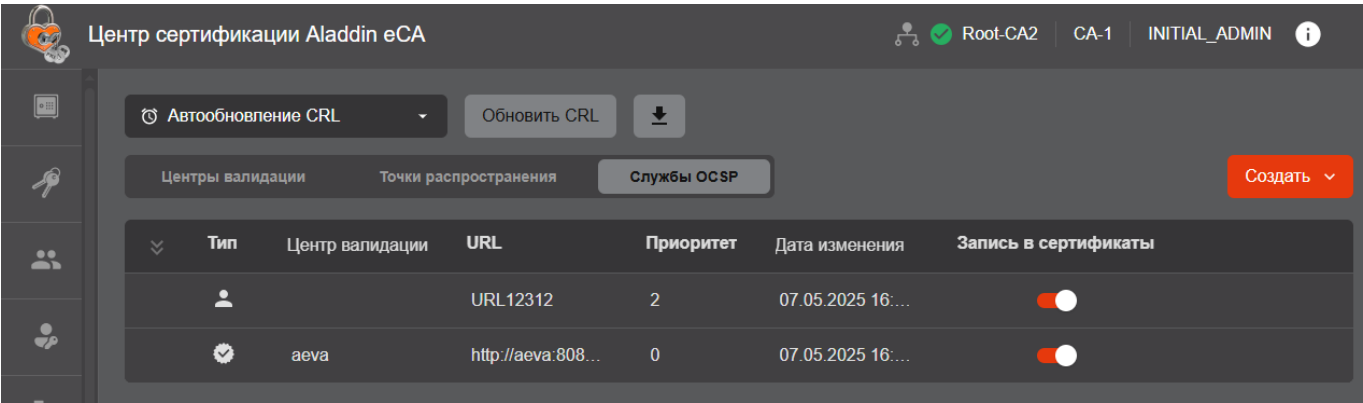


Рисунок 204) список в табличном виде:

- Тип – типа службы OSCP. (пользовательская или автоматическая).
- Центр валидации – IP-адрес или полное доменное имя компьютера с установленным Центром валидации Aladdin eCA (только для автоматических служб).
- URL – адрес сервера службы OSCP.
- Приоритет – числовое значение от 0 до 1000. Службы OSCP располагаются в списке в порядке убывания назначенного им приоритета. Если приоритеты служб OSCP совпадают, то выше в списке будет располагаться служба, в параметры которой изменения были внесены позднее, начиная с даты и времени ее создания.
- Дата изменения – дата и время последнего редактирования параметров службы OSCP (изменение URL и приоритета).
- Переключатель, позволяющий управлять записью служб OSCP в выпускаемые сертификаты. При выключенном переключателе запись служб OSCP в сертификаты не выполняется.

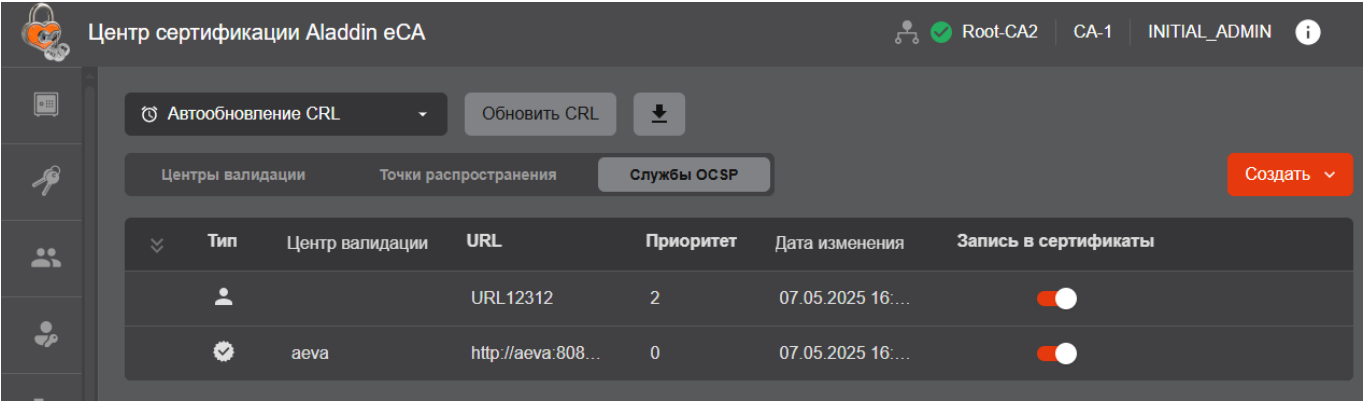


Рисунок 204 –Список зарегистрированных служб OSCP

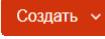
Управление службами OSCP включает следующие операции:

- Создание (регистрация) пользовательских служб OSCP.
- Редактирование пользовательских и автоматических служб OSCP.
- Удаление пользовательских служб OSCP.
- Объединение пользовательских и автоматических служб OSCP в кластеры.

7.10.6.1 Создание пользовательской службы OSCP

Порядок создания пользовательской службы OSCP:

- Перейдите на вкладку «Службы OCSP» раздела «Центры валидации».

Нажмите кнопку  и выберите в списке «Пользовательская» (см.

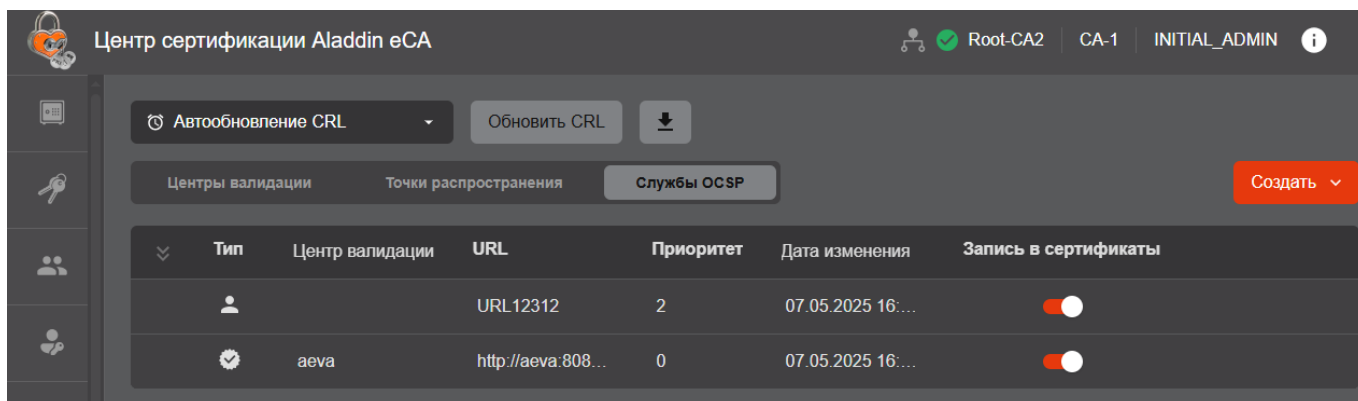


Рисунок 204).

- В открывшемся окне (см. Рисунок 205) выполните следующие действия:
  - В поле «URL» укажите URL службы OCSP.  
При указании URL возможны следующие сообщения об ошибках:
    - «Указан URL существующей службы OCSP» - введенный URL совпадает с URL ранее зарегистрированной службы OCSP.
    - «Некорректный ввод» - введенный URL содержит один и несколько пробелов.
  - В поле «Приоритет» укажите приоритет службы OCSP (числовое значение от 0 до 1000).  
Службы OCSP располагаются в списке в порядке убывания назначенного им приоритета. Если приоритеты служб OCSP совпадают, то выше в списке будет располагаться служба OCSP, в параметры которой изменения были внесены позднее, начиная с момента ее создания.

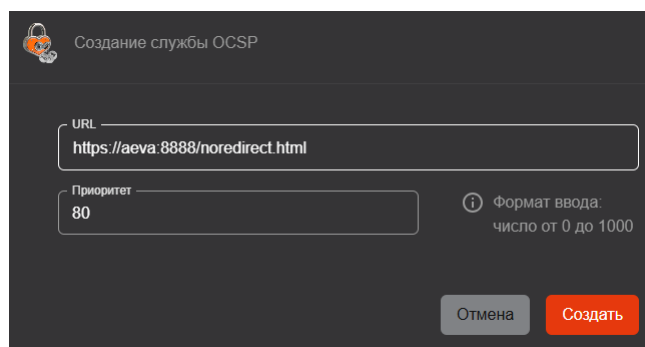



Рисунок 205 – Создание службы OCSP

- Нажмите кнопку «Создать».

В результате будет создана пользовательская служба OCSP.

#### 7.10.6.2 Редактирование пользовательской службы OCSP

Для редактирования параметров пользовательской службы OCSP выполните следующие действия:

- Перейдите на вкладку «Службы OCSP» раздела «Центры валидации».
- Наведите указателем мыши на выбранную службу в списке и нажмите кнопку  «Редактировать» (см. Рисунок 206).

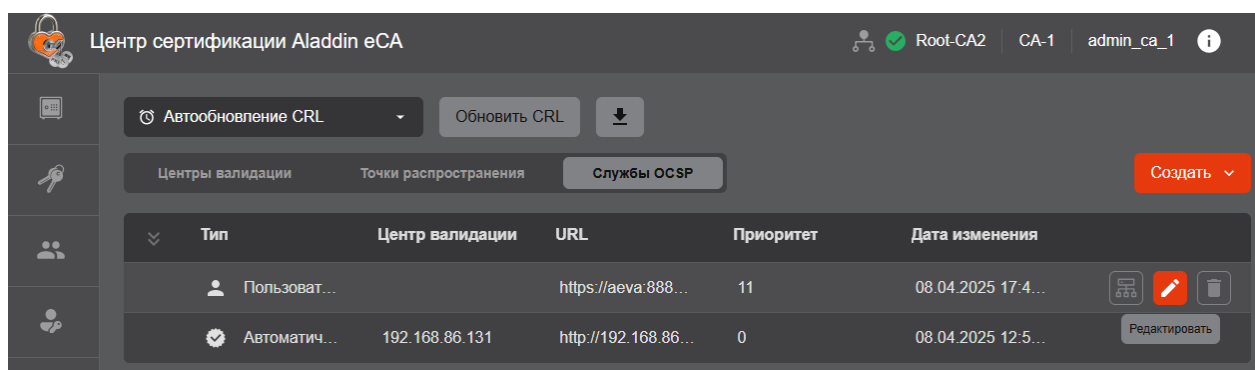


Рисунок 206 – Инициализация процесса редактирования службы OCSP

- В открывшемся окне (см. Рисунок 207) в соответствующих полях измените URL и приоритет службы OCSP (описание и правила заполнения полей см. в разделе 7.10.6.1). После этого нажмите кнопку <Сохранить изменения>.

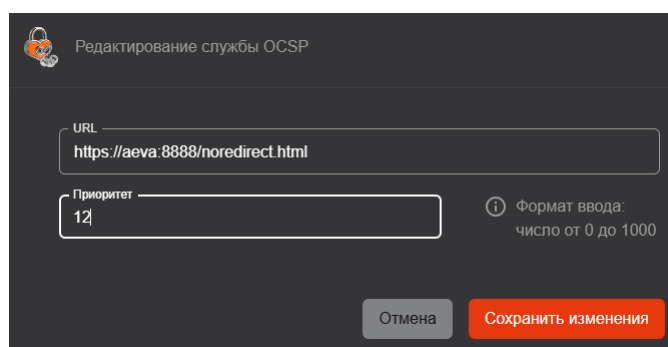



Рисунок 207 – Редактирования пользовательской службы OCSP

### 7.10.6.3 Редактирование автоматической службы OCSP

Для редактирования параметров автоматической службы OCSP выполните следующие действия:

- Перейдите на вкладку «Службы OCSP» раздела «Центры валидации».
- Наведите указателем мыши на выбранную автоматическую службу в списке и нажмите кнопку  «Редактировать» (см. Рисунок 206).
- В открывшемся окне (см. Рисунок 208) в соответствующем поле измените приоритет автоматической службы OCSP (описание и правила заполнения полей см. в разделе 7.10.6.1). После этого нажмите кнопку <Сохранить изменения>.

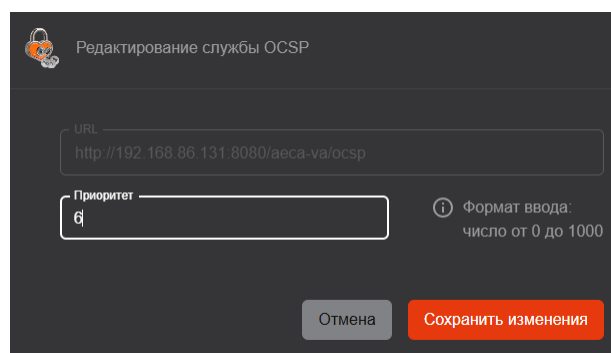



Рисунок 208 – Окно редактирования автоматической службы OCSP

### 7.10.6.4 Удаление пользовательской службы OCSP

Для удаления пользовательской службы OCSP выполните следующие действия:

- Перейдите на вкладку «Службы OCSP» раздела «Центры валидации».

- Наведите указателем мыши на выбранную службу в списке и нажмите кнопку  <Удалить> (см. Рисунок 209).

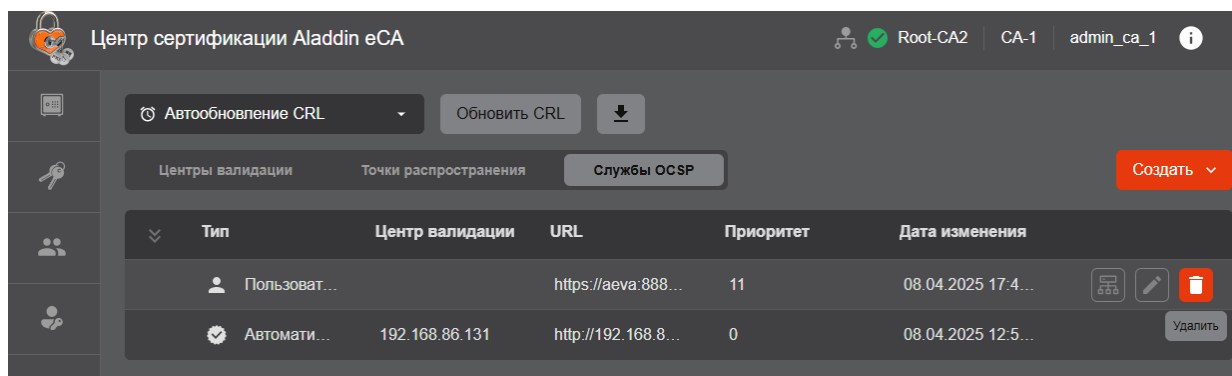


Рисунок 209 – Инициализация процесса удаления службы OCSP

- В открывшемся окне (см. Рисунок 210) подтвердите удаление службы, нажав кнопку <Удалить>.

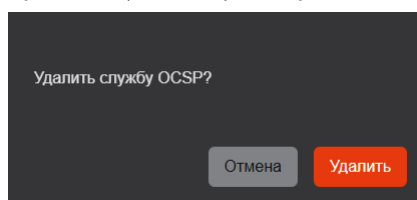


Рисунок 210 – Подтверждение удаления пользовательской службы OCSP

#### 7.10.6.5 Создание кластера служб OCSP

Объединения служб OCSP в кластеры может потребоваться для проксирования доступа к ним с целью распределения нагрузки. Кластер может быть организован как из автоматических, так и из пользовательских служб OCSP.

Создание кластера возможно двумя способами:

- Путем создания нового кластера и добавления в него уже существующих служб OCSP.
- Путем создания кластера на базе ранее созданной службы OCSP.

Порядок создания нового кластера и добавления в него ранее зарегистрированных служб OCSP:

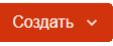

- Перейдите на вкладку «Службы OCSP» раздела «Центры валидации».
- Нажмите кнопку  и выберите в списке «Кластер».
- В открывшемся окне (см. Рисунок 211) выполните следующие действия:
  - В поле «URL» укажите URL балансировщика нагрузки.  
При указании URL возможны следующие сообщения об ошибках:
    - «Указан URL существующей службы OCSP» - введенный URL совпадает с URL существующей (ранее зарегистрированной) точки распространения.
    - «Некорректный ввод» - введенный URL содержит один и несколько пробелов.
  - В поле «Приоритет» укажите приоритет кластера (числовое значение от 0 до 1000).  
Кластеры и службы OCSP располагаются в списках в порядке убывания назначенного им приоритета. Если приоритеты кластеров и/или служб OCSP совпадают, то выше в списке будет располагаться кластер и/или служба, в параметры которых изменения были внесены позднее, начиная с даты создания.
  - Нажмите кнопку <Продолжить>.

Рисунок 211 – Создание кластера служб OCSP. Шаг 1

- В открывшем окне (см. Рисунок 212) выполните следующие действия:
  - В списке «Выбрать» с помощью флажков выберите URL служб OCSP, которые необходимо объединить в кластер, и щелкните значок ➤. В результате выбранные службы будут перемещены в список «Выбрано».
  - Чтобы изменить список служб OCSP, объединяемых в кластер, в списке «Выбрано» с помощью флажков выберите URL служб, исключаемых из кластера, и щелкните значок ◀. В результате выбранные службы будут перемещены в список «Выбрать».
  - Чтобы найти службу в списках, используйте поля поиска.
  - Нажмите кнопку <Создать кластер>.

Рисунок 212 – Создание кластера служб OCSP. Шаг 2

В результате будет создан кластер служб OCSP в соответствии с назначенным приоритетом.  
Порядок создания кластера на базе существующей пользовательской службы OCSP:

- Перейдите на вкладку «Службы OCSP» раздела «Центры валидации».
- Выделите выбранную пользовательскую службу OCSP в списке и нажмите кнопку <Создать кластер>  (см. Рисунок 213).



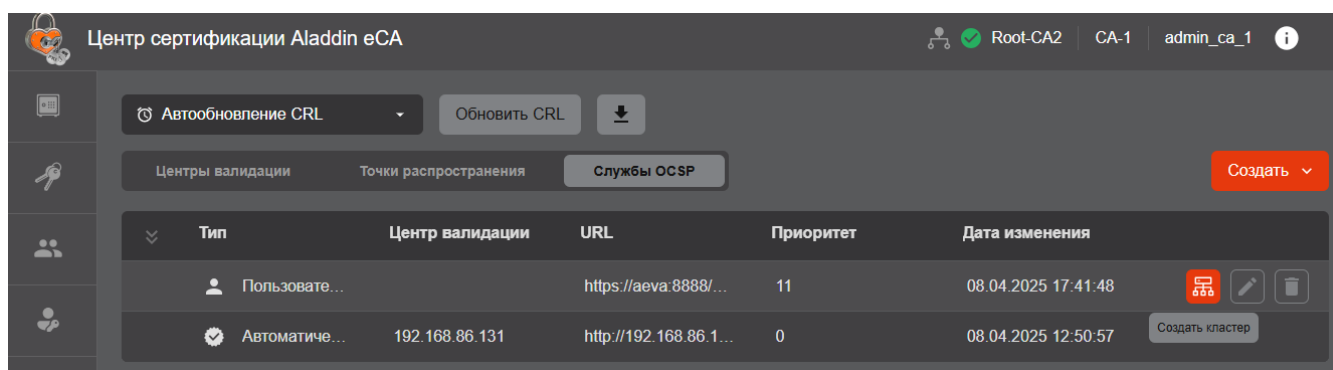


Рисунок 213 – Инициализация процесса создания кластера служб OCSP

- В открывшемся окне создания кластера (см. Рисунок 214) выполните следующие действия:
  - В списке «Выбрать» с помощью флажков выберите URL служб OCSP, которые необходимо объединить в кластер, и щелкните значок ➤. В результате выбранные службы будут перемещены в список «Выбрано».
  - Чтобы изменить список служб OCSP, объединяемых в кластер, в списке «Выбрано» с помощью флажков выберите URL служб, исключаемых из кластера, и щелкните значок ◀.
  - Чтобы найти службу в списках, используйте поля поиска.
  - Нажмите кнопку <Создать кластер>.

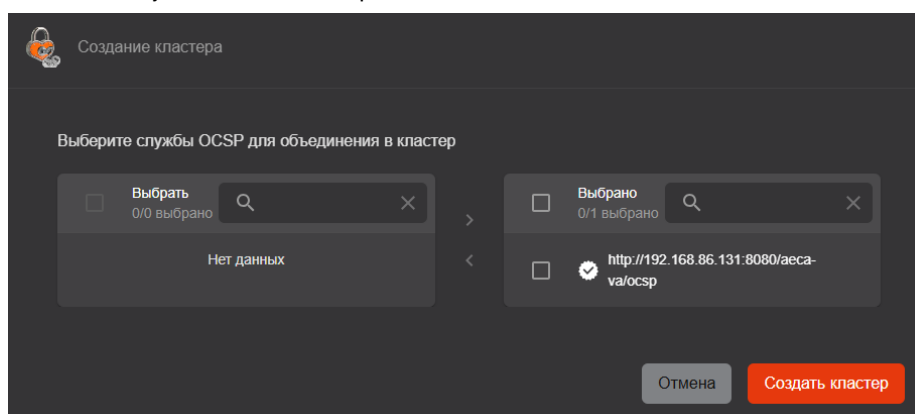


Рисунок 214 – Создание кластера из пользовательской службы OCSP

В результате будет создан кластер с URL и приоритетом пользовательской службы OCSP, на основании которой он был создан.

#### 7.10.6.6 Просмотр состава кластера служб OCSP

Для просмотра служб OCSP, объединённых в кластер, выполните следующие действия:

- Перейдите на вкладку «Службы OCSP» раздела «Центры валидации».
- Раскройте состав кластер в списке. Для этого в строке выбранного кластера щелкните значок ▼ (см. Рисунок 215).

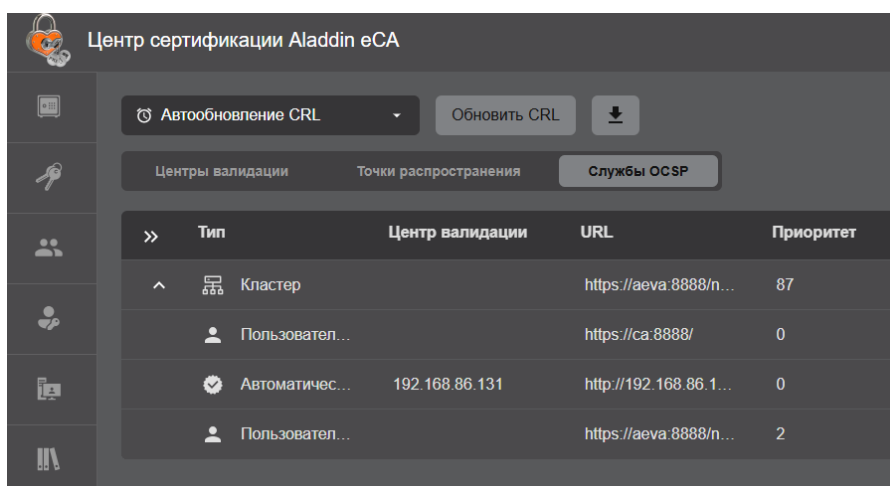


Рисунок 215 – Просмотр состава кластера служб OCSP

- Чтобы скрыть состав кластера, щелкните значок

#### 7.10.6.7 Редактирование кластера служб OCSP

Для редактирования состава кластера служб OCSP выполните следующие действия:

- Перейдите на вкладку «Службы OCSP» раздела «Центры валидации».
- Наведите указателем мыши на выбранный кластер в списке и нажмите кнопку «Редактировать кластер» (см. Рисунок 216).

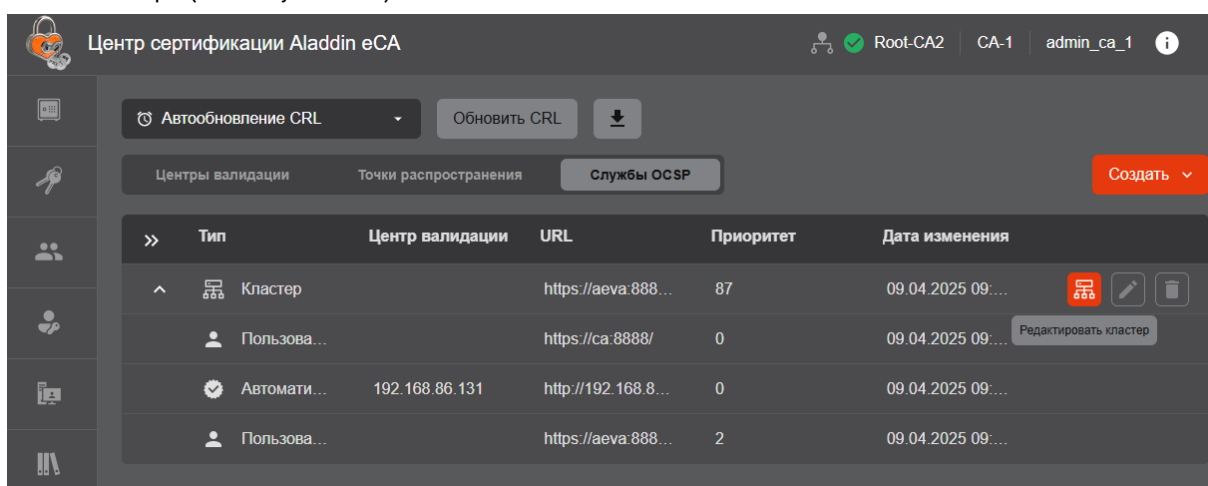


Рисунок 216 – Инициализация процесса редактирования состава кластера

- В открывшем окне управления кластером (см. Рисунок 217) измените состав кластера и нажмите кнопку «Сохранить изменения».
  - Чтобы добавить службы OCSP в кластер, выберите URL служб в списке «Выбрать» с помощью флажков и щелкните значок . В результате выбранные службы будут перемещены в список «Выбрано».
  - Чтобы исключить службы OCSP из кластера, выберите URL служб в списке «Выбрано» с помощью флажков и щелкните значок . В результате выбранные службы будут перемещены в список «Выбрать».
  - Чтобы найти службу в списках, используйте поля поиска.

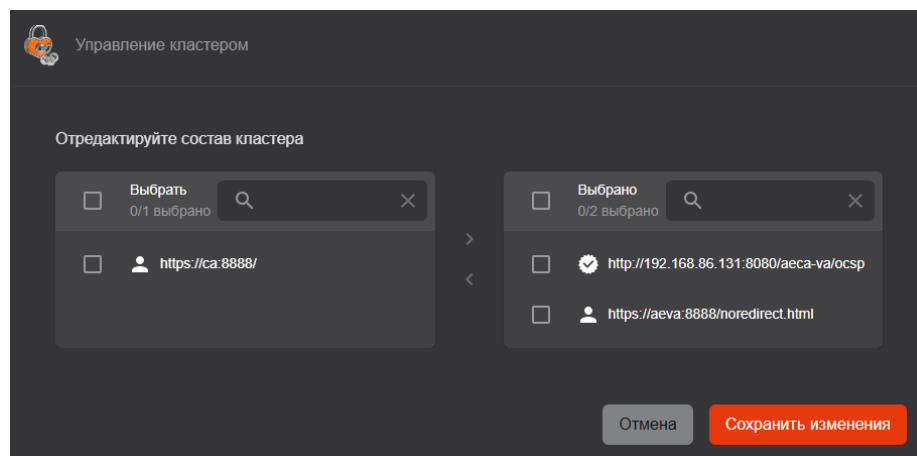



Рисунок 217 – Редактирование состава кластера служб OCSP

Для редактирования параметров кластера служб OCSP выполните следующие действия:

- Перейдите на вкладку «Службы OCSP» раздела «Центры валидации».
- Наведите указателем мыши на выбранный кластер служб OCSP в списке и нажмите кнопку  «Редактировать» (см. Рисунок 218).

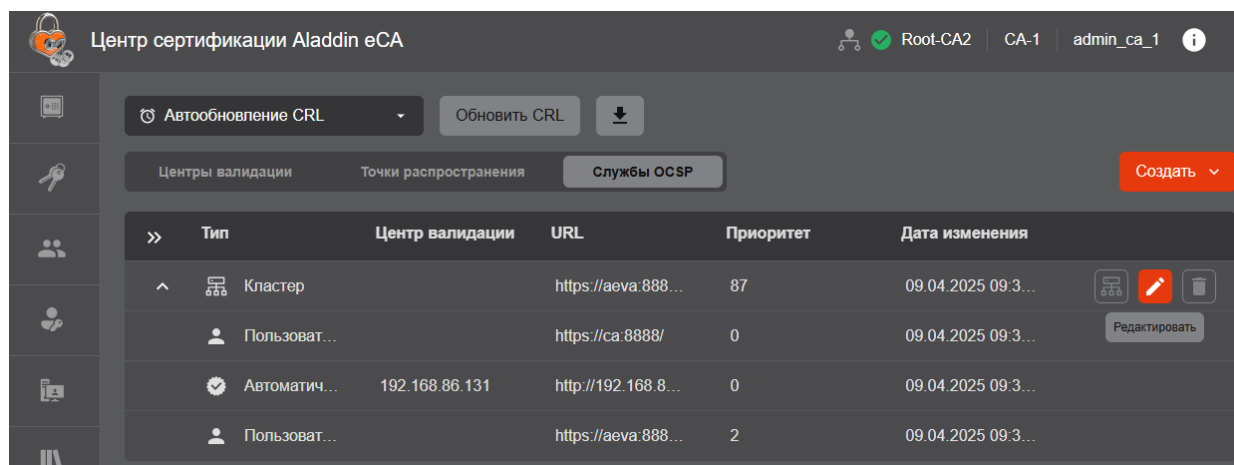


Рисунок 218 – Инициализация процесса редактирования параметров кластера

- В открывшемся окне (см. Рисунок 219) в соответствующих полях измените URL, приоритет кластера служб OCSP и нажмите кнопку «Сохранить изменения» (описание и правила заполнения полей см. в разделе 7.10.6.5).

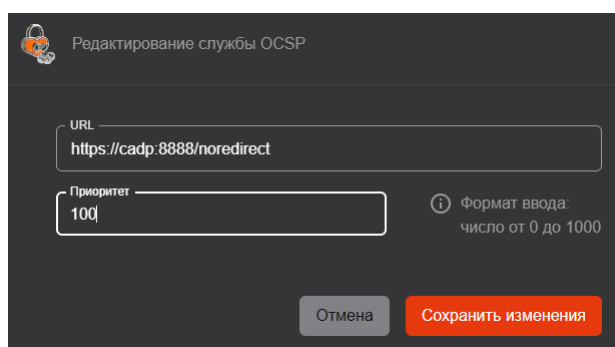



Рисунок 219 – Редактирование параметров кластера службы OCSP

#### 7.10.6.8 Удаление кластера служб OCSP

Для удаления кластера служб OCSP выполните следующие действия:

- Перейдите на вкладку «Службы OCSP» раздела «Центры валидации».

- Наведите указателем мыши на выбранный кластер в списке и нажмите кнопку  <Удалить> (см. Рисунок 220).

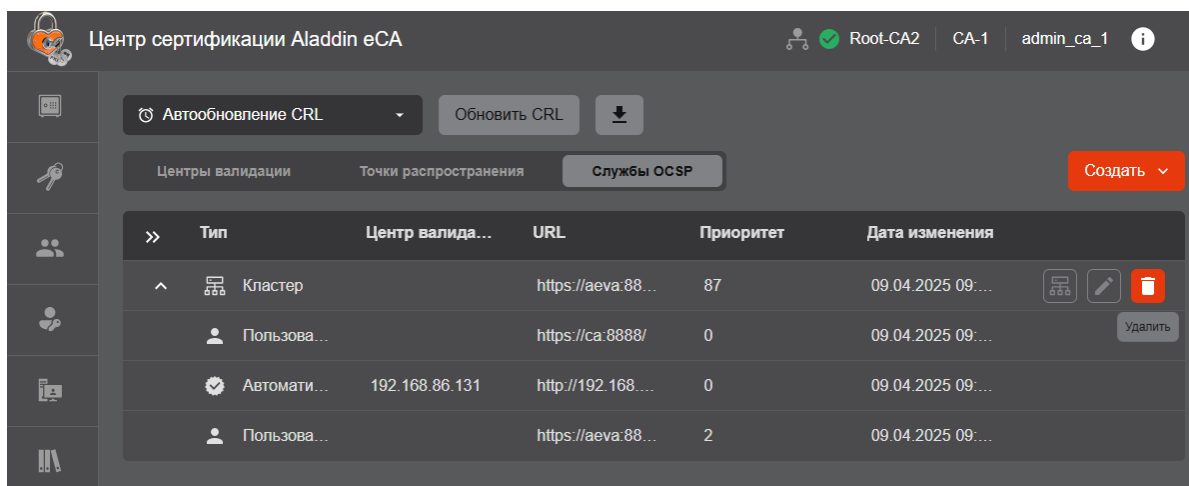


Рисунок 220 – Инициализация процесса удаления кластера служб OSCP

- В открывшемся окне (см. Рисунок 221) подтвердите удаление, нажав кнопку <Удалить>.

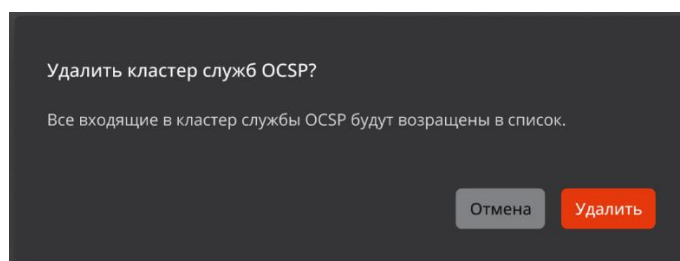


Рисунок 221 – Подтверждение удаления кластера служб OSCP

В результате кластер служб OSCP будет удален. При этом службы, входящие в кластер, будут исключены из него и доступны в списке служб OSCP.

## 7.10.7 Настройка технического решения «Центра валидации»

### 7.10.7.1 Настройка с использованием веб-сервера Nginx

#### Для Astra Linux SE 1.7

Подготовьте сервер, на котором будет размещена пользовательская точка публикации списков отозванных сертификатов, для этого последовательно выполните действия для установки веб-сервера Nginx:

- Установите пакет из официального репозитория ОС (для РЕД ОС) или расширенного репозитория (для Astra Linux SE 1.7), выполнив команду с правами суперпользователя:

```
sudo apt install nginx
```

- Запустите установленный веб-сервер, выполнив команду:

```
systemctl start nginx
```

- Добавьте веб-сервер в автозагрузку, выполнив команду:

```
systemctl enable nginx
```

- Создайте файл конфигурации, выполнив команду:

```
sudo nano /etc/nginx/conf.d/crl-dp.conf
```

Добавьте в созданный конфигурационный файл `/etc/nginx/conf.d/crl-dp.conf` следующее содержимое:

```
server {
    listen 80;
    server_name localhost;

    location /crl-dp/ {
        root /var/www;
        autoindex off;
    }
}
```

где `/var/www/crl-dp` – каталог, в котором будут размещены файлы CRL, Delta CRL и AIA для распространения (скачивания).

- Удалите файлы `/etc/nginx/sites-enabled/default` и `/etc/nginx/sites-available/default` (при их наличии в системе), выполнив команды:

```
sudo rm /etc/nginx/sites-enabled/default
sudo rm /etc/nginx/sites-available/default
```

- Создайте каталог `/var/www/crl-dp`, выполнив команду:

```
sudo mkdir /var/www/crl-dp
```

- Выполните перезапуск веб-сервера Nginx для применения изменений конфигурации, выполнив команду:

```
sudo systemctl restart nginx
```

- Экспортируйте из Центра сертификации, согласно подразделу 7.10.8 настоящего руководства, для распространения следующие файлы:
  - список отозванных сертификатов CRL;
  - список изменений последнего опубликованного CRL – DeltaCRL;
  - сертификаты центров сертификации.
- Разместите в каталоге `/var/www/crl-dp` полученные файлы CRL, Delta CRL и/или AIA.
- Убедитесь, что файлы CRL, Delta CRL или AIA доступны для скачивания. Для этого необходимо на любом другом АРМ, для которого сервер пользовательской точки распространения CRL DP является достижимым, перейти в браузере по ссылке:

```
http://IP/crl-dp/FILENAME
```

где `IP` – IP-адрес сервера пользовательской точки распространения CRL DP, `FILENAME` – имя любого из файлов, добавленных в каталог `/var/www/crl-dp`, например:

```
http://192.168.0.125/crl-dp/SUB_CA.crl
```

### Для ОС РЕД ОС 7.3

Подготовьте сервер, на котором будет размещена пользовательская точка публикации списков отозванных сертификатов, для этого последовательно выполните действия для установки веб-сервера Nginx:

- Установите пакет из официального репозитория ОС (для РЕД ОС) или расширенного репозитория (для Astra Linux SE 1.7), выполнив команду с правами суперпользователя:

```
sudo dnf install nginx
```

- Запустите установленный веб-сервер, выполнив команду:

```
systemctl start nginx
```

- Добавьте веб-сервер в автозагрузку, выполнив команду:

```
systemctl enable nginx
```

- Создайте файл конфигурации, выполнив команду:

```
sudo nano /etc/nginx/conf.d/crl-dp.conf
```

Добавьте в созданный конфигурационный файл `/etc/nginx/conf.d/crl-dp.conf` следующее содержимое:

```
server {
    listen 80;
    server_name localhost;

    location /crl-dp/ {
        root /var/www;
        autoindex off;
    }
}
```

где `/var/www/crl-dp` – каталог, в котором будут размещены файлы CRL, Delta CRL и AIA для распространения (скачивания).

- Удалите файлы `/etc/nginx/sites-enabled/default` и `/etc/nginx/sites-available/default` (при их наличии в системе), выполнив команды:

```
sudo rm /etc/nginx/sites-enabled/default
sudo rm /etc/nginx/sites-available/default
```

- Расширьте политики selinux, выполнив команду:

```
sudo semanage permissive -a httpd_t
```

- Создайте каталог `/var/www/crl-dp`, выполнив команду:

```
sudo mkdir /var/www/crl-dp
```

- Выполните перезапуск веб-сервера Nginx для применения изменений конфигурации, выполнив команду:

```
sudo systemctl restart nginx
```

- Экспортируйте из Центра сертификации, согласно подразделу 7.10.8 настоящего руководства, для распространения следующие файлы:
  - список отозванных сертификатов CRL;
  - список изменений последнего опубликованного CRL – DeltaCRL;

- сертификаты центров сертификации.
- Разместите в каталоге `/var/www/crl-dp` полученные файлы CRL, Delta CRL и/или AIA.
- Убедитесь, что файлы CRL, Delta CRL или AIA доступны для скачивания. Для этого необходимо на любом другом АРМ, для которого сервер пользовательской точки распространения CRL DP является достижимым, перейти в браузере по ссылке:

```
http://IP/crl-dp/FILENAME
```

где `IP` – IP-адрес сервера пользовательской точки распространения CRL DP, `FILENAME` – имя любого из файлов, добавленных в каталог `/var/www/crl-dp`, например:

```
http://192.168.0.125/crl-dp/SUB_CA.crl
```

### Для ОС АЛЬТ 8 СП

Подготовьте сервер, на котором будет размещена пользовательская точка публикации списков отозванных сертификатов, для этого последовательно выполните действия для установки веб-сервера Nginx:

- Установите пакет из официального репозитория ОС, выполнив команду с правами суперпользователя:

```
sudo apt-get install nginx
```

- Запустите установленный веб-сервер, выполнив команду:

```
systemctl start nginx
```

- Добавьте веб-сервер в автозагрузку, выполнив команду:

```
systemctl enable nginx
```

- Создайте файл конфигурации, выполнив команду:

```
sudo nano /etc/nginx/sites-enabled.d/crl-dp.conf
```

Добавьте в созданный конфигурационный файл `/etc/nginx/sites-enabled.d/crl-dp.conf` следующее содержимое:

```
server {
    listen 80;
    server_name localhost;

    location /crl-dp/ {
        root /var/www;
        autoindex off;
    }
}
```

где `/var/www/crl-dp` – каталог, в котором будут размещены файлы CRL, Delta CRL и AIA для распространения (скачивания).

- Удалите файлы `/etc/nginx/sites-enabled.d/default.conf` и `/etc/nginx/sites-available.d/default.conf` (при их наличии в системе), выполнив команды:

```
sudo rm /etc/nginx/sites-enabled.d/default.conf
sudo rm /etc/nginx/sites-available.d/default.conf
```

- Создайте каталог `/var/www/crl-dp`, выполнив команду:

```
sudo mkdir /var/www/crl-dp
```

- Выполните перезапуск веб-сервера Nginx для применения изменений конфигурации, выполнив команду:

```
sudo systemctl restart nginx
```

- Экспортируйте из Центра сертификации, согласно подразделу 7.10.8 настоящего руководства, для распространения следующие файлы:
  - список отозванных сертификатов CRL;
  - список изменений последнего опубликованного CRL – DeltaCRL;
  - сертификаты центров сертификации.
- Разместите в каталоге `/var/www/crl-dp` полученные файлы CRL, Delta CRL и/или AIA.
- Убедитесь, что файлы CRL, Delta CRL или AIA доступны для скачивания. Для этого необходимо на любом другом АРМ, для которого сервер пользовательской точки распространения CRL DP является достижимым, перейти в браузере по ссылке:

```
http://IP/crl-dp/FILENAME
```

где `IP` – IP-адрес сервера пользовательской точки распространения CRL DP, `FILENAME` – имя любого из файлов, добавленных в каталог `/var/www/crl-dp`, например:

```
http://192.168.0.125/crl-dp/SUB_CA.crl
```

### 7.10.7.2 Настройка с использованием веб-сервера Apache

#### Для ОС Astra Linux SE 1.7

Подготовьте сервер, на котором будет размещена пользовательская точка публикации списков отозванных сертификатов, для этого последовательно выполните действия для установки веб-сервера Apache:

- Установите пакет, выполнив команду с правами суперпользователя (от имени пользователя root, либо с использованием sudo):

```
sudo apt install apache2
```

- Активируйте модули, выполнив команды:

```
sudo a2enmod ssl
sudo a2enmod proxy
sudo a2enmod proxy_http
sudo a2enmod headers
sudo a2enmod cgi
sudo a2enmod rewrite
sudo a2enmod http2
```

- Добавьте веб-сервер в автозагрузку, выполнив команду с правами суперпользователя:

```
sudo systemctl enable apache2
```

- Создайте файл конфигурации, выполнив команду:

```
sudo nano /etc/apache2/conf-available/crl-dp.conf
```

Добавьте в созданный конфигурационный файл `/etc/nginx/sites-available/crl-dp` следующее содержимое:



```
<VirtualHost *:80>
    AstraMode off
    ServerName localhost

    Alias /crl-dp/ "/var/www/crl-dp/"
    <Directory "/var/www/crl-dp/">
        Options -Indexes
        AllowOverride None
        Require all granted

        <Files "*">
            Header set Content-Disposition "attachment"
        </Files>
    </Directory>
</VirtualHost>
```

где `/var/www/crl-dp` – каталог, в котором будут размещаться файлы CRL, Delta CRL и AIA для распространения (скачивания).

- Создайте в каталоге `/etc/apache2/conf-enabled` ссылку на созданный конфигурационный файл `/etc/apache2/conf-available/crl-dp.conf`, выполнив команду:

```
sudo ln -s /etc/apache2/conf-available/crl-dp.conf /etc/apache2/conf-enabled/
```

- Активируйте модуль `headers`, выполнив команду:

```
sudo a2enmod headers
```

- Создайте каталог `/var/www/crl-dp`, выполнив команду:

```
sudo mkdir /var/www/crl-dp
```

- Выполните перезапуск веб-сервера Apache для применения изменений конфигурации, выполнив команду:

```
sudo systemctl restart apache2
```

- Экспортируйте из Центра сертификации, согласно подразделу 7.10.8 настоящего руководства, для распространения следующие файлы:
  - список отозванных сертификатов CRL;
  - список изменений последнего опубликованного CRL – DeltaCRL;
  - сертификаты центров сертификации.
- Разместите в каталоге `/var/www/crl-dp` полученные файлы CRL, Delta CRL и/или AIA.
- Убедитесь, что файлы CRL, Delta CRL или AIA доступны для скачивания. Для этого необходимо на любом другом АРМ, для которого сервер пользовательской точки распространения CRL DP является достижимым, перейти в браузере по ссылке:

```
http://IP/crl-dp/FILENAME
```

где `IP` – IP-адрес сервера пользовательской точки распространения CRL DP, `FILENAME` – имя любого из файлов, добавленных в каталог `/var/www/crl-dp`, например:

```
http://192.168.0.125/crl-dp/SUB_CA.crl
```

### Для ОС РЕД ОС 7.3

Подготовьте сервер, на котором будет размещена пользовательская точка публикации списков отозванных сертификатов, для этого последовательно выполните действия для установки веб-сервера Apache:

- Установите пакет, выполнив команду с правами суперпользователя (от имени пользователя root, либо с использованием sudo):

```
sudo dnf install httpd
```

- Установите дополнительный модуль для использования протокола ssl в apache, выполнив команду с правами суперпользователя (от имени пользователя root, либо с использованием sudo):

```
sudo dnf install mod_ssl
```

- Добавьте веб-сервер в автозагрузку, выполнив команду с правами суперпользователя:

```
sudo systemctl enable httpd
```

- Создайте файл конфигурации, выполнив команду:

```
sudo nano /etc/httpd/conf.d/crl-dp.conf
```

Добавьте в созданный конфигурационный файл `/etc/httpd/conf.d/crl-dp.conf` следующее содержимое:

```
<VirtualHost *:80>
    ServerName localhost

    Alias /crl-dp/ "/var/www/crl-dp/"
    <Directory "/var/www/crl-dp/">
        Options -Indexes
        AllowOverride None
        Require all granted

        <Files "*">
            Header set Content-Disposition "attachment"
        </Files>
    </Directory>
</VirtualHost>
```

где `/var/www/crl-dp` – каталог, в котором будут размещаться файлы CRL, Delta CRL и AIA для распространения (скачивания).

- Создайте каталог `/var/www/crl-dp`, выполнив команду:

```
sudo mkdir /var/www/crl-dp
```

- Выполните перезапуск веб-сервера Apache для применения изменений конфигурации, выполнив команду:

```
sudo systemctl restart httpd
```

- Экспортируйте из Центра сертификации, согласно подразделу 7.10.8 настоящего руководства, для распространения следующие файлы:
  - список отозванных сертификатов CRL;
  - список изменений последнего опубликованного CRL – DeltaCRL;
  - сертификаты центров сертификации.
- Разместите в каталоге `/var/www/crl-dp` полученные файлы CRL, Delta CRL и/или AIA.
- Убедитесь, что файлы CRL, Delta CRL или AIA доступны для скачивания. Для этого необходимо на любом другом АРМ, для которого сервер пользовательской точки распространения CRL DP является достижимым, перейти в браузере по ссылке:

```
http://IP/crl-dp/FILENAME
```

где `IP` – IP-адрес сервера пользовательской точки распространения CRL DP, `FILENAME` – имя любого из файлов, добавленных в каталог `/var/www/crl-dp`, например:

```
http://192.168.0.125/crl-dp/SUB_CA.crl
```

### Для ОС АЛЪТ 8 СП

Подготовьте сервер, на котором будет размещена пользовательская точка публикации списков отозванных сертификатов, для этого последовательно выполните действия для установки веб-сервера Apache:

- Установите пакет, выполнив команду с правами суперпользователя (от имени пользователя root, либо с использованием sudo):

```
sudo apt-get install apache2-mod_http2
```

- Установите модуль ssl, выполнив команду с правами суперпользователя (от имени пользователя root, либо с использованием sudo):

```
sudo apt-get install apache2-mod_ssl
```

- Создайте файлы:
  - `/etc/httpd2/conf/mods-available/http2.load`, выполнив команду с правами суперпользователя:

```
sudo cat /etc/httpd2/conf/mods-available/http2.load
```

Внесите следующий текст в созданный файл:

```
LoadModule http2_module /usr/lib64/apache2/modules/mod_http2.so
```

- `/etc/httpd2/conf/mods-available/http2.conf` выполнив команду с правами суперпользователя:

```
sudo cat /etc/httpd2/conf/mods-available/http2.conf
```

Внесите следующий текст в созданный файл:

```
# mod_http2 doesn't work with mpm_prefork
<IfModule !mpm_prefork>
    Protocols h2 h2c http/1.1

    # # HTTP/2 push configuration
    #
    # H2Push          on
    #
    # # Default Priority Rule
```

```
#
# H2PushPriority * After 16
#
# # More complex ruleset:
#
# H2PushPriority * after
# H2PushPriority text/css before
# H2PushPriority image/jpeg after 32
# H2PushPriority image/png after 32
# H2PushPriority application/javascript interleaved
#
# # Configure some stylesheet and script to be pushed by the webserver
#
# <FilesMatch "\.html$">
#     Header add Link "</style.css>; rel=preload; as=style"
#     Header add Link "</script.js>; rel=preload; as=script"
# </FilesMatch>
# Since mod_http2 doesn't support the mod_logio module (which provide the %O
format),
# you may want to change your LogFormat directive as follow:
#
# LogFormat "%v:%p %h %l %u %t \"%r\" %>s %B \"%{Referer}i\" \"%{User-Agent}i\""
vhost_combined
# LogFormat "%h %l %u %t \"%r\" %>s %B \"%{Referer}i\" \"%{User-Agent}i\""
combined
# LogFormat "%h %l %u %t \"%r\" %>s %B" common
</IfModule>
```

- Активируйте модули, выполнив команды:

```
sudo a2enmod ssl
sudo a2enmod proxy
sudo a2enmod proxy_http
sudo a2enmod headers
sudo a2enmod cgi
sudo a2enmod rewrite
sudo a2enmod http2
```

- Включите https порт по умолчанию, выполнив команду с правами суперпользователя:

```
sudo a2enport https
```

- Создайте файл конфигурации, выполнив команду:

```
nano /etc/httpd2/conf/sites-available/crl-dp.conf
```

Добавьте в созданный конфигурационный файл `/etc/httpd2/conf/sites-available/crl-dp.conf` следующее содержимое:

```
<VirtualHost *:80>
    ServerName localhost
```

```
Alias /crl-dp/ "/var/www/crl-dp/"
<Directory "/var/www/crl-dp/">
    Options -Indexes
    AllowOverride None
    Require all granted

    <Files "*">
        Header set Content-Disposition "attachment"
    </Files>
</Directory>
</VirtualHost>
```

где `/var/www/crl-dp` – каталог, в котором будут размещаться файлы CRL, Delta CRL и AIA для распространения (скачивания).

- Создайте в каталоге `/etc/httpd2/conf/sites-enabled` ссылку на созданный конфигурационный файл `/etc/httpd2/conf/sites-available/crl-dp.conf`, выполнив команду:

```
ln -s /etc/httpd2/conf/sites-available/crl-dp.conf /etc/httpd2/conf/sites-enabled/
```

- Удалите из каталога `/etc/httpd2/conf/sites-enabled` ссылку на файл `000-default.conf`, выполнив команду:

```
sudo rm /etc/httpd2/conf/sites-enabled/000-default.conf
```

- Активируйте модуль `headers`, выполнив команду:

```
a2enmod headers
```

- Создайте каталог `/var/www/crl-dp`, выполнив команду:

```
sudo mkdir /var/www/crl-dp
```

- Выполните перезапуск веб-сервера Apache для применения изменений конфигурации, выполнив команду:

```
sudo systemctl restart httpd2
```

- Экспортируйте из Центра сертификации, согласно подразделу 7.10.8 настоящего руководства, для распространения следующие файлы:
  - список отозванных сертификатов CRL;
  - список изменений последнего опубликованного CRL – DeltaCRL;
  - сертификаты центров сертификации.
- Разместите в каталоге `/var/www/crl-dp` полученные файлы CRL, Delta CRL и/или AIA.
- Убедитесь, что файлы CRL, Delta CRL или AIA доступны для скачивания. Для этого необходимо на любом другом АРМ, для которого сервер пользовательской точки распространения CRL DP является достижимым, перейти в браузере по ссылке:

```
http://IP/crl-dp/FILENAME
```

где `IP` – IP-адрес сервера пользовательской точки распространения CRL DP, `FILENAME` – имя любого из файлов, добавленных в каталог `/var/www/crl-dp`, например:

```
http://192.168.0.125/crl-dp/SUB_CA.crl
```

## 7.10.8 Получение файлов CRL, Delta CRL и AIA

### 7.10.8.1 Получение файлов посредством запуска скрипта из состава программы

Предварительно необходимо подготовить скрипт, отредактировав его исходный код, выполнив команду:

```
sudo nano /opt/aecaCa/scripts/export-ca-data.sh
```

Внесите актуальные значения следующих параметров:

- идентификатор центра сертификации, файлы CRL, Delta CRL и AIA которого будут экспортированы (параметр `CA_ID` можно выделить, как крайний параметр URL центра сертификации, например: `https://sub01.presale.aeca/access-certificates/4a660253-09bf-4cc6-a363-871a9c4cbd8c`, где `4a660253-09bf-4cc6-a363-871a9c4cbd8c` – идентификатор ЦС);
- путь к папке хранения сертификата для авторизации в ЦС (параметр `CERTIFICATE_PATH`), в случае использования значений по умолчанию для этих параметров необходимо создать каталог `/opt/aecaCa/dist/account`;
- путь к файлу контейнера p12 для авторизации в ЦС (параметр `P12_PATH`);
- пароль от контейнера p12 для авторизации в ЦС (параметр `P12_PASSWORD`);
- путь к файлу сертификата для авторизации в ЦС (параметр `CERT_PATH`), в случае использования значений по умолчанию необходимо создать каталог `/opt/aecaCa/dist/account`;
- путь к файлу ключа сертификата для авторизации в ЦС (параметр `KEY_PATH`), в случае использования значений по умолчанию для этих параметров необходимо создать каталог `/opt/aecaCa/dist/account`;
- хост ЦС (может быть как localhost, так и внешний адрес, параметр `SERVICE_HOST`);
- путь к папке экспорта файлов CRL, Delta CRL и AIA (параметр `DOWNLOAD_PATH`);
- задержка между проверками статуса в секундах (параметр `STATUS_CHECK_DELAY`).
- Для экспорта файлов запустите скрипт, выполнив команду (с правами суперпользователя или sudo):

```
sudo bash /opt/aecaCa/scripts/export-ca-data.sh
```

В результате успешного выполнения скрипта в каталог, указанный в параметре `DOWNLOAD_PATH`, будут экспортированы файлы CRL, Delta CRL и AIA, а также архив «certificates.zip» со списком сертификатов, выпущенных ЦС, идентификатор которого указан в параметре `CA_ID`.

### 7.10.8.2 Получение файлов посредством использования методов REST API

Для получения файлов CRL, Delta CRL и AIA необходимо аутентифицироваться в программе по сертификату доступа. Аутентификация осуществляется путем обращения к методу идентификации и аутентификации по сертификату доступа публичного API (см. описание метода и пример его использования в разделе 1.1 документа «Центр сертификатов доступа Aladdin Enterprise Certificate Authority Certified Edition. Руководство администратора. Часть 2. Приложение 3. Описание методов REST API» RU.АЛДЕ.03.01.020 32 01-2).

В результате аутентификации по сертификату доступа будет получен маркер доступа, который будет использоваться далее.

Если при дальнейшем использовании маркера доступа в ответе на обращение к методам API будет содержаться сообщение об ошибке «Срок действия JWT токена истек», необходимо использовать метод обновления маркера доступа (см. описание метода и пример его использования в разделе 1.2 документа «Центр сертификатов доступа Aladdin Enterprise Certificate Authority Certified Edition. Руководство администратора. Часть 2. Приложение 3. Описание методов REST API» RU.АЛДЕ.03.01.020 32 01-2).

Для получения файла CRL необходимо использовать метод получения CRL по идентификатору Центра сертификации (см. описание метода в разделе 6.7 документа «Центр сертификатов доступа Aladdin Enterprise

Пример использования метода (через утилиту curl):

85BTYgvGL5ns5kXfCe2Wxmr7oPj-  
7XMAzBI98JydXkLEbmRx7F1OTeNW1ZY3JKwKvi9yFxbWrojB3yNq2ak39cvNj4AFKCEBF0nE8UxKPoyXKDXeg  
C0xEv2UK8mhF7Um4od9B1LWlCuNqKEXyqTGr1DDKJcYjoWBh49pQFAc3mG\_bv7pBtTY7\_vwuVNAelBAqj1kUm  
\_scA\_1-gARBh-oaU\_ZTGXNe-zpXKIiTDM-uFXLTuImZXRA - маркер доступа, полученный в результате аутентификации.

Полученный ответ на обращение к методу (при отсутствии ошибок) необходимо сохранить в файл с расширением «crl».

Для получения файла AIA необходимо использовать метод получения сертификата Центра сертификации по идентификатору Центра сертификации (см. описание метода в разделе 6.5 документа «Центр сертификатов доступа Aladdin Enterprise Certificate Authority Certified Edition. Руководство администратора. Часть 2. Приложение 3. Описание методов REST API» RU.АЛДЕ.03.01.020 32 01-2).

Пример использования метода (через утилиту curl):

```
curl -k --location 'https://192.168.111.100/export-  
service/api/v2/public/export/certificate-authorities/e5291624-fac6-4d5f-ae7-  
d57be0372489/certificate' --header 'Cookie:  
token=eyJhbGciOiJSUzUxMiJ9.eyJzZXNzaW9uSWQiOiI2Njc3NGU1ZS1jODkzLTRmOWQtODM4Yy1lMzQzZG  
Q1MGE3ZjU1LCJpYXQiojE3MTAzMTIzODAsImV4cCI6MTcxMDMxMjU2MH0.MyyCQr89HeahIsnsn_vUXxeSqw  
FVlWRJUtpIkVMTbxq7BrzjG1cjFNJ9rEXx9jGKeSaTMbuwhmjX4aODGnPWCSFc18DUCqFA-  
85BTYgvGL5ns5kXfCe2Wxmr7oPj-  
7XMAzBI98JydXkLEbmRx7F1OTeNW1ZY3JKwKvi9yFxbWrojB3yNq2ak39cvNj4AFKCEBF0nE8UxKPoyXKDXeg  
C0xEv2UK8mhF7Um4od9B1LWlCuNqKEXyqTGr1DDKJcYjoWBh49pQFAc3mG_bv7pBtTY7_vwuVNAelBAqj1kUm  
_scA_1-gARBh-oaU_ZTGXNe-zpXKIiTDM-uFXLTuImZXRA'
```

где:

192.168.111.100 – IP-адрес хоста AECA-CA;

e5291624-fac6-4d5f-ae7-d57be0372489 – идентификатор Центра сертификации (может быть получен из URL карточки Центра сертификации);

eyJhbGciOiJSUzUxMiJ9.eyJzZXNzaW9uSWQiOiI2Njc3NGU1ZS1jODkzLTRmOWQtODM4Yy1lMzQzZG  
Q1MGE3ZjU1LCJpYXQiojE3MTAzMTIzODAsImV4cCI6MTcxMDMxMjU2MH0.MyyCQr89HeahIsnsn\_vUXxeSqw  
FVlWRJUtpIkVMTbxq7BrzjG1cjFNJ9rEXx9jGKeSaTMbuwhmjX4aODGnPWCSFc18DUCqFA-  
85BTYgvGL5ns5kXfCe2Wxmr7oPj-  
7XMAzBI98JydXkLEbmRx7F1OTeNW1ZY3JKwKvi9yFxbWrojB3yNq2ak39cvNj4AFKCEBF0nE8UxKPoyXKDXeg  
C0xEv2UK8mhF7Um4od9B1LWlCuNqKEXyqTGr1DDKJcYjoWBh49pQFAc3mG\_bv7pBtTY7\_vwuVNAelBAqj1kUm  
\_scA\_1-gARBh-oaU\_ZTGXNe-zpXKIiTDM-uFXLTuImZXRA - маркер доступа, полученный в результате аутентификации.

Ответ на обращение к методу (при отсутствии ошибок) необходимо сохранить в файл с расширением «pem».

### 7.10.9 Параметры точек распространения в сертификате

В создаваемых Центром сертификации Aladdin eCA сертификатах субъектов в разделе «x509v3 extensions»:

- В подразделе «x509v3 CRL Distributions Points» указаны URL-адреса точек распространения CRL в соответствии с перечнем и порядком точек распространения CRL.
- В подразделе «x509v3 Freshest CRL» указаны URL-адреса точек распространения Delta CRL в соответствии с перечнем и порядком точек распространения Delta CRL.
- В подразделе «Authority Information Access» в полях «CA Issuers» указаны URL-адреса точек распространения AIA в соответствии с перечнем и порядком точек распространения AIA.
- В подразделе «Authority Information Access» в полях «OCSP» указаны URL-адреса служб OCSP в соответствии с перечнем и порядком служб OCSP.

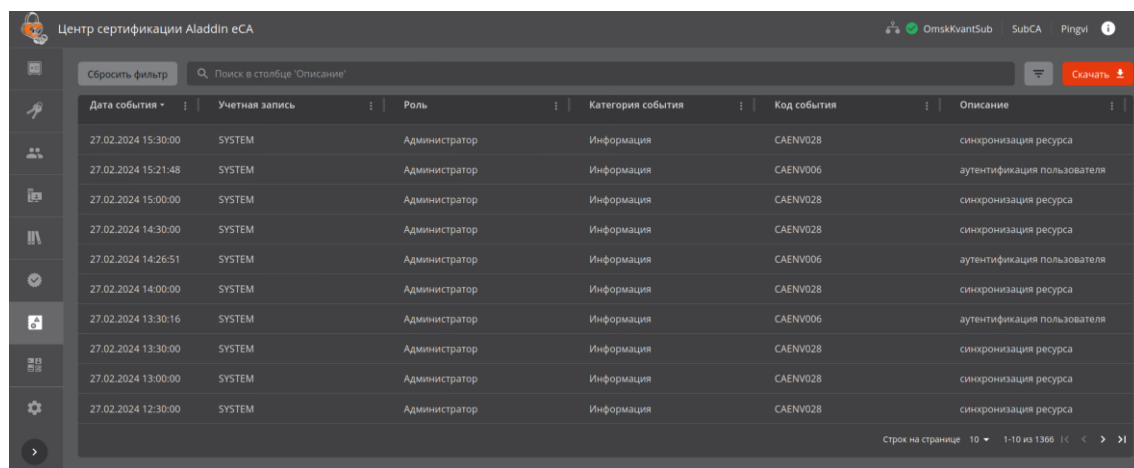


## 7.11 Раздел «Журнал событий»

Журнал событий предназначен для выявления случаев нарушения политики безопасности при эксплуатации ЦС Aladdin eCA. В журнале аудита регистрируются системные события, связанные с работой ПО, а также события, связанные с изменениями настроек и действиями пользователей.

Раздел «Журнал событий» предназначен для полного или выборочного просмотра истории событий сервера, формирования и выгрузки журнала событий по заданным критериям.

- Переход в раздел «Журнал событий» (см. Рисунок 222) осуществляется через боковое меню, расположенное слева на главном экране (см. Рисунок 52).
- Данный раздел доступен только пользователям с ролью «администратор».



Скриншот интерфейса «Центр сертификации Aladdin eCA». В центре экрана отображается таблица событий. Вверху есть панель с кнопкой «Сбросить фильтр», полем поиска «Поиск в столбце 'Описание'» и кнопкой «Скачать». Таблица имеет следующие столбцы: «Дата события», «Учетная запись», «Роль», «Категория события», «Код события» и «Описание». В таблице перечислены события от 27.02.2024 15:30:00 до 27.02.2024 12:30:00, все с ролью «Администратор» и категорией «Информация». Внизу справа указано «Строк на странице 10» и «1-10 из 1366».


Дата события	Учетная запись	Роль	Категория события	Код события	Описание
27.02.2024 15:30:00	SYSTEM	Администратор	Информация	CAENV028	синхронизация ресурса
27.02.2024 15:21:48	SYSTEM	Администратор	Информация	CAENV006	аутентификация пользователя
27.02.2024 15:00:00	SYSTEM	Администратор	Информация	CAENV028	синхронизация ресурса
27.02.2024 14:30:00	SYSTEM	Администратор	Информация	CAENV028	синхронизация ресурса
27.02.2024 14:26:51	SYSTEM	Администратор	Информация	CAENV006	аутентификация пользователя
27.02.2024 14:00:00	SYSTEM	Администратор	Информация	CAENV028	синхронизация ресурса
27.02.2024 13:30:16	SYSTEM	Администратор	Информация	CAENV006	аутентификация пользователя
27.02.2024 13:30:00	SYSTEM	Администратор	Информация	CAENV028	синхронизация ресурса
27.02.2024 13:00:00	SYSTEM	Администратор	Информация	CAENV028	синхронизация ресурса
27.02.2024 12:30:00	SYSTEM	Администратор	Информация	CAENV028	синхронизация ресурса

Рисунок 222 – Экран раздела «Журнал событий»

- Программный компонент «Центр сертификации Aladdin eCA» оснащен функцией сбора диагностической информации, которая получает и аккумулирует записи о событиях для последующего анализа в базе данных «аесаса» (имя базы данных по умолчанию, конфигурация базы данных указана в файле `/opt/aecaCa/scripts/config.sh`).
- В процессе работы программного компонента «Центр сертификации Aladdin eCA» системные службы и компоненты приложения регистрируют все производимые действия. Произшедшие события записываются в файлы регистрации событий с расширением `.log`, расположенные в папках соответствующих сервисов, которыми были инициированы события по пути `/opt/aecaCa/dist/logs/'имя сервиса'`. Файлы регистрации событий, создаваемые в подкаталогах `/opt/aecaCa/dist/logs/`, имеют права доступа 640 (rw-r-----). Срок хранения файлов регистрации событий составляет 10 дней с ограничением размера в 50 Мб.
- На данном экране (см. Рисунок 222) отображаются все зарегистрированные события (из списка Таблица 23 **Ошибка! Источник ссылки не найден.**) в виде таблицы с пагинацией.
- В таблице отображены следующие информационные элементы (табличные поля):
  - дата события;
  - имя учётной записи, действия которой повлекли событие;
  - роль (администратор, оператор);
  - категория события (информационное, ошибка);
  - код события;
  - описание.
- В разделе «Журнал событий» доступны следующие операции:
  - просмотр подробного описания события в его карточке;
  - выгрузка журнала событий в файл формата `.csv` в объеме, выполненной выборки;

- полный или выборочный просмотр журнала событий.

### 7.11.1 Управление экранной таблицей

- Для каждой колонки экранной таблицы (справа от названия заголовка) доступна кнопка управления действиями  <Действия в колонке>. По нажатию данной кнопки разворачивается меню (см. Рисунок 223) в котором возможно (в зависимости от применённых ранее действий – фильтр, сортировка, изменение ширины, скрытие колонки):
  - очистить сортировку, если ранее было применено данное действие, и вернуться к отображению всех событий в колонке;
  - сортировать по возрастанию/убыванию значений в колонке;
  - очистить фильтр, если ранее было применено данное действие, и вернуться к отображению всех событий в колонке;
  - отфильтровать, отобразив поле для выбора критерия фильтрации;
  - сбросить размер колонок, сбросив ширину колонок к значению «по умолчанию»;
  - скрыть колонку из отображаемых на экране;
  - показать все колонки, отобразив на экране ранее скрытые колонки.

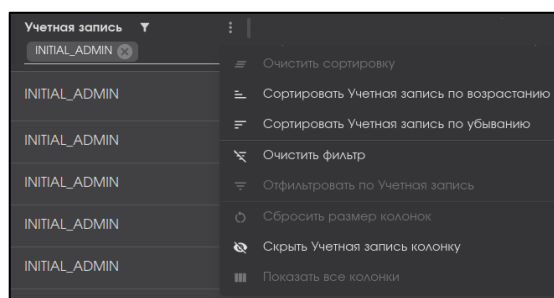
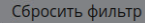


Рисунок 223 – Кнопка <Действия в колонке>

- Для сброса применённых фильтров следует нажать кнопку <Сбросить фильтр>  в результате чего в экранной таблице раздела «Журнал событий» будут отображены все зарегистрированные события.

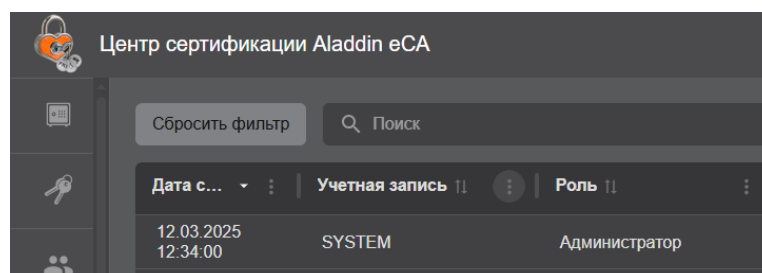



Рисунок 224 – Кнопка <Сбросить фильтр>

### 7.11.2 Выборка событий с помощью фильтров

Локальные фильтры расположены в заголовках столбцов списка. Каждый фильтр предназначен для выборки записей о событиях по параметрам, представленным в данном столбце. Вы можете выполнить выборку записей, применив несколько фильтров.

По умолчанию локальные фильтры скрыты. Чтобы раскрыть списки фильтров, нажмите .

Чтобы выполнить выборку записей о событиях, раскройте список фильтра в выбранном столбце и укажите критерии для выборки.

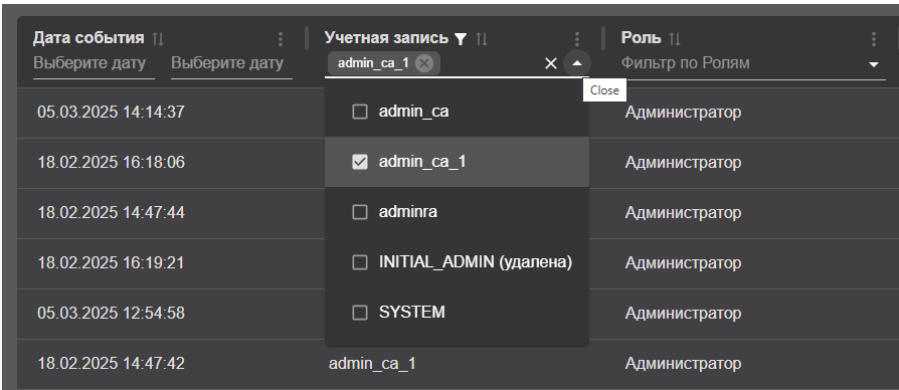



Рисунок 225 – Выборка записей о событиях с помощью локального фильтра

В журнале событий локальные фильтры позволяют отобрать записи о событиях по следующим критериям:

- временной отрезок, за который было зарегистрировано событие;
- имена учетных записей пользователей, которые были инициаторами действий, в результате которых были зарегистрированы события;
- роли учетных записей пользователей, которые были инициаторами действий, в результате которых были зарегистрированы события;
- категории событий, которые отражают информационный характер событий или ошибку;
- коды событий – уникальные идентификаторы событий определенного типа.

Чтобы отменить действие выбранного фильтра, нажмите в заголовке столбца  и выберите в списке «Очистить фильтр».

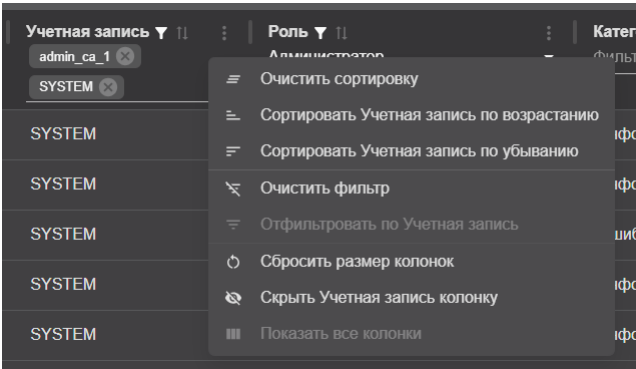

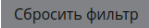


Рисунок 226 – Отмена действия фильтра или исключение выбранных критериев

Чтобы скрыть фильтры, нажмите . При этом действие фильтров не отменяется.

Для полной отмены всех применённых фильтров нажмите кнопку <Сбросить фильтр>  на верхней панели раздела «Журнал событий».



7.11.3 Сортировка событий

Средства сортировки событий на экране раздела «Журнал событий» представлены элементами выбора направления сортировки в заголовке таблицы экранной формы (см. Рисунок 227):

- дата события – упорядочивание осуществляется от старых к новым или от новых к старым записям событий;
- учётная запись – упорядочивание осуществляется в алфавитном порядке;
- роль – упорядочивание осуществляется в алфавитном порядке;
- код события – упорядочивание данных в порядке возрастания или убывания кода.

Дата события ▾	Учетная запись [1]	Роль [1]	Категория события [1]	Код события [1]	Описание [1]
----------------	--------------------	----------	-----------------------	-----------------	--------------

Рисунок 227 – Поля сортировки содержимого экрана раздела «Журнал событий»

- Для выполнения сортировки по выбранной колонке таблицы нажмите на заголовок выбранной колонки или используйте кнопку <Действие колонки> (см. раздел 7.11.1).
- 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 каждой колонке:
  - нажмите кнопку  <Действия в колонке> и в раскрывшемся окне выберите пункт «Очистить сортировку» (см. Рисунок 223);
  - или несколько раз нажмите на заголовке колонки, для которой применена сортировка.

#### 7.11.4 Поиск событий

Строка поиска (см. Рисунок 231) предназначена для поиска записей событий в журнале по содержимому колонки «Описание» и полям подраздела «Подробности» карточки события. Поиск запускается автоматически при вводе искомого значения в строку поиска, результат поиска будет отражён на экранной таблице.

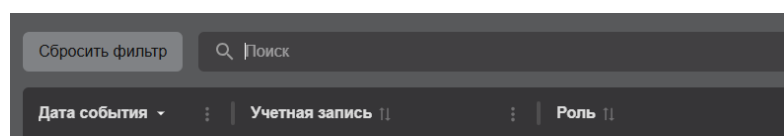


Рисунок 228 – Поисковая строка в разделе «Журнал событий»

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

#### 7.11.5 Карточка события

- Просмотр подробного описания события возможен посредством окна «Свойства события» (карточка события).
- Переход к окну «Свойства события» (см. Рисунок 229) осуществляется при нажатии на строку события в разделе «Журнал событий» (см. Рисунок 222).

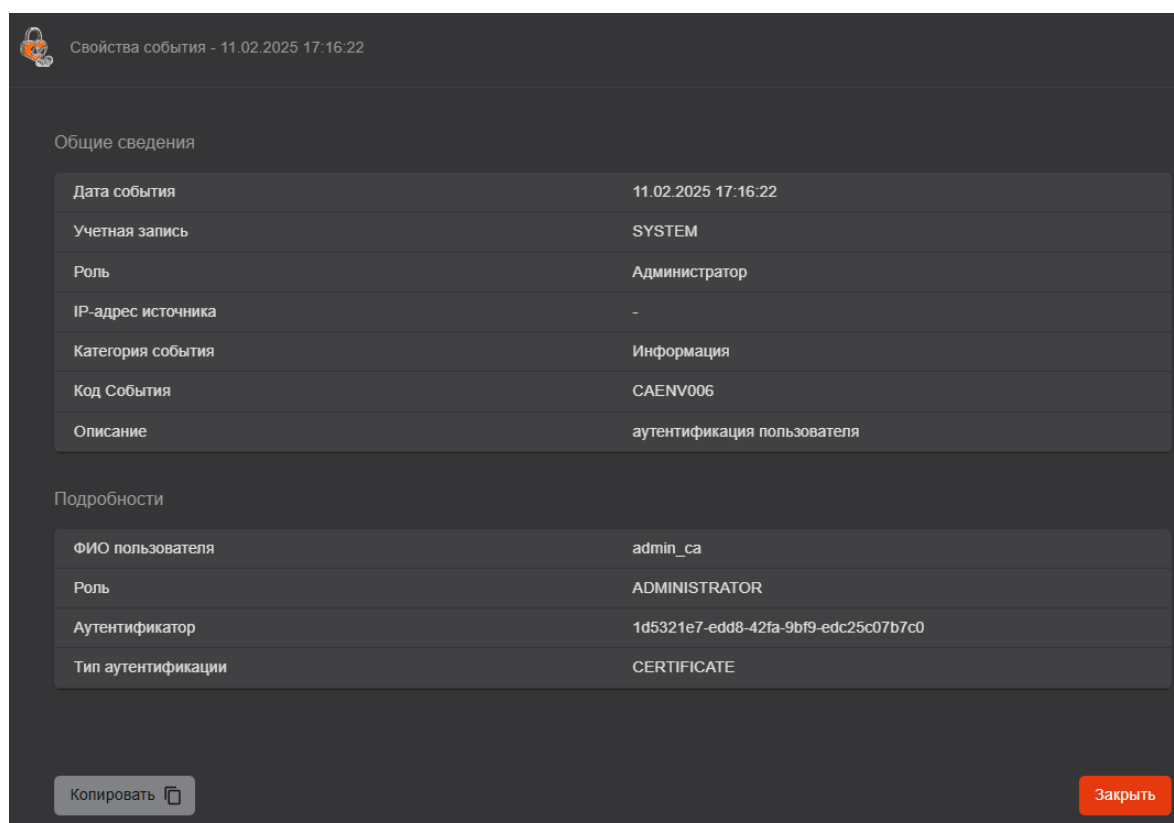



Рисунок 229 – Окно «Свойства события» (карточка события)

- Карточка события включает в себя следующую информацию:
  - подраздел «Общие сведения», содержащий следующие поля:
    - «Дата события» – содержит дату и время события;
    - «Учетная запись» – содержит логин учетной записи инициатора события;
    - «Роль» – содержит роль учетной записи инициатора события;
    - «IP-адрес источника» - IP-адрес узла, с которого была выполнена аутентификация пользователя (инициатора события);
    - «Категория события» – содержит категорию события (Информация или Ошибка);
    - «Код события», содержащее код события (список кодов событий см. в Таблица 23);
    - «Описание».
  - подраздел «Подробности», содержащий поля расширенного описания события. Состав полей см. в Таблица 23.
- Доступные действия в карточке события:
  - копирование события в буфер обмена (см. подраздел 7.11.6);
  - закрытие окна с помощью нажатия на кнопку <Закрыть>.

#### 7.11.6 Копирование события в буфер обмена

Для копирования события в буфер обмена следует:

- открыть карточку события (см. Рисунок 229);
- в карточке события нажать на кнопку  «Копировать». При этом происходит копирование содержимого полей карточки события в буфер обмена в формате «Название поля: значение в поле»;

- после этого вставить содержимое буфера обмена (например, в текстовый файл – см. Рисунок 230).

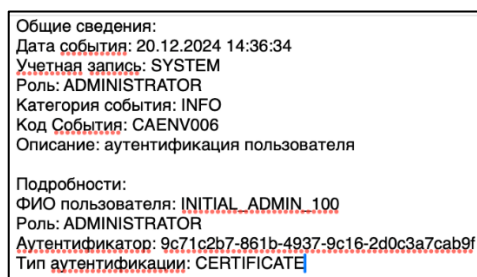


Рисунок 230 – Пример копирования события в текстовый файл

#### 7.11.7 Экспорт журнала событий




- Определите параметры экспортируемого журнала событий, для этого настройте фильтры в соответствии с заданными критериями:
  - датой (выбранным периодом);
  - учётной записью. Значение учётной записи пользователя и его роли записываются в момент совершения события. В случае редактирования учётной записи пользователя (изменения отображаемого имени или роли учётной записи) запись события остаётся неизменной;
  - ролью;
  - категорией события;
  - кодом события.
- Без применения фильтров, будут экспортированы все события.
- Для выгрузки журнала событий нажмите кнопку <Скачать>, расположенную на верхней панели экрана раздела «Журнал событий». Кнопка меняет своё состояние в зависимости от статуса процесса:
  - скачать  – система готова к новому формированию и скачиванию журнала событий;
  - скачивание выполняется  – начинается подготовка файла, содержащего записи журнала событий, соответствующие критериям фильтра или слову для поиска (при отсутствии заданных в фильтре или строке поиска значений будут экспортированы все записи журнала событий). Нажатие на кнопку в текущем состоянии не повлечёт никаких действий;
  - скачать (готово)  – файл журнала событий готов для скачивания. Нажатие на кнопку запускает скачивание файла журнала событий по указанному пути (в соответствии с настройками браузера). После завершения скачивания файла, статус кнопки возвращается в состояние «Скачать».
- Выгруженный файл имеет формат .csv, содержимое файла представлено в кодировке UTF-8 с разделителем полей “;” и доступно для открытия любым текстовым редактором (рекомендуемая программа просмотра записей журнала событий – MS Excel).
- Время хранения записей в журнале событий составляет 180 дней по умолчанию с момента создания журнала (см. раздел 7.11.8 настоящего руководства).
- Возможные сообщения журнала событий приведены в таблице ниже (Таблица 23).

Таблица 23 – Сообщения журнала событий

Причина, вызвавшая запись в журнал	Код события	Категория события	Содержание описания в журнале
запуск службы	CAENV000	INFO	запуск службы:<наименование сервиса>:<параметры запуска если есть>
остановка службы	CAENV001	INFO	остановка службы:<наименование сервиса>
импорт лицензии	CAENV002	INFO	импорт лицензии:<CN-корневого>:<CN-CA>:<срок действия>:<флаг OCSP>:<кол-во активных>
ошибка импорта лицензии	CAENV003	ERROR	ошибка импорта лицензии:<CN-корневого>:<CN-CA>:<срок действия>:<флаг OCSP>:<кол-во активных>:<текст ошибки>
проверка лицензии	CAENV004	INFO	проверка лицензии:<CN-корневого>:<CN-CA>:<срок действия>:<флаг OCSP>:<кол-во активных>
ошибка проверки лицензии	CAENV005	ERROR	ошибка проверки лицензии:<CN-корневого>:<CN-CA>:<срок действия>:<флаг OCSP>:<кол-во активных>:<текст ошибки>
аутентификация пользователя	CAENV006	INFO	аутентификация пользователя:<имя>:<роль>:<серийный номер сертификата>:<тип аутентификации>
ошибка аутентификации	CAENV007	ERROR	ошибка аутентификации:<серийный номер сертификата>:<текст ошибки>
активация центра сертификации	CAENV008	INFO	активация центра сертификации:<CN>:<DNS>
ошибка активации	CAENV009	ERROR	ошибка активации центра сертификации:<CN>:<DNS>:<текст ошибки>
создание запроса на сертификат ЦС	CAENV010	INFO	Успешное создание запроса на сертификат центра сертификации:<CN>:<DNS>
ошибка создания запроса	CAENV011	ERROR	Ошибка создания запроса на сертификат центра сертификации:<CN>:<DNS>:<текст ошибки>
импорт сертификата центра сертификации	CAENV012	INFO	Успешный импорт сертификата центра сертификации и цепочки сертификатов, успешные проверки цепочки сертификатов, успешная проверка сопоставления открытых ключей:<CN>:<CN-корневого>

Причина, вызвавшая запись в журнал	Код события	Категория события	Содержание описания в журнале
ошибка импорта сертификата центра сертификации	CAENV013	ERROR	ошибка импорта сертификата центра сертификации:<CN>:<CN-корневого>:<текст ошибки>
выпуск сертификата	CAENV014	INFO	выпуск сертификата:<CN>:<SAN>:<шаблон>:<вид операции>:<сценарий>:<ресурсная система>:<алгоритм> где <вид операции> - один из вариантов “PKCS12”, “по запросу” <сценарий> - один из вариантов “подпись запроса подчиненного ЦС”, “сертификат учетной записи”, “сертификат субъекта”
ошибка выпуска сертификата	CAENV015	ERROR	ошибка выпуска сертификата:<CN>:<SAN>:<шаблон>:<вид операции>:<сценарий>:<ресурсная система>:<алгоритм>:<текст ошибки>
регистрация центра валидации	CAENV016	INFO	регистрация центра валидации:<указанный адрес центра валидации>
ошибка регистрации	CAENV017	ERROR	ошибка регистрации центра валидации:<указанный адрес центра валидации>:<текст ошибки>
активация OCSP центра валидации	CAENV018	INFO	активация OCSP:<адрес центра валидации>:<серийный номер сертификата>
ошибка активации	CAENV019	ERROR	ошибка активации OCSP:<адрес центра валидации>:<серийный номер сертификата>:<текст ошибки>
настройка периода CRL	CAENV020	INFO	настройка периода CRL:<периода CRL>:<перекрытие CRL>:<период DeltaCRL>
ошибка настройки	CAENV021	ERROR	ошибка настройки периода CRL:<периода CRL>:<перекрытие CRL>:<период DeltaCRL>:<текст ошибки>
публикация CRL	CAENV022	INFO	публикация CRL:<номер CRL>:<срок действия>:<адрес точки публикации>
ошибка публикации	CAENV023	ERROR	ошибка публикации CRL:<номер CRL>:<срок действия>:<адрес точки публикации>:<текст ошибки>
добавление ресурсной системы	CAENV024	INFO	добавление ресурсной системы:<наименование>:<тип>:<адрес>:<точка>:<служебный логин>



Причина, вызвавшая запись в журнал	Код события	Категория события	Содержание описания в журнале
ошибка добавления	CAENV025	ERROR	ошибка добавления ресурсной системы:<наименование>:<тип>:<адрес>:<точка>:<служебный логин>:<текст ошибки>
изменение ресурсной системы	CAENV026	INFO	изменение ресурсной системы:<наименование>:<тип>:<адрес>:<точка>:<служебный логин>
ошибка изменения	CAENV027	ERROR	ошибка изменения ресурсной системы:<наименование>:<тип>:<адрес>:<точка>:<служебный логин>:<текст ошибки>
синхронизация ресурса	CAENV028	INFO	синхронизация ресурса:<наименование>:<кол-во субъектов>
ошибка синхронизации	CAENV029	ERROR	ошибка синхронизации ресурса:<наименование>:<кол-во субъектов>:<текст ошибки>
создание учетной записи	CAENV030	INFO	Создание учетной записи:<лог.имя>:<роль>
ошибка создания	CAENV031	ERROR	Ошибка создания учетной записи:<лог.имя>:<роль>:<текст ошибки>
изменение учетной записи	CAENV032	INFO	изменение учетной записи:<лог.имя>:<роль>:< серийный номер сертификата>
ошибка изменения прав	CAENV033	ERROR	ошибка изменения учетной записи:<лог.имя>:<роль>:< серийный номер сертификата>:<текст ошибки>
сохранение прав оператора	CAENV034	INFO	ввод прав оператора:<лог.имя>:<[список прав]>
ошибка сохранения	CAENV035	ERROR	ошибка сохранения прав оператора:<лог.имя>:<[список прав]>:<описание ошибки>
установка сертификата веб-сервера	CAENV036	INFO	установка сертификата веб -сервера:< серийный номер сертификата>
ошибка установки	CAENV037	ERROR	ошибка установки сертификата веб -сервера:< серийный номер сертификата>:<описание ошибки>
изменение списка издателей	CAENV038	INFO	изменение списка разрешенных издателей:<имя издателя>:<” добавлен” или “удален”>

Причина, вызвавшая запись в журнал	Код события	Категория события	Содержание описания в журнале
ошибка изменения	CAENV039	ERROR	ошибка изменения списка разрешенных издателей:<имя издателя>:<"добавлен" или "удален">:<текст ошибки>
подключение к ключевому носителю	CAENV042	INFO	подключение к ключевому носителю:<маркировка носителя>:<тип носителя>
ошибка подключения	CAENV043	ERROR	подключение к ключевому носителю:<маркировка носителя>:<тип носителя>:<описание ошибки>
создание контейнера на ключевом носителе	CAENV044	INFO	создание контейнера на ключевом носителе:<маркировка носителя>:<ID-контейнера>:<алгоритм>
ошибка создания	CAENV045	ERROR	ошибка создания контейнера на ключевом носителе:<маркировка носителя>:<ID-сертификата>:<алгоритм>:<описание ошибки>
запись сертификата на ключевой носитель	CAENV046	INFO	запись сертификата на ключевой носитель:<маркировка носителя>:<ID-сертификата>
ошибка записи	CAENV047	ERROR	ошибка записи сертификата на ключевой носитель:<маркировка носителя>:<ID-сертификата>:<описание ошибки>
публикация сертификата в ресурсной системе	CAENV048	INFO	публикация сертификата в ресурсной системе:<ресурс>:<CN-субъекта>:<серийный номер сертификата>
ошибка публикации	CAENV049	ERROR	ошибка публикации сертификата в ресурсной системе:<ресурс>:<CN-субъекта>:<серийный номер сертификата>:<текст ошибки>
сохранение журнала в CSV	CAENV050	INFO	сохранение журнала в CSV:<фильтр>
ошибка сохранения	CAENV051	ERROR	ошибка сохранения журнала в CSV:<фильтр>:<текст ошибки>
генерация CRL	CAENV052	INFO	генерация CRL:<номер CRL>:<срок действия>
ошибка генерации	CAENV053	ERROR	ошибка генерации CRL:<номер CRL>:<срок действия>:<текст ошибки>
отправка уведомления на почту	CAENV054	INFO	отправка уведомления на почту:<CN>:<email>:<шаблон>

Причина, вызвавшая запись в журнал	Код события	Категория события	Содержание описания в журнале
ошибка отправки	CAENV055	ERROR	ошибка отправки уведомления на почту:<CN>:<email>:<шаблон>:<текст ошибки>
отзыв сертификата	CAENV056	INFO	Отзыв сертификата: после обновления:certSerialNumber:<ID-сертификата>
приостановка сертификата	CAENV057	INFO	Приостановка сертификата: после обновления:certSerialNumber:<ID-сертификата>
реактивация сертификата	CAENV058	INFO	Активация сертификата: после обновления:certSerialNumber:<ID-сертификата>:revocationReason:<Причина отзыва>
начало удаления центра сертификации	CAENV059	INFO	Начало удаления центра сертификации: после обновления: <CN>:<CN-корневого или подчиненного>, DNS <" суффикс различающегося имени">
окончание удаления центра сертификации	CAENV060	INFO	Конец удаления центра сертификации: после обновления <CN>:<CN-корневого или подчиненного>, DNS <" суффикс различающегося имени">
ошибка при удалении центра сертификации	CAENV061	ERROR	ошибка удаления центра сертификации:<CN>:<CN-корневого или подчиненного>, DNS <" суффикс различающегося имени"> :<текст ошибки>
начало очистки журнала событий	CAENV064	INFO	Начало очистки журнала событий
окончание очистки журнала событий	CAENV065	INFO	Конец очистки журнала событий
ошибка при очистке журнала событий	CAENV066	ERROR	Ошибка очистки журнала события: <фильтр>:<текст ошибки>
начало архивации журнала событий	CAENV067	INFO	Начало архивации журнала событий
окончание архивации журнала событий	CAENV068	INFO	Конец архивации журнала событий
ошибка при архивации журнала событий	CAENV069	ERROR	Ошибка архивации журнала события: <фильтр>:<текст ошибки>

Причина, вызвавшая запись в журнал	Код события	Категория события	Содержание описания в журнале
добавить шаблон сертификата в “Центр регистрации”	CAENV070	INFO	Добавить шаблон сертификата <наименование шаблона> в “Центр регистрации”
ошибка при добавлении шаблона сертификата в “Центр регистрации”	CAENV071	ERROR	Ошибка при добавлении шаблона сертификата <наименование шаблона> в “Центр регистрации”
убрать шаблон сертификата в “Центр регистрации”	CAENV072	INFO	Убрать шаблон сертификата <наименование шаблона> в “Центр регистрации”
ошибка при уборке шаблона сертификата в “Центр регистрации”	CAENV073	ERROR	Ошибка при уборке шаблона сертификата <наименование шаблона> в “Центр регистрации”
успешная проверка контрольных сумм	CAENV074	INFO	Успешная проверка целостности исполняемых файлов.
неуспешная проверка контрольных сумм	CAENV075	ERROR	Проверка целостности исполняемых файлов прошла неуспешно: <список файлов, которые не удалось проверить>
Распаковка ключей ЦС	CAENV076	INFO	Успешная проверка целостности контейнеров закрытых ключей центра сертификации при распаковке.
Ошибка при распаковке ключей ЦС	CAENV077	ERROR	Неуспешная проверка целостности контейнеров закрытых ключей центра сертификации при распаковке: <текст ошибки>
Скачан контейнер PKCS#12	CAENV078	INFO	Успешный экспорт контейнера закрытого ключа за пределы программы <серийный номер сертификата в контейнере>
Скачан сертификат	CAENV079	INFO	Скачан сертификат
Скачена цепочка сертификата	CAENV080	INFO	Скачана цепочка сертификата
Экспорт запроса на сертификат ЦС	CAENV081	INFO	Успешный экспорт запроса на сертификат центра сертификации за пределы программы
Ошибка экспорта запроса на сертификат ЦС	CAENV082	ERROR	Неуспешный экспорт запроса на сертификат центра сертификации за пределы программы

Причина, вызвавшая запись в журнал	Код события	Категория события	Содержание описания в журнале
Ошибка экспорта контейнера PKCS#12	CAENV085	ERROR	Ошибка экспорта контейнера закрытого ключа за пределы программы <серийный номер сертификата в контейнере>
Успешное создание резервной копии	CAENV086	INFO	Успешное создание резервной копии <путь к созданной резервной копии>
Ошибка создания резервной копии	CAENV087	ERROR	Ошибка создания резервной копии: <текст ошибки>
Успешное восстановление из резервной копии	CAENV088	INFO	Успешное восстановление из резервной копии <путь к использованной резервной копии>
Ошибка восстановления из резервной копии	CAENV089	ERROR	Ошибка восстановления из резервной копии: <текст ошибки>
Ошибка синхронизации субъекта	CAENV090	ERROR	Ошибка синхронизации субъекта:текущее значение:идентификатор субъекта:<идентификатор субъекта>,DN субъекта:<DN субъекта>,идентификатор PC<идентификатор PC>:<причина ошибки>
Создание правила доступа	CAENV091	INFO	создание правила доступа:текущее значение:Категория правила доступа: категория правила доступа,Субъекты правила доступа:[ субъекты правила доступа],Объекты правила доступа:[объекты правила доступа],Операции правила доступа:[операции правила доступа]
Ошибка создания правила доступа	CAENV092	ERROR	Ошибка создания правила доступа: <текст ошибки>
Редактирование правила доступа	CAENV093	INFO	редактирование правила доступа:до обновления:Субъекты правила доступа:[ субъекты правила доступа],Объекты правила доступа:[объекты правила доступа], после обновления:Субъекты правила доступа:[ субъекты правила доступа],Объекты правила доступа:[объекты правила доступа]
Ошибка изменения правила доступа	CAENV094	ERROR	Ошибка изменения правила доступа: <текст ошибки>

Причина, вызвавшая запись в журнал	Код события	Категория события	Содержание описания в журнале
Удаление правила доступа	CAENV095	INFO	удаление правила доступа:текущее значение:Категория правила доступа: категория правила доступа,Субъекты правила доступа:[ субъекты правила доступа],Объекты правила доступа:[объекты правила доступа],Операции правила доступа:[операции правила доступа]
Ошибка удаления правила доступа	CAENV096	ERROR	Ошибка удаления правила доступа: <текст ошибки>
Добавление Syslog-сервера	CAENV097	INFO	Успешное добавление Syslog-сервера: <адрес хоста>:<порт>:<протокол>:<флаг отправки сообщений>
Ошибка добавления Syslog-сервера	CAENV098	ERROR	Ошибка добавления Syslog-сервера: <текст ошибки>
Изменение параметров Syslog-сервера	CAENV099	INFO	Успешное изменение параметров Syslog-сервера: <адрес хоста>:<порт>:<протокол>:<флаг отправки сообщений>
Ошибка изменения параметров Syslog-сервера	CAENV100	ERROR	Ошибка изменения параметров Syslog-сервера: <текст ошибки>
Удаление Syslog-сервера	CAENV101	INFO	Успешное удаление Syslog-сервера: <адрес хоста>:<порт>:<протокол>:<флаг отправки сообщений>
Ошибка удаления Syslog-сервера	CAENV102	ERROR	Ошибка удаления Syslog-сервера: <текст ошибки>
Создание корневого ЦС	CAENV103	INFO	Создание корневого ЦС: <Отображаемое имя ЦС>, <Имя ЦС>, <Суффикс различающегося имени>, <Криптопровайдер RSA>, <Криптопровайдер ECDSA>, <Криптопровайдер ГОСТ>, <Срок действия ЦС>, <Алгоритм ключа>, <Длина ключа>, <Алгоритм хэш-суммы>, <Место хранения закрытого ключа>
Ошибка создания корневого ЦС	CAENV104	ERROR	Ошибка создания корневого ЦС: <Отображаемое имя ЦС>, <Имя ЦС>, <Причина ошибки>

Причина, вызвавшая запись в журнал	Код события	Категория события	Содержание описания в журнале
Создание подчиненного ЦС	CAENV105	INFO	Создание подчиненного ЦС: <Отображаемое имя ЦС>, <Имя ЦС>, <Имя корневого ЦС>, <Суффикс различающегося имени>, <Криптопровайдер RSA>, <Криптопровайдер ECDSA>, <Криптопровайдер ГОСТ>, <Алгоритм ключа>, <Длина ключа>, <Алгоритм хэш-суммы>, <Место хранения закрытого ключа>
Ошибка создания подчиненного ЦС	CAENV106	ERROR	Ошибка создания подчиненного ЦС: <Отображаемое имя ЦС>, <Имя ЦС>, <Причина ошибки>
Экспорт закрытого ключа ЦС	CAENV107	INFO	Экспорт закрытого ключа ЦС: <Идентификатор ЦС>: <Отображаемое имя ЦС>: <Имя ЦС>: <Экспортирован из хранилища>
Ошибка экспорта закрытого ключа ЦС	CAENV108	ERROR	Ошибка экспорта закрытого ключа ЦС: <Идентификатор ЦС>: <Отображаемое имя ЦС>: <Имя ЦС>: <Хранилище>: <Текст ошибки>
Скачан закрытый ключ ЦС	CAENV109	INFO	Скачан закрытый ключ ЦС: <Идентификатор ЦС>: <Отображаемое имя ЦС>: <Имя ЦС>
Ошибка скачивания закрытого ключа ЦС	CAENV110	ERROR	Ошибка скачивания закрытого ключа ЦС: <Идентификатор ЦС>: <Отображаемое имя ЦС>: <Имя ЦС>: <Текст ошибки>
Импорт закрытого ключа ЦС	CAENV111	INFO	Импорт закрытого ключа ЦС: <Идентификатор ЦС>: <Отображаемое имя ЦС>: <Имя ЦС>: <Импортирован в хранилище>
Ошибка импорта закрытого ключа ЦС	CAENV112	ERROR	Ошибка импорта закрытого ключа ЦС: <Идентификатор ЦС>: <Отображаемое имя ЦС>: <Имя ЦС>: <Хранилище>: <Текст ошибки>

7.11.8 Архивирование и очистка журнала событий

- Программный компонент «Центр сертификации Aladdin eCA» обеспечивает настраиваемое архивирование событий с одновременной очисткой Журнала событий в части заархивированных событий.
- Для настройки параметров архивации и очистки отредактируйте переменные окружения, используемые сервисом logs-service в конфигурационном файле `/opt/aecaCa/scripts/config.sh`:
  - `archive_millis_ago` – время хранения событий (по умолчанию 180 дней) в миллисекундах. Записи со сроком давности большим или равным времени хранения будут заархивированы;
  - `archive_cron` – периодичность запуска архивации (значение указывается в формате CRON-выражения, значение по умолчанию – `'0 0 0 1 * *'`). По умолчанию процесс архивации будет запущен при наступлении первого числа каждого месяца;
  - `archive_path` – путь сохранения сформированного архива.
- Архив в формате .zip, содержащий .csv файл, с именем `logs-<дата и время создания архива>.zip` будет сохранён на сервере, где развёрнут Центр сертификации, в папке (по умолчанию) `/opt/aecaCa/dist/archive`.

7.12 Раздел «Шаблоны»

Расширить возможности Центра сертификации возможно при помощи создания специализированных индивидуальных шаблонов сертификатов.

- Переход в раздел «Шаблоны» (см. Рисунок 231) осуществляется через боковое меню, расположенное слева на экране (см. Рисунок 52).

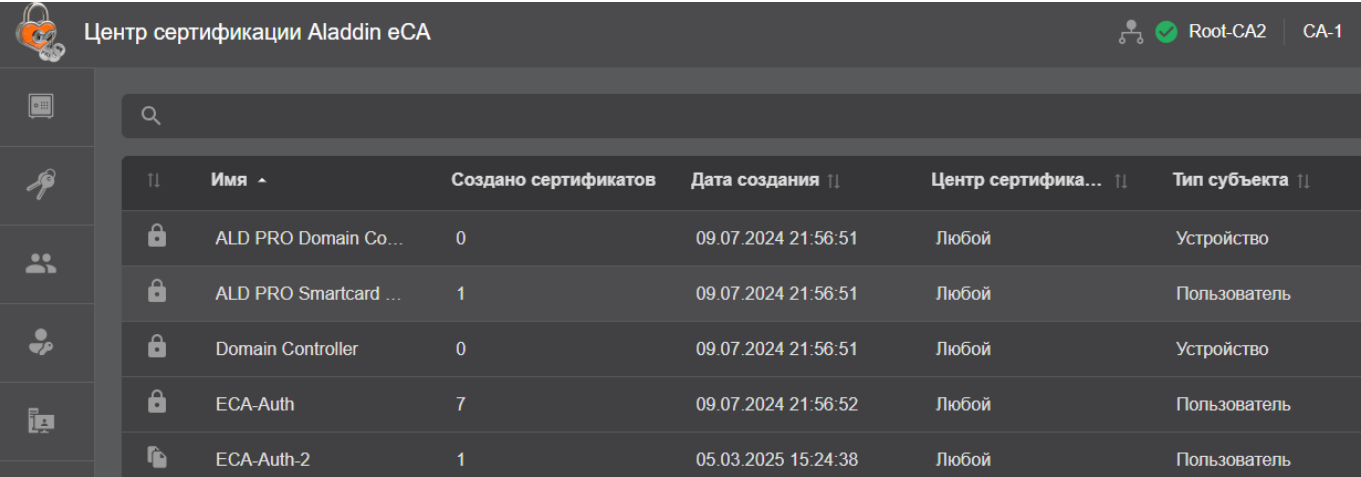





Рисунок 231 – Экран раздела «Шаблоны»

- 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. В случае клонирования предустановленного шаблона или импортированного по умолчанию будет предложено имя в формате «Копия\_имя исходного шаблона», при клонировании импортированного шаблона по умолчанию будет предложено имя шаблона в формате «``»;
- создано сертификатов – количество сертификатов, выпущенных по данному шаблону;
- 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 «WEB-Server», «ECA-WEB-Server», «OCSP Signer», «Domain Controller», «ALD PRO Domain Controller», «SCEP Management», для которых устанавливается значение типа субъекта «Устройство»).**

- Просмотр набора полей предустановленных шаблонов<sup>33</sup> возможен по клику «мышкой» на выбранный шаблон. Список предустановленных шаблонов:
  - Domain Controller;
  - Smartcard Logon;
  - WEB-Client;
  - WEB-Server;
  - S/MIME;
  - ECA-Auth;
  - ECA-User;
  - ECA-WEB-server;
  - ALD PRO Domain Controller;
  - ALD PRO Smartcard Logon;
  - OCSP Signer;
  - Root CA;
  - Sub CA;
  - SCEP Management.
- Действия доступные над всеми видами шаблонов:

<sup>33</sup> Значения полей шаблонов сертификатов по умолчанию см. в Приложение 2. Описание полей предустановленных шаблонов сертификатов.

- просмотр полного списка шаблонов или по результатам поиска;
- загрузка новых шаблонов сертификатов MS CS;
- клонирование (создание) шаблона;
- поиск шаблонов;
- сортировка шаблонов.
- Действия доступные над клонированными и импортированными видами шаблонов:
  - редактирование шаблона;
  - сохранение результатов редактирования шаблона;
  - удаление шаблона или массовое удаление шаблонов.
- Добавленные шаблоны доступны для использования на вкладке
- Все шаблоны на экране раздела отображаются в виде таблицы с пагинацией.

### 7.12.1 Поиск шаблонов

Строка поиска (см. Рисунок 232) 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.

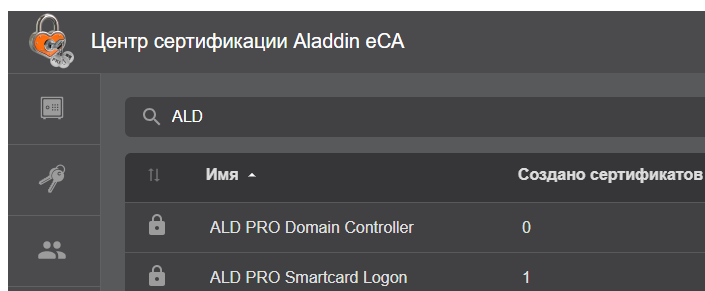



Рисунок 232 – Поисковая строка в разделе «Шаблоны»

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


### 7.12.2 Сортировка шаблонов

- Средство сортировки списка шаблонов представлено элементом выбора направления сортировки в заголовках колонок экранной таблицы (см. Рисунок 231) – 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.

### 7.12.3 Карточка шаблона

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

Рисунок 233 – Окно карточки шаблона

- В открывшемся окне администратору доступны:
  - кнопка возврата на вкладку «Шаблоны»;
  - кнопка  для клонирования текущего шаблона;
  - кнопка «Сохранить» для записи изменений полей текущего шаблона, доступная для всех шаблонов, кроме предустановленных;
  - поле «Имя шаблона»;
  - поле «Идентификатор» содержит постоянный идентификатор шаблона;
  - дата и время создания шаблона (для предустановленных шаблонов – это дата и время развёртывания/обновления Центра сертификации, для импортируемых шаблонов – это дата и время загрузки шаблонов в Центр сертификации, для новых шаблонов – это дата и время клонирования шаблона);
  - дата и время изменения шаблона;
  - информация, сформированная в виде вкладок «Свойства», «Расширения», «Компоненты имени сертификата».

#### 7.12.3.1 Вкладка шаблона «Свойства»

На вкладке шаблона «Свойства» доступны поля (см. Рисунок 234):

- общие:
  - поле «Период действия сертификата». Формат ввода: 1d,1m,1y - час, день, месяц, год;
  - 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).
  - чек-бокс «Публиковать сертификат в ресурсную систему».


- Шифрование (перечень доступных алгоритмов зависит от криптопровайдеров выбранного для данного шаблона центра сертификации – издателя сертификатов):
  - RSA;
  - ECDSA
  - ГОСТ Р 34.10-2012.

The screenshot shows the 'Свойства' (Properties) tab for a certificate template. It is divided into two main sections: 'Общие' (General) and 'Шифрование' (Encryption). In the 'Общие' section, the 'Период действия сертификата' (Validity period) is set to '2y', the 'Формат ввода' (Input format) is 'ddmmyy', the 'Центр сертификации' (CA) is 'CA-1', and the 'Тип субъекта' (Subject type) is 'Пользователь'. There is a checkbox for 'Публиковать сертификат в ресурсную систему' (Publish certificate to the resource system). In the 'Шифрование' section, 'RSA' and 'ECDSA' are selected with checkboxes, and their 'Минимальная длина ключа' (Minimum key length) is set to 1024 and 256 respectively. 'ГОСТ Р 34.10-2012' is not selected.

Рисунок 234 – Вкладка «Свойства» шаблона сертификата

#### 7.12.4 Вкладка шаблона «Расширения»

На вкладке шаблона «Расширения» доступны:

- список с множественным выбором «Использование ключа»;
- чек-бокс «Считать это расширение критическим» для списка «Использование ключа»;
- список с множественным выбором «Расширенное использование ключа»;
- кнопка  рядом со списком «Расширенное использование ключа», при нажатии на которую открывается модальное окно «Идентификаторы расширенного использования ключа», в котором есть возможность создавать пользовательские идентификаторы расширенного использования ключа (подробнее см. раздел 7.12.11). Кнопка доступна только для шаблонов, не входящих в перечень предустановленных<sup>34</sup>;
- 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 наличии данного атрибута у субъекта). SID может быть получен только для субъектов ресурсных систем MS AD, SambaDC, РЕД АДМ и Альт Домен.
- список с возможностью удаления и добавления элементов «OID политики сертификата»;
- чек-бокс «Считать это расширение критическим» для списка «OID политики сертификата».

<sup>34</sup> Перечень предустановленных шаблонов см. в Приложение 2. Описание полей предустановленных шаблонов сертификатов

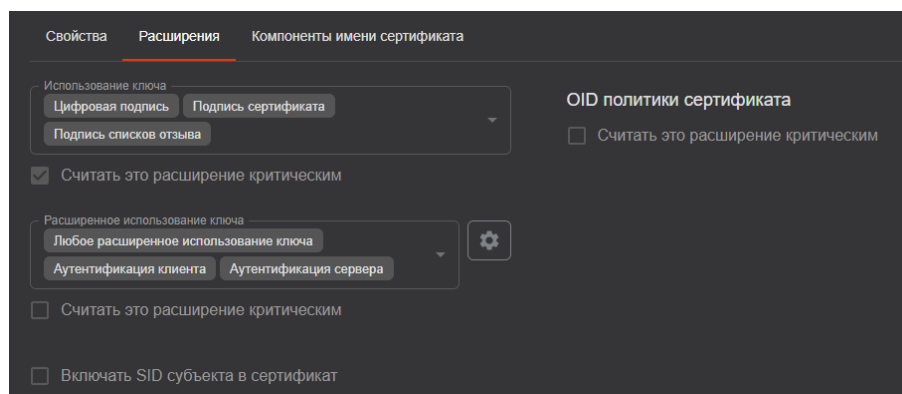


Рисунок 235 – Вкладка «Расширения» шаблона сертификата

При наведении курсора на значения в поле «Расширенное использование ключа», а также на значения в выпадающем списке, отображается всплывающая подсказка, содержащая «OID» и «Описание» выбранного значения (см. Рисунок 236).

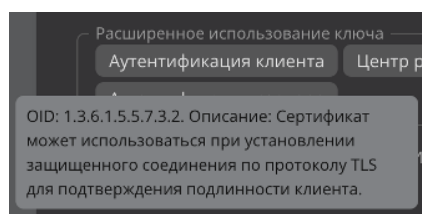


Рисунок 236 – Всплывающая подсказка значения расширенного использования ключа

#### 7.12.4.1 Вкладка шаблона «Компоненты имени сертификата»

На вкладке шаблона «Компоненты имени сертификата» доступны (см. Рисунок 237):

- отличительное имя субъекта;
- альтернативное имя субъекта.

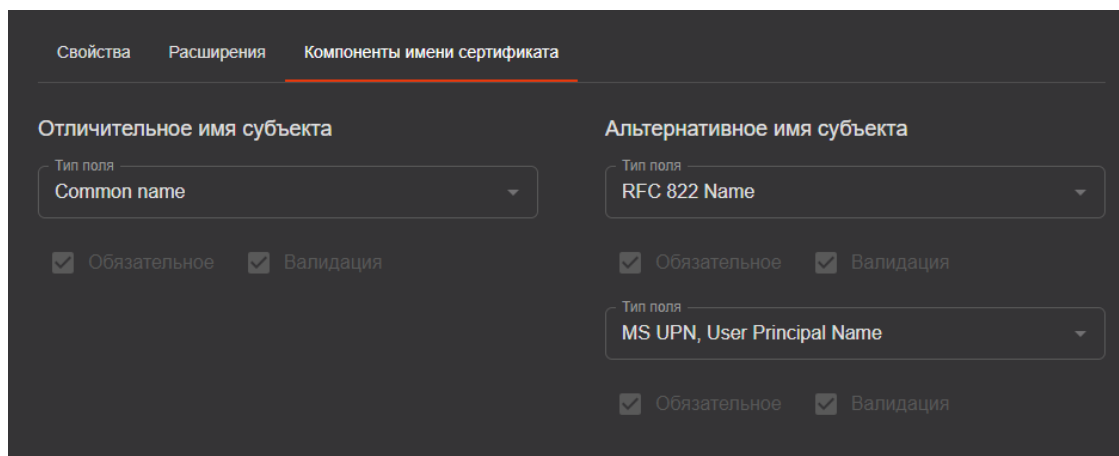



Рисунок 237 – Вкладка «Компоненты имени сертификата» шаблона сертификата

#### 7.12.5 Создание нового шаблона

- Создание индивидуального шаблона возможно на базе существующих в системе шаблонов и состоит из трёх этапов:
  - клонирования выбранного шаблона;
  - редактирование клонированного шаблона в соответствии со спецификой индивидуального шаблона;

- сохранения изменений, внесённых в клонированный шаблон.

7.12.5.1 Клонирование шаблона

- Выделите предустановленный шаблон на вкладке «Шаблоны» указателем «мышь».
- Нажмите появившуюся в строке кнопку <Клонировать> .
- В открывшемся окне подтверждения действия (см. Рисунок 238) при необходимости отредактируйте имя нового шаблона в соответствующем поле и нажмите кнопку <Клонировать> для создания нового шаблона на основании выбранного предустановленного шаблона.
- Имя нового шаблона должно быть уникально, может содержать кириллицу, латиницу, любые символы, ограничители ввода между параметрами – пробелы, длина вводимого имени не ограничена с максимальной памятью до 1 Гб.
- Если имя сохраняемого шаблона не уникально, ниже поля ввода имени шаблона появится текстовое предупреждение, и операция сохранения не будет выполнена.
- Для прерывания действия клонирования шаблона нажмите кнопку <Отмена>.

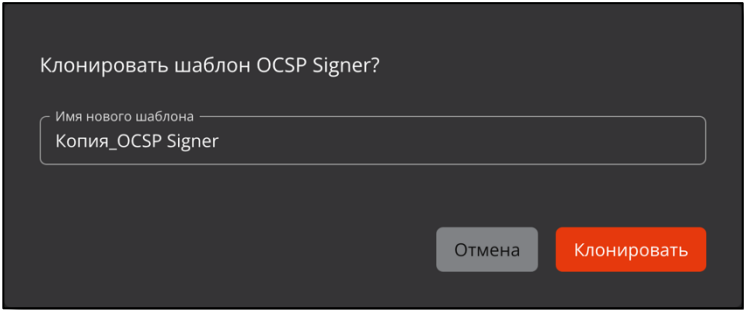


Рисунок 238 – Экран раздела меню «Шаблоны»

- В случае успешного клонирования шаблона сертификата администратор будет уведомлен сообщением на экране «Шаблон успешно клонирован». В результате создаётся полная копия выбранного шаблона.

7.12.6 Редактирование шаблона

- Редактирование применимо для клонированного шаблона или импортированного (загруженного) шаблона MS CS.
- Редактирование предустановленных шаблонов недоступно.
- Для выбранного шаблона доступны для редактирования элементы, указанные в таблице ниже (Таблица 24).

Таблица 24 – Поля шаблона, доступные для изменения через графический интерфейс

Название		Тип	Допустимые значения
Имя шаблона		Строка	Ограничение: 255 символов
Вкладка «Свойства»			
Раздел «Свойства»	Период действия сертификата	Строка	*у *mo *d Значение не может превышать 25 лет
	Центр сертификации	Список	<ul style="list-style-type: none"><li>• список созданных центров сертификации;</li><li>• любой.</li></ul>

Название		Тип	Допустимые значения
	Тип субъекта	Список	<ul style="list-style-type: none"> <li>• корневой Центр сертификации;</li> <li>• подчинённый Центр сертификации;</li> <li>• устройство;</li> <li>• пользователь.</li> </ul>
Раздел «Шифрование»	Алгоритм ключа	Три чек-бокса	<ul style="list-style-type: none"> <li>• RSA</li> <li>• ECDSA</li> <li>• ГОСТ Р 34.10-2012</li> </ul> Доступно включение всех чек-боксов одновременно
	Минимальная длина ключа	Три списка (список для каждого чек-бокса)	RSA: <ul style="list-style-type: none"> <li>• 1024</li> <li>• 1536</li> <li>• 2048</li> <li>• 3072</li> <li>• 4096</li> <li>• 6144</li> <li>• 8192</li> </ul> ECDSA: <ul style="list-style-type: none"> <li>• 256</li> <li>• 384</li> <li>• 521</li> </ul> ГОСТ Р 34.10-2012: <ul style="list-style-type: none"> <li>• 256</li> <li>• 512</li> </ul>
Вкладка «Расширения сертификата»			
Использование ключа		Список с множественным выбором	<ul style="list-style-type: none"> <li>• Цифровая подпись</li> <li>• Подтверждение подлинности</li> <li>• Шифрование ключей</li> <li>• Шифрование данных</li> <li>• Согласование ключей</li> <li>• Подпись сертификатов</li> <li>• Подпись списков отзыва</li> <li>• Только шифрование</li> <li>• Только расшифрование</li> </ul>
Чек-бкс «Считать это расширение критическим» для поля «Использование ключа»		Чек-бкс	<ul style="list-style-type: none"> <li>• Включен</li> <li>• Выключен</li> </ul>
Чек-бкс «Включать SID субъекта в сертификат»		Чек-бкс	<ul style="list-style-type: none"> <li>• Включен</li> <li>• Выключен</li> </ul>
Расширенное использование ключа		Список с множественным выбором	<ul style="list-style-type: none"> <li>• Любое расширенное использование ключа</li> <li>• CSN 369791 TLS клиент</li> <li>• CSN 369791 TLS сервер</li> <li>• Аутентификация клиента</li> </ul>

Название	Тип	Допустимые значения
		<ul style="list-style-type: none"> <li>• Подписание кода</li> <li>• EAP через LAN (EAPOL)</li> <li>• EAP через PPP</li> <li>• Подписание ETSI TSL</li> <li>• Защита электронной почты</li> <li>• ICAO подписание списка отклонений</li> <li>• Управление Intel AMT</li> <li>• Интернет-обмен ключами для IPsec</li> <li>• Аутентификация клиента Kerberos</li> <li>• Центр распространения ключей Kerberos</li> <li>• Подписание коммерческого MS кода</li> <li>• Подписание MS документа</li> <li>• Восстановление MS EFS</li> <li>• Зашифрованная MS файловая система</li> <li>• Подписание индивидуального MS кода</li> <li>• Вход с MS смарт-картой</li> <li>• OCSP подписант</li> <li>• Подписание Adobe PDF</li> <li>• Аутентификация PIV карты</li> <li>• SCVP клиент</li> <li>• SCVP сервер</li> <li>• Домен SIP</li> <li>• SSH клиент</li> <li>• SSH сервер</li> <li>• Аутентификация сервера</li> <li>• Отметка времени</li> <li>• ICAO подписание основного списка</li> </ul>
Чек-бокс «Считать это расширение критическим» для поля «Расширенное использование ключа»	Чек-бокс	<ul style="list-style-type: none"> <li>• Включен</li> <li>• Выключен</li> </ul>
OID политики сертификата	Поле ввода	OID в формате, определенном стандартом ITU X.660
Чек-бокс «Считать это расширение критическим» для поля «OID политики сертификата»	Чек-бокс	<ul style="list-style-type: none"> <li>• Включен</li> <li>• Выключен</li> </ul>
Вкладка «Компоненты имени сертификата»		
Отличительное имя субъекта (SDN)	Список с множественным выбором	<ul style="list-style-type: none"> <li>• Common name</li> <li>• Unique Identifier (UID)</li> <li>• Given name</li> <li>• Initials</li> </ul>



Название	Тип	Допустимые значения
		<ul style="list-style-type: none"> <li>• Surname</li> <li>• Organizational Unit</li> <li>• Organization</li> <li>• Locality</li> <li>• State or Province</li> <li>• Domain Component</li> <li>• Country</li> <li>• Postal Code</li> <li>• Business Category</li> <li>• Telephone number</li> <li>• Pseudonym</li> <li>• Postal address</li> <li>• Street</li> <li>• Name</li> <li>• Title</li> <li>• Domain qualifier</li> <li>• Description</li> <li>• Unstructured address</li> <li>• Unstructured name</li> <li>• Email Address (E)</li> <li>• Serial number</li> <li>• ИНН</li> <li>• ОГРН</li> <li>• ОГРНИП</li> <li>• СНИСЛ</li> <li>• ИНН ЮЛ</li> </ul>
Чек-бокс «Обязательное» для полей отличительного имени субъекта (SDN)	Чек-бокс	<ul style="list-style-type: none"> <li>• Включен</li> <li>• Выключен</li> </ul> <p>Значение по умолчанию (при добавлении нового поля) – выключен. Доступен для каждого поля отличительного имени субъекта.</p>
Чек-бокс «Валидация» для полей отличительного имени субъекта (SDN)	Чек-бокс	<ul style="list-style-type: none"> <li>• Включен</li> <li>• Выключен</li> </ul> <p>Значение по умолчанию (при добавлении нового поля) – выключен.</p>
Альтернативное имя субъекта (SAN)	Список с множественным выбором	<ul style="list-style-type: none"> <li>• RFC 822 Name</li> <li>• DNS Name</li> <li>• IP address</li> <li>• Directory Name</li> <li>• Uniform resource identifier</li> <li>• Registered Identifier (OID)</li> <li>• MS UPN, User Principal Name</li> <li>• MS GUID, Globally Unique Identifier</li> <li>• Kerberos KPN, Kerberos 5 Principal Name</li> <li>• Permanent Identifier</li> </ul>

Название	Тип	Допустимые значения
		<ul style="list-style-type: none"> <li>Xmpp address</li> <li>Service Name</li> <li>Subject Identification Method</li> </ul>
Чек-бокс «Обязательное» для полей альтернативного имени субъекта (SAN)	Чек-бокс	<ul style="list-style-type: none"> <li>Включен</li> <li>Выключен</li> </ul> <p>Значение по умолчанию (при добавлении нового поля) – выключен. Доступен для каждого поля альтернативного имени субъекта.</p>
Чек-бокс «Валидация» для полей альтернативного имени субъекта (SAN)	Чек-бокс	<ul style="list-style-type: none"> <li>Включен</li> <li>Выключен</li> </ul> <p>Значение по умолчанию (при добавлении нового поля) – выключен.</p>

- Для полей «Отличительное имя субъекта» (SDN) и «Альтернативное имя субъекта» (SAN) во вкладке «Компоненты имени сертификата» доступна функция поиска при выборе значений (см. Рисунок 239 и Рисунок 240).



Рисунок 239 – Поиск при выборе значения в поле «Отличительное имя субъекта»

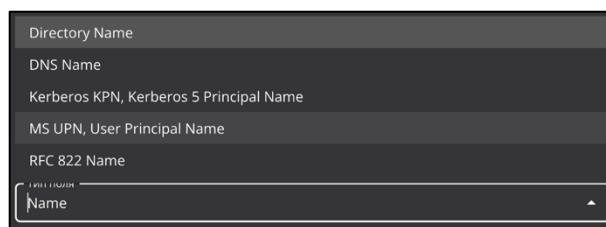


Рисунок 240 – Поиск при выборе значения в поле «Альтернативное имя субъекта»

- При выборе параметров шифрования выбирается минимальная длина ключа, т.е. при выпуске сертификата по данному шаблону для выбора минимальной длины ключа будут доступны значения начиная от установленного минимального и все значения более установленного минимального значения длины ключа.
- Формат ввода периода действия сертификата: 1d,1m,1y - час, день, месяц, год.
- Используйте предлагаемые чек-боксы для дополнительной настройки шаблона сертификата:
  - Если включен чек-бокс «Считать это расширение критическим» для расширения, оно помечается как критическое при создании сертификата по данному шаблону (см. Рисунок 241). При обработке сертификата, имеющего атрибуты, для которых установлены чек-боксы «Считать это расширение критическим», могут быть отклонены, если правила обработки полей сертификатов системы не содержат отмеченных атрибутов (подробнее см. стандарт RFC 5280).

☒ **Считать это расширение критическим**

Рисунок 241 – Поле чек-бокса «Считать это расширение критическим»

- При включенном чек-боксе «Обязательное» для поля будет необходимо указать минимум одно значение в процессе создания сертификата по данному шаблону, а при выключенном чек-боксе значения для данного поля могут быть не указаны. При включенном чек-боксе «Валидации» для поля будет выполняться валидация значений, указываемых пользователем для данного поля в процессе создания сертификата (см. Рисунок 242).

☐ **Обязательное** ☒ **Валидация**

Рисунок 242 – Поле чек-бокса «Обязательное» и «Валидация»

- Используйте кнопки <Добавить поле> (см. Рисунок 243) на вкладках шаблона «Расширения» и «Компоненты имени сертификата» для формирования специализированного шаблона сертификата.

Добавить поле +

Рисунок 243 – Кнопка <Добавить поле> шаблона специализированного сертификата

#### 7.12.6.1 Сохранение внесённых изменений в шаблон

- Для сохранения внесённых изменений в шаблоне нажмите кнопку в карточке шаблона <Сохранить> **Сохранить**, расположенную в правом верхнем углу экранной формы. Сохранение изменений происходит без подтверждения.
- При переходе обратно на текущую вкладку «Шаблоны» или другую вкладку Центра сертификации в случае, если предварительно внесённые в редактируемый шаблон изменения не были сохранены, появляется окно подтверждения действия (см. Рисунок 244), в котором при нажатии кнопки:
  - <Покинуть страницу> внесённые изменения в текущем шаблоне будут утеряны и осуществлён выход из карточки шаблона;
  - <Отмена> будет осуществлено закрытие окна подтверждения и возврат к редактируемой карточке шаблона.


Вы действительно хотите покинуть страницу без сохранения?

Отмена

Покинуть страницу

Рисунок 244 – Подтверждение выхода из карточки шаблона без сохранения изменений

#### 7.12.7 Удаление шаблона

- Данная функция применима только для созданных, клонированных и загруженных шаблонов.
- Данная функция НЕ применима для предустановленных шаблонов.
- При наведении на строку с нужным шаблоном будет доступна иконка  <Удалить>. После нажатия на кнопку <Удалить> будет выведено на экран окно подтверждения действия (см. Рисунок 245), где возможно отменить выбранное действие, нажав кнопку <Отмена>, или подтвердить удаление выбранного шаблона, нажав кнопку <Удалить>.

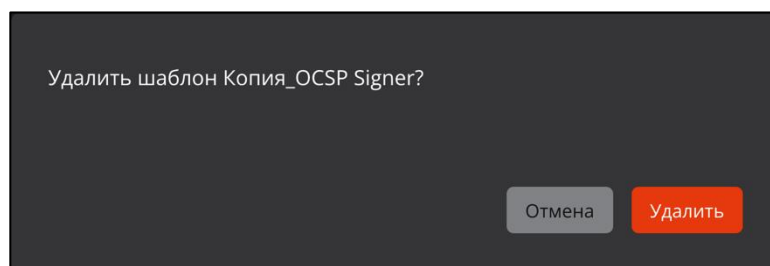





Рисунок 245 – Окно подтверждения удаления шаблона сертификата

- В случае успешного выполнения удаления шаблона сертификата администратор будет уведомлен сообщением на экране «Шаблон успешно удалён».
- Выбранный шаблон удаляется из системы и становится недоступным для всех операций. Сертификаты, выпущенные на этом шаблоне, остаются действительными.

### 7.12.8 Массовая операция (удаления) с шаблонами

- Для массовой операции удаления, применяемой к выбранному множеству шаблонов, нажмите кнопку  «Массовые операции», которая запускает окно выполнения массовой операции.
- В открывшемся окне (см. Рисунок 246) до применения поиска в левом столбце окна будут отображены первые 100 шаблонов в алфавитном порядке. В случае, если найдено более 100 шаблонов, то требуется уточнить параметры в строке поиска. Также поиск возможно осуществить по имени шаблона, который подлежит удалению. Поиск производится для видов шаблонов: импортированный и клонированный, к которым применима операция удаления.
- 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.

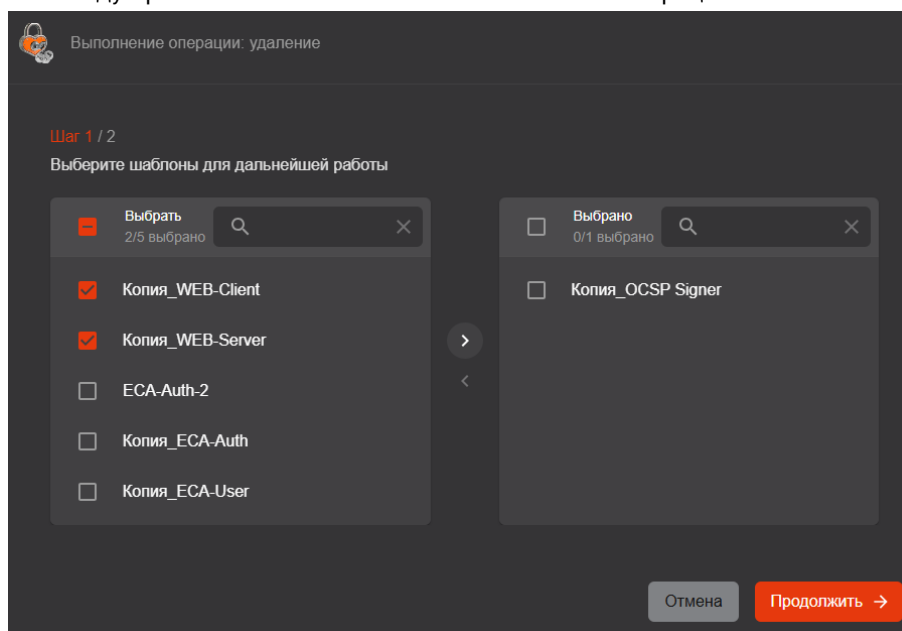



Рисунок 246 – Окно выполнения массовых операций. Шаг 2. Создание списка выбранных шаблонов

- В случае необходимости исключения из выбранных шаблонов, к которым будет применена массовая операция, отметьте флажками шаблоны из списка в правой части окна, и нажмите кнопку  (см. Рисунок 247).

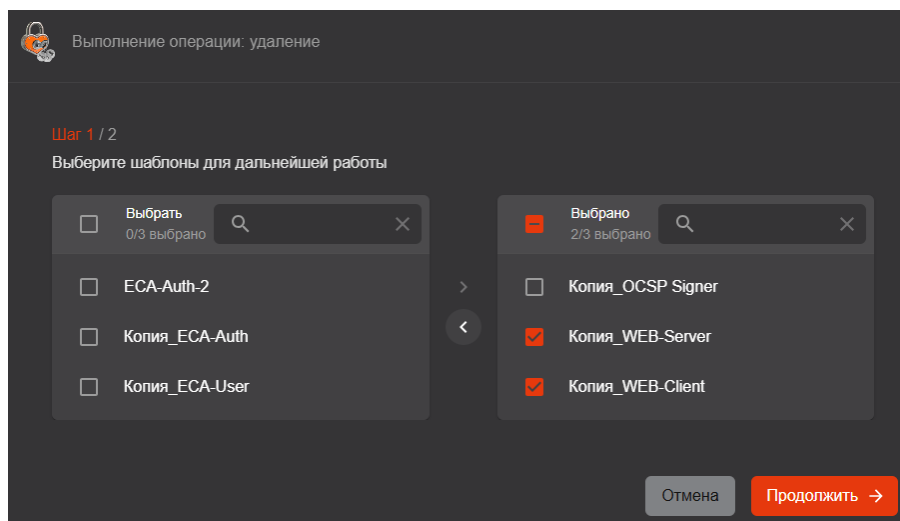


Рисунок 247 – Окно выполнения массовых операций. Шаг 2. Редактирование списка выбранных шаблонов

- Для перехода на следующий шаг нажмите кнопку <Продолжить>.
- В открывшемся окне подтвердите действие, нажав кнопку «Применить» (см. Рисунок 248).

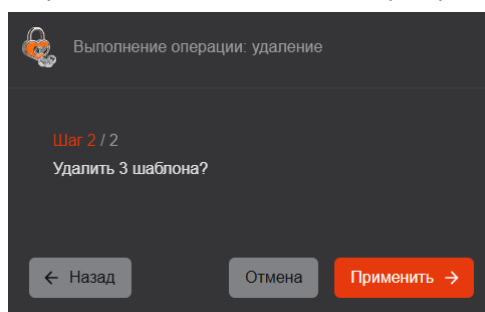


Рисунок 248 – Окно выполнения массовых операций. Шаг 3

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

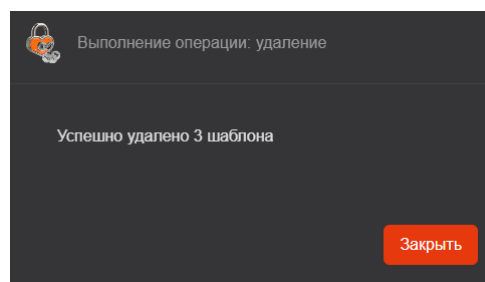


Рисунок 249 – Окно выполнения массовых операций. Шаг 4

## 7.12.9 Шаблоны MSCS


### 7.12.9.1 Экспорт шаблонов из MSCS

- Для экспорта шаблонов запустите скрипт `mscs2aeca.ps1` из комплекта поставки на рабочем месте с установленным Центром сертификации MSCS от имени администратора.
- Для успешного выполнения скрипта необходимо интернет-соединение. Для успешного выполнения скрипта в офлайн режиме требуется предварительно скачать и установить пакет NuGet.
- Скрипт запускается как консольное приложение и работает в режиме командной строки, графический интерфейс не предусмотрен. Запуск скрипта произвести от имени администратора.
- Результатом работы скрипта является сохранение всех шаблонов сертификатов из MSCS в папку `C:\temp\` на хосте.

- Шаблоны сохраняются в формате .csv с разделителем точка с запятой.
- При импорте шаблона из MSCS к названию шаблона должен добавляться префикс «MSCS\_». Если в системе уже существует шаблон, совпадающий с именем импортируемого, то к имени импортируемого должен добавляться суффикс «\_1» и т.д. (счетчик копий).

### 7.12.9.2 Загрузка шаблона MSCS

Для загрузки полученных шаблонов MSCS в Центр Сертификации Aladdin Enterprise CA:

- нажмите кнопку <Загрузить шаблоны> . В открывшемся окне выберите .csv файл шаблонов MSCS в локальной папке и нажмите кнопку <Открыть>.
- В результате шаблоны MSCS будут импортированы, и администратор будет уведомлён сообщением на экране «XX шаблонов успешно загружено», где «XX» - количество успешно загруженных шаблонов (см. Рисунок 250).

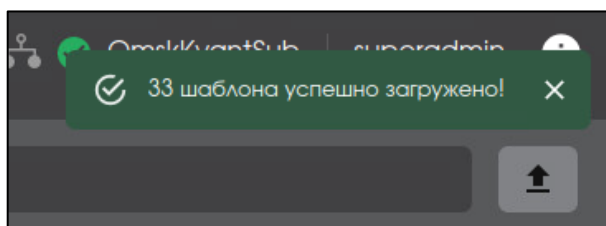


Рисунок 250 – Уведомление об успешной загрузке шаблонов MSCS

- В случае, если шаблоны не были импортированы, администратор будет уведомлен сообщением «Невозможно загрузить шаблоны» (см. Рисунок 250).

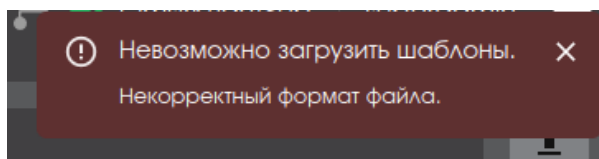


Рисунок 251 – Уведомление о неудачной загрузке шаблонов MSCS

- Поля, загружаемые из файла импорта шаблонов MSCS, приведены в Таблица 25.

Таблица 25 – Поля, загружаемые из файла шаблонов MSCS

Название поля в файле	Описание	Название поле в AECA
TmplName	Имя шаблона	Имя шаблона
DN	Отличительное имя	Отличительное имя
SubjName	Альтернативное имя субъекта и требование обязательности в одной строке	Альтернативное имя субъекта; флажок «Обязательное»
Alghoritm	Алгоритм шифрования	Алгоритм шифрования
AlgMinLen	Минимальная длина ключа	Минимальная длина ключа
ValidPeriod	Период действия	Период действия
KeyUsage, CritExts	Использование ключа	Использование ключа; флажок “считать это расширение критическим”
EKU,	Расширенное использование ключа	Расширенное использование ключа;

Название поля в файле	Описание	Название поле в AECA
CritExts		флажок “считать это расширение критическим”
Polices, CritExts	Политики	OID политики сертификата; флажок “считать это расширение критическим”

- При импорте шаблонов из MSCS значение параметра «Тип субъекта» для импортируемого шаблона определяются на основании значения в поле «SubjType»:
  - значение «User» - тип субъекта «Пользователь»;
  - значение «Computer» - тип субъекта «Устройство»;
  - значение «CA» - тип субъекта «Корневой ЦС»;
  - значение «CrossCA» -тип субъекта «Подчиненный ЦС».
- При импорте шаблонов из MSCS для параметра «Центр сертификации» импортируемого шаблона будет установлено значение «Любой».
- При повторной загрузке файла шаблонов MSCS, все шаблоны будут загружены повторно. Имя шаблона будет сформировано из значения, записанного в поле шаблона «TplName», и присвоением порядкового номера (счетчик копий).

#### 7.12.10 Работа с шаблонами сертификатов

- Загруженные и созданные шаблоны доступны для использования при выпуске сертификатов на вкладке «Сертификаты» и «Субъекты» (см. подраздел 7.4 и 7.7 настоящего Руководства администратора).

##### 7.12.10.1 Идентификатор шаблона

- При формировании заявки на сертификат необходимо указывать идентификатор шаблона – название шаблона или его идентификатор.
- Идентификатор нового (клонированного) шаблона возможно выделить из URL шаблона. Откройте созданный шаблон, выделите адрес, указанный в строке браузера, определите идентификатор шаблона, исходя из структуры URL-адреса. Например:

`https://172.22.5.21/template/8548d5dc-c063-40f9-842d-3e35326fca01`

имеет структуру

`протокол://ip-адрес или имя сервера ЦС/наименование раздела/идентификатор шаблона`

Таким образом, идентификатор созданного шаблона имеет вид `8548d5dc-c063-40f9-842d-3e35326fca01`.

- Для предустановленных шаблонов идентификаторы приведены в таблице ниже (Таблица 26).

Таблица 26 – Идентификаторы предустановленных шаблонов


Название шаблона	Идентификатор
ALD PRO Domain Controller	11ec34a4-d03e-4059-92f0-9c09b08bffe
ALD PRO Smartcard Logon	18d9bd4e-6f15-423f-8137-ac8416ad6874
Domain Controller	bf2dac0a-f05f-49dd-95b4-e50691489b6a
ECA-Auth	8ecba810-7f48-4c4e-b803-99a97146e2ba
OCSP Signer	aac2e49b-9c8e-4869-80c1-eef526ba75ab

Root CA	9129245a-eaad-4ebc-a2a4-8845ac0336fb
Smartcard Logon	aa03e458-50cd-46b8-82cd-d5612ed3b647
S/MIME	0c234243-18cf-4c05-b699-537731b2436f
Sub CA	af3b0355-1798-4c64-98f7-a9c70407db1c
WEB-Client	059a38f5-f345-4275-b79f-e7e6cc3cbb68
WEB-Server	08c66f99-218a-46ef-bdee-6a2b3b26a4f1
SCEP Management	3e5df3d4-683c-4252-b862-467589c2225b
ECA-WEB-server	25bbd733-4d8c-43ce-ba5a-e9826eb7b16c
ECA-User	2d58b30c-3965-4555-9af4-fec4552af21e

### 7.12.11 Работа с идентификаторами расширенного использования ключа

Модальное окно «Идентификаторы расширенного использования ключа» (см. Рисунок 252) обеспечивает возможность просмотра идентификаторов расширенного использования ключа, а также создание и удаление пользовательских идентификаторов расширенного использования ключа.

Модальное окно «Идентификаторы расширенного использования ключа» доступно пользователю с ролью «Администратор».

Открытие модального окна «Идентификаторы расширенного использования ключа» осуществляется из вкладки «Расширения» карточки шаблона (см. раздел 7.12.4) нажатием на кнопку  рядом со списком «Расширенное использование ключа».

Для закрытия модального окна следует нажать кнопку «Закрыть».

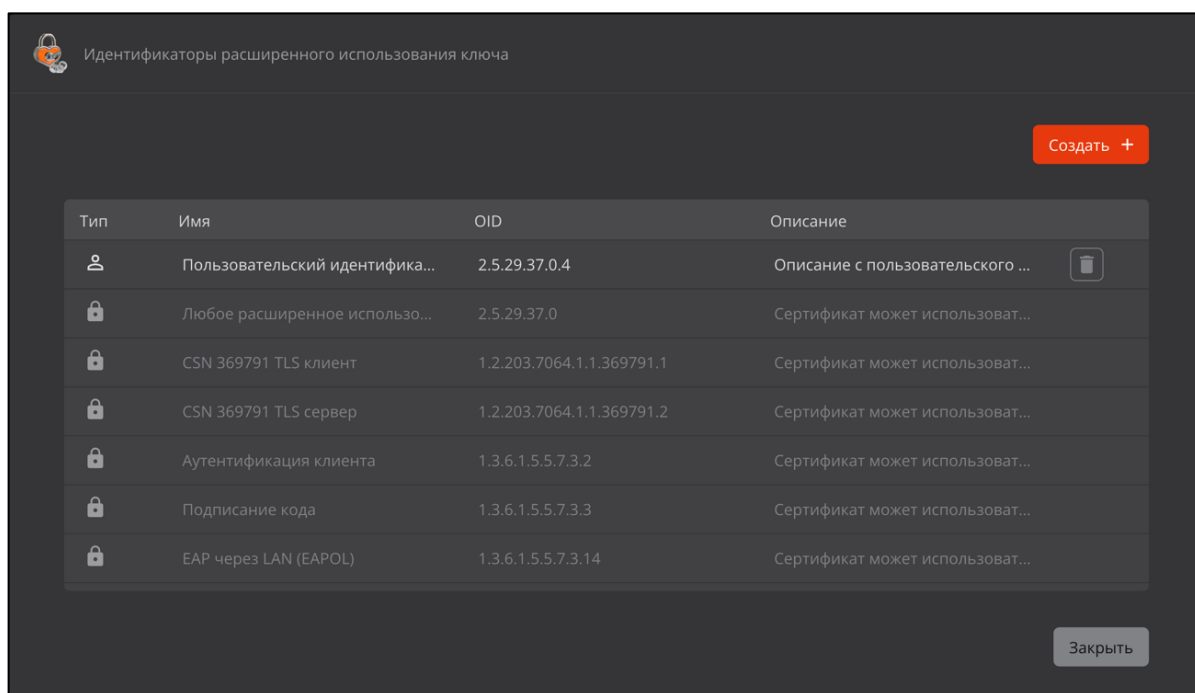




Рисунок 252 – Модальное окно «Идентификаторы расширенного использования ключа»

В модальное окне в табличной форме отображена следующая информация об идентификаторах расширенного использования ключа:

- тип – условное обозначение вида:



-  – предустановленные по умолчанию идентификаторы расширенного использования ключа, созданные в момент установки Центра сертификации Aladdin eCA<sup>35</sup>. Не подлежат редактированию;
  -  – созданные пользователем (пользовательские) идентификаторы расширенного использования ключа.
- имя;
  - OID;
  - описание.

В модальном окне доступны следующие действия:

- создание пользовательских идентификаторов расширенного использования ключа (см. раздел 7.12.11.1);
- удаление пользовательских идентификаторов расширенного использования ключа (см. раздел 7.12.11.2).

#### 7.12.11.1 Создание пользовательского идентификатора расширенного использования ключа

Для создания пользовательского идентификатора расширенного использования ключа выполните следующие шаги:

- В Модальном окне «Идентификаторы расширенного использования ключа» нажмите кнопку <Создать>;
- В появившемся модальном окне «Создание идентификатора расширенного использования ключа» введите следующие поля (см. Рисунок 253):
  - имя – имя создаваемого идентификатора расширенного использования ключа. Поле является уникальным и обязательно к заполнению. При вводе существующего значения будет отображено сообщение об ошибке «Указанное имя уже используется»;
  - OID – OID создаваемого идентификатора расширенного использования ключа в формате OID<sup>36</sup>. Поле является уникальным и обязательным к заполнению. При вводе существующего значения будет отображено сообщение об ошибке «Указанный OID уже используется»;
  - описание – описания создаваемого идентификатора расширенного использования ключа. не является обязательным к заполнению.

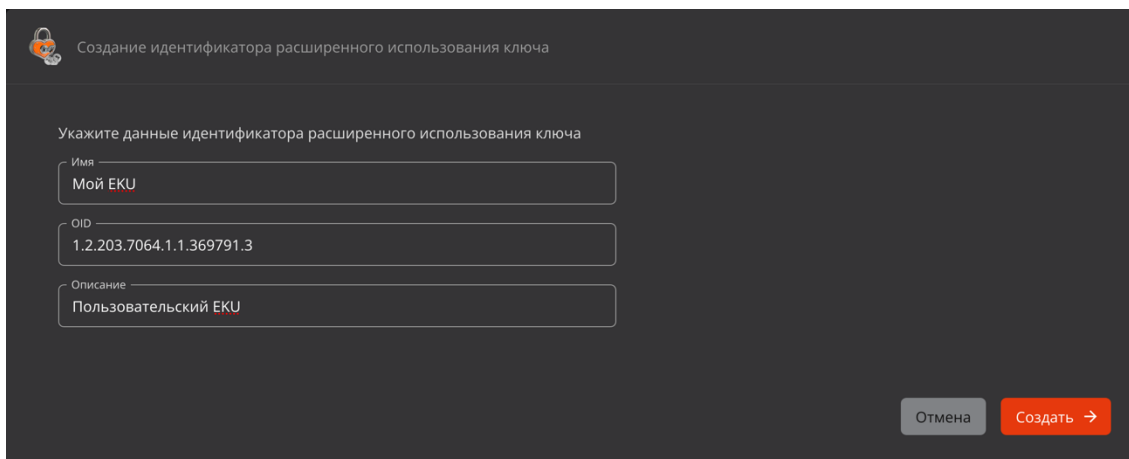


Рисунок 253 – Модальное окно «Идентификаторы расширенного использования ключа»

- Для создания идентификатора расширенного использования ключа нажмите кнопку <Создать>.


<sup>35</sup> Описание предустановленных идентификаторов расширенного использования ключа см. в Приложение 5. Описание предустановленных идентификаторов расширенного использования ключа.

<sup>36</sup> В соответствии с рекомендацией ITU X.660.

После этого будет создан пользовательский идентификатор расширенного использования ключа.

#### 7.12.11.2 Удаление пользовательского идентификатора расширенного использования ключа

Для удаления пользовательского идентификатора расширенного использования ключа выполните следующие шаги:

- В Модальном окне «Идентификаторы расширенного использования ключа» найдите пользовательский идентификатор, который необходимо удалить;
- В строке с идентификатором нажмите на кнопку  «Удалить».

После этого пользовательский идентификатор расширенного использования будет удален.

**Если идентификатор расширенного использования ключа используется в шаблонах, то удаление завершится с ошибкой: «Удаление идентификатора недоступно, так как он используется в шаблоне <Имя текущего шаблона>». Если шаблонов несколько, то отображается имя первого по алфавиту шаблона.**

**Удаление предустановленных идентификатор расширенного использования недоступно.**

### 7.13 Раздел «Настройки»

- Раздел «Настройки» обеспечивает:
  - управление работой веб-сервера и доступом к нему: возможность смены ключей веб-сервера и управление издателями сертификатов учётных записей для доступа к нему;
  - управление перечнем подключенных к программе Syslog-серверов, на которые будет выполняться оправа данных о событиях аудита программы.
- Переход в раздел «Настройки» (см. Рисунок 254) осуществляется через боковое меню, расположенное слева на главном экране (см. Рисунок 52).
- Раздел «Настройки» включает в себя следующие вкладки:
  - Веб-сервер;
  - Syslog.
- Данный раздел доступен только в режиме администратора.

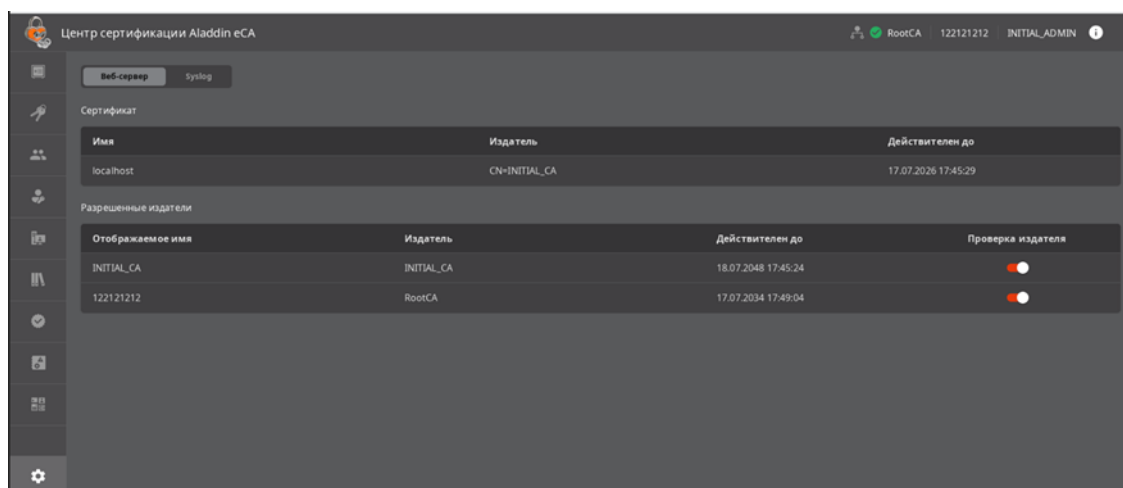


Рисунок 254 – Экран раздела «Настройки»

- Вкладка «Веб-сервер» позволяет осуществлять просмотр данных текущего сертификата веб-сервера, изменение текущего сертификата веб-сервера, просмотр и редактирование списка разрешенных издателей сертификатов.
- На экране вкладки «Веб-сервер» отображены (см. Рисунок 254) присутствуют следующие подразделы:

- Сертификат;
- Разрешенные издатели.
- В подразделе «Сертификат» в табличной форме отображена следующая информация о текущем сертификате веб-сервера:
  - в поле «Имя» - CN, указанный в сертификате;
  - в поле «Издатель» - SDN издателя сертификата;
  - в поле «Действителен до» - дата окончания действия сертификата.
- В подразделе «Разрешенные издатели» в табличной форме отображается следующая информация об издателях сертификатов:
  - в поле «Отображаемое имя» - отображаемое имя центра сертификации;
  - в поле «Издатель» - CN, указанный в сертификате центра;
  - в поле «Действителен до» - дата окончания действия сертификата центра.
  - для каждого издателя в списке в столбце «Проверка издателя» присутствует переключатель, позволяющий включить или исключить центр сертификации из списка разрешенных издателей.

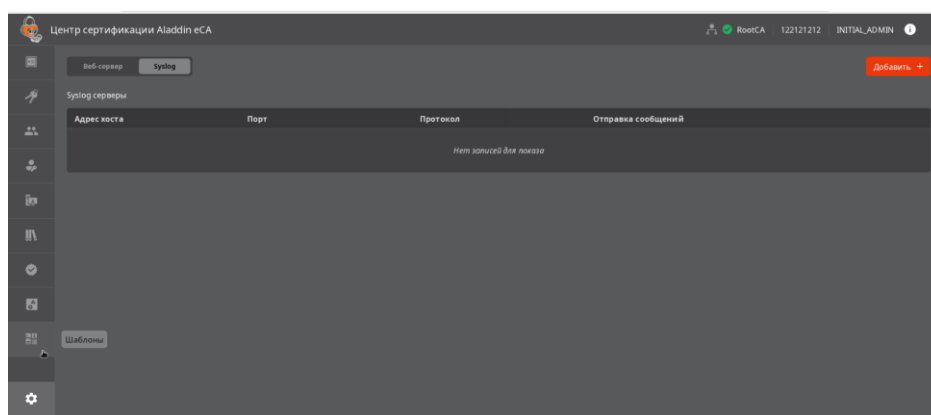



Рисунок 255 - Экран раздела «Настройки», вкладка «Syslog»

- Вкладка «Syslog» позволяет осуществлять просмотр списка и параметров Syslog-серверов, добавление Syslog-сервера в список, редактирование параметров Syslog-серверов из списка, включая управление отправкой сообщений на данный Syslog-сервер, удаление Syslog-серверов из списка.
- На экране вкладки «Syslog» (Рисунок 255) в подразделе «Syslog серверы» присутствуют следующие элементы:
  - Кнопка «Добавить», предназначенная для добавления нового Syslog-сервера в список;
  - Подраздел «Syslog-серверы».
- В подразделе «Syslog-серверы» в табличной форме содержится следующая информация:
  - в поле «Адрес хоста» - адрес хоста Syslog-сервера;
  - в поле «Порт» - порт Syslog-сервера;
  - в поле «Протокол» - протокол, по которому выполняется отправка сообщение на Syslog-сервер;
  - в поле «Отправка сообщений» присутствует переключатель, позволяющий включить или выключить отправки сообщение на данный Syslog-сервер.

### 7.13.1 Установка сертификата веб-сервера

- Предварительно необходимо выпустить сертификат для **субъекта локальной ресурсной системы** (для автоматически созданного локального субъекта при развёртывании Центра сертификации (см. 7.8.5 настоящего руководства) или нового созданного субъекта) (см. Приложение 1) со значениями в полях шаблона WEB-Server при выпуске сертификата:
  - «общее имя» – имя веб-сервера, отображаемое на экране, в разделе «Настройки», рекомендуется указать имя сервера;
  - «доменное имя» – имя хоста, на котором развёрнут Центр сертификации, должно совпадать указанным в файле `/etc/hosts`.
- Для смены ключей выберите веб-сервер и нажмите появившуюся кнопку .
- В появившемся окне (см. Рисунок 256) выберите файл сертификата и введите пароль файла контейнера, заданный при выпуске сертификата веб-сервера.
- Нажмите активировавшуюся кнопку <Сменить ключи>.

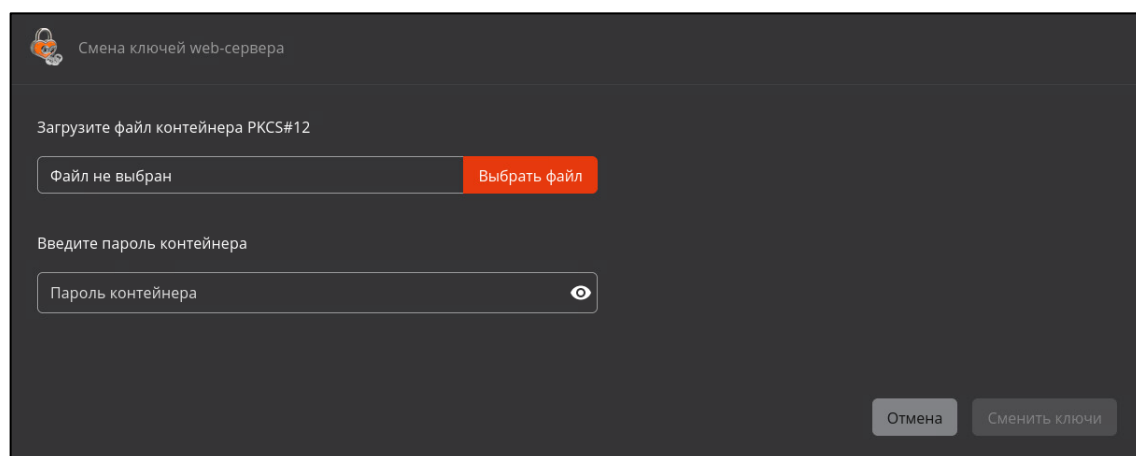


Рисунок 256 – Окно смены ключей веб-сервера

- После смены сертификата веб-сервера администратор будет уведомлён сообщением «Сертификат изменён» (см. Рисунок 257).

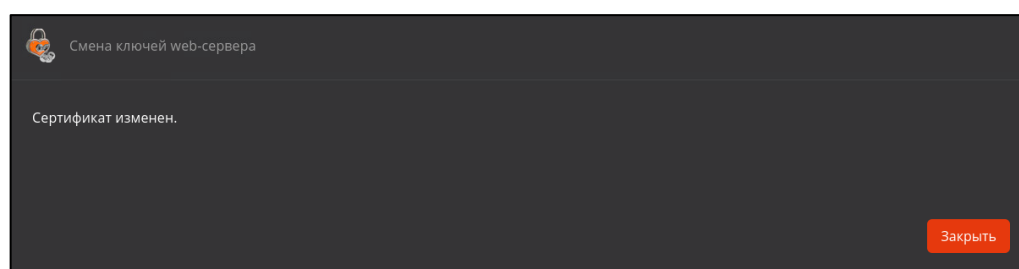


Рисунок 257 – Окно уведомления об успешной смене ключей веб-сервера

- Далее будет выполнена автоматическая перезагрузка веб-сервера. В результате перезагрузки веб-сервера в «Журнал событий» будет записано событие с кодом CAENV040 в случае успешной перезагрузки веб-сервера или событие с кодом CAENV041 в случае ошибки в процессе перезагрузки веб-сервера.
- Для установки безопасного соединения с серверной частью Центра сертификации Aladdin eCA (после установки нового сертификата веб-сервера) снова запустите браузер и выполните подключение к Центру сертификации.

- Администратору будет предложено выбрать сертификат для идентификации и аутентификации (или оставить текущий, издатель, которого активирован в «Разрешённых издателях») (см. Рисунок 258). Более подробно процедура аутентификации по сертификату приведена в разделе 6 документа RU.АЛДЕ.03.01.020 32 01-1.

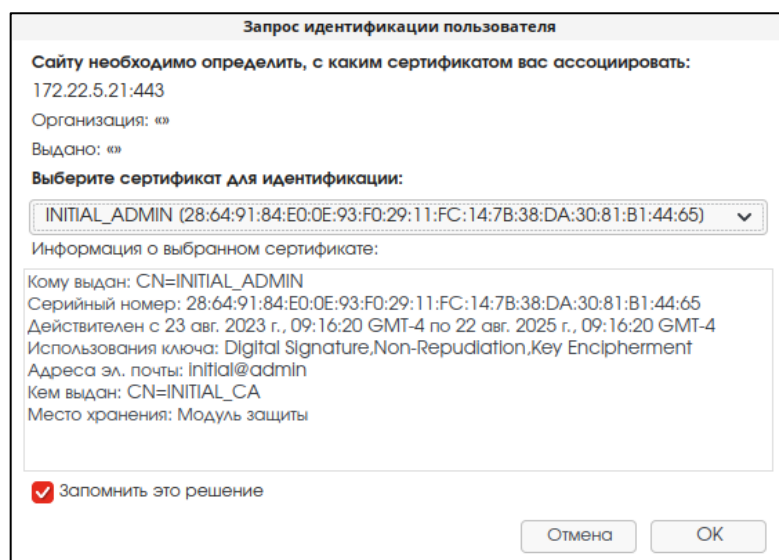




Рисунок 258 – Выбор сертификата пользователя

### 7.13.2 Разрешённые издатели

- На экранной таблице в поле «Разрешённые издатели» отображены текущие сертификаты Центров сертификации (технологического и созданного, при установке программного средства и загрузки лицензии).
- Для доступа пользователя с ролью администратор/оператор к текущему веб-серверу необходимо активировать издателя сертификата учётной записи, передвинув ползунок вправо .
- Для исключения издателя из «разрешённых» необходимо выделить издателя и деактивировать в поле «Проверка издателя», передвинув ползунок влево . С сертификатом пользователя, выпущенным исключённым издателем, аутентификация не будет успешной, в доступе к веб-серверу будет отказано.

### 7.13.3 Добавление Syslog-сервера

- Для добавления Syslog-сервера необходимо в разделе «Настройки» на вкладке «Syslog» нажать на кнопку «Добавить».
- В отобразившемся модальном окне «Добавление Syslog-сервера» (Рисунок 259) необходимо указать следующие параметры добавляемого Syslog-сервера:
  - в поле «Адрес хоста» - адрес хоста Syslog-сервера (IP-адреса или DNS-имя);

**В случае, если адрес хоста Syslog-сервера не указан, в поле «Адрес хоста» будет отображаться сообщение об ошибке «Обязательно к заполнению» (кнопка «Добавить» будет недоступна).**

**В случае, если указанный адрес хоста Syslog-сервера содержит пробел, в поле «Адрес хоста» будет отображаться сообщение об ошибке «Некорректный ввод» (кнопка «Добавить» будет недоступна).**

- в поле «Порт» - порт Syslog-сервера (число в диапазоне от 0 до 65535);

**В случае, если порт не указан, в данном поле ввода будет отображаться сообщение об ошибке «Обязательно к заполнению» (кнопка «Добавить» будет недоступна для нажатия).**

**В случае, если в поле «Порт» указано значение, не соответствующее формату ввода, в данном поле будет отображаться сообщение об ошибке «Некорректный ввод» (кнопка «Добавить» будет недоступна для нажатия).**

- в поле «Протокол» выбрать протокол UDP (указан по умолчанию) или TCP.
- после этого нажать ставшую доступной кнопку «Добавить».

Рисунок 259 – Модальное окно добавления Syslog-сервера

- После нажатия на кнопку «Добавить» в список Syslog-серверов будет добавлен новый Syslog-сервер с параметрами, указанными в модальном окне «Добавление Syslog-сервера». При этом переключатель «Отправка сообщений» у добавленного Syslog-сервера по умолчанию будет находиться во включенном состоянии.

**Если в списке уже присутствуют 10 Syslog-серверов, после нажатия на кнопку «Добавить» будет отображаться сообщение об ошибке «Ошибка. Максимальное количество Syslog-серверов – 10» (Рисунок 260). При этом новый Syslog-сервер не будет добавлен в список.**

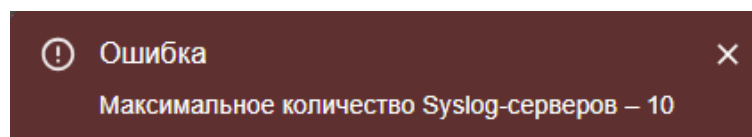


Рисунок 260 – Ошибка при превышении максимального количества Syslog-серверов

#### 7.13.4 Редактирование параметров Syslog-сервера

- Для редактирования параметров Syslog-сервера необходимо в разделе «Настройки» на вкладке «Syslog» в строке любого из имеющихся в списке Syslog-серверов нажать на кнопку «Редактировать».
- В отобразившемся модальном окне «Редактирование Syslog-сервера» (Рисунок 261) допустимо редактирование следующих параметров Syslog-сервера:
  - Адрес хоста;

**В случае, если адрес хоста Syslog-сервера не указан, в поле «Адрес хоста» будет отображаться сообщение об ошибке «Обязательно к заполнению» (кнопка «Сохранить изменения» будет недоступна).**

**В случае, если указанный адрес хоста Syslog-сервера содержит пробел, в поле «Адрес хоста» будет отображаться сообщение об ошибке «Некорректный ввод» (кнопка «Сохранить изменения» будет недоступна).**

- Порт (в формате числа в диапазоне 0-65535);

**В случае, если порт не указан, в данном поле ввода будет отображаться сообщение об ошибке «Обязательно к заполнению» (кнопка «Сохранить изменения» будет недоступна для нажатия).**

**В случае, если в поле «Порт» указано значение, не соответствующее формату ввода, в данном поле будет отображаться сообщение об ошибке «Некорректный ввод» (кнопка «Сохранить изменения» будет недоступна для нажатия).**

- Протокол (UDP или TCP).

Рисунок 261 – Модальное окно редактирования Syslog-сервера

### 7.13.5 Удаление Syslog-сервера

- Для редактирования параметров Syslog-сервера необходимо в разделе «Настройки» на вкладке «Syslog» в строке любого из имеющихся в списке Syslog-серверов нажать на кнопку «Удалить».
- В отобразившемся диалоговом окне подтверждения удаления Syslog-сервера (Рисунок 262) в строке «Удалить Syslog-сервер?» будет содержаться адрес хоста удаляемого Syslog-сервера (Рисунок 262).
- Для удаления выбранного Syslog-сервера нажать на кнопку «Удалить».

Рисунок 262 – Диалоговое окно подтверждения удаления Syslog-сервера

- После нажатия на кнопку «Удалить» в диалоговом окне подтверждения удаления Syslog-сервер будет удален из списка отображаемых на вкладке «Syslog» в разделе «Настройки». При этом должно отображаться сообщение о успешном удалении Syslog-сервера (Рисунок 263).

Рисунок 263 – Сообщение об успешном удалении Syslog-сервера

## 8 ПОИСК И УСТРАНЕНИЕ НЕИСПРАВНОСТЕЙ

Ид.	Проблема	Возможная причина	Способы решения
П001	Заблокированы кнопки выпуска сертификатов	Истёк срок действия лицензии или исчерпан лимит доступных для выпуска сертификатов	Проверьте в окне «О программе» срок действия лицензии и количество доступных для выпуска сертификатов (см. раздел 3.1)
П002	Прекращение установки ПО или обновление Aladdin eCA	1. Нехватка аппаратных ресурсов	Произведите оценку ресурса вашего ПК в соответствии с требованием к аппаратным ресурсам, указанным в первой части Руководства администратора
		2. Не корректная установка или отсутствие программного компонента, указанного в требовании	Проверьте наличие установленного ПО согласно разделу 3 Руководство администратора RU.АЛДЕ.03-01.020-01 32.  Также проверьте и при необходимости переключите текущую версию java-компонентов, выполнив команды: <pre>sudo update-alternatives --config java sudo update-alternatives --config javac sudo update-alternatives --config javap</pre>
П003	Нет подключения к ресурсной системе	1. Включен протокол TLS	Измените настройку конфигурационного файла контроллера домена <code>/etc/samba/smb.conf</code> , добавив в раздел <code>[global]</code> : <pre>ldap server require strong auth = no</pre>
		2. Проверить подключение к контроллеру домена Samba	Проверьте подключение к контроллеру домена, используя инструмент <code>ldapsearch</code> :  - получение списка пользователей <pre>ldapsearch -D "Administrator@pki-test.local" -w "Qwerty1234" -b "DC=pki-test,DC=local" -H "ldap://192.168.111.148" "(objectCategory=user)"</pre> - получение списка компьютеров <pre>ldapsearch -D "Administrator@pki-test.local" -w "Qwerty1234" -b "DC=pki-test,DC=local" -H "ldap://192.168.111.148" "(objectCategory=computer)"</pre> - получение списка групп безопасности <pre>ldapsearch -D "Administrator@pki-test.local" -w "Qwerty1234" -b "DC=pki-test,DC= pki-test" -H "ldap://192.168.111.148" "(objectCategory=group)"</pre> где: <code>Administrator@pki-test.local</code> – имя администратора домена; <code>Qwerty1234</code> – пароль администратора домена; <code>pki-test, pki-test</code> – доменное имя; <code>192.168.111.148</code> – ip-адрес контроллера домена.  В ответ на запрос вы должны получить список объектов, чтобы убедиться, что установлено соединение с ldap-сервером и он отвечает на запросы.
		3. Проверить подключение к контроллеру домена ALD PRO	Проверьте подключение к контроллеру домена, используя инструмент <code>ldapsearch</code> :  - получение списка пользователей <pre>ldapsearch -D "uid=admin,cn=users,cn=accounts,dc=domain,dc=local"</pre>



			<pre>-w "Qwerty1234" -b "dc=domain,dc=local" -H "ldap://192.168.0.10" "(objectclass=x-ald-user)"</pre> <p>- получение списка компьютеров</p> <pre>ldapsearch -D "uid=admin,cn=users,cn=accounts,dc=domain,dc=local" -w "Qwerty1234" -b "dc=domain,dc=local" -H "ldap://192.168.0.10" "(objectclass=nshost)"</pre> <p>- получение списка групп безопасности</p> <pre>ldapsearch -D "uid=admin,cn=users,cn=accounts,dc=domain,dc=local" -w "Qwerty1234" -b "dc=domain,dc=local" -H "ldap://192.168.0.10" "(objectclass=ipausergroup)"</pre> <p>где:</p> <p>users, accounts</p> <p>Qwerty1234 – пароль администратора домена;</p> <p>domain, local – доменное имя;</p> <p>192.168.111.148 – ip-адрес контроллера домена.</p> <p>В ответ на запрос вы должны получить список объектов, чтобы убедиться, что установлено соединение с ldap-сервером и он отвечает на запросы.</p>
П004	Вход в интерфейс Центра сертификации с выпущенным сертификатом невозможен в браузере Chromium	Браузер Chromium не поддерживает сертификаты с алгоритмом шифрования ECDSA512	Использовать другой браузер
П005	Вход в интерфейс Центра сертификации невозможен в браузере Firefox. Ошибка SEC_ERROR_BAD_SIGNATURE	<p>Проблема возникает при наличии в хранилище сертификатов ОС сертификата ЦС с аналогичным SDN издателю сертификата веб-сервера.</p> <p>Она связана с алгоритмом проверки сертификата веб-сервера браузером Firefox для решения уязвимости, связанной с подлогом серверного сертификата:</p> <ol style="list-style-type: none"> <li>1. Firefox получает сертификат веб-сервера от сервера</li> <li>2. После этого выполняет поиск в хранилище сертификатов ОС сертификата ЦС по SDN издателя сертификата</li> <li>3. И далее выполняет проверку цепочки по открытым ключам</li> </ol>	<ol style="list-style-type: none"> <li>1. Проверьте состав сертификатов доверенных ЦС в хранилище ОС</li> <li>2. В случае несоответствия установите сертификат издателя сертификата веб-сервера</li> </ol>
П006	Вход в интерфейс Центра сертификации невозможен. Ошибка 500	Удалён сертификат технологического ЦС	<p>Проверить файл <code>opt/aeca/p12/truststore.jks</code> на предмет содержания записи о сертификате технологического центра сертификации, созданного при установке ПО Aladdin eCA.</p> <p>Запись о сертификате технологического ЦС следующего вида:</p> <pre>keytool -import -alias managementca -file cert.pem - keystore ./truststore.jks</pre> <p>где <code>cert.pem</code> – сертификат технологического ЦС, может быть получен в результате конвертации контейнера PKCS#12 <code>opt/aeca/p12/superadmin.p12</code>:</p>

			<pre>openssl pkcs12 -in superadmin.p12 -out cert.pem -nodes -clcerts</pre> <p>Пароль контейнера сертификата технологического ЦС указан в файле <code>/opt/aeca/generated_passwords.txt</code></p>
П007	Невозможно подключиться к токenu для выпуска сертификата после установки JC-WebClient. Сообщение «ПО JCWebClient не установлено»	Требуется разрешить ПО JC-WebClient доступ к ресурсу	<p>1. В адресную строку браузера введите: <code>https://localhost:24738/admin/token_manager.html</code></p> <p>2. Во всплывающем окне предупреждения браузера подтвердите действия.</p>
П008	Пустой файл шаблонов по завершению работы скрипта <code>mcs2aeca.ps1</code> экс порта шаблонов MSCS	Требуется настройка <code>tls</code>	<p>Откройте Powershell от имени администратора и задайте версию протокола безопасности, выполнив команду:</p> <pre>[Net.ServicePointManager]::SecurityProtocol = [Net.SecurityProtocolType]::Tls12</pre>
П009	Невозможно применить выпущенный Центром сертификации Aladdin eCA сертификат в операционной системе Windows (в частности, WinServer2012/2016)	Сертификат доступа сгенерирован с использованием алгоритма хеширования sha256, и операционная система Windows не поддерживает данный алгоритм	<p>Конвертируйте сертификат, сгенерированный с использованием алгоритма хеширования sha256, в формате .p12 в формат .pem с помощью openssl:</p> <pre>openssl pkcs12 -in &lt;имя контейнера&gt;.p12 -out &lt;имя декодированного файла&gt;.pem</pre> <pre>openssl pkcs12 -keypbe PBE-SHA1-3DES -certpbe PBE-SHA1-3DES -export -in &lt;имя декодированного файла&gt;.pem -out &lt;имя контейнера&gt;.p12</pre>
П010	Ошибка Cannot read properties of undefined (reading 'data')	Установленное ранее ssl соединение недействительно. Возникает, если в момент обновления сертификата веб-сервера было открыто несколько вкладок, либо был перезапущен (по каким-либо причинам) веб-сервер	Перезагрузите страницу браузера
П011	Ошибка запроса к стороннему сервису. ...	Ошибка подключения к Центру сертификации по протоколу https	Выполните настройку безопасного соединения согласно разделу 5 «Безопасность соединения» настоящего руководства
П012	Не удается выполнить авторизацию при ресурсной системе ALD PRO/FreeIPA. Сообщение: «Не удалось проверить цепочку сертификатов»	Клиент вводился в домен до обновления конфигурации сертификатов домена	<p>На клиенте выполнить команды:</p> <pre>sudo kinit &lt;администратор домена&gt;</pre> <pre>sudo ipa-certupdate</pre> <p>И повторить попытку авторизации.</p>
П013	Периодическая остановка или падение службы aecaservice	Недостаток оперативной памяти на хосте	<p>1. Проверьте потребление оперативной памяти на хосте с помощью команды <code>top</code>:</p> <ul style="list-style-type: none"> <li>- в <code>MiB Mem</code> значение <code>total</code> – это общий объем оперативной памяти;</li> <li>- в <code>MiB Mem</code> значение <code>free</code> – это свободная оперативная память;</li> <li>- в строке таблицы <code>USER=aeca</code> значение в колонке <code>RES</code> – это потребляемая ЦС оперативная память.</li> </ul>

Для корректной работы ЦС сумма `free` и `RES` должна быть не менее 10 Гб<sup>37</sup>.

2. Если полученное значение меньше 10 Гб, то при исчерпании свободной оперативной памяти `oom-killer` останавливает ЦС. В данном случае рекомендуется проанализировать состав стороннего ПО на хосте и его потребление памяти, например, с помощью команд `top` или `htop`.

3. После этого следует либо добавить необходимое количество оперативной памяти, либо удалить с хоста стороннее ПО, освободив этим оперативную память.

---

<sup>37</sup> Требования к аппаратному обеспечению см. в разделе 2.2 Руководства администратора. Часть 1. Установка и обслуживание Центра сертификации Aladdin Enterprise Certification Authority.

## ПРИЛОЖЕНИЕ 1. СОЗДАНИЕ СЕРТИФИКАТА ДЛЯ СУБЪЕКТА

**Внимание!** Создание сертификата с закрытым ключом PKCS#12 и создание сертификата на ключевом носителе возможны только для существующего субъекта локальной (см. подраздел 7.8.5 настоящего руководства) или подключенных ресурсных систем (см. подраздел 7.8.6 настоящего руководства)!

Создание сертификата субъекта по запросу, возможно как для существующего предварительно созданного локального субъекта (см. подраздел 7.8.5.1 настоящего руководства) или субъекта внешней ресурсной системы (см. подраздел 7.8.6 настоящего руководства), так и субъекта, создаваемого в процессе выпуска сертификата. При этом субъект на основании запроса будет создан только при успешном создании для него сертификата создаваемого в процессе выпуска сертификата.

**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!

### 1.1 Способы создания сертификатов

- На вкладке «Сертификаты» при нажатии на кнопку <Создать сертификат> доступен выпуск сертификата (см. Рисунок 264):
  - с закрытым ключом для существующего субъекта;
  - на основании запроса;
  - на ключевом носителе.

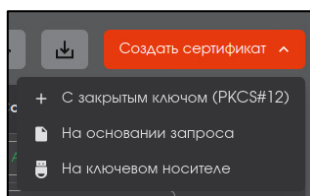


Рисунок 264 - Кнопка «Создать сертификат» на вкладке «Сертификаты»

- На вкладке «Учётные записи» при выделении строки учётной записи и нажатии кнопки <Создать сертификат> доступен выпуск сертификата для учётной записи (см. Рисунок 265):
  - с закрытым ключом;
  - на основании запроса;
  - на ключевом носителе.

Сертификат будет создан с использованием внутреннего шаблона ECA-Auth. Значение поля «Common Name» будет заполнено автоматически и соответствовать логину учетной записи, для которой выпускается сертификат.

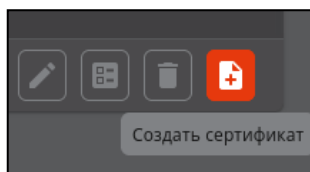


Рисунок 265 - Кнопка «Создать сертификат» на вкладке «Учётные записи»

- На вкладке «Субъекты» при выделении строки субъекта и нажатии кнопки «Создать сертификат» доступен выпуск сертификата (см. Рисунок 266):
  - с закрытым ключом;
  - на основании запроса;
  - на ключевом носителе.

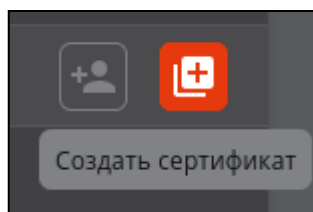


Рисунок 266 - Кнопка «Создать сертификат» на вкладке «Субъекты»

- В результате нажатия на кнопку создания сертификата появится окно создания сертификата.

## 1.2 Параметры криптографии сертификатов учётных записей пользователей и Центров сертификации

В таблице определены комбинации сертификатов Центра сертификации, к которому происходит подключение пользователя (оператора/администратора), и используемого для аутентификации сертификата учётной записи пользователя, при которых будет происходить успешная аутентификация пользователя Aladdin eCA.

Таблица 27 – Успешные комбинации сертификатов Центра сертификации и учётной записи пользователя при аутентификации на сервере

Операционная система	Алгоритм и длина ключа сертификата Центра сертификации	Алгоритм и длина ключа сертификата учётной записи пользователя
Astra Linux Special Edition 1.7 Смоленск	RSA: 2048-4096, SHA256-SHA512	RSA: 2048-8196. ECDSA: 256-521 ГОСТ Р 34.10-2012 <sup>38</sup> : 256-512
	ECDSA: 256-521, SHA256-SHA512	
	ГОСТ Р 34.10-2012: 256-512, ГОСТ Р 34.11-2012	
Astra Linux Special Edition версия 1.8 Смоленск	RSA: 2048-4096, SHA256-SHA512	RSA: 2048-8196. ECDSA: 256-521 ГОСТ Р 34.10-2012 <sup>39</sup> : 256-512
	ECDSA: 256-521, SHA256-SHA512	
	ГОСТ Р 34.10-2012: 256-512, ГОСТ Р 34.11-2012	

<sup>38</sup> Аутентификация пользователя Aladdin eCA по сертификату с алгоритмом ключа ГОСТ Р 34.10-2012 доступна только при наличии подключения Aladdin eCA к СКЗИ «КриптоПро CSP» и использовании «српнх» в качестве веб-сервера для Aladdin eCA.

<sup>39</sup> Аутентификация пользователя Aladdin eCA по сертификату с алгоритмом ключа ГОСТ Р 34.10-2012 доступна только при наличии подключения Aladdin eCA к СКЗИ «КриптоПро CSP» и использовании «српнх» в качестве веб-сервера для Aladdin eCA.

РЕД ОС 7.3	RSA: 2048-4096, SHA1-SHA512	RSA: 1024-8196. ECDSA: 256-521 ГОСТ Р 34.10-2012 <sup>40</sup> : 256-512
	ECDSA: 256-521, SHA1-SHA512	
	ГОСТ Р 34.10-2012: 256-512, ГОСТ Р 34.11-2012	
РЕД ОС 8	RSA: 2048-4096, SHA1-SHA512	RSA: 1024-8196. ECDSA: 256-521 ГОСТ Р 34.10-2012 <sup>41</sup> : 256-512
	ECDSA: 256-521, SHA1-SHA512	
	ГОСТ Р 34.10-2012: 256-512, ГОСТ Р 34.11-2012	
ОС Альт 8 СП, релиз 10, Сервер	RSA: 2048-4096, SHA1-SHA512	RSA: 1024-8196. ECDSA: 256-521 ГОСТ Р 34.10-2012 <sup>42</sup> : 256-512
	ECDSA: 256-521, SHA1-SHA512	
	ГОСТ Р 34.10-2012: 256-512, ГОСТ Р 34.11-2012	

### 1.3 Публикация сертификата в ресурсную систему

- После успешного создания сертификата при 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 (см. чек-бокс «Публиковать сертификат в ресурсную систему» в подразделе 7.12.3.1).

В случае успешной публикации сертификата в ресурсную систему отобразится всплывающее сообщение «Сертификат успешно опубликован в ресурсную систему». В журнал событий записывается событие с кодом CAENV048.

В случае ошибки публикации сертификата в ресурсную систему отобразится всплывающее сообщение «Ошибка публикации сертификата в ресурсную систему». В журнал событий записывается событие с кодом CAENV049. Также сертификат будет помечен, как требующий публикации.

<sup>40</sup> Аутентификация пользователя Aladdin eCA по сертификату с алгоритмом ключа ГОСТ Р 34.10-2012 доступна только при наличии подключения Aladdin eCA к СКЗИ «КриптоПро CSP» и использовании «српгiнх» в качестве веб-сервера для Aladdin eCA.


<sup>41</sup> Аутентификация пользователя Aladdin eCA по сертификату с алгоритмом ключа ГОСТ Р 34.10-2012 доступна только при наличии подключения Aladdin eCA к СКЗИ «КриптоПро CSP» и использовании «српгiнх» в качестве веб-сервера для Aladdin eCA.

<sup>42</sup> Аутентификация пользователя Aladdin eCA по сертификату с алгоритмом ключа ГОСТ Р 34.10-2012 доступна только при наличии подключения Aladdin eCA к СКЗИ «КриптоПро CSP» и использовании «српгiнх» в качестве веб-сервера для Aladdin eCA.

- ЦС Aladdin eCA выполняет автоматическую публикацию сертификатов, требующих публикации при включенном флаге `ldap_automatically_certificates_publication_enable` по расписанию, заданному в параметре `ldap_automatically_certificates_publication_cron` (в конфигурационном файле `/opt/aecaCa/scripts/config.sh`). Также для выполнения публикации необходимо, чтобы владельцем сертификата являлся подключенный к ресурсной системе субъект. При успешной публикации с сертификата снимается пометка, что он требует публикации.
- Сертификат публикуется в формате LDIF в атрибут `userCertificate` (для ресурсных систем Samba DC, Альт Домен и MS AD) и `userCertificate;binary` (для ресурсных систем ALD Pro и FreeIPA) выбранного субъекта ресурсной системы, для которого выпущен сертификат, путём добавления, а не перезаписи атрибута.
- Для успешной публикации сертификатов в ресурсную систему ALD Pro и FreeIPA требуется подключение к ресурсной системе от имени пользователя, с минимальным набором прав пользователя:
  - наличие роли «Service Role» для подключения к ресурсной системе;
  - наличие роли «helpdesk» или роли «User Administrator» для публикации сертификатов пользователей;
  - наличие роли «Enrollment Administrator» для публикации сертификатов контроллеров домена.

## 1.4 Создание сертификата с закрытым ключом PKCS#12

**Создание сертификата возможно только для существующего субъекта! Предварительно создайте локальный субъект (см. подраздел 7.8.5.1 настоящего руководства) или выберите субъект внешней ресурсной системы (см. подраздел 7.8.6 настоящего руководства).**

- В появившемся окне (см. Рисунок 267):
  - при выпуске сертификата в разделе «Сертификаты» необходимо на шаге 1 ввести частичное или полное значение любого атрибута субъекта, для которого будет выпущен сертификат;
  - поиск субъектов выполняется по значениям в их атрибутах и является регистронезависимым;
  - в результате будут отображены найденные субъекты с указанием краткой информации:
    - «CN» – значение атрибута «Common Name» субъекта;
    - «ID» – идентификатор субъекта;
    - «UPN» – значение атрибута «MS UPN, User Principal Name» субъекта;
    - «DNS» – значение атрибута «DNS Name» субъекта;
    - пиктограммы наличия подключения субъекта к ресурсной системе  (см. Рисунок 267).
  - в результате поиска в полях «CN», «UPN» и «DNS» отображаются все значения соответствующего полю атрибута субъекта, разделитель значений в поле – запятая с пробелом;
  - в результате поиска поля «CN», «UPN» и «DNS» не отображаются, если в соответствующем данному полю атрибуте у субъекта отсутствуют значения;
  - выберите субъект и нажмите кнопку «Продолжить» для перехода к шагу 1;
  - при выпуске сертификата в разделах «Субъекты» и «Учётные записи» шаг 1 не требуется и первым шагом будет выбор шаблона для выпуска сертификата (см. Рисунок 268).

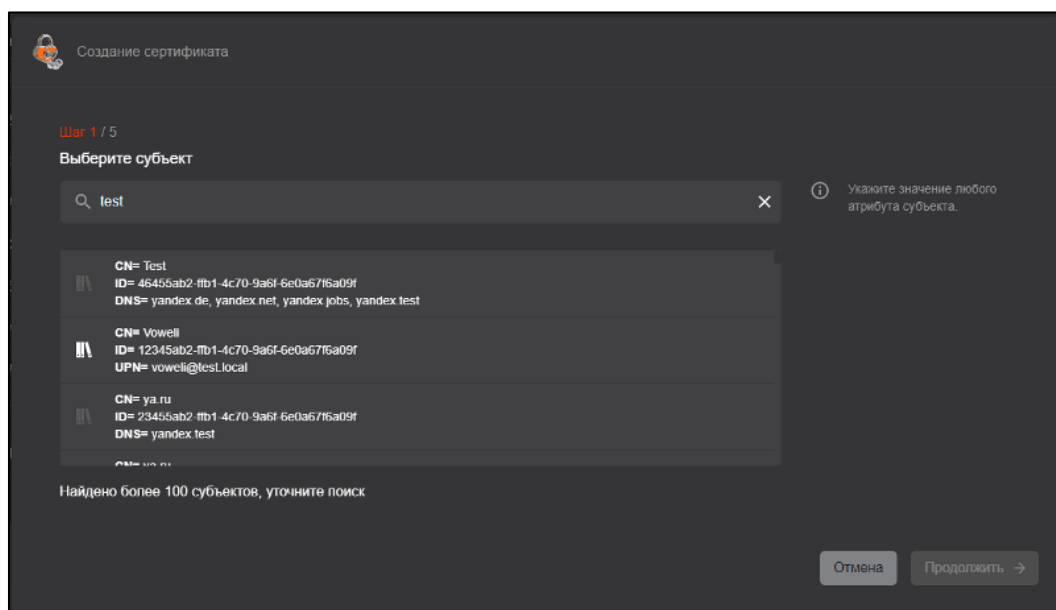


Рисунок 267 - Окно создания сертификата PKCS#12. Шаг 1. Поиск субъекта

- В открывшемся окне (см. Рисунок 268) необходимо выбрать шаблон из выпадающего списка в поле «Выберите шаблон» для выпуска 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 (см. подраздел 7.12 настоящего руководства). 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 выпуске сертификата из раздела «Учётные записи» шаблон будет определён по умолчанию и выбору не подлежит. Переход на следующий шаг осуществляется по ставшей активной кнопке «Продолжить» после выбора шаблона.

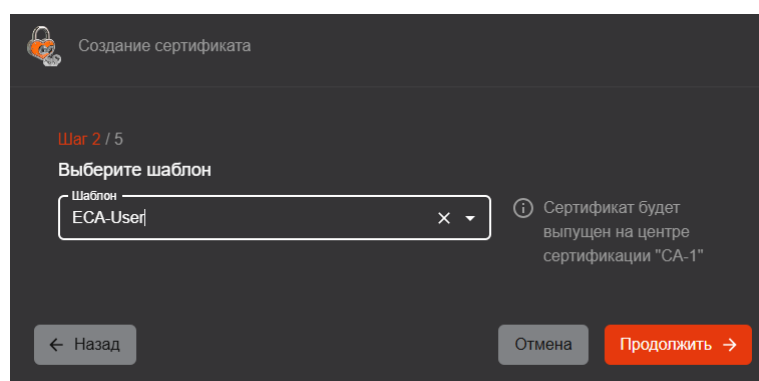




Рисунок 268 - Окно создания сертификата PKCS#12. Шаг 2. Выбор шаблона сертификата

- В окне Шага 3 указаны атрибуты в соответствии с выбранным (на предыдущем шаге) шаблоном сертификата (подробное описание полей предустановленных шаблонов см. в Приложение 2. Описание полей предустановленных шаблонов сертификатов). Значение атрибутов заполняется автоматически в соответствии с данными в карточке субъекта (см. подраздел 7.8.4 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 становится активной – красного цвета). Также дополнительно добавленное значение атрибута можно удалить по кнопке  справа от соответствующего поля атрибута (см. Рисунок 269).

- Если данные атрибутов отсутствуют, то необходимо ввести значения в соответствующие поля в карточке субъекта (см. раздел 7.8.4 настоящего руководства).
- Необязательные поля могут оставаться незаполненными.
- Нажмите ставшую активной кнопку <Продолжить> для перехода к следующему шагу.

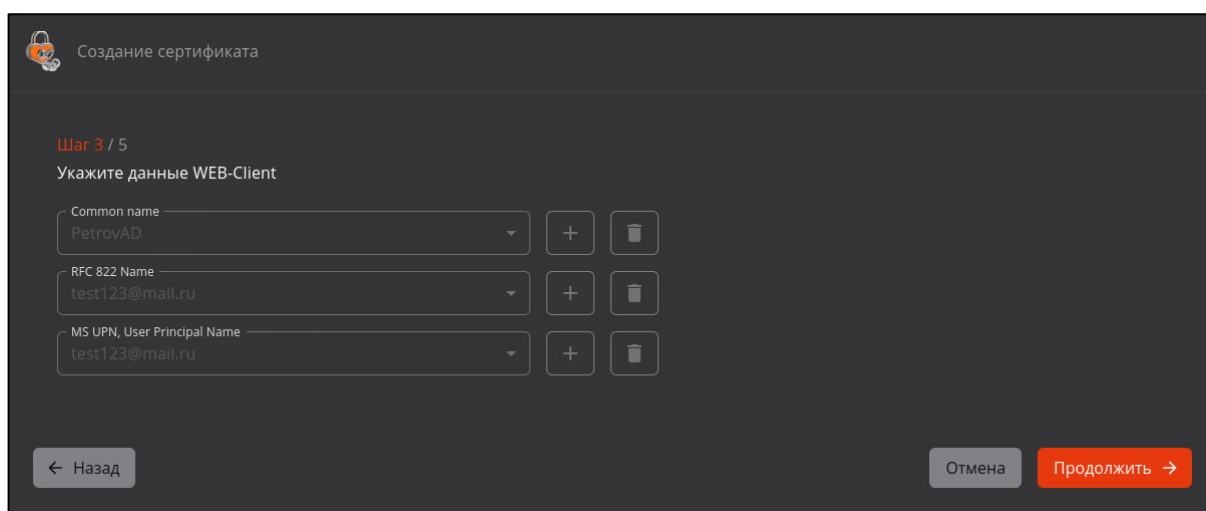



Рисунок 269 - Окно создания сертификата PKCS#12. Шаг 3. Атрибуты сертификата

- Далее необходимо создать пароль с подтверждением (см. Рисунок 270) в соответствии с правилами 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.

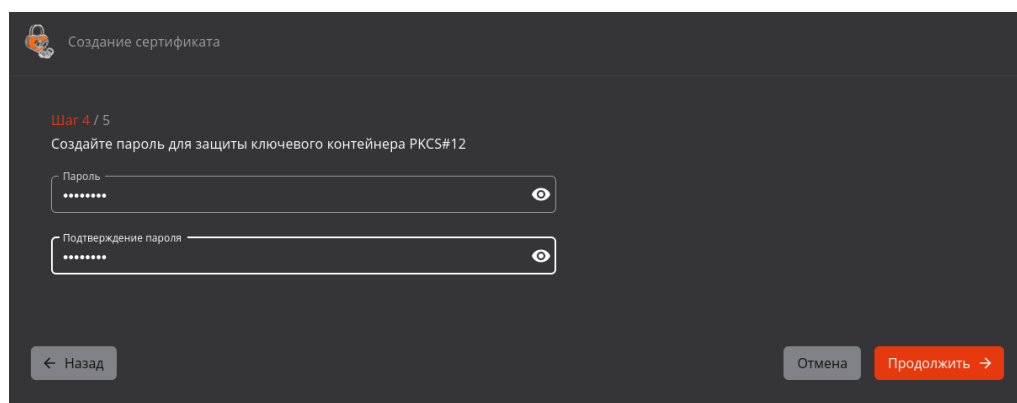


Рисунок 270 - Окно создания сертификата PKCS#12. Шаг 4. Ввод пароля контейнера

- Далее необходимо выбрать параметры криптографии из выпадающего списка значений алгоритма ключа (см. Рисунок 271). По умолчанию выбрано значение «RSA-2048».

**Доступные алгоритмы определяются выбранным шаблоном (если криптопровайдер алгоритма не заявлен в шаблоне, его выбор будет недоступен), а также зависят от криптопровайдеров центра сертификации<sup>43</sup>, 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>.

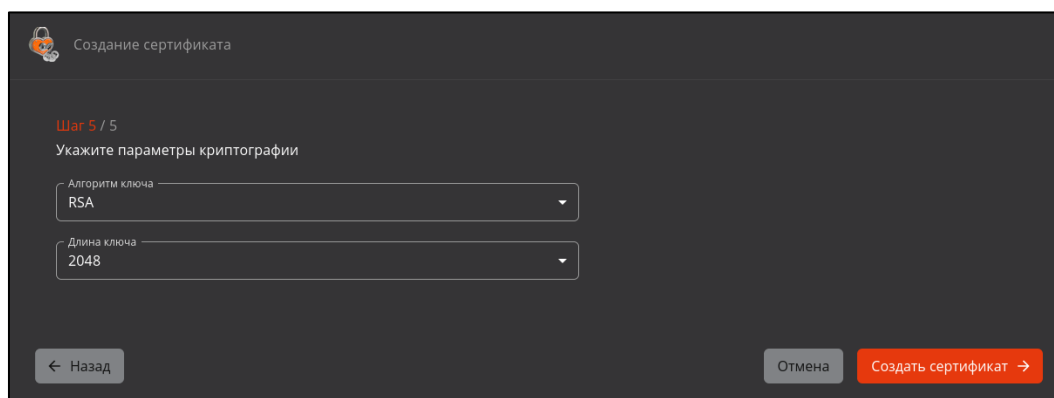


Рисунок 271 – Окно создания сертификата PKCS#12. Шаг 5. Выбор параметров криптографии

- Далее по нажатию кнопки <Создать сертификат> открывается финальное окно создания сертификата и отображается краткая информация о созданном сертификате (см. Рисунок 289).

**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.**

<sup>43</sup> Выбор криптопровайдеров осуществляется при создании центра сертификации.

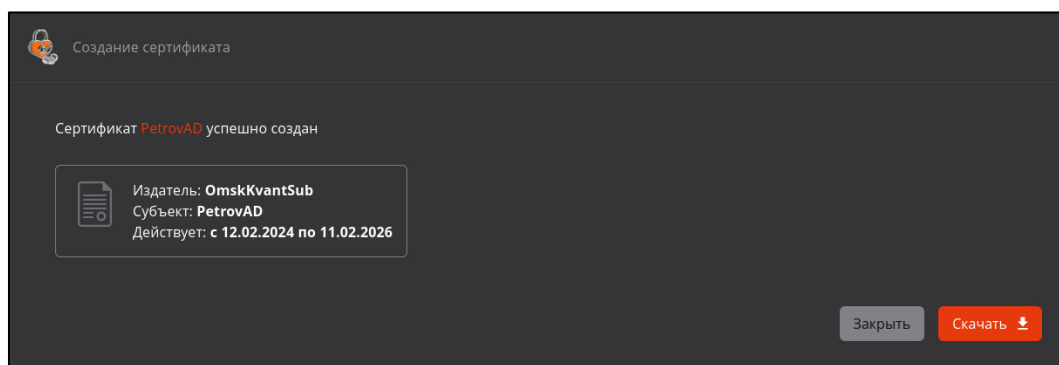


Рисунок 272 – Окно создания сертификата PKCS#12. Информирование об успешном создании сертификата

- В результате выпуска сертификата с закрытым ключом PKCS#12 для существующего субъекта сгенерирована ключевая пара в соответствии с заданными параметрами криптографии.
- При успешном создании сертификата и выполнении всех условий ниже происходит его публикация в ресурсную систему (подробнее см. п 1.3 Публикация сертификата в ресурсную систему):
  - сертификат был создан для субъекта, подключенного к ресурсной системе;
  - сертификат создан по шаблону, в котором включена публикация сертификата в ресурсную систему.

## 1.5 Создание сертификата субъекта по запросу

**Создание сертификата возможно как для существующего предварительно созданного локального субъекта (см. подраздел 7.8.5.1 настоящего руководства) или субъекта внешней ресурсной системы (см. подраздел 7.8.6 настоящего руководства), так и субъекта, создаваемого в процессе выпуска сертификата. При этом субъект на основании запроса будет создан только при успешном создании для него сертификата.**

- Предварительные условия выполнения сценария:
  - файл-запрос для субъекта должен быть подготовлен заранее в стороннем центре сертификации (например, при помощи ПО «Единый клиент JaCarta»);
  - расширение файл-запроса должно быть `***.csr` или `***.req`;
  - 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.

### 1.5.1 Создание сертификата субъекта по запросу в разделе «Сертификаты»

В разделе «Сертификаты» после нажатия на кнопку «Создать сертификат» в выпадающем списке выберите функцию «На основании запроса».

- В открывшемся окне (см. Рисунок 273) загрузите файл-запрос (загружается по кнопке <Выбрать файл>).

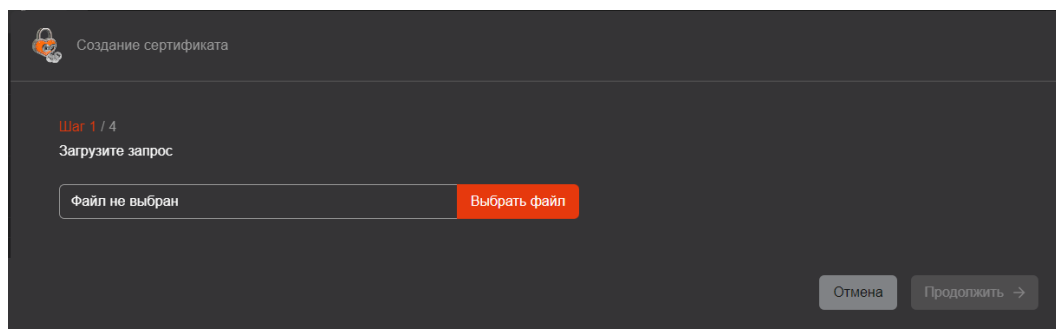


Рисунок 273 – Окно создания сертификата по запросу в разделе «Сертификаты». Шаг 1. Загрузка запроса

- После выбора файла-запроса на данном шаге автоматически выполняется поиск субъекта по CN, указанному в файле-запроса:
  - Если найден всего один субъект, то на данном шаге под полем выбора файла отображается текст «По данным в запросе найден субъект CN (ID: subjectID)», где CN – значение атрибута CN субъекта, а subjectID – идентификатор данного субъекта. А также опции выбора субъекта, для которого будет создан сертификат (см. Рисунок 274):
    - «Создать сертификат для субъекта CN (ID: subjectID)», где CN – значение атрибута CN субъекта, а subjectID – идентификатор данного субъекта. Данная опция выбрана по умолчанию. Выберите данную опцию, чтобы создать сертификат для указанного субъекта;
    - «Создать сертификат для нового субъекта». Выберите данную опцию, чтобы создать сертификат для нового субъекта, который будет создан на основании данных запроса.

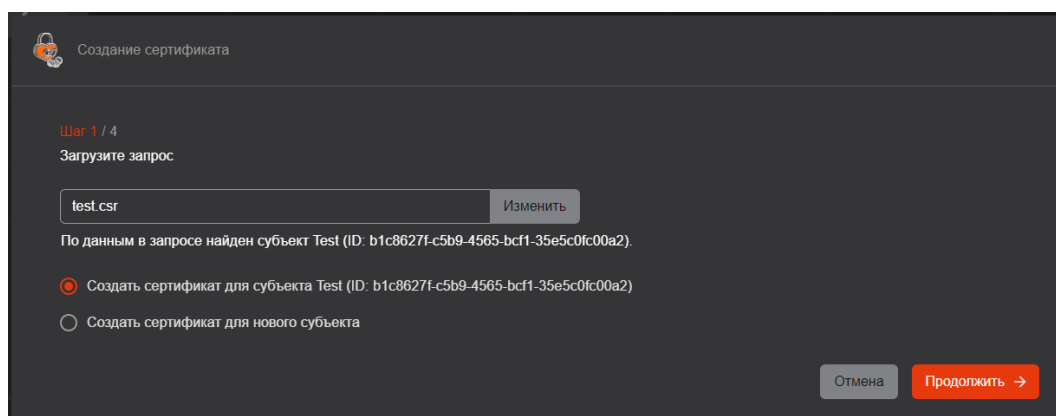


Рисунок 274 – Окно создания сертификата по запросу в разделе «Сертификаты». Шаг 1. Загрузка запроса. Найден один субъект

- Если найдено несколько субъектов, на данном шаге под полем выбора файла отображается текст «По данным в запросе найдено несколько субъектов». А также опции выбора субъекта, для которого будет создан сертификат (см. Рисунок 275):
  - «Выбрать субъект на следующем шаге». Данная опция выбрана по умолчанию. Выберите данную опции, чтобы на следующем шаге выбрать субъект, для которого будет создан сертификат<sup>44</sup>;
  - «Создать сертификат для нового субъекта». Выберите данную опцию, чтобы создать сертификат для нового субъекта, который будет создан на основании данных запроса.

<sup>44</sup> Если данная опция выбрана, общее количество шагов в данном сценарии будет увеличено на 1, так как будет присутствовать шаг 2/5 с выбором субъекта. При выборе других опций на шаге 1 общее количество шагов сценария не изменится и будет составлять 4, так как шаг 2/5 будет отсутствовать

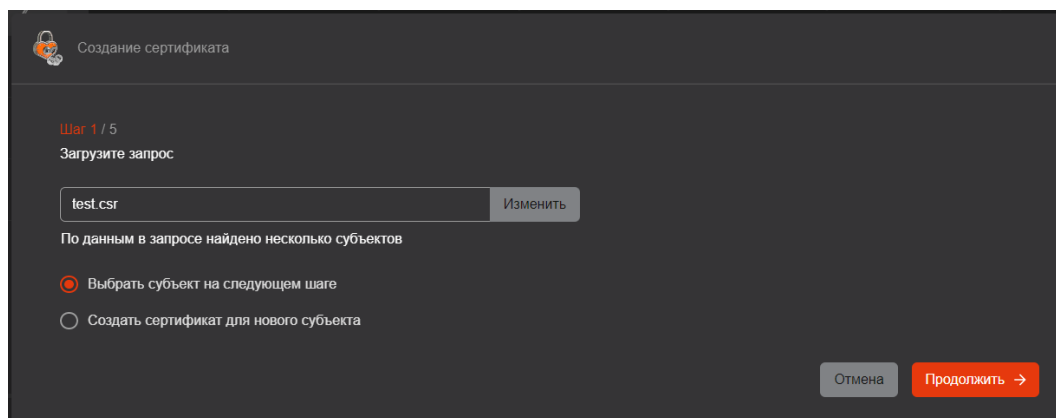


Рисунок 275 – Окно создания сертификата по запросу в разделе «Сертификаты». Шаг 1. Загрузка запроса. Найдено несколько субъектов

- Если не найден ни один субъект, то на данном шаге под полем выбора файла отображается текст «По данным в запросе не найдены субъекты. Сертификат будет создан для нового субъекта» (см. Рисунок 276). Далее по сценарию сертификат будет создаваться для нового субъекта, который будет создан на основании данных запроса;

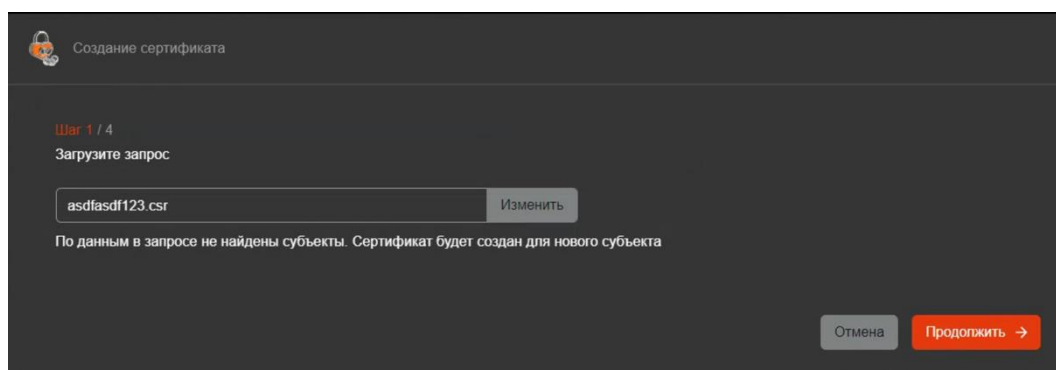



Рисунок 276 – Окно создания сертификата по запросу в разделе «Сертификаты». Шаг 1. Загрузка запроса. Не найден ни один субъект

- Если по данному запросу ранее уже был выпущен сертификат, в поле загрузки файла отображается сообщение об ошибке «По данному запросу уже был выпущен сертификат». При этом кнопка «Продолжить» недоступна для нажатия, и необходимо либо выбрать другой файл-запроса, либо отменить создание сертификата.
- Переход на шаг 2 возможен только при условии, что на шаге 1 была выбрана опция «Выбрать субъект на следующем шаге», иначе шаг 2 будет пропущен и произойдет переход сразу к шагу 3<sup>45</sup>. Нажмите кнопку <Продолжить> для перехода к следующему шагу.
- (Шаг 2/5) В появившемся окне (см. Рисунок 277):
  - отображается поисковая строка, в которой автоматически указан CN из импортированного на предыдущем шаге запроса, а также субъекты, соответствующие критерию поиска;
  - при этом указанное автоматически значение в поисковой строке может быть изменено, и можно ввести частичное или полное значение любого атрибута субъекта, для которого будет выпущен сертификат;
  - поиск субъектов выполняется по значениям в их атрибутах и является регистронезависимым;

<sup>45</sup> При пропуске шага 2 общее количество шагов станет 4, а нумерация шагов сдвинется: шаг 3/5 станет шагом 2/4, шаг 4/5 – шагом 3/4, шаг 5/5 – шагом 4/4.

- в списке субъектов для каждого субъекта отображается краткая информация, содержащая:
  - «CN» – значение атрибута «Common Name» субъекта;
  - «ID» – идентификатор субъекта;
  - «UPN» – значение атрибута «MS UPN, User Principal Name» субъекта;
  - «DNS» – значение атрибута «DNS Name» субъекта;
  - пиктограммы наличия подключения субъекта к ресурсной системе CN, UPN (при наличии), ID и пиктограмму, отображающая наличие подключения субъекта к ресурсной системе 
- в результате поиска в полях «CN», «UPN» и «DNS» отображаются все значения соответствующего полю атрибута субъекта, разделитель значений в поле – запятая с пробелом;
- в результате поиска поля «CN», «UPN» и «DNS» не отображаются, если в соответствующем данному полю атрибуте у субъекта отсутствуют значения;
- выберите субъект и нажмите кнопку <Продолжить> для перехода к следующему шагу;

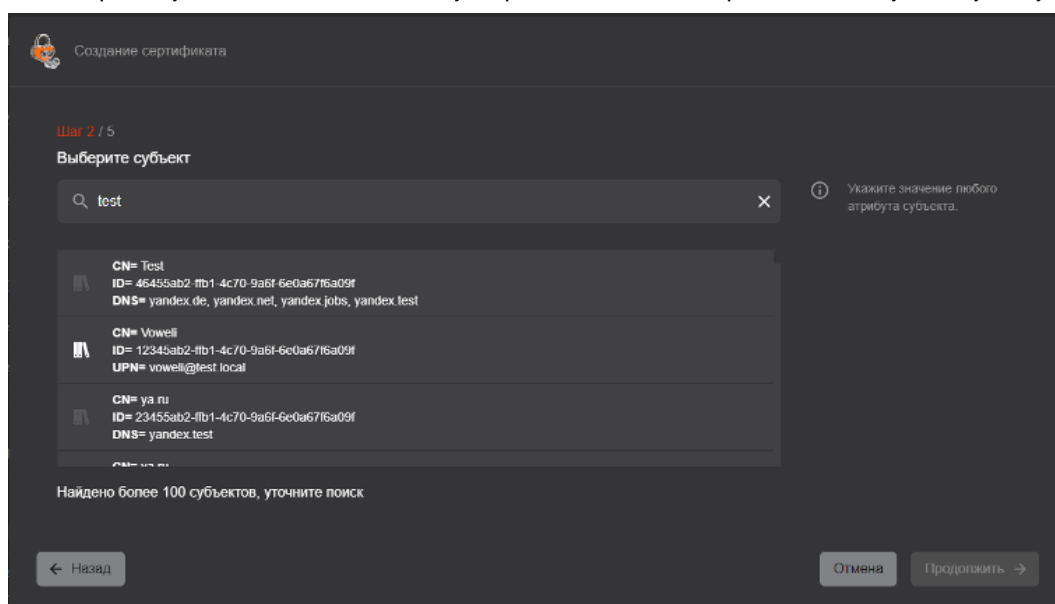


Рисунок 277 – Окно создания сертификата по запросу в разделе «Сертификаты». Шаг 2. Выбор субъекта

- (Шаг 2/4 или 3/5) В появившемся окне (см. Рисунок 278) выберите шаблон, на основании которого будет создан сертификат (предполагается, что администратор заранее знает какой шаблон необходимо выбрать). 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 (см. подраздел 7.12 настоящего руководства). 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.

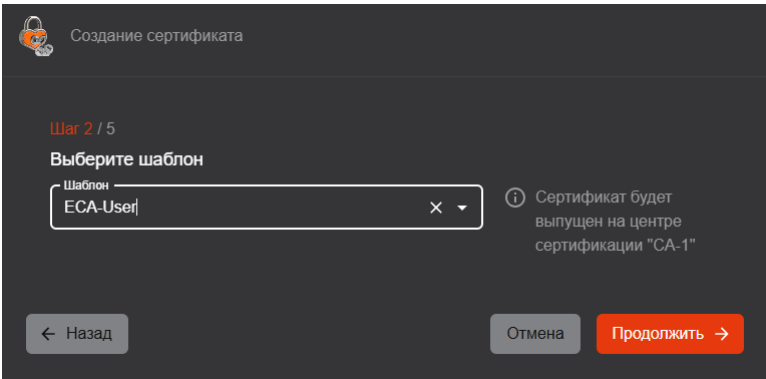


Рисунок 278 – Окно создания сертификата по запросу в разделе «Сертификаты». Шаг 3. Выбор шаблона

- После выбора шаблона нажмите кнопку <Продолжить> для перехода к следующему шагу.
- (Шаг 3/4 или 4/5) Программа проверяет запрос на соответствие полей запроса на сертификат и атрибутов субъекта по правилам, приведённым в Таблица 28. Проверка является регистронезависимой. При этом в случае, если в процессе выпуска сертификата по запросу создается новый субъект, то валидация значений из полей запроса на соответствие атрибутам субъекта не производится (и возможность возникновения ошибки №4 из Таблица 28 исключена).

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 279 и Рисунок 280).

Перечень возможных ошибок представлен в Таблица 29.


Таблица 28 – 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 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


Поле в шаблоне	Значение поля в запросе	Атрибут субъекта АЕСА	Возможность создания сертификата	Поле в сертификате	Возможные ошибки*
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
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	-








Поле в шаблоне	Значение поля в запросе	Атрибут субъекта АЕСА	Возможность создания сертификата	Поле в сертификате	Возможные ошибки*
Нет	Есть	Нет	Да	Отсутствует	Ошибка №3
Нет	Нет	Нет	Да	Отсутствует	-
Нет	Есть	Есть	Да	Отсутствует	Ошибка №3
Нет	Нет	Есть	Да	Отсутствует	-


Создание сертификата

Шаг 3 / 4


Невозможно создать сертификат по запросу **Dena Marshall** по шаблону **WEB-Client**

Измените данные запроса или выберите другой шаблон.

Поля	В шаблоне	Значение из запроса	Значение в сертификате
Различающееся имя субъекта			
CN		Anton	 Значение в поле не соответствует значению атрибута субъекта
Альтернативное имя субъекта			
RFC822NAME		email@address.com	 Значение в поле не соответствует значению атрибута субъекта
DNS_NAME		www.domain.com	 Поле отсутствует в шаблоне
MS_UPN		email@address.com	 Значение в поле не соответствует значению атрибута субъекта
MS_GUID		e4134486122d452495c771503eabf73f	 Поле отсутствует в шаблоне

← Назад

Отмена

Продолжить →

Рисунок 279 – Окно создания сертификата по запросу в разделе «Сертификаты». Шаг 4. Результат обработки запроса с ошибкой в поле различающегося имени субъекта

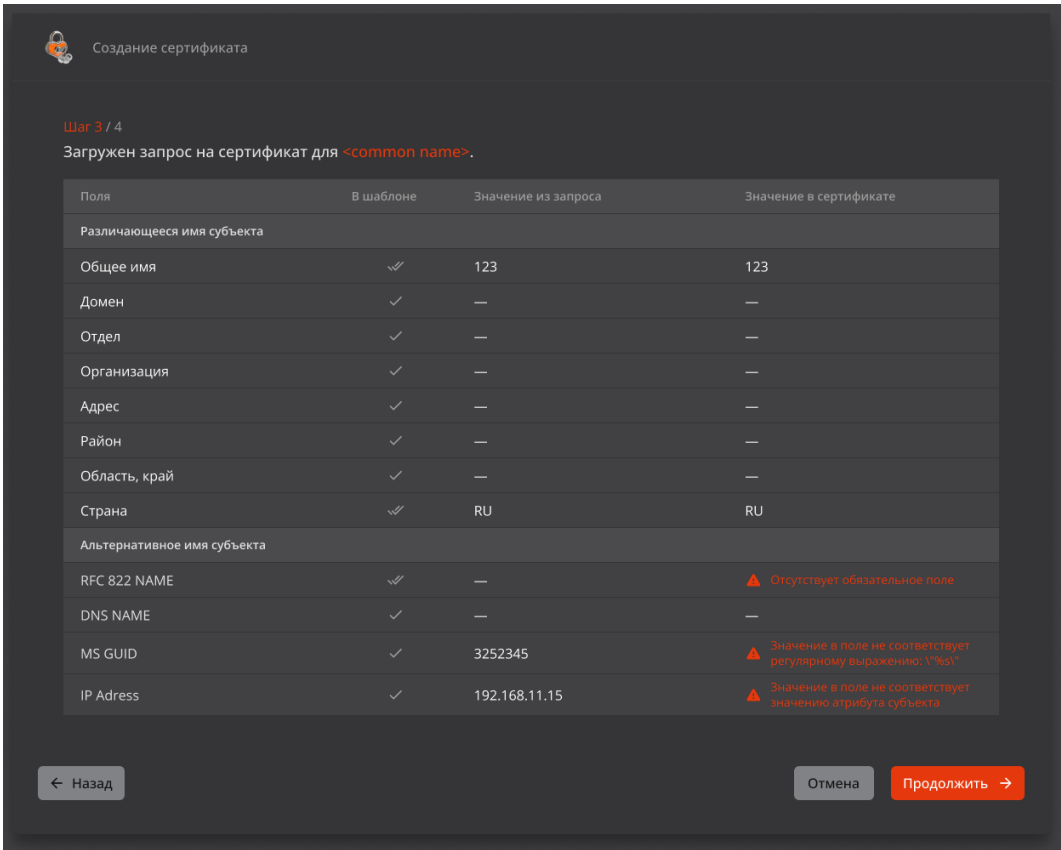


Рисунок 280 – Окно создания сертификата по запросу в разделе «Сертификаты». Шаг 4. Результат обработки запроса с ошибками в полях альтернативного имени субъекта

Таблица 29 – Перечень возможных ошибок обработки запроса

Ошибка	Сообщение
Ошибка №1	«Отсутствует обязательное поле» <sup>46</sup>
Ошибка №2	«Значение в поле не соответствует регулярному выражению: \"%s\\\"'», где \"%s\\\"» <sup>47</sup>
Ошибка №3	«Поле отсутствует в шаблоне»
Ошибка №4	«Значение в поле не соответствует значению атрибута субъекта»



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>.

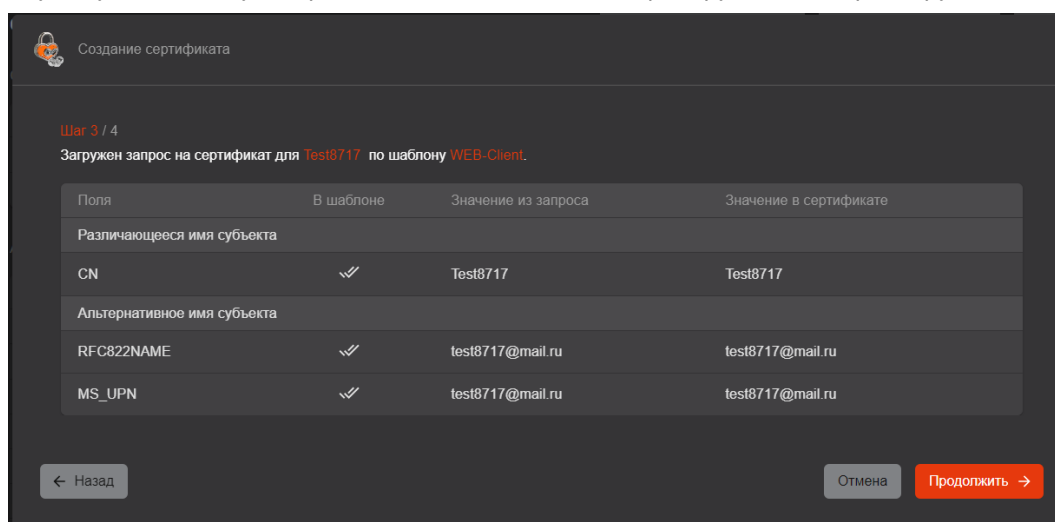
В результате успешной обработки запроса на сертификат субъекта на следующем шаге отображается (см. Рисунок 281):

<sup>46</sup> Описание полей предустановленных шаблонов см. в Приложение 2. Описание полей предустановленных шаблонов сертификатов.

<sup>47</sup> Правила валидации значений полей предустановленных шаблонов см. в Приложение 4. Правила валидации значений полей по умолчанию предустановленных шаблонов сертификатов.

- 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<sup>48</sup>, то они идентифицируются по параметру OID.





Поля	В шаблоне	Значение из запроса	Значение в сертификате
Различающееся имя субъекта			
CN	<input checked="" type="checkbox"/>	Test8717	Test8717
Альтернативное имя субъекта			
RFC822NAME	<input checked="" type="checkbox"/>	test8717@mail.ru	test8717@mail.ru
MS_UPN	<input checked="" type="checkbox"/>	test8717@mail.ru	test8717@mail.ru

Рисунок 281 – Окно создания сертификата по запросу в разделе «Сертификаты». Шаг 4. 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.


<sup>48</sup> Для справки – <https://www.alvestrand.no/objectid/2.5.4.html>, раздел Subdirectory references.

- (Шаг 4/4 или 5/5) В появившемся окне указаны атрибуты в соответствии с шаблоном сертификата<sup>49</sup>. Значение атрибутов заполняется автоматически в соответствии с данными в карточке субъекта<sup>50</sup> 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 становится активной – красного цвета).

Также дополнительно добавленное значение атрибута можно удалить по кнопке  справа от соответствующего поля атрибута (см. Рисунок 282).

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

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» ).

Необязательные поля могут оставаться незаполненными.

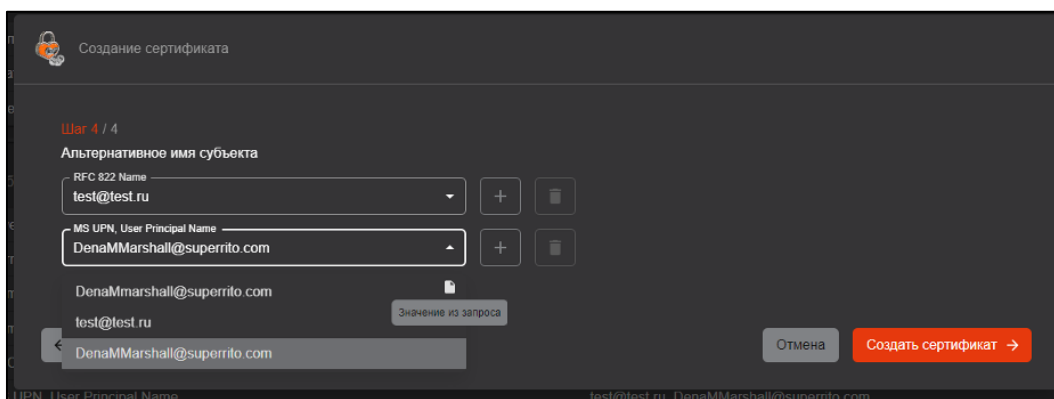


Рисунок 282 – Окно создания сертификата по запросу в разделе «Сертификаты». Шаг 5. Атрибуты сертификата

- Далее по нажатию кнопки <Создать сертификат> открывается финальное окно создания сертификата и отображается краткая информация о созданном сертификате (см. Рисунок 283). У созданного сертификата значения в полях SDN соответствуют значениям в соответствующих полях SDN запроса, на основе которого был создан сертификат.
- В журнал событий при успешном создании сертификата на основании запроса записывается событие с кодом CAENV078. При попытке повторного создания сертификата на основании одного запроса на данном шаге отображается ошибка, а в журнал событий записывается событие с кодом CAENV015.

**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.**

<sup>49</sup> Подробное описание полей предустановленных шаблонов см. в Приложение 2. Описание полей предустановленных шаблонов сертификатов.

<sup>50</sup> Подробнее см. раздел 7.8.4 настоящего руководства.

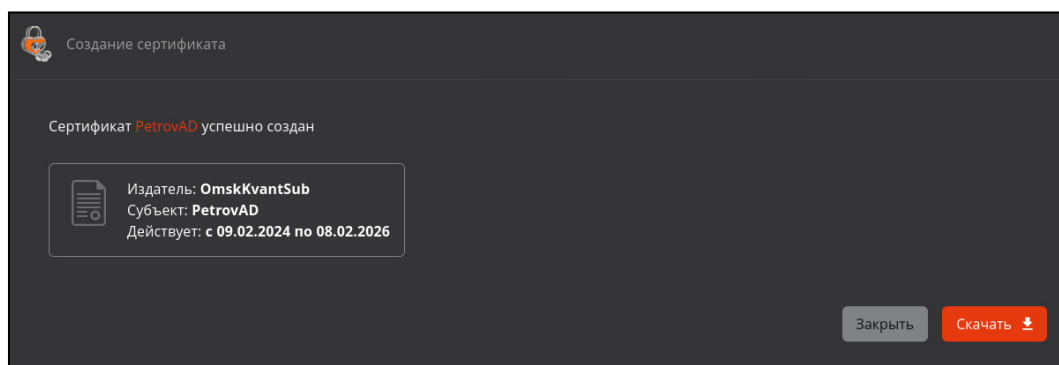


Рисунок 283 – Окно создания сертификата по запросу в разделе «Сертификаты». Результат успешного создания сертификата

- При успешном создании сертификата и выполнении всех условий ниже происходит его публикация в ресурсную систему (подробнее см. п 1.3 Публикация сертификата в ресурсную систему):
  - сертификат был создан для субъекта, подключенного к ресурсной системе;
  - сертификат создан по шаблону, в котором включена публикация сертификата.

### 1.5.2 Создание сертификата субъекта по запросу в разделе «Субъекты»

В разделе «Субъекты» (в списке субъектов или в карточке субъекта) после нажатия на кнопку «Создать сертификат» выберите из выпадающего списка функцию «На основании запроса».

- В открывшемся окне загрузить файл-запрос, а также выберите шаблон сертификата в соответствии с запросом (предполагается, что администратор заранее знает, для какого субъекта загружается файл-запрос и какой шаблон необходимо выбрать). 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 (см. подраздел 7.12 настоящего руководства). 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. По файлу запроса возможен только одноразовый выпуск сертификата.
- При необходимости, возможно перезагрузить файл-запрос в мастере создания сертификата без сброса текущего прогресса по кнопке <Изменить>.
- После загрузки файла запроса и выбора шаблона нажмите активировавшуюся кнопку <Продолжить>.

Рисунок 284 – Окно создания сертификата по запросу в разделе «Субъекты». Шаг 1. Загрузка запроса и выбор шаблона

- Программа проверяет запрос на соответствие полей запроса на сертификат и атрибутов субъекта по правилам, приведённым в Таблица 28. Проверка является регистронезависимой.
- 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 285 и Рисунок 286).
- Перечень возможных ошибок представлен в Таблица 29.

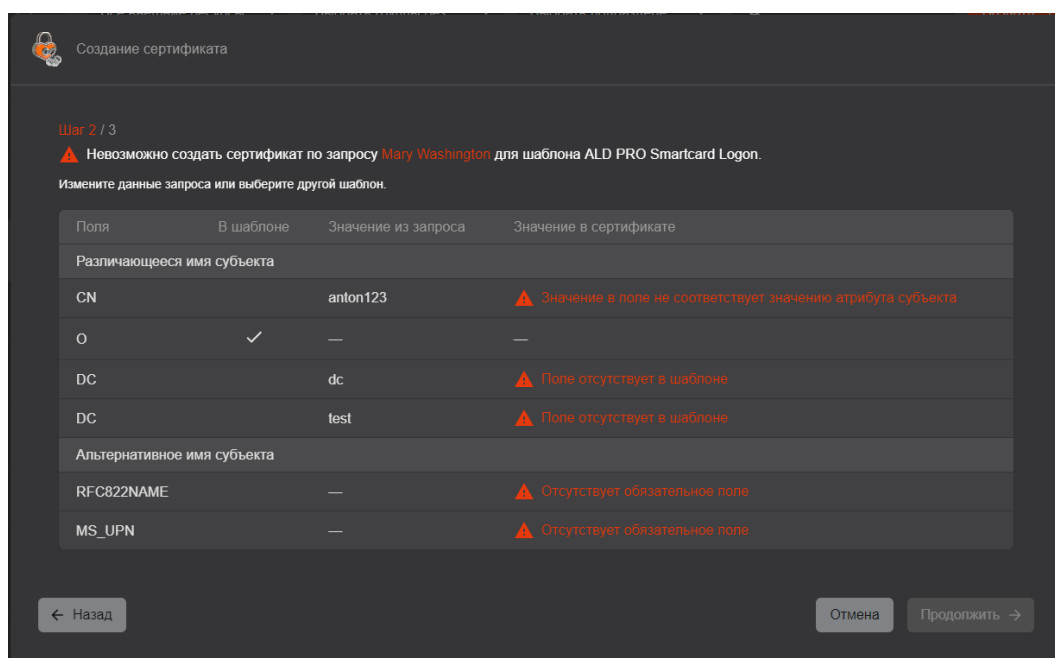


Рисунок 285 – Окно создания сертификата по запросу в разделе «Субъекты». Шаг 2. Результат обработки запроса с ошибкой в поле различающегося имени субъекта

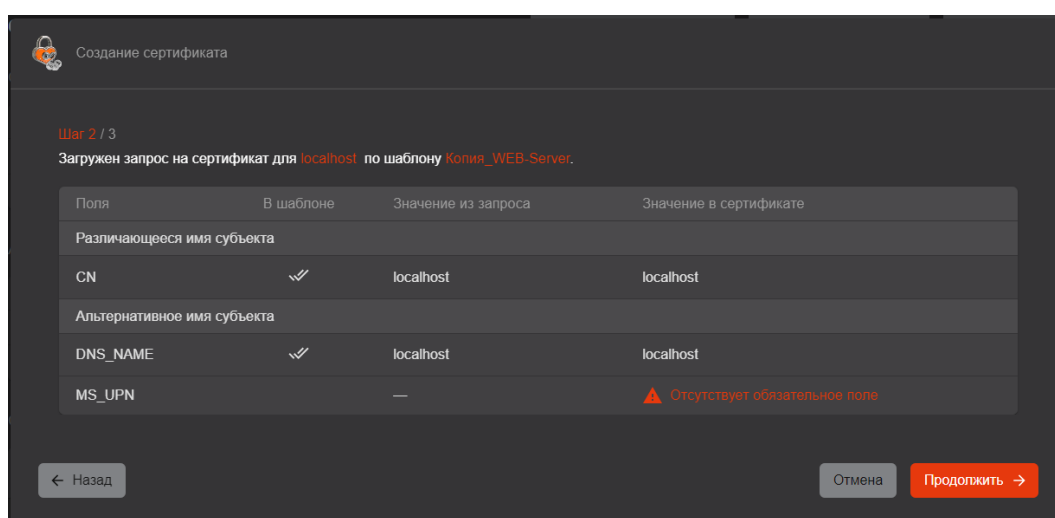




Рисунок 286 – Окно создания сертификата по запросу в разделе «Субъекты». Шаг 2. Результат обработки запроса с ошибками в полях альтернативного имени субъекта

- 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>.
- В результате успешной обработки запроса на сертификат субъекта на следующем шаге отображается (см. Рисунок 287):
  - 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<sup>51</sup>, то они идентифицируются по параметру OID.

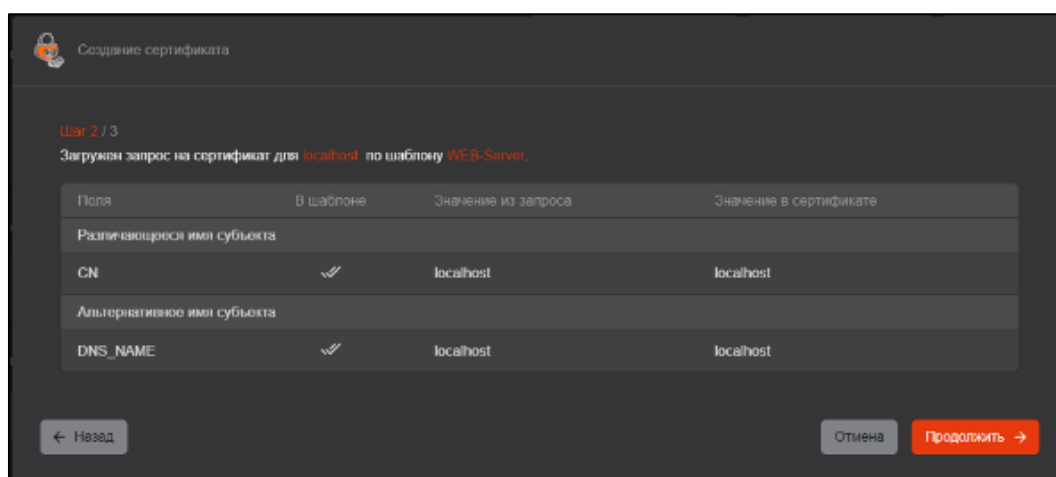



Рисунок 287 – Окно создания сертификата по запросу в разделе «Субъекты». Шаг 2. Результат успешной обработки запроса

- 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 открывшемся окне указаны атрибуты в соответствии с шаблоном сертификата (подробное описание полей предустановленных шаблонов см. в Приложение 2. Описание полей предустановленных шаблонов сертификатов). Значение атрибутов заполняется автоматически в соответствии с данными в карточке субъекта (см. раздел 7.8.4 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 становится активной – красного цвета). Также дополнительно добавленное значение атрибута можно удалить по кнопке  справа от соответствующего поля атрибута (см. Рисунок 288).
- Перечень доступных для выбора значений в полях SAN включает в себя:

<sup>51</sup> Для справки – <https://www.alvestrand.no/objectid/2.5.4.html>, раздел Subdirectory references.

- 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».
- Необязательные поля могут оставаться незаполненными.

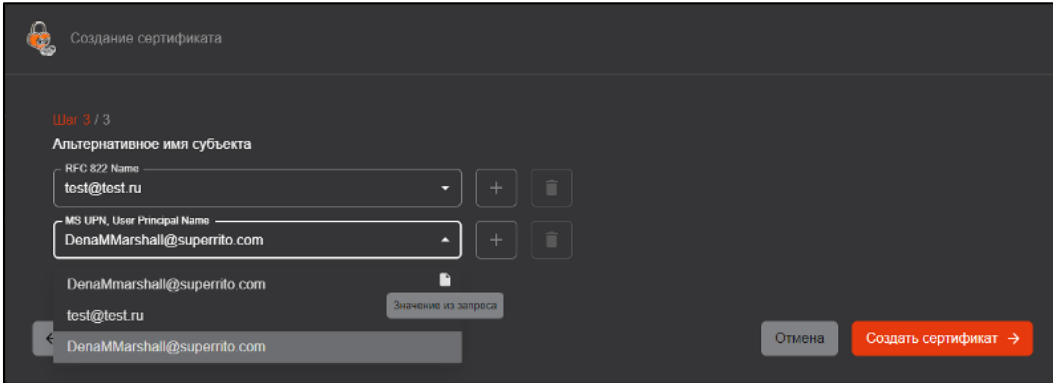


Рисунок 288 – Окно создания сертификата по запросу в разделе «Субъекты». Шаг 4. Атрибуты сертификата

- Далее по нажатию кнопки «Создать сертификат» открывается финальное окно создания сертификата и отображается краткая информация о созданном сертификате (см. Рисунок 289). У созданного сертификата значения в полях SDN соответствуют значениям в соответствующих полях SDN запроса, на основе которого был создан сертификат.
- В журнал событий при успешном создании сертификата на основании запроса записывается событие с кодом CAENV078. При попытке повторного создания сертификата на основании одного запроса на данном шаге отображается ошибка, а в журнал событий записывается событие с кодом CAENV015.

**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.**

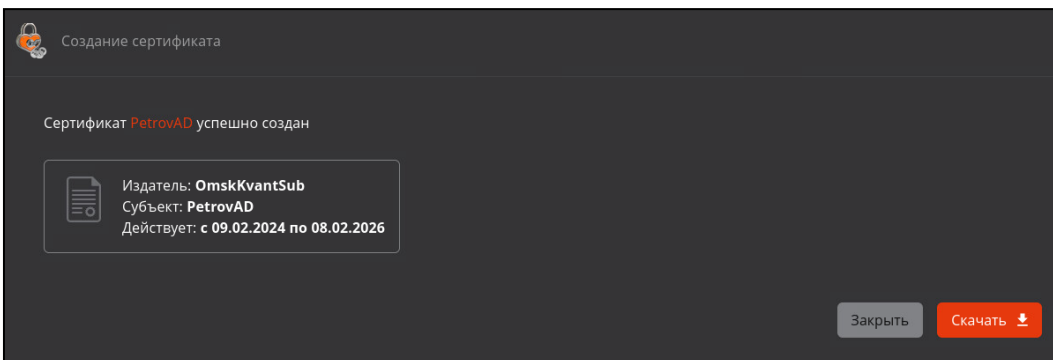


Рисунок 289 – Окно создания сертификата по запросу в разделе «Субъекты». Шаг 4. Информирование об успешном создании сертификата

- При успешном создании сертификата и выполнении всех условий ниже происходит его публикация в ресурсную систему (подробнее см. п. 1.3 Публикация сертификата в ресурсную систему):
  - сертификат был создан для субъекта, подключенного к ресурсной системе;
  - сертификат создан по шаблону, в котором включена публикация сертификата в ресурсную систему.




## 1.6 Создание сертификата субъекта на ключевом носителе

**Создание сертификата возможно только для существующего субъекта! Предварительно создайте локальный субъект (см. подраздел 7.8.5.1 настоящего руководства) или выберите субъект внешней ресурсной системы (см. подраздел 7.8.6 настоящего руководства).**

Центр сертификации Aladdin eCA поддерживает следующие виды ключевых носителей для создания сертификата:

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

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 сертификат> - «На ключевом носителе» запускает сценарий по созданию сертификата на ключевом носителе. Осуществляется проверка подключения ключевого носителя, определяется наличие свободной памяти, достаточной для записи создаваемого сертификата.
- В случае если электронный ключ успешно подключен, в открывшемся окне:
  - при выпуске сертификата в разделе «Сертификаты» необходимо на шаге 1 ввести частичное или полное значение любого атрибута субъекта, для которого будет выпущен сертификат доступа;
  - поиск субъектов выполняется по значениям в их атрибутах и является регистронезависимым;
  - в результате поиска будут отображены найденные субъекты с указанием краткой информации (см. Рисунок 290):
    - «CN» – значение атрибута «Common Name» субъекта;
    - «ID» – идентификатор субъекта;
    - «UPN» – значение атрибута «MS UPN, User Principal Name» субъекта;
    - «DNS» – значение атрибута «DNS Name» субъекта;
    - пиктограммы наличия подключения субъекта к ресурсной системе .
  - в результате поиска в полях «CN», «UPN» и «DNS» отображаются все значения соответствующего поля атрибута субъекта, разделитель значений в поле – запятая с пробелом;
  - в результате поиска поля «CN», «UPN» и «DNS» не отображаются, если в соответствующем данному полю атрибуте у субъекта отсутствуют значения;
  - выберите субъект и нажмите кнопку <Продолжить> для перехода к шагу 2;
  - при выпуске сертификата в разделах «Субъекты» и «Учётные записи» шаг 1 не требуется и первым шагом будет выбор ключевого носителя и шаблона для выпуска сертификата (см. Рисунок 291).

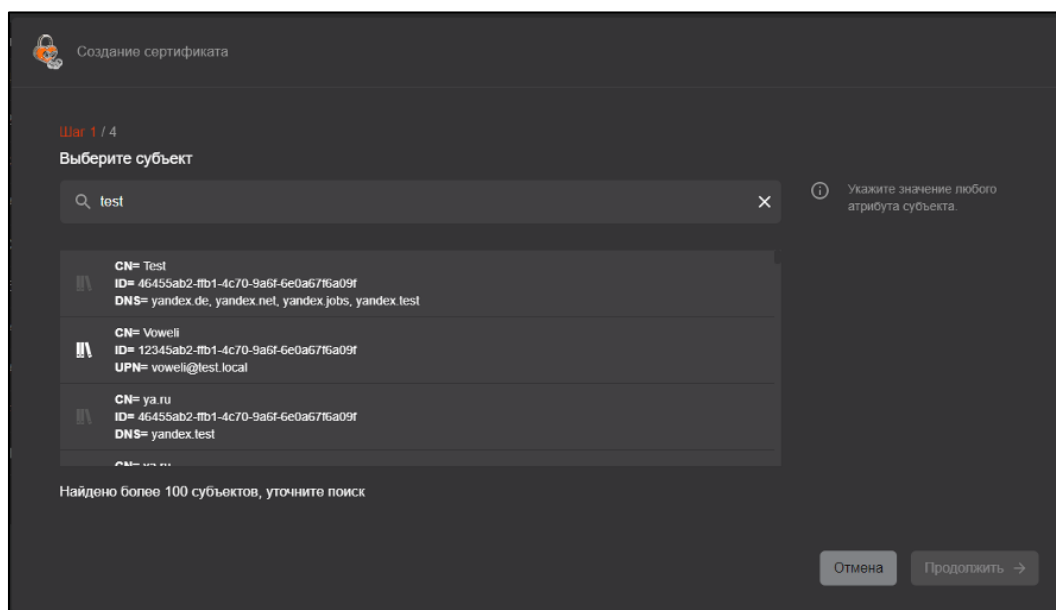


Рисунок 290 – Окно создания сертификата на электронном ключе в разделе «Сертификаты». Шаг 1

- В открывшемся окне (см. Рисунок 291) необходимо выбрать ключевой носитель из выпадающего списка в поле «Устройство», ввести PIN-код пользователя ключевого носителя (от 4 до 16 символов) и указать шаблон для выпуска сертификата. При выпуске сертификата из раздела «Субъекты» шаблон будет определён по умолчанию и выбору не подлежит. 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 (см. подраздел 7.12 настоящего руководства). 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.

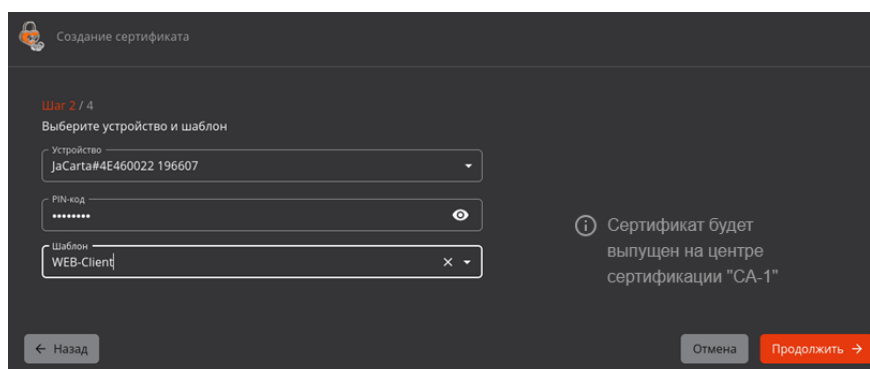




Рисунок 291 – Окно создания сертификата на электронном ключе. Шаг 2

- В окне Шага 3 указаны атрибуты в соответствии с выбранным (на предыдущем шаге) шаблоном сертификата (подробное описание полей предустановленных шаблонов см. в Приложение 2. Описание полей предустановленных шаблонов сертификатов). Значение атрибутов заполняется автоматически в соответствии с данными в карточке субъекта (см. раздел 7.8.4 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 становится активной – красного цвета). Также дополнительно добавленное значение атрибута можно удалить по кнопке  справа от соответствующего поля атрибута (см. Рисунок 292).
- Необязательные поля могут оставаться незаполненными.

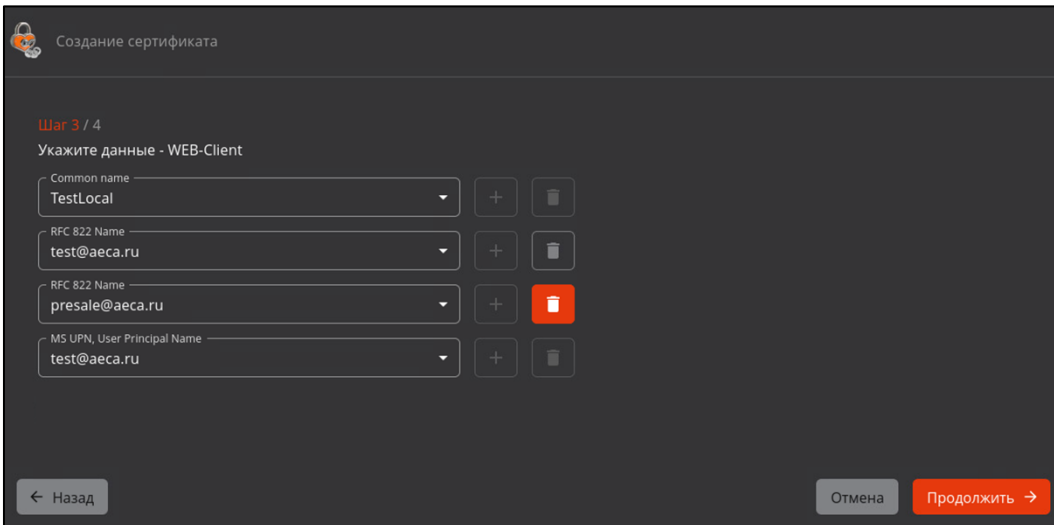


Рисунок 292 – Окно создания сертификата на электронном ключе. Шаг 3. Удаление добавленного значения атрибута

- Нажмите кнопку <Продолжить>, ставшую активной, после заполнения всех обязательных полей шаблона сертификата на шаге 3 (см. Рисунок 292).
- Далее необходимо выбрать параметры криптографии (см. Рисунок 293):
  - 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 и длины ключа нажмите кнопку <Создать сертификат>.

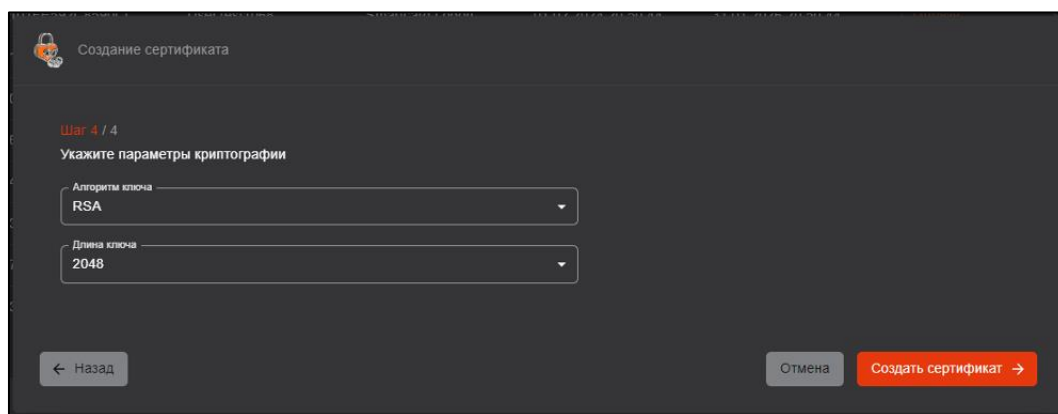


Рисунок 293 – Окно создания сертификата на электронном ключе. Шаг 4

- 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;
  - создание сертификата;
  - запись сертификата на ключевой носитель.
- Процессы выполняются автоматически и после завершения станут доступны кнопки <Скачать сертификат> (контейнер сертификата PKCS#12) и <Скачать цепочку сертификатов> (см. Рисунок 294).

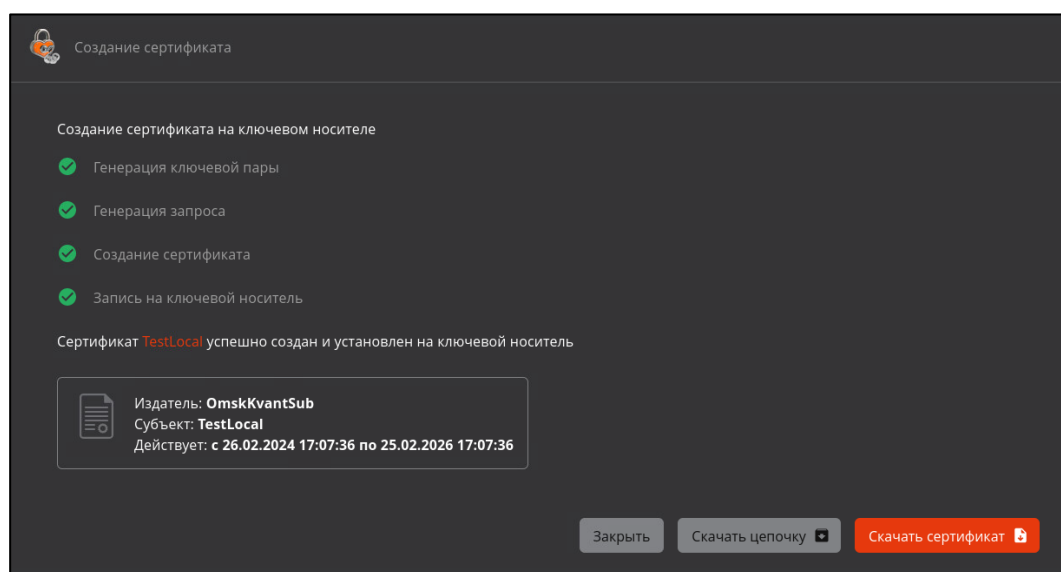


Рисунок 294 – Окно успешного создания сертификата субъекта на электронном ключе

- При успешном создании сертификата и выполнении всех условий ниже происходит его публикация в ресурсную систему (подробнее см. п. 1.3 Публикация сертификата в ресурсную систему):
  - сертификат был создан для субъекта, подключенного к ресурсной системе;
  - сертификат создан по шаблону, в котором включена публикация сертификата в ресурсную систему.

#### 1.6.1 Сообщения об ошибках при создании сертификата на ключевом носителе

- В случае, если ПО JC-WebClient предварительно не установлено, то администратор будет уведомлен об этом информационным сообщением (см. Рисунок 295). Для выпуска сертификата на электронном ключе установите ПО JC-WebClient версии 4.3.2 или 4.3.3.

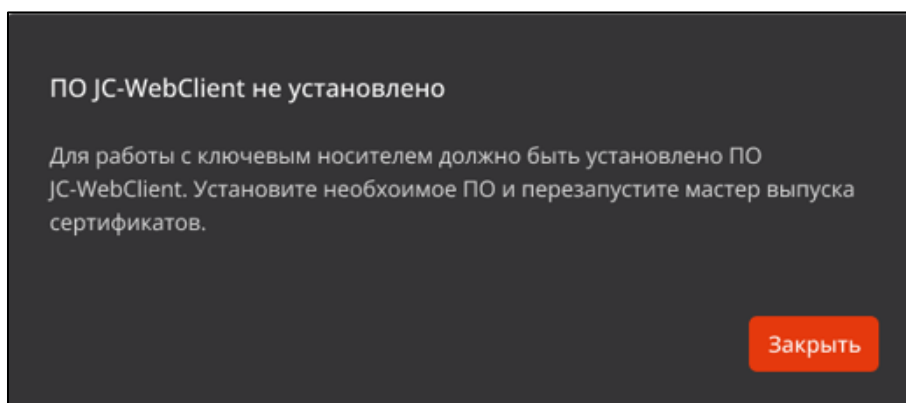


Рисунок 295 – Окно информационного сообщения «ПО JC-WebClient не установлено»

- В случае, если электронный носитель не подключен, то администратор будет уведомлен об этом информационным сообщением (см. Рисунок 296). Для выпуска сертификата подключите электронный ключ и перезапустите мастер создания сертификата.

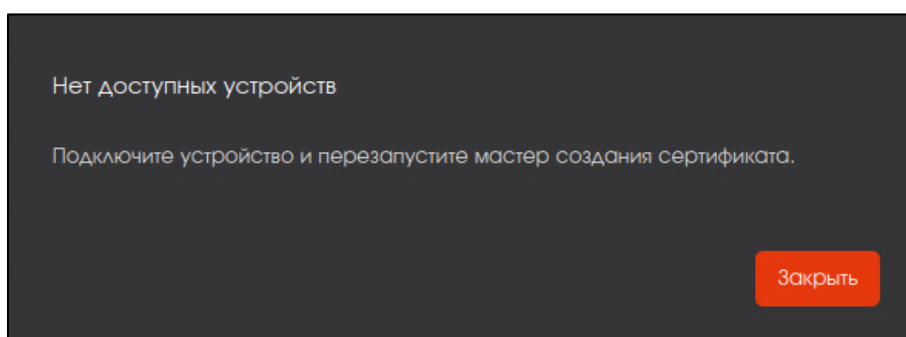


Рисунок 296 – Окно информационного сообщения «Нет доступных устройств»

- В случае, если выбранный для выпуска сертификата алгоритм не поддерживается выбранной моделью ключевого носителя, администратор будет уведомлён об этом информационным сообщением.
- В случае возникновения ошибок, связанных с работой JC-WebClient, администратор будет уведомлён сообщением, согласно с описанием 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 2. ОПИСАНИЕ ПОЛЕЙ ПРЕДУСТАНОВЛЕННЫХ ШАБЛОНОВ СЕРТИФИКАТОВ

Имя шаблона	Идентификатор	Период действия сертификата	Включать SID в сертификат	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	1024	- Цифровая подпись - Подтверждение подлинности - Шифрование ключей	+	- Аутентификация клиента - Защита электронной почты	-	Common name	+	+	-		
					ECDSA	256										
					ГОСТ Р 34.10-2012	Выключен										
ECA-User	e97d92b1-2e6e-4ed2-943f-6508113feac6	2y	-	-	RSA	1024	- Цифровая подпись - Подтверждение подлинности - Шифрование ключей	+	- Аутентификация клиент - Защита электронной почты	-	Common name	+	+	-		
					ECDSA	256										
					ГОСТ Р 34.10-2012	256										
ECA-WEB-Server	076f61dc-5ff4-43cc-8cf9-6b833adf1092	2y	-	-	RSA	1024	- Цифровая подпись - Шифрование ключей	+	- Аутентификация сервера	-	Common name	+	+	DNS name	+	+
					ECDSA	256										
					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 <sup>52</sup>	+	+	DNS name <sup>53</sup>	+	+
					ECDSA	256								MS GUID <sup>54</sup>		
					ГОСТ Р 34.10-2012	Выключен										

<sup>52</sup> Имя контроллера домена.

<sup>53</sup> FQDN –полное доменное имя вашего сервера.

<sup>54</sup> 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.

Smartcard Logon	aa03e458-50cd-46b8-82cd-d5612ed3b647	2y	-	-	RSA	1024	- Цифровая подпись - Подтверждение подлинности - Шифрование ключей - Шифрование данных	+	- Аутентификация клиента - Защита электронной почты - Вход с MS смарт-картой	-	Common name <sup>55</sup>	+	+	MS UPN <sup>56</sup>	+	+			
					ECDSA	256								RFC 822 Name <sup>57</sup>	+	+			
					ГОСТ Р 34.10-2012	Выключен													
WEB-Client	059a38f5-f345-4275-b79f-e7e6cc3cbb68	2y	-	-	RSA	1024	- Цифровая подпись - Подтверждение подлинности - Шифрование ключей	+	- Аутентификация клиента - Защита электронной почты	-	Common name <sup>58</sup>	+	+	MS UPN <sup>59</sup>	+	+			
					ECDSA	256								RFC 822 Name <sup>60</sup>	+	+			
					ГОСТ Р 34.10-2012	Выключен													
WEB-Server	08c66f99-218a-46ef-bdee-6a2b3b26a4f1	2y	-	-	RSA	1024	- Цифровая подпись - Шифрование ключей	+	Аутентификация сервера	-	Common name <sup>61</sup>	+	+	DNS name <sup>62</sup>	+	+			
					ECDSA	256													
					ГОСТ Р 34.10-2012	Выключен													
S/MIME	0c234243-18cf-4c05-b699-537731b2436f	2y	-	-	RSA	1024	- Цифровая подпись - Подтверждение подлинности - Шифрование ключей - Шифрование данных	+	- Аутентификация клиента - Защита электронной почты - Вход с MS смарт-картой	-	Common name <sup>63</sup>	+	+	RFC 822 Name <sup>64</sup>	+	+			
					ECDSA	256													
					ГОСТ Р 34.10-2012	Выключен													

<sup>55</sup> Имя пользователя.

<sup>56</sup> Имя входа пользователя в формате e-mail адреса.

<sup>57</sup> Почтовый адрес пользователя, может совпадать с MS UPN.

<sup>58</sup> Имя web-клиента.

<sup>59</sup> Имя входа пользователя в формате e-mail адреса.

<sup>60</sup> Почтовый адрес пользователя, может совпадать с MS UPN.

<sup>61</sup> Имя web-сервера.

<sup>62</sup> FQDN – полное доменное имя вашего сервера.

<sup>63</sup> Имя пользователя.

<sup>64</sup> почтовый адрес пользователя, может совпадать с MS UPN

ALD PRO Domain Controller	11ec34a4-d03e-4059-92f0-9c09b08bffeaa	2y	-	-	RSA	1024	- Цифровая подпись - Подтверждение подлинности - Шифрование ключей - Шифрование данных	+	- Центр распространения ключей Kerberos - Аутентификация сервера	-	Common name <sup>65</sup>	+	+	MS UPN <sup>66</sup>	+	+				
					ECDSA	256					Organization <sup>67</sup>	-	+	Kerberos KPN <sup>68</sup>	+	+				
					ГОСТ Р 34.10-2012	Выключен														
ALD PRO Smartcard Logon	18d9bd4e-6f15-423f-8137-ac8416ad6874	2y	-	-	RSA	1024	- Цифровая подпись - Подтверждение подлинности - Шифрование ключей - Шифрование данных	+	- Аутентификация клиента - Центр распространения ключей Kerberos - Аутентификация сервера	-	Common name <sup>69</sup>	+	+	MS UPN <sup>70</sup>	+	+				
					ECDSA	256					Organization <sup>71</sup>	-	+	RFC 822 Name <sup>72</sup>	+	+				
					ГОСТ Р 34.10-2012	Выключен														
OCSP Signer	aac2e49b-9c8e-4869-80c1-eef526ba75ab	2y	-	-	RSA	1024	Цифровая подпись	+	OCSP подписант	-	Common name	+	+	-						
					ECDSA	256														
					ГОСТ Р 34.10-2012	Выключен														
Root CA	9129245a-eaad-4ebc-a2a4-8845ac0336fb	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)	-	+				

<sup>65</sup> Имя контроллера домена ALD PRO.

<sup>66</sup> Данные в формате «krbtgt/полное имя домена@полное имя домена».

<sup>67</sup> Организация.

<sup>68</sup> Данные в формате «krbtgt/полное имя домена@полное имя домена».

<sup>69</sup> Имя пользователя ALD PRO.

<sup>70</sup> Имя входа пользователя в формате e-mail адреса.

<sup>71</sup> Организация.

<sup>72</sup> Почтовый адрес пользователя, может совпадать с MS UPN.



											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								-	+				
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	-	+
											Unique Identifier (UID)	-	+	DNS name	-	+
					ECDSA	256					Given name	-	+	MS UPN	-	+
					ГОСТ Р 34.10-2012	256					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 4. ПРАВИЛА ВАЛИДАЦИИ ЗНАЧЕНИЙ ПОЛЕЙ ПО УМОЛЧАНИЮ ПРЕДУСТАНОВЛЕННЫХ ШАБЛОНОВ СЕРТИФИКАТОВ

Поле	Правило валидации
<b>Поля SDN</b>	
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", "A"-"Я", "a"-"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.
<b>Поля SAN</b>	
RFC 822 Name	Допустимые символы: "A"-"Z", "a"-"z", "0"-"9", ".", "@", "_", "-". Формат значения: "text@text". Пример заполнения: <a href="mailto:ivanova@example.com">ivanova@example.com</a> .
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", ".", ":". 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,

Поле	Правило валидации
	<p>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.</p> <p>В качестве идентификатора RDN допускается указание OID (формат OID должен соответствовать рекомендации ITU X.660).</p>
Registered Identifier (OID)	<p>Допустимые символы: "0"-"9", ".".</p> <p>Формат значения: OID в соответствии с рекомендацией ITU X.660.</p>
MS UPN, User Principal Name	<p>Допустимые символы: "A"-"Z", "a"-"z", "A"-"Я", "a"-"я", "ё", "Ё", "0"-"9", ".", "@", "_", "-", "/".</p> <p>Формат значения: "text@text".</p> <p>Пример заполнения: "krbtgt/ald.pro@ald.pro".</p>
MS GUID, Globally Unique Identifier	<p>Допустимые символы: "A"-"F", "a"-"f", "0"-"9".</p> <p>Длина значения должна составлять 32 символа.</p> <p>Пример значения: "92625ee510e248479554779d1f43f751".</p>
Kerberos KPN, Kerberos 5 Principal Name	<p>Допустимые символы: "A"-"Z", "a"-"z", "A"-"Я", "a"-"я", "ё", "Ё", "0"-"9", ".", "@", "_", "-", "/".</p> <p>Формат значения: "text@text".</p> <p>Пример заполнения: "krbtgt/ald.pro@ald.pro".</p>
Permanent Identifier	<p>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".</p>
Xmpp address	<p>Допустимые символы: "A"-"Z", "a"-"z", "A"-"Я", "a"-"я", "ё", "Ё", "0"-"9", ".", "@", "_", "-", "/".</p> <p>Формат значения: "text@text".</p>
Subject Identification Method	<p>Формат значения: "OID::text::text", где "OID" – OID в соответствии с рекомендацией ITU X.660, а "text" – любая последовательность символов.</p>

## ПРИЛОЖЕНИЕ 5. ОПИСАНИЕ ПРЕДУСТАНОВЛЕННЫХ ИДЕНТИФИКАТОРОВ РАСШИРЕННОГО ИСПОЛЬЗОВАНИЯ КЛЮЧА

Имя	OID	Описание
Любое расширенное использование ключа	2.5.29.37.0	Сертификат может использоваться для любых целей.
CSN 369791 TLS клиент	1.2.203.7064.1.1.369791.1	Сертификат может использоваться как сертификат CSN 369791 TLS клиента.
CSN 369791 TLS сервер	1.2.203.7064.1.1.369791.2	Сертификат может использоваться как сертификат CSN 369791 TLS сервера.
Аутентификация клиента	1.3.6.1.5.5.7.3.2	Сертификат может использоваться при установлении защищенного соединения по протоколу TLS для подтверждения подлинности клиента.
Подписание кода	1.3.6.1.5.5.7.3.3	Сертификат может использоваться при создании ЭЦП программных компонентов.
EAP через LAN (EAPoL)	1.3.6.1.5.5.7.3.14	Сертификат может использоваться для 802.1X (EAPoL, EAP-over-LAN).
EAP через PPP	1.3.6.1.5.5.7.3.13	Сертификат может использоваться для EAP в среде PPP.
Подписание ETSI TSL	0.4.0.2231.3.0	Сертификат может использоваться для TSL (Trust-service Status Lists) подписи.
Защита электронной почты	1.3.6.1.5.5.7.3.4	Сертификат может использоваться для защиты электронной почты (подпись, шифрование, соглашение о ключах).
ICAO подписание списка отклонений	2.23.136.1.1.8	Сертификат может использоваться для подписания списка отклонений ICAO.
Управление Intel AMT	2.16.840.1.113741.1.2.3	Сертификат может использоваться при работе технологии Intel Advanced Management Technology (AMT).
Интернет-обмен ключами для IPsec	1.3.6.1.5.5.7.3.17	Сертификат может быть назначен IPSEC SA и может использоваться для инициации обмена ключами через IPsec Internet.
Аутентификация клиента Kerberos	1.3.6.1.5.2.3.4	Сертификат может использоваться для аутентификации клиента Kerberos.

Центр распространения ключей Kerberos	1.3.6.1.5.2.3.5	Сертификат может использоваться для проверки подлинности KDC.
Подписание коммерческого MS кода	1.3.6.1.4.1.311.2.1.22	Сертификат может использоваться для подписания коммерческого кода (зарегистрирован компанией Microsoft).
Подписание MS документа	1.3.6.1.4.1.311.10.3.12	Сертификат может использоваться для подписания документов (зарегистрирован компанией Microsoft).
Восстановление MS EFS	1.3.6.1.4.1.311.10.3.4.1	Сертификат может использоваться для восстановления документов, защищенных с помощью шифрованной файловой системы (EFS, зарегистрирован компанией Microsoft).
Зашифрованная MS файловая система	1.3.6.1.4.1.311.10.3.4	Сертификат может использоваться для шифрования файлов с помощью шифрованной файловой системы (EFS, зарегистрирован компанией Microsoft).
Подписание индивидуального MS кода	1.3.6.1.4.1.311.2.1.21	Сертификат может использоваться для подписания индивидуального кода (зарегистрирован компанией Microsoft).
Вход с MS смарт-картой	1.3.6.1.4.1.311.20.2.2	Сертификат может использоваться физическим лицом для входа в систему с помощью смарт-карты.
OCSP подписант	1.3.6.1.5.5.7.3.9	Сертификат может использоваться для формирования электронной подписи OCSP-запросов.
Подписание Adobe PDF	1.2.840.113583.1.1.5	Сертификат может использоваться для подписания документов Adobe PDF.
Аутентификация PIV карты	2.16.840.1.101.3.6.8	Сертификат может использоваться для аутентификации карты PIV.
SCVP клиент	1.3.6.1.5.5.7.3.16	Сертификат может использоваться как сертификат клиента при использовании протокола Server-Based Certificate Validation Protocol (SCVP).
SCVP сервер	1.3.6.1.5.5.7.3.15	Сертификат может использоваться как сертификат сервера при использовании протокола Server-Based Certificate Validation Protocol (SCVP).
Домен SIP	1.3.6.1.5.5.7.3.20	Сертификат может использоваться как сертификат Session Initiation Protocol (SIP) доменов.
SSH клиент	1.3.6.1.5.5.7.3.21	Сертификат может использоваться как сертификат SSH клиента.
SSH сервер	1.3.6.1.5.5.7.3.22	Сертификат может использоваться как сертификат SSH сервера.

Аутентификация сервера	1.3.6.1.5.5.7.3.1	Сертификат может использоваться при установлении защищенного соединения по протоколу TLS для подтверждения подлинности сервера.
Отметка времени	1.3.6.1.5.5.7.3.8	Сертификат может использоваться для привязки хеша объекта ко времени из доверенного источника времени.
ICAO подписание основного списка	2.23.136.1.1.3	Сертификат может использоваться для подписания основного списка ICAO.

## ОБОЗНАЧЕНИЯ И СОКРАЩЕНИЯ

ОС	–	Операционная система
ПО	–	Программное обеспечение
СУБД	–	Система управления базами данных
УЦ	–	Удостоверяющий центр
ЦС	–	Центр сертификатов
АеСА СА	–	Центр сертификатов Aladdin Enterprise Certificate Authority Certified Edition
АеСА VA	–	Aladdin Enterprise Certificate Authority Validation Authority
CN	–	Common Name
CRL	–	Certificate Revocation List, список отозванных сертификатов
Delta CRL	–	список изменений последнего опубликованного списка отозванных сертификатов (CRL)
AIA	–	Authority Information Access
SSL	–	Secure Sockets Layer – протокол безопасности, создающий зашифрованное соединение между веб-сервером и веб-браузером.
UPN	–	User Principal Name
URL	–	Uniform Resource Locator
UUID	–	Universally Unique Identifier



## ТЕРМИНЫ И ОПРЕДЕЛЕНИЯ

**Автоматическая точка** – это автоматически сформированная запись URL-адреса точки распространения CRL, Delta CRL или AIA зарегистрированного Центра валидации Aladdin Enterprise Certificate Authority в Центре сертификации в разделе и на вкладке «Центры валидации».

**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.

**Активированный ЦС** – это экземпляр центра сертификации в информационной системе, который используется в настоящий момент для выпуска сертификатов на основании запроса и сертификатов доступа субъектов.

**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.

**Кластер** – это группа точек распространения определенного типа (CRL, Delta CRL и AIA) или служб OCSP, доступ к которым осуществляется по единому URL (путем использования внешних средств балансирования нагрузки).

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

**Корневой ЦС** – экземпляр центра сертификации в информационной системе, имеющий абсолютное доверие со стороны всех участников процесса строгой аутентификации. С точки зрения службы безопасности предприятия должен быть обеспечен максимальным уровнем защиты (отдельный ПК, отключенный от сети, с доступом ограниченного круга лиц). Корневой ЦС владеет само подписанным сертификатом, который должен распространяться доверенным способом в информационной системе.

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

**Пагинация** – это постраничный вывод информации на экране разделов. Ссылочный блок для разграничения содержимого размещен внизу экранной страницы и представляет цифровой диапазон, отображающий:

- количество элементов на одной странице – возможно выбрать из выпадающего списка – выводить 5, 10 или 25 элементов на одну страницу;
- нумерацию элементов страницы, которая в настоящее время открыта у пользователя, из общего количества созданных элементов;
- указатели для навигации по страницам.

**Подчиненный ЦС** – экземпляр центра сертификации в информационной системе, обладающий функцией управления политиками строгой аутентификации или функцией управления жизненным циклом сертификатов субъектов информационной системы. Подчиненный ЦС владеет сертификатом, выданным вышестоящим ЦС (Корневым или другим Подчиненным), который используется для проверки всей цепочки доверия сертификатов.

**Пользовательская точка** – это запись URL-адреса, созданная администратором с целью регистрации сторонней точки распространения CRL, Delta CRL или AIA, существующей или развёртываемой на сервере в информационной системе.

**Приоритет** – это очередность записи URL-адреса точки распространения или службы OCSP в сертификате и, соответственно, в списках, отображаемом на вкладках «Точки распространения» и «Службы OCSP».

**Разрешённые издатели** – это список Центров сертификации, сертификаты которых клиент может использовать для авторизации на сервере, на котором развёрнут Центр сертификации с актуальным списком разрешённых издателей.

**Ресурсная система (внешняя)** – это подключаемая служба каталогов, которая предоставляет информацию об имеющихся субъектах.

**Ресурсная система (локальная)** – это ресурсная система, создаваемая автоматически при установке программного средства «Центр сертификатов доступа Aladdin Enterprise Certificate Authority Certified Edition», представляющая собой базу данных субъектов и формируемая из сведений, вводимых при выпуске сертификата для нового субъекта.

**Сервис валидации** – служба, составная часть Центра сертификации, отвечающая за предоставление информации о действительности сертификатов. Предоставляет сервисы CRL DP, OCSP.

**Сервис регистрации** – служба, составная часть Центра сертификации, отвечающая за обработку запросов на выдачу сертификатов от субъектов информационной системы.

**Сервис сертификатов** – служба, составная часть Центра сертификации, непосредственно отвечающая за жизненный цикл сертификатов (выдача, отзыв).

**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.

**Сертификат веб-сервера** – это сертификат, с помощью которого сервер, на котором развёрнут программный компонент «Центр сертификации Aladdin Enterprise Certification Authority», устанавливает с клиентом tls-соединение.

**Событие безопасности** – идентифицированное возникновение состояния системы, сервиса или сети, указывающего на возможное нарушение политики информационной безопасности, или сбой средств контроля, или ранее неизвестную ситуацию, которая может быть значимой для безопасности.

**Список отозванных сертификатов** (Certificate Revocation List – **CRL**) – список аннулированных (отозванных) сертификатов, издаётся центром сертификации по запросу или с заданной периодичностью на основании запросов об отзыве сертификатов.

**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).

**Технологический ЦС** – экземпляр центра сертификации в информационной системе, обладающий функцией первичной настройки программного компонента «Центр сертификации Aladdin Enterprise Certification Authority».

**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 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.).

## ЛИСТ РЕГИСТРАЦИИ ИЗМЕНЕНИЙ

[illegible]