



Центр сертификатов доступа

# Aladdin Enterprise Certificate Authority Certified Edition

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

Изделие	RU.АЛДЕ.03.01.020
Документ	RU.АЛДЕ.03.01.020 32 01-2
Версия	2.4
Листов	275
Дата	28.05.2025

## 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 реэкспорт продукта ограничения.

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

© АО "Аладдин Р.Д.", 1995—2026. 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 предназначается 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.), подтверждённые или включённые 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 незамедлительно вернёте в Компанию все экземпляры ПО и все копии такового 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 реэкспорт 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 УСТАНОВЛИВАТЬ И НЕ ИСПОЛЬЗОВАТЬ ДАННОЕ ПРОГРАММНОЕ ОБЕСПЕЧЕНИЕ.

## АННОТАЦИЯ

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

Документ предназначен для администраторов Центра сертификатов доступа, 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 комплекса «Центр сертификации Aladdin Enterprise Certification Authority»<sup>2</sup> из состава Центра сертификатов доступа. Перед эксплуатацией программы 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.

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

---

<sup>1</sup> Далее по документу –программное средство, еСА

<sup>2</sup> Далее по документу – программа, еСА-СА

## СОДЕРЖАНИЕ

Аннотация .....	5
1 Роли управления.....	10
2 Режимы функционирования программы .....	13
3 Лицензирование программы.....	14
3.1 Лицензионные ограничения.....	14
3.2 Первичное лицензирование.....	15
3.3 Продление срока действия лицензии.....	17
4 Начало работы с программой.....	19
4.1 Инициализация Центра сертификации с генерацией ключа .....	19
4.1.1 Инициализация корневого Центра сертификации с генерацией ключа .....	19
4.1.2 Инициализация подчинённого Центра сертификации с генерацией ключа .....	24
4.2 Инициализация Центра сертификации с импортом ключа .....	29
4.3 Переопределение сведений, отображаемых в окне авторизации и в заголовке вкладки браузера .....	35
5 Аутентификация в программе.....	36
5.1 Аутентификация с использованием сертификата, перенесённого на жёсткий диск.....	36
5.2 Аутентификация с использованием сертификата на ключевом носителе .....	39
5.2.1 Настройка СВТ для двухфакторной аутентификации администратора по сертификату на ключевом носителе .....	39
5.2.1.1 Установка Единого Клиента JaCarta .....	40
5.2.1.2 Настройка веб-браузера Firefox.....	40
5.2.1.3 Настройка веб-браузера Chromium для РЕД ОС, РОСА «XPOM» 12 Сервер, SberLinux OS Server и Альт Сервер.....	41
5.2.1.4 Настройка веб-браузера Chromium для Astra Linux Special Edition .....	42
5.2.2 Двухфакторная аутентификация администратора по сертификату на ключевом носителе .....	42
5.3 Аутентификации доменных учётных записей в eCA-CA .....	43
5.3.1 Аутентификация в eCA-CA по имени и паролю доменного пользователя.....	43
5.3.2 Аутентификация в eCA-CA по Kerberos-билету доменного пользователя.....	43
6 Безопасность соединения.....	44
6.1 Настройка доверенного соединения .....	44
7 Технологические составляющие программы .....	46
7.1 Назначение технологических составляющих.....	46
7.2 Установка и настройка технологических составляющих.....	46
7.3 Удаление технологических составляющих .....	47
7.4 Восстановление доступа к программе в случае некорректного удаления технологических составляющих и/или блокировки доступа .....	47
8 Функции управления программы .....	48
8.1 Верхняя панель .....	48
8.2 Боковая панель .....	49
8.3 Раздел «Центр сертификации» .....	52
8.3.1 Вкладка «Свои сертификаты» .....	52
8.3.1.1 Просмотр параметров сертификата ЦС в карточке ЦС .....	55
8.3.1.2 Создание корневого центра сертификации с генерацией ключа.....	56
8.3.1.3 Создание подчинённого центра сертификации с генерацией ключа.....	62
8.3.1.4 Создание центра сертификации с импортом внешнего ключа .....	62
8.3.1.5 Скачивание запроса на сертификат для центра сертификации в состоянии «Запрос» .....	62
8.3.1.6 Импорт сертификата (цепочки сертификатов) подчинённого центра сертификации.....	62
8.3.1.7 Удаление центра сертификации .....	65
8.3.1.8 Экспорт закрытого ключа центра сертификации .....	66
8.3.1.9 Импорт закрытого ключа центра сертификации.....	68
8.3.1.10 Повторный импорт сертификата (цепочки сертификатов) подчинённого ЦС .....	69
8.3.2 Вкладка «Сертификаты Подчиненных центров».....	70
8.3.2.1 Просмотр списка сертификатов подчинённого ЦС.....	71
8.3.2.2 Подписание запроса в Корневом Центре сертификации .....	71
8.3.2.3 Просмотр свойств сертификата подчинённого ЦС в карточке сертификата подчинённого ЦС .....	72
8.3.2.4 Отзыв сертификата .....	73

8.3.2.5	Скачивание сертификата/цепочки сертификатов.....	73
8.3.2.6	Переформирование сертификата подчинённого ЦС .....	73
8.4	Раздел «Сертификаты» .....	74
8.4.1	Выпуск сертификата.....	75
8.4.2	Поиск сертификатов .....	75
8.4.3	Сортировка сертификатов .....	76
8.4.4	Фильтрация сертификатов.....	76
8.4.4.1	Применение фильтров .....	76
8.4.4.2	Сброс применённых фильтров .....	77
8.4.5	Скачивание сертификатов .....	77
8.4.6	Статус сертификатов .....	78
8.4.7	Карточка сертификата.....	80
8.4.8	Экспорт списка выпущенных сертификатов .....	82
8.4.9	Массовые операции с сертификатами .....	83
8.5	Раздел «Учётные записи».....	86
8.5.1	Создание учётной записи пользователя локального ресурса .....	87
8.5.2	Создание учетной записи для подключённого субъекта .....	88
8.5.3	Изменение статуса учётной записи .....	88
8.5.4	Редактирование учётной записи.....	89
8.5.5	Назначение прав оператору .....	89
8.5.6	Удаление учётной записи .....	89
8.5.7	Выпуск сертификата для учётной записи .....	90
8.6	Управление правилами доступа .....	90
8.6.1	Создание правила доступа .....	91
8.6.2	Редактирование правила доступа .....	94
8.6.3	Удаление правила доступа .....	95
8.7	Управление субъектами доступа .....	95
8.7.1	Фильтрация субъектов ресурсных систем.....	96
8.7.2	Карточка субъекта.....	96
8.7.2.1	Карточка субъекта, подключённого к ресурсной системе .....	96
8.7.2.2	Карточка локального субъекта.....	100
8.7.2.3	Редактирование атрибутов субъекта.....	101
8.7.3	Субъекты локальной ресурсной системы.....	103
8.7.3.1	Создание нового субъекта локальной ресурсной системы.....	103
8.7.4	Субъекты внешнего ресурса.....	104
8.7.5	Создание сертификата для субъекта ресурсной системы .....	105
8.7.6	Создание учётной записи для субъекта .....	105
8.8	Раздел «Ресурсные системы».....	106
8.8.1	Регистрация точки подключения.....	107
8.8.2	Карточка ресурсной системы.....	112
8.8.3	Синхронизация ресурсных систем.....	113
8.8.3.1	Виды синхронизации ресурсных систем.....	113
8.8.3.2	Режимы синхронизации ресурсных систем .....	114
8.8.3.3	Полная синхронизация ресурсной системы в ручном режиме .....	114
8.8.3.4	Частичная синхронизация точки подключения в ручном режиме .....	114
8.8.4	Редактирование параметров точки подключения .....	115
8.8.5	Удаление зарегистрированной ресурсной системой .....	116
8.8.6	Удаление точки подключения к ресурсной системе.....	117
8.9	Раздел «Центры валидации» .....	118
8.9.1	Настройка периодичности автоматического обновления CRL .....	118
8.9.2	Публикация списка отозванных сертификатов CRL по команде .....	121
8.9.3	Экспорт актуального списка отозванных сертификатов CRL .....	121
8.9.4	Регистрация Центра валидации в eCA-CA.....	122
8.9.5	Управление Центрами валидации.....	122
8.9.6	Управление точками распространения .....	125
8.9.6.1	Создание пользовательской точки распространения .....	126
8.9.6.2	Редактирование пользовательской точки распространения.....	129

8.9.6.3	Редактирование автоматической точки распространения.....	130
8.9.6.4	Удаление пользовательской точки распространения .....	131
8.9.6.5	Создание кластера точек распространения .....	131
8.9.6.6	Просмотр состава кластера точек распространения .....	133
8.9.6.7	Редактирование кластера точек распространения .....	134
8.9.6.8	Удаление кластера точек распространения .....	135
8.9.7	Управление службами OCSP.....	136
8.9.7.1	Создание пользовательской службы OCSP .....	137
8.9.7.2	Редактирование пользовательской службы OCSP .....	138
8.9.7.3	Редактирование автоматической службы OCSP.....	138
8.9.7.4	Удаление пользовательской службы OCSP .....	139
8.9.7.5	Создание кластера служб OCSP .....	139
8.9.7.6	Просмотр состава кластера служб OCSP.....	142
8.9.7.7	Редактирование кластера служб OCSP.....	142
8.9.7.8	Удаление кластера служб OCSP .....	144
8.9.8	Получение файлов CRL, Delta CRL и AIA.....	144
8.9.8.1	Получение файлов посредством запуска скрипта из состава программы .....	144
8.9.8.2	Получение файлов посредством использования методов REST API.....	145
8.9.9	Параметры точек распространения в сертификате .....	147
8.10	Журнал событий.....	147
8.10.1	Фиксируемые события .....	147
8.10.2	Просмотр журнала событий.....	184
8.10.2.1	Просмотр записей, не помещённых в архив .....	184
8.10.2.2	Просмотр записей, помещённых в архив .....	186
8.10.3	Экспорт журнала событий.....	186
8.10.4	Архивация журнала событий .....	186
8.10.5	Передача информации о событиях в сторонние системы по протоколу Syslog .....	187
8.11	Управление шаблонами сертификатов .....	188
8.11.1	Общие сведения о работе с шаблонами сертификатов .....	188
8.11.2	Просмотр информации о шаблонах сертификатов.....	190
8.11.3	Просмотр карточки шаблона сертификата .....	191
8.11.4	Настройка выпуска сертификатов с закрытым ключом (PKCS#12).....	195
8.11.5	Создание пользовательского шаблона .....	195
8.11.6	Удаление шаблонов сертификатов .....	205
8.11.7	Импорт шаблонов MS CS.....	207
8.12	Смена сертификата веб-сервера .....	208
8.13	Управление разрешёнными издателями.....	210
8.14	Управление правилами сопоставления атрибутов .....	210
8.14.1	Создание правила сопоставления атрибутов .....	211
8.14.2	Редактирование правила сопоставления атрибутов .....	212
8.14.3	Удаление правила сопоставления атрибутов .....	212
8.15	Управление параметрами рассылки уведомлений об истечении срока действия сертификатов субъектов.....	212
8.15.1	Добавление почтового сервера .....	212
8.15.2	Редактирование параметров почтового сервера.....	214
8.15.3	Удаление почтового сервера .....	214
8.15.4	Добавление шаблона рассылки.....	215
8.15.5	Редактирование шаблона рассылки.....	217
8.15.6	Удаление шаблона рассылки .....	217
8.15.7	Отправка тестового уведомления.....	218
8.16	Управление рассылкой Syslog-сообщений.....	218
8.16.1	Добавление Syslog-сервера.....	218
8.16.2	Редактирование параметров Syslog-сервера .....	219
8.16.3	Удаление Syslog-сервера .....	220
8.17	Просмотр сведений о лицензии и её импорт .....	220
9	Поиск и устранение неисправностей.....	221
Приложение 1.	Создание сертификата для субъекта.....	224

1.1 Способы создания сертификатов .....	224
1.2 Параметры криптографии сертификатов учётных записей пользователей и Центров сертификации .....	225
1.3 Публикация сертификата в ресурсную систему .....	226
1.4 Создание сертификата с закрытым ключом PKCS#12.....	226
1.5 Создание сертификата субъекта по запросу.....	229
1.5.1 Создание сертификата субъекта по запросу в разделе «Сертификаты» .....	229
1.5.2 Создание сертификата субъекта по запросу в разделе «Субъекты».....	238
1.6 Создание сертификата субъекта на ключевом носителе .....	242
1.7 Создание короткоживущего сертификата.....	246
Приложение 2. Описание полей предустановленных шаблонов сертификатов.....	247
Приложение 3. Правила валидации значений полей по умолчанию предустановленных шаблонов сертификатов .....	261
Приложение 4. Описание предустановленных идентификаторов расширенного использования ключа .....	263
Приложение 5. Формат и правила записи значений в поля сертификата на бумажном носителе .....	265
5.1 Формат сертификата на бумажном носителе для физического лица.....	265
5.2 Формат сертификата на бумажном носителе для юридического лица.....	265
5.3 Правила записи значений в поля сертификата на бумажном носителе для физического лица.....	266
5.4 Правила записи значений в поля сертификата на бумажном носителе для юридического лица .....	268
5.5 Пример сертификата на бумажном носителе для физического лица .....	269
5.6 Пример сертификата на бумажном носителе для юридического лица .....	271
Обозначения и сокращения.....	272
Термины и определения .....	273

# 1 РОЛИ УПРАВЛЕНИЯ

В еСА-СА определены следующие роли пользователей:

- «Оператор»

Пользователь с ролью «Оператор» имеет доступ к еСА-СА через веб-интерфейс и программный интерфейс API. Пользователь с данной ролью обладает правами на работу с субъектами, над которыми он может осуществлять свои ролевые права в соответствии с правилами доступа, и предназначенными для них сертификатами (выпуск, отзыв, приостановка и возобновление сертификата), имеет полномочия запуска обновления списка субъектов из ресурсной системы. Для конкретного «Оператора» можно определить перечень субъектов, над которыми он может осуществлять свои ролевые права, а также перечень групп субъектов, над элементами которых он может осуществлять свои ролевые права.

- «Администратор»

Пользователь с ролью «Администратор» имеет неограниченные права доступа к ОС и серверу, на котором развёрнут еСА-СА, а также доступ через веб-интерфейс или программный интерфейс API к функциональным задачам и к функциям управления учётными записями. Все учётные записи могут быть созданы, отредактированы, удалены или заблокированы только пользователем с ролью «Администратор».

Доступные действия пользователей в соответствии с назначенными ролями приведены в таблице 1.

Таблица 1 - Полномочия пользователей в соответствии с назначенной ролью

Тип действия, осуществляемого пользователем, над объектом программы	Возможные роли пользователей	
	Оператор	Администратор
Установка или обновление программы	-	+
Установка лицензии на программу	-	+
Внесение изменений в конфигурационную информацию лицензии на программу	-	+
Просмотр информации о лицензии на ПО	-	+
Инициализация центра сертификации	-	+
Чтение конфигурационной информации о планах архивации в автоматическом режиме из базы данных	-	+
Внесение изменений в конфигурационную информацию о планах архивации в автоматическом режиме из базы данных	-	+
Чтение информации об уведомлениях об истечении срока действия сертификата	-	+
Внесение изменений в информацию об уведомлениях об истечении срока действия сертификата	-	+
Просмотр журнала событий	-	+
Архивация журнала событий	-	+
Экспорт журнала событий	-	+
Просмотр списка сертификатов центра сертификации (свои и подчинённые)	-	+
Импорт и экспорт закрытого ключа центра сертификации	-	+
Удаление сертификата центра сертификации	-	+
Просмотр цепочки сертификатов центра сертификации	-	+
Скачивание цепочки сертификатов центра сертификации	-	+
Скачивание сертификата центра сертификации	-	+
Скачивание сертификата центра сертификации в контейнере #pkcs12	-	+
Подписание запроса на сертификат подчинённого центра сертификации	-	+
Импортирование сертификата центра сертификации (активация центра сертификации)	-	+

Тип действия, осуществляемого пользователем, над объектом программы	Возможные роли пользователей	
	Оператор	Администратор
Создание сертификатов доступа для полного набора субъектов ресурсных систем	-	+
Создание сертификатов доступа для ограниченного набора субъектов ресурсных систем	+	+
Просмотр списка сертификатов доступа для полного набора субъектов ресурсных систем	-	+
Просмотр списка сертификатов доступа для ограниченного набора субъектов ресурсных систем	+	+
Экспорт списка выпущенных сертификатов для полного набора субъектов ресурсных систем	-	+
Экспорт списка выпущенных сертификатов для ограниченного набора субъектов ресурсных систем	+	+
Скачивание сертификата доступа для полного набора субъектов ресурсных систем	-	+
Скачивание сертификата доступа для ограниченного набора доступных субъектов ресурсных систем	+	+
Скачивание сертификата доступа субъекта в контейнере #pkcs12 для полного набора субъектов ресурсных систем	-	+
Скачивание сертификата доступа субъекта в контейнере #pkcs12 для ограниченного набора субъектов ресурсных систем	+	+
Скачивание цепочки сертификатов для полного набора субъектов ресурсных систем	-	+
Скачивание цепочки сертификатов для ограниченного набора субъектов ресурсных систем	+	+
Управление статусом сертификата доступа субъекта для полного набора субъектов ресурсных систем	-	+
Управление статусом сертификата доступа субъекта для ограниченного набора субъектов ресурсных систем	+	+
Создание учётной записи с определением роли для субъектов ресурсных систем	-	+
Управление учётными записями субъектов ресурсных систем	-	+
Просмотр учётных записей субъектов ресурсных систем	-	+
Просмотр ограниченного списка субъектов ресурсных систем	+	+
Просмотр полного списка субъектов ресурсных систем	-	+
Просмотр списка полного набора зарегистрированных ресурсных систем	-	+
Просмотр списка ограниченного набора зарегистрированных ресурсных систем	+	+
Регистрация ресурсных систем	-	+
Обновление полного набора субъектов ресурсных систем	-	+
Обновление ограниченного набора субъектов ресурсных систем	+	+
Просмотр списка зарегистрированных центров валидации	-	+
Управление настройкой обновления списков отозванных сертификатов	-	+
Экспорт списка отозванных сертификатов	-	+
Моментальная публикация списка отозванных сертификатов	-	+
Просмотр шаблонов сертификатов	-	+
Создание нового шаблона сертификата	-	+
Импорт шаблонов сертификатов	-	+
Редактирование созданных шаблонов сертификатов	-	+
Удаление созданных шаблонов сертификатов	-	+
Просмотр идентификаторов расширенного использования ключа	-	+

Тип действия, осуществляемого пользователем, над объектом программы	Возможные роли пользователей	
	Оператор	Администратор
Просмотр ограниченного набора идентификаторов расширенного использования ключа	+	+
Создание пользовательских идентификаторов расширенного использования ключа	-	+
Удаление пользовательских идентификаторов расширенного использования ключа	-	+
Просмотр списка разрешённых издателей	-	+
Управление проверкой издателя	-	+
Перезагрузка веб-сервера	-	+
Контроль целостности исполняемых файлов программы	-	+

## 2 РЕЖИМЫ ФУНКЦИОНИРОВАНИЯ ПРОГРАММЫ

Основным режимом функционирования еСА-СА является нормальный режим. В нормальном режиме должны исправно функционировать клиентская и серверная части программы, обеспечивая возможность круглосуточного функционирования, с перерывами на обслуживание (обновление программы).

Функционирование корневого и/или подчинённого еСА-СА предусматривает автономный режим (Stand alone operation) или сетевой режим работы.

Сетевой режим работы еСА-СА обеспечивает возможность кластеризации с целью отказоустойчивости.

## 3 ЛИЦЕНЗИРОВАНИЕ ПРОГРАММЫ

### 3.1 Лицензионные ограничения

Лицензию необходимо импортировать для каждого eCA-CA.

Лицензия на право использования eCA-CA содержит следующие атрибуты:

- Название организации и ИНН – атрибут может отсутствовать (пример, АО «Аладдин Р.Д.» (ИНН: 7719165935)).
  - Серийный номер лицензии – атрибут может отсутствовать.
  - Исполнение – атрибут может отсутствовать.
  - Срок действия лицензии – лицензия ограничена сроком действия (срок действия лицензии может быть неограничен).
  - Тип технической поддержки – атрибут может отсутствовать.
  - Срок действия технической поддержки – лицензия ограничивает срок действия технической поддержки (атрибут может отсутствовать).
  - Доступные типы центров сертификации – лицензия ограничивает типы Центров сертификации (корневой или подчиненный), которые могут быть созданы.
  - Доступные имена (CN) центров сертификации – лицензия ограничивает имена корневых и подчиненных Центров сертификации, которые могут быть указаны при их создании. Для подчиненных Центров сертификации лицензия ограничивает доступные имена Центров сертификации, которыми могут быть подписаны запросы на выпуск их сертификатов.
  - Доступные имена (CN) корневых центров сертификации – лицензия ограничивает доступные имена корневых Центров сертификации (атрибут отсутствует, если лицензия позволяет создавать только корневые Центры сертификации).
  - Максимальное количество субъектов с действующими сертификатами – лицензия ограничивает максимальное количество субъектов, которые могут быть владельцами действующих сертификатов.
  - Максимальное количество сертификатов для субъекта – лицензия ограничивает максимальное количество сертификатов для одного субъекта.
  - Максимальное количество DNS-имен для субъекта – лицензия ограничивает максимальное количество значений DNS-имен для одного субъекта.
  - Максимальное количество подключаемых доменов – максимальное количество ресурсных систем, которые могут быть подключены.
  - Максимальное количество подключаемых центров валидации – лицензия ограничивает максимальное количество «Центров валидации Aladdin Enterprise Validation Authority», которые могут быть подключены.
  - Максимальное количество подключаемых центров регистрации – лицензия ограничивает максимальное количество eCA-RA, которые могут быть подключены.
  - Возможность использования OCSP – лицензия ограничивает возможность использования службы OCSP.
  - Возможность создания wildcard-сертификатов – лицензия ограничивает возможность выпуска wildcard-сертификатов.
  - Возможность использования HSM – лицензия ограничивает возможность использования программно-аппаратного криптографического модуля «КриптоПро HSM».
  - Возможность использования ключевых носителей Рутокен.
- После истечения срока действия лицензии выпуск сертификатов для субъектов недоступен.
- Возможность создания короткоживущих (short-lived, throwaway) сертификатов – лицензия ограничивает возможность выпуска короткоживущих (short-lived, throwaway) сертификатов.

Сведения об установленной лицензии доступны для просмотра в окне «О программе» (см. Рисунок 1), а также на вкладке «Лицензия» раздела «Настройки» (см. Рисунок 2). На вкладку «Лицензия» раздела «Настройки» можно перейти из окна «О программе», нажав на ссылку «Параметры лицензии и техподдержки».

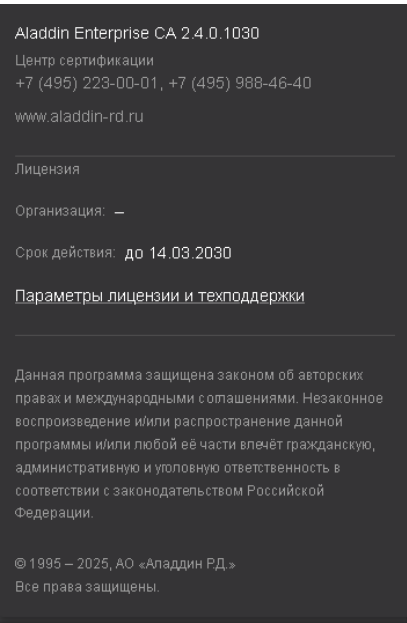


Рисунок 1 – Окно «О программе»

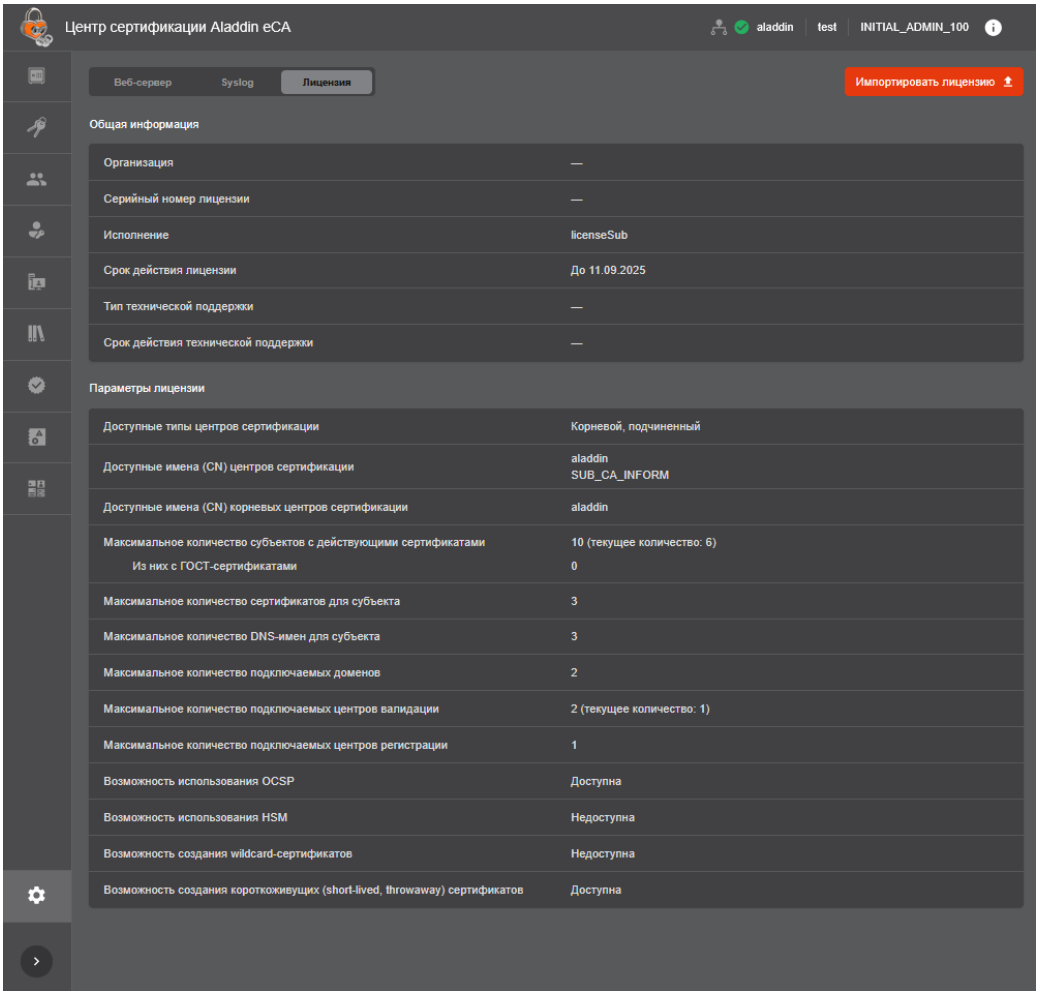


Рисунок 2 – Просмотр параметров лицензии

### 3.2 Первичное лицензирование

Порядок установки лицензии при первичной инициализации:

- При первом подключении к веб-интерфейсу после установки eCA-CA в появившемся окне инициализации выберите файл лицензии с расширением LIC (см. Рисунок 3).  
Один экземпляр лицензии предназначен для одного экземпляра eCA-CA.

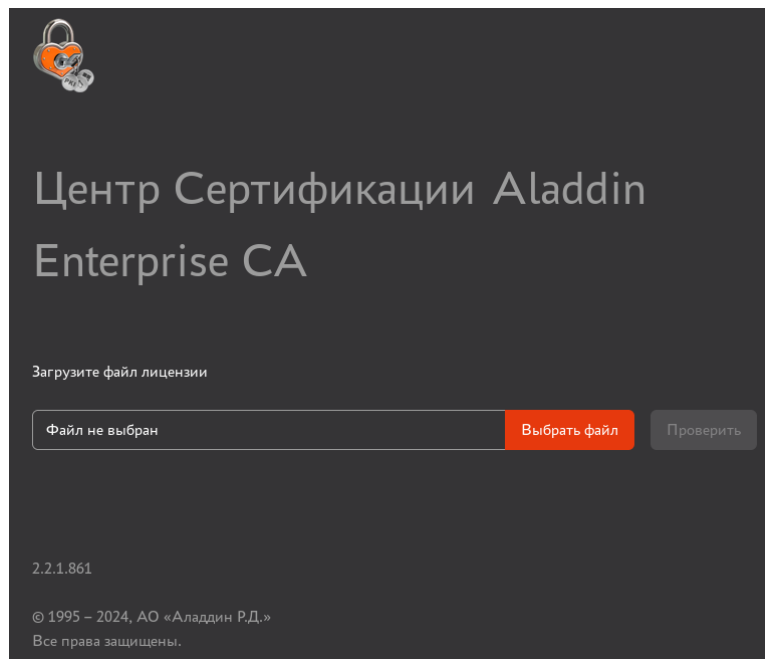


Рисунок 3 – Выбор файла с лицензией

- Нажмите кнопку **<Проверить>** для проверки валидности файла лицензии.
- При проверке лицензии продукта проверяется подпись, срок действия и ключевые поля:
- При несовпадении ключевых полей – «productid» и «id» выводится сообщение «Данная лицензия не предназначена для продукта Aladdin Enterprise CA».
  - При несовпадении подписи лицензии выводится сообщение «Подпись неверна».
  - При истечении срока действия лицензии выводится сообщение «Срок лицензии истёк».
  - При невозможности чтения содержимого файла лицензии выводится сообщение «Некорректный файл».

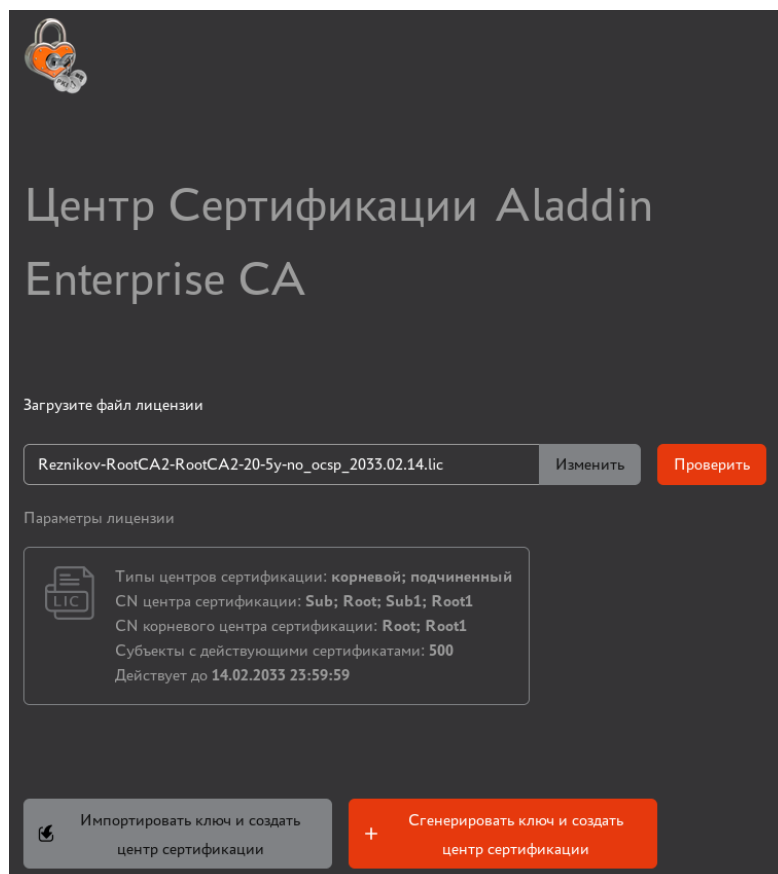


Рисунок 4 – Проверка лицензии выполнена успешно

После успешной проверки будут отображены параметры лицензии (см. Рисунок 4):

- Перечень возможных типов Центров сертификации в поле «Типы центров сертификации».
- Перечень доступных для выбора имён Центра сертификации в поле «CN центра сертификации»<sup>1</sup>.
- Перечень имён корневых Центров сертификации в поле «CN корневого центра сертификации».
- Максимальное количество субъектов с действующими сертификатами в поле «Субъекты с действующими сертификатами».
- Срок действия лицензии в поле «Действует до».

После успешной проверки лицензии перейдите к инициализации Центра сертификации:

- Нажмите кнопку **<Сгенерировать ключ и создать центр сертификации>** для инициализации с генерацией ключа (см. раздел 4.1).
- Нажмите кнопку **<Импортировать ключ и создать центр сертификации>** для перехода к инициализации Центра сертификации с импортом ключа из контейнера PKCS#12 (см. раздел 4.2).

### 3.3 Продление срока действия лицензии

После истечения срока действия установленной лицензии доступ к функционалу еСА-СА прекращается. Для возобновления доступа к программе импортируйте действительную лицензию.

Порядок продления срока действия лицензии:

- На вкладке «Лицензия» раздела «Настройки» нажмите кнопку **<Импортировать лицензию>** (см. Рисунок 2).
- В открывшемся окне импорта лицензии будет доступна информация о текущей установленной лицензии.
- Выберите файл лицензии в формате LIC.

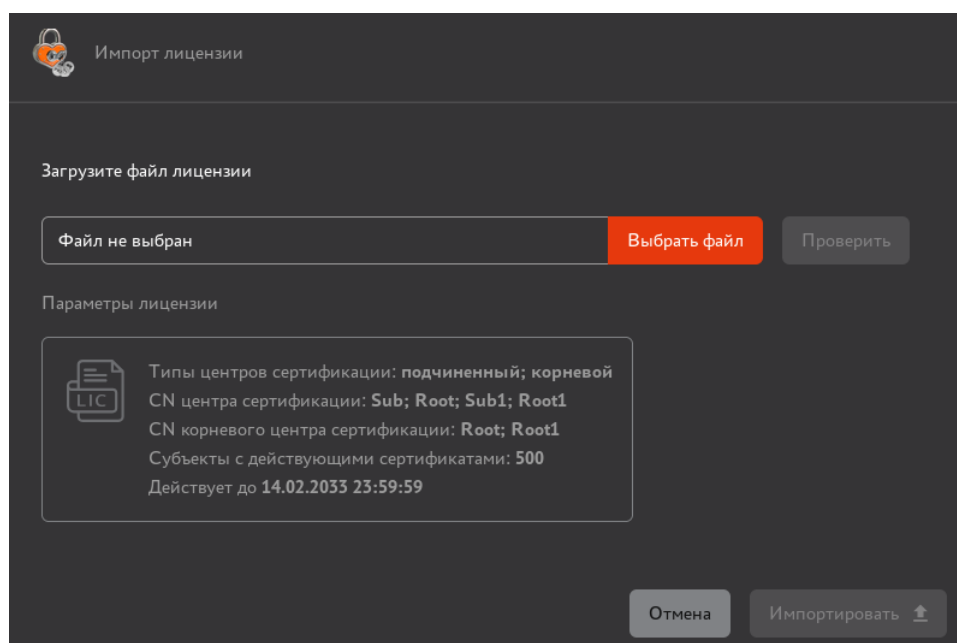


Рисунок 5 – Окно импорта лицензии

- 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 Центров сертификации поле «CN центра сертификации»;

<sup>1</sup> Подчиненным Центрам сертификации возможно задавать имена из перечня доступных для выбора имён Центров сертификации, которые отсутствуют в перечне доступных имен корневых Центров сертификации.

- перечень имён корневых Центров сертификации в поле «CN корневого центра сертификации». Данное поле не отображается, если лицензия позволяет создать только корневой Центр сертификации;
- максимальное количество субъектов с действующими сертификатами в поле «Субъекты с действующими сертификатами»;
- срок действия лицензии в поле «Действует до».

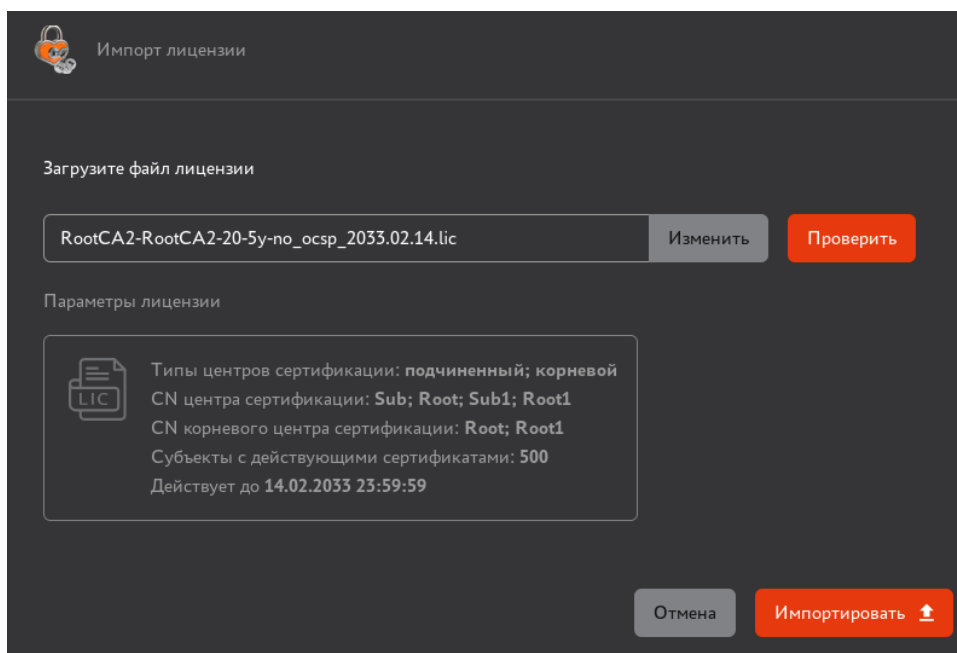


Рисунок 6 – Окно импорта лицензии после успешной проверки на валидность

- Нажмите кнопку **<Импортировать>** для установки лицензии.
- После успешного импорта лицензии:
  - на экран будет выведено уведомление об успешной установке лицензии «Успешно. Лицензия загружена»;
  - будут обновлены данные лицензии в поле «Действует до» окна «О программе»;
  - в журнале событий будет зарегистрировано событие с кодом CAENV002.
- После успешной установки лицензии функционал программы доступен в полном объёме.
- При попытке импорта лицензии, в которой в перечень имён Центров сертификации не входят имена действующих<sup>1</sup> Центров сертификации (учитывается комбинация имени Центра сертификации и корневого Центра сертификации)<sup>2</sup>, генерируется сообщение об ошибке «В импортируемой лицензии отсутствует имя действующего Центра сертификации».

<sup>1</sup> Имеющих статус «Активирован» или «Не активирован».

<sup>2</sup> Импортируемая лицензия позволяет повторно создать любой из действующих ЦС.

## 4 НАЧАЛО РАБОТЫ С ПРОГРАММОЙ

### 4.1 Инициализация Центра сертификации с генерацией ключа

#### 4.1.1 Инициализация корневого Центра сертификации с генерацией ключа

Для инициализации корневого Центра сертификации с генерацией ключа выполните следующие действия:

- На первом шаге мастера инициализации (см. Рисунок 7) выберите тип Центра сертификации «Корневой» и нажмите кнопку **<Продолжить>**. Если лицензия поддерживает создание только корневых центров сертификации, данный шаг отсутствует.

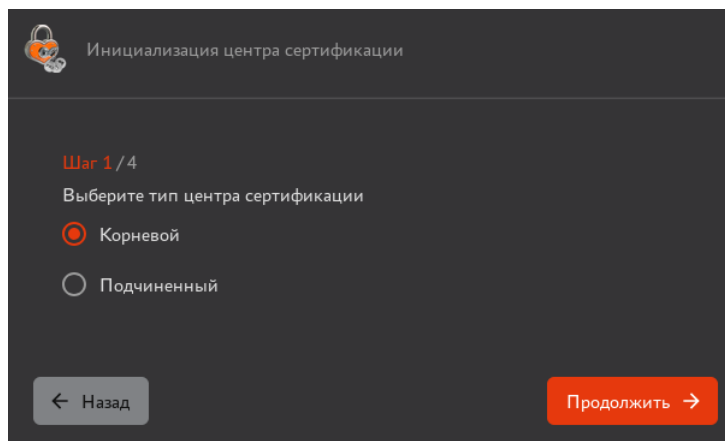


Рисунок 7 — Выбор типа создаваемого Центра сертификации

- На следующем шаге мастера инициализации (см. Рисунок 8) заполните следующие поля и нажмите кнопку **<Продолжить>**:

Рисунок 8 – Указание отображаемого имени и суффикса различающегося имени

- В поле «Отображаемое имя» укажите имя создаваемого Центра сертификации, которое будет отображаться в веб-интерфейсе.
- В списке «Имя центра сертификации» (Common Name) выберите имя создаваемого корневого Центра сертификации из перечня возможных имён, указанных в лицензии.

- В поле «Суффикс различающегося имени» укажите суффикс различающегося имени корневого сертификата. Длина вводимого суффикса различающегося имени не должна превышать 250 байт (включая как имя Центра сертификации, так и суффиксы). Ввод атрибутов возможен в любом порядке, но в сертификате порядок атрибутов будет установлен в соответствии с номерами пунктов, указанными в таблице 2.

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
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
31	DATEOFBIRTH=	Дата рождения OID: 1.3.6.1.5.5.7.9.1
32	PLACEOFBIRTH=	Место рождения OID: 1.3.6.1.5.5.7.9.2
33	ROLE=	Роль OID: 2.5.4.72

- На следующем шаге мастера инициализации (см. Рисунок 9) в соответствующих списках выберите криптопровайдеров для криптографических операций для доступных алгоритмов и нажмите кнопку **<Продолжить>**:

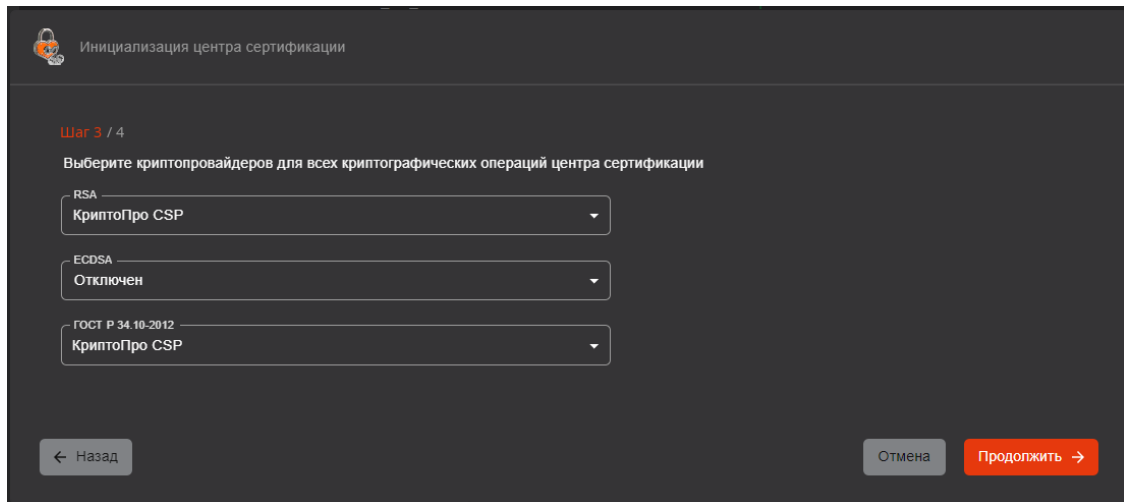


Рисунок 9 — Выбор криптопровайдеров

- «RSA» – список выбора криптопровайдера для алгоритма RSA:
  - Стандартный (по умолчанию).
  - КристоПро CSP <sup>1</sup> (доступен только при наличии активного и подключённого криптопровайдера СКЗИ «КристоПро CSP»).
  - Отключен.
- «ECDSA» – список выбора криптопровайдера для алгоритма ECDSA:
  - Стандартный (по умолчанию).
  - Отключен.
- «ГОСТ Р 34.10–2012» – список выбора криптопровайдера для алгоритма ГОСТ Р 34.10–2012:
  - КристоПро CSP (доступен только при наличии активного и подключённого криптопровайдера СКЗИ «КристоПро CSP»).
  - Отключен (по умолчанию).
- На следующем шаге мастера инициализации (см. Рисунок 10) укажите срок действия сертификата Центра сертификации, параметры криптографии и нажмите кнопку **<Создать ЦС>**:
  - В поле «Срок действия сертификата» с помощью календаря выберите срок действия корневого сертификата (по умолчанию – 15 лет). Максимальный срок действия сертификата определяется шаблоном «Root CA» <sup>2</sup>, по которому будет выпущен сертификат.
  - В списке «Алгоритм ключа» (состав алгоритмов зависит от выбранных провайдеров) выберите алгоритм:
    - RSA;
    - ECDSA;
    - ГОСТ Р 34.10–2012.

<sup>1</sup> Подробная информация по настройке взаимодействия eCA-CA с СКЗИ «КристоПро CSP» приведена в приложении 5 документа «Aladdin Enterprise Certificate Authority Certified Edition. Руководство администратора. Часть 1. Установка и обслуживание «Центра сертификации Aladdin Enterprise Certification Authority».

<sup>2</sup> Информация про шаблон «Root CA» приведена в приложении 2 «Описание полей предустановленных шаблонов сертификатов»

Рисунок 10 — Указание срока действия Центра сертификации и параметров криптографии

- В списке «Длина ключа» выберите длину 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).
- В списке «Алгоритм хэш–суммы» выберите алгоритм хэш-суммы:
  - Для алгоритма ключа RSA и ECDSA: SHA1, SHA256, SHA384, SHA512 (по умолчанию).

**Внимание!** Рекомендуется выбирать алгоритмы хэш–суммы **SHA256, SHA384 или SHA512** (в случае если в качестве алгоритма ключа выбран **RSA или ECDSA**).

- Для алгоритма ключа ГОСТ Р 34.10–2012 – ГОСТ Р 34.11–2012.
- В списке «Место хранения закрытого ключа» выберите место хранения закрытого ключа:
  - Доступные варианты выбора, если криптопровайдером выбранного алгоритма ключа является СКЗИ «КриптоПро CSP»:
    - Локальное хранилище Aladdin eCA (выбрано по умолчанию, требует заранее подготовленной на биологическом датчике случайных чисел (далее – БДСЧ) криптопровайдера СКЗИ «КриптоПро CSP» гаммы).
    - КриптоПро CSP (HDIMAGE).
    - КриптоПро HSM (доступно только при наличии подключения криптопровайдера СКЗИ «КриптоПро CSP» к ПАКМ «КриптоПро HSM»).
  - Для всех других криптопровайдеров в данном поле установлено неизменяемое значение «Локальное хранилище Aladdin eCA».

- Если криптопровайдером хотя бы одного из алгоритмов выбран «КриптоПро CSP», то при выборе места хранения «Локальное хранилище Aladdin eCA» или «КриптоПро CSP (HDIMAGE)» убедитесь, что размер внешней гаммы (размер файла `/opt/aecaCa/dist/gamma/db1/kis_1`) позволяет сгенерировать необходимое количество закрытых ключей. На генерацию одного закрытого ключа длиной 256 бит расходуется 36 байт гаммы, на генерацию одного закрытого ключа длиной 512 бит расходуется 36\*2 байта гаммы и т.д. Если размер внешней гаммы недостаточен, то подготовьте внешнюю гамму при помощи утилиты `genkpim` (см. приложение 5 документа «Центр сертификатов доступа Aladdin Enterprise Certificate Authority Certified Edition. Руководство администратора. Часть 1. Установка и обслуживание Центра сертификации Aladdin Enterprise Certification Authority»).
- С помощью чекбокса «Экспортируемый закрытый ключ» определите возможность экспорта ключа из хранилища.

В случае неудачной попытки создания Центра сертификации выводится одно из сообщений об ошибке, приведённых в таблице 3.

Таблица 3 – Перечень сообщений в случае неудачной попытки создания Центра сертификации

Текст ошибки	Причина																						
Ошибка. Некорректный компонент суффикса различающегося имени – <Имя компонента>	Ввод неизвестного компонента (атрибута) суффикса различающегося имени субъекта																						
Ошибка. Поле <Имя компонента> отсутствует в шаблоне	Ввод компонента (атрибута) суффикса различающегося имени, отсутствующего в выбранном шаблоне																						
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 <code>attributeName</code> : Значение не соответствует регулярному выражению: « <code>regex</code> »	<p>Ошибка валидации введённого значения атрибута различающегося имени<sup>1</sup>. Возможные значения переменной «<code>attributeName</code>» и соответствующие им значения переменной «<code>regex</code>» представлены в таблице ниже:</p> <table> <tr> <th><code>attributeName</code></th><th><code>regex</code></th></tr> <tr> <td>C</td><td><code>^[A-Za-z]{2}\$</code></td></tr> <tr> <td>DN</td><td><code>^[A-Za-z0-9"()+,\.\/:=? ]+\$</code></td></tr> <tr> <td>EMAILADDRESS</td><td><code>^[A-Za-zA-Яa-я0-9._-]+@[A-Za-zA-Яa-я0-9._-]+\$</code></td></tr> <tr> <td>SERIALNUMBER</td><td><code>^[A-Za-z0-9"()+,\.\/:=? ]+\$</code></td></tr> <tr> <td>INN</td><td><code>^\d{12}\$</code></td></tr> <tr> <td>OGRN</td><td><code>^\d{13}\$</code></td></tr> <tr> <td>OGRNIP</td><td><code>^\d{15}\$</code></td></tr> <tr> <td>SNILS</td><td><code>^\d{11}\$</code></td></tr> <tr> <td>INNLE</td><td><code>^\d{10}\$</code></td></tr> <tr> <td>DATEOFBIRTH</td><td><code>^(?:31\.(0[13578] 1[02]) (?:30 29)\.(0[13-9] 1[0-2]) (?:0[1-9] 1[0-9] 2[0-8])\.(0[1-9] 1[0-2]) \d{4}29.02\.(?:\d{2}(?:0[48] [2468][048] [13579][26]) (?:02468[048] [13579][26])00))\$</code></td></tr> </table>	<code>attributeName</code>	<code>regex</code>	C	<code>^[A-Za-z]{2}\$</code>	DN	<code>^[A-Za-z0-9"()+,\.\/:=? ]+\$</code>	EMAILADDRESS	<code>^[A-Za-zA-Яa-я0-9._-]+@[A-Za-zA-Яa-я0-9._-]+\$</code>	SERIALNUMBER	<code>^[A-Za-z0-9"()+,\.\/:=? ]+\$</code>	INN	<code>^\d{12}\$</code>	OGRN	<code>^\d{13}\$</code>	OGRNIP	<code>^\d{15}\$</code>	SNILS	<code>^\d{11}\$</code>	INNLE	<code>^\d{10}\$</code>	DATEOFBIRTH	<code>^(?:31\.(0[13578] 1[02]) (?:30 29)\.(0[13-9] 1[0-2]) (?:0[1-9] 1[0-9] 2[0-8])\.(0[1-9] 1[0-2]) \d{4}29.02\.(?:\d{2}(?:0[48] [2468][048] [13579][26]) (?:02468[048] [13579][26])00))\$</code>
<code>attributeName</code>	<code>regex</code>																						
C	<code>^[A-Za-z]{2}\$</code>																						
DN	<code>^[A-Za-z0-9"()+,\.\/:=? ]+\$</code>																						
EMAILADDRESS	<code>^[A-Za-zA-Яa-я0-9._-]+@[A-Za-zA-Яa-я0-9._-]+\$</code>																						
SERIALNUMBER	<code>^[A-Za-z0-9"()+,\.\/:=? ]+\$</code>																						
INN	<code>^\d{12}\$</code>																						
OGRN	<code>^\d{13}\$</code>																						
OGRNIP	<code>^\d{15}\$</code>																						
SNILS	<code>^\d{11}\$</code>																						
INNLE	<code>^\d{10}\$</code>																						
DATEOFBIRTH	<code>^(?:31\.(0[13578] 1[02]) (?:30 29)\.(0[13-9] 1[0-2]) (?:0[1-9] 1[0-9] 2[0-8])\.(0[1-9] 1[0-2]) \d{4}29.02\.(?:\d{2}(?:0[48] [2468][048] [13579][26]) (?:02468[048] [13579][26])00))\$</code>																						
Ошибка при создании Центра сертификации. Неизвестная ошибка	Внутренняя ошибка ПО																						

При успешном создании корневого Центра сертификации и завершении инициализации в открывшемся окне (см. Рисунок 11) вы можете:

<sup>1</sup> Правила валидации значений атрибутов представлены в приложении 3 «Правила валидации значений полей по умолчанию предустановленных шаблонов сертификатов».

- Выгрузить сертификат созданного корневого Центра сертификации – кнопка **<Скачать сертификат>**.
- Выгрузить цепочку сертификатов – кнопка **<Скачать цепочку>**.
- Открыть страницу созданного Центра сертификации – кнопка **<Открыть центр сертификации>**.

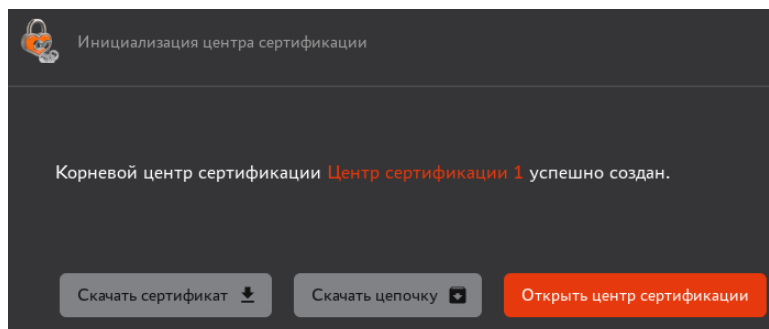


Рисунок 11 – Корневой Центр сертификации успешно создан

#### 4.1.2 Инициализация подчинённого Центра сертификации с генерацией ключа

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

- На первом шаге мастера инициализации (см. Рисунок 7) выберите тип Центра сертификации «Подчинённый» и нажмите кнопку **<Продолжить>**.
- На следующем шаге мастера инициализации (см. Рисунок 12) заполните следующие поля и нажмите кнопку **<Продолжить>**:

Рисунок 12 — Указание отображаемого имени и суффикса различающегося имени

- В поле «Отображаемое имя» введите имя создаваемого Центра сертификации, которое будет отображаться в веб-интерфейсе. Имя может содержать буквы латинского и/или кириллического алфавита, цифры от 0 до 9, символы таблицы ASCII. Максимальная длина имени 200 символов.
- В списке «Имя центра сертификации» (Common Name) выберите имя создаваемого корневого Центра сертификации из перечня возможных имён, указанных в лицензии.

- В поле «Суффикс различающегося имени» укажите суффикс различающегося имени корневого сертификата. Длина вводимого суффикса различающегося имени не должна превышать 250 байт (включая как имя Центра сертификации, так и суффиксы). Ввод атрибутов возможен в любом порядке, но в сертификате порядок атрибутов будет установлен в соответствии с номерами пунктов, указанными в таблице 2.
- На следующем шаге мастера инициализации (см. рисунок 13) в соответствующих списках выберите криптопровайдеров для криптографических операций для доступных алгоритмов и нажмите кнопку **<Продолжить>**:
  - «RSA» – поле выбора криптопровайдера для алгоритма RSA, допустимые варианты выбора:
    - Стандартный (по умолчанию);
    - КриптоПро CSP<sup>1</sup> (доступен только при наличии активного и подключённого криптопровайдера СКЗИ «КриптоПро CSP»);
    - 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 подключённого криптопровайдера СКЗИ «КриптоПро CSP»);
    - Отключен (по умолчанию).

Рисунок 13 — Инициализация подчинённого ЦС. Шаг 3 мастера инициализации


**Внимание!** 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.

- На следующем шаге мастера инициализации выберите параметры криптографии (см. Рисунок 14) и нажмите кнопку **<Создать ЦС>**:
  - «Алгоритм ключа» (состав алгоритмов зависит от выбранных провайдеров):
    - RSA;
    - ECDSA;

<sup>1</sup> Подробная информация по настройке взаимодействия еCA-CA с СКЗИ «КриптоПро CSP» описана в приложении 5 документа «Центр сертификатов доступа Aladdin Enterprise Certificate Authority Certified Edition. Руководство администратора. Часть 1. Установка и обслуживание «Центра сертификации Aladdin Enterprise Certification Authority».

- 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 БДСЧ криптопровайдера СКЗИ «КриптоПро CSP» гаммы);
    - КриптоПро CSP (HDIMAGE);
    - КриптоПро HSM (доступно только при наличии подключения криптопровайдера СКЗИ «КриптоПро CSP» к ПАКМ «КриптоПро HSM»).
  - Для других криптопровайдеров в данном поле указано неизменяемое значение «Локальное хранилище Aladdin eCA».
- Если криптопровайдером хотя бы одного из алгоритмов выбран «КриптоПро CSP», то при выборе места хранения «Локальное хранилище Aladdin eCA» или «КриптоПро CSP (HDIMAGE)» убедитесь, что размер внешней гаммы (размер файла `/opt/aecaCa/dist/gamma/db1/kis_1`) позволяет сгенерировать необходимое количество закрытых ключей. На генерацию одного закрытого ключа длиной 256 бит расходуется 36 байт гаммы, на генерацию одного закрытого ключа длиной 512 бит расходуется 36\*2 байта гаммы и т.д. Если размер внешней гаммы недостаточен, то подготовьте внешнюю гамму при помощи утилиты `genkpim` (см. приложение 5 документа «Центр сертификатов доступа Aladdin Enterprise Certificate Authority Certified Edition. Руководство администратора. Часть 1. Установка и обслуживание Центра сертификации Aladdin Enterprise Certification Authority»).
- С помощью чек-бокса «Экспортируемый закрытый ключ» определите возможность экспорта ключа из хранилища.

**Внимание!** 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 Центра сертификации.



Инициализация центра сертификации

Шаг 4 / 4

Задайте параметры криптографии

Алгоритм ключа

RSA

Длина ключа

3072

Алгоритм хэш-суммы

SHA384

Место хранения закрытого ключа центра сертификации

Место хранения

Локальное хранилище Aladdin eCA

☒ Экспортируемый закрытый ключ

Для генерации ключей по алгоритмам, криптопровайдером которых является «КриптоПро CSP», требуется наличие внешней гаммы. Убедитесь в ее достаточном объеме.

← Назад

Отмена

Создать ЦС →

Рисунок 14 — Инициализация подчинённого ЦС. Шаг 4 мастера инициализации

- В случае неудачной попытки создания Центра сертификации будет отображено одно из сообщений об ошибке, приведённых в таблице 4.

Таблица 4 – Перечень сообщений в случае неудачной попытки создания Центра сертификации

Текст ошибки	Причина
Ошибка. Некорректный компонент суффикса различающегося имени – <Имя компонента>	Ввод неизвестного компонента (атрибута) суффикса различающегося имени субъекта
Ошибка. Поле <Имя компонента> отсутствует в шаблоне	Ввод компонента (атрибута) суффикса различающегося имени, отсутствующего в выбранном шаблоне.
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.

Текст ошибки	Причина																						
Ошибка. Ошибка атрибута attributeName: Значение не соответствует регулярному выражению: «regex»	Ошибка валидации введенного значения атрибута различающегося имени <sup>1</sup> . Возможные значения переменной «attributeName» и соответствующие им значения переменной «regex» представлены в таблице ниже:																						
	<table><tr><td>attributeName</td><td>regex</td></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-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><tr><td>DATEOFBIRTH</td><td>^(?:31\.(0[13578] 1[02]) (?30 29)\.(0[13-9] 1[0-2]) (?0[1-9] 1[0-9] 2[0-8])\.(0[1-9] 1[0-2]))\.\d{4} 29\.(02\.(?:\d{2}(?:0[48] [2468][048] 13579)[26]) (?02468 [048][13579][26])00))\$</td></tr></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}\$	DATEOFBIRTH	^(?:31\.(0[13578] 1[02]) (?30 29)\.(0[13-9] 1[0-2]) (?0[1-9] 1[0-9] 2[0-8])\.(0[1-9] 1[0-2]))\.\d{4} 29\.(02\.(?:\d{2}(?:0[48] [2468][048] 13579)[26]) (?02468 [048][13579][26])00))\$
	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}\$																						
DATEOFBIRTH	^(?:31\.(0[13578] 1[02]) (?30 29)\.(0[13-9] 1[0-2]) (?0[1-9] 1[0-9] 2[0-8])\.(0[1-9] 1[0-2]))\.\d{4} 29\.(02\.(?:\d{2}(?:0[48] [2468][048] 13579)[26]) (?02468 [048][13579][26])00))\$																						
Ошибка при создании Центра сертификации. Неизвестная ошибка	Внутренняя ошибка ПО																						

При успешном создании Подчинённого Центра сертификации и завершении инициализации Центра сертификации откроется соответствующее окно (см. Рисунок 15), в котором будут возможны следующие действия:

- Скачать запрос на сертификат созданного подчинённого Центра сертификации.
- Импортировать цепочку сертификатов Центра сертификации, подписавшего запрос на сертификат подчинённого ЦС, и сам сертификат Подчинённого ЦС.
- Закрыть окно инициализации Подчинённого Центра сертификации.

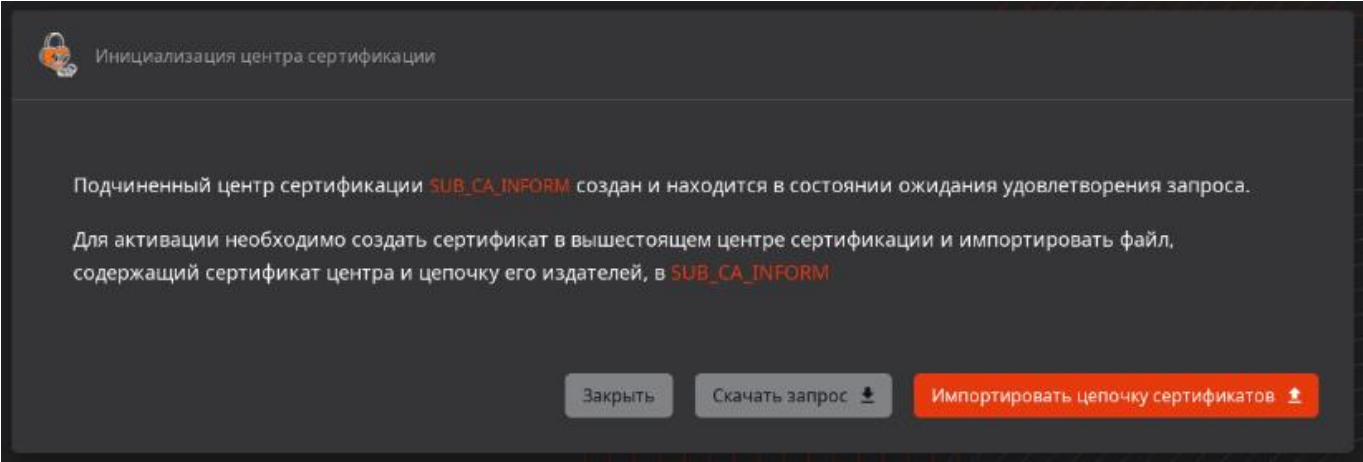


Рисунок 15 – Запрос на создание сертификата Подчинённого Центра сертификации создан

- Скачайте созданный запрос на сертификат Подчинённого Центра сертификации в формате `.csr`.
- На данном этапе Подчинённый Центр сертификации создан и отображается на вкладке «Свои сертификаты» и имеет статус «Запрос» (см. Рисунок 16).

<sup>1</sup> Правила валидации значений атрибутов представлены в приложении 3 «Правила валидации значений полей по умолчанию предустановленных шаблонов сертификатов».

Для перевода Подчинённого Центра сертификации в состояние «Активирован» необходимо выполнить подписание запроса на Корневом Центре сертификации (см. раздел 8.3.2.2) и затем импортировать подписанный сертификат Подчинённого Центра сертификации и его цепочку сертификатов<sup>1</sup> (см. раздел 8.3.1.6).

До момента активации у Подчинённого Центра сертификации в контейнере закрытого ключа содержится самоподписанный технологический сертификат, а после успешной активации в контейнере закрытого ключа Подчинённого Центра сертификации будут содержаться закрытый ключ данного Центра сертификации и цепочка сертификатов данного Центра сертификации.

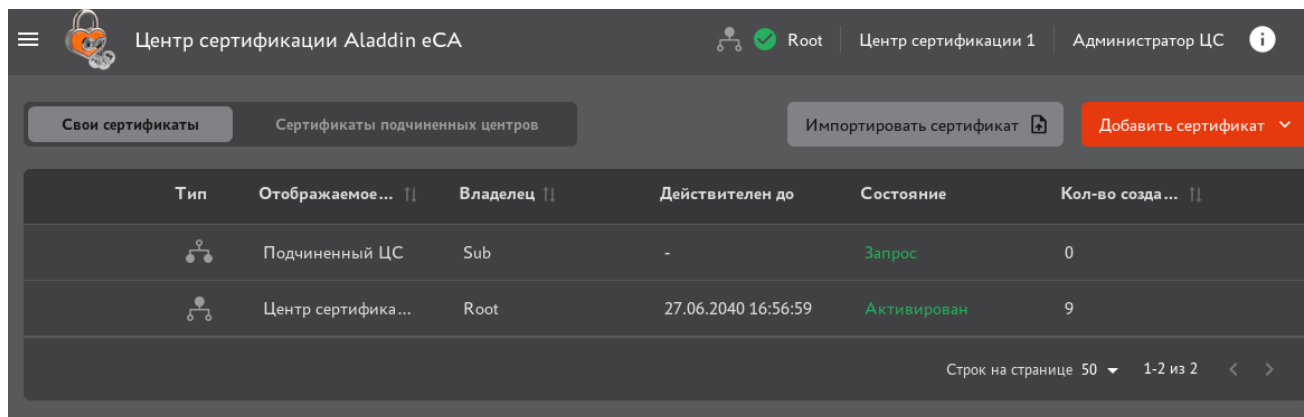


Рисунок 16 – Подчинённый Центр сертификации в состоянии «Запрос»

## 4.2 Инициализация Центра сертификации с импортом ключа

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

- В появившемся модальном окне «Окно инициализации центра сертификации с импортом ключа. Шаг 1/3» (см. Рисунок 17) выберите файл контейнера ключей PKCS#12 и введите пароль от него.

**Внимание!** eCA-CA поддерживает следующие алгоритмы хэш–суммы ключа при импорте контейнера Корневого Центра сертификации: SHA1, SHA256, SHA384, SHA512, SHA3–256, SHA3–384, SHA3–512, RSASSA–PSS.

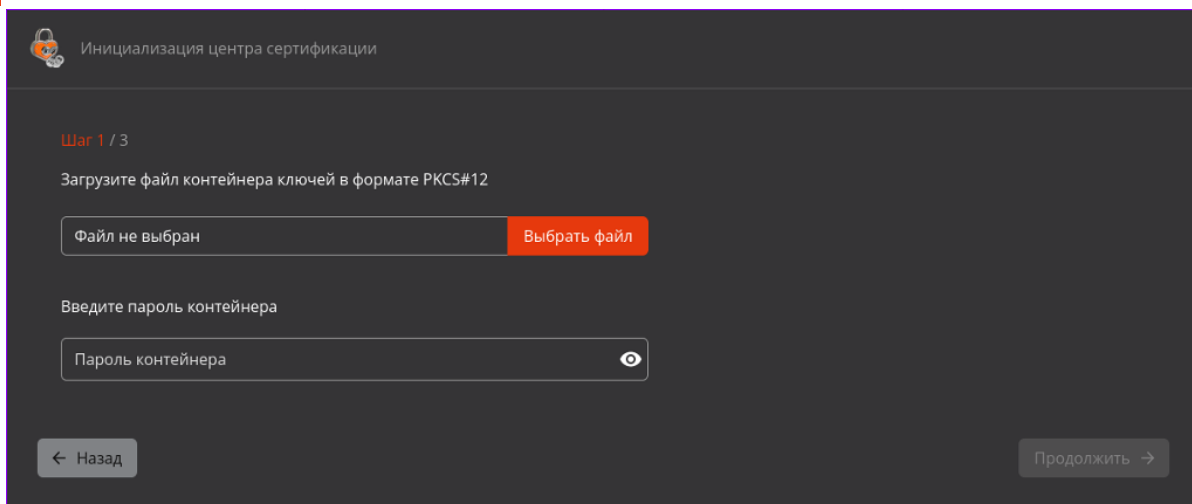


Рисунок 17 – Выбор контейнера ключей PKCS#12

- После выбора файла и ввода пароля необходимо нажать кнопку **<Проверить>**, которая появляется после их заполнения (см. Рисунок 18).

<sup>1</sup> **Цепочка сертификатов** — это последовательность цифровых сертификатов, которая устанавливает доверие между конечным сертификатом и корневым центром сертификации.

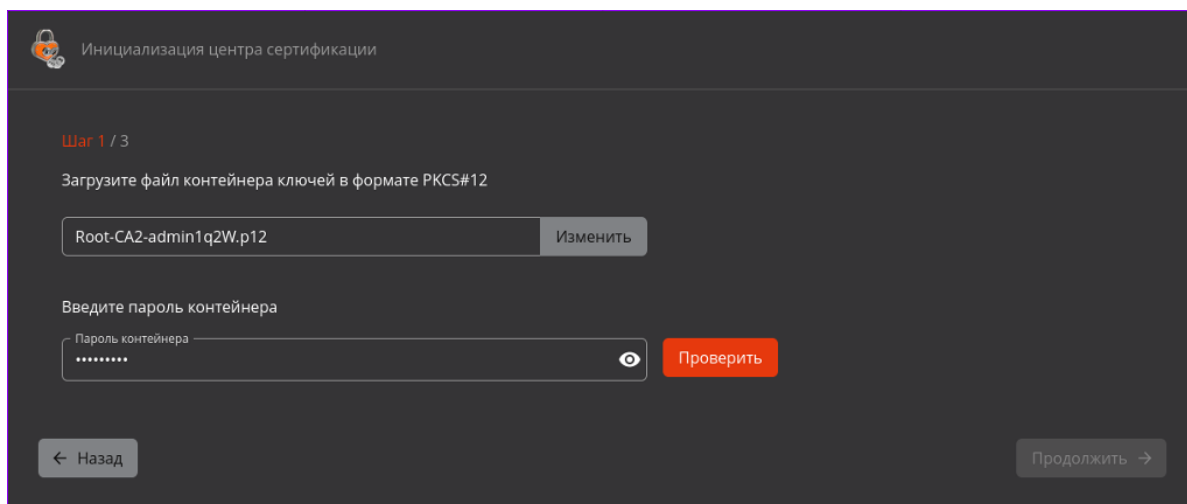


Рисунок 18 – Проверка сертификата

Список возможных ошибок, возникающих при проверке сертификата, приведен в таблице 5.

Таблица 5 – Возможные ошибки при проверке контейнера ключей PKCS#12

Ошибка	Причина
<b>Формат файла</b>	
Ошибка. Некорректный формат файла контейнера.	Формат файла контейнера не соответствует PKCS#12.
Ошибка. Неверный пароль контейнера.	Не удалось открыть контейнер с помощью указанного пароля.
<b>Лицензионные ограничения</b>	
Ошибка. Лицензионные ограничения не позволяют создать <Тип ЦС> ЦС.	Тип Центра сертификации из контейнера не входит в разрешённые типы Центров сертификации из лицензии.
Ошибка. Лицензионные ограничения не позволяют создать ЦС с именем <Имя ЦС>.	Указанное в контейнере «CN» суффикса различающегося имени значение не входит в перечень значений имени Центра сертификации из лицензии.
Ошибка. Лицензионные ограничения не позволяют создать ЦС с издателем <Имя издателя>.	Указанное в контейнере имя издателя сертификата не входит в перечень значений имени корневых Центров сертификации из лицензии.
<b>Сертификат</b>	
Ошибка. Срок действия сертификата истёк.	Текущая дата превышает дату завершения срока действия сертификата, указанную в контейнере.
Ошибка. Срок действия сертификата <Имя> из цепочки истёк.	Текущая дата превышает завершения срока действия сертификата какого-либо сертификата из цепочки сертификатов (за исключением сертификата из контейнера).
Ошибка. Сертификат не является сертификатом ЦС.	У сертификата в поле 2.5.29.19 «Basic Constraints» (Основные ограничения) не указано, что субъектом является Центр сертификации.
<b>Параметры криптографии</b>	
Ошибка. Неподдерживаемый алгоритм ключа: <Алгоритм> <Длина ключа>.	Неподдерживаемый алгоритм ключа или его длина.
Ошибка. Неподдерживаемый алгоритм хэш–суммы: <Алгоритм>.	Неподдерживаемый алгоритм хэш–суммы.
<b>Прочее</b>	
Ошибка. Неизвестная ошибка.	Внутренняя ошибка ПО.

После проверки данных контейнера PKCS#12 выводится следующая информация (см. Рисунок 19 и Рисунок 20) в информационном элементе «Сертификат» раздела «Параметры контейнера»:

- Наименование издателя.
- Наименование субъекта.
- Срок действия сертификата.

- Цепочка сертификатов.
- Алгоритм ключа.
- Длина ключа.

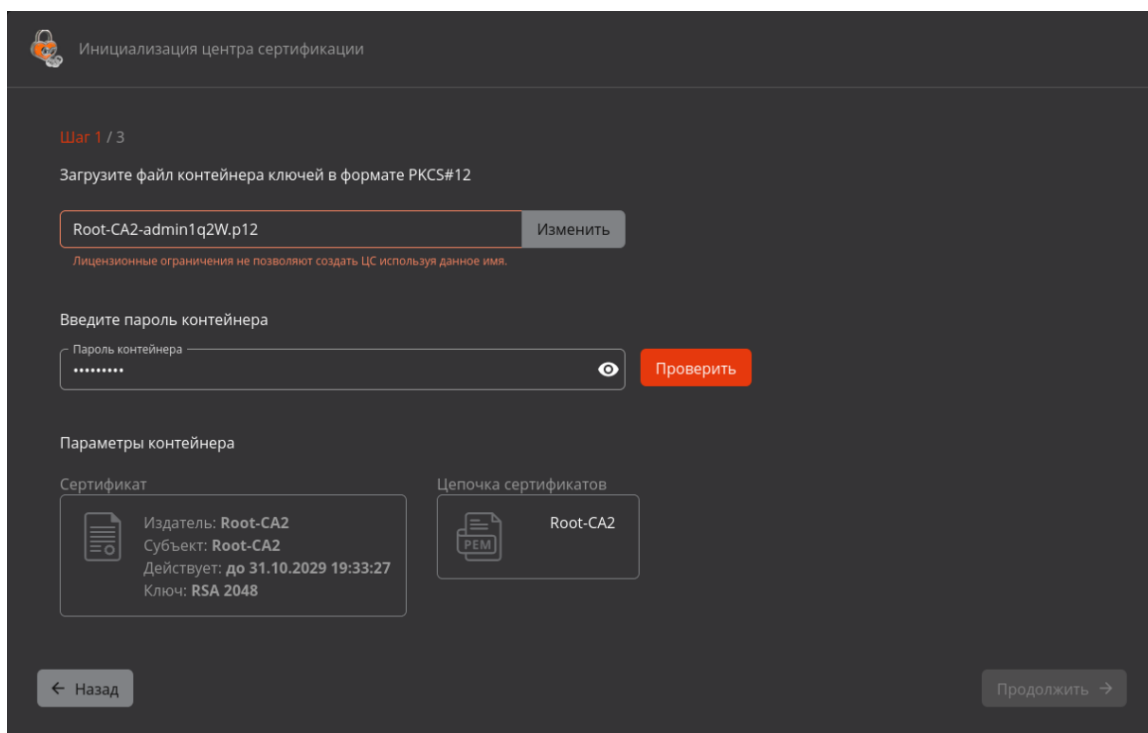


Рисунок 19 – Проверка сертификата выполнена с ошибкой

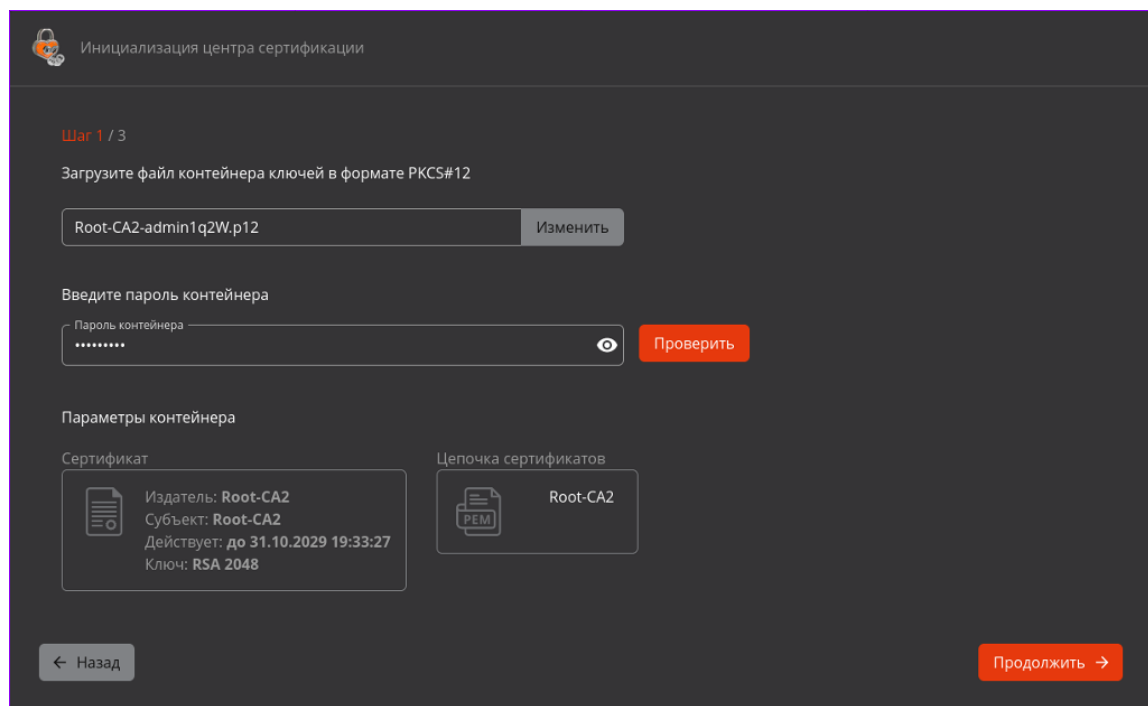


Рисунок 20 – Проверка сертификата выполнена успешно

- Для перехода к следующему шагу нажмите кнопку **<Продолжить>**.


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

- На следующем шаге мастера инициализации выполните следующие действия:
  - В поле «Отображаемое имя» – введите имя создаваемого Центра сертификации, которое будет отображаться в интерфейсе eCA-CA. Имя может содержать буквы латинского и/или кириллического алфавита, цифры от 0 до 9, символы таблицы ASCII, максимальная длина 200 символов.
  - В списке «Место хранения закрытого ключа центра сертификации» выберите место хранения закрытого ключа. Список мест хранения зависит от:
    - алгоритма ключа, указанного в контейнере PKCS#12;
    - криптопровайдера закрытого ключа, определяемого при проверке контейнера PKCS#12<sup>1</sup>;
    - наличия активного криптопровайдера СКЗИ «КриптоПро CSP» на хосте eCA-CA;
    - наличия подключения криптопровайдера СКЗИ «КриптоПро CSP» к ПАКМ «КриптоПро HSM».

Варианты мест хранения закрытого ключа представлены в таблице 6.

Таблица 6 – Варианты мест хранения закрытого ключа

Алгоритм ключа	Криптопровайдер ключа	Место хранения
RSA	Стандартный	Локальное хранилище Aladdin eCA. КриптоПро CSP (HDIMAGE) - при наличии активного криптопровайдера СКЗИ «КриптоПро CSP» на хосте eCA-CA. КриптоПро HSM - при активном криптопровайдере СКЗИ «КриптоПро CSP» на хосте eCA-CA и подключении криптопровайдера СКЗИ «КриптоПро CSP» к ПАКМ «КриптоПро HSM».
RSA	КриптоПро CSP	КриптоПро CSP (HDIMAGE) - при наличии активного криптопровайдера СКЗИ «КриптоПро CSP» на хосте eCA-CA. КриптоПро HSM - при активном криптопровайдере СКЗИ «КриптоПро CSP» на хосте eCA-CA и подключении криптопровайдера СКЗИ «КриптоПро CSP» к ПАКМ «КриптоПро HSM».
ECDSA	Стандартный	Локальное хранилище Aladdin eCA.
ГОСТ Р 34.11–2012	КриптоПро CSP	КриптоПро CSP (HDIMAGE) - при наличии активного криптопровайдера СКЗИ «КриптоПро CSP» на хосте eCA-CA КриптоПро HSM - при активном криптопровайдере СКЗИ «КриптоПро CSP» на хосте eCA-CA и подключении криптопровайдера СКЗИ «КриптоПро CSP» к ПАКМ «КриптоПро HSM».


Инициализация центра сертификации

Шаг 2 / 3

Укажите отображаемое имя и место хранения закрытого ключа

Отображаемое имя

NameCA

Длина: 200 символов

Место хранения закрытого ключа центра сертификации

Локальное хранилище Aladdin eCA

← Назад

Отмена

Продолжить →

Допустим ввод следующих символов:  
0-9, A-Z, a-z, A-Я, а-я, символы из ASCII таблицы

Для данного ключа с криптопровайдером Стандартный доступны следующие места хранения: Локальное хранилище Aladdin eCA, КриптоПро CSP (HDIMAGE), КриптоПро HSM

Рисунок 21 – Окно инициализации Центра сертификации. Шаг 2/3

<sup>1</sup> Данная зависимость обусловлена тем, что возможности работы с закрытым ключом в Java зависят от криптопровайдера, создавшего данный ключ. Например, при использовании криптопровайдера СКЗИ «КриптоПро CSP» работа происходит не с самим закрытым ключом, а с его дескриптором и доступ к данным закрытого ключа отсутствует.

АО "Аладдин Р.Д.", 1995—2026 г.

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

Смп. 32 / 275

- 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 22 и Рисунок 23):
  - «RSA» – поле выбора криптопровайдера для алгоритма RSA, допустимые варианты выбора:
    - Стандартный (по умолчанию);
    - КриптоПро CSP<sup>1</sup> (доступен только при наличии активного и подключённого криптопровайдера СКЗИ «КриптоПро CSP»);
    - 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 подключённого криптопровайдера СКЗИ «КриптоПро CSP»).
    - Отключен (по умолчанию).
  - поле «Алгоритм хэш–суммы»:
    - Для корневого Центра сертификации значение берётся из контейнера PKCS#12 (см. Рисунок 22). При этом поле заблокировано. Поддерживаются следующие алгоритмы хэш–суммы ключа: SHA1, SHA256, SHA384, SHA512, SHA3–256, SHA3–384, SHA3–512, RSASSA–PSS.
    - Для Подчинённого Центра сертификации необходимо возможно выбрать следующие значения (см. Рисунок 23):
      - 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 22 — Выбор криптопровайдеров и параметров криптографии для Корневого Центра сертификации

<sup>1</sup> Подробная информация по настройке взаимодействия eCA-CA с СКЗИ «КриптоПро CSP» описана в приложении 5 документа «Центр сертификатов доступа Aladdin Enterprise Certificate Authority Certified Edition. Руководство администратора. Часть 1. Установка и обслуживание «Центра сертификации Aladdin Enterprise Certification Authority».

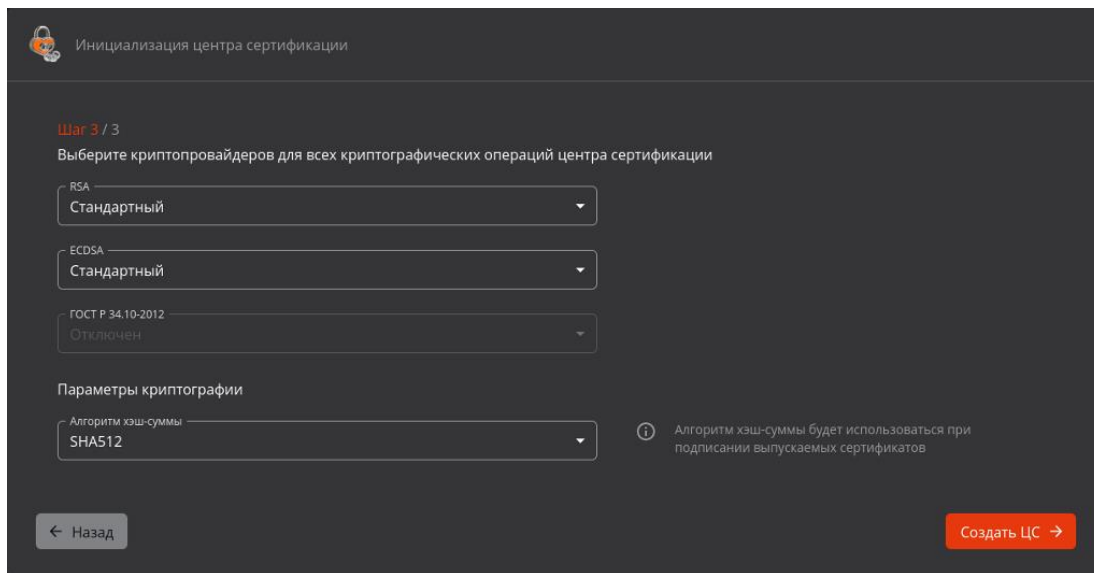


Рисунок 23 – Выбор криптопровайдеров и параметров криптографии для Подчинённого Центра сертификации

**Внимание!** 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 Центра сертификации отобразится модальное окно с сообщением об успешном создании и активации Центра сертификации (см. Рисунок 24 и Рисунок 25). В модальном окне есть следующие кнопки:

- <Скачать сертификат> – при нажатии происходит скачивание сертификата созданного Центра сертификации;
- <Скачать цепочку сертификатов> – при нажатии происходит скачивание цепочки сертификатов созданного Центра сертификации;
- <Открыть созданный центр сертификации> – при нажатии на кнопку происходит переход в раздел «Центр сертификации» с активной вкладкой «Свои сертификаты».

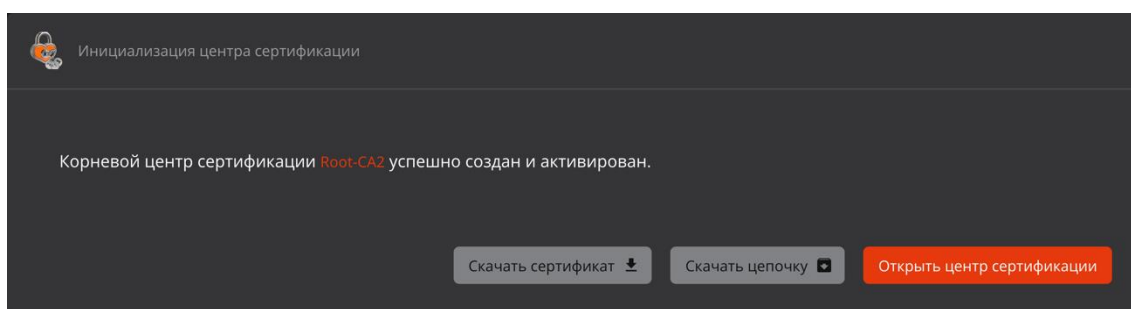


Рисунок 24 – Окно завершения инициализации корневого Центра сертификации

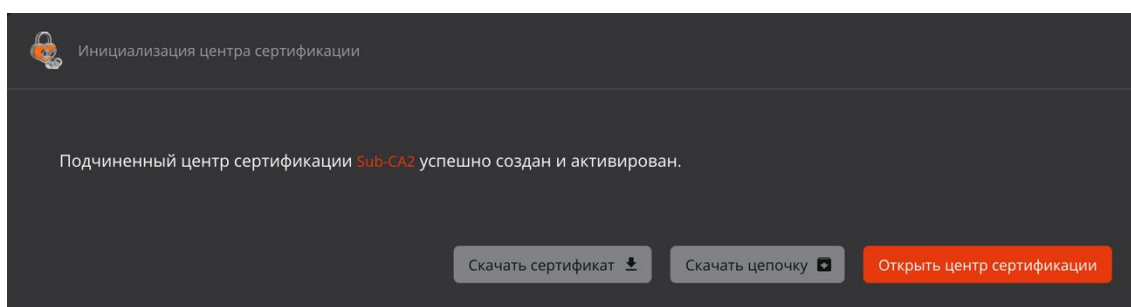


Рисунок 25 – Окно завершения инициализации Подчинённого Центра сертификации

### 4.3 Переопределение сведений, отображаемых в окне авторизации и в заголовке вкладки браузера

Для переопределения сведений, отображаемых в окне авторизации и в заголовке вкладки браузера (см. рисунок 26):

1. В конфигурационном файле `/opt/aecaCa/scripts/config.sh` задайте необходимые значения параметрам:
  - `login_window_product_name` (для переопределения названия продукта, отображаемого в окне авторизации);
  - `login_window_component_name` (для переопределения названия компонента, отображаемого в окне авторизации);
  - `tab_title` (для переопределения текста, отображаемого в заголовке вкладок браузера).
2. Для применения внесённых настроек запустите сценарий обновления при помощи команды с правами суперпользователя:

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

3. Установщик предложит выбрать необходимое действие в интерактивном режиме.
4. Введите в терминале цифру «2».
5. Дождитесь окончания выполнения сценария обновления.

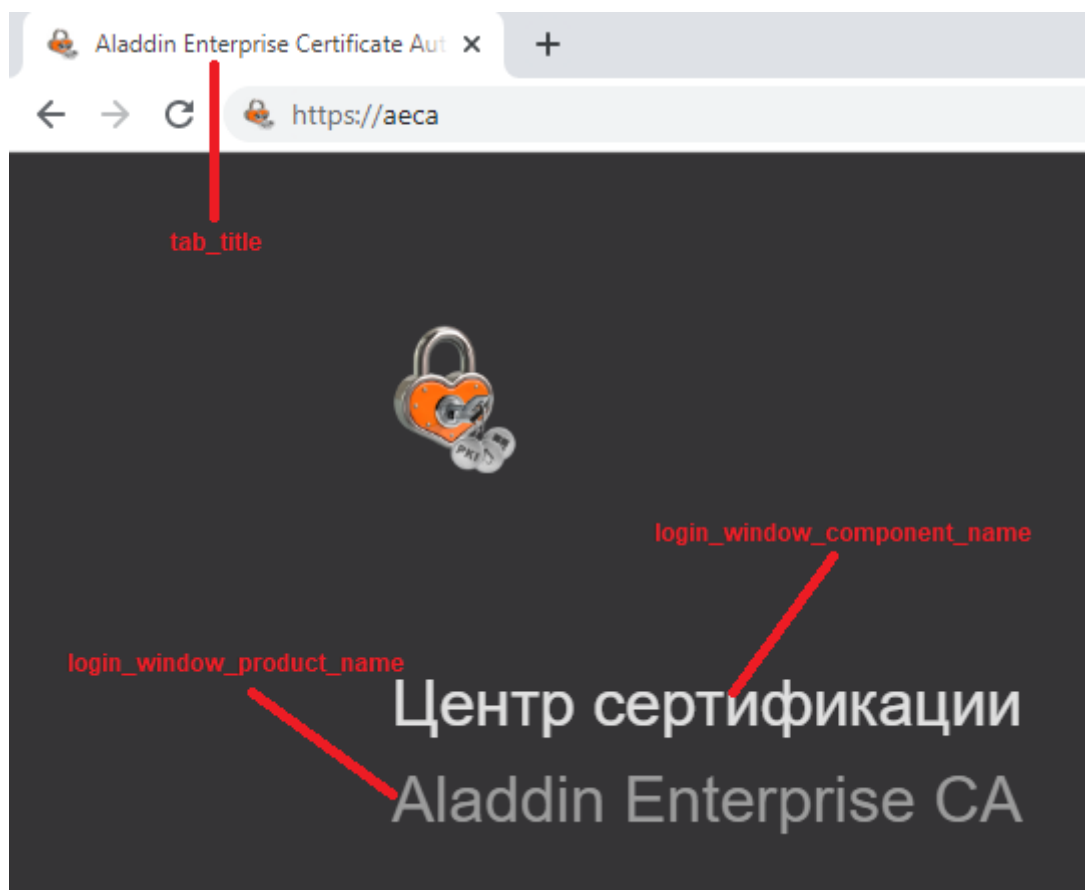


Рисунок 26 — Сведения, отображаемые в окне авторизации и в заголовке вкладки браузера

## 5 АУТЕНТИФИКАЦИЯ В ПРОГРАММЕ

В еСА-СА возможна аутентификация только для ролей:

- «Администратор»;
- «Оператор».

Аутентификация в еСА-СА осуществляется посредством окна авторизации.

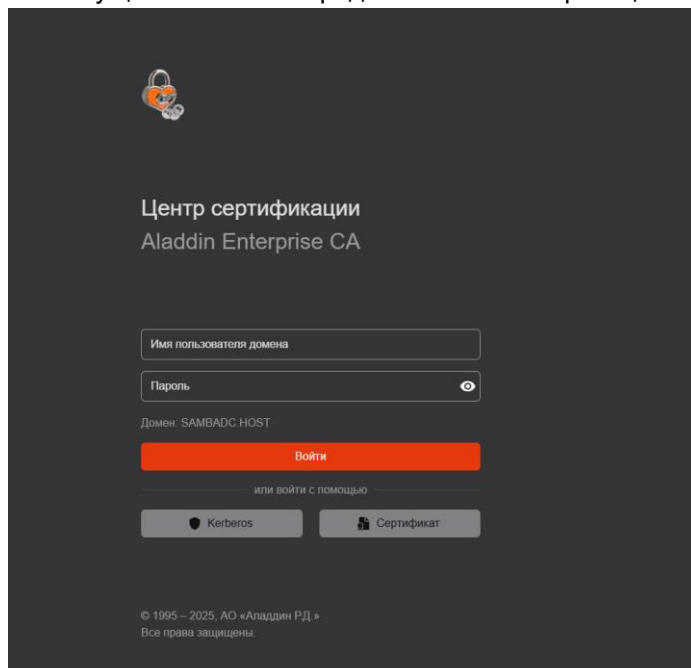


Рисунок 27 — Окно авторизации еСА-СА

### 5.1 Аутентификация с использованием сертификата, перенесённого на жёсткий диск

Полученный администратором контейнер сертификата доступа для аутентификации на веб-сервере еСА-СА необходимо перенести любым удобным способом на жёсткий диск средства вычислительной техники (далее – СВТ) для его дальнейшей установки в хранилище сертификатов веб-браузера для сохранения информации о доверенных сертификатах с целью успешного подключения к серверу на клиентской стороне.

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

- Откройте веб-браузер **Firefox – Настройки – Приватность и Защита – Сертификаты** (см. Рисунок 28). Нажмите кнопку **<Просмотр сертификатов>**.

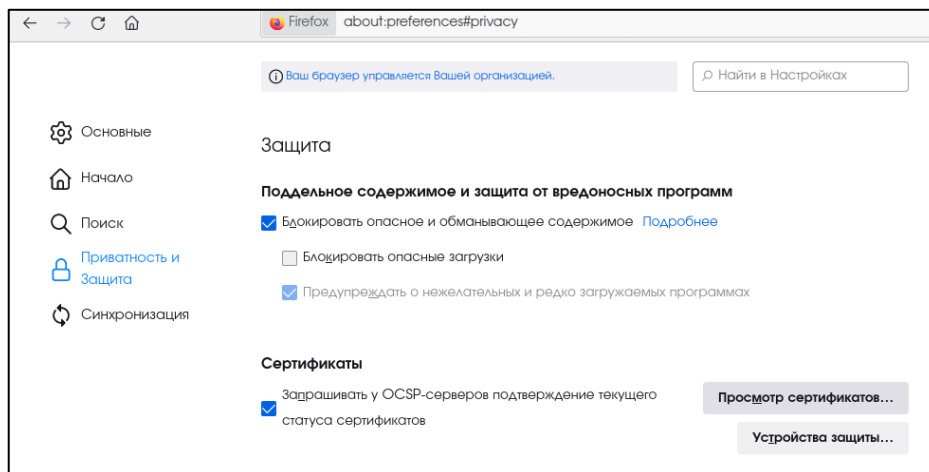


Рисунок 28 – Окно настроек веб-браузера

- Выберите вкладку «Ваши сертификаты», в открывшейся вкладке нажмите кнопку **<Импортировать>** (см. Рисунок 29).

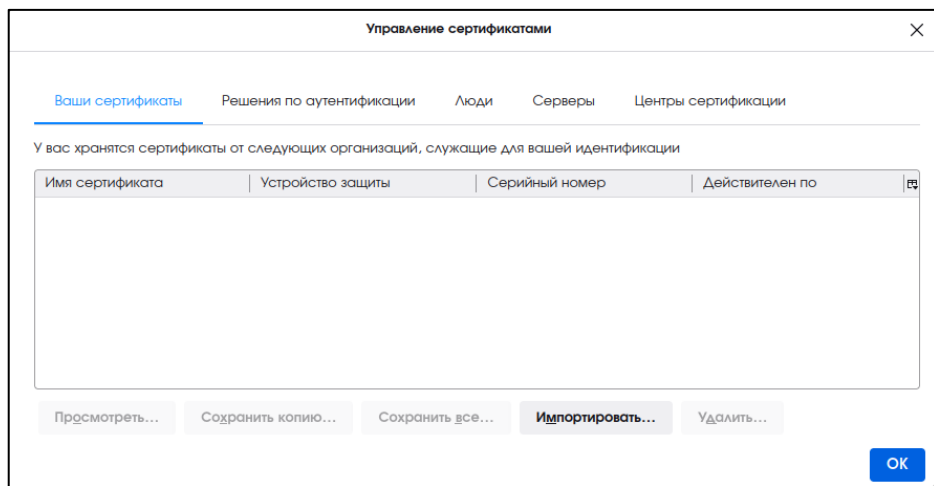


Рисунок 29 – Окно управления сертификатами

- Выберите контейнер .p12, содержащий закрытый ключ и сертификат доступа, перенесённый на жесткий диск, выпущенный для учётной записи пользователя (см. Рисунок 30).

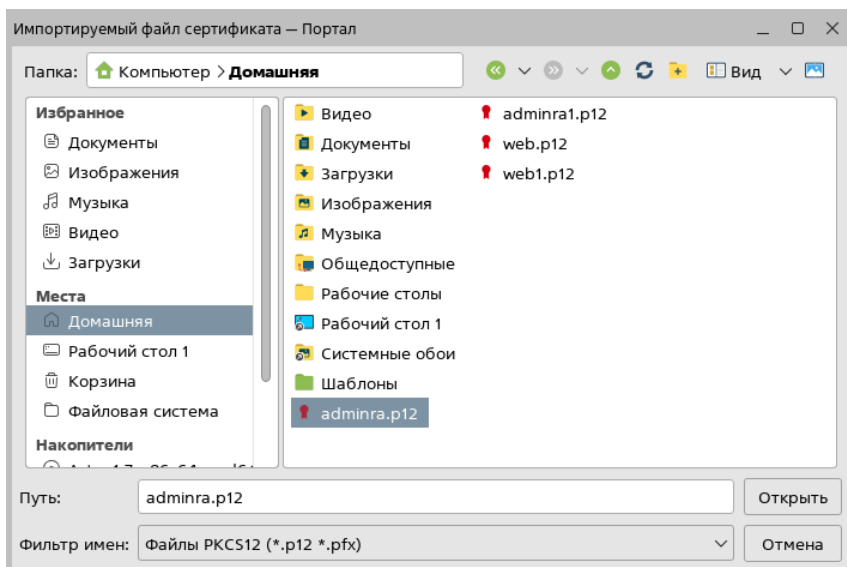


Рисунок 30 – Окно выбора импортируемого файла сертификата

- В открывшемся окне введите пароль от контейнера .p12 и нажмите кнопку **<Ок>** (см. Рисунок 31). Пароль от контейнера является атрибутом безопасности и должен быть передан администратором с контейнером закрытого ключа и сертификата.

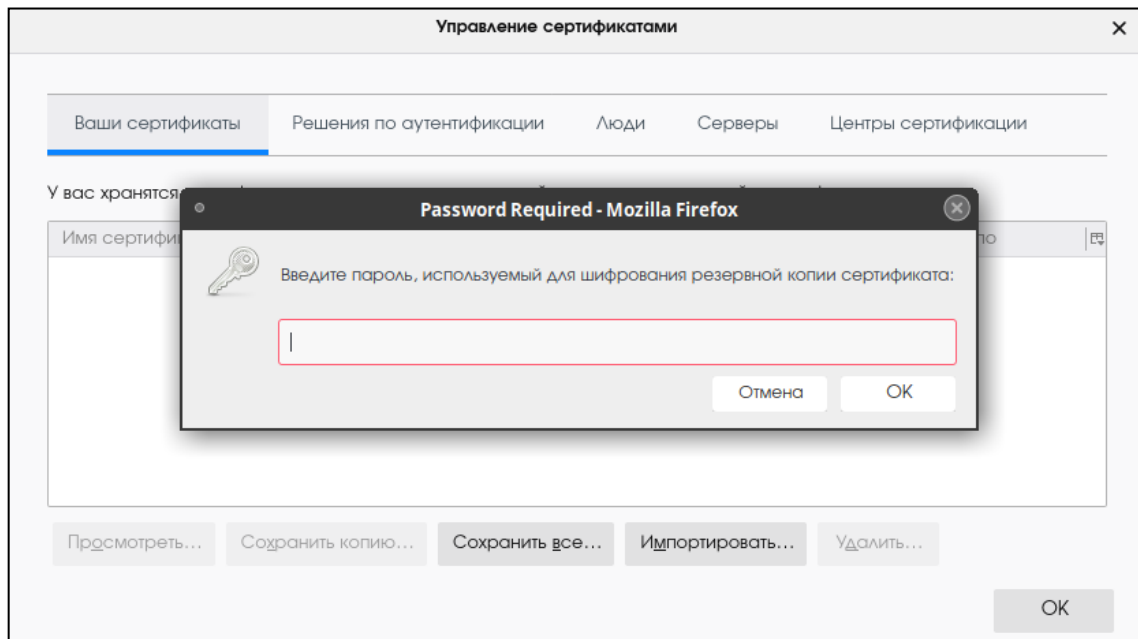


Рисунок 31 – Окно ввода пароля контейнера

- В адресной строке веб-браузера введите IP-адрес или полное доменное имя сервера, выдавшего импортированный сертификат доступа, на котором произведена установка eCA-CA (например, <https://172.22.5.21>).
- В открывшемся окне выберите сертификат для аутентификации на веб-сервере eCA-CA (см. Рисунок 32). Нажмите кнопку **<ОК>**.

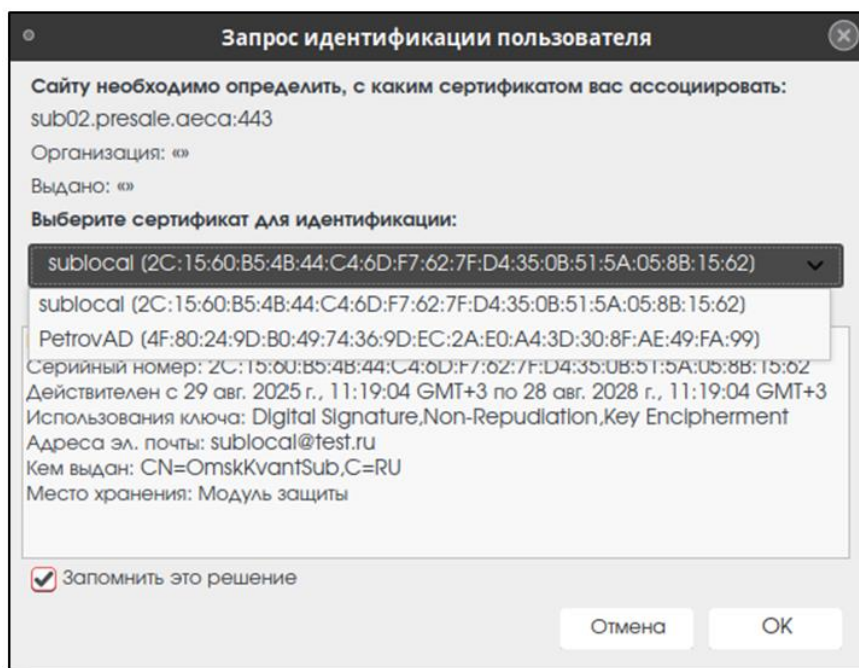


Рисунок 32 – Выбор сертификата для аутентификации

- Далее откроется страница с предупреждением системы безопасности (см. Рисунок 33). Нажмите кнопку **<Дополнительно>** и далее кнопку **<Принять риск и продолжить>**.

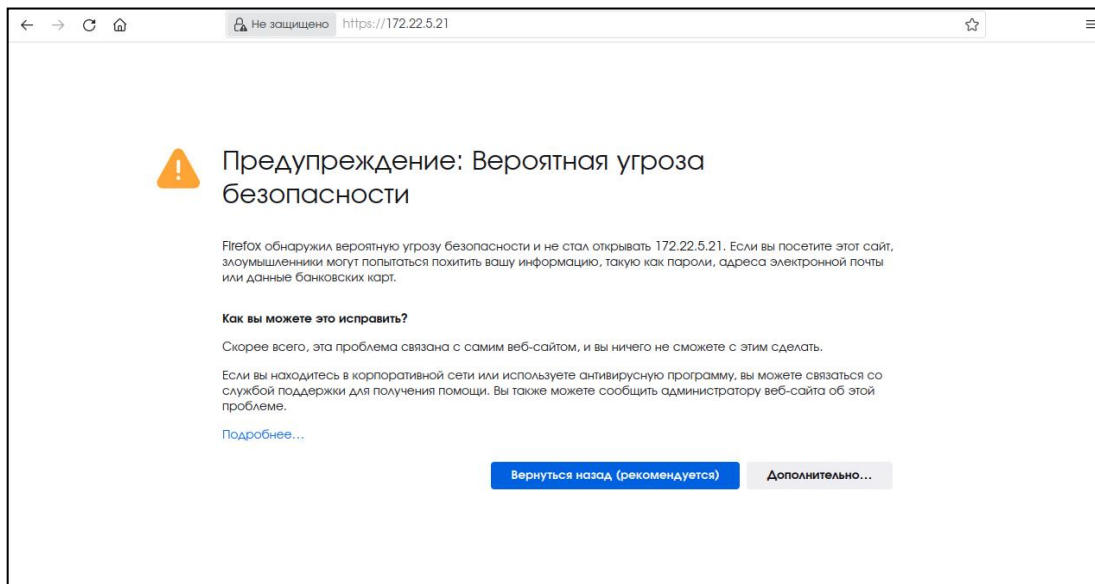


Рисунок 33 – Страница с предупреждением системы безопасности

В случае отказа в доступе к веб-интерфейсу еСА-СА пользователь будет уведомлён сообщением об ошибке. Возможные причины отказа:

- сертификат доступа пользователя не импортирован в доверенное хранилище веб-браузера;
- отсутствие издателя сертификата доступа, импортированного в доверенное хранилище веб-браузера, в списке разрешённых издателей веб-сервера;
- остановка работы служб еСА-СА на веб-сервере;
- срок действия сертификата доступа истёк;
- действия сертификата было приостановлено или сертификат отозван.

В случае отказа доступа обратитесь к пользователю с ролью «Администратор» еСА-СА.

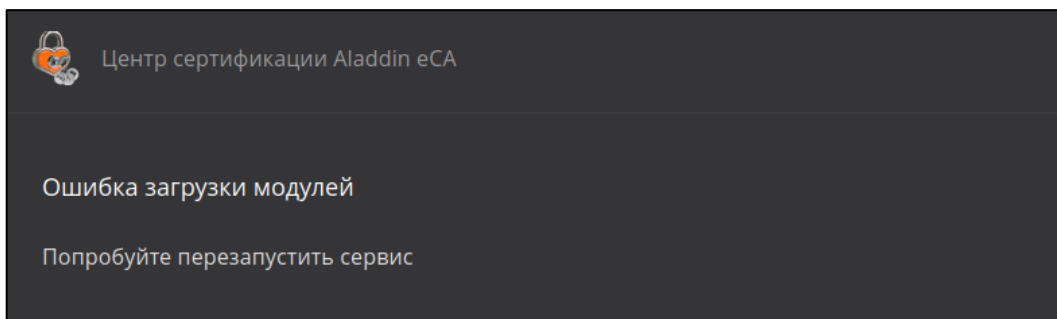


Рисунок 34 – Ошибка загрузки модулей

В случае успешной аутентификации пользователя будет сформировано защищённое соединение клиент – сервер и предоставлен доступ к веб-интерфейсу еСА-СА.

## 5.2 Аутентификация с использованием сертификата на ключевом носителе

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

Для настройки сначала выполните установку Единого Клиента JaCarta, а затем выполните настройку веб-браузера (настройку Firefox см. в разделе 5.2.1.2, настройку Chromium в зависимости от ОС см. в подразделах 5.2.1.3 и 5.2.1.4).

### 5.2.1.1 Установка Единого Клиента JaCarta

Для поддержки ключевых носителей выполните 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\_KG-AO.public.
  - 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 «Единый Клиент JaCarta. Руководства администратора».

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

```
apt install libnss3-tools
```

**Внимание!** Текущий локальный пользователь должен иметь права на файлы к папке `~/.pki/nssdb/`.

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

### 5.2.1.2 Настройка веб-браузера Firefox

Выполните настройку веб-браузера **Firefox**, если подключение к серверу eCA-CA будет выполнено в этом веб-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>1</sup> (см. Рисунок 35) и подтвердите загрузку модуля, нажав кнопку **<ОК>**;

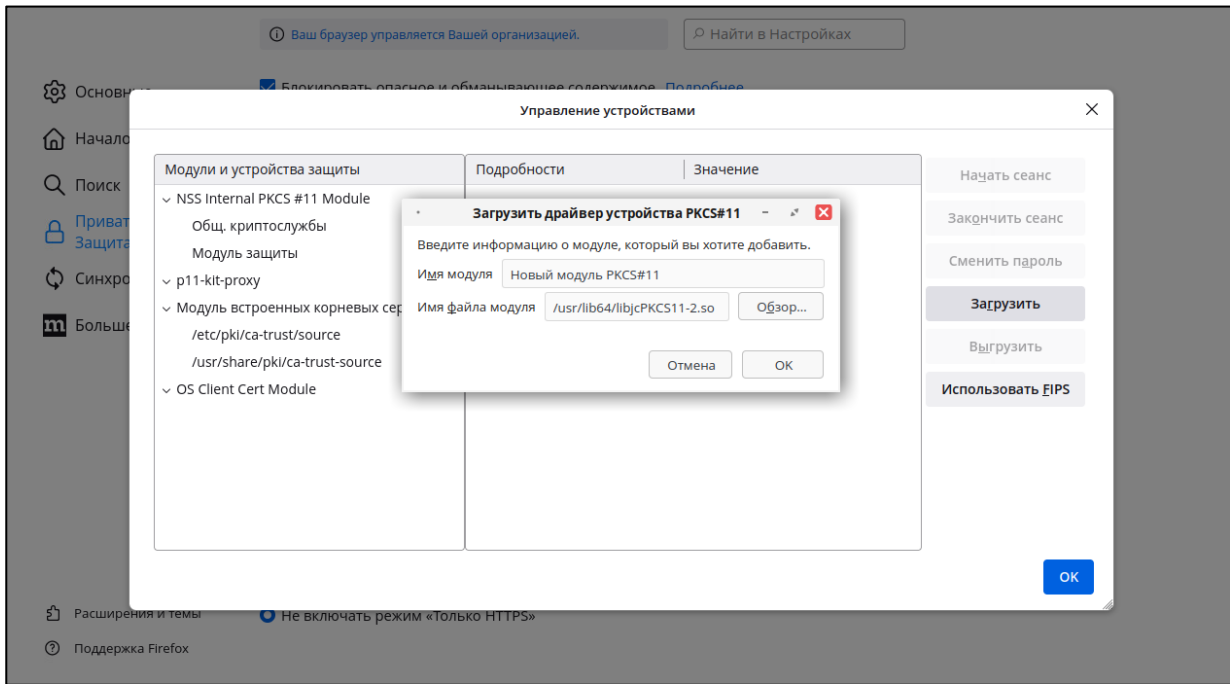


Рисунок 35 – Настройка веб-браузера Firefox

- перезапустите веб-браузер.

### 5.2.1.3 Настройка веб-браузера Chromium для РЕД ОС, РОСА «ХРОМ» 12 Сервер, SberLinux OS Server и Альт Сервер

Выполните настройку веб-браузера **Chromium**, если подключение к серверу eCA-CA будет выполнено в этом веб-браузере:

- удалите каталог локальной библиотеки сертификатов, выполнив команду:

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

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

```
mkdir -p ~/.pki/nssdb
```

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

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

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

```
modutil -dbdir sql:.pki/nssdb/ -add "JaCarta" -libfile /usr/lib64/libjcpkcs11-2.so
```

- перезапустите веб-браузер.

<sup>1</sup> Файл модуля `libjcpkcs11-2.so` создается при успешной установке Единого Клиента JaCarta (описание установки было выше в 5.2.1). 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 35).

#### 5.2.1.4 Настройка веб-браузера Chromium для Astra Linux Special Edition

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

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

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

- перезапустите веб-браузер.

#### 5.2.2 Двухфакторная аутентификация администратора по сертификату на ключевом носителе

Порядок двухфакторной аутентификации администратора по сертификату на ключевом носителе:

- Полученный оператором ключевой носитель с записанным на нём сертификатом доступа для аутентификации на веб-сервере eCA-CA необходимо подключить в USB-порт предварительного настроенного СBT – рабочего места оператора/администратора для его дальнейшей аутентификации с целью успешного подключения к серверу на клиентской стороне.
- Откройте веб-браузер, для которого была выполнена первичная настройка двухфакторной аутентификации (согласно разделу 5.2.1 настоящего руководства), и введите в адресной строке IP-адрес или полное доменное имя сервера (в зависимости от SAN, указанного в сертификате веб-сервера), выдавшего импортированный сертификат доступа, на котором произведена установка eCA-CA (например, <https://172.22.5.21>).
- В появившемся окне введите PIN-код ключевого носителя.

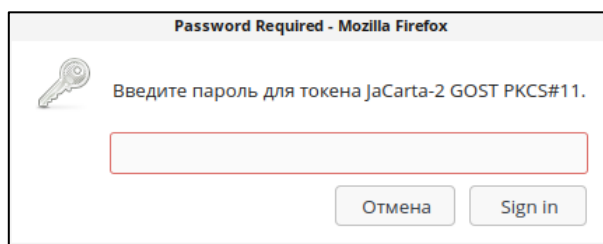


Рисунок 36 – Окно ввода PIN-кода ключевого носителя

- В появившемся окне выберите сертификат с подключённого ключевого носителя.

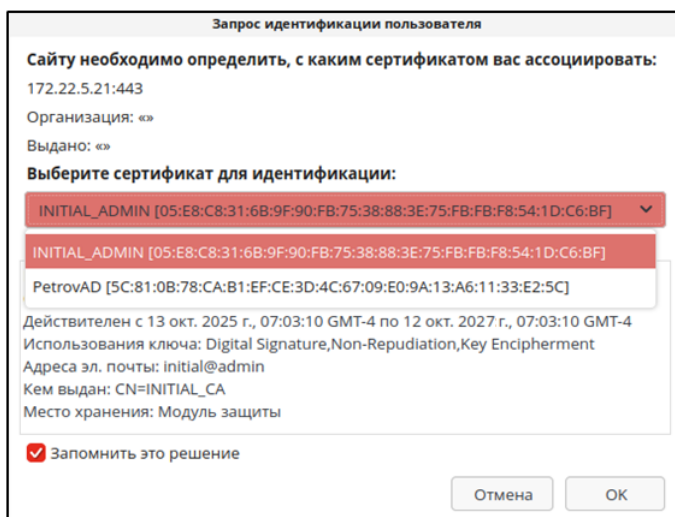


Рисунок 37 – Выбор сертификата пользователя для аутентификации на сервере

**Внимание!** 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 eCA-CA.

### 5.3 Аутентификации доменных учётных записей в еСА-СА

Для обеспечения аутентификации доменных учётных записей в еСА-СА:

1. Зарегистрируйте точку подключения (см. 8.8.1).
2. Создайте учётные записи еСА-СА на основе доменных пользователей (см. 8.7.6) либо настройте в конфигурационном файле создание автоматических учётных записей при помощи параметров:
  - `ldap_automatic_accounts_enable;`
  - `ldap_automatic_accounts_administrators_group_guid;`
  - `ldap_automatic_accounts_operators_group_guid.`
3. Укажите в конфигурационном файле параметры подключения к домену:
  - `kerberos_service_principal;`
  - `kerberos_keytab_location;`
  - `kerberos_krb5_location;`
  - `kerberos_ad_domain;`
  - `kerberos_ad_server;`
  - `resource_type;`
  - `resource_base_dn;`
  - `kerberos_enabled;`
  - `ldap_enabled.`

#### 5.3.1 Аутентификация в еСА-СА по имени и паролю доменного пользователя

Для аутентификации в еСА-СА по имени и паролю доменного пользователя:

- В окне авторизации еСА-СА (см. рисунок 27) введите имя и пароль доменного пользователя.
- Нажмите кнопку «Войти».

#### 5.3.2 Аутентификация в еСА-СА по Kerberos-билету доменного пользователя

Для аутентификации еСА-СА по Kerberos-билету доменного пользователя:

- В окне авторизации еСА-СА (см. рисунок 27) введите имя доменного пользователя.
- Нажмите кнопку Kerberos.
- Нажмите кнопку «Войти».

## 6 БЕЗОПАСНОСТЬ СОЕДИНЕНИЯ

Подключение клиента к серверу «eCA-CA» 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 eCA-CA, 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.

### 6.1 Настройка доверенного соединения

Для настройки доверенного соединения:

- Подготовьте сертификаты Центра сертификации, на основе которых строится цепочка доверия к сертификатам, или цепочку сертификатов Центра сертификации, с которым требуется установить безопасное соединение.
- Установите сертификаты Центра сертификации цепочки доверия в доверенное хранилище веб-браузера. Процесс установки сертификатов рассмотрим на примере веб-браузера Firefox:
  - Откройте веб-браузер Firefox – Настройки – Приватность и Защита – Сертификаты (см. Рисунок 38). Нажмите кнопку **<Просмотр сертификатов>**.

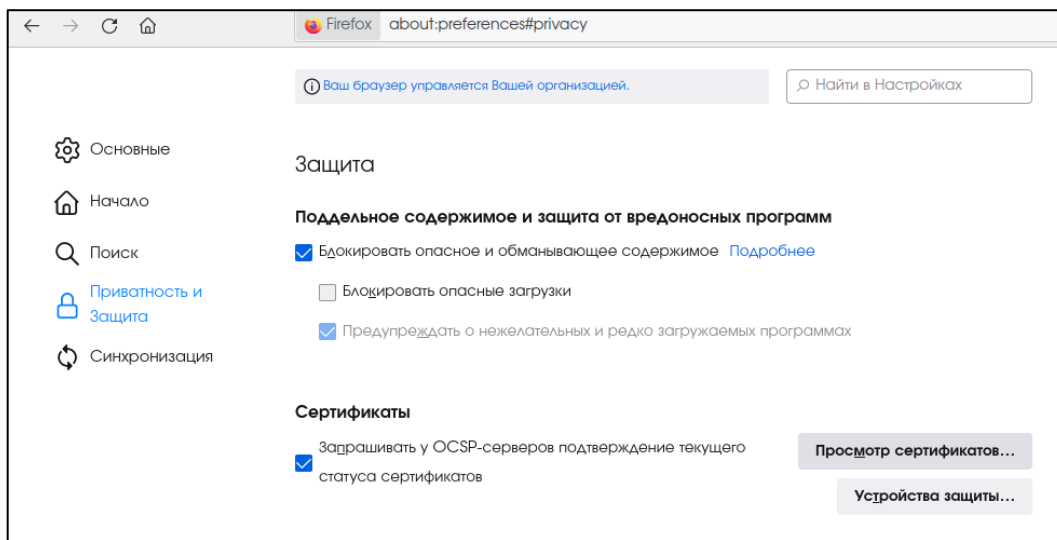


Рисунок 38 – Окно настроек веб-браузера

- 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». Поочередно импортируйте все сертификаты Центра сертификации, участвующие в построении цепочки доверия (см. Рисунок 39) или импортируйте цепочку сертификатов.

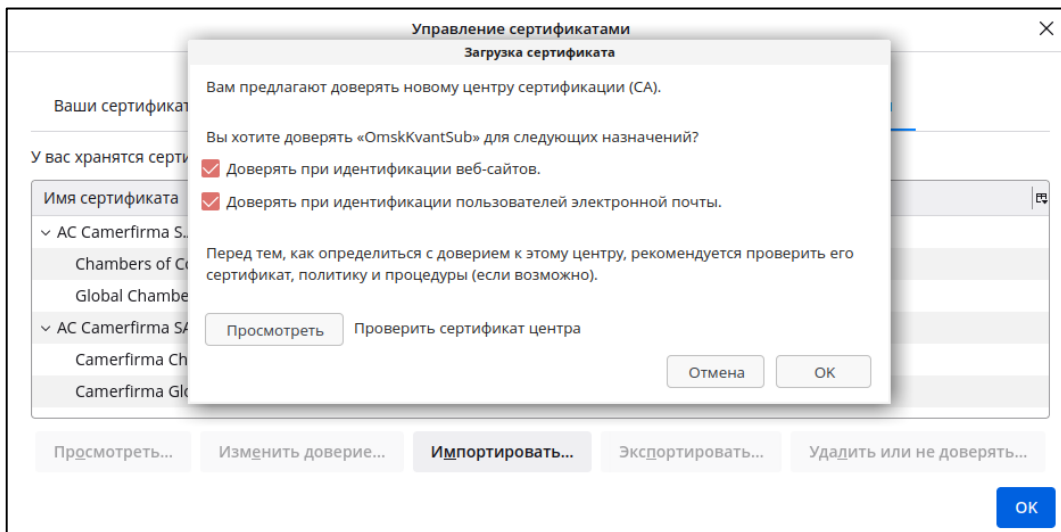


Рисунок 39 – Окно управления сертификатами

- Создать локальный субъект для веб-сервера, выпустите для него сертификат по шаблону «WEB-Server» (см. раздел 8.4.1) и установите сертификат (см. раздел 8.12), если это не сделано ранее.
- Перезапустите веб-браузер.
- Для безопасного доверенного соединения при обращении к серверу eCA-CA используйте доменное имя (см. Рисунок 40), указанное в атрибуте DNS-name суффикса сервера Subject alternative name (SAN) сертификата веб-сервера (см. Рисунок 41) и соответственно указанное в конфигурационном файле `/etc/hosts/` сервера eCA-CA.



Рисунок 40 – Адресная строка в веб-браузере

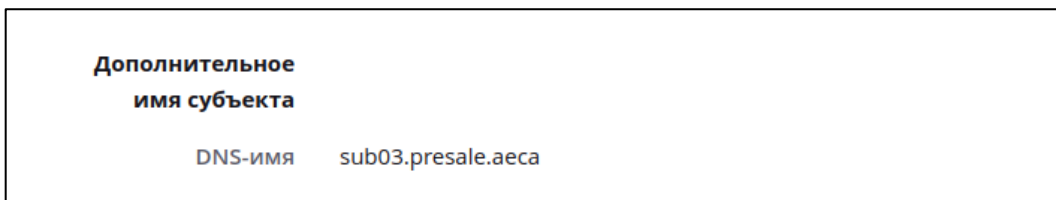


Рисунок 41 – Сертификат веб-сервера

## 7 ТЕХНОЛОГИЧЕСКИЕ СОСТАВЛЯЮЩИЕ ПРОГРАММЫ

### 7.1 Назначение технологических составляющих

Технологические составляющие создаются автоматически, с целью первичного запуска eCA-CA.

**Внимание!** Технологический Центр сертификации использовать для выпуска сертификатов запрещено.

### 7.2 Установка и настройка технологических составляющих

Перед установкой eCA-CA возможно задать в конфигурационном файле `/opt/aecaCa/scripts/config.sh` переменные окружения, используемые сервисом «settings-service» (см. документ «Центр сертификатов доступа Aladdin Enterprise Certificate Authority Certified Edition. Руководство администратора. Часть 1. Установка и обслуживание «Центра сертификации Aladdin Enterprise Certification Authority»):

- параметры технологического Центра сертификации;
- криптографические параметры сертификата технологического Центра сертификации;
- задание параметров учётной записи;
- криптографические параметры сертификата учётной записи администратора;
- криптографические параметры сертификата веб-сервера.

В процессе установки eCA-CA 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 eCA-CA в каталоге `/opt/aecaCa/dist/certificates/account/` будет размещён сертификат администратора инициализации **INITIAL\_ADMIN.p12**, необходимый для дальнейшей аутентификации на веб-сервере. Пароль от контейнера с сертификатом указан в файле `/opt/aecaCa/dist/certificates/account/INITIAL_ADMIN.txt`.

Первичная авторизация в открывшемся веб-интерфейсе установленного eCA-CA по умолчанию выполняется под учётной записью **INITIAL\_ADMIN** с правами администратора.

В открывшемся веб-интерфейсе 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 «Настройки».

### 7.3 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 еСА-СА.

Для удаления технологических составляющих, необходимых для первичного запуска еСА-СА, после развёртывания еСА-СА и загрузки лицензии, выполните следующие действия:

- Создайте Центр сертификации любого типа.
- Удостоверьтесь в том, что созданный Центр сертификации активен.
- Создайте учётную запись с ролью «Администратор» (см. раздел 8.5.1 настоящего руководства).
- Выпустите сертификат для созданной учётной записи, сохранив контейнер с ключевой парой (сертификат и закрытый ключ) в формате PKCS#12 (см. раздел 8.5.7 настоящего руководства).
- Выполните аутентификацию по выпущенному сертификату учётной записи.
- Выпустите сертификат веб-сервера, сохранив контейнер с ключевой парой (сертификат и закрытый ключ) в формате PKCS#12 (см. раздел 8.4.1 настоящего руководства).
- Установите выпущенный сертификат веб-сервера через соответствующее меню раздела «Настройки» (см. раздел 8.12 настоящего руководства).
- Выключите проверку издателя технологического Центра сертификации (см. раздел 8.13 настоящего руководства).
- Удалите технологический Центр сертификации (см. раздел 8.3.1.7 настоящего руководства).

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

В случае блокировки доступа к еСА-СА, возникшей в результате некорректного удаления технологических составляющих, восстановление доступа возможно произвести двумя способами:

- Восстановление из резервной копии (см. раздел 10 документа «Центр сертификатов доступа Aladdin Enterprise Certificate Authority Certified Edition. Руководство администратора. Часть 1. Установка и обслуживание «Центра сертификации Aladdin Enterprise Certification Authority»).
- Восстановление технологических составляющих (см. раздел 11 документа «Центр сертификатов доступа Aladdin Enterprise Certificate Authority Certified Edition. Руководство администратора. Часть 1. Установка и обслуживание «Центра сертификации Aladdin Enterprise Certification Authority»).

## 8 ФУНКЦИИ УПРАВЛЕНИЯ ПРОГРАММЫ

### 8.1 Верхняя панель

Верхняя панель (см. Рисунок 42) веб-интерфейса фиксирована и отображается на любом шаге или переходе между разделами.



Рисунок 42 – Верхняя панель окна «Центра сертификации»

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

- тип активного Центра сертификации (возможные варианты: Корневой или Подчинённый);
- обозначение статуса Центра сертификации.  
При отсутствии ошибок и предупреждений отображается активный статус:

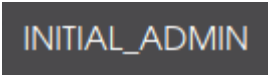
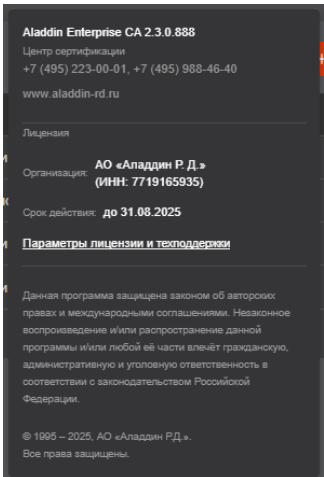
  - активный . При наведении курсора отображается всплывающее сообщение «Активный»;

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

  - истёк срок действия сертификата текущего активного Центра сертификации . При наведении курсора отображается всплывающее сообщение «Истек срок действия сертификата ЦС»;
  - истекает<sup>1</sup> срок действия сертификата текущего активного Центра сертификации . При наведении курсора отображается всплывающее сообщение «Истекает срок действия сертификата ЦС»;
  - закрытый ключ Центра сертификации недоступен<sup>2</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 Центра сертификации, заданное в применённой лицензии (не изменяемое). При наведении курсора всплывают заданные имя и значения суффикса различающегося имени Центра сертификации;
- отображаемое имя текущего активного Центра сертификации (задаётся при первичной активации лицензии);



<sup>1</sup> До истечения остаётся менее 90 дней.

<sup>2</sup> При запуске серверного компонента eCA-CA 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.

-  – текущая авторизация учётной записи пользователя;
-  – сведения о текущей версии программы, контактная информация разработчика, информация о лицензии.

## 8.2 Боковая панель

В зависимости от ширины окна веб-браузера боковая панель может:

- либо быть закреплённой и отображаться на любом шаге или переходе между разделами (при ширине окна веб-браузера более или равной 1200px). При этом боковая панель отображается в полном (см. Рисунок 43) или компактном (см. Рисунок 44) 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 веб-браузера менее 1200px).

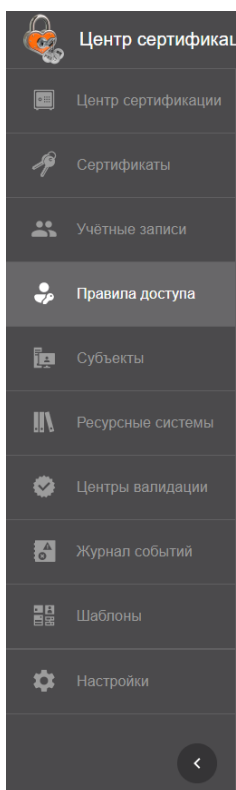


Рисунок 43 – Полный вид боковой панели



Рисунок 44 – Компактный вид боковой панели

Боковая панель состоит из разделов, определяющих соответствующие функции программы, и создана для организации управления программой:

- Раздел «Центр сертификации» – в данном разделе возможно:
  - выпустить сертификат Центра сертификации;
  - подписать запрос на выпуск сертификата Подчинённого Центра сертификации;
  - скачать цепочку сертификатов активного Центра сертификации;
  - скачать сертификат корневого и Подчинённого Центра сертификации в формате .pem;
  - отозвать сертификат Подчинённого Центра сертификации;
  - посмотреть карточку Центра сертификации;
  - Переформировать сертификат Подчинённого 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 Центром сертификации, 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 (включая историю изменения статуса сертификата);
  - скачать сертификат субъекта в формате .pem;
  - скачать цепочку сертификатов;
  - скачивание бумажного сертификата (файл, содержащий сведения из сертификата).
  - скачать список всех выпущенных сертификатов в формате .csv;
  - применить массовые операции к выбранным сертификатам (отзыв, приостановка, возобновление);
- Раздел «Учётные записи» – в данном разделе возможно:
  - создать новую учетную запись;
  - отредактировать существующую учетную запись;
  - заблокировать или активировать существующую учетную запись;
  - 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;
  - посмотреть карточку субъекта;
  - отредактировать атрибуты 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 (далее – ЦВ);
  - зарегистрировать сторонние ЦВ;
  - объединить точки распространения или службы OCSP в кластер;
  - настроить публикацию CRL/ Delta CRL/ AIA в домен.
- 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:
  - просмотр данных текущего сертификата веб-сервера;
  - изменение текущего сертификата веб-сервера;
  - просмотр и редактирование списка разрешённых издателей<sup>1</sup> сертификатов.
  - просмотр списка и параметров Syslog-серверов<sup>2</sup>;
  - добавление Syslog-сервера в список;
  - редактирование параметров Syslog-серверов из списка, включая управление (вкл./выкл.) отправкой сообщений на данный Syslog-сервер;
  - удаление Syslog-серверов из списка;
  - просмотр параметров текущей лицензии;
  - изменение текущей лицензии;
  - просмотр параметров, редактирование параметров, активация/деактивация, добавление и удаление почтового сервера, используемого для отправки уведомлений об истечении сертификатов субъектов, отправка тестового уведомления (для проверки правильности настроек почтового сервера);
  - просмотр параметров, редактирование параметров, активация/деактивация, добавление и удаление шаблонов рассылки почтовых уведомлений об истечении сертификатов субъектов.
  - просмотр, редактирование, удаление правил сопоставления атрибутов объектов

<sup>1</sup> Разрешённый издатель – центр сертификации, сертификаты которого разрешено использовать для аутентификации в программе.

<sup>2</sup> Syslog-сервер – программное обеспечение, осуществляющее регистрацию сообщений от клиентов по стандарту Syslog.

(пользователей, компьютеров и сервисов<sup>1</sup>) ресурсных систем с атрибутами субъектов данных PC в eCA-CA при синхронизации.

Далее в настоящем документе приводится полное описание доступных функций управления eCA-CA для каждого раздела.

### 8.3 Раздел «Центр сертификации»

Переход на экран управления центра сертификации осуществляется по выбору раздела «Центр сертификации» бокового меню, расположенного слева на главном экране (см. Рисунок 43).

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».

#### 8.3.1 Вкладка «Свои сертификаты»

Вид раздела «Центр сертификации» – вкладка «Свои сертификаты» показан на рисунке ниже (Рисунок 45).

Тип	Отображаемое ...	Владелец	Действителен до	Состояние	Кол-во созда...
▼	NOT GOST	SUB_CA_INFORM	08.08.2034 15:51:47	Активирован	42702
▼	Testp1234	SUB_CA_INFORM	12.08.2034 16:34:56	Не активирован	8
▼	TEST111	SUB_CA_INFORM	02.11.2034 17:12:36	Не активирован	0
▼	test 3	SUB_CA_INFORM	07.08.2034 16:09:32	Не активирован	8
▼	Testp123	SUB_CA_INFORM	12.08.2034 16:34:56	Не активирован	1
▼	OCSP 1	SUB_CA_INFORM	11.10.2034 20:34:46	Не активирован	12
	qwewqewqe	SUB_CA_INFORM	-	Запрос	0
	Test	SUB_CA_INFORM	-	Запрос	0
▼	hfh	SUB_CA_INFORM	14.08.2034 15:50:52	Не активирован	52
▼	Центр сертификац...	SUB_CA_INFORM	11.10.2034 20:34:46	Не активирован	12

Рисунок 45 – Экран раздела «Центр сертификации» – вкладка «Свои сертификаты»

На данной вкладке после инициализации отображены сертификат технологического Центра сертификации, создаваемый по умолчанию при установке eCA-CA, и сертификат Центра сертификации, созданный при инициализации.

**Внимание!** Технологический Центр сертификации использовать для выпуска сертификатов запрещено.

Сертификаты Центров сертификации в формате `.pem` хранятся в базе данных (имя базы данных и ее конфигурация указана в конфигурационном файле `/opt/aecaCa/scripts/config.sh`).



Открытый и закрытый ключи Центра сертификации хранятся в контейнере PKCS#12. Место хранения выбирается при создании ЦС.

Пароль контейнера PKCS#12 хранится в базе данных в зашифрованном по алгоритму AES256 виде.

<sup>1</sup> Получение сервисов выполняется только из ресурсных систем «ALD PRO», «FreeIPA» и «ROSA Dynamic Directory».

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 7;
- тип – тип центра сертификации:
  -  – для корневого Центра сертификации;
  -  – для Подчинённого Центра сертификации;











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 7 – 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 eCA-SA 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 Центром сертификации администратору доступны действия, приведённые в таблице 8.

Таблица 8 – Возможные операции, совершаемые над Центром сертификации на вкладке «Свои сертификаты»

Операция	Состояние «Запрос»	Состояние «Активирован»	Состояние «Не активирован»	Необходимое действие для выполнения операции
Скачать сертификат	–	+	+	Выделить сертификат и нажать кнопку  <Скачать>
Скачать цепочку сертификатов	–	+	+	
Скачать список отозванных сертификатов	–	+	+	
Скачать запрос на сертификат	+	–	–	
Удалить центр сертификации	+	–	+	Выделить сертификат и нажать кнопку  <Удалить>
Импортировать сертификат	+	–	–	Выделить сертификат и нажать кнопку  <Загрузить> или кнопку  Импортировать сертификат
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>1</sup>

Технологический Центр сертификации может быть удалён после выпуска и загрузки нового сертификата для текущего сервера (см. раздел 7.3 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 8.3.1.2);
- Для добавления сертификата Центра сертификации с импортом внешнего ключа из контейнера PKCS#12 выберите опцию «Импорт внешнего ключа» (подробнее см. раздел 8.3.1.2).

<sup>1</sup> При успешной активации центра сертификации в журнале событий регистрируется запись с кодом CAENV008.

### 8.3.1.1 Просмотр параметров сертификата ЦС в карточке ЦС

Для просмотра параметров сертификата нажмите на строку сертификата таблицы на вкладке «Свои сертификаты (см. рисунки 46 и 47).

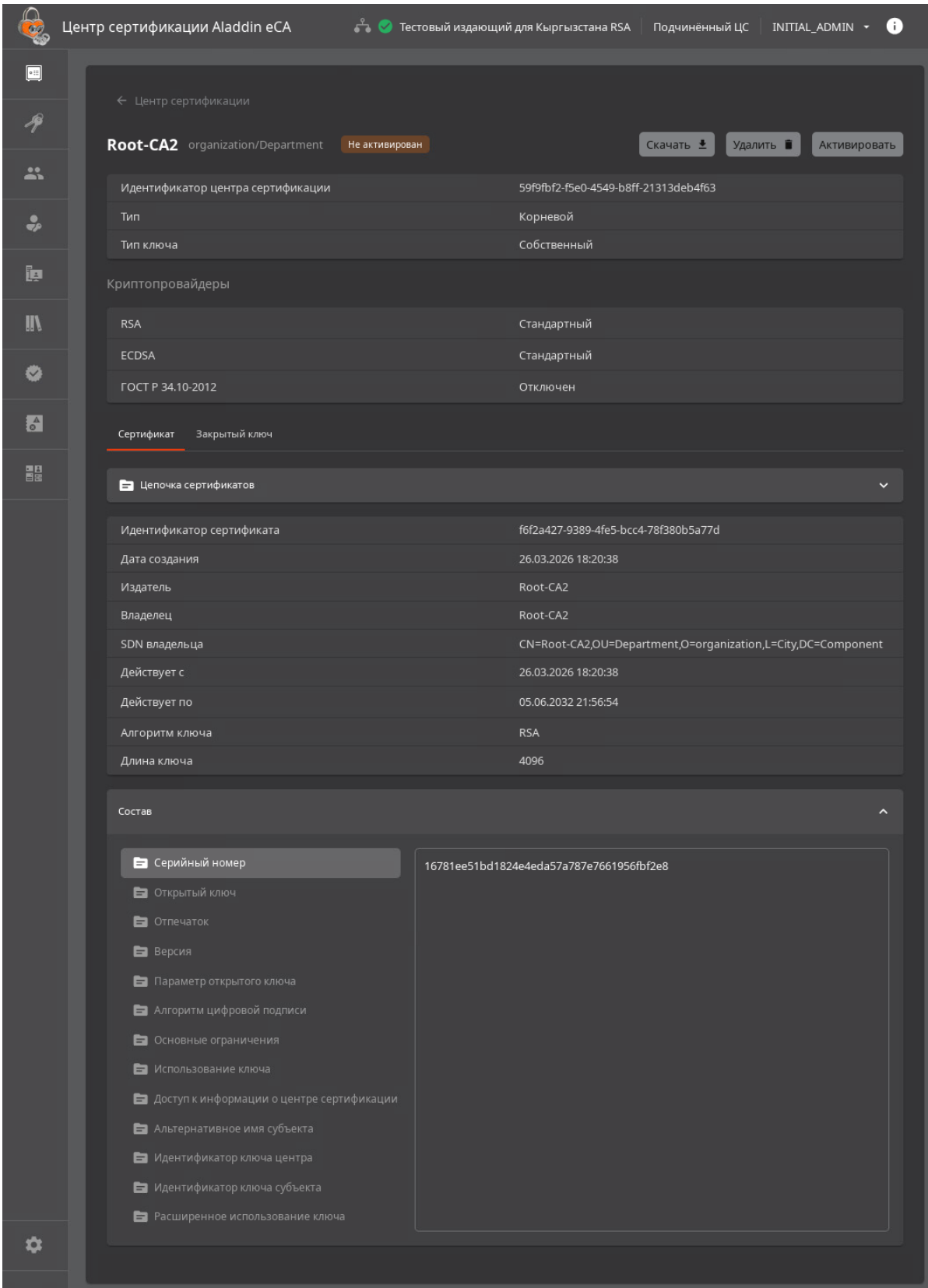


Рисунок 46 — Карточка корневого Центра сертификации

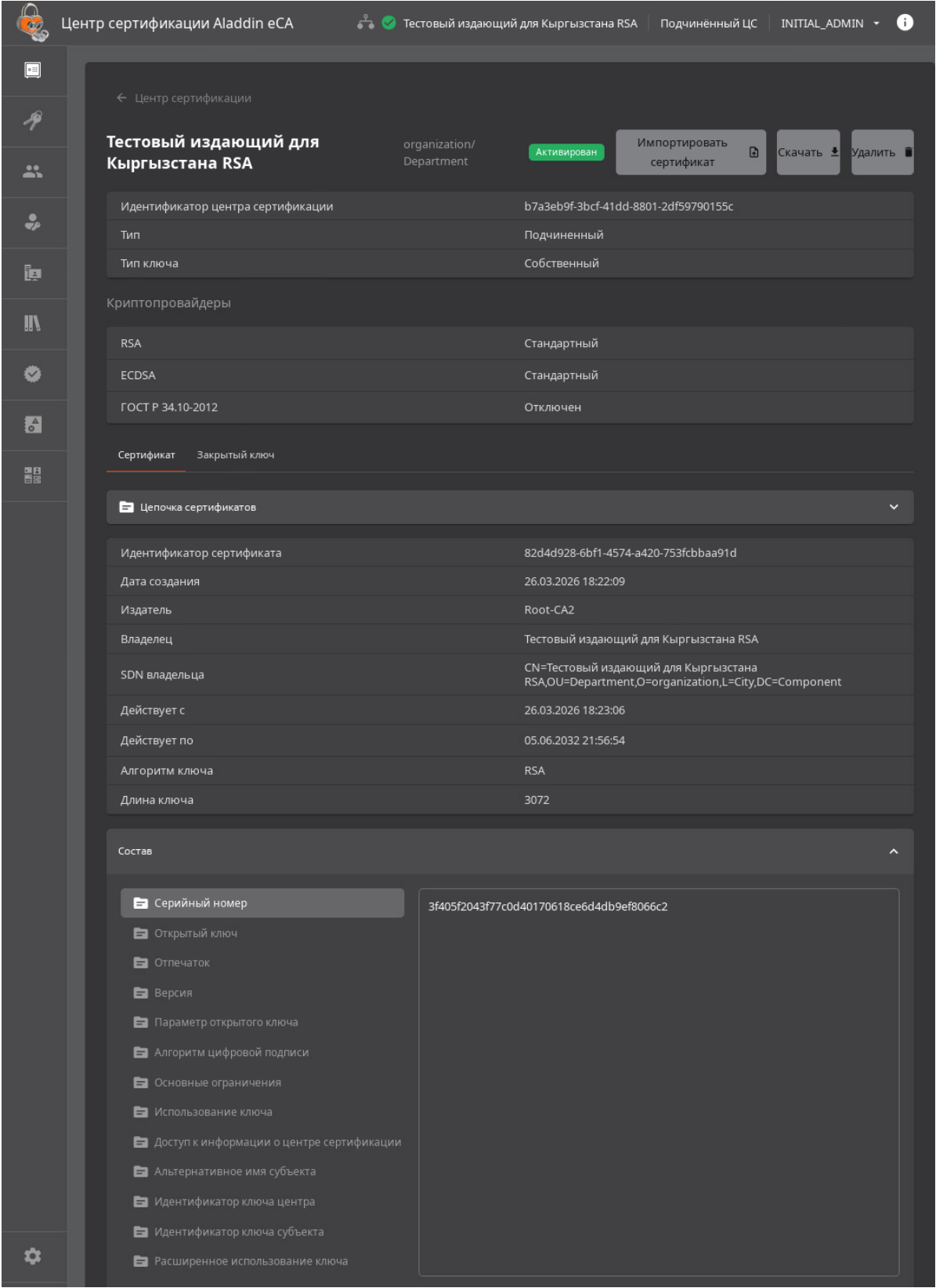


Рисунок 47 — Карточка подчинённого Центра сертификации

### 8.3.1.2 Создание корневого центра сертификации с генерацией ключа

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

- На вкладке «Свои сертификаты» нажмите кнопку **Добавить сертификат** **<Добавить сертификат>** и выпадающем списке выберите опцию «Создать ключ».

- Если текущая лицензия позволяет создание корневого и Подчинённого Центров сертификации, то отобразится модальное окно «Окно инициализации корневого ЦС. Шаг 1/5» с шагом выбора лицензии (см. Рисунок 48). 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.

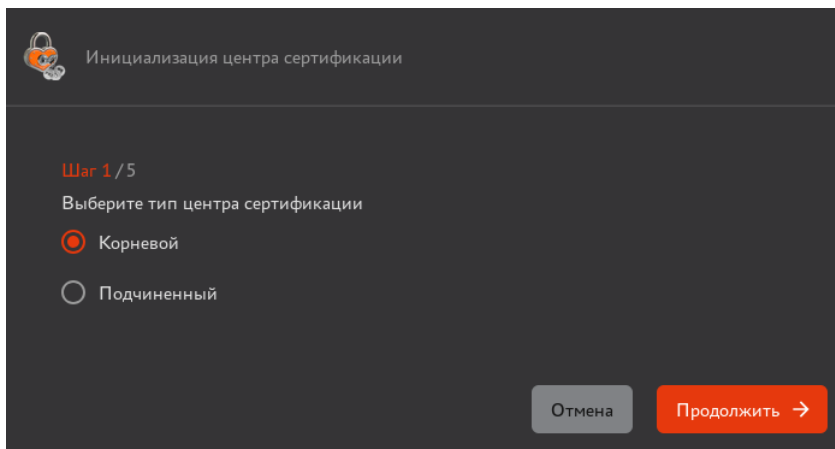


Рисунок 48 – Выбор типа центра сертификации

- На шаге 2/5 (см. Рисунок 49) заполните поля:

Рисунок 49 – Окно инициализации корневого центра сертификации. Шаг 2/5

- «Отображаемое имя» – введите имя создаваемого Центра сертификации, которое будет отображаться в интерфейсе eCA-CA. 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 имён 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, указанных в таблице 2.
- 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 50):

Рисунок 50 – Окно инициализации корневого центра сертификации. Шаг 3/5

- «RSA» – поле выбора криптопровайдера для алгоритма RSA, допустимые варианты выбора:
  - Стандартный (по умолчанию);
  - КриптоПро CSP<sup>1</sup> (доступен только при наличии активного и подключённого криптопровайдера СКЗИ «КриптоПро CSP», работающего на сервере совместно с eCA-CA);
  - 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 подключённого криптопровайдера СКЗИ «КриптоПро CSP», работающего на сервере совместно с eCA-CA);
  - Отключен (по умолчанию).

**Внимание!** 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.

- После выбора криптопровайдеров нажмите кнопку <Продолжить> для перехода к следующему шагу.
- На шаге 4/5 необходимо выбрать шаблон сертификата Корневого Центра сертификации. В списке шаблонов отображаются все имеющиеся в программе шаблоны с типом «Корневой» (см. Рисунок 51).

<sup>1</sup> Подробная информация по настройке взаимодействия eCA-CA с СКЗИ «КриптоПро CSP» описана в приложении 5 документа «Центр сертификатов доступа Aladdin Enterprise Certificate Authority Certified Edition. Руководство администратора. Часть 1. Установка и обслуживание «Центра сертификации Aladdin Enterprise Certification Authority».

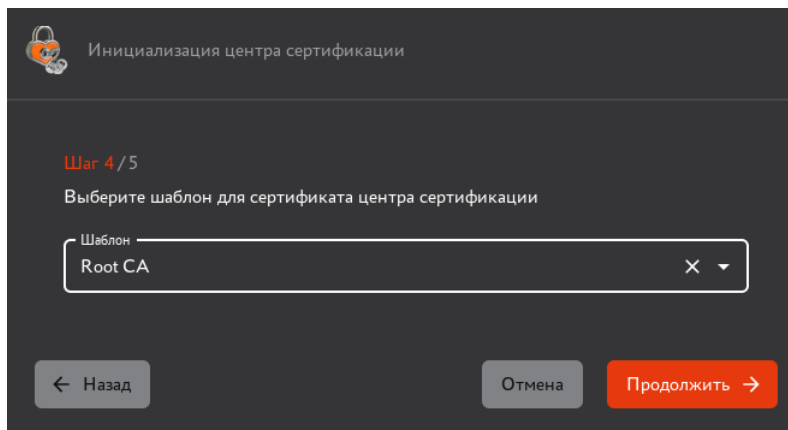



Рисунок 51 – Окно инициализации корневого центра сертификации. Шаг 4/5

- После выбора шаблона нажмите кнопку **<Продолжить>** для перехода к следующему шагу.
- На шаге 5/5 необходимо указать срок действия сертификата Центра сертификации и задать параметры криптографии (см. Рисунок 52). 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 БДСЧ криптопровайдера СКЗИ «КриптоПро CSP» гаммы);
      - КриптоПро CSP (HDIMAGE);
      - КриптоПро HSM (доступно только при наличии подключения криптопровайдера СКЗИ «КриптоПро CSP» к ПАКМ «КриптоПро HSM»).
    - Для всех других криптопровайдеров в данном поле указано неизменяемое значение «Локальное хранилище Aladdin eCA».

- Если криптопровайдером хотя бы одного из алгоритмов выбран «КриптоПро CSP», то при выборе места хранения «Локальное хранилище Aladdin eCA» или «КриптоПро CSP (HDIMAGE)» убедитесь, что размер внешней гаммы (размер файла /opt/aecaCa/dist/gamma/db1/kis\_1) позволяет сгенерировать необходимое количество закрытых ключей. На генерацию одного закрытого ключа длиной 256 бит расходуется 36 байт гаммы, на генерацию одного закрытого ключа длиной 512 бит расходуется 36\*2 байта гаммы и т.д. Если размер внешней гаммы недостаточен, то подготовьте внешнюю гамму при помощи утилиты `genkprim` (см. приложение 5 документа «Центр сертификатов доступа Aladdin Enterprise Certificate Authority Certified Edition. Руководство администратора. Часть 1. Установка и обслуживание «Центра сертификации Aladdin Enterprise Certification Authority»).
- 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.

**Внимание!** 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.


Инициализация центра сертификации

Шаг 5 / 5

Укажите срок действия ЦС и параметры криптографии

Срок действия ЦС

20.04.2041

Максимальный срок действия ЦС определяется шаблоном

Параметры криптографии

Алгоритм ключа

RSA

Длина ключа

4096

Алгоритм хэш-суммы

SHA512

Место хранения закрытого ключа центра сертификации

Место хранения

Локальное хранилище Aladdin eCA

Экспортируемый закрытый ключ

☒

Назад

Отмена

Создать ЦС

Рисунок 52 – Окно инициализации корневого центра сертификации. Шаг 5/5

После задания значений нажмите ставшую активной кнопку **<Создать ЦС>**.

В случае неудачной попытки создания Центра сертификации выводится одно из сообщений об ошибке, приведённых в таблице .

Таблица 9 – Перечень сообщений в случае неудачной попытки создания Центра сертификации

Текст ошибки	Причина
Ошибка. Некорректный компонент суффикса различающегося имени – <Имя компонента>	Ошибка ввода неизвестного имени компонента суффикса различающегося имени

АО "Аладдин Р.Д.", 1995—2026  
г.

Руководство администратора. Часть 2. Функции управления «Центра сертификации Aladdin Enterprise Certification Authority»  
Смп. 60 / 275

Текст ошибки	Причина																						
Ошибка. Поле <Имя компонента> отсутствует в шаблоне	Ошибка ввода компонента суффикса различающегося имени, отсутствующего в выбранном шаблоне.																						
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 введённого значения атрибута различающегося имени<sup>1</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> <tr> <td>DATEOFBIRTH</td><td>^(\d{4})(\d{2})(\d{2})(\d{2})(\d{2})(\d{2})(?:(\d+)?(Z ([+-]\d{2})(\d{2}))?)\$</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}\$	DATEOFBIRTH	^(\d{4})(\d{2})(\d{2})(\d{2})(\d{2})(\d{2})(?:(\d+)?(Z ([+-]\d{2})(\d{2}))?)\$
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}\$																						
DATEOFBIRTH	^(\d{4})(\d{2})(\d{2})(\d{2})(\d{2})(\d{2})(?:(\d+)?(Z ([+-]\d{2})(\d{2}))?)\$																						
Ошибка при создании Центра сертификации. Неизвестная ошибка	Внутренняя ошибка ПО																						

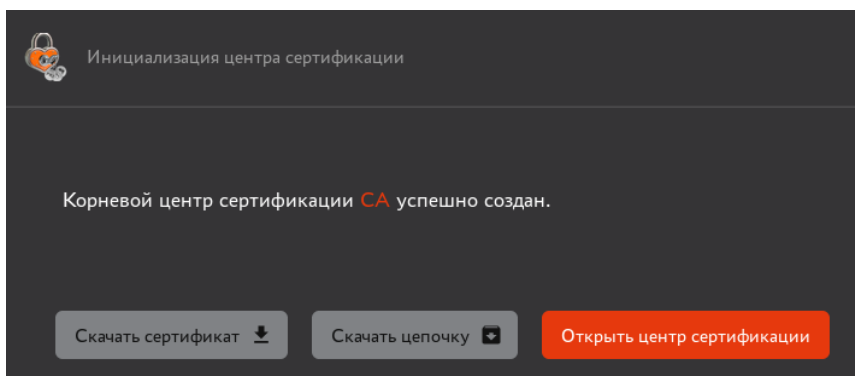


Рисунок 53 – Окно завершения инициализации корневого центра сертификации

При успешном создании Корневого Центра сертификации и завершении инициализации Центра сертификации будет отображено соответствующее окно (см. Рисунок 53). В нём возможно:

- скачать сертификат созданного Корневого Центра сертификации;
- скачать цепочку сертификатов в формате `.pem`;
- или открыть страницу созданного Центра сертификации.

Также в результате успешного создания данного Центра сертификации в контейнере закрытого ключа данного Центра сертификации будут содержаться закрытый ключ данного Центра сертификации и цепочка сертификатов данного Центра сертификации.

<sup>1</sup> Правила валидации значений атрибутов представлены в приложении 3 «Правила валидации значений полей по умолчанию предустановленных шаблонов сертификатов».

### 8.3.1.3 Создание подчинённого центра сертификации с генерацией ключа

Для создания Центра сертификации на вкладке «Свои сертификаты» нажмите кнопку

Добавить сертификат ▾

<Добавить сертификат>.

После этого в выпадающем списке выберите опцию «Создать ключ» для создания Центра сертификации с генерацией собственного ключа – дальнейшие шаги создания Центра сертификации описаны в разделе 4.1.2 при создании сертификата подчинённого Центра сертификации;

Новый Центр сертификации будет создан на основании текущей лицензии.

### 8.3.1.4 Создание центра сертификации с импортом внешнего ключа

Для создания Центра сертификации на вкладке «Свои сертификаты» нажмите кнопку

Добавить сертификат ▾

<Добавить сертификат>.

После этого в выпадающем списке выберите опцию «Импорт внешнего ключа» для создания Центра сертификации с генерацией собственного ключа – дальнейшие шаги создания Центра сертификации описаны в разделе 4.2.

Новый Центр сертификации будет создан на основании текущей лицензии.

### 8.3.1.5 Скачивание запроса на сертификат для центра сертификации в состоянии «Запрос»

В случае, если запрос на сертификат Подчинённого Центра сертификации по каким-либо причинам не был скачан в окне мастера инициализации, выполните следующие действия:

- На вкладке «Свои сертификаты» выбрать созданный Подчинённый Центр сертификации в состоянии «Запрос» (см. Рисунок 54).

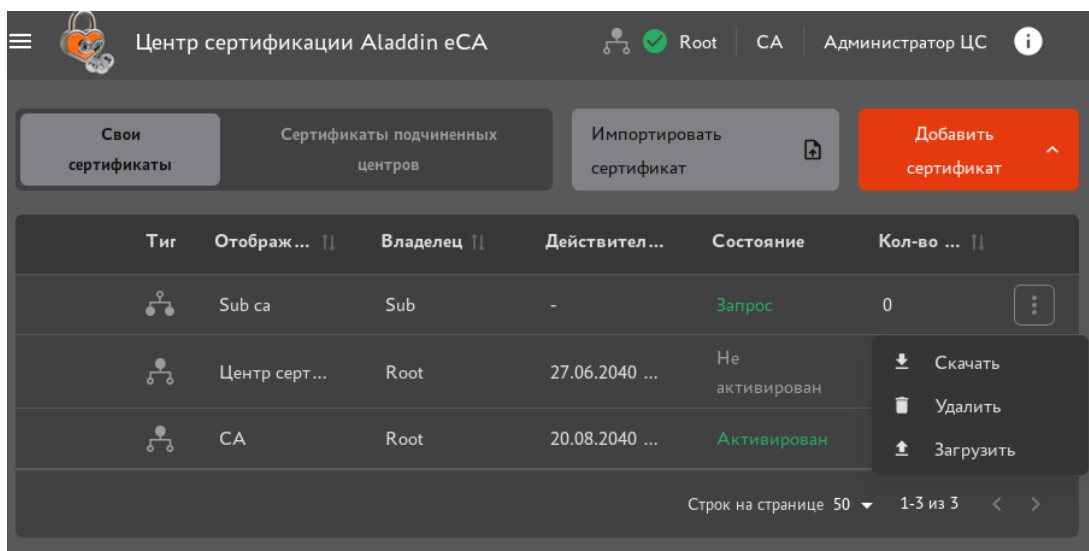



Рисунок 54 – Скачивание запроса на сертификат



- Нажать появившуюся в строке выбранного Центра сертификации кнопку  и скачать запрос в формате `.csr`.
- Далее следует подписать скачанный запрос на Корневом Центре сертификации согласно разделу 8.3.2.2 настоящего руководства администратора.

### 8.3.1.6 Импорт сертификата (цепочки сертификатов) подчинённого центра сертификации

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

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

После подписания запроса на сертификат на Корневом Центре сертификации необходимо импортировать цепочку сертификатов для Подчинённого Центра сертификации в состоянии «Запрос», выполнив следующие действия:

- На вкладке «Свои сертификаты» выбрать Подчинённый Центр сертификации в состоянии «Запрос», по запросу которого был сформирован сертификат и цепочка сертификатов в формате `.pem` или `.p7b` в разделе 8.3.1.5 данного руководства. Нажать кнопку  **<Загрузить>** (см. Рисунок 54) 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 55) выбрать скачанный ранее файл цепочки сертификата для загрузки в формате `.pem` или `.p7b`. Нажать кнопку **<Загрузить>**, активированную после выбора файла цепочки сертификатов.

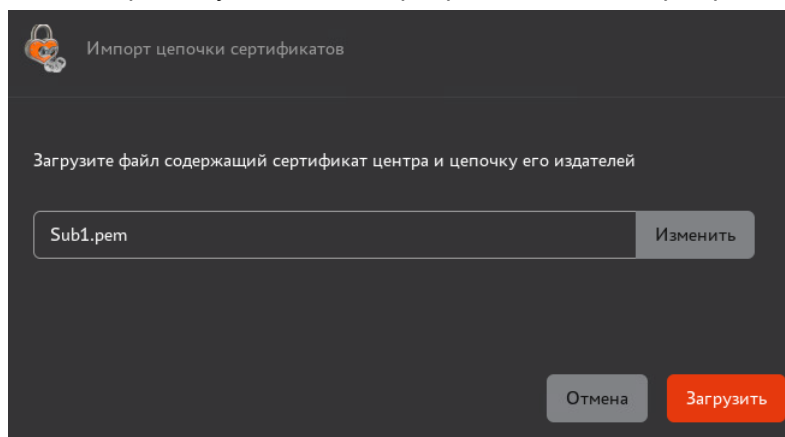


Рисунок 55 – Окно импорта цепочки сертификатов

В процессе загрузки будет осуществлена проверка загружаемого сертификата, а именно:

- имени Подчинённого Центра сертификации, указанного в импортируемом сертификате (компонент «Common name» в поле «Subject») на соответствие имени, указанному в лицензии Подчинённого Центра сертификации;
- имени корневого Центра сертификации, указанного в его сертификате (компонент «Common name» в поле «Subject») на соответствие имени корневого Центра сертификации, указанному в лицензии;
- соответствия порядка расположения компонентов SDN в поле «Subject» в сертификате Подчинённого Центра сертификации порядку, указанному в таблице 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 Центра сертификации, создаваемых eCA-CA 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;
- 31) DATEOFBIRTH;
- 32) PLACEOFBIRTH;
- 33) ROLE.

В случае несоответствия каких-либо параметров импортируемого сертификата (цепочки сертификатов) администратор будет уведомлён сообщением об ошибке импорта сертификата Подчинённого Центра сертификации. Перечень сообщений об ошибках приведён в таблице 10. При этом в журнале событий будет зарегистрировано событие с кодом CAENV013.

Таблица 10 – Перечень сообщений в случае неудачной попытки импорта сертификата

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 Подчинённого ЦС, указанное в сертификате, не соответствует лицензии.	Ошибка несоответствия имени подчинённого ЦС, указанного в его сертификате (компонент «Common name» в поле «Subject» сертификата подчинённого ЦС) имени (перечню имён), 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 имён) корневого ЦС, указанному в лицензии.
Ошибка. Неизвестная ошибка.	Внутренняя ошибка ПО.

После успешной загрузки цепочки сертификатов открывается окно с уведомлением об успешной загрузке сертификата (см. Рисунок 56) и отображается следующая информация о сертификате Центра сертификации: издатель, субъект, срок действия сертификата. Также в результате успешной загрузки цепочки сертификатов в контейнере закрытого ключа данного Центра сертификации будут содержаться закрытый ключ данного Центра сертификации и цепочка сертификатов данного Центра сертификации. В журнал событий производится запись события CAENV012.

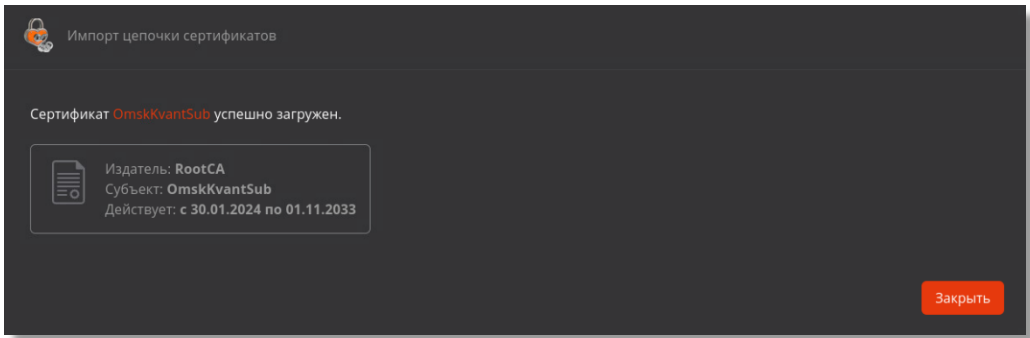


Рисунок 56 – Окно уведомления об успешном загрузке сертификата

- По нажатию на кнопку **<Закрыть>** в последнем окне импорта цепочки сертификатов:
  - сертификат присваивается Подчинённому Центру сертификации;
  - работа мастера импорта цепочки сертификатов завершается;
  - Центр сертификации автоматически активируется.

### 8.3.1.7 Удаление центра сертификации

**Внимание!** При удалении Корневого Центра сертификации будут автоматически удалены все Подчиненные удаляемому центру Центры сертификации, развернутые на данном хосте. Если при этом автоматически удаленный Подчинённый Центр сертификации был активным, необходимо восстановить доступ к программе в соответствии с инструкцией, приведённой в разделе 11 документа «Центр сертификатов доступа Aladdin Enterprise Certificate Authority Certified Edition. Руководство администратора. Часть 1. Установка и обслуживание Центра сертификации Aladdin Enterprise Certification Authority».

Условия удаления Центра сертификации:

- удаляемый Центр сертификации находится в состоянии «Не активирован» (см. Рисунок 57);



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

Рисунок 57 – Раздел «Центр сертификации» – Вкладка «Свои сертификаты» – Состояние удаляемого Центра сертификации

- выключена проверка издателя – удаляемого Центра сертификации (см. Рисунок 58, раздел 8.13 настоящего руководства).

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 58 – Раздел «Настройки» – Поле «Разрешённые издатели» – Выключение издателя из разрешённых

Для удаления Центра сертификации, наведите указатель мыши на строку с выбранным Центром сертификации и нажмите кнопку  или откройте карточку выбранного Центра сертификации и нажмите кнопку . В появившемся окне подтверждения внимательно ознакомьтесь с рекомендациями (см. Рисунок 59).

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

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

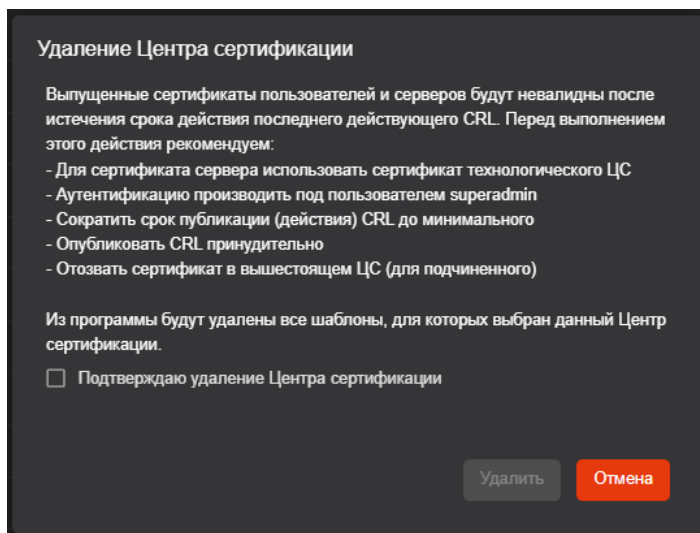


Рисунок 59 – Окно подтверждения удаления Центра сертификации

Сертификаты, ранее выпущенные удалённым Центром сертификации, будут действительны до следующего запланированного обновления списка отозванных сертификатов.

Центр валидации удалённого Центра сертификации необходимо самостоятельно удалить на сервере отзыва.

Для подтверждения удаления Центра сертификации установите флаг в чек-боксе «Подтверждаю удаление Центра сертификации» и нажмите ставшую активной кнопку **<Удалить>**. Для прерывания процесса удаления Центра сертификации нажмите кнопку **<Отмена>**.

#### 8.3.1.8 Экспорт закрытого ключа центра сертификации

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

- В разделе «Центр сертификации» перейти на вкладку «Свои сертификаты», затем перейдите в карточку Центра сертификации с состоянием «Не активирован» и с разрешённым экспортом закрытого ключа.
- В открывшейся карточке Центра сертификации перейдите на вкладку «Закрытый ключ». На данной вкладке нажмите на кнопку **<Экспортировать ключ>** (см. Рисунок 60).

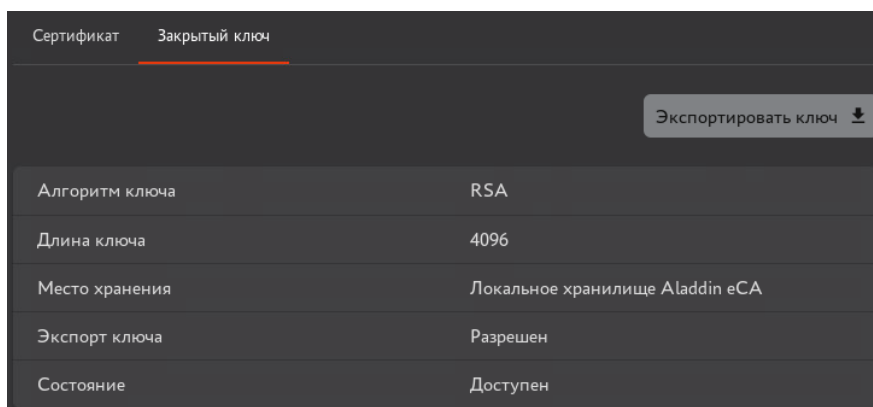


Рисунок 60 – Вкладка «Закрытый ключ» с возможностью экспорта закрытого ключа

- В отобразившемся окне «Экспорт закрытого ключа центра сертификации» задайте пароль для защиты контейнера PKCS#12, в который будем записан закрытый ключ данного Центра сертификации, и подтвердить введенный пароль (см. Рисунок 61).  
Пароль должен содержать не менее 8 (восьми) символов с использованием цифр, заглавных и прописных букв, ввод осуществляется на латинице.

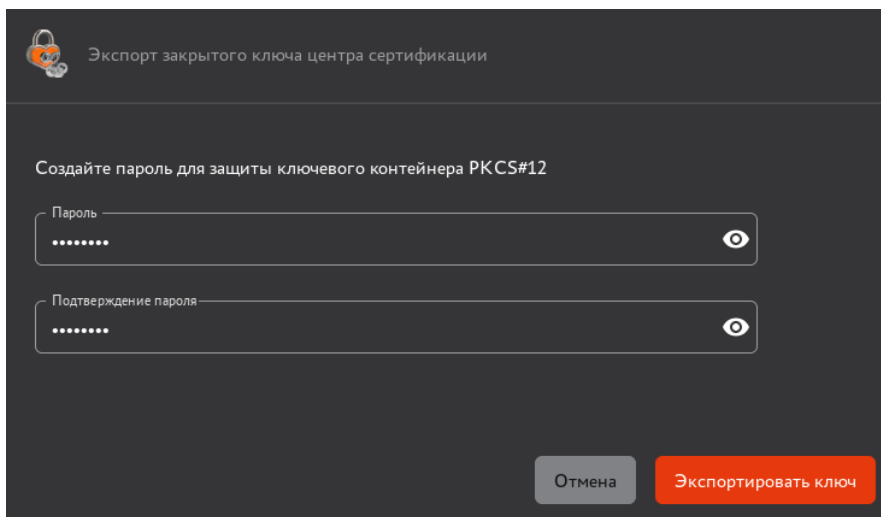


Рисунок 61 – Создание пароля для контейнера PKCS#12 при экспорте закрытого ключа

- 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 62).  
И будет доступно скачивание контейнера PKCS#12, содержащего экспортированный закрытый ключ Центра сертификации, 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 Центра сертификации, будет недоступно. В случае утери экспортированного контейнера закрытого ключа его восстановление будет невозможно.

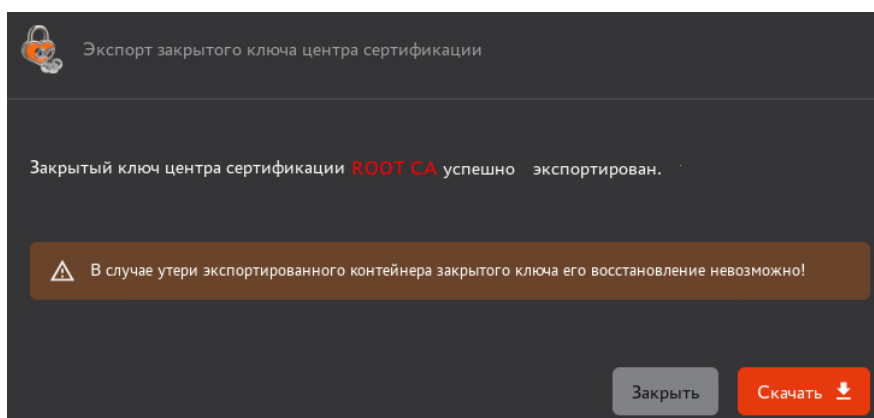


Рисунок 62 – Окно с успешным результатом экспорта закрытого ключа Центра сертификации

В результате выполнения экспорта закрытого ключа Центра сертификации:

- Закрытый ключ Центра сертификации будет удален из места хранения, определенного при создании данного Центра сертификации.
- Центр сертификации, 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.

### 8.3.1.9 Импорт закрытого ключа центра сертификации

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

- В разделе «Центр сертификации» перейдите на вкладку «Свои сертификаты», затем в карточку Центра сертификации с состоянием «Ключ экспортирован».
- В открывшейся карточке Центра сертификации перейдите на вкладку «Закрытый ключ». В данной вкладке нажмите на кнопку **<Импортировать ключ>** (см. Рисунок 63).

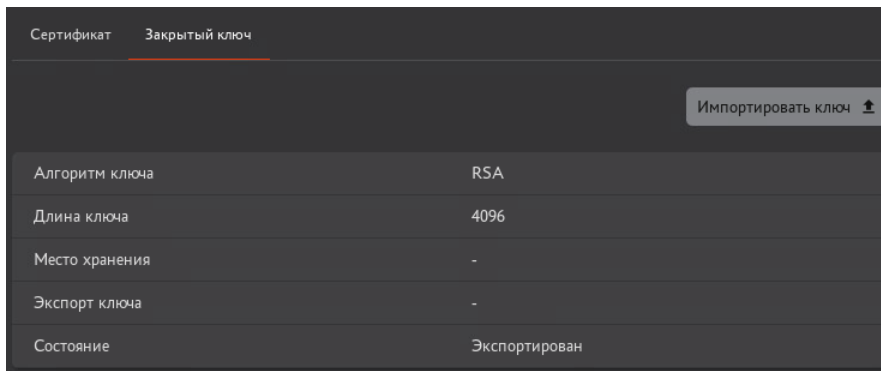


Рисунок 63 – Вкладка «Закрытый ключ» с возможностью импорта закрытого ключа

- В отобразившемся окне «Импорт закрытого ключа центра сертификации» на шаге 1 необходимо выбрать место хранения для закрытого ключа Центра сертификации (см. Рисунок 64).

Доступные варианты выбора, если криптопровайдером алгоритма ключа Центра сертификации является СКЗИ «КриптоПро CSP»:

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

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

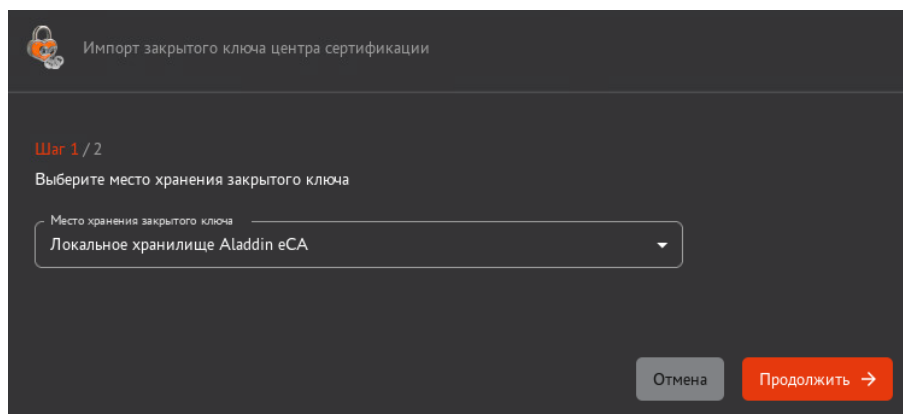


Рисунок 64 – Окно «Импорт закрытого ключа центра сертификации». Шаг 1/2

- Для перехода к следующему шагу нажмите на кнопку **<Продолжить>**.
- На шаге 2 загрузите файл контейнера закрытого ключа и введите пароль от него (см. Рисунок 65). Допустимое расширение для загружаемых файлов – **.p12**. При загрузке файла с иным расширением в поле загрузки файла будет отображено сообщение об ошибке «Некорректный формат файла».

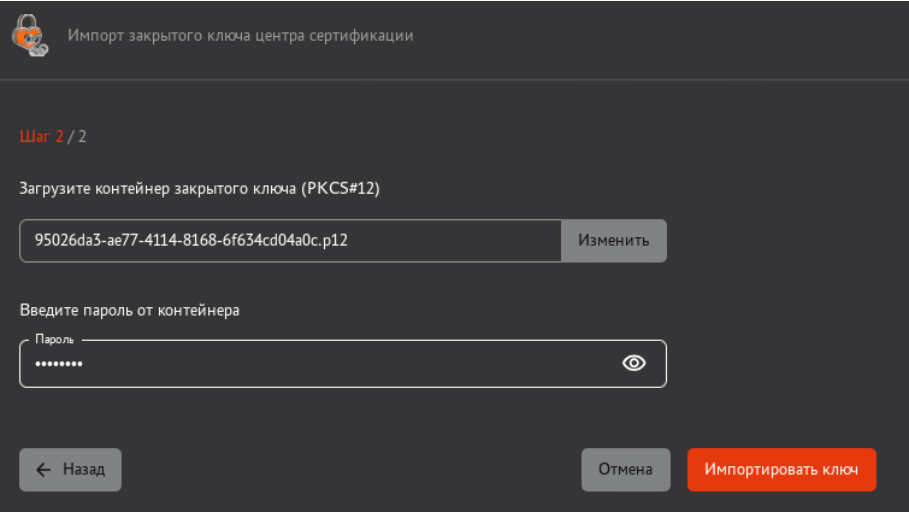


Рисунок 65 – Окно «Импорт закрытого ключа центра сертификации». Шаг 2/2

- 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 одно из сообщений об ошибке, представленных в таблице 11.

Таблица 11 – Перечень сообщений в случае неудачной попытки импорта закрытого

Текст ошибки	Причина
Неверный пароль	Указание неверного пароля от контейнера закрытого ключа Центра сертификации
Закрытый ключ не соответствует открытому ключу ЦС	При попытке импорта закрытого ключа, не соответствующего открытому ключу данного Центра сертификации
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 Центра сертификации

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 66).

В окне «Импорт закрытого ключа центра сертификации» будет доступно закрытие данного окна путем нажатия на кнопку **<Закрыть>**.

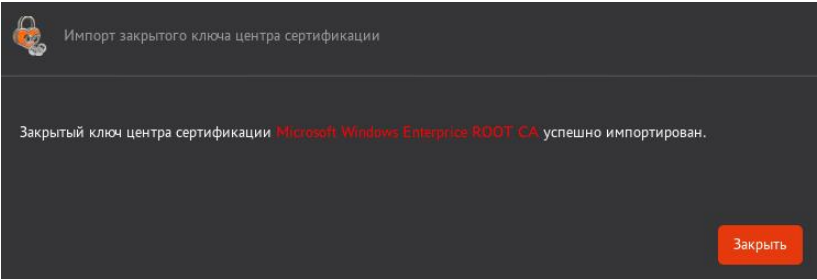


Рисунок 66 – Окно с успешным результатом импорта закрытого ключа Центра сертификации

В результате выполнения импорта закрытого ключа Центра сертификации:

- Закрытый ключ Центра сертификации будет помещен в хранилище, выбранное на шаге 1 окна «Импорт закрытого ключа центра сертификации»;
- Центр сертификации, ключ которого был импортирован, перейдет в состояние «Не активирован».

### 8.3.1.10 Повторный импорт сертификата (цепочки сертификатов) подчинённого ЦС

Для повторного импорт сертификата (цепочки сертификатов) подчинённого ЦС:

- Перейдите в карточку подчинённого ЦС, срок действия сертификата которого не истёк или закрытый ключ которого не экспортирован.
- Нажмите на кнопку «Импортировать сертификат».

- В окне импорта цепочки сертификатов (см. рисунок 67) выберите файл цепочки сертификатов и нажмите кнопку «Загрузить».

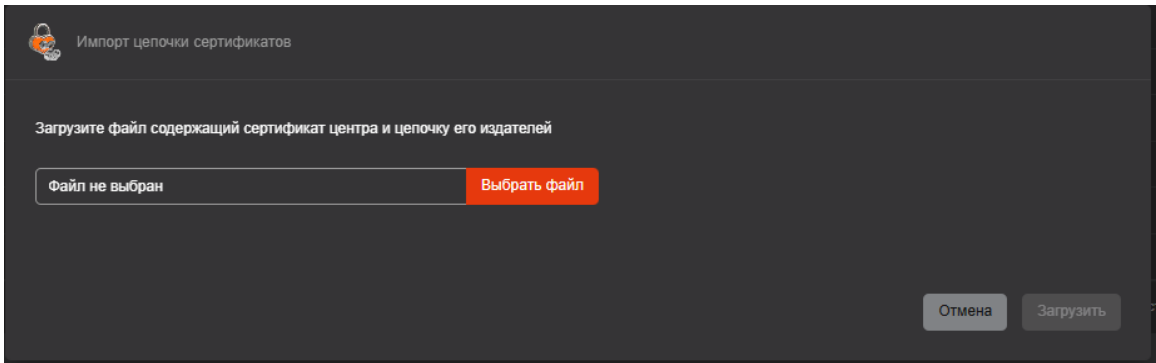


Рисунок 67 — Окно импорта цепочки сертификата

- В окне с уведомлением об успешной загрузке сертификата ознакомьтесь с информацией и нажмите кнопку «Закрыть».

В результате импорта нового сертификата (цепочки сертификатов):

- предыдущий сертификат починенного ЦС будет заменён новым сертификатом, включая его замену в контейнере закрытого ключа данного ЦС;
- в точки распространения AIA данного подчинённого ЦС будет опубликован новый сертификат данного ЦС.

### 8.3.2 Вкладка «Сертификаты Подчиненных центров»

Вкладка «Сертификаты Подчиненных центров» (см. Рисунок 68) предназначена для работы с Сертификатами Подчиненных Центров сертификации. В списке сертификатов подчиненных Центров сертификации 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 таблице .

Таблица 12 – Действия над сертификатами Подчиненных центров

Состояние сертификата	Функции управления сертификатами		
	скачать	удалить	отозвать
Действительный	+	-	+
Отозван	+	-	-
Истёк срок	+	-	-

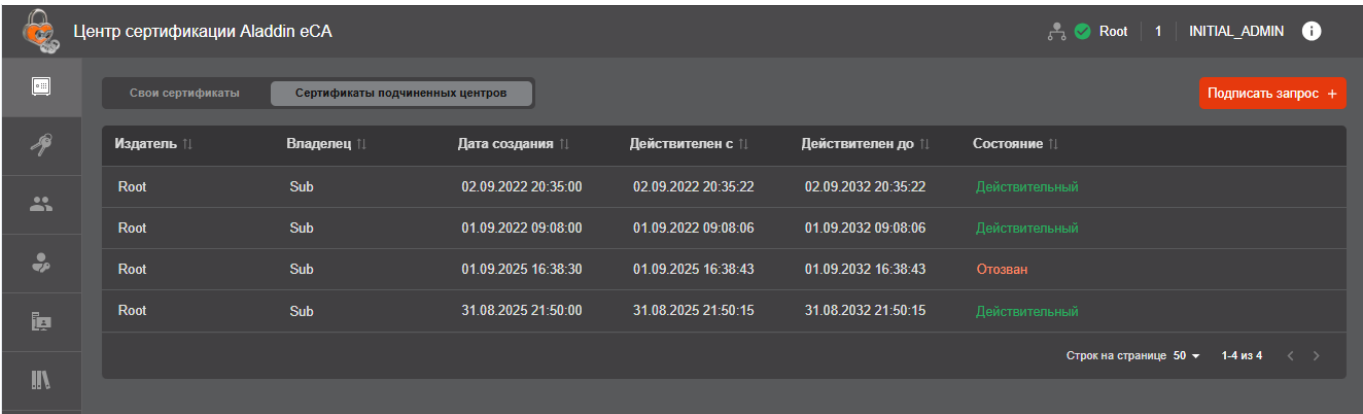


Рисунок 68 – Экран «Сертификаты Подчиненных центров»

В соответствии с состоянием Подчинённого сертификата при помощи кнопок управления, расположенных на табличных полях, возможны действия, приведённые в таблице ниже (Таблица 12).

### 8.3.2.1 Просмотр списка сертификатов подчинённого ЦС

Для просмотра списка сертификатов подчинённого ЦС:

- В меню еСА-СА выберите раздел «Центр сертификации», нажав по соответствующему элементу управления (кнопки) в меню (в левой части экрана).
- В верхней части отобразившегося окна раздела выберите вкладку «Сертификаты подчинённых центров».

### 8.3.2.2 Подписание запроса в Корневом Центре сертификации

После предварительного скачивания запроса на сертификат Подчинённого Центра сертификации и переноса его на Корневой Центр сертификации выполните следующие действия:

- При активном Корневом Центре сертификации, от имени которого будет выдан сертификат, на вкладке «Сертификаты Подчиненных центров» нажмите кнопку **<Подписать запрос>** (см. Рисунок 69).

**Внимание!** Подписание файла–запроса и выдача подписанного сертификата производится от Центра сертификации в состоянии «Активирован» на вкладке «Сертификаты подчинённых центров». Запрос на сертификат Подчинённого Центра сертификации может быть подписан Корневым Центром сертификации только один раз. Выпускаемые сертификаты Подчиненных Центров сертификации должны подписываться с использованием алгоритма хэш–суммы Центра сертификации, на котором подписывается запрос, вне зависимости от указанного в запросе алгоритма хэш–суммы.

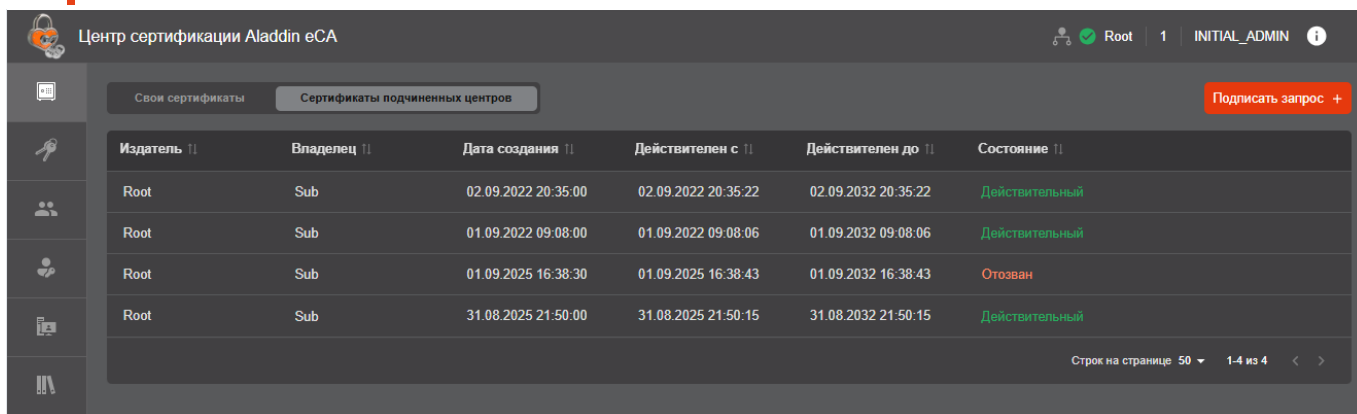


Рисунок 69 – Окно «Сертификаты Подчиненных ЦС»

- В открывшемся окне загрузите файл-запрос в формате `.csr`, нажав кнопку **<Выбрать файл>** (см. Рисунок 70).
- Выберите шаблон сертификата Подчинённого Центра сертификации (например, предварительно подготовленный шаблон путём редактирования клонированного предустановленного шаблона Центра сертификации в разделе «Шаблоны»).

Срок действия сертификата Подчинённого Центра сертификации определяется шаблоном «Sub CA» <sup>1</sup>, но не превышает срок действия сертификата Корневого Центра сертификации.

<sup>1</sup> Про шаблон «Sub CA» см. в приложении 2 «Описание полей предустановленных шаблонов сертификатов».

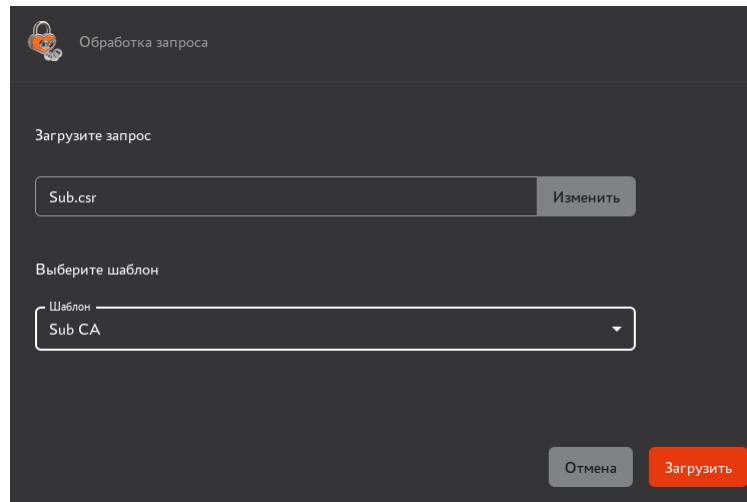


Рисунок 70 – Окно выбора файла запроса

На текущем шаге, после выбора файла запроса, возможно изменить выбор, нажав кнопку **<Изменить>** (см. Рисунок 70).

- Нажмите кнопку **<Загрузить>** (см. Рисунок 70).

При нажатии кнопки **<Загрузить>** происходит загрузка файл запроса в Корневой Центр сертификации (текущий активный Корневой Центр сертификации из категории «Свои сертификаты»). Далее администратор видит уведомление о том, что сертификат Подчинённого Центра сертификации успешно сформирован и подписан Корневым Центром сертификации (см. Рисунок 71).

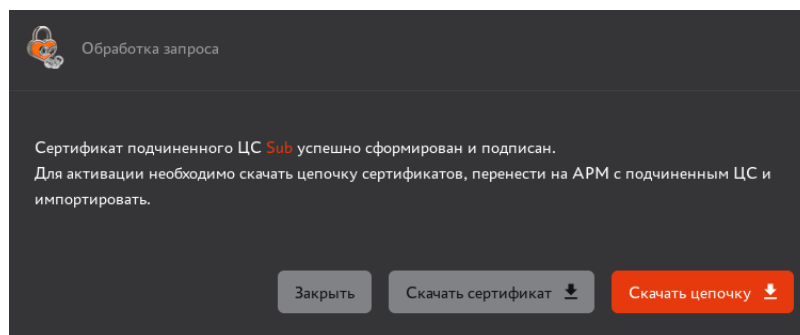



Рисунок 71 – Окно успешного формирования и подписи сертификата

- Необходимо скачать цепочку сертификатов Центра сертификации 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 Подчинённых центров», выбрав нужный сертификат и нажав появившуюся кнопку  для скачивания сертификата или цепочки сертификатов, выбрав соответствующий пункт в раскрывшемся меню.

Далее перенесите сертификат на Подчинённый Центр сертификации и выполните импорт цепочки сертификатов согласно разделу 8.3.1.6 настоящего руководства.

### 8.3.2.3 Просмотр свойств сертификата подчинённого ЦС в карточке сертификата подчинённого ЦС

Свойства сертификата представлены в карточке сертификата (см. Рисунок 72). Для просмотра карточки сертификата подчинённого ЦС перейдите на вкладку «Сертификаты подчинённых центров» и щёлкните на строке необходимого сертификата.

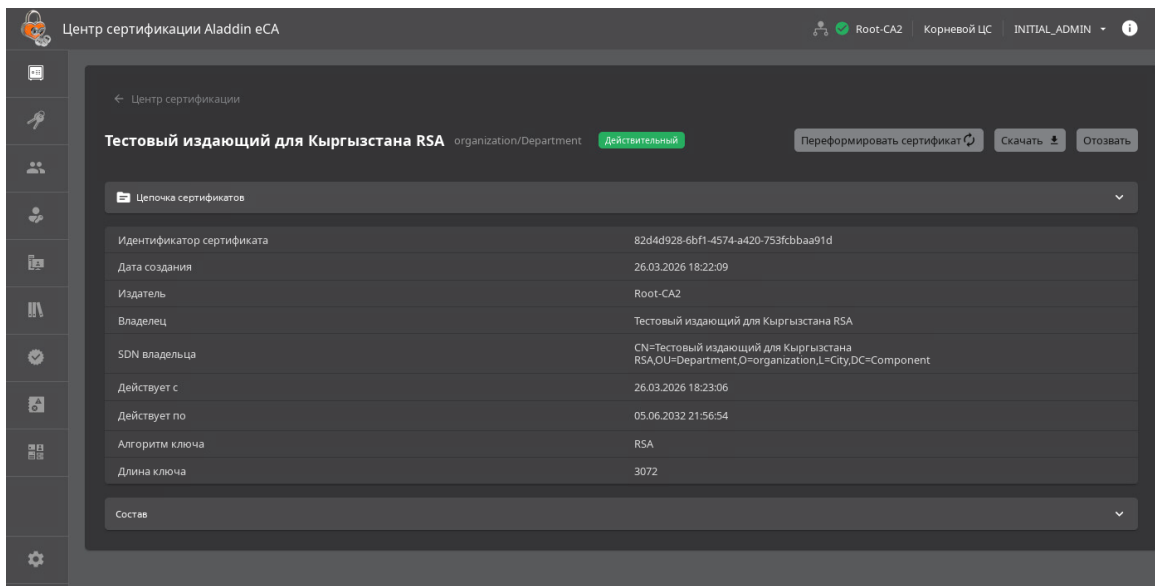


Рисунок 72 — Карточка сертификата Подчинённого Центра сертификации

#### 8.3.2.4 Отзыв сертификата

Для отзыва сертификата нажмите кнопку «Отозвать» либо в строке выбранного сертификата, либо в его карточке.

#### 8.3.2.5 Скачивание сертификата/цепочки сертификатов

Для скачивания сертификата/цепочки сертификатов:

1. Нажмите кнопку «Скачать» (либо в строке выбранного сертификата, либо в его карточке).
2. Выберите один из вариантов меню «Скачать сертификат» или «Скачать цепочку».

#### 8.3.2.6 Переформирование сертификата подчинённого ЦС

Для переформирования сертификата подчинённого ЦС:

1. Выберите в списке сертификат, имеющий состояние «Действительный», и перейдите в его карточку.
2. Нажмите кнопку «Переформировать сертификат».
3. В окне подтверждения переформирования сертификата подчинённого ЦС (см. рисунок 73) включите чекбокс «Подтверждаю переформирование сертификата подчинённого центра» и нажмите кнопку «Переформировать».

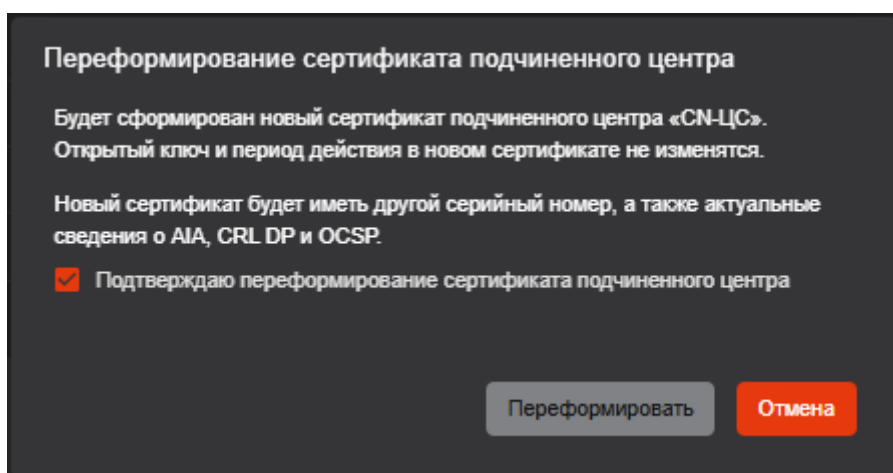


Рисунок 73 — Окно подтверждения переформирования сертификата подчинённого ЦС

В случае успешного переформирования:

- Будет выведено сообщение «Сертификат успешно переформирован».
- Будет сформирован новый сертификат подчинённого Центра сертификации. Открытый ключ и период действия в новом сертификате не изменятся.

- Новый сертификат будет иметь другой серийный номер, а также актуальные сведения о AIA, CRL DP и OCSP.

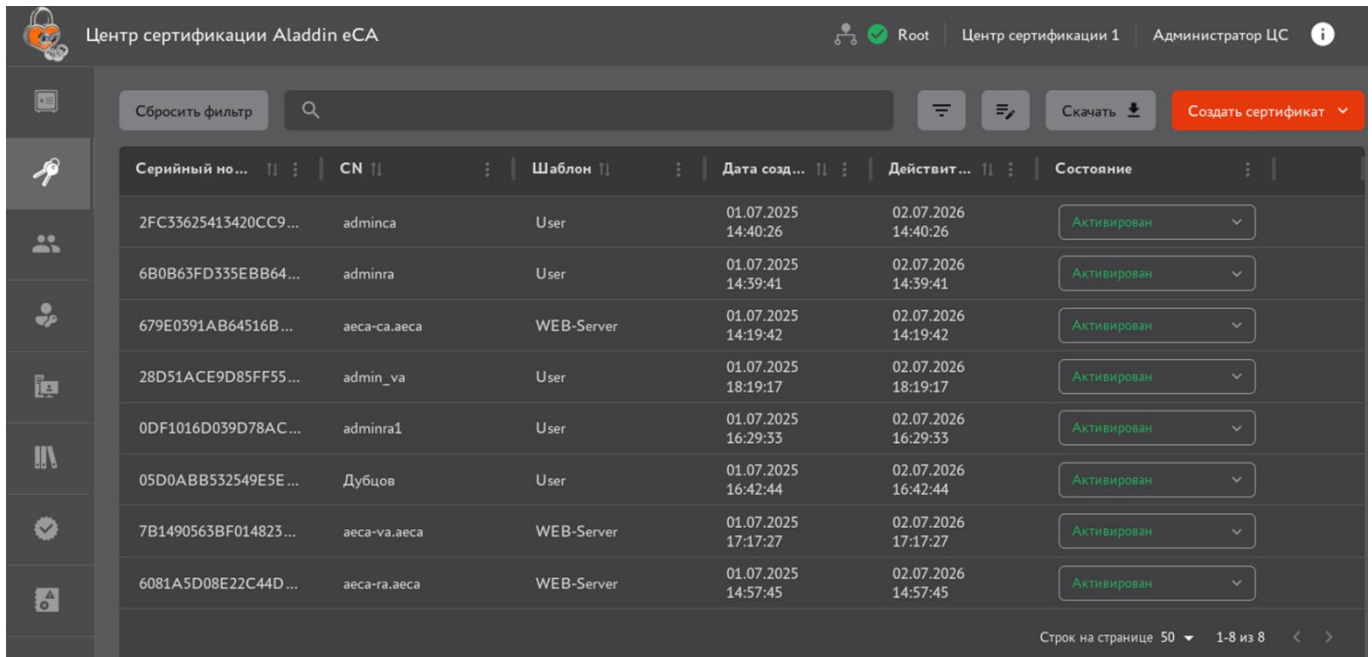
## 8.4 Раздел «Сертификаты»

**Внимание!** Технологический Центр сертификации использовать для выпуска сертификатов запрещено.

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 Центром сертификации осуществляется по выбору раздела «Сертификаты» бокового меню, расположенного слева на главном экране (см. Рисунок 43).

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



Центр сертификации Aladdin eCA

Root | Центр сертификации 1 | Администратор ЦС

Сбросить фильтр | Поиск | Сортировка | Фильтры | Скачать | Создать сертификат

Серийный номер	CN	Шаблон	Дата созд...	Действит...	Состояние
2FC33625413420CC9...	adminca	User	01.07.2025 14:40:26	02.07.2026 14:40:26	Активирован
6B0B63FD335EBB64...	adminra	User	01.07.2025 14:39:41	02.07.2026 14:39:41	Активирован
679E0391AB64516B...	aeca-ca.aeca	WEB-Server	01.07.2025 14:19:42	02.07.2026 14:19:42	Активирован
28D51ACE9D85FF55...	admin_va	User	01.07.2025 18:19:17	02.07.2026 18:19:17	Активирован
0DF1016D039D78AC...	adminra1	User	01.07.2025 16:29:33	02.07.2026 16:29:33	Активирован
05D0ABB532549E5E...	Дубцов	User	01.07.2025 16:42:44	02.07.2026 16:42:44	Активирован
7B1490563BF014823...	aeca-va.aeca	WEB-Server	01.07.2025 17:17:27	02.07.2026 17:17:27	Активирован
6081A5D08E22C44D...	aeca-ra.aeca	WEB-Server	01.07.2025 14:57:45	02.07.2026 14:57:45	Активирован

Строк на странице 50 | 1-8 из 8

Рисунок 74 – 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;
  - скачивание бумажного сертификата (файл, содержащий сведения из сертификата).
  - 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 и через REST API.

**Внимание!** 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.

#### 8.4.1 Выпуск сертификата

Для выпуска сертификата для существующего или нового субъекта нажмите кнопку **<Создать сертификат>** и выберите способ создания из выпадающего списка (см. Рисунок 75):

- с закрытым ключом (PKCS# 12);
- на основании запроса;
- на ключевом носителе.

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

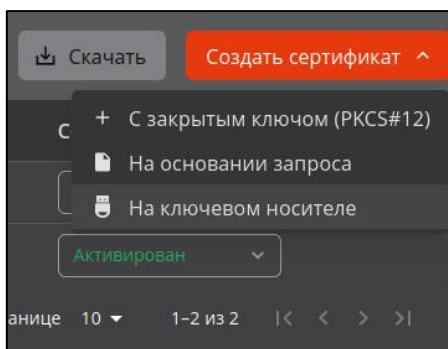


Рисунок 75 – Выпуск сертификата в разделе «Сертификаты»

#### 8.4.2 Поиск сертификатов

Строка поиска (см. Рисунок 76) 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.

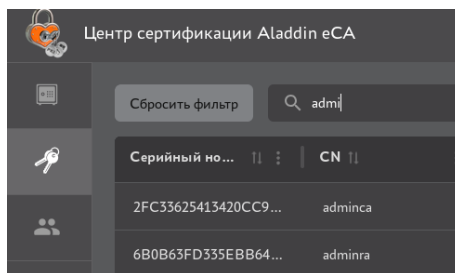



Рисунок 76 – Поисковая строка в разделе «Сертификаты»

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

### 8.4.3 Сортировка сертификатов

Средства сортировки выпущенных сертификатов представлены элементами выбора направления сортировки в заголовке таблицы экранной формы (см. Рисунок 77):

- «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.

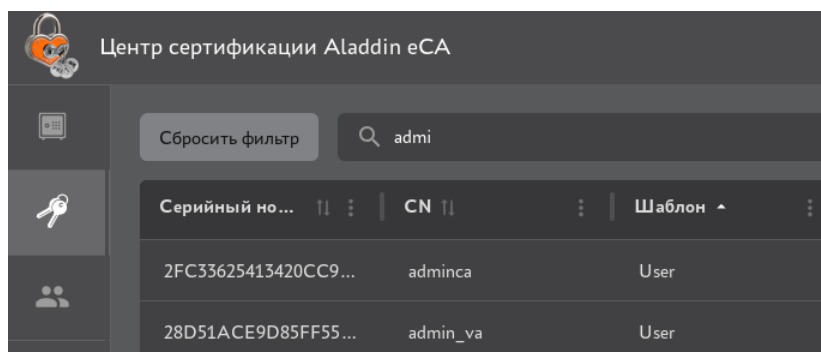




Рисунок 77 – Сортировка сертификатов

Также отобразить в определённом порядке список сертификатов (отсортировать) в колонке возможно по нажатию кнопки  **<Действия в колонке>**, выбрав и нажав в раскрывшемся меню «Сортировать...» (см. Рисунок 79).


### 8.4.4 Фильтрация сертификатов

#### 8.4.4.1 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 78):

- 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).

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 .

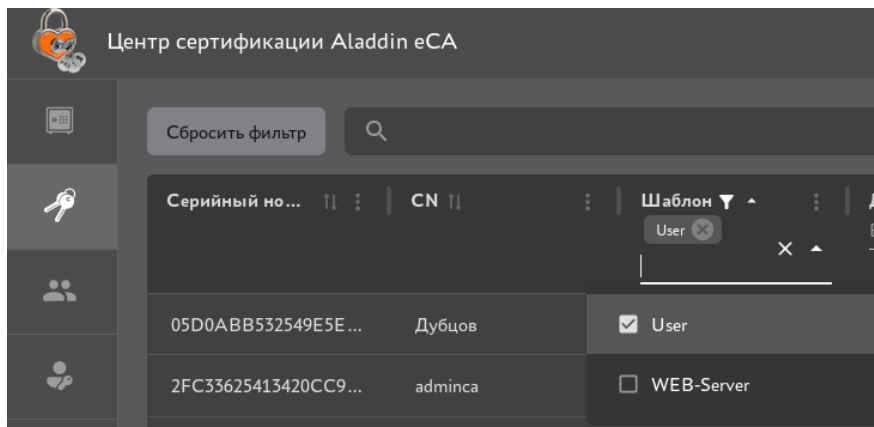


Рисунок 78 – Поля фильтра заголовков экранной таблицы

#### 8.4.4.2 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 79);

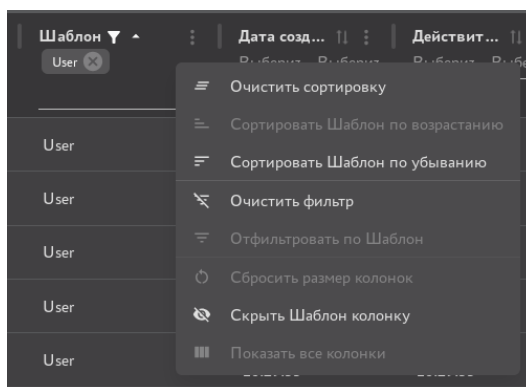


Рисунок 79 – Кнопка <Очистить> фильтр

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

#### 8.4.5 Скачивание сертификатов

Для скачивания наведите указатель мыши на выбранный сертификат в экранной таблице, нажмите появившуюся кнопку **Скачать** (см. Рисунок 74) и в раскрывшемся меню выберите пункт **<Скачать сертификат>** или **«Скачать цепочку»** в формате **.pem** (см. Рисунок 80).

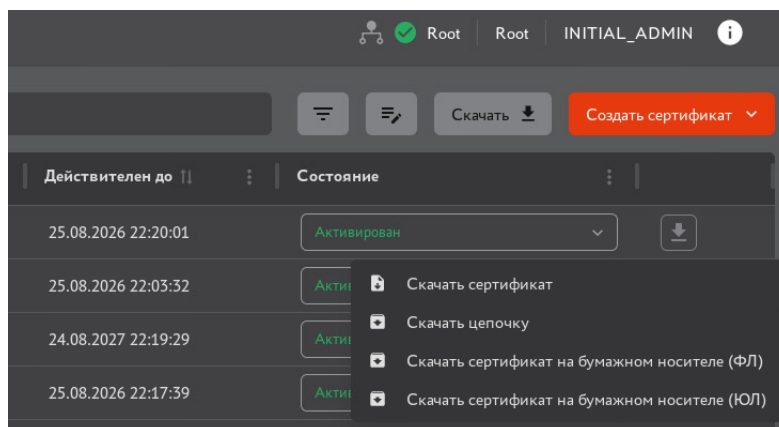



Рисунок 80 – Скачивание сертификата и цепочки сертификатов

Для изготовления и экспорта документа, содержащего значения полей данного сертификата (далее –сертификат на бумажном носителе) нажмите кнопку  и во всплывающем меню выберите **<Скачать сертификат на бумажном носителе (ФЛ)>** (для физических лиц) или **<Скачать сертификат на бумажном носителе (ЮЛ)>** (для юридических лиц).

Изготавливаемый и экспортируемый сертификат на бумажном носителе представлять собой HTML-файл с названием формата **[Common Name субъекта].html**.

Формат сертификата на бумажном носителе для каждого типа, а также правила записи значений в поля сертификата на бумажном носителе представлены в приложении 5.

#### 8.4.6 Статус сертификатов

Возможные варианты состояния и доступные действия над сертификатами в зависимости от состояния приведены в таблице 13.

Таблица 13 – 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 81).

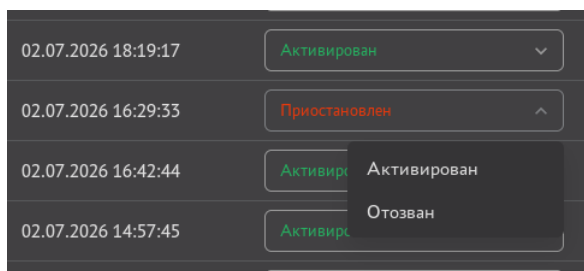


Рисунок 81 – Выпадающее меню смены состояния сертификата

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 82)

**Внимание!** 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».

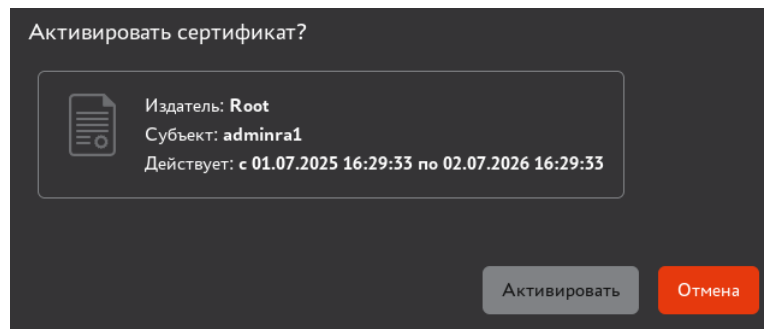


Рисунок 82 – Окно активации сертификата

- отзыв (см. Рисунок 83);

**Внимание!** Данную операцию нельзя отменить.

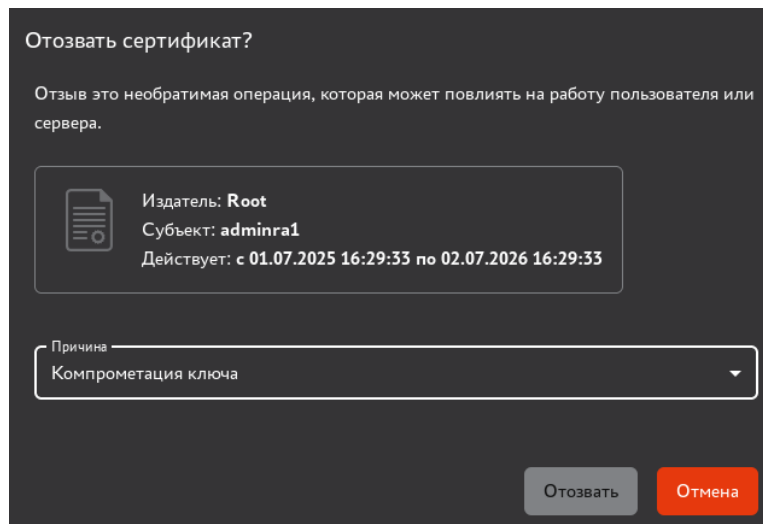


Рисунок 83 – Окно отзыва сертификата

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 (keyCompromised);
  - компрометация Центра сертификации (сACompromised);
  - заменен (сертификат) – заменен на иной сертификат;
  - без указания причины (unspecified).
- Приостановка действия сертификата (см. Рисунок 84):

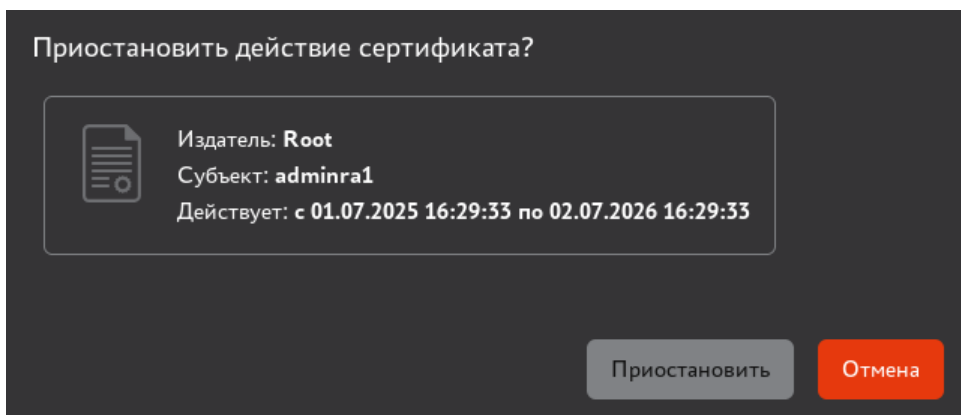


Рисунок 84 – Окно приостановки действия сертификата

#### 8.4.7 Карточка сертификата

Просмотр данных сертификата возможен посредством страницы «Карточка сертификата».

Переход к экрану «Карточка сертификата» (см. Рисунок 85) осуществляется при нажатии на строку сертификата таблицы главного экрана раздела «Сертификаты» (см. Рисунок 74).

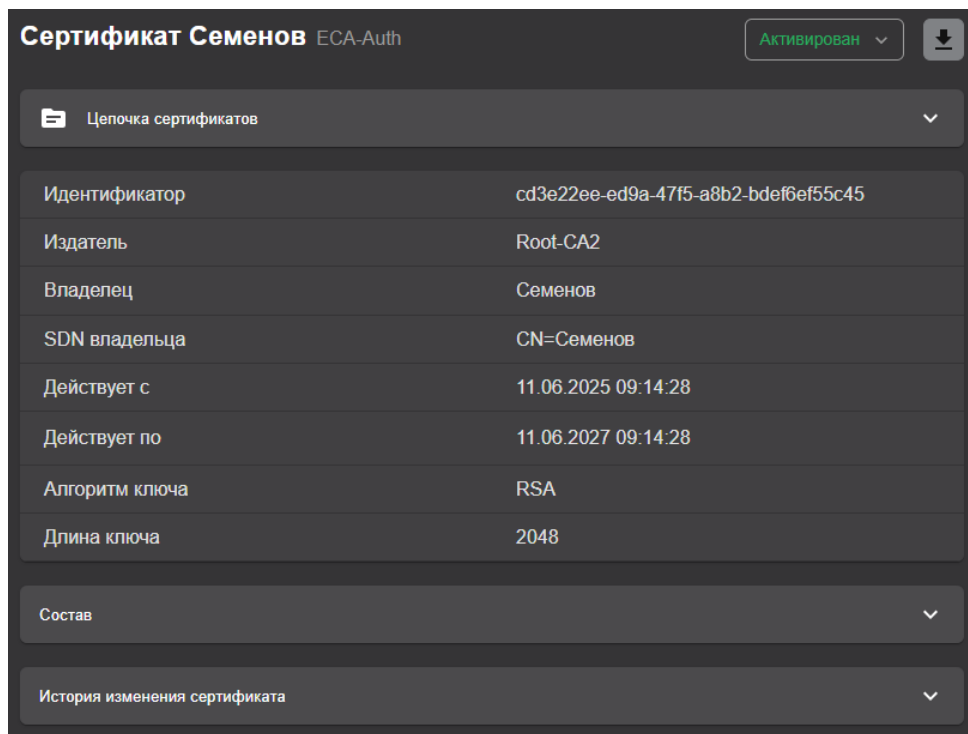


Рисунок 85 – Окно «Карточка сертификата»

Оглавление карточки сертификата включает в себя:

- тип сертификата;
- принадлежность;
- тип субъекта.

Для возврата на главный экран раздела «Сертификаты» проследовать по стрелке ← Сертификаты.

Для изменения статуса сертификата выбрать из выпадающего списка действие в соответствии с таблицей 13.

**Внимание!** 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 нажмите кнопку  и во всплывающем меню (см. Рисунок 86) выберите <Скачать сертификат> субъекта или <Скачать цепочку сертификатов>.

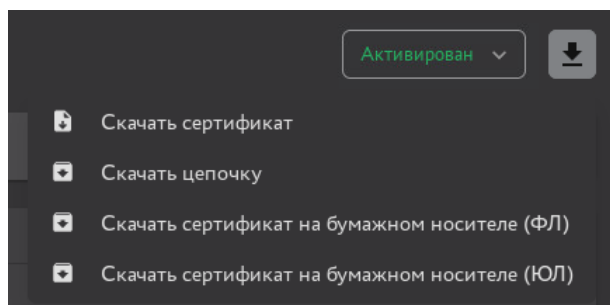




Рисунок 86 – Скачивание сертификата

Для изготовления и экспорта документа, содержащего значения полей данного сертификата (далее –сертификат на бумажном носителе) нажмите кнопку  и во всплывающем меню (см. Рисунок 86) выберите **<Скачать сертификат на бумажном носителе (ФЛ)>** (для физических лиц) или **<Скачать сертификат на бумажном носителе (ЮЛ)>** (для юридических лиц). Изготавливаемый и экспортируемый сертификат на бумажном носителе представлять собой HTML-файл с названием формата [Common Name субъекта].html. Формат сертификата на бумажном носителе для каждого типа, а также правила записи значений в поля сертификата на бумажном носителе представлены в приложении 5.

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 Центра сертификации, на основе которого строится цепочка доверия сертификатам, до конечного Центра сертификации, выдавшего текущий сертификат субъекта (см. Рисунок 87).

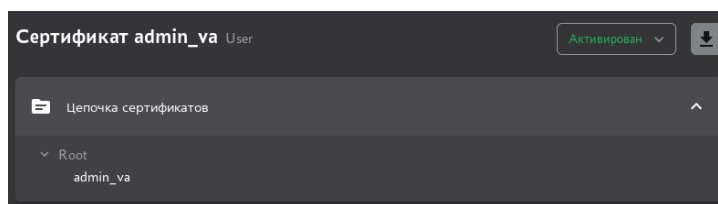



Рисунок 87 – Окно карточки сертификата. Подменю «Цепочка сертификатов»

- «Состав». Раскройте вкладку, нажав в строке с именем вкладки символ . На раскрывшемся экране отображены следующие поля (см. Рисунок 88):

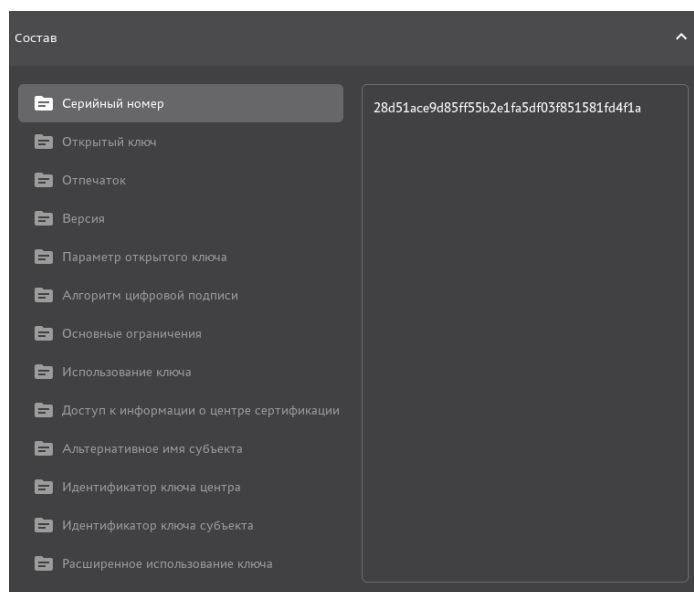



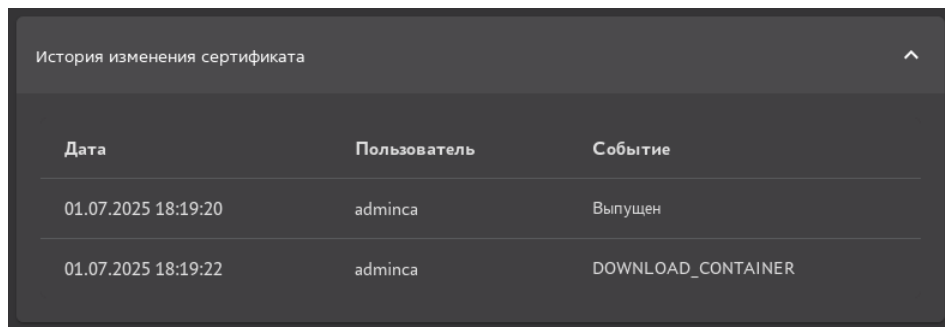
Рисунок 88 – Окно карточки сертификатов. Вкладка «Состав»

- 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 сертификации;
- идентификатор ключа субъекта;
- расширенное использование ключа.

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

- «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 89):
  - дата – дата совершенного действия;
  - пользователь – учётная запись, под которой было совершено данное действие;
  - событие – действие, совершённое над сертификатом.



История изменения сертификата		
Дата	Пользователь	Событие
01.07.2025 18:19:20	adminca	Выпущен
01.07.2025 18:19:22	adminca	DOWNLOAD_CONTAINER




Рисунок 89 – Окно карточки сертификатов. Вкладка «История изменения сертификата»

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

#### 8.4.8 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**. Происходит формирование списка сертификатов, по завершению действия и готовности к выгрузке списка сертификатов кнопка переходит в состояние  **Скачать (готово)**. Нажмите кнопку  **Скачать (готово)** для сохранения подготовленного списка сертификатов.

Сохранение списка сертификатов выполняется в виде zip-архива.


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:

- fingerprint – содержит уникальный числовой отпечаток сертификата;
- cafingerprint – содержит уникальный числовой отпечаток сертификата Центра сертификации, 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.

#### 8.4.9 Массовые операции с сертификатами

Порядок выполнения массовых операций с сертификатами:

- Для запуска мастера массовых операций с сертификатами нажмите кнопку  **<Массовые операции>** (см. рисунок 90).

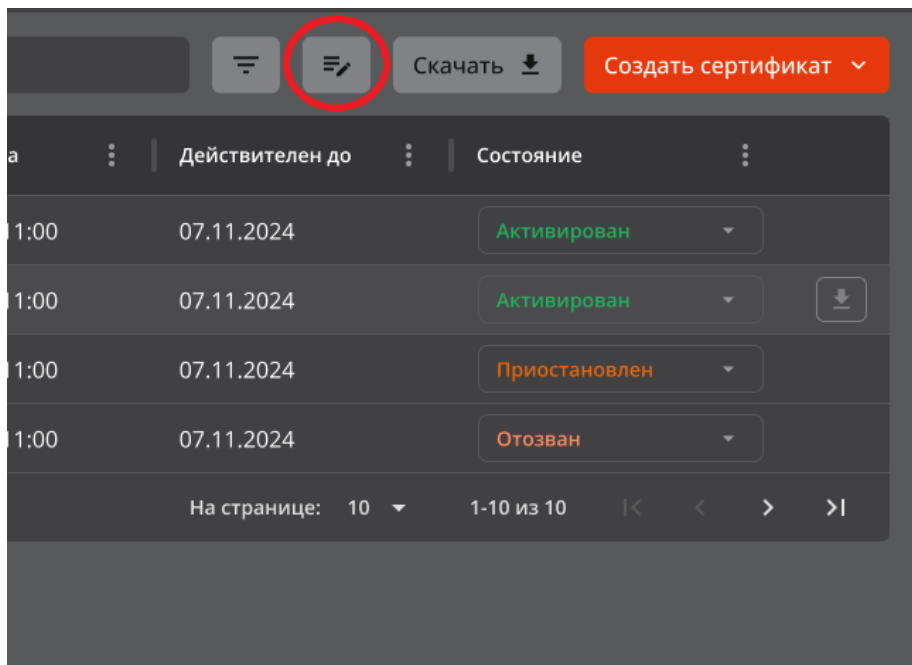


Рисунок 90 – Расположение кнопки запуска мастера массовых операций с сертификатами

- Выберите необходимую операцию из раскрывающегося списка (см. рисунок 91).

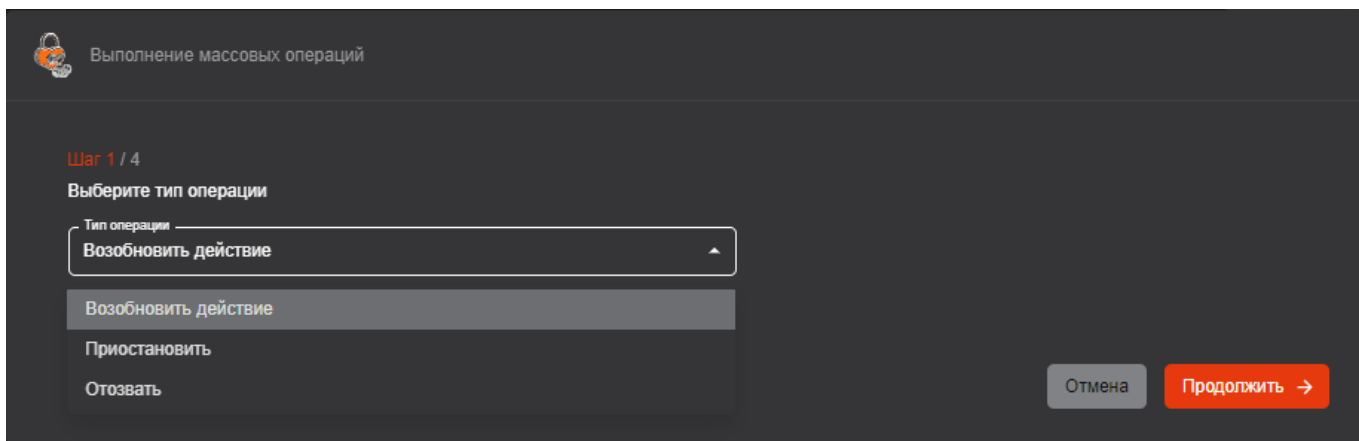


Рисунок 91 — Окно выполнения массовых операций. Шаг 1. Выбор типа операции

Доступны следующие типы операций:

- возобновление действия;
- приостановить;
- отозвать.

При выборе операции «Отозвать» дополнительно необходимо будет указать причину отзыва из выпадающего списка (см. рисунок 92).

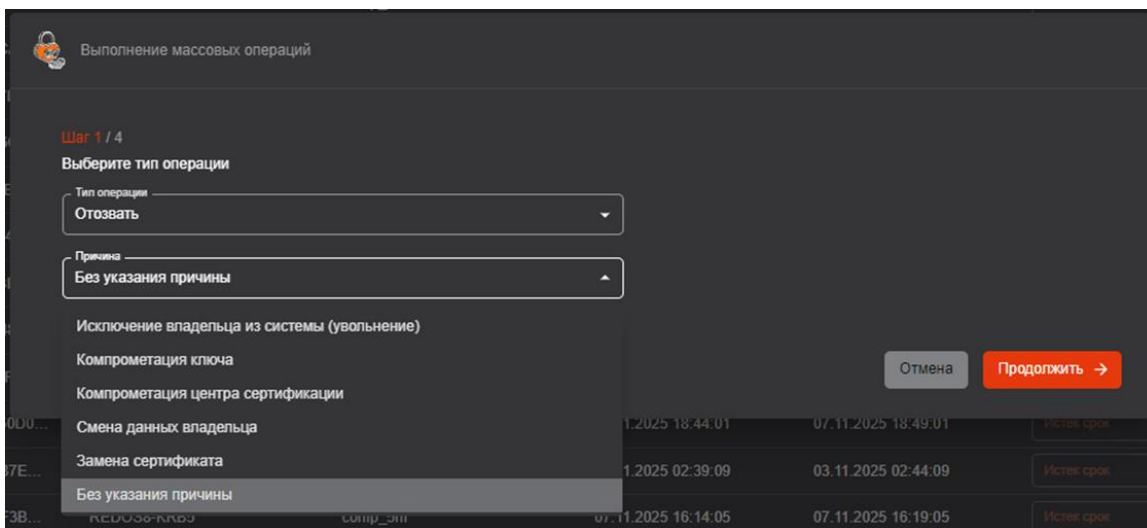


Рисунок 92 — Окно выполнения массовых операций. Шаг 1. Выбор причины отзыва

- Нажмите кнопку **<Продолжить>**.

До применения поиска в левом столбце окна будет доступен просмотр первых 100 сертификатов с соответствующим статусом (в зависимости от выбранной операции на шаге 1) в алфавитном порядке по атрибуту Common Name (см. рисунок 93). Для просмотра сертификатов применяйте прокрутку списка. Сертификаты отображаются в формате «CN в сертификате (SN: серийный номер сертификата)». Поиск в столбце «Выбрать» и «Выбрано» осуществляется по вхождению поискового запроса в SDN или SAN, указанному в сертификате. Поиск сертификатов производится с учётом текущего статуса сертификата и выбранного типа операции на шаге 1, отображается (с учётом использования прокрутки) не более 100 результатов поиска.

Например, при выборе типа операции «Возобновить» поиск осуществляется только среди сертификатов со статусом «Приостановлен», для которых допустимо выполнить данный тип операции.

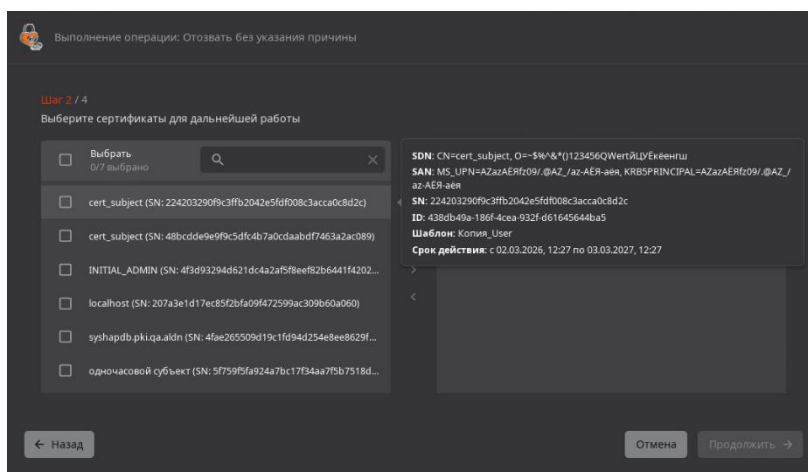





Рисунок 93 — Окно выполнения массовых операций. Шаг 2

При наведении курсора на сертификат в списке отображается всплывающее сообщение с текстом следующего формата:

- **SDN:** Поля SDN сертификата в формате "ключ=значение". Разделитель полей — запятая с пробелом. Множественные значения для одного поля указываются через запятую.

- **SAN:** Поля SAN сертификата в формате "ключ=значение". Разделитель полей — запятая с пробелом. Множественные значения для одного поля указываются через запятую. Если сертификат не имеет полей SAN, в данном поле всплывающего окна будет указан прочерк ("-").
  - **SN:** серийный номер сертификата.
  - **ID:** идентификатор сертификата.
  - **Шаблон:** шаблон, по которому был создан сертификат.
  - **Срок действия:** с {дата и время начала действия сертификата} по {дата и время окончания действия сертификата}
- 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.
  - 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 .
  - Для перехода на следующий шаг нажмите кнопку **<Продолжить>**.
  - В открывшемся окне подтвердите действие, нажав кнопку **<Применить>** (см. Рисунок 94).

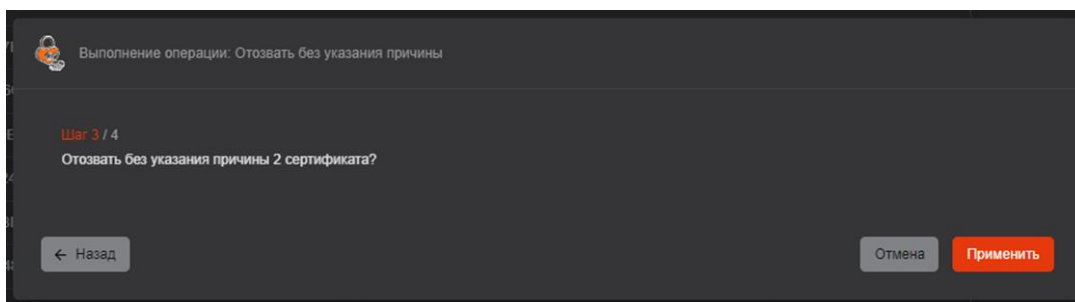


Рисунок 94 – Окно выполнения массовых операций. Шаг 3

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

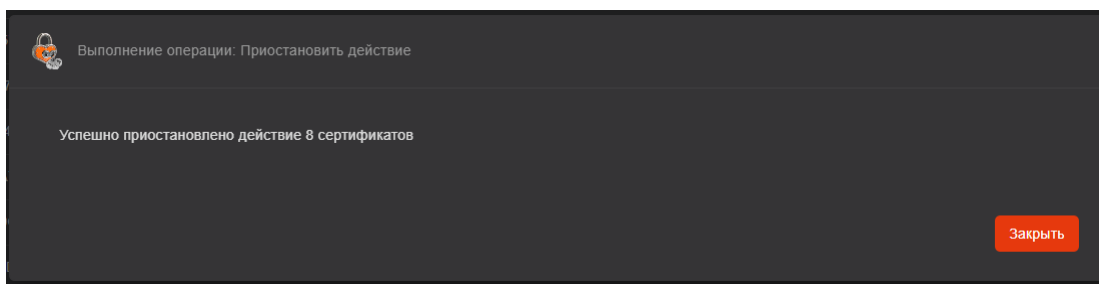


Рисунок 95 – Окно выполнения массовых операций. Шаг 4. Успешное выполнение операции со всеми сертификатами

Если выбранная на шаге 1 операция не может быть выполнена со всеми сертификатами в связи с лицензионными ограничениями, выбранными на шаге 2, то в окне шага 4 отображается количество и перечень CN из сертификатов, для которых операция не была завершена успешно. Для копирования содержимого окна в буфер обмена нажмите кнопку «Копировать».



Рисунок 96 — Окно выполнения массовых операций. Шаг 4. Успешное выполнение операции с частью сертификатов

## 8.5 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 97).

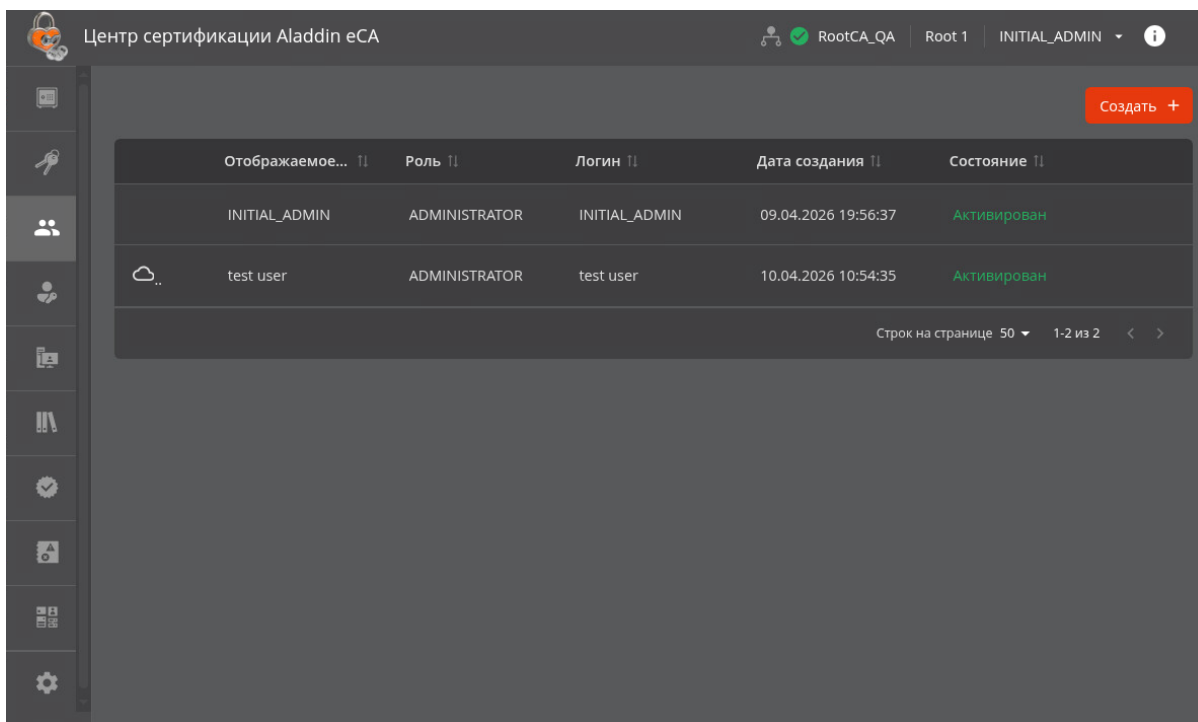


Рисунок 97 — Экран раздела меню «Учётные записи»

В разделе «Учётные записи» присутствуют:

- кнопка «Создать» для создания новой учетной записи;
- таблица с перечнем учетных записей. Для каждой учетной записи указаны отображаемое имя, роль, логин, дата создания, состояние. Для учетной записи, созданной на основе субъекта, присутствует индикация (в виде пиктограммы «Облако»). Для автоматических учетных записей присутствует дополнительная индикация (в виде пиктограммы «Синхронизируемый пользователь», при наведении курсора на которую отображается всплывающее сообщение «Автоматическая учетная запись».
- Для учетных записей, не являющихся автоматическими, доступны кнопки «Редактировать», «Заблокировать» или «Активировать» (в зависимости от текущего состояния учетной записи), «Удалить» (недоступна для удаления текущей пользователя текущей сессии).
- Для автоматических учетных записей доступна кнопка «Заблокировать» или «Активировать» (в зависимости от текущего состояния учетной записи). Для автоматических учетных записей кнопки «Редактировать» и «Удалить» недоступны для нажатия.

- Для учетных записей, не являющихся автоматическими, доступна кнопка создания сертификата (при наведении курсора на данную кнопку отображается всплывающее окно «Создать сертификат») с возможностью создания сертификата:
  - с закрытым ключем (PKCS#12);
  - на ключевом носителе.
- Для автоматических учетных записей кнопка создания сертификата должна быть недоступна для нажатия.

Вход под учётной записью пользователя на сервер осуществляется при помощи сертификата, выпущенного с использованием шаблона «User». Подробнее о настройке аутентификации для входа в учётную запись см. раздел 5 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 eCA-RA;
- успешное обновление маркера доступа, включая его обновление в eCA-RA.


eCA-CA автоматически блокирует учётные записи пользователей с ролью «Оператор», период пассивности которых превысил значение, указанное в параметре `block_inactive_account_delay`<sup>1</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>2</sup> конфигурационного файла.

**Внимание!** При обновлении ПО до версии 2.4 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.

**Внимание!** Действия с учётными записями могут быть ограничены параметром `ldap_accounts_status_sync_enabled` конфигурационного файла.

### 8.5.1 Создание учётной записи пользователя локального ресурса

Порядок создания учётной записи для пользователя eCA-CA:

- На панели слева выберите раздел «Учётные записи» .
- Нажмите кнопку **Создать +** (см. Рисунок 97).
- В открывшемся окне выполните следующие действия (см. Рисунок 98):
  - выберите роль учётной записи;
  - укажите имя, которое отображается на верхней панели веб-интерфейса после авторизации пользователя;
  - логин – имя учётной записи (данные для поля «Common Name» при выпуске сертификата пользователя).

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

<sup>1</sup> По умолчанию в данном параметре указано значение «0», обозначающее отсутствие ограничения на неактивность пользователей.

<sup>2</sup> По умолчанию – каждую полночь.

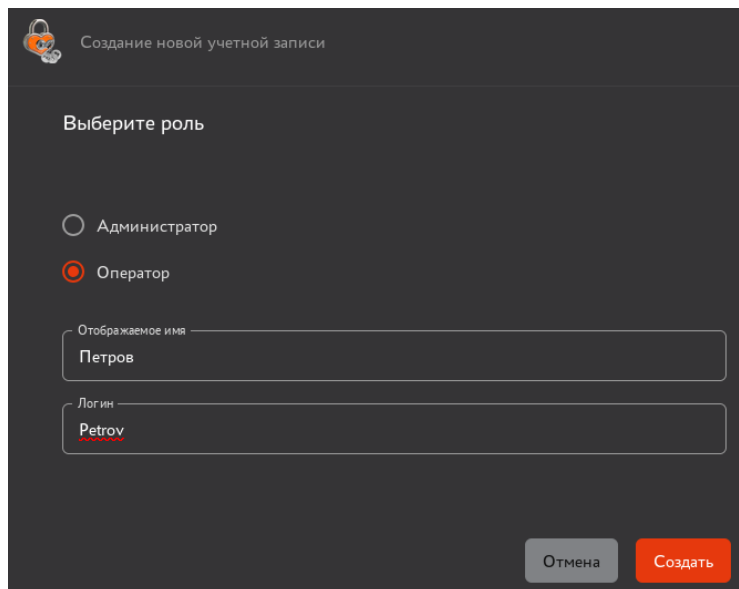


Рисунок 98 – Окно создания новой учётной записи локального пользователя

- Нажмите кнопку **Создать**.

Для созданной учётной записи пользователя с ролью «Оператор» создайте правила доступа шаблонам и субъектам (см. раздел 8.5.5).

Для созданной учётной записи пользователя с ролью «Администратора» настройка прав не требуется, так как ограничений для этой роли не будет.

### 8.5.2 Создание учётной записи для подключённого субъекта

Для создания учётной записи доменного пользователя перейдите в раздел «Субъекты» и создайте учётную запись в соответствии с разделом 8.7.6 настоящего руководства.

### 8.5.3 Изменение статуса учётной записи

При наведении курсора на строку с данными выбранной учётной записи отображаются инструменты управления учётной записью (возможность управления статусом текущей учётной записи) (см. Рисунок 99):

- 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.

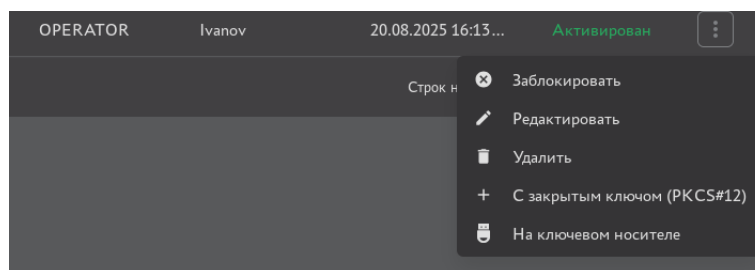
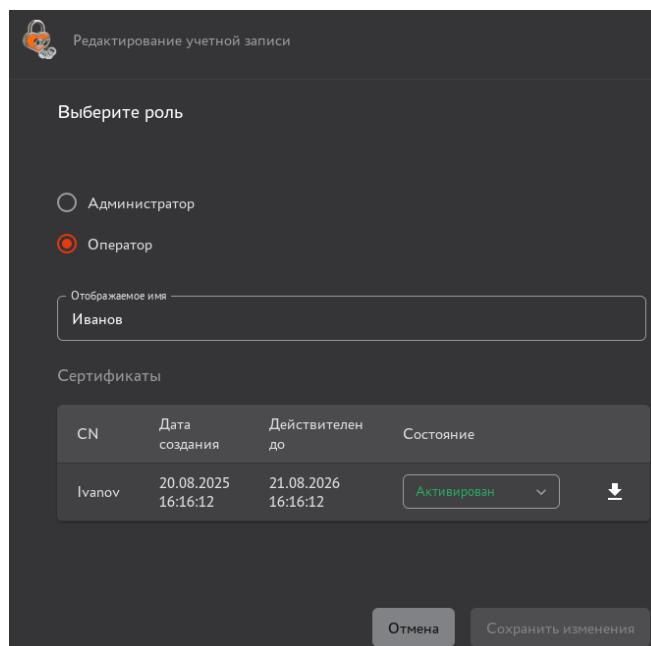


Рисунок 99 – Доступные действия над учётными записями

### 8.5.4 Редактирование учётной записи

По нажатию на кнопку **<Редактировать>**  (в строке учётной записи) открывается карточка учётной записи, содержащая следующие поля (см. Рисунок 100):



Редактирование учетной записи

Выберите роль

☐ Администратор

☒ Оператор

Отображаемое имя

Иванов

Сертификаты

CN	Дата создания	Действителен до	Состояние
Ivanov	20.08.2025 16:16:12	21.08.2026 16:16:12	Активирован

Отмена Сохранить изменения

Рисунок 100 – Окно редактирование учётной записи

- 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 таблице 13), а также кнопку скачивания сертификата в формате .pem.

Переход в карточку связанного сертификата возможен по нажатию на строку выбранного сертификата в карточке учётной записи.

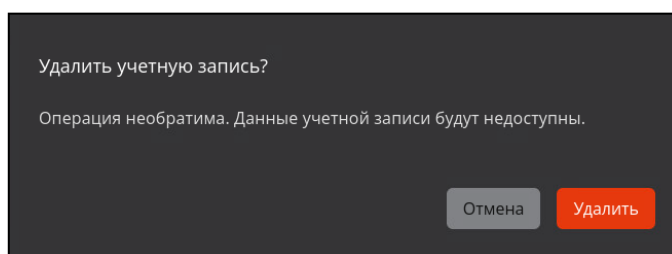
Карточка учётной записи, которая в текущий момент авторизована, доступна только для просмотра.

### 8.5.5 Назначение прав оператору

Для назначения прав оператору перейдите в раздел «Правила доступа» и произведите назначение прав в соответствии с разделом 8.6 настоящего руководства.

### 8.5.6 Удаление учётной записи

По нажатию на кнопку **<Удалить>**  (в строке учётной записи) открывается окно подтверждения удаления учётной записи (см. Рисунок 101)




Удалить учетную запись?

Операция необратима. Данные учетной записи будут недоступны.

Отмена Удалить

Рисунок 101 – Окно подтверждения удаления учётной записи

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

### 8.5.7 Выпуск сертификата для учётной записи

По нажатию на кнопку **<Создать сертификат>**  (в строке учётной записи) в выпадающем меню выберите способ выпуска (см. Рисунок 102):

- с закрытым ключом;
- на ключевом носителе.

Сертификат будет создан с использованием выбранного шаблона. Значение поля «Common Name», будет заполнено автоматически и соответствовать логину учётной записи, для которой выпускается сертификат.

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

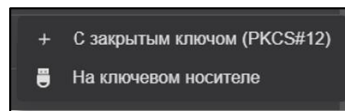


Рисунок 102 – Раздел «Учётные записи». Кнопка выпуска сертификата

### 8.6 Управление правилами доступа

Пользователи с ролью «Администратор» имеют возможность при помощи правил доступа предоставлять пользователям с ролью «Оператор» и группам безопасности зарегистрированных ресурсных систем<sup>1</sup> доступ:

- к шаблонам сертификатов. Доступные операции с шаблонами: просмотр и использование шаблонов при создании сертификатов для субъектов;
- только к сертификатам субъектов. Доступные операции с сертификатами субъектов: создание, просмотр, управление статусом, публикация в домен. Доступные операции с субъектами: просмотр;
- к субъектам и их сертификатам. Доступные операции с локальными субъектами: создание, просмотр, редактирование, удаление. Доступные операции с внешними субъектами: просмотр, редактирование не загружаемых из домена атрибутов. Доступные операции с сертификатами субъектов: создание, просмотр, управление статусом, публикация в домен.

Доступ по правилу, в котором субъектом доступа является группа безопасности, не наследуется для её дочерних групп.

Управление правилами доступа осуществляется в разделе «Правила доступа».

Раздел «Правила доступа» доступен только пользователям с ролью «Администратор».

Переход в раздел «Правила доступа» осуществляется через боковое меню, расположенное слева на главном экране (см. Рисунок 43).

В данном разделе отображаются все существующие правила доступа (см. Рисунок 103).

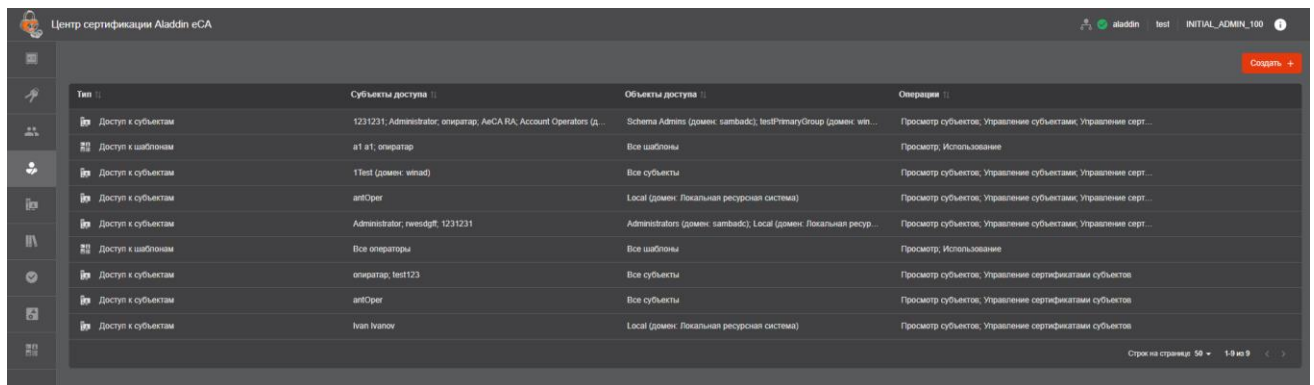


Рисунок 103 – Экран раздела меню «Правила доступа»

<sup>1</sup> Назначение правил доступа группам безопасности зарегистрированных ресурсных систем предназначено для наследования данных правил операторами, учётные записи которых созданы на основе субъектов данных групп безопасности.

## 8.6.1 Создание правила доступа

Для создания правила доступа:

1. Перейдите в раздел «Правила доступа» и нажмите кнопку «Создать».
2. На шаге 1 мастера создания правила доступа выберите тип правила доступа «Доступ к шаблонам», «Доступ только к сертификатам субъектов» или «Доступ к субъектам и их сертификатам» (см. рисунок 104) и нажмите кнопку «Продолжить».

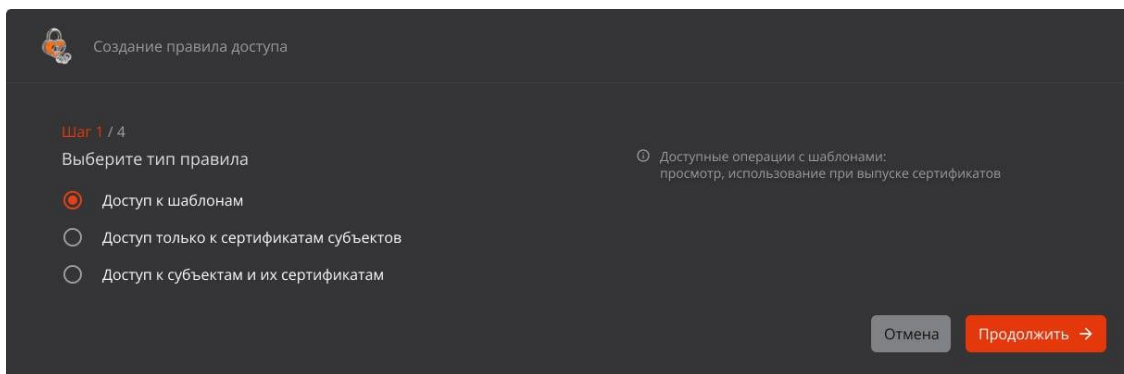


Рисунок 104 – Окно «Создание правила доступа». Шаг 1

3. На шаге 2 окна мастера создания правила доступа выберите субъектов доступа: «Все операторы» или «Выбрать операторов или группы».
4. Если выбрана опция «Выбрать операторов или группы»:
  - 4.1. В выпадающем списке поля «Тип» выберите тип: «Операторы» (см. рисунок 105) или «Группы» (см. рисунок 106).
  - 4.2. Перенесите субъекты доступа в правый столбец («Выбрано») путём нажатия на стрелку вправо.

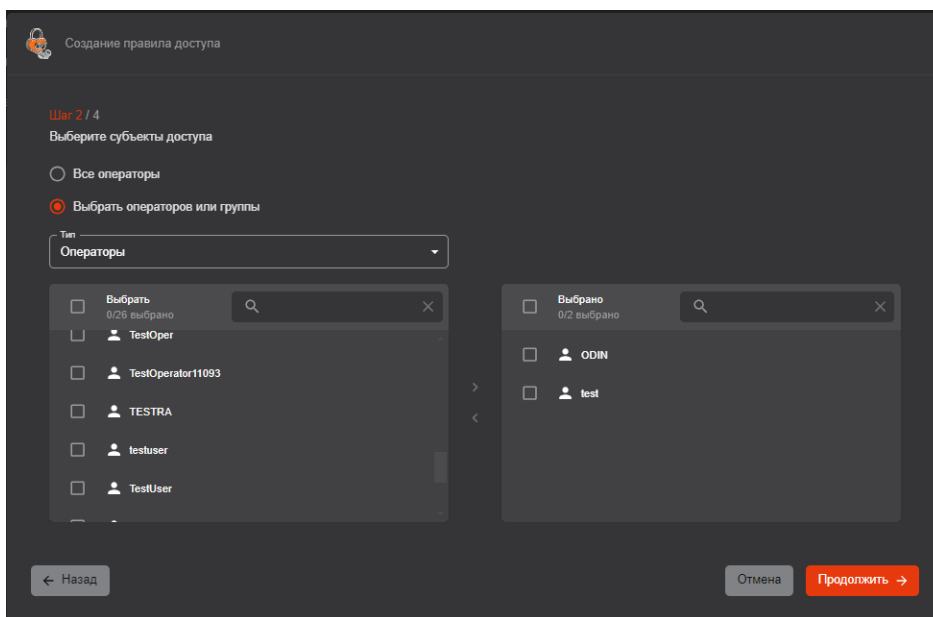


Рисунок 105 – Окно «Создание правила доступа». Шаг 2. Операторы

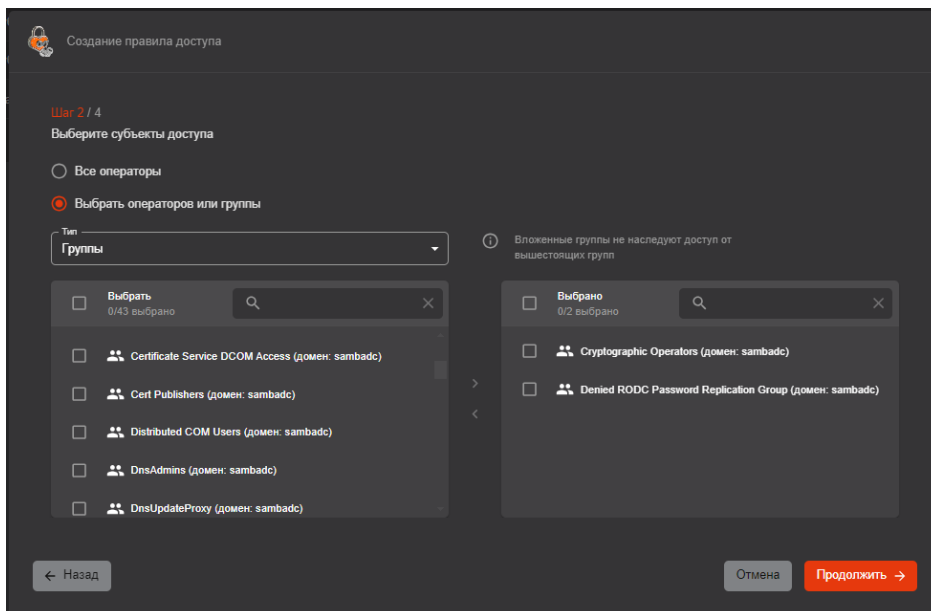


Рисунок 106 – Окно «Создание правила доступа». Шаг 2. Группы

5. Нажмите кнопку «Продолжить».
6. На шаге 3 мастера создания правила доступа выберите объекты доступа:
  - 6.1. Если на шаге 1 был выбран тип «Доступ к шаблонам», то выберите «Выбрать шаблоны» или «Все шаблоны».
  - 6.2. Если выбрано «Выбрать шаблоны», то необходимые шаблоны перенесите в правый столбец («Выбрано») путём нажатия на стрелку вправо (см. рисунок 107).

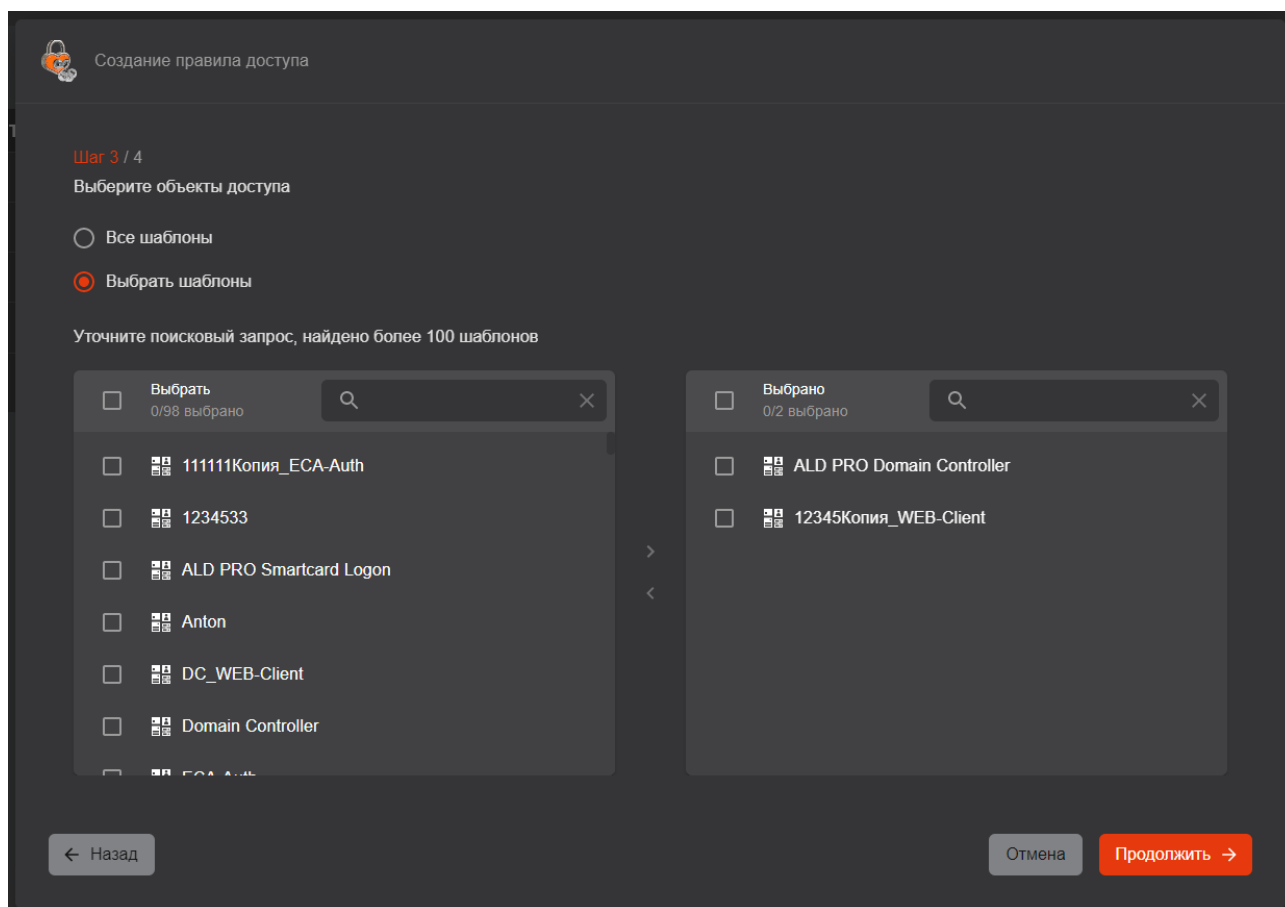


Рисунок 107 – Окно «Создание правила доступа». Шаг 3. Выбор шаблонов

- 6.3. Если на шаге 1 мастера создания правила доступа был выбран тип «Доступ к субъектам и их сертификатам», то выберите «Все субъекты» или «Выбрать группы».
- 6.4. Если выбрано «Выбрать группы»:

6.4.1. В выпадающем списке поля «Домен» выберите домен (см. рисунок 108) или локальную ресурсную систему (см. рисунок 109).

6.4.2. Перенесите объекты доступа в правый столбец («Выбрано») путём нажатия на стрелку вправо.

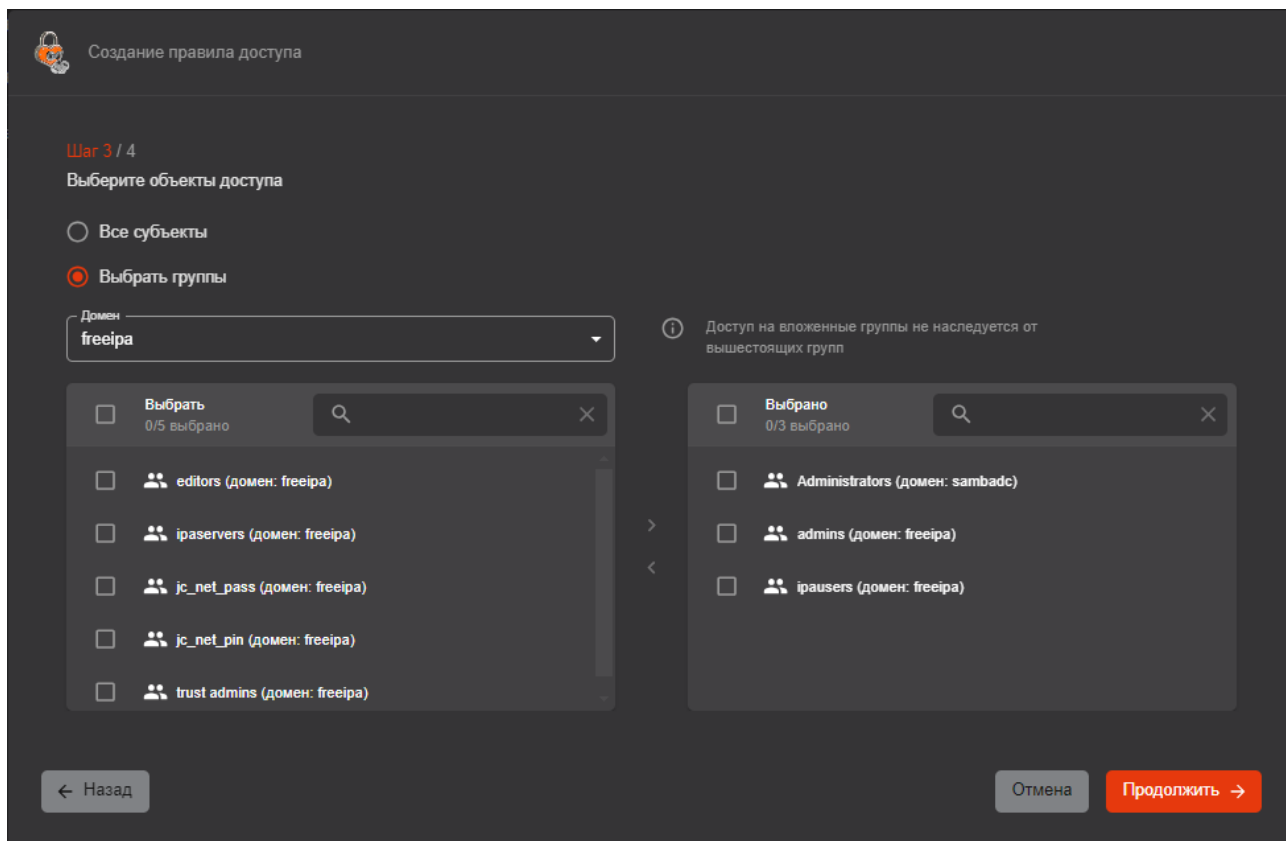


Рисунок 108 – Окно «Создание правила доступа». Шаг 3. Выбор групп. Домен

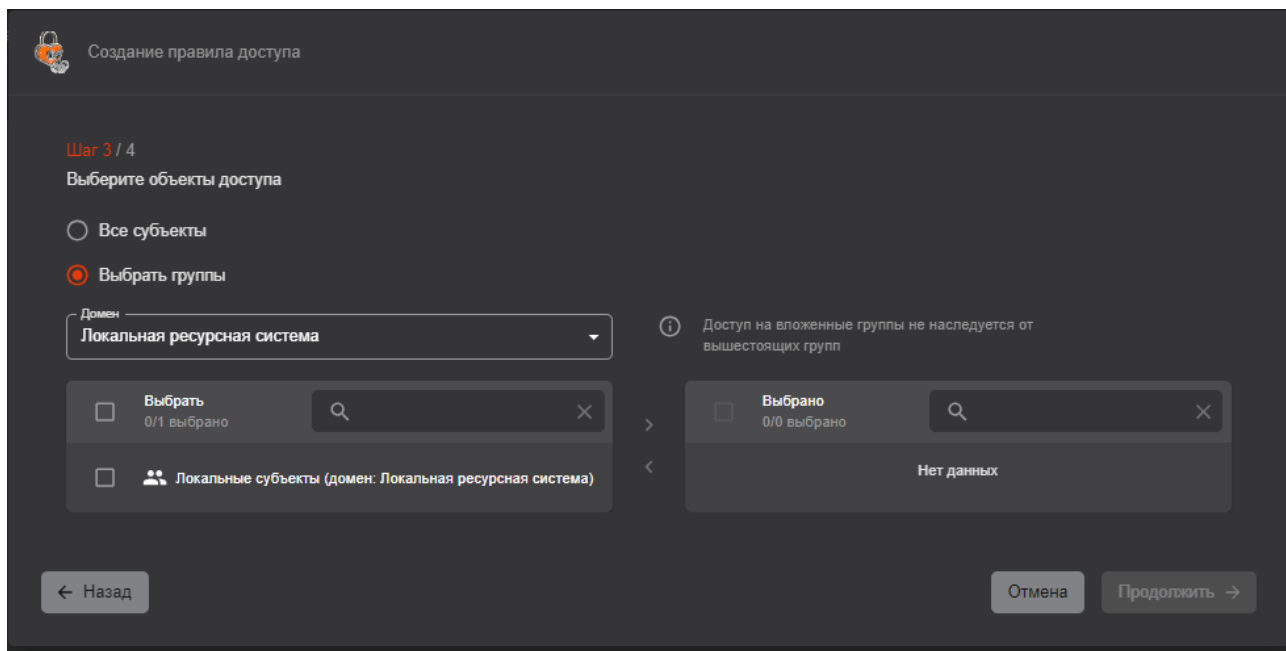


Рисунок 109 – Окно «Создание правила доступа». Шаг 3. Выбор групп. Локальная ресурсная система

7. Нажмите кнопку «Продолжить».
8. На шаге 4 мастера создания правила доступа ознакомьтесь с информацией о создаваемом правиле доступа и нажмите кнопку «Создать правило» (см. рисунок 110).

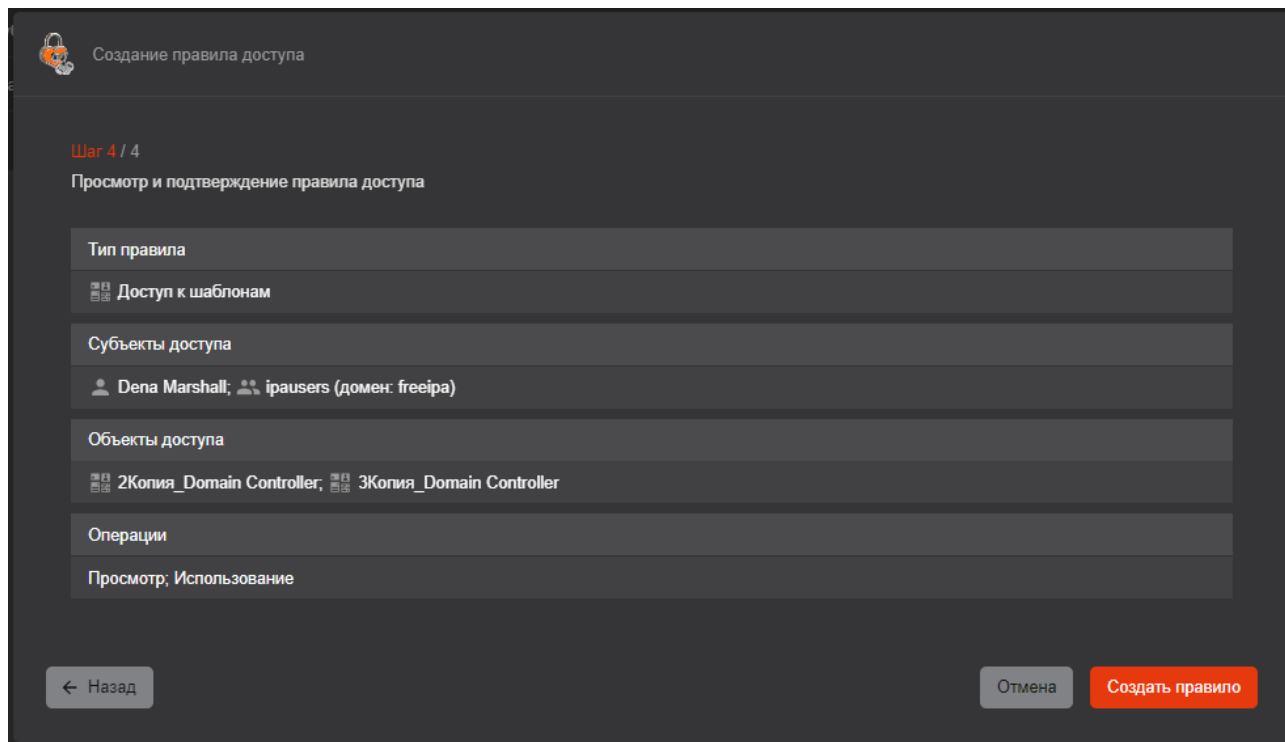



Рисунок 110 – Окно «Создание правила доступа». Шаг 4. Подтверждение

Созданное правило будет отображаться в списке правил доступа на вкладке «Правила доступа».

## 8.6.2 Редактирование правила доступа

Для редактирования правила доступа:

1. Перейдите в раздел «Правила доступа» и нажмите на кнопку «Редактировать»  в строке правила доступа, которое необходимо отредактировать.
2. В мастере редактирования правила доступа отредактируйте параметры правила аналогично их выбору в ходе создания правила (см. 8.6.1).<sup>1</sup>
3. В окне шага 3 мастера редактирования правила доступа (см. рисунок 111) ознакомьтесь с изменёнными параметрами и нажмите кнопку «Сохранить изменения».

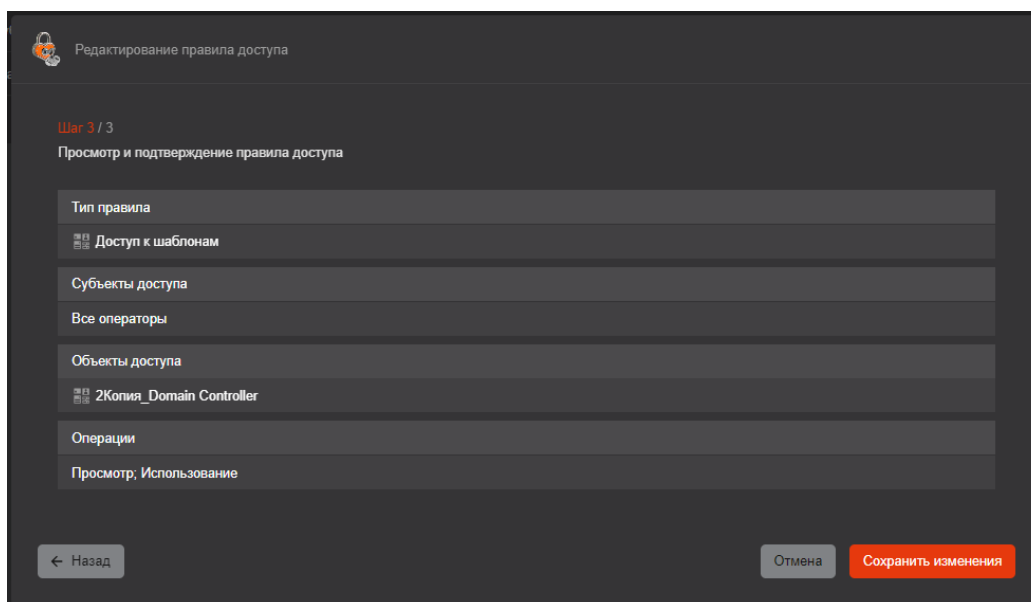



Рисунок 111 – Окно «Редактирование правила доступа». Шаг 3

<sup>1</sup> Редактирование типа правила недоступно.

### 8.6.3 Удаление правила доступа

Для удаления правила доступа:

1. Перейдите в раздел «Правила доступа» и нажмите на кнопку «Удалить»  в строке правила доступа, которое необходимо удалить.
2. В окне подтверждения удаления правила доступа (см. рисунок 112) ознакомьтесь с значением полей удаляемого правила доступа и подтвердите действие нажатием на кнопку «Удалить».

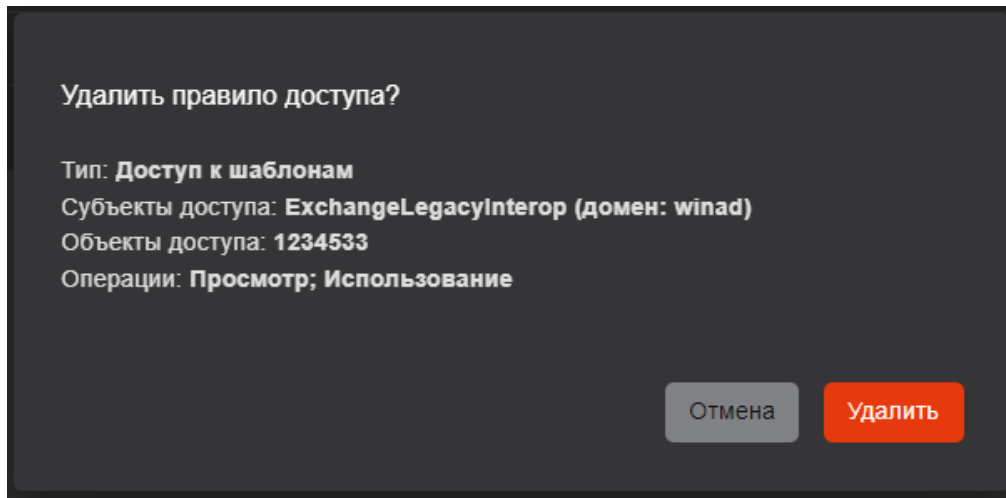


Рисунок 112 – Окно подтверждения удаления правила доступа

### 8.7 Управление субъектами доступа

Раздел «Субъекты» предоставляет доступ к операциям с подключёнными к ресурсной системе и локальными субъектами. Раздел отображается пользователям с ролью «Администратор» или «Оператор».

Для учётной записи с ролью «Оператор» в разделе «Субъекты» доступны только те субъекты, к которым ей прямо или косвенно предоставлены полномочия в соответствии с текущими правилами доступа (см. 8.6).

В разделе доступны следующие операции с субъектами:

- просмотр списка субъектов ресурсных систем с возможностью выбора ресурсной системы и группы безопасности внутри неё;
- создание локального субъекта;
- переход в карточку субъекта при нажатии на субъект в списке;
- просмотр и редактирование атрибутов субъектов в их карточках;
- поиск субъекта по имени (части имени) в разделе «Субъекты»;
- создание учётной записи пользователя Центра сертификации для субъекта;
- создание сертификата для субъекта;
- просмотр списка сертификатов, созданных для субъекта, а также основные сведения о данных сертификатах: поля «Серийный номер», «CN», «Шаблон», «Дата создания», «Действителен до», «Опубликован в ресурсную систему», «Состояние».
- управление состоянием сертификатов субъекта в карточке субъекта (отзыв, приостановка, активация);
- публикация сертификата субъекта в ресурсную систему в карточке субъекта (только для подключённых к ресурсной системе субъектов);
- экспорт сертификата субъекта;
- переход в карточку сертификата из карточки субъекта.

Переход в раздел «Субъекты» осуществляется через боковое меню, расположенное слева на главном экране (см. рисунок 113).

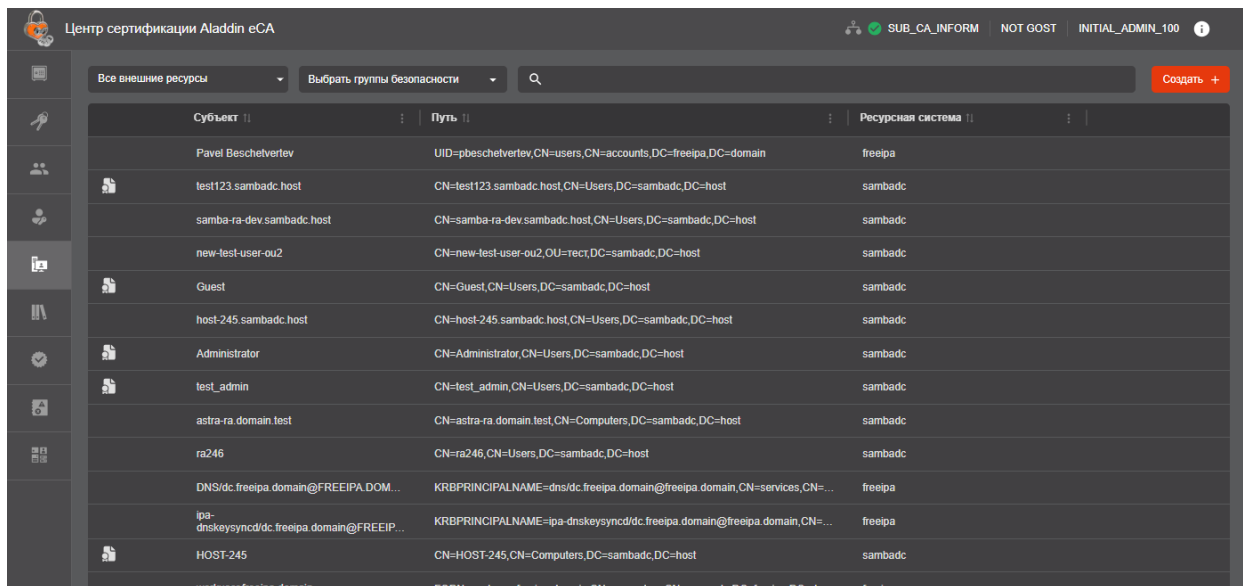


Рисунок 113 – Экран раздела «Субъекты»

### 8.7.1 Фильтрация субъектов ресурсных систем

Для уточнения состава отображаемых субъектов воспользуйтесь элементами фильтрации (см. рисунок 114):

- В поле «Ресурсная система» в выпадающем меню выберите локальную ресурсную систему, подключённый ресурс или все внешние ресурсы.
- В поле «Выбрать группы безопасности» в выпадающем меню выберите необходимую группу. Если группа безопасности не выбрана, то будут отображены все субъекты выбранного источника. В данном поле отображаются только группы безопасности, в которых в ресурсной системе присутствуют субъекты. Для отображения субъектов, не входящих в группы безопасности, укажите значение «Без группы безопасности».
- Для поиска субъекта введите текст в поисковую строку . Поиск осуществляется по вхождению текста, в значения атрибутов субъекта в его карточке и в путь субъекта.

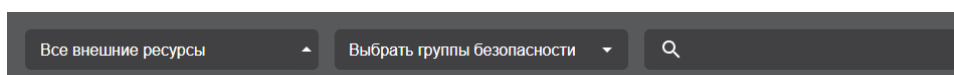


Рисунок 114 – Верхняя панель экранной формы вкладки «Субъекты»

### 8.7.2 Карточка субъекта

Переход к экрану «Карточка субъекта» осуществляется при нажатии на строку субъекта главного экрана раздела «Субъекты» (см. Рисунок 113).

#### 8.7.2.1 Карточка субъекта, подключённого к ресурсной системе

В окне карточки субъекта (см. рисунки 115 и 116) доступны следующие элементы:

- Имя субъекта (в формате «Субъект name», где «name» - значение атрибута «Common name» данного субъекта<sup>1</sup>);
  - Кнопки:
    - «Создать учётную запись»<sup>2</sup>;
    - «Создать сертификат»;
    - Кнопка изменения параметра отображения атрибутов («Атрибуты со значениями» или «Все атрибуты»);

<sup>1</sup> При наличии нескольких значений в атрибуте «Common name» представляет собой строку, состоящую из всех значений данного атрибута, разделённых нижним подчёркиванием.

<sup>2</sup> Доступно только пользователю с ролью «Администратор».

- Список «Сведения о субъекте», содержащий следующие строки в формате «ключ – значение»:
  - Ресурсная система;
  - Статус в ресурсной системе;
  - Идентификатор;
  - SID. Данное поле должно отображаться только при наличии у субъекта значения атрибута «SID»<sup>1</sup>;
- Список «Атрибуты», содержащий следующие строки в формате «ключ – значение»:
  - Common name;
  - Unique Identifier (UID);
  - Email Address (E);
  - Serial number;
  - Given name;
  - Initials;
  - Surname;
  - Organizational unit;
  - Organization;
  - Locality;
  - State or province;
  - Domain component;
  - Country;
  - Unstructured address;
  - Unstructured name;
  - Postalcode;
  - Business category;
  - Telephone number;
  - Pseudonym;
  - Postal address;
  - Street;
  - Name;
  - Title;
  - Domain Qualifier;
  - Description;
  - Role;
  - Дата рождения;
  - Место рождения;
  - ИНН;
  - ОГРН;
  - ОГРНИП;
  - СНИЛС;
  - ИНН ЮЛ;
  - MS GUID, Globally Unique Identifier;
  - RFC 822 NAME;
  - MS UPN, UserPrincipalName;
  - DNS Name;
  - IP address;
  - Directory Name;
  - Uniform resource identifier;

<sup>1</sup> Атрибут «SID» могут иметь только субъекты, полученные из ресурсных систем «MS AD», «SambaDC», «РЕД АДМ», «Альт Домен».

- Registered identifier;
- Kerberos KPN, Kerberos 5 Principal;
- Permanent identifier;
- Xmpp address;
- Service Name;
- Subject Identification Method;
- Список «Сертификаты», содержащий следующие поля:
  - Серийный номер;
  - CN;
  - Шаблон;
  - Дата создания;
  - Действителен до;
  - Статус сертификата;
  - Опубликован в ресурсную систему;
  - Элементы управления:
    - Изменение состояния сертификата (приостановка, отзыв, активация).
    - Публикация в ресурсную систему;
    - Экспорт сертификата;
    - Переход в карточку сертификата при нажатии на сертификат в списке.

← Субъекты

Субъект Dena Marshall

Создать учетную запись

Создать сертификат

Все атрибуты

Сведения о субъекте

Ресурсная система	winad
Статус пользователя в ресурсной системе	Активен
Идентификатор	000000a6-d0c3-4a4e-aea6-be5ad83a3ba2
SID	S-1-5-21-2383553880-3503761536-1682916708-2615

Атрибуты

ИНН		
ИНН ЮП		
ОГРН		
ОГРНИП		
СНИЛС		
Business category		
Common name	Dena Marshall	
Country		
Description		
Domain component		
Domain qualifier	CN=Dena Marshall,OU=created-users,DC=winad,DC=local	
Email Address (E)	Thenterage87@test.local, DenaMMarshall@superrito.com	
Given name	Dena	
Initials		
Locality		
Name	Dena Marshall	
Organization	org	
Organizational unit		
Postal address		
Postal code		
Pseudonym		
Serial number		
State or province		
Street		
Surname	Marshall	
Telephone number		
Title		
Unique Identifier (UID)		
Unstructured address		
Unstructured name		
Directory Name		
DNS Name	Dena123	
IP address		
Kerberos KPN, Kerberos 5 Principal Name	text@text	
MS GUID, Globally Unique Identifier	Ad35FdBe23654ADCaFd3AC65EdFfa213	
MS UPN, User Principal Name	Thenterage87@test.local	
Permanent identifier		
Registered Identifier (OID)		
RFC 822 Name	Thenterage87@test.local, DenaMMarshall@superrito.com	
Service Name		
Subject Identification Method		
Uniform resource identifier		
Xmpp address		

Сертификаты

Серийный номер	CN	Шабло...	Дата создания	Действ... до	Опубликован в ресурсную систему	Состояние
53fd7a3ef4e950f83203...	Dena Marshall	Smartcard Logon	29.10.2024 15:37:45	29.10.2026 15:37:45	19.11.2024 17:07:08	Отозван
7b0f69dd4500f3fd103...	Dena Marshall	Smartcard Logon	28.10.2024 15:28:38	28.10.2026 15:28:38	19.11.2024 17:25:53	Отозван
10d269569294fbc90c6...	Dena Marshall	Smartcard Logon	30.10.2024 10:16:05	30.10.2026 10:16:05		Отозван
3f63e1b5bd294c43125...	Dena Marshall	Smartcard Logon	29.10.2024 16:46:45	29.10.2026 16:46:45		Отозван

Рисунок 115 — Окно «Карточка субъекта» для субъекта, подключённого к ресурсной системе

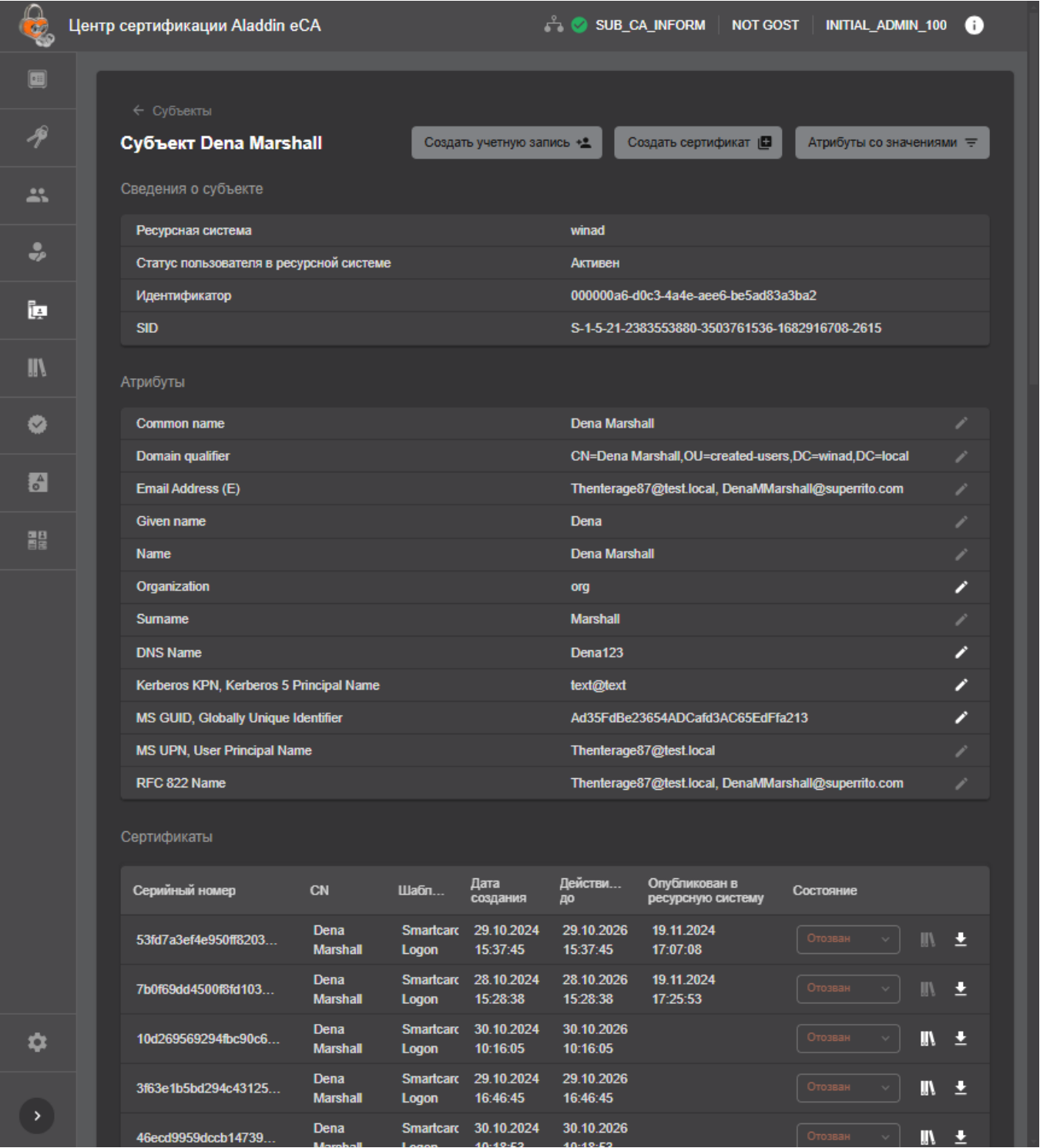


Рисунок 116 — Окно «Карточка субъекта» для субъекта, подключённого к ресурсной системе (включено отображение атрибутов «Атрибуты со значениями»)

8.7.2.2 Карточка локального субъекта

В окне карточки субъекта (см. рисунок 117) доступны следующие элементы:

- Имя субъекта (в формате «Субъект name», где «name» - значение атрибута «Common name» данного субъекта<sup>1</sup>);
- Кнопки — соответствую кнопкам карточки подключённого к ресурсной системе субъекта (см. 8.7.2.1).

<sup>1</sup> При наличии нескольких значений в атрибуте «Common name» должно представлять собой строку, состоящую из всех значений данного атрибута, разделенных нижним подчеркиванием.

- Список «Сведения о субъекте», содержащий следующие строки в формате «ключ – значение»:
  - Ресурсной система (значение всегда «Локальная ресурсная система»);
  - Статус в ресурсной системе (значение всегда отсутствует);
  - Идентификатор;
  - SID. Данное поле должно отображаться только при наличии у субъекта значения атрибута «SID»<sup>1</sup>;
- Список «Атрибуты» — соответствует списку «Атрибуты» карточки подключённого к ресурсной системе субъекта (см. 8.7.2.1).
- Список «Сертификаты» — соответствует списку «Сертификаты» карточки подключённого к ресурсной системе субъекта (см. 8.7.2.1).

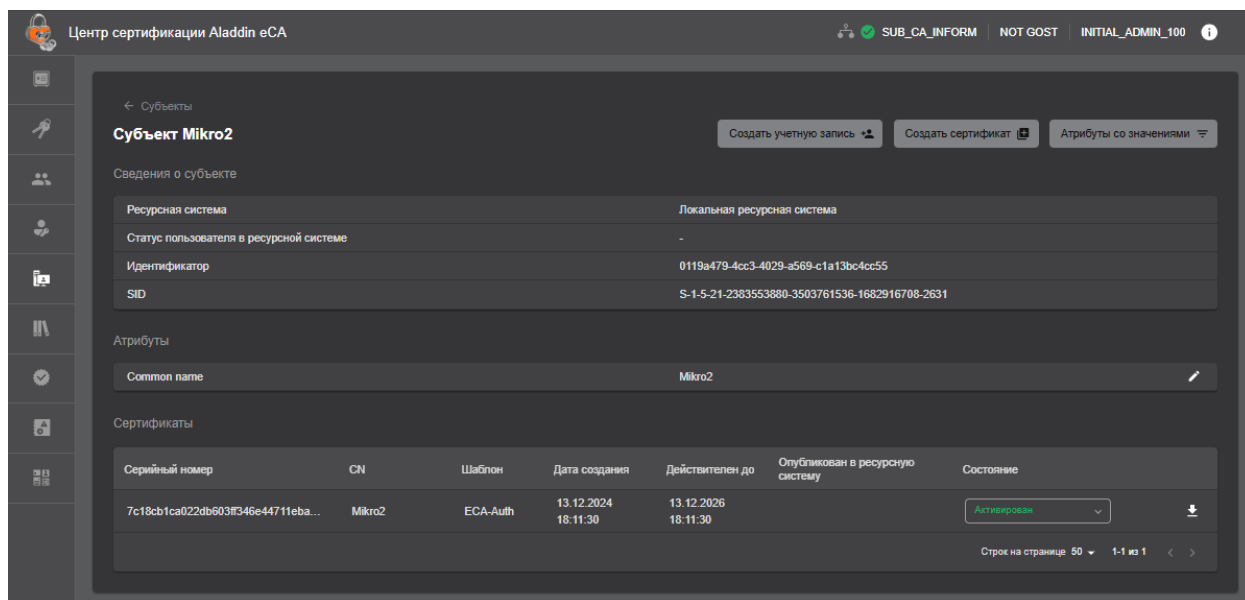


Рисунок 117 —Окно «Карточка субъекта» для локального субъекта

### 8.7.2.3 Редактирование атрибутов субъекта

На карточке субъекта для всех полей в списке «Атрибуты», кроме получаемых Центром сертификации из ресурсной системы, доступен элемент вызова диалогового окна редактирования значения атрибутов<sup>2</sup> (пиктограмма «Карандаш»).

При редактировании атрибутов осуществляется валидация введенных значений (см. таблицу 14).


Таблица 14 – Допустимые значения атрибутов

Поле	Правило валидации
Country	Допустимые символы: "A"-"Z", "a"-"z". Длина значения должна составлять 2 символа.
Domain qualifier	Допустимые символы: "A"-"Z", "a"-"z", "0"-"9", "", "(", ")", "+", ",", "-", ".", "/", ":", "=", "?", пробел.
Email Address (E)	Допустимые символы: "A"-"Z", "a"-"z", "A"-"Я", "a"-"я", "0"-"9", ".", "@", "_", "-". Формат значения: "text@text".
Serial number	Допустимые символы: "A"-"Z", "a"-"z", "0"-"9", "", "(", ")", "+", ",", "-", ".", "/", ":", "=", "?", пробел.
RFC 822 Name	Допустимые символы: "A"-"Z", "a"-"z", "A"-"Я", "a"-"я", "0"-"9", ".", "@", "_", "-". Формат значения: "text@text".
DNS Name	Допустимые символы: "A"-"Z", "a"-"z", "A"-"Я", "a"-"я", "0"-"9", "-", ".", "**".
IP address	Допустимые символы: "A"-"F", "a"-"f", "0"-"9", ".", ":".


<sup>1</sup> Атрибут «SID» имеют только субъекты, полученные из ресурсных систем «MS AD», «SambaDC», «ПЕД АДМ», «Алът Домен».

<sup>2</sup> Доступно для пользователя с ролью «Администратор» и «Оператор», только если оператору предоставлены полномочия на управление субъектом. Если у оператора нет полномочий на управление субъектом, пиктограмма «Карандаш» для всех полей в списке «Атрибуты» неактивна.

Поле	Правило валидации
	Формат значения: IPv4-адрес или IPv6-адрес.
Directory Name	Формат значения: последовательность идентификаторов относительных отличительных имён (RDN) и их значений, отделённых запятой или запятой с пробелом (например, O=organization, OU=Department, L=City, DC=Component, C=RU...). Допускается использование следующих идентификаторов RDN: EMAILADDRESS, CN, UID, SERIALNUMBER, OU, O, L, ST, C, T, SURNAME, STREET, INITIALS, GIVENNAME, DC, UNSTRUCTUREDADDRESS, UNSTRUCTUREDNAME, POSTALCODE, BUSINESSCATEGORY, TELEPHONENUMBER, PSEUDONYM, POSTALADDRESS, NAME, DN, DESCRIPTION. В качестве идентификатора RDN допускается указание OID (формат OID должен соответствовать рекомендации ITU X.660).
Registered Identifier (OID)	Допустимые символы: "0"-"9", ".", "-". Формат значения: OID в соответствии с рекомендацией ITU X.660.
MS UPN, User Principal Name	Допустимые символы: "A"-"Z", "a"-"z", "A"-"Я", "a"-"я", "0"-"9", ".", "@", "_", "-", "/". Формат значения: "text@text".
MS GUID, Globally Unique Identifier	Допустимые символы: "A"-"F", "a"-"f", "0"-"9". Длина значения должна составлять 32 символа.
Kerberos KPN, Kerberos 5 Principal Name	Допустимые символы: "A"-"Z", "a"-"z", "A"-"Я", "a"-"я", "0"-"9", ".", "@", "_", "-", "/". Формат значения: "text@text".
Permanent Identifier	Формат значения: "value/OID", где "value" – любая последовательность символов, а "OID" – OID в соответствии с рекомендацией ITU X.660. Допускается отсутствие значения "text", например, "/1.2.2.3.4.5".
Xmpp address	Допустимые символы: "A"-"Z", "a"-"z", "A"-"Я", "a"-"я", "0"-"9", ".", "@", "_", "-", "/". Формат значения: "text@text".
Subject Identification Method	Формат значения: "OID::text::text", где "OID" – OID в соответствии с рекомендацией ITU X.660, а "text" – любая последовательность символов.
Дата рождения	Формат значения: дата в формате «DD.MM.YYYY».
ИНН	Допустимые символы: "0"-"9". Длина значения должна составлять 12 или 14 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 или 14 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 118).

- 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<sup>1</sup> 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!

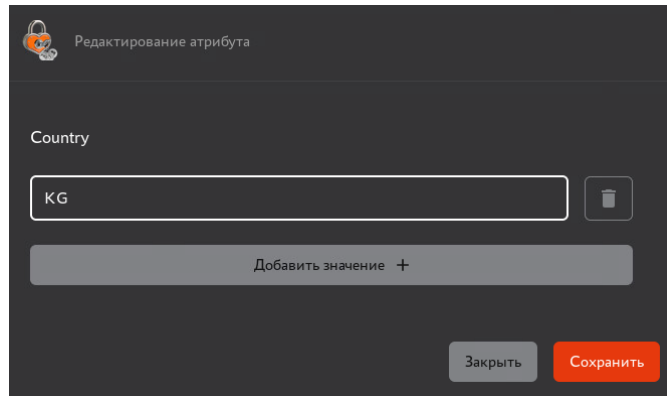


Рисунок 118 — Окно редактирования значения атрибута в карточке субъекта

### 8.7.3 Субъекты локальной ресурсной системы

Локальную базу субъектов формируют:

- субъекты, созданные Администратором при помощи REST API или UI;
- субъекты отключенной ресурсной системы (удалённой ранее зарегистрированной ресурсной системы). 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 eCA-CA при подключении ресурсной системы, но отсутствующие в списке субъектов, полученном по результатам выполнения полной синхронизации ресурсной системы. Атрибут субъекта «isBlocked» принимает значение «false».

Локальный субъект отключенной ресурсной системы при подключении ресурсной системы, где существует данный субъект, будет перенесён из базы локальной ресурсной системы (атрибут субъекта «isConnected» примет значение «true»). При этом будет выполнено обновление атрибутов субъекта в соответствии с его атрибутами из ресурсной системы, остальные текущие атрибуты (то есть те, которые не были получены из ресурсной системы) не изменятся.


Проверка субъектов осуществляется по атрибуту «id».

#### 8.7.3.1 Создание нового субъекта локальной ресурсной системы

Создание локального субъекта доступно пользователю с ролью:

- «Администратор»;
- «Оператор», если оператору предоставлены полномочия на управление субъектами для локальной ресурсной системы. Только при помощи REST API.

Для создания нового локального субъекта:

1. Нажмите кнопку «Создать»  (см. рисунок 113).
2. В окне «Создание субъекта» (см. рисунок 119):
  - 2.1. Введите имя создаваемого субъекта (CN).
  - 2.2. Для добавления прочих атрибутов SDN и SAN:
    - 2.2.1. Нажмите кнопку «Добавить атрибут +» и выберите атрибуты в списке возможных атрибутов (см. рисунок 120).

<sup>1</sup> Для субъекта, подключённого к ресурсной системе, данное поведение существует в случае, когда у субъекта в ресурсной системе отсутствует поле CN.

2.2.2. Укажите значения выбранным атрибутам или удалите атрибуты, нажав кнопку «Удалить» .

3. Нажмите кнопку «Создать субъект».

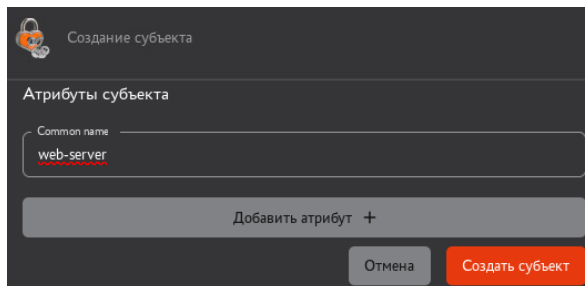


Рисунок 119 – Окно «Создание субъекта»

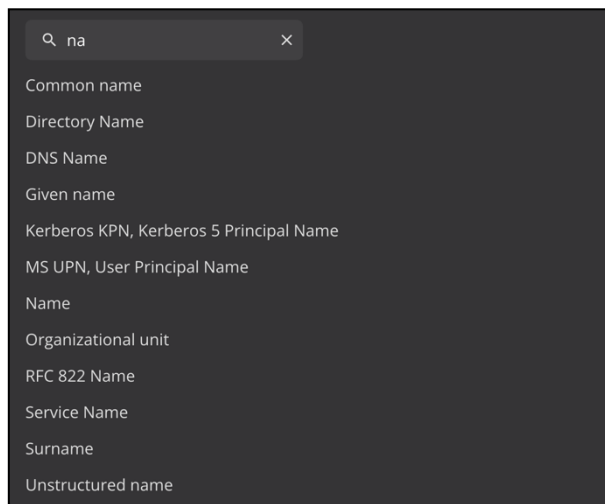


Рисунок 120 – Добавление атрибута субъекта

#### 8.7.4 Субъекты внешнего ресурса

Внешний (подключенный) ресурс формируется в результате регистрации службы каталогов доменных служб Samba DC, РЕД АДМ, ALD PRO, FreeIPA, Dynamic Directory, Альт Домен или MS Active Directory.

Подключенный ресурс будет отображён только после регистрации ресурсной системы на вкладке «Ресурсная система» (см. раздел 8.8.1 настоящего руководства).

Обновление списков и данных субъектов ресурсной системы происходит по правилам, приведённым в разделе 8.8.3 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 121).

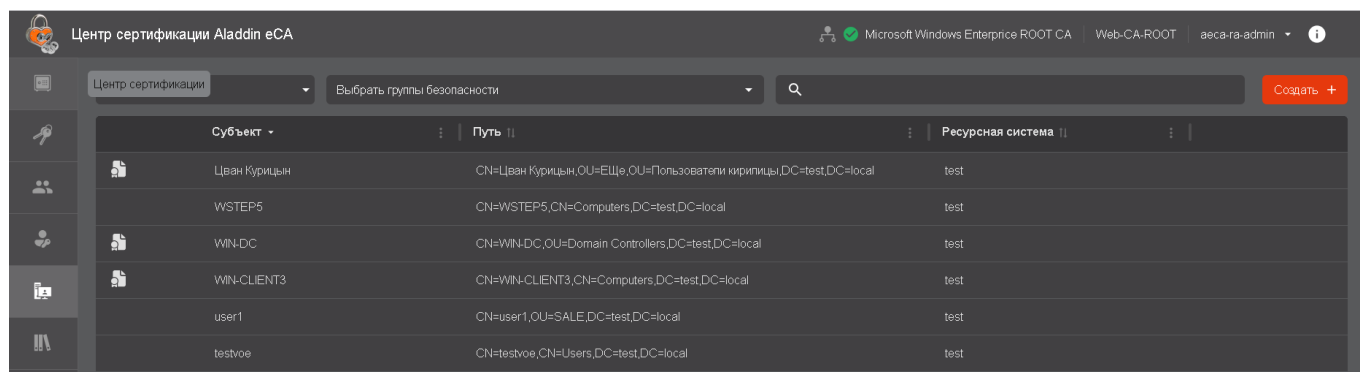



Рисунок 121 – Экран раздела меню «Субъекты». Подключенный ресурс

Загрузка данных осуществляется из всей ресурсной системы, начиная с точки подключения, указанной в настройках подключения Корневого каталога.

Для каждого полученного из ресурсной системы пользователя и компьютера или сервиса будет создан (обновлён) субъект и загружены его атрибуты. Управление правилами сопоставления атрибутов осуществляется администратором в разделе «Настройки» на вкладке «Синхронизация с ресурсными системами» (см. 8.14).

Идентификация подключённых субъектов в Центре сертификации осуществляется по атрибуту `Id`.

### 8.7.5 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 122):

- 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»).

**Внимание!** 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.

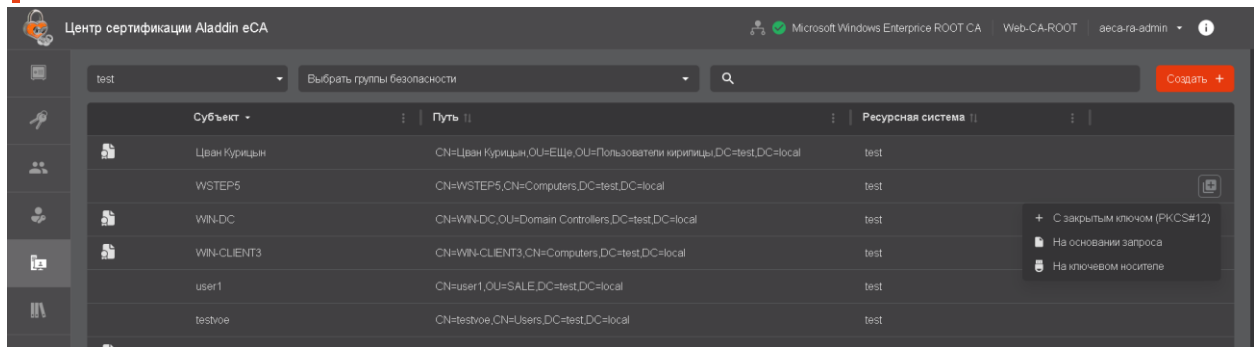


Рисунок 122 – Окно выпуска сертификата для субъекта ресурсной системы

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 чекбоксе «Публиковать сертификат в ресурсную систему» окна выпуска сертификата. По умолчанию флаг выполнения публикации сертификата включён.



После выбора шаблона субъекта ресурсной системы на следующем шаге поля автоматически заполняются данными субъекта.

Если значения атрибутов отсутствуют, то необходимо их ввести в соответствующие поля в карточке субъекта.

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

### 8.7.6 Создание учётной записи для субъекта

Для создания учётной записи для субъекта:

1. Перейдите в раздел «Субъекты» (см. рисунок 113). Нажмите кнопку «Создать учетную запись» в списке субъектов  или в карточке субъекта  **Создать учетную запись**.
2. В окне «Создание новой учетной записи»:
  - 2.1. Выберите роли создаваемой учётной записи: «Администратор» или «Оператор».
  - 2.2. Укажите отображаемое имя создаваемой учётной записи в поле «Отображаемое имя».<sup>1</sup>
  - 2.3. Укажите логин создаваемой учётной записи в поле «Логин».<sup>35</sup>
  - 2.4. Нажмите кнопку «Создать».

<sup>1</sup> По умолчанию в данном поле будет указано значение атрибута «Common name» субъекта, на основании которого создается учетная запись. При наличии нескольких значений в атрибуте «Common name» в поле «Отображаемое имя» по умолчанию будут указаны все значения в виде строки, где разделителем значений является нижнее подчеркивание («\_»).

Рисунок 123 – Окно создания новой учётной записи

Для созданной учётной записи с ролью «Оператор» произведите настройку прав доступа к группам и объектам ресурсной системы в соответствии с разделом 8.5.5 настоящего руководства<sup>1</sup>.

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

## 8.8 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 еСА-СА, может иметь несколько точек подключения.


Переход в раздел «Ресурсные системы» осуществляется через боковое меню, расположенное слева на главном экране (см. Рисунок 124).

На основном экране раздела «Ресурсные системы» отображены следующие информационные поля (см. Рисунок 124):

- имя домена – домен подключённой ресурсной системы;
- последнее обновление – дата и время последней синхронизации с базой субъектов ресурсной системы;
- статус – статус ресурсной системы, который назначается в соответствии с критериями, приведёнными в таблице 15.

Таблица 15 – 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:

<sup>1</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.

- полная синхронизация ресурсной системы (см. раздел 8.8.3.3);
- частичная синхронизация ресурсной системы (синхронизация точки подключения ресурсной системы) (см. раздел 8.8.3.4);
- удаление зарегистрированной ресурсной системы (см. Раздел 8.8.5);
- удаление точки подключения зарегистрированной ресурсной системы (см. раздел 8.8.6).

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».

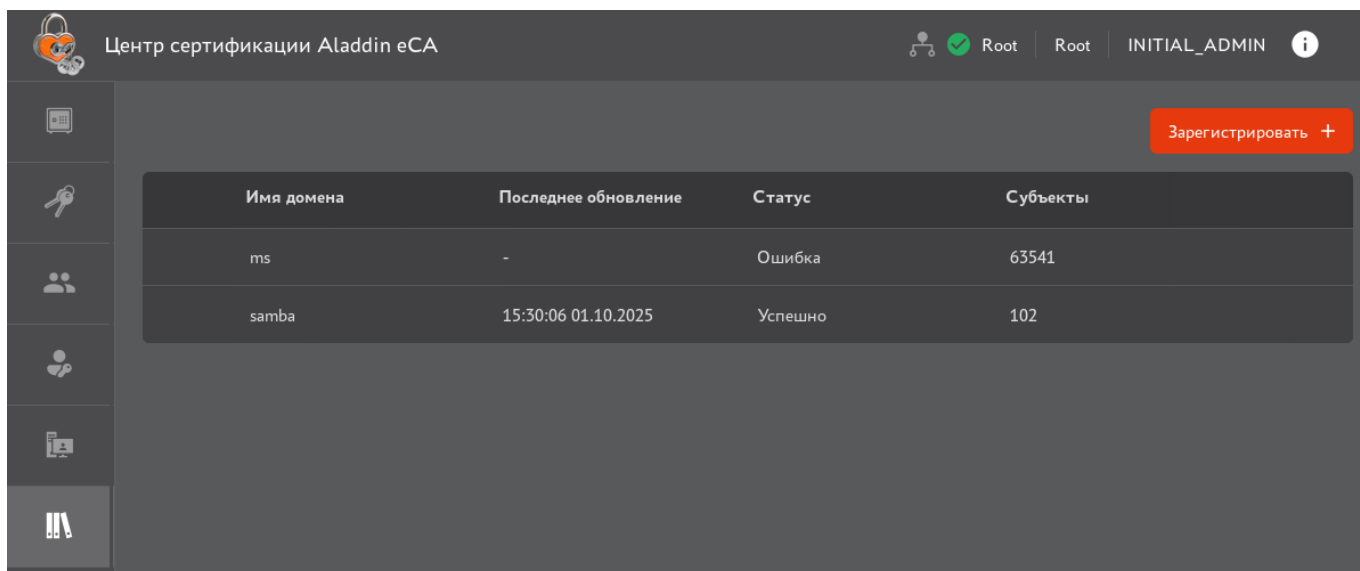


Рисунок 124 – Экран раздела «Ресурсные системы»

еCA-CA позволяет взаимодействовать с несколькими ресурсными системами: Samba DC, РЕД АДМ, MS AD, FreeIPA, Dynamic Directory, ALD PRO и Альт Домен:

- список субъектов (пользователей, компьютеров и сервисов (только для ALD PRO, Dynamic Directory 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 8.8.1);
- переход в карточку ресурсной системы (см. раздел 8.8.2);
- запуск полной синхронизации ресурсной системы (см. раздел 8.8.3.3);
- удаление зарегистрированной ресурсной системы (см. раздел 8.8.5).

### 8.8.1 Регистрация точки подключения

Для подключения ресурсной системы ALD PRO, Dynamic Directory или FreeIPA к еCA-CA необходимо предварительно создать роль на контроллере домена ALD Pro/FreeIPA со следующим 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 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 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).

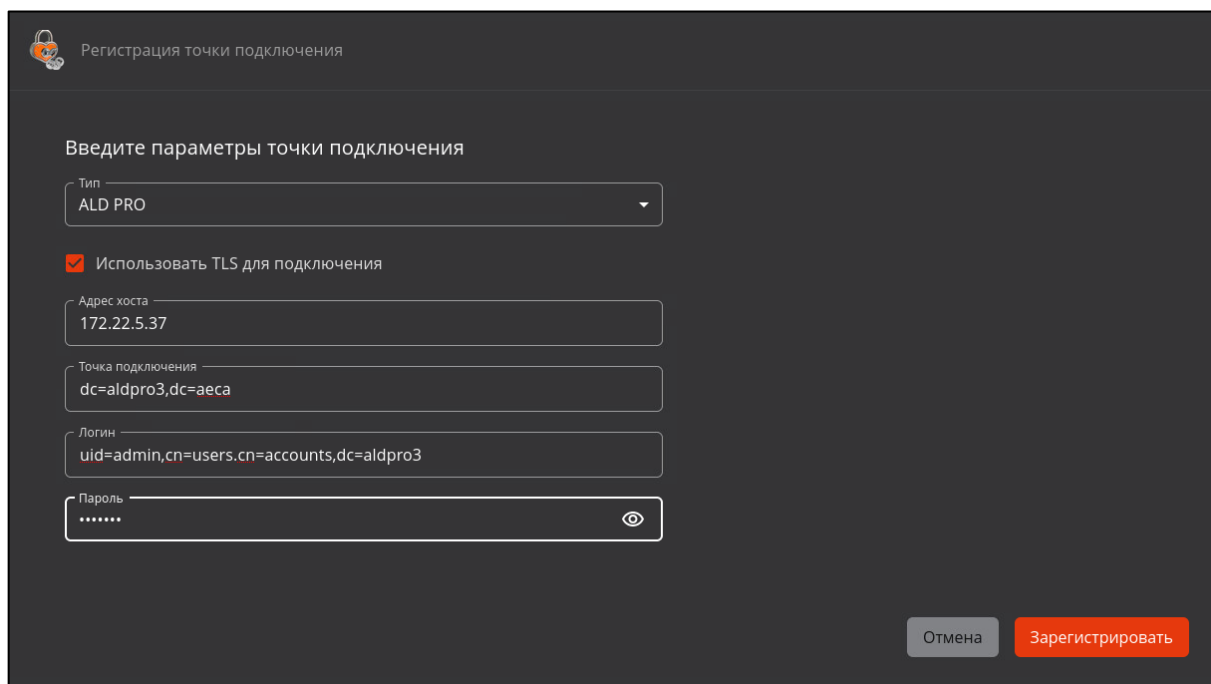
Порядок регистрации точки подключения:

- 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, Dynamic Directory, 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, Dynamic Directory 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 125, Рисунок 126, Рисунок 127, Рисунок 128, Рисунок 129, Рисунок 130).

- 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

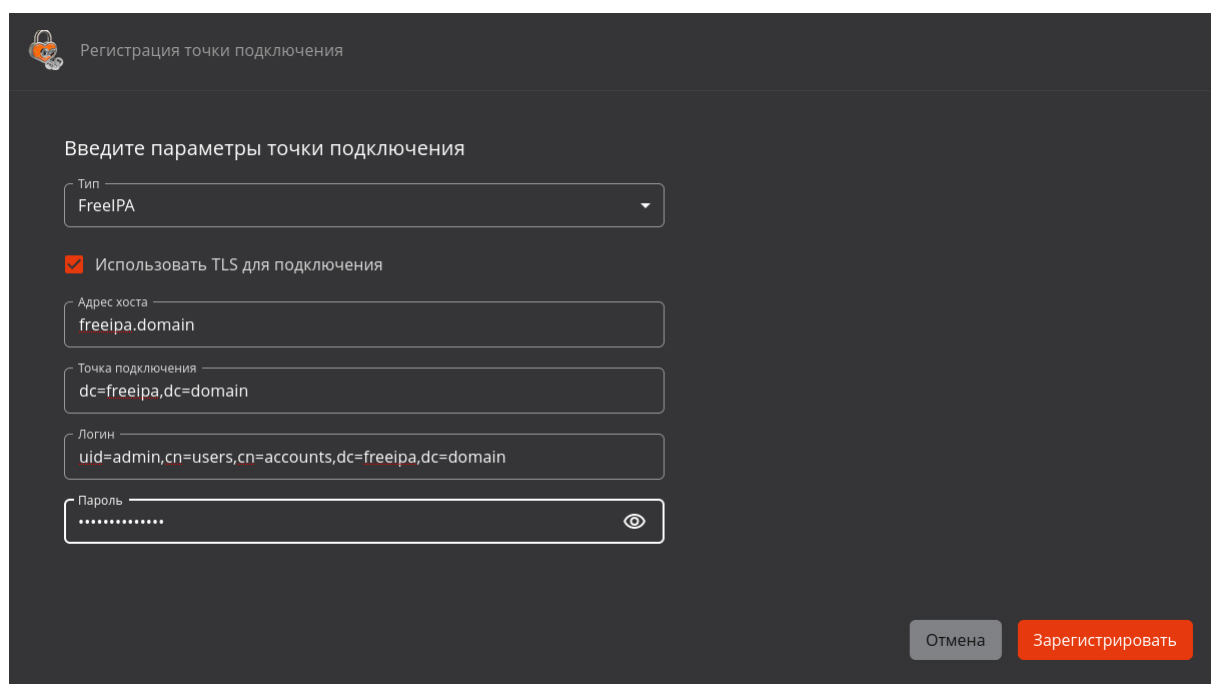
Точка подключения  
dc=aldpro3,dc=aeca

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

Пароль  
.....

Отмена Зарегистрировать

Рисунок 125 – Пример регистрации ресурсной системы ALD PRO



Регистрация точки подключения

Введите параметры точки подключения

Тип  
FreeIPA

☒ Использовать TLS для подключения

Адрес хоста  
freeipa.domain

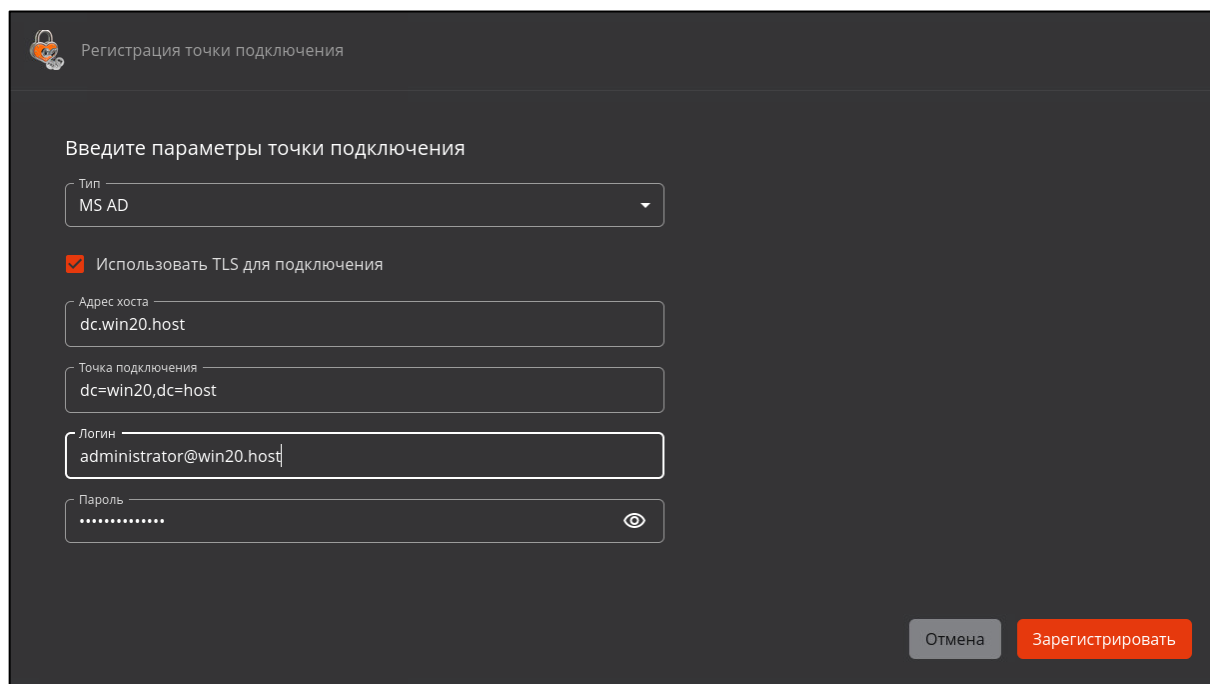
Точка подключения  
dc=freeipa,dc=domain

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

Пароль  
.....

Отмена Зарегистрировать

Рисунок 126 – Пример регистрации ресурсной системы FreeIPA



Регистрация точки подключения

Введите параметры точки подключения

Тип  
MS AD

☒ Использовать TLS для подключения

Адрес хоста  
dc.win20.host

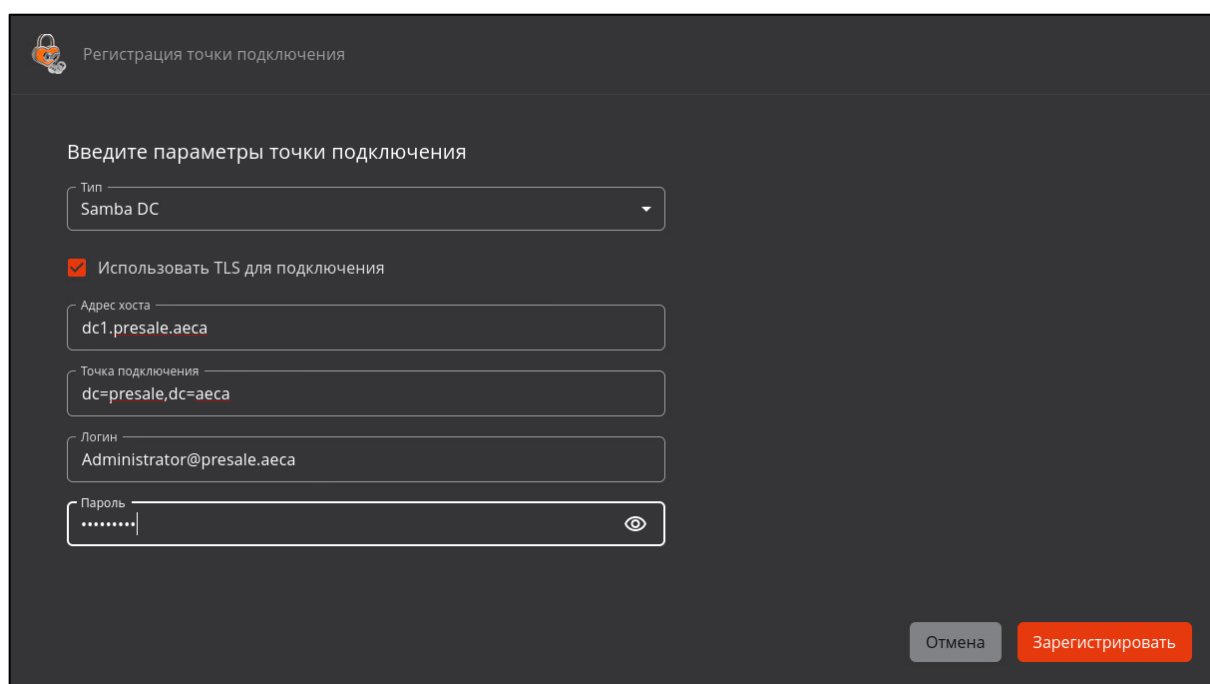
Точка подключения  
dc=win20,dc=host

Логин  
administrator@win20.host

Пароль  
.....

Отмена Зарегистрировать

Рисунок 127 – 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

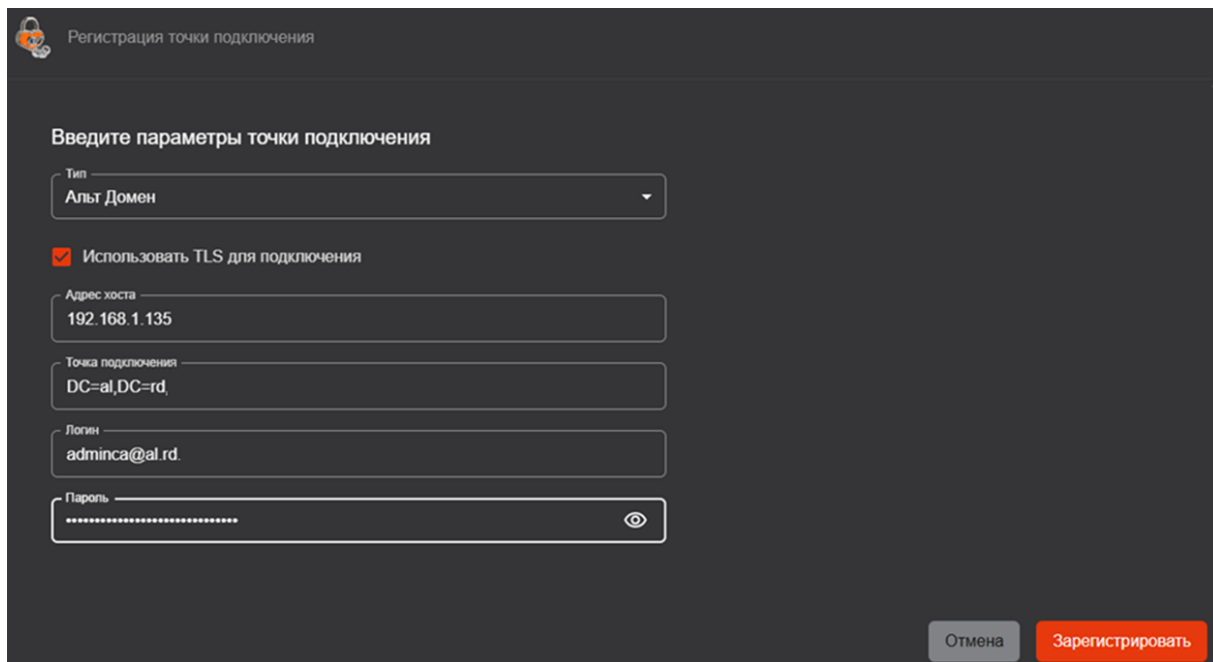
Точка подключения  
dc=presale,dc=aeca

Логин  
Administrator@presale.aeca

Пароль  
.....

Отмена Зарегистрировать

Рисунок 128 – 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

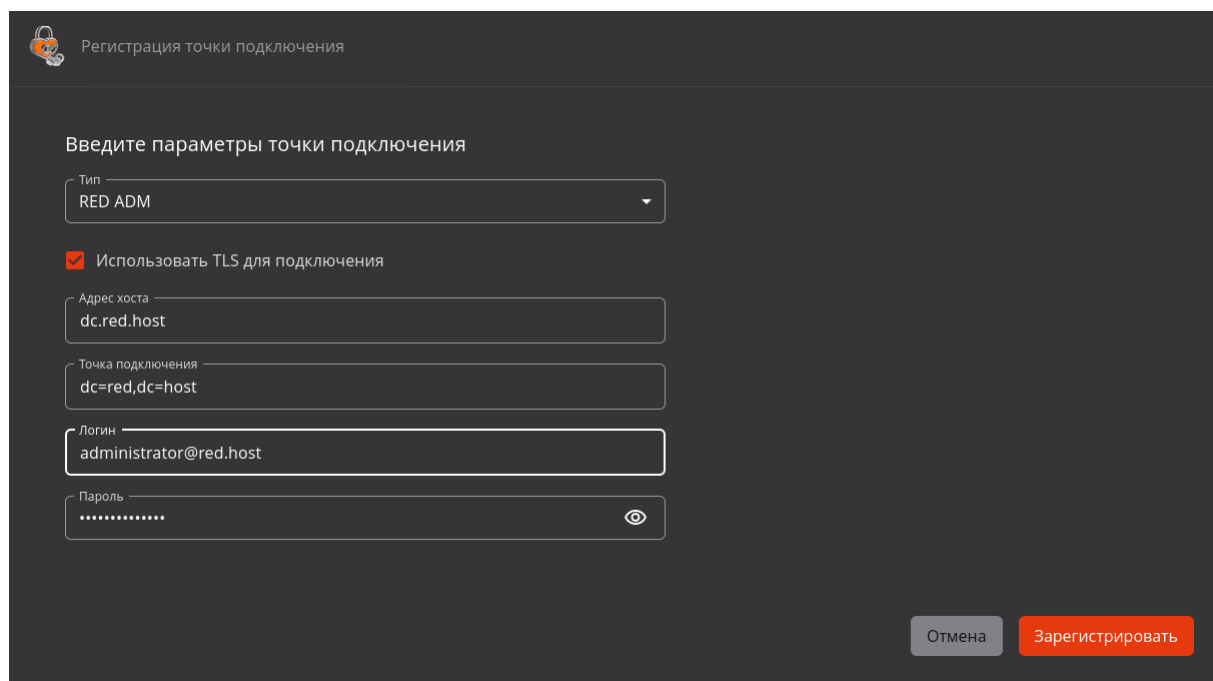
Точка подключения  
DC=al,DC=rd

Логин  
adminca@al.rd

Пароль  
.....

Отмена Зарегистрировать

Рисунок 129 – 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 130 – 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 131).

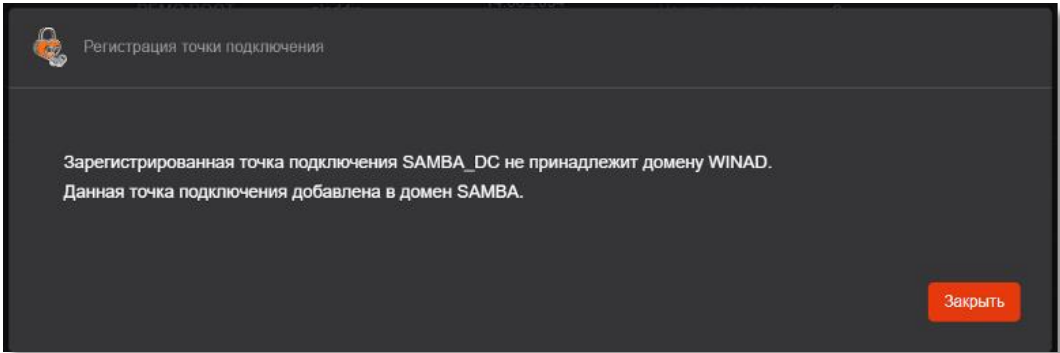


Рисунок 131 – Модальное окно с информацией о принадлежности регистрируемой точки подключения другой ресурсной системе

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

### 8.8.2 Карточка ресурсной системы

Просмотр информации о ресурсной системе возможен в её карточке. Переход к «Карточке ресурсной системы» (см. Рисунок 132) осуществляется при нажатии на строку ресурсной системы в разделе «Ресурсные системы» (см. Рисунок 124).

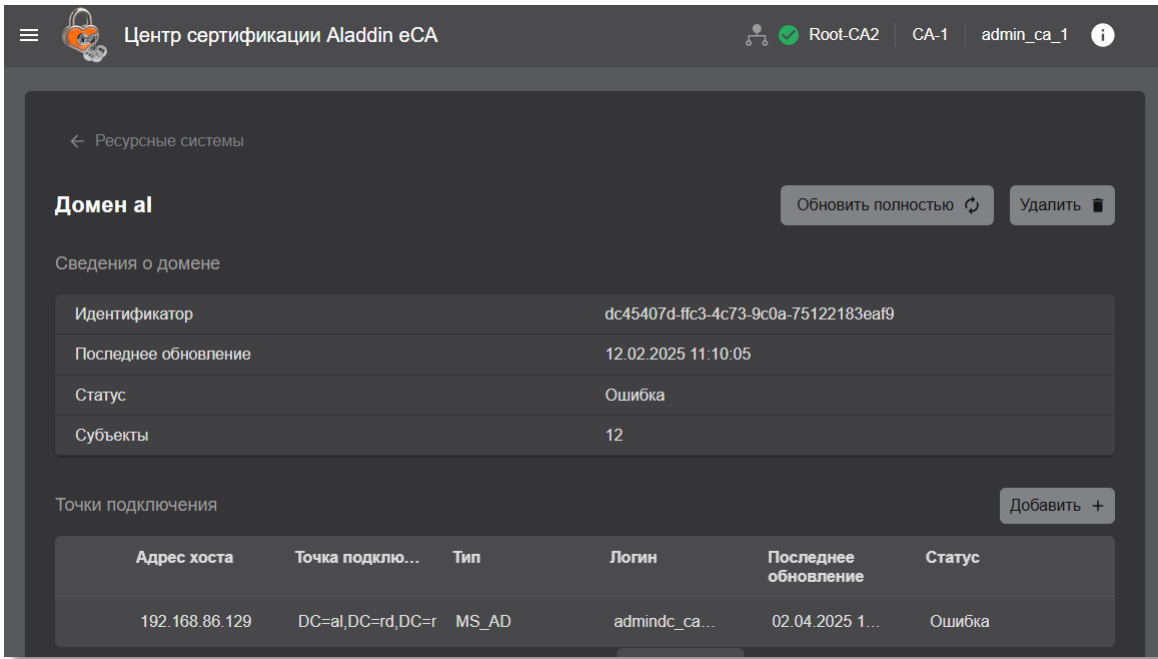


Рисунок 132 – Карточка ресурсной системы


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, приведёнными в таблице выше (Таблица 15);
- 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 своём DN-объекты, получаемые из точки подключения;

- тип – тип ресурсной системы: SambaDC, Альт домен, ALD PRO, MS\_AD, FreeIPA, Dynamic Directory, RED ADM.
- логин (имя) учётной записи администратора контроллера домена;
- дата и время последней попытки синхронизации точки подключения;
- статус точки подключения, который назначается в соответствии с критериями, приведёнными в таблице ниже (Таблица 16);

Таблица 16 – 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 8.8.3.4);
- удаление точки подключения зарегистрированной ресурсной системы (см. раздел 8.8.6).

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 8.8.3.3);
- удаление зарегистрированной ресурсной системы (см. Раздел 8.8.5);
- регистрация новой точки подключения к ресурсной системе (см. раздел 8.8.1);
- запуск частичной синхронизации точки подключения (см. раздел 8.8.3.4);
- изменение параметров, указанные при регистрации точки подключения (см. раздел 8.8.4);
- удаление точки подключения (см. раздел 8.8.6).

### 8.8.3 Синхронизация ресурсных систем

#### 8.8.3.1 Виды синхронизации ресурсных систем

еСА-СА поддерживает следующие виды синхронизации:

- Полная.  
Синхронизация списка субъектов (пользователей, компьютеров и сервисов (только для ALD PRO, Dynamic Directory 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.

**Внимание!** Субъекты ресурсной системы, которые не могут быть синхронизированы, будут отсутствовать в списке субъектов данной ресурсной системы.

Синхронизация ресурсной системы производится постранично<sup>1</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`.

### 8.8.3.2 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).
- Ручной режим синхронизации.  
В данном режиме запуск синхронизации выполняется по команде пользователя с ролью «Администратор»:
  - запуск полной синхронизации выбранных ресурсных систем (см. раздел 8.8.3.3).
  - запуск частичной синхронизации выбранных точек подключения к ресурсным системам (см. раздел 8.8.3.4)

### 8.8.3.3 Полная синхронизация ресурсной системы в ручном режиме

Запуск полной синхронизации ресурсной системы может осуществляться путём нажатия на кнопку **<Обновить>** для ресурсной системы в разделе «Ресурсные системы» (см. Рисунок 133) или путём нажатия на кнопку **<Обновить полностью>** в карточке ресурсной системы (см. Рисунок 132).

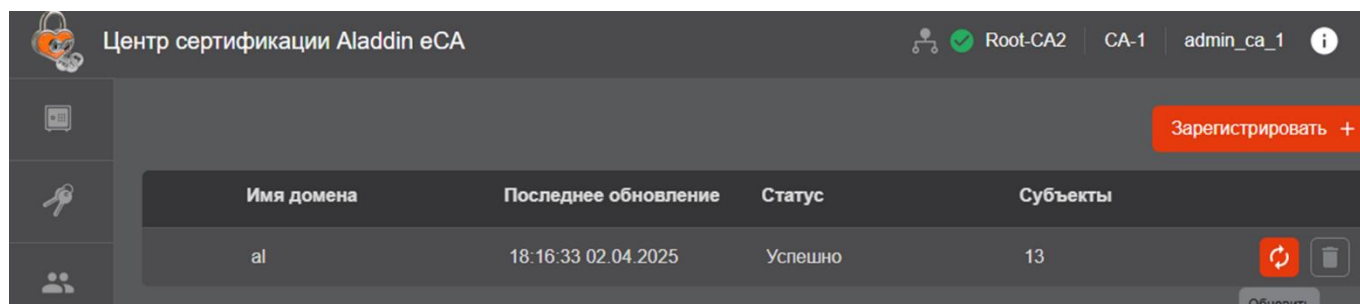


Рисунок 133 – Запуск полной синхронизации ресурсной системы из раздела «Ресурсные системы»

### 8.8.3.4 Частичная синхронизация точки подключения в ручном режиме

Запуск частичной синхронизации точки подключения осуществляется путём нажатия на кнопку **<Обновить>** для выбранной точки подключения в карточке ресурсной системы (см. Рисунок 134).

<sup>1</sup> еСА-СА получает данные из ресурсной системы частями, выполняя несколько запросов с ограничением на максимальное количество выдаваемых объектов вместо одного запроса на выгрузку сразу всех данных.

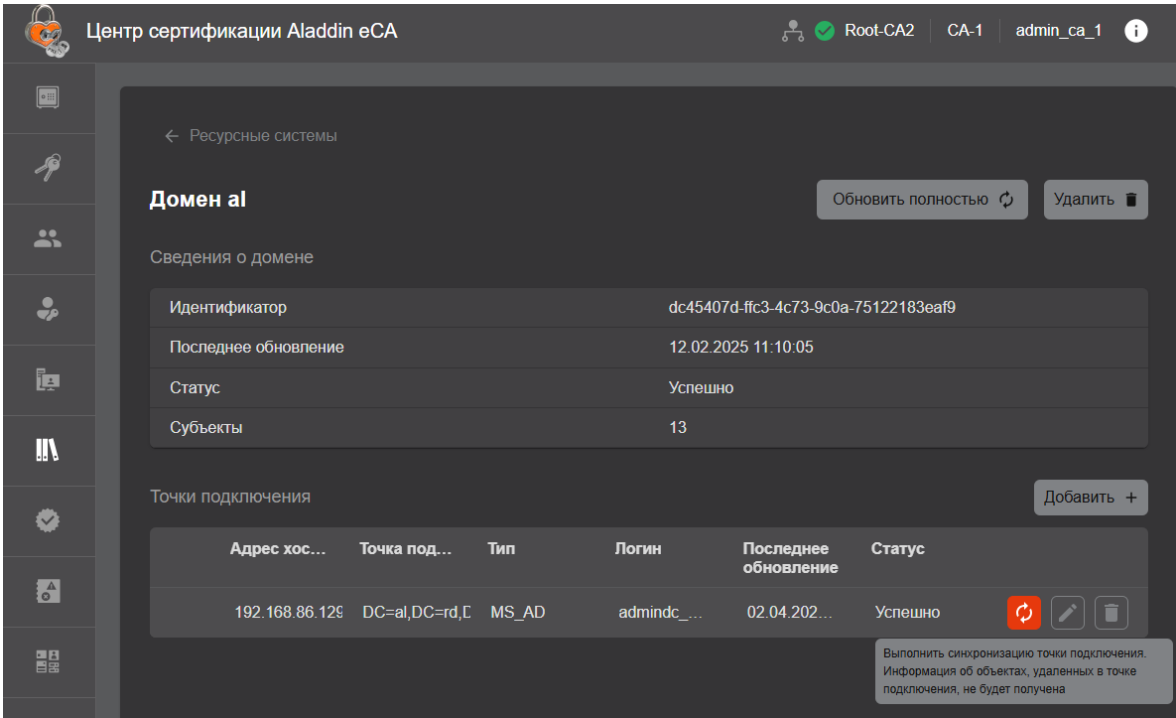



Рисунок 134 – Запуск частичной синхронизации точки подключения

### 8.8.4 Редактирование параметров точки подключения

Для редактирования параметров точки подключения необходимо в карточке ресурсной системы нажать на кнопку **<Редактировать>**  около точки подключения (см. Рисунок 135).

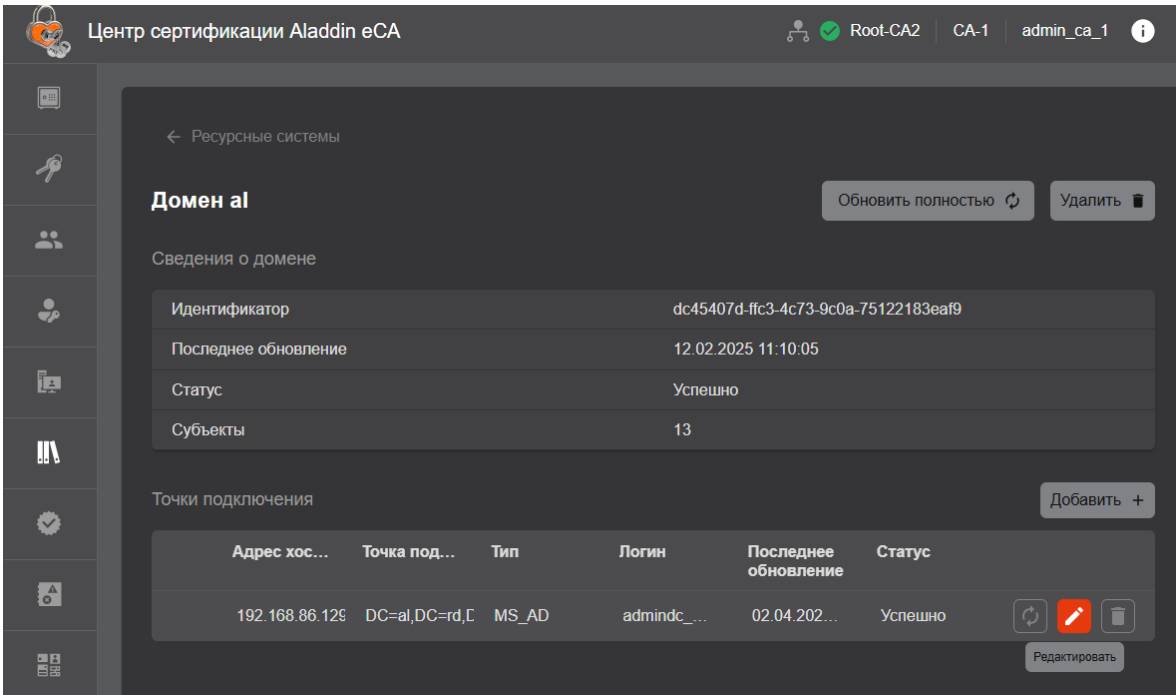


Рисунок 135 – Окно раздела «Ресурсная система». Кнопка редактирования РС

После этого открывается окно для редактирования полей, заполненных при создании точки подключения. Тип подключаемого ресурса изменить невозможно (см. Рисунок 136).

Рисунок 136 – Окно редактирования подключения к PC

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

### 8.8.5 Удаление зарегистрированной ресурсной системой

Порядок удаления ресурсной системы:

- Удаление ресурсной системы может осуществляться путем нажатия на кнопку **<Удалить>** для ресурсной системы в разделе «Ресурсные системы» (см. Рисунок 137) или путем нажатия на кнопку **<Удалить>** в карточке ресурсной системы (см. Рисунок 132).

Имя домена	Последнее обновление	Статус	Субъекты
al	09:30:00 03.04.2025	Успешно	13

Рисунок 137 – Удаление ресурсной системы из раздела «Ресурсные системы»

- После этого отобразится окно подтверждения выбранного действия (см. Рисунок 138).

Удалить домен sambadc?

Операторы, которым предоставлены права на группы, полученные из sambadc, потеряют свои полномочия.

Удалятся организационные единицы и группы безопасности, полученные из домена sambadc.

Субъекты, полученные из домена, будут переведены в локальную ресурсную систему.

Отмена Удалить

Рисунок 138 – 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.

### 8.8.6 Удаление точки подключения к ресурсной системе

Удаление точки подключения осуществляется путем нажатия на кнопку **<Удалить>** для точки подключения в карточке ресурсной системы (см. Рисунок 139).

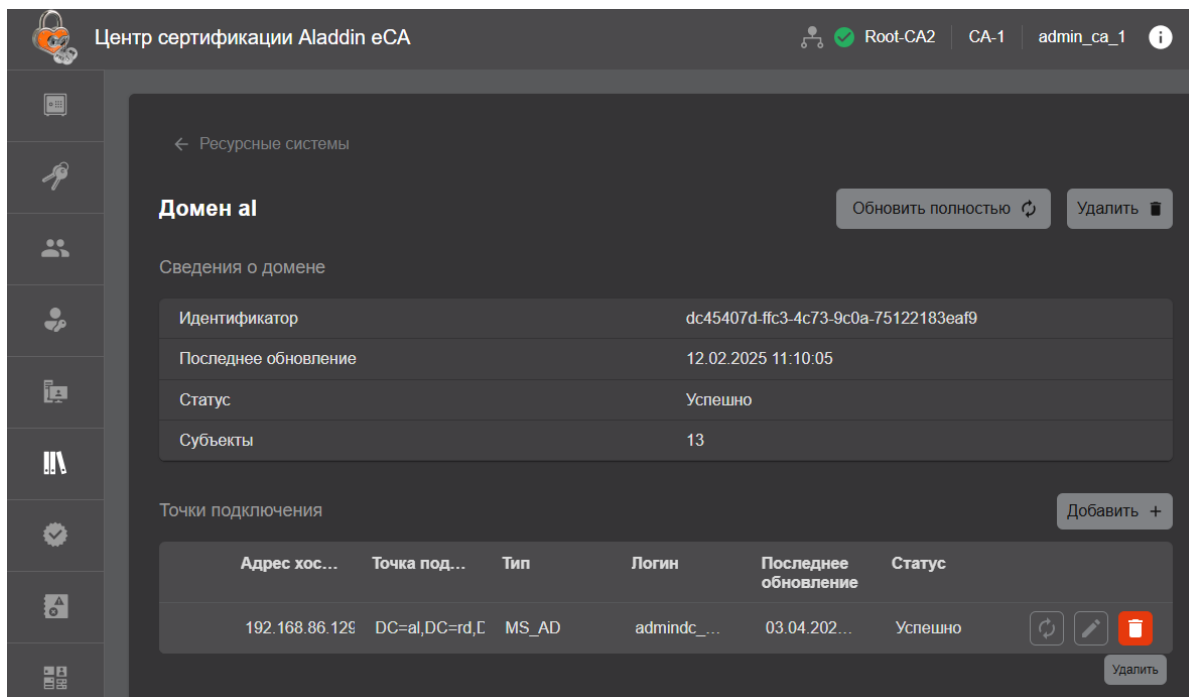


Рисунок 139 – Удаление ресурсной системы из карточки ресурсной системы

После этого отобразится окно подтверждения выбранного действия (см. Рисунок 140).

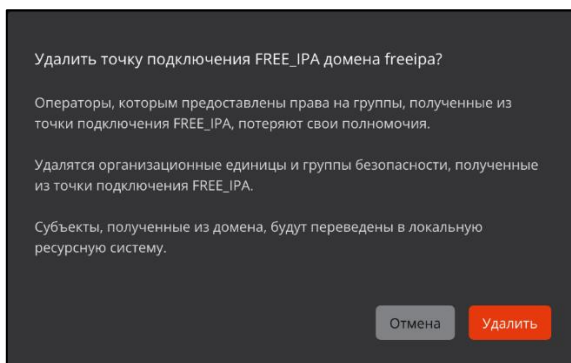


Рисунок 140 – Окно подтверждения удаления точки подключения

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.

## 8.9 Раздел «Центры валидации»

Переход в раздел «Центры валидации» выполняется через боковое меню, расположенное слева на главном экране (см. Рисунок 141). Данный раздел доступен только для пользователя с ролью «Администратор».

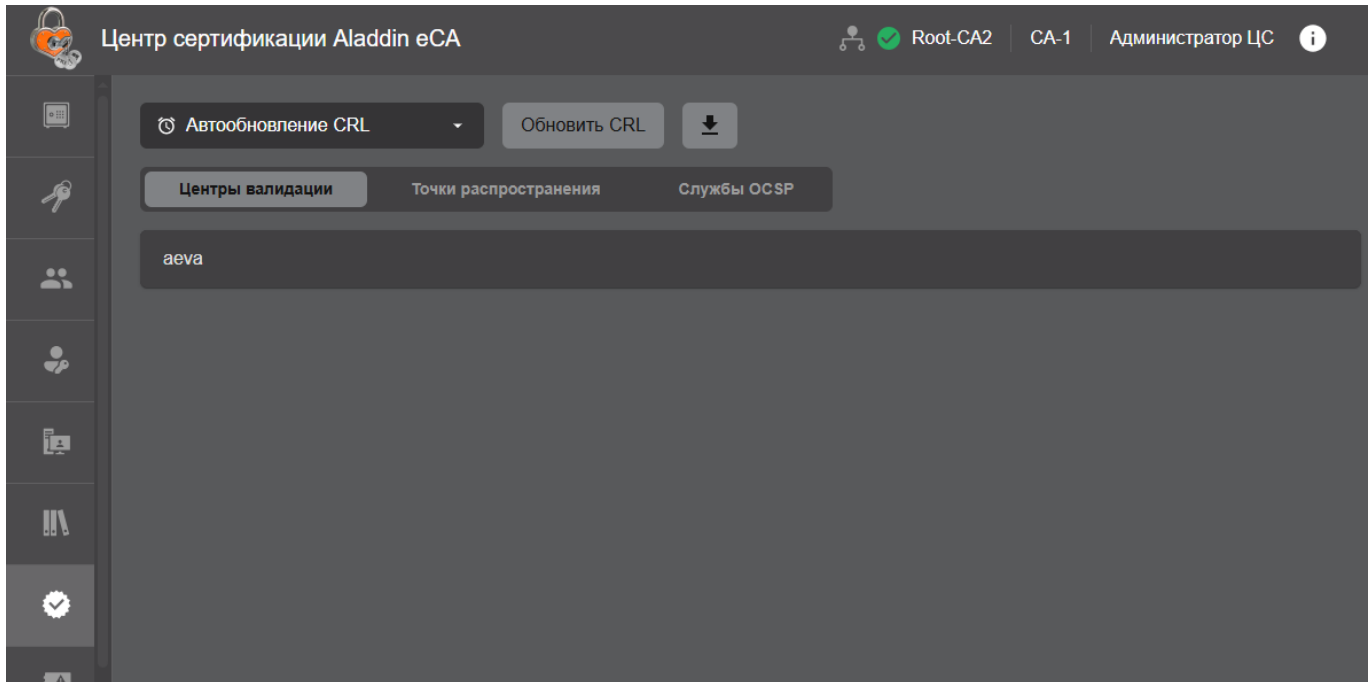


Рисунок 141 – Раздел «Центр валидации»

Раздел «Центры валидации» предназначен для выполнения следующих сценариев:

- Публикация списков отозванных сертификатов CRL по команде уполномоченного пользователя.
- Настройка параметров ЦВ.
- Удаление ЦВ.
- Настройка периода автоматического обновления точек публикации CRL и срока действия перекрытия Delta CRL для активного Центра сертификации.
- Экспорт актуального списка отозванных сертификатов CRL и разностного списка отозванных сертификатов DELTA 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 ЦВ.
- Создание пользовательской службы OCSP.

### 8.9.1 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 142). 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.

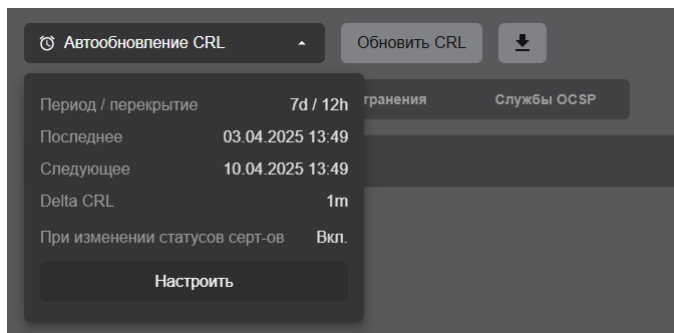


Рисунок 142 – Просмотр настроек автоматического обновления CRL

**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 142).
- В открывшемся окне выполните настройку следующих параметров автоматического обновления CRL (см. Рисунок 143):

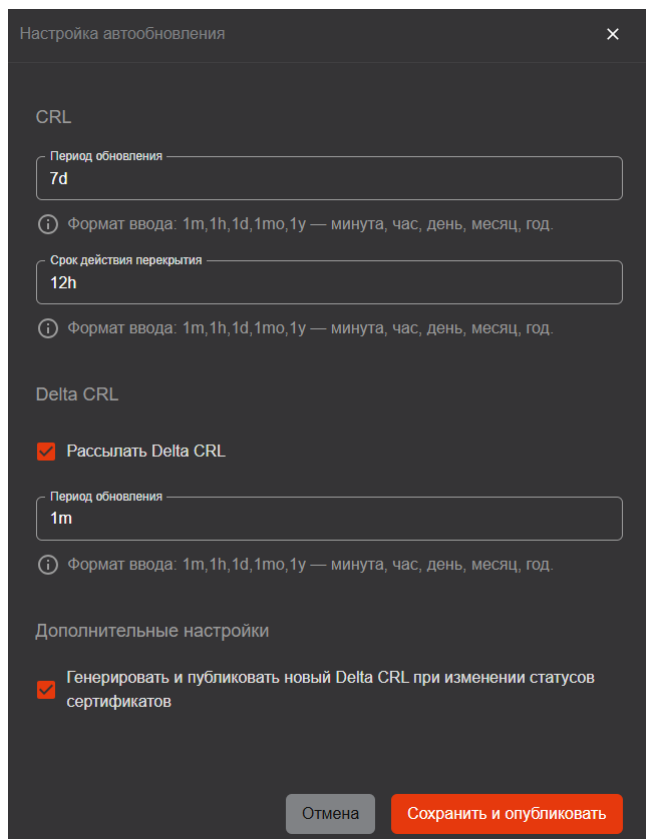


Рисунок 143 – Настройка автоматического обновления CRL

- 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 включённой 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.

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 рекомендаций:

- 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, приведённые ниже.
- Срок действия перекрытия (crlOverlapTime) не должен быть больше периода обновления Delta CRL (deltaCrlperiod), если выполняется следующее условие, приведённое 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:

- <This 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:
  - <This Update> = <Время создания CRL>
  - <Next Publish> = <This Update> + <crlperiod>
  - <Next Update> = <Next Publish> + <crlOverlapTime>
- для Delta CRL:
  - <This Update> = <время создания Delta CRL>
  - <Next Publish> = <This Update> + <deltaCrlperiod>
  - <Next Update> = <Next Publish>

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.

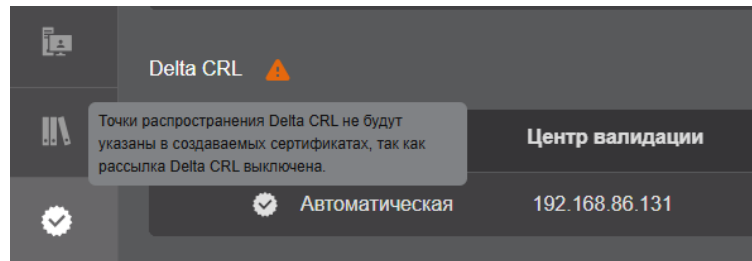


Рисунок 144 – Индикация точки распространения Delta CRL при выключенной рассылке Delta CRL

### 8.9.2 Публикация списка отозванных сертификатов CRL по команде

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 145). 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`).

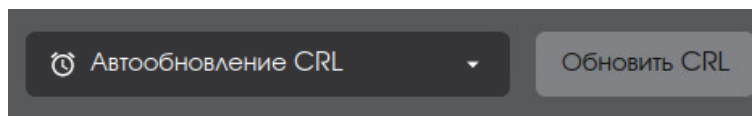



Рисунок 145 – Обновление CRL по команде администратора

### 8.9.3 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 еСА-СА выполните одно из следующих действий:
  - Если в еСА-СА не зарегистрирован ни один ЦВ и CRL ранее не публиковался, то опубликуйте и выгрузите новый CRL (см. Рисунок 146). Для этого в соответствующем поле укажите срок действия CRL и нажмите кнопку **<Сгенерировать и скачать>**.

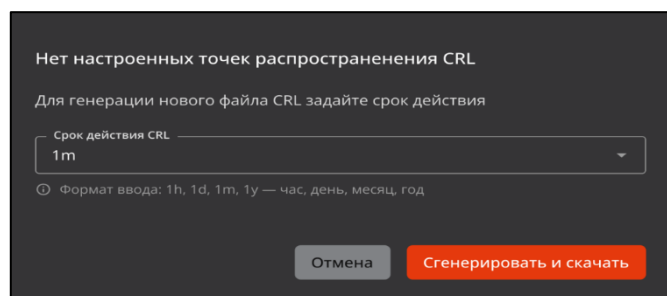


Рисунок 146 – Публикация и выгрузка нового CRL

- Если в еСА-СА не зарегистрирован ни один ЦВ, а CRL ранее публиковался, то выполните одно из следующих действий (см. Рисунок 147):
  - 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>**.

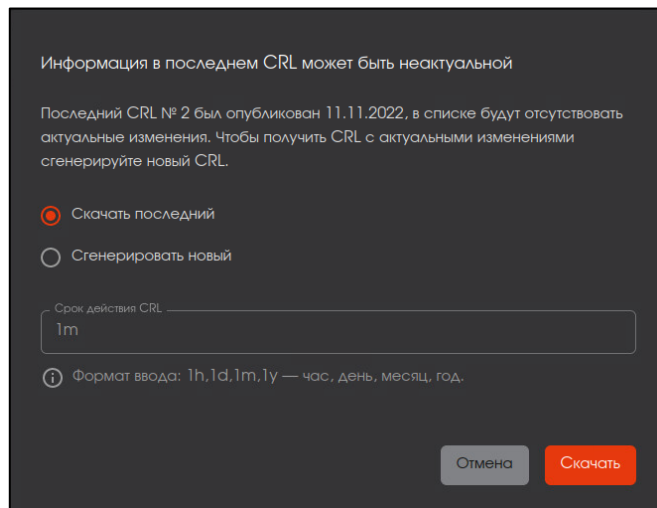


Рисунок 147 – Выгрузка последнего опубликованного CRL

- Если в еCA-CA зарегистрирован хотя бы один ЦВ, скачайте последний опубликованный CRL, нажав кнопку **<Скачать последний>** (см. Рисунок 148).

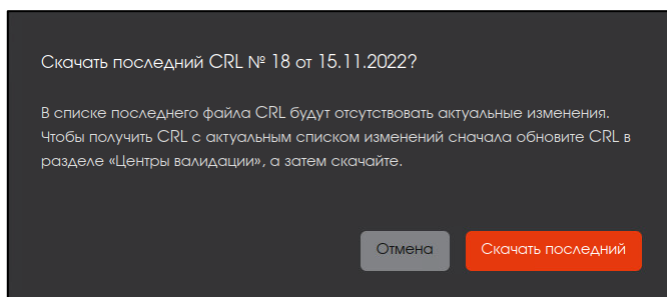


Рисунок 148 – Выгрузка последнего опубликованного CRL

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

#### 8.9.4 Регистрация Центра валидации в еCA-CA

Для регистрации Центра валидации в еCA-CA согласно руководству администратора еCA-VA:

1. Создайте в еCA-VA подключение к еCA-CA.
2. Аутентифицируйтесь в еCA-VA как администратор еCA-CA.
3. Создайте в еCA-VA Центр валидации для конкретного Центра сертификации.

#### 8.9.5 Управление Центрами валидации

В разделе «Центры валидации» еCA-CA отображаются сведения только о Центрах валидации текущего активного Центра сертификации.

Сведения о каждом Центре валидации представлены в его карточке.

Для просмотра карточки Центра валидации (см. Рисунок 149) перейдите на вкладку «Центры валидации» раздела «Центры валидации» и щёлкните по строке Центра валидации.

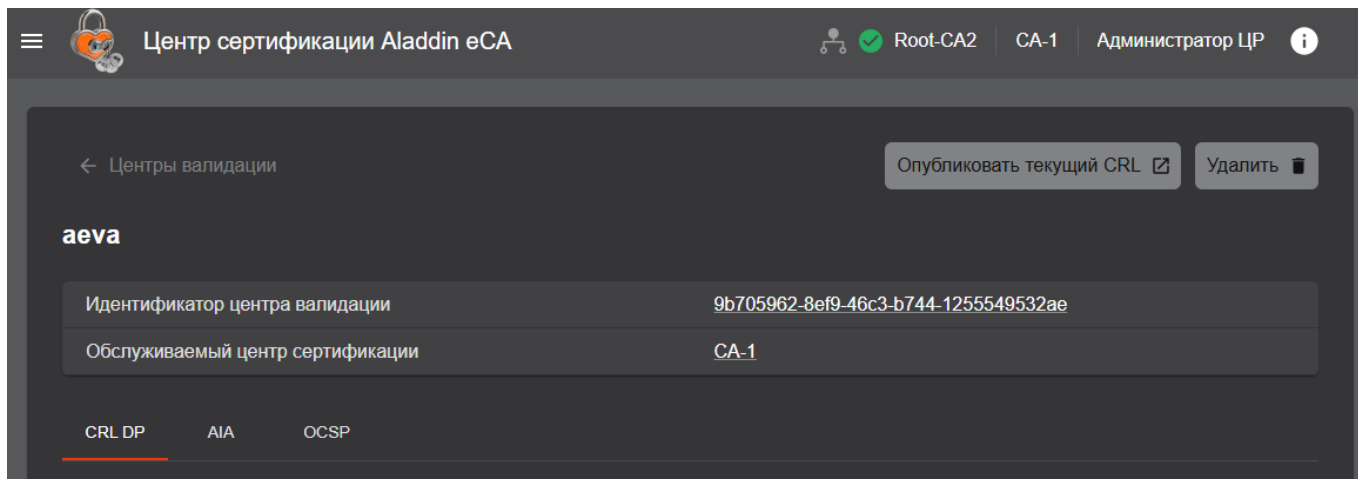





Рисунок 149 – Карточка зарегистрированного центра валидации

В карточке ЦВ доступны следующие действия:

- Просмотр информации об идентификаторе центра валидации.
- Просмотр информации об обслуживаемом центре сертификации.
- Публикация последнего сгенерированного CRL в Центре валидации Aladdin eCA. Для этого нажмите кнопку **<Опубликовать текущий CRL>**.
- Удаление центра валидации. Для этого наведите указателем мыши на выбранный центр валидации в списке, нажмите кнопку  **<Удалить>** или в карточке центра валидации нажмите кнопку  и в открывшемся окне (см. Рисунок 150) подтвердите удаление, нажав кнопку .

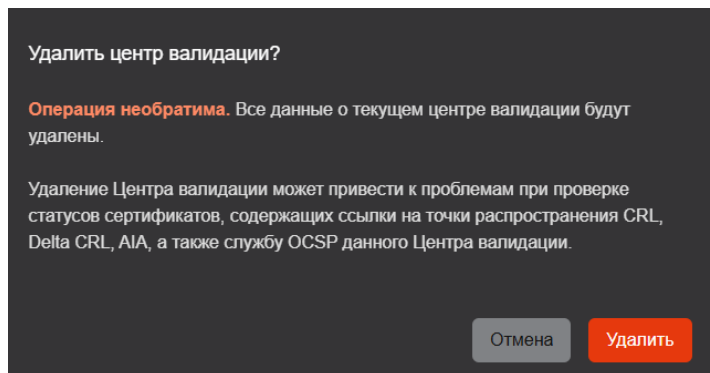



Рисунок 150 –Подтверждение удаления центра валидации

- Для службы CRL DP на вкладке «CRL DP» (см. Рисунок 151) доступны следующие действия:
  - Выгрузка списка отозванных сертификатов CRL. Для этого нажмите кнопку **<Скачать CRL>**.
  - Выгрузка разностного списка отзыва сертификатов DELTA CRL. Для этого нажмите кнопку **<Скачать DELTA CRL>**.
  - Просмотр URL выгрузки CRL, который будет включаться в выпускаемые сертификаты (см. 8.9.9). Чтобы скопировать URL в буфер обмена, щёлкните рядом с URL значок .

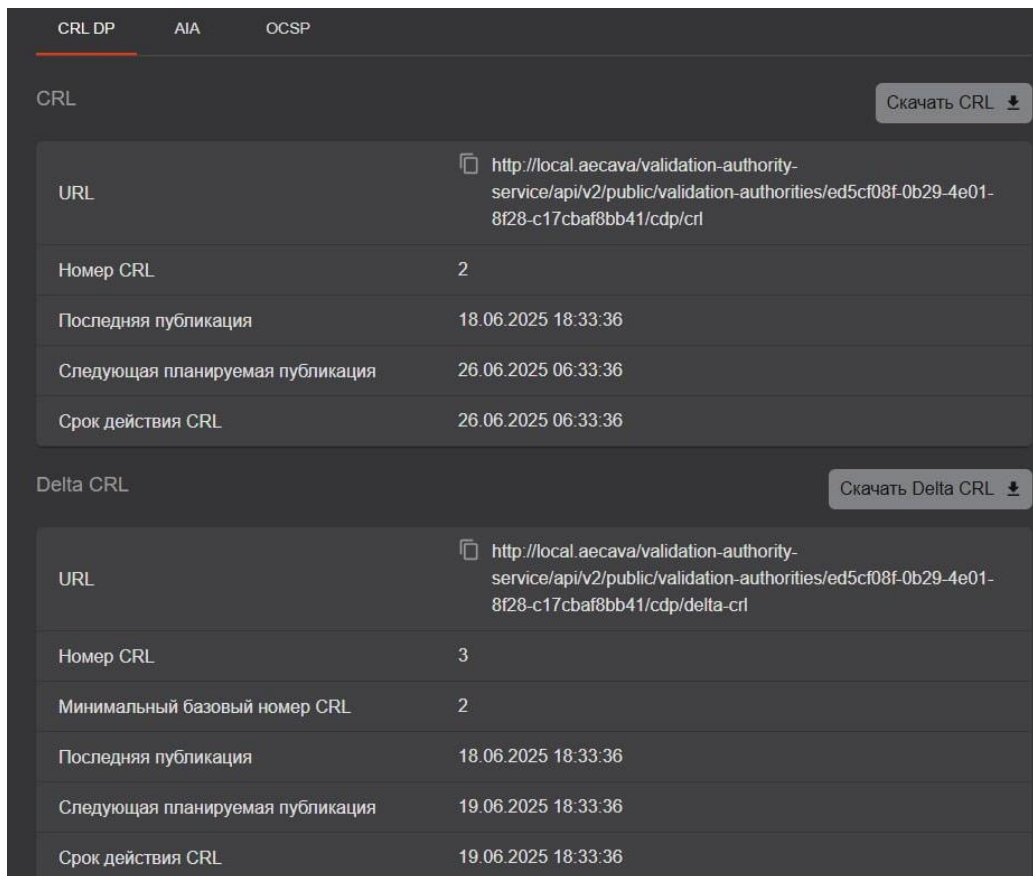


Рисунок 151 – Вкладка «CRL» карточки центра валидации

- Просмотр URL выгрузки DELTA CRL, который будет включаться в выпускаемые сертификаты (см. 8.9.9). Чтобы скопировать URL в буфер обмена, щёлкните рядом с URL значок
- Просмотр порядковых номеров публикации CRL и DELTA CRL.
- Просмотр даты и времени последней публикации CRL и DELTA CRL.
- Просмотр даты и времени следующей публикации CRL и DELTA CRL.
- Просмотр даты и времени окончания срока действия CRL и DELTA CRL.
- Для службы AIA на вкладке «AIA» (см. Рисунок 152) доступны следующие действия:
  - Выгрузка опубликованного сертификата текущего издающего центра сертификации. Для этого нажмите кнопку **<Скачать сертификат>**.
  - Просмотр URL выгрузки сертификата издателя, который будет включаться в выпускаемые сертификаты (см. раздел 8.9.9). Чтобы скопировать URL в буфер обмена, щёлкните рядом с URL значок .
  - Просмотр имени владельца (центра сертификации).
  - Просмотр SDN владельца (центра сертификации).
  - Просмотр срока действия сертификата Центра сертификации.
  - Просмотр алгоритма и длины ключа, на котором был выпущен закрытый ключ Центра сертификации.
- Для службы OCSP на вкладке «OCSP» (см. Рисунок 153) доступны следующие действия:
  - Просмотр URL OCSP-сервера. URL будет включаться в выпускаемые сертификаты (см. раздел 8.9.9). Чтобы скопировать URL в буфер обмена, щёлкните рядом с адресом OCSP значок .
  - Просмотр статуса OCSP-службы.

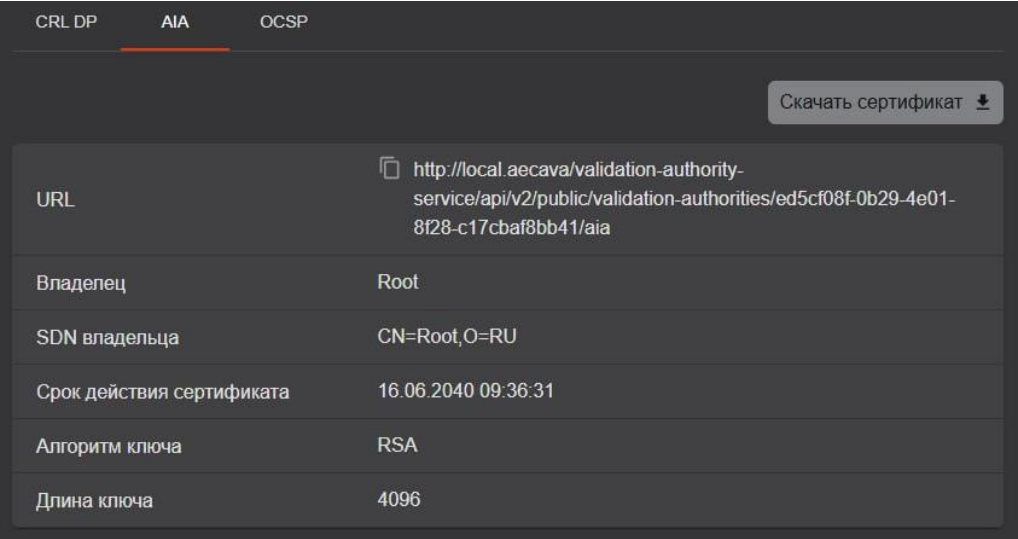


Рисунок 152 – Вкладка «AIA» карточки центра валидации

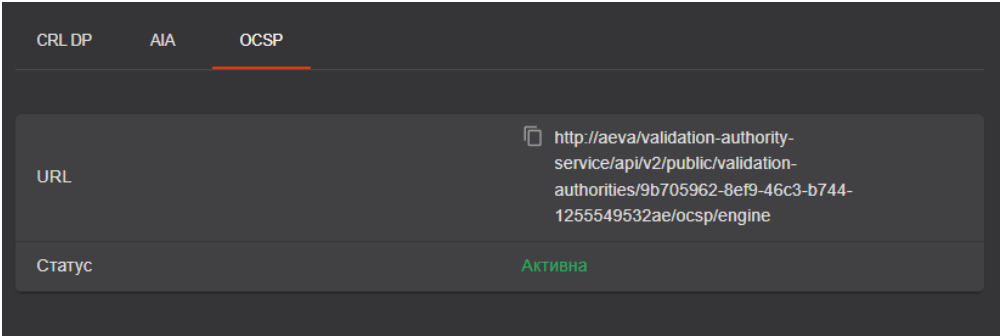


Рисунок 153 – Вкладка «OCSP» карточки центра валидации

### 8.9.6 Управление точками распространения

Вкладка «Точки распространения» раздела «Центры валидации» предназначена для:

- Просмотра URL точек распространения CRL, Delta CRL и AIA, подключенных eCA-VA, 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 8.9.9).
- 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 154):

- Тип – тип точки распространения (автоматическая или пользовательская).
- Центр валидации – IP–адрес или полное доменное имя компьютера с установленным eCA-VA (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 154 – 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.

#### 8.9.6.1 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 eCA-CA 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 и Dynamic Directory. 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, Dynamic Directory и FreeIPA – в формате Distinguished Names.

**Внимание!** Успешная публикация в ALD PRO, Dynamic Directory 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=PublicKey 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 **Создать** и выберите в списке «Пользовательская».
- В открывшемся окне (см. Рисунок 155) выполните следующие действия:

Рисунок 155 – Создание точки распространения

- 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.
- 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 156) выполните следующие действия:

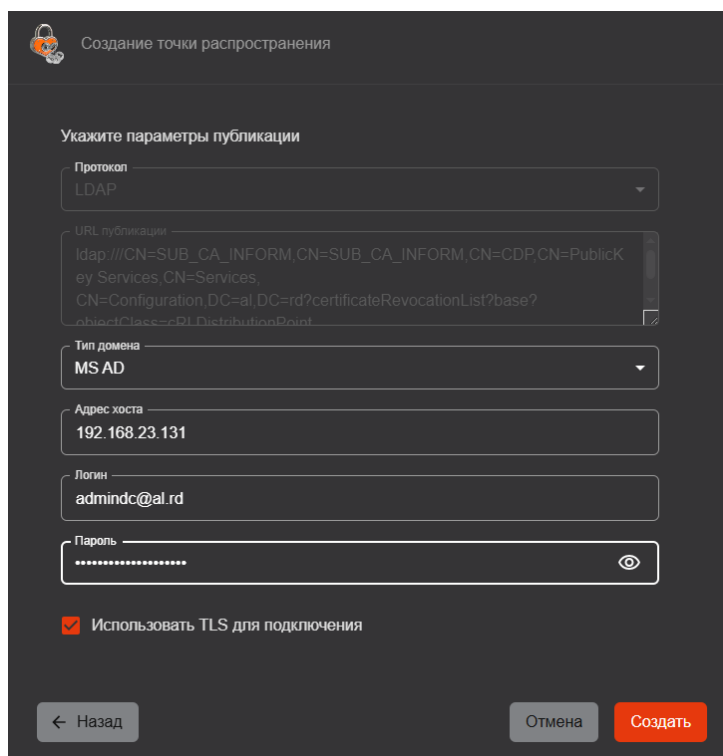



Рисунок 156 – Указание параметров публикации для точки распространения

- В списке «Тип домена» выберите тип доменной службы каталогов ресурсной системы (Samba DC, Альт Домен, ALD PRO, MS AD, Dynamic Directory, 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>**.

### 8.9.6.2 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 157).

CRL







Тип	Центр ва...	URL	Приоритет	Дата изм...	Публикац...	Дата пуб...	Запись в сертификаты	
	—	https://ae...	15	07.05.20...	Ошибка	18.06.20...	<input type="checkbox"/>	 
	aeva	http://aev...	0	07.05.20...	Ошибка	18.06.20...	<input checked="" type="checkbox"/>	 Редактировать


Рисунок 157 – Инициализация процесса редактирования пользовательской точки распространения

- В открывшемся окне (см. Рисунок 158) выполните следующие действия:

 Редактирование точки распространения

URL точки распространения  
https://aeca/validation?distributionPoint=true3

Приоритет  
13

 Формат ввода: число от 0 до 1000

☐ Публиковать CRL в точку распространения

Рисунок 158 – Редактирование пользовательской точки распространения

- При необходимости в соответствующих полях измените URL и приоритет точки распространения (описание и правила заполнения полей см. в разделе 8.9.6.1).
- 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.

- В открывшемся окне (см. Рисунок 159) выберите тип доменной службы, укажите адрес контроллера домена, имя и пароль учетной записи администратора контроллера домена (описание и правила заполнения полей см. в разделе 8.9.6.1) и нажмите кнопку **<Сохранить изменения>**.

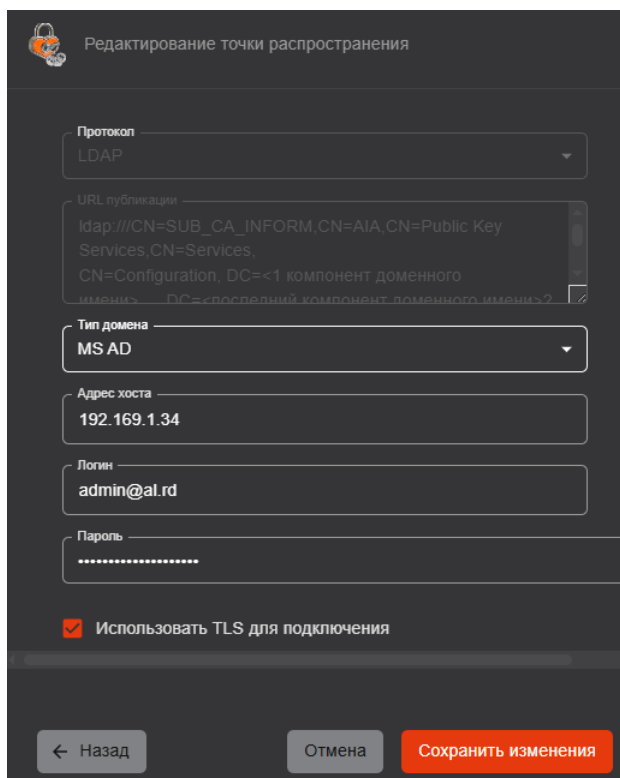



Рисунок 159 – Редактирование параметров публикации пользовательской точки распространения

### 8.9.6.3 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 157).
- В открывшемся окне (см. Рисунок 160) в соответствующем поле измените приоритет автоматической точки распространения (описание и правила заполнения полей см. в разделе 8.9.6.1). После этого нажмите кнопку **<Продолжить>**.

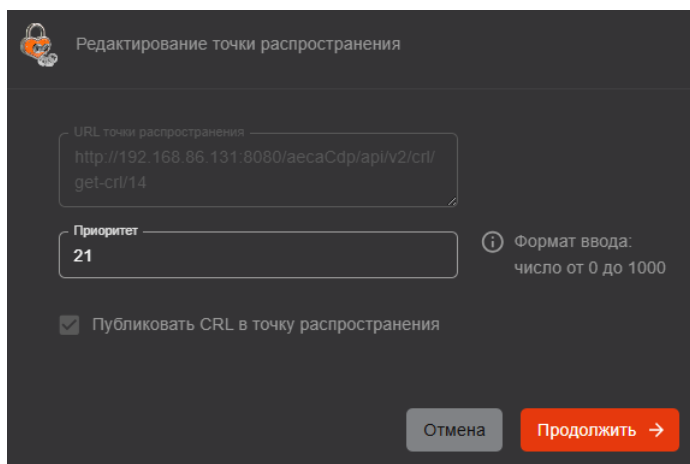


Рисунок 160 – Редактирование автоматической точки распространения

- В открывшемся окне (см. Рисунок 161) нажмите кнопку **<Сохранить изменения>**.

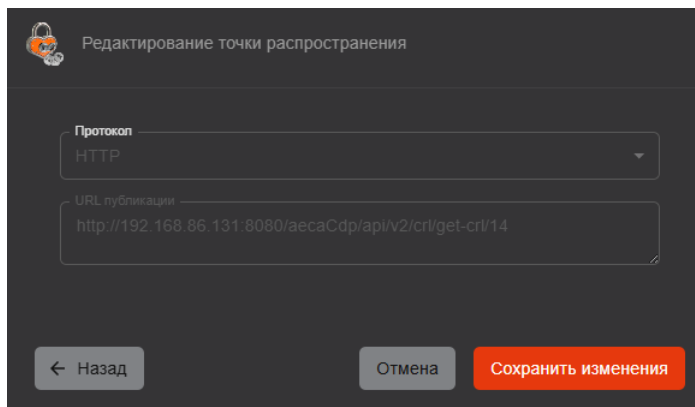



Рисунок 161 – Редактирование автоматической точки распространения

#### 8.9.6.4 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 162).

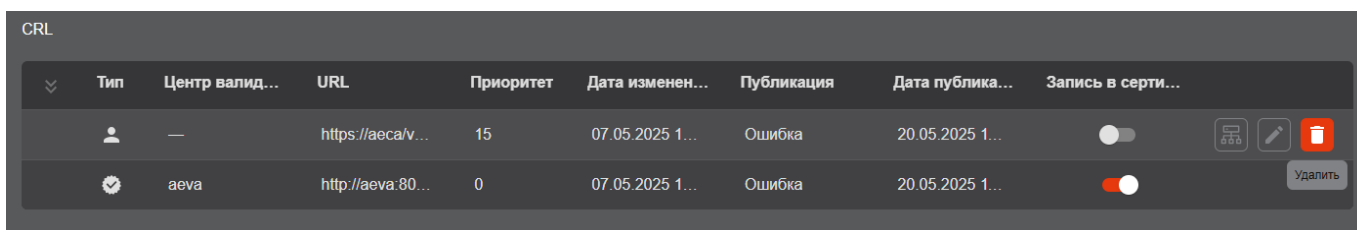


Рисунок 162 –Инициализация процесса удаления точки распространения

- В открывшемся окне (см. Рисунок 163) подтвердите удаление точки распространения, нажав кнопку **<Удалить>**.

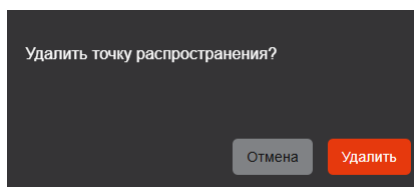


Рисунок 163 – Подтверждение удаления пользовательской точки распространения

#### 8.9.6.5 Создание кластера точек распространения

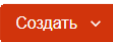
Объединения точек распространения в кластеры может потребоваться для проксирования доступа к ним с целью распределения нагрузки.

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 164) 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 164 – Создание кластера точек распространения. Шаг 1

- В открывшемся окне (см. Рисунок 165) выполните следующие действия:
  - В списке «Выбрать» с помощью флажков выберите URL точек распространения, которые необходимо объединить в кластер, и щёлкните 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 щёлкните значок ➤. В результате выбранные точки распространения будут перемещены в список «Выбрать».
  - Чтобы найти точки распространения в списках, используйте поля поиска.
  - Нажмите кнопку **<Создать кластер>**.

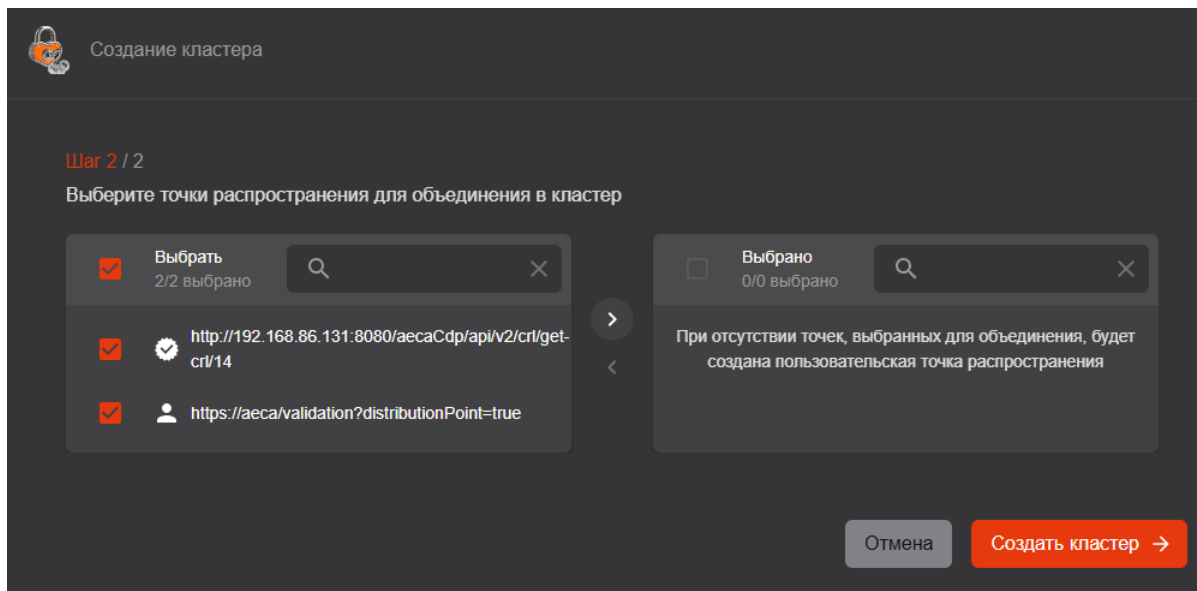



Рисунок 165 – Создание кластера точек распространения. Шаг 2

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 166).

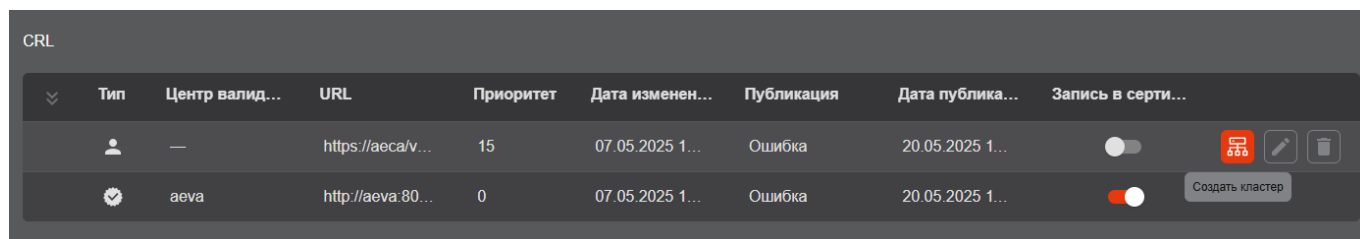





Рисунок 166 – Создание кластера на основе зарегистрированной точки распространения

- В открывшемся окне (см. Рисунок 165) выполните следующие действия:
  - В списке «Выбрать» с помощью флажков выберите URL точек распространения, которые необходимо объединить в кластер, и щёлкните 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 щёлкните 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.

#### 8.9.6.6 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 щёлкните значок  (см Рисунок 167).

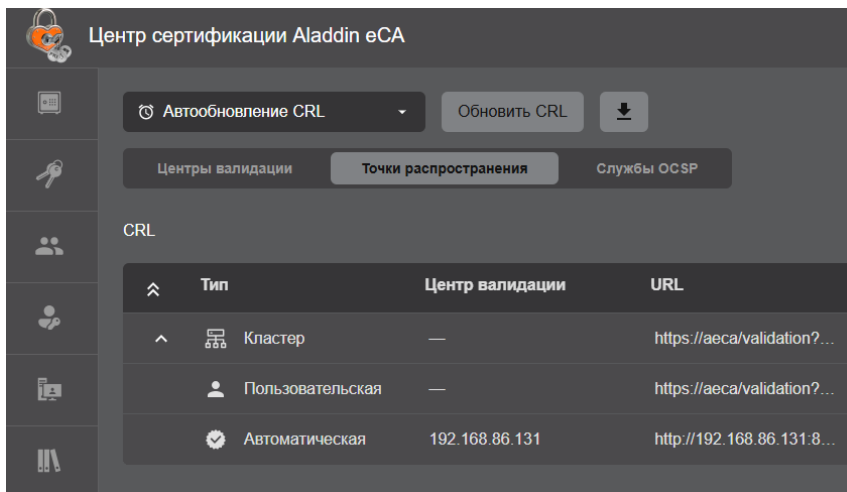


Рисунок 167 – Просмотр состава кластера точек распространения

- Чтобы скрыть состав кластера, щёлкните значок

#### 8.9.6.7 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 168).

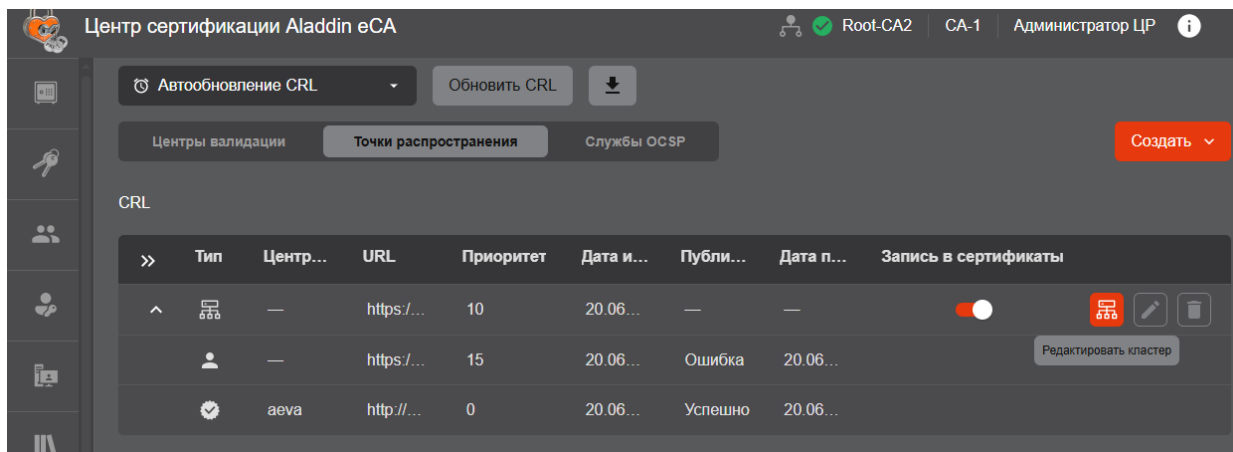


Рисунок 168 – Инициализация процесса редактирования кластера

- В открывшемся окне управления кластером (см. Рисунок 169) измените состав кластера и нажмите кнопку **<Сохранить изменения>**.

В списке «Выбрать» с помощью флажков выберите URL точек распространения, которые необходимо добавить в кластер, и щёлкните 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 щёлкните значок . Чтобы найти точки распространения в списках, используйте поля поиска.

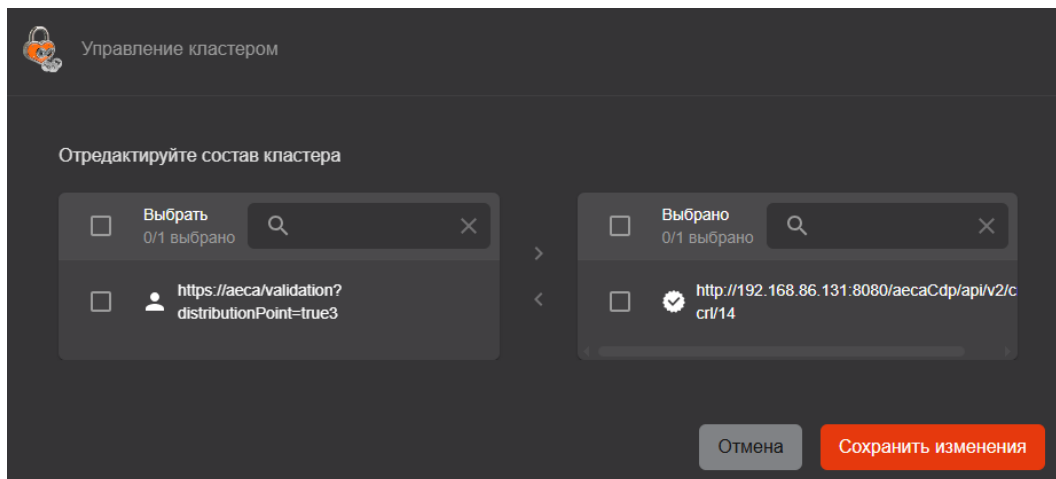



Рисунок 169 – Редактирование состава кластера

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 170).

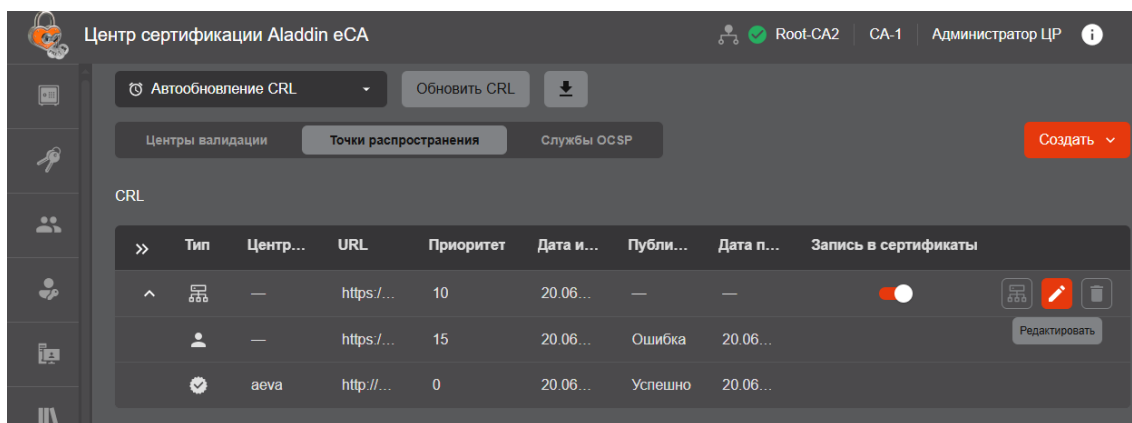


Рисунок 170 – Инициализация процесса редактирования параметров кластера

- В открывшемся окне (см. Рисунок 171) в соответствующих полях измените URL, приоритет кластера точек распространения и нажмите кнопку **<Сохранить изменения>**.

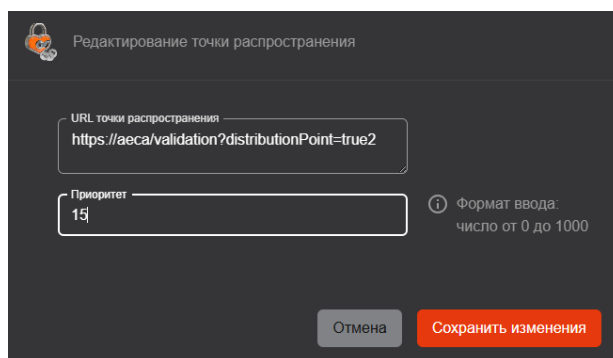



Рисунок 171 – Редактирования кластера точек распространения

#### 8.9.6.8 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 172).

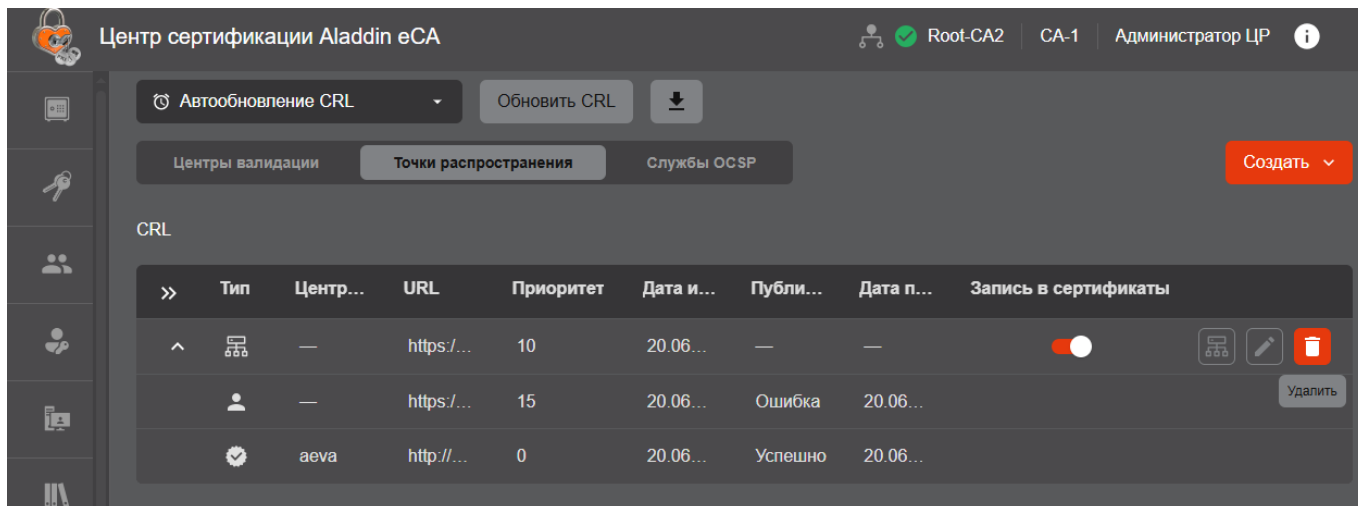


Рисунок 172 – Инициализация процесса удаления кластера

- В открывшемся окне (см. Рисунок 173) подтвердите удаление, нажав кнопку **<Удалить>**.

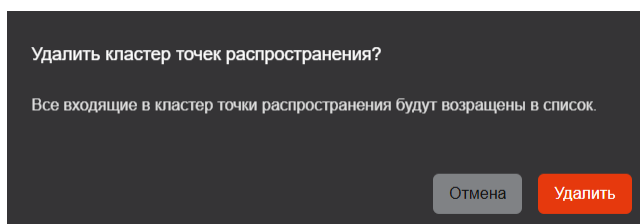


Рисунок 173 –Подтверждение удаления кластера

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

## 8.9.7 Управление службами OCSP

Управление службами OCSP предполагает:

- Просмотр URL служб OCSP, созданных в eCA-VA, образующих **автоматические службы**. Данные службы обозначены в списке значком (поле «Тип»). Создание, активация и управление службой OCSP для выбранного ЦВ выполняется уполномоченным администратором в «Центре валидации Aladdin Enterprise Validation Authority». Порядок создание и активация службы OCSP приведен в документе «Центр сертификатов доступа Aladdin Enterprise Certificate Authority Certified Edition. Руководство администратора. Часть 4. «Центр валидации Aladdin Enterprise Validation Authority».
- Регистрацию сторонних служб OCSP, существующих или развёртываемых на серверах в информационной системе, образующих **пользовательские службы**. Данные службы обозначены в списке значком (поле «Тип»).
- Управление приоритетом служб OCSP. Приоритет определяет очерёдность записи URL служб OCSP в сертификаты субъектов (см. раздел 8.9.9).
- Управление записью служб OCSP в выпускаемые сертификаты. Объединение служб OCSP в кластеры для проксирования доступа к ним с целью распределения нагрузки.

Информация о службах OCSP представлена на вкладке «Службы OCSP» раздела «Центры валидации» списком в табличном виде:

- Тип – типа службы OCSP. (пользовательская или автоматическая).
- Центр валидации – IP–адрес или полное доменное имя компьютера с установленным eCA-VA (только для автоматических служб).
- URL – адрес сервера службы OCSP.

- Приоритет – 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, в параметры которой изменения были внесены позднее, начиная с даты и времени ее создания.
- Дата изменения – дата и время последнего редактирования параметров службы OCSP (изменение URL и приоритета).
- Переключатель, позволяющий управлять записью служб OCSP в выпускаемые сертификаты. При выключенном переключателе запись служб OCSP в сертификаты не выполняется.

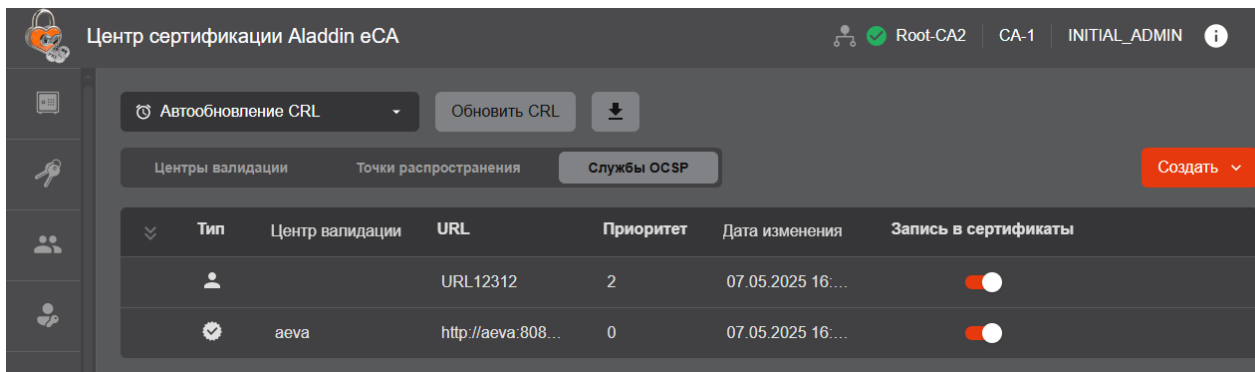


Рисунок 174 –Список служб OCSP

Управление службами OCSP включает следующие операции:

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

#### 8.9.7.1 Создание пользовательской службы OCSP

Порядок создания пользовательской службы OCSP:

- Перейдите на вкладку «Службы OCSP» раздела «Центры валидации».
- Нажмите кнопку **Создать** и выберите в списке «Пользовательская».
- В открывшемся окне (см. Рисунок 175) 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 её создания.

Создание службы OCSP

URL  
https://aeva.8888/noredirect.html

Приоритет  
80

Формат ввода:  
число от 0 до 1000

Отмена Создать


Рисунок 175 – Создание службы OCSP

- Нажмите кнопку **<Создать>**.

В результате будет создана пользовательская служба OCSP.

#### 8.9.7.2 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 176).

Центр сертификации Aladdin eCA

Root-CA2 CA-1 Администратор ЦП

Автообновление CRL Обновить CRL

Центры валидации Точки распространения **Службы OCSP** Создать

Тип	Центр валидации	URL	Приоритет	Дата изменения	Запись в сертификаты	
		URL12312	2	07.05.2025 16:1...	<input type="checkbox"/>	
	aeva	http://aeva/valid...	0	19.06.2025 14:3...	<input type="checkbox"/>	Редактировать

Рисунок 176 –Инициализация процесса редактирования службы OCSP

- В открывшемся окне (см. Рисунок 177) в соответствующих полях измените URL и приоритет службы OCSP (описание и правила заполнения полей см. в разделе 8.9.7.1). После этого нажмите кнопку **<Сохранить изменения>**.

Редактирование службы OCSP

URL  
https://aeva.8888/noredirect.html

Приоритет  
12

Формат ввода:  
число от 0 до 1000


Отмена Сохранить изменения

Рисунок 177 – Редактирования пользовательской службы OCSP

#### 8.9.7.3 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 176).
- В открывшемся окне (см. Рисунок 178) в соответствующем поле измените приоритет автоматической службы OCSP (описание и правила заполнения полей см. в разделе 8.9.7.1). После этого нажмите кнопку **<Сохранить изменения>**.

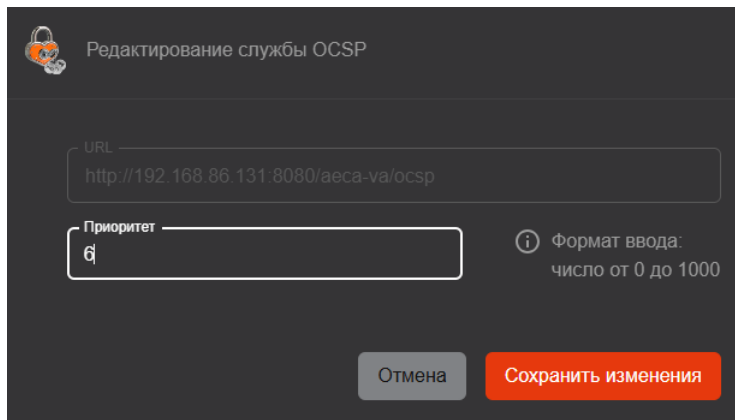



Рисунок 178 – Окно редактирования автоматической службы OCSP

#### 8.9.7.4 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 179).

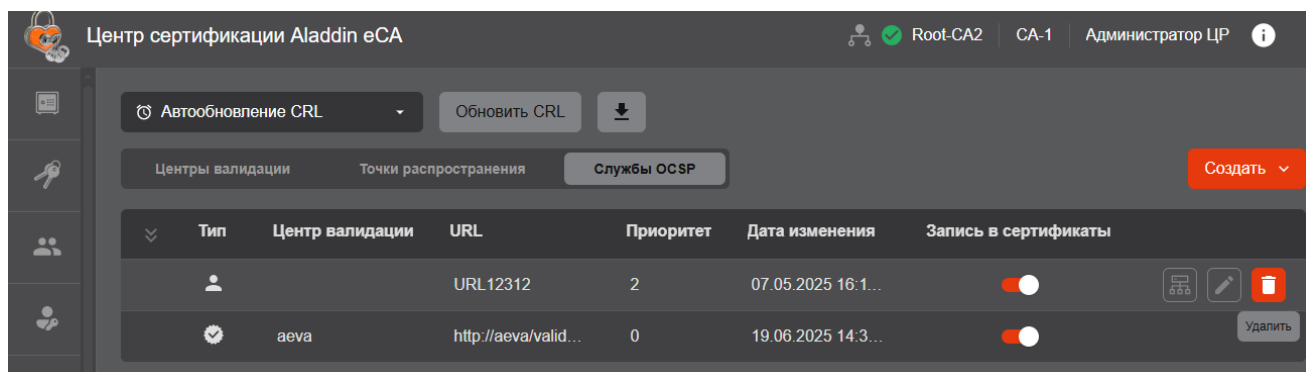


Рисунок 179 –Инициализация процесса удаления службы OCSP

- В открывшемся окне (см. Рисунок 180) подтвердите удаление службы, нажав кнопку **<Удалить>**.

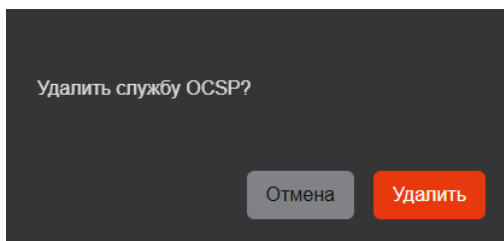


Рисунок 180 – Подтверждение удаления пользовательской службы OCSP

#### 8.9.7.5 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:

- Путём создания нового кластера и добавления в него уже существующих служб OCSP.
- Путём 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 **Создать** и выберите в списке «Кластер».
- В открывшемся окне (см. Рисунок 181) выполните следующие действия:

- В поле «URL» укажите URL балансировщика нагрузки.

При указании URL возможны следующие сообщения об ошибках:

- «Указан URL существующей службы OCSP» – введённый URL совпадает с URL существующей (ранее зарегистрированной) точки распространения.
- «Некорректный ввод» – введённый 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 181 – Создание кластера служб OCSP. Шаг 1

- В открывшем окне (см. Рисунок 182) выполните следующие действия:
  - В списке «Выбрать» с помощью флажков выберите URL служб OCSP, которые необходимо объединить в кластер, и щёлкните 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 щёлкните значок ◀. В результате выбранные службы будут перемещены в список «Выбрать».
  - Чтобы найти службу в списках, используйте поля поиска.
  - Нажмите кнопку **<Создать кластер>**.

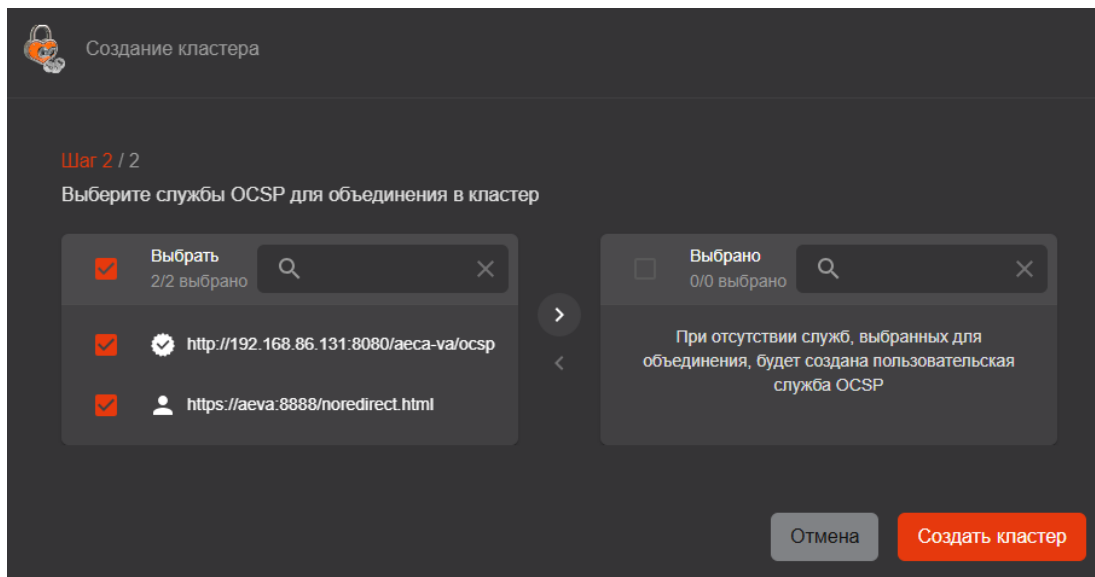


Рисунок 182 – Создание кластера служб OCSP. Шаг 2

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 183).

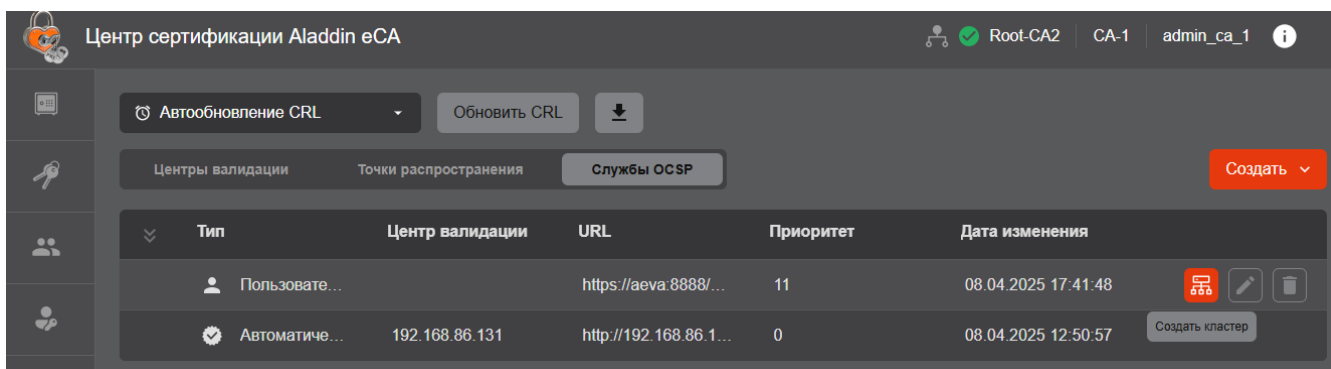


Рисунок 183 – Инициализация процесса создания кластера служб OCSP

- В открывшемся окне создания кластера (см. Рисунок 184) выполните следующие действия:

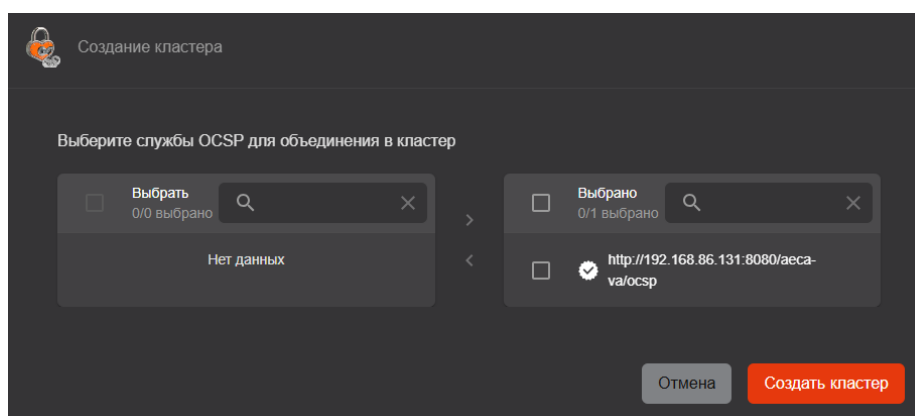



Рисунок 184 – Создание кластера из пользовательской службы OCSP


- В списке «Выбрать» с помощью флажков выберите URL служб OCSP, которые необходимо объединить в кластер, и щёлкните 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 щёлкните значок .
- Чтобы найти службу в списках, используйте поля поиска.
- Нажмите кнопку **<Создать кластер>**.

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

#### 8.9.7.6 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 щёлкните значок  (см. Рисунок 185).

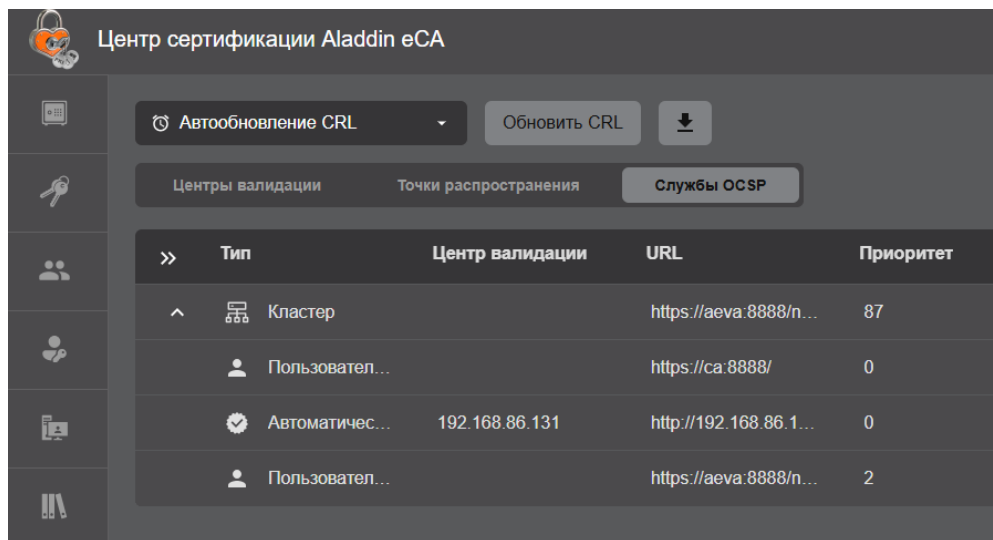



Рисунок 185 –Просмотр состава кластера служб OCSP

- Чтобы скрыть состав кластера, щёлкните значок .

#### 8.9.7.7 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 186).

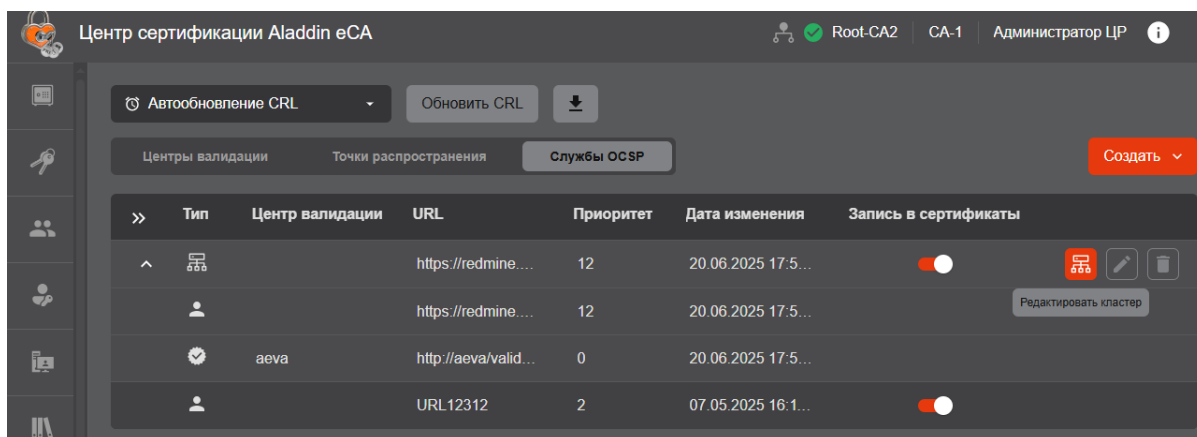


Рисунок 186 – Инициализация процесса редактирования состава кластера

- В открывшем окне управления кластером (см. Рисунок 187) измените состав кластера и нажмите кнопку **<Сохранить изменения>**.

- Чтобы добавить службы OCSP в кластер, выберите URL служб в списке «Выбрать» с помощью флажков и щёлкните 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 щёлкните значок ◀. В результате выбранные службы будут перемещены в список «Выбрать».
- Чтобы найти службу в списках, используйте поля поиска.

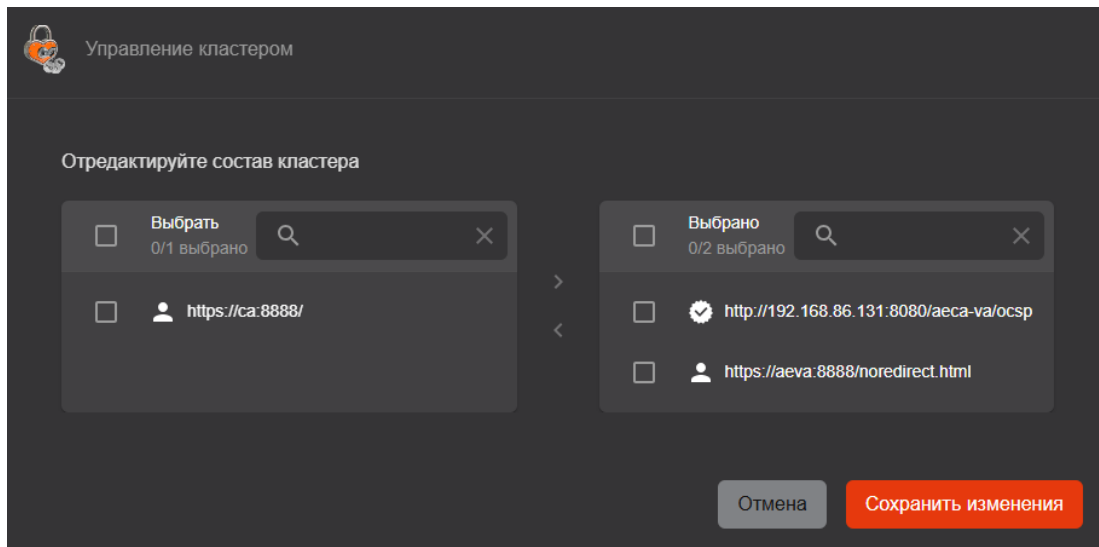



Рисунок 187 – Редактирование состава кластера служб OCSP

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 188).

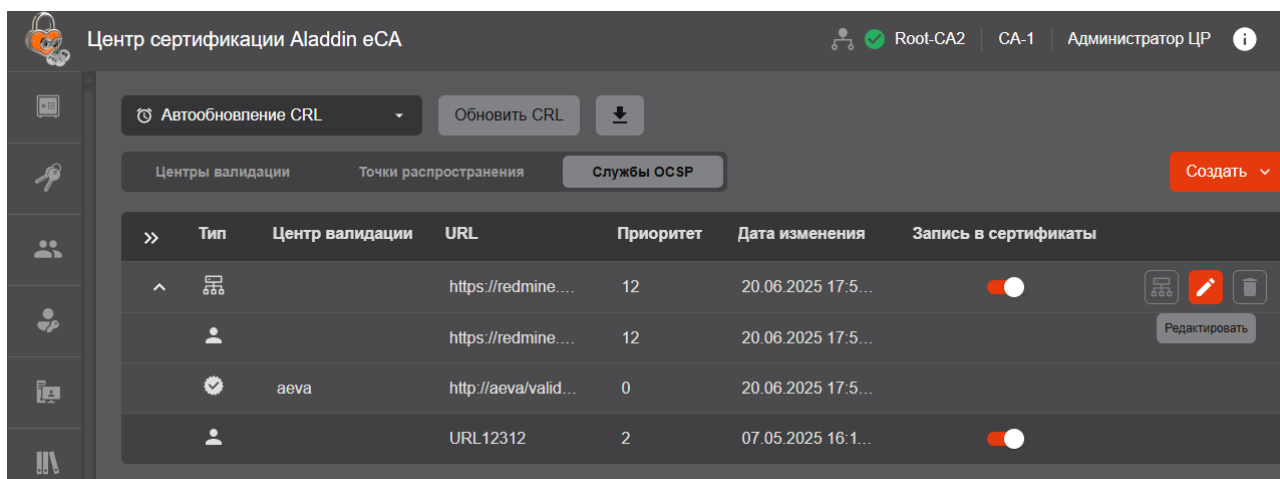



Рисунок 188 – Инициализация процесса редактирования параметров кластера

- В открывшемся окне (см. Рисунок 189) в соответствующих полях измените URL, приоритет кластера служб OCSP и нажмите кнопку **<Сохранить изменения>** (описание и правила заполнения полей см. в разделе 8.9.7.5).

Рисунок 189 – Редактирование параметров кластера службы OSCP

### 8.9.7.8 Удаление кластера служб OSCP

Для удаления кластера служб OSCP выполните следующие действия:

- Перейдите на вкладку «Службы OSCP» раздела «Центры валидации».
- Наведите указателем мыши на выбранный кластер в списке и нажмите кнопку  **<Удалить>** (см. Рисунок 190).

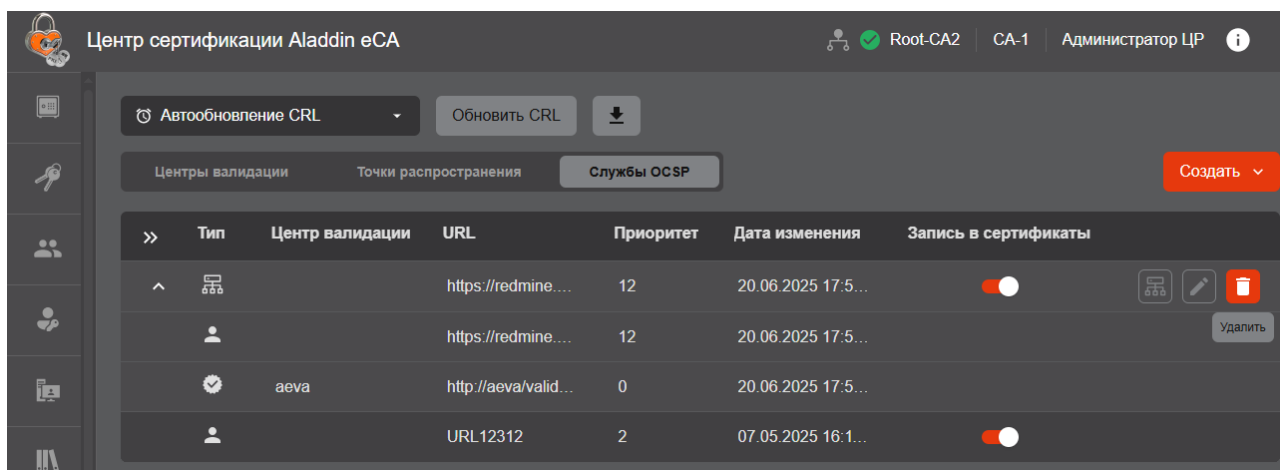


Рисунок 190 – Инициализация процесса удаления кластера служб OSCP

- В открывшемся окне (см. Рисунок 191) подтвердите удаление, нажав кнопку **<Удалить>**.

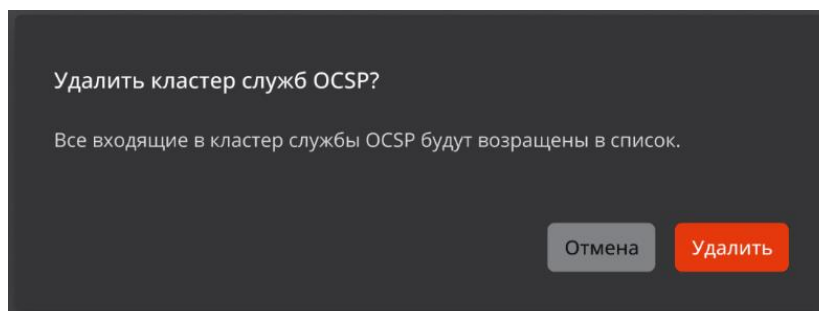


Рисунок 191 – Подтверждение удаления кластера служб OSCP

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

## 8.9.8 Получение файлов CRL, Delta CRL и AIA

### 8.9.8.1 Получение файлов посредством запуска скрипта из состава программы

Предварительно необходимо подготовить скрипт, отредактировав его исходный код выполнив команду с правами суперпользователя:

```
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 Центра сертификации);
- путь к папке хранения сертификата для авторизации в Центре сертификации (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 Центре сертификации (параметр `P12_PATH`);
- пароль от контейнера p12 для авторизации в Центре сертификации (параметр `P12_PASSWORD`);
- путь к файлу сертификата для авторизации в Центре сертификации (параметр `CERT_PATH`), в случае использования значений по умолчанию необходимо создать каталог `/opt/aecaCa/dist/account`;
- путь к файлу ключа сертификата для авторизации в Центре сертификации (параметр `KEY_PATH`), в случае использования значений по умолчанию для этих параметров необходимо создать каталог `/opt/aecaCa/dist/account`;
- хост Центра сертификации (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:

```
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 Центром сертификации, идентификатор которого указан в параметре `CA_ID`.

### 8.9.8.2 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 документе «Центр сертификатов доступа Aladdin Enterprise Certificate Authority Certified Edition. Руководство администратора. Часть 3. Описание методов REST API «Центра сертификации Aladdin Enterprise Certification Authority»).

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 документе «Центр сертификатов доступа Aladdin Enterprise Certificate Authority Certified Edition. Руководство администратора. Часть 3. Описание методов REST API «Центра сертификации Aladdin Enterprise Certification Authority»).

Для получения файла CRL необходимо использовать метод получения CRL по идентификатору Центра сертификации (см. описание метода в документе «Центр сертификатов доступа Aladdin Enterprise Certificate Authority Certified Edition. Руководство администратора. Часть 3. Описание методов REST API «Центра сертификации Aladdin Enterprise Certification Authority»).

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/crl' --header 'Cookie: token=eyJhbGciOiJSUzUxMiJ9.eyJzZXNzaW9uSWQ9I2Njc3NGU1ZS1jODkzLTRmOWQtdm4Yy1lMzQzZGQ1MGE3ZjU1LCJpYXQiOiJlMzMTAzMtIzODAsImV4cCI6MTcxMDMxMjU2MH0.MyyCQr89HeahIsnsn_vUXxeSqwFV1WRJUtpIkVMTbxq7BrzjG1cjFNJ9rEXx9jGKeSaTMbuwhmjX4aODGnPWCSFc18DUCqFA-85BTYgVGL5ns5kXfCe2Wxmr7oPj-7XMAzBI98JydXkLEbmRx7F1OteNW1ZY3JkwKvi9yFxbWrojB3yNq2ak39cvNj4AFKCEBF'
```

OnE8UxKPoyXKDXegC0xEv2UK8mhF7Um4od9B1LWlCuNqKExyqTGr1DDKJcYjyoWBh49pQFAC3mG\_bv7pBtTY7\_vwuVNAelBAqj1kUm\_scA\_1-gARBh-oaU\_ZTGXNe-zpXKIiTDM-uFXLTuImZXRA'

где:

192.168.111.100 – IP-адрес хоста eCA-CA;

e5291624-fac6-4d5f-ae7-d57be0372489 – идентификатор Центра сертификации (может быть

получен из URL карточки Центра сертификации);

[eyJhbGciOiJSUzUxMiJ9.eyJzZXNzaW9uSWQoIiI2Njc3NGU1ZS1jODkzLTRmOWQtODM4Yy1lMzQzZG](#)  
[Q1MGE3ZjUiLCJpYXQiOjE3MTAzMTIzODAsImV4cCI6MTcxMDMxMjU2MH0.MyyCqR89HeahIsnsn\\_vUXxeSqw](#)  
[FvLWRJUtpIkVMtbxq7BrzjGlcfFNJ9rEXx9jGKeSaTMbuwhmjX4aODGNPWCSFc18DUCqFA-85BTYgvGL5](#)  
[ns5kXfCe2WxmR7oPj-7XMAzBI98JydXkLEbmRx7F10teNW1ZY3JkwKvi9yFxbWrojB3yNq2ak39cvNj4AFKC](#)  
[EBF0nE8UxKPoyXKDXegC0xEv2UK8mhF7Um4od9B1LWLcuNqKExyqTGr1DDKJcYjoWBh49pQFAc3mG\\_bv7pBtT](#)  
[Y7\\_vwuVNAelBAqjlKum\\_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 Delta CRL необходимо использовать метод получения Delta CRL по идентификатору Центра сертификации (см. описание метода в документе «Центр сертификатов доступа Aladdin Enterprise Certificate Authority Certified Edition. Руководство администратора. Часть 3. Описание методов REST API «Центра сертификации Aladdin Enterprise Certification Authority»).

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/delta-crl' --header 'Cookie: token=eyJhbGciOiJSUzUxMiJ9.eyJzZXNzaW9uSWQiOiI2Njc3NGU1ZS1jODkzLTRmOWQtODM4Yy1lMzQzZGQ1MGE3ZjUiLCJpYXQiOiJlMzMTAzMTIzODAsImV4cCI6MTMtcxMDMxMjU2MH0.MyyCqR89HeahIsns_n_vUXxeSqwFVlWRJUtpIkVMTbxq7BrzjG1cjFNJ9rEXx9jGKeSaTMbuwhmjX4aODGnPWCSFc18DUCqFA-85BTYgvGL5ns5kXfCe2Wxmr7oPj-7XMAzBI98JydXkLEbmRx7F10teNW1ZY3JkwKvi9yFxbWrojB3yNq2ak39cvNj4AFKCEBF0nE8UxKPoyXKDXegC0xEv2UK8mhF7Um4od9B1LWlCuNqKEXyqTGr1DDKJcYjoWBh49pQFAC3mGbv7pBtTY7vwuVNAelBAqj1kUm_sCA1-gARBh-oaU_ZTGXNe-zpXKIiTDM-uFXLTuImZXRA'
```

где:

192.168.111.100 – IP-адрес хоста eCA-CA;

e5291624-fac6-4d5f-ae7-d57be0372489 – идентификатор Центра сертификации (может быть

получен из URL карточки ЦС)

eyJhbGciOiJSUzUxMiJ9.eyJzZXNzaW9uSWQiOiI2Njc3NGU1ZS1jODkzLTRmOWQtODM4Yy1lMzQzZGQ1MGE3ZjUiLCJpYXQiOiJEMTAzMTEzODAsImV4cCI6MTcxMDMxMjU2MH0.MyyCqR89HeahIsnsn\_vUXxeSqwFVlWRJUtpIkVMtbxq7BrzjG1cjFNJ9rEXx9jGKeSaTMbuwhmjX4aODGnPWCSFc18DUCqFA-85BTYgvGL5ns5kXfCe2Wxmr7oPj-7XMAZBI98JydXkLEbmRx7F10teNW1ZY3JkwKvi9yFxbWroJB3yNq2ak39cvNj4AFKCEBF0nE8UxKPoyXKDXegC0xEv2UK8mhF7Um4od9B1LWlCuNqKExyqTGr1DDKJcYjowBh49pQFAc3mG\_bv7pBtTY7\_vwuVNAelBAqjlKUm\_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 **ctrl**.

Для получения файла AIA необходимо использовать метод получения сертификата Центра сертификации по идентификатору Центра сертификации (см. описание метода в документе «Центр сертификатов доступа Aladdin Enterprise Certificate Authority Certified Edition. Руководство администратора. Часть 3. Описание методов REST API «Центра сертификации Aladdin Enterprise Certification Authority»).

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.eyJzZXNzaW9uSWQoI2Njc3NGU1ZS1jODkzLTRmOWQtODM4Yy1lMzQzZGQ1MGE3ZjUiLCJpYXQiOiE3M0ZMTAzMTIzODAsImV4cCI6MTcxMDMxMjU2MH0.MyyCqR89HeahIsnnsn_vUXxeSqwFVlWRJUtpIkVMTbxq7BrzjG1cjFNJ9rEXx9jGKeSaTMbuwhmjX4aODGnPWCSFc18DUCqFA-85BTYgvGL5ns5kXfCe2Wxmr7oPj-7XMAzBI98JydXkLEbmRx7F10tenNW1ZY3JkwKvi9yFxbWrojb3yNq2ak39cvNj4AFKCEBF0nE8UXKPoyXKDXegC0xEv2UK8mhF7Um4od9B1LW1CuNqKEXyqTGr1DDKJcYjowBh49pQFAC3mGbv7pBtTY7vwuVNAelBAqj1kUm_sCA1-gARBh-oaUZTGXNe-zpXKIiTDM-uFXLTuImZXRA'
```

где:

192.168.111.100 – IP–адрес хоста eCA-CA;

e5291624-fac6-4d5f-ae7-d57be0372489 – идентификатор Центра сертификации (может быть

получен из URL карточки Центра сертификации);

eyJhbGciOiJSUzUxMiJ9.eyJzZXNzaW9uSWQoI2Njc3NGU1ZS1jODkzLTRmOWQtODM4Yy1lMzQzZGQ1MGE3ZjU1LCJpYXQoIjE3MTAzMTIzODAsImV4cCI6MTcxMDMxMjU2MH0.MyyCQr89HeahIsnsn\_vUXxeSqwFV1WRJUtpIKvMTbxq7BrzjG1cjFNJ9rEXx9jGKeSaTMbuwhmjX4aODGnPWCSFc18DUCqFA-85BTYgvGL5ns5kXfCe2Wxmr7oPj-7XMAzBI98JydXkLEbmRx7F1OteNW1ZY3JkwKvi9yFxbWrojB3yNq2ak39cvNj4AFKCEBF0nE8UxKPoyXKDXegC0xEv2UK8mhF7Um4od9B1LWlCuNqKExyqTGr1DDKJcYjoWBh49pQFAc3mG\_bv7pBtTY7vuwVNAelBAqj1kUm\_sCA\_l-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».

### 8.9.9 Параметры точек распространения в сертификате

В создаваемых eCA-CA 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.

## 8.10 Журнал событий

### 8.10.1 Фиксируемые события

Фиксируемые в журнале события представлены в таблице 17.

Таблица 17 — Фиксируемые события

Причина, вызвавшая запись в журнал	Код события	Категория события	Содержание описания в журнале
Запуск службы	CAENV000	INFO	Описание: Запуск службы Атрибуты: – Название службы
Остановка службы	CAENV001	INFO	Описание: Остановка службы Атрибуты: – Название службы
Импорт лицензии	CAENV002	INFO	Описание: Импорт лицензии Атрибуты: – Срок действия – CN сертификата центра сертификации – CN сертификата корневого центра сертификации
Ошибка импорта лицензии	CAENV003	ERROR	Описание: Ошибка импорта лицензии Атрибуты: – Срок действия – CN сертификата центра сертификации – CN сертификата корневого центра сертификации – Причина ошибки
Проверка лицензии	CAENV004	INFO	Описание: Проверка лицензии Атрибуты: –
Ошибка проверки лицензии	CAENV005	ERROR	Описание: Ошибка проверки лицензии Атрибуты:

Причина, вызвавшая запись в журнал	Код события	Категория события	Содержание описания в журнале
			– Причина ошибки
Аутентификация пользователя	CAENV006	INFO	Описание: Аутентификация пользователя Атрибуты: – Id пользователя – Отображаемое имя пользователя – Роль пользователя – IP-адрес – Аутентификатор – Тип аутентификации
Ошибка аутентификации	CAENV007	ERROR	Описание: Ошибка аутентификации пользователя Атрибуты: – Id пользователя – Отображаемое имя пользователя – Роль пользователя – IP-адрес – Аутентификатор – Тип аутентификации – Причина ошибки
Активация центра сертификации	CAENV008	INFO	Описание: Активация центра сертификации Атрибуты: – CN сертификата центра сертификации – Subject Alternative Name сертификата центра сертификации
Ошибка активации центра сертификации	CAENV009	ERROR	Описание: Ошибка активации центра сертификации Атрибуты: – CN сертификата ЦС – Subject Alternative Name сертификата центра сертификации – Причина ошибки
Создание запроса на сертификат ЦС	CAENV010	INFO	Описание: Создание запроса на сертификат ЦС Атрибуты: – CN запроса – Subject Alternative Name запроса
Ошибка создания запроса на сертификат ЦС	CAENV011	ERROR	Описание: Ошибка создания запроса Атрибуты: – CN запроса – Subject Alternative Name запроса – Причина ошибки
Импорт сертификата центра сертификации	CAENV012	INFO	Описание: Импорт сертификата центра сертификации Атрибуты: – CN сертификата центра сертификации – CN сертификата корневого центра сертификации
Ошибка импорта сертификата центра сертификации	CAENV013	ERROR	Описание: Ошибка импорта сертификата центра сертификации Атрибуты: – CN сертификата центра сертификации – CN сертификата корневого центра сертификации – Причина ошибки

Причина, вызвавшая запись в журнал	Код события	Категория события	Содержание описания в журнале
Выпуск сертификата	CAENV014	INFO	Описание: Выпуск сертификата Атрибуты: – CN сертификата – Subject Alternative Name сертификата – Идентификатор шаблона – Вид операции – Сценарий – Контроль соответствия полей в сертификате атрибутам субъекта
Ошибка выпуска сертификата	CAENV015	ERROR	Описание: Ошибка выпуска сертификата Атрибуты: – CN сертификата – Subject Alternative Name сертификата – Идентификатор шаблона – Вид операции – Сценарий – Контроль соответствия полей в сертификате атрибутам субъекта – Причина ошибки
Регистрация центра валидации	CAENV016	INFO	Описание: Регистрация центра валидации Атрибуты: – Адрес центра валидации
Ошибка регистрации центра валидации	CAENV017	ERROR	Описание: Ошибка регистрации центра валидации Атрибуты: – Адрес центра валидации – Причина ошибки
Активация OCSP центра валидации	CAENV018	INFO	Описание: Активация OCSP центра валидации Атрибуты: – Адрес центра валидации
Ошибка активации OCSP центра валидации	CAENV019	ERROR	Описание: Ошибка активации OCSP центра валидации Атрибуты: – Причина ошибки
Изменение параметров обновления CRL	CAENV020	INFO	Описание: Изменение параметров обновления CRL Атрибуты: – Идентификатор центра сертификации – Отображаемое имя центра сертификации – Период действия CRL (может отсутствовать; будет присутствовать только при изменении данного параметра; исходное/конечное значение) – Период действия перекрытия (может отсутствовать; будет присутствовать только при изменении данного параметра; исходное/конечное значение) – Период действия Delta CRL (может отсутствовать; будет присутствовать только при изменении данного параметра; исходное/конечное значение) – Генерировать и публиковать новый CRL при изменении статусов сертификатов (может отсутствовать; будет присутствовать только при

Причина, вызвавшая запись в журнал	Код события	Категория события	Содержание описания в журнале
			изменении данного параметра; исходное/конечное значение)
Ошибка изменения параметров обновления CRL	CAENV021	ERROR	<p>Описание: Ошибка изменения параметров обновления CRL</p> <p>Атрибуты:</p> <ul style="list-style-type: none"> <li>– Идентификатор центра сертификации (может отсутствовать)</li> <li>– Отображаемое имя центра сертификации (может отсутствовать)</li> <li>– Период действия CRL (может отсутствовать)</li> <li>– Период действия перекрытия (может отсутствовать)</li> <li>– Период действия Delta CRL (может отсутствовать)</li> <li>– Генерировать и публиковать новый CRL при изменении статусов сертификатов (может отсутствовать)</li> <li>– Причина ошибки</li> </ul>
Публикация CRL	CAENV022	INFO	<p>Описание: Публикация CRL</p> <p>Атрибуты:</p> <ul style="list-style-type: none"> <li>– Номер CRL</li> <li>– Срок действия</li> <li>– Адрес точки публикации</li> <li>– Идентификатор центра сертификации</li> </ul>
Ошибка публикации CRL	CAENV023	ERROR	<p>Описание: Ошибка публикации CRL</p> <p>Атрибуты:</p> <ul style="list-style-type: none"> <li>– Номер CRL</li> <li>– Срок действия</li> <li>– Адрес точки публикации</li> <li>– Идентификатор центра сертификации</li> <li>– Причина ошибки</li> </ul>
Добавление ресурсной системы	CAENV024	INFO	<p>Описание: Добавление ресурсной системы</p> <p>Атрибуты:</p> <ul style="list-style-type: none"> <li>– Наименование ресурса</li> <li>– Тип ресурса</li> </ul>

Причина, вызвавшая запись в журнал	Код события	Категория события	Содержание описания в журнале
			<ul style="list-style-type: none"> <li>– IP-адрес</li> <li>– Точка подключения</li> </ul>
Ошибка добавления ресурсной системы	CAENV025	ERROR	<p>Описание: Ошибка добавления ресурсной системы</p> <p>Атрибуты:</p> <ul style="list-style-type: none"> <li>– Наименование ресурса</li> <li>– Тип ресурса</li> <li>– IP-адрес</li> <li>– Точка подключения</li> <li>– Причина ошибки</li> </ul>
Изменение ресурсной системы	CAENV026	INFO	<p>Описание: Изменение ресурсной системы</p> <p>Атрибуты:</p> <ul style="list-style-type: none"> <li>– наименование</li> <li>– тип</li> <li>– адрес</li> <li>– точка</li> <li>– служебный логин</li> </ul>
Ошибка изменения ресурсной системы	CAENV027	ERROR	<p>Описание: Ошибка изменения ресурсной системы</p> <p>Атрибуты:</p> <ul style="list-style-type: none"> <li>– наименование</li> <li>– тип</li> <li>– адрес</li> <li>– точка</li> <li>– служебный логин</li> <li>– Причина ошибки</li> </ul>
Синхронизация ресурса	CAENV028	INFO	<p>Описание: Синхронизация ресурса</p> <p>Атрибуты:</p> <ul style="list-style-type: none"> <li>– Наименование ресурса</li> <li>– Количество субъектов</li> </ul>
Ошибка синхронизации ресурса	CAENV029	ERROR	<p>Описание: Ошибка синхронизации ресурса</p> <p>Атрибуты:</p> <ul style="list-style-type: none"> <li>– Наименование ресурса</li> <li>– Количество субъектов</li> <li>– Причина ошибки</li> </ul>
Создание учетной записи	CAENV030	INFO	<p>Описание: Создание учетной записи</p> <p>Атрибуты:</p> <ul style="list-style-type: none"> <li>– Идентификатор</li> <li>– Отображаемое имя</li> <li>– Логин</li> <li>– Идентификатор связанного субъекта (может отсутствовать)</li> <li>– Роль</li> <li>– Статус</li> <li>– Тип учетной записи</li> </ul>
Ошибка создания учетной записи	CAENV031	ERROR	<p>Описание: Ошибка создания учетной записи</p> <p>Атрибуты:</p> <ul style="list-style-type: none"> <li>– Идентификатор (может отсутствовать)</li> <li>– Отображаемое имя (может отсутствовать)</li> <li>– Логин (может отсутствовать)</li> <li>– Идентификатор связанного субъекта (может отсутствовать)</li> <li>– Роль (может отсутствовать)</li> </ul>

Причина, вызвавшая запись в журнал	Код события	Категория события	Содержание описания в журнале
			<ul style="list-style-type: none"> <li>– Статус (может отсутствовать)</li> <li>– Тип учетной записи (может отсутствовать)</li> <li>– Причина ошибки</li> </ul>
Изменение учетной записи	CAENV032	INFO	<p>Описание: Изменение учетной записи</p> <p>Атрибуты:</p> <ul style="list-style-type: none"> <li>– Идентификатор</li> <li>– Отображаемое имя (может отсутствовать)</li> </ul> <p>Исходное значение/конечное значение</p> <ul style="list-style-type: none"> <li>– Логин</li> <li>– Идентификатор связанного субъекта</li> <li>– Роль (может отсутствовать). Исходное значение/конечное значение</li> <li>– Статус (может отсутствовать). Исходное значение/конечное значение</li> <li>– Тип учетной записи (может отсутствовать)</li> </ul>
Ошибка изменения учетной записи	CAENV033	ERROR	<p>Описание: Ошибка изменения учетной записи</p> <p>Атрибуты:</p> <ul style="list-style-type: none"> <li>– Идентификатор (может отсутствовать)</li> <li>– Отображаемое имя (может отсутствовать)</li> <li>– Логин (может отсутствовать)</li> <li>– Идентификатор связанного субъекта (может отсутствовать)</li> <li>– Роль (может отсутствовать)</li> <li>– Статус (может отсутствовать)</li> <li>– Тип учетной записи (может отсутствовать)</li> <li>– Причина ошибки</li> </ul>
Удаление учётной записи	CAENV034	INFO	<p>Описание: Удаление учетной записи</p> <p>Атрибуты:</p> <ul style="list-style-type: none"> <li>– Идентификатор</li> <li>– Отображаемое имя</li> <li>– Логин</li> <li>– Идентификатор связанного субъекта (может отсутствовать)</li> <li>– Роль</li> <li>– Статус</li> <li>– Тип учетной записи</li> </ul>
Ошибка удаления учётной записи	CAENV035	ERROR	<p>Описание: Ошибка удаления учетной записи</p> <p>Атрибуты:</p> <ul style="list-style-type: none"> <li>– Идентификатор (может отсутствовать)</li> <li>– Отображаемое имя (может отсутствовать)</li> <li>– Логин (может отсутствовать)</li> <li>– Идентификатор связанного субъекта (может отсутствовать)</li> <li>– Роль (может отсутствовать)</li> <li>– Статус (может отсутствовать)</li> <li>– Тип учетной записи (может отсутствовать)</li> <li>– Причина ошибки</li> </ul>
Установка сертификата веб-сервера	CAENV036	INFO	<p>Описание: Установка сертификата веб-сервера</p> <p>Атрибуты:</p> <ul style="list-style-type: none"> <li>– Серийный номер сертификата</li> </ul>

Причина, вызвавшая запись в журнал	Код события	Категория события	Содержание описания в журнале
			<ul style="list-style-type: none"> <li>– CN в сертификате</li> <li>– SDN издателя</li> <li>– Действует с</li> <li>– Действует по</li> </ul>
Ошибка установки сертификата веб-сервера	CAENV037	ERROR	<p>Описание: Ошибка установки сертификата веб-сервера</p> <p>Атрибуты:</p> <ul style="list-style-type: none"> <li>– Серийный номер сертификата (может отсутствовать)</li> <li>– CN в сертификате (может отсутствовать)</li> <li>– SDN издателя (может отсутствовать)</li> <li>– Действует с (может отсутствовать)</li> <li>– Действует по (может отсутствовать)</li> <li>– Причина ошибки</li> </ul>
Изменение списка разрешённых издателей	CAENV038	INFO	<p>Описание: Изменение списка разрешённых издателей</p> <p>Атрибуты:</p> <ul style="list-style-type: none"> <li>– Список идентификаторов активных издателей (Исходное значение; Конечное значение)</li> </ul>
Ошибка изменения списка разрешённых издателей	CAENV039	ERROR	<p>Описание: Ошибка изменения списка разрешённых издателей</p> <p>Атрибуты:</p> <ul style="list-style-type: none"> <li>– имя издателя</li> <li>– ” добавлен” или ”удален”</li> <li>– Причина ошибки</li> </ul>
Подключение к ключевому носителю	CAENV042	INFO	<p>Описание: Подключение к ключевому носителю</p> <p>Атрибуты:</p> <ul style="list-style-type: none"> <li>– Маркировка носителя</li> </ul>
Ошибка подключения к ключевому носителю	CAENV043	ERROR	<p>Описание: Ошибка подключения к ключевому носителю</p> <p>Атрибуты:</p> <ul style="list-style-type: none"> <li>– Маркировка носителя</li> <li>– Причина ошибки</li> </ul>
Создание контейнера на ключевом носителе	CAENV044	INFO	<p>Описание: Создание контейнера на ключевом носителе</p> <p>Атрибуты:</p> <ul style="list-style-type: none"> <li>– Маркировка носителя</li> </ul>
Ошибка создания контейнера на ключевом носителе	CAENV045	ERROR	<p>Описание: Ошибка создания контейнера на ключевом носителе</p> <p>Атрибуты:</p> <ul style="list-style-type: none"> <li>– Маркировка носителя</li> <li>– Причина ошибки</li> </ul>
Запись сертификата на ключевой носитель	CAENV046	INFO	<p>Описание: Запись сертификата на ключевой носитель</p> <p>Атрибуты:</p> <ul style="list-style-type: none"> <li>– Маркировка носителя</li> </ul>
Ошибка записи сертификата на ключевой носитель	CAENV047	ERROR	<p>Описание: Ошибка записи сертификата на ключевой носитель</p> <p>Атрибуты:</p> <ul style="list-style-type: none"> <li>– маркировка носителя</li> <li>– ID-сертификата</li> </ul>

Причина, вызвавшая запись в журнал	Код события	Категория события	Содержание описания в журнале
			– Причина ошибки
Публикация сертификата в ресурсную систему	CAENV048	INFO	Описание: Публикация сертификата в ресурсную систему Атрибуты: – Идентификатор субъекта – DN субъекта – Идентификатор PC – Отображаемое имя ресурсной системы – Серийный номер сертификата
Ошибка публикации сертификата в ресурсную систему	CAENV049	ERROR	Описание: Ошибка публикации сертификата в ресурсную систему Атрибуты: – Идентификатор субъекта – DN субъекта – Идентификатор PC – Отображаемое имя ресурсной системы – Серийный номер сертификата – Причина ошибки
Сохранение журнала в CSV	CAENV050	INFO	Описание: Сохранение журнала в CSV Атрибуты: – Фильтр: дата и время фиксации события (начиная с указанной включительно) – Фильтр: дата и время фиксации события (до включительно) – Фильтр: категории события (полное соответствие) – Фильтр: учётные записи (полное соответствие) – Фильтр: системные события
Ошибка сохранения журнала в CSV	CAENV051	ERROR	Описание: Ошибка сохранения журнала в CSV Атрибуты: – фильтр – Причина ошибки
Генерация CRL	CAENV052	INFO	Описание: Генерация CRL Атрибуты: – Идентификатор центра сертификации – Отображаемое имя центра сертификации – Номер CRL – Срок действия CRL
Ошибка генерации CRL	CAENV053	ERROR	Описание: Ошибка генерации CRL Атрибуты: – Идентификатор центра сертификации (может отсутствовать) – Отображаемое имя центра сертификации (может отсутствовать) – Номер CRL (может отсутствовать) – Срок действия CRL (может отсутствовать) – Причина ошибки
Отправка уведомления на почту	CAENV054	INFO	Описание: Отправка уведомления на почту Атрибуты: – CN

Причина, вызвавшая запись в журнал	Код события	Категория события	Содержание описания в журнале
			– Email – Шаблон
Ошибка отправки уведомления на почту	CAENV055	ERROR	Описание: Ошибка отправки уведомления на почту Атрибуты: – CN – Email – Шаблон – Причина ошибки
Отзыв сертификата	CAENV056	INFO	Описание: Отзыв сертификата Атрибуты: – Серийный номер сертификата – Идентификатор сертификата – Код причины отзыва – Причина отзыва
Приостановка сертификата	CAENV057	INFO	Описание: Приостановка сертификата Атрибуты: – Серийный номер сертификата – Идентификатор сертификата – Код причины отзыва – Причина отзыва
Реактивация сертификата	CAENV058	INFO	Описание: Реактивация сертификата Атрибуты: – Серийный номер сертификата – Идентификатор сертификата – Код причины отзыва – Причина отзыва
Начало удаления центра сертификации	CAENV059	INFO	Описание: Начало удаления центра сертификации Атрибуты: – CN сертификата центра сертификации – CN сертификата корневого центра сертификации – Subject Alternative Name сертификата центра сертификации
Окончание удаления центра сертификации	CAENV060	INFO	Описание: Окончание удаления центра сертификации Атрибуты: – CN сертификата центра сертификации – CN сертификата корневого центра сертификации – Subject Alternative Name сертификата центра сертификации
Ошибка удаления центра сертификации	CAENV061	ERROR	Описание: Ошибка удаления центра сертификации Атрибуты: – CN сертификата центра сертификации – CN сертификата корневого центра сертификации – Subject Alternative Name сертификата центра сертификации – Причина ошибки
Начало очистки журнала событий	CAENV064	INFO	Описание: Начало очистки журнала событий Атрибуты: –
Окончание очистки журнала событий	CAENV065	INFO	Описание: Окончание очистки журнала событий Атрибуты: –

Причина, вызвавшая запись в журнал	Код события	Категория события	Содержание описания в журнале
Ошибка очистки журнала события	CAENV066	ERROR	Описание: Ошибка очистки журнала события Атрибуты: – фильтр – Причина ошибки
Начало архивации журнала событий	CAENV067	INFO	Описание: Начало архивации журнала событий Атрибуты: –
Окончание архивации журнала событий	CAENV068	INFO	Описание: Окончание архивации журнала событий Атрибуты: –
Ошибка архивации журнала события	CAENV069	ERROR	Описание: Ошибка архивации журнала события Атрибуты: – фильтр – Причина ошибки
Успешная проверка целостности исполняемых файлов	CAENV074	INFO	Описание: Успешная проверка целостности исполняемых файлов Атрибуты: -
Неуспешная проверка целостности исполняемых файлов	CAENV075	ERROR	Описание: Неуспешная проверка целостности исполняемых файлов Атрибуты: – Файл с ошибкой КС – Причина ошибки
Распаковка ключей ЦС	CAENV076	INFO	Описание: Распаковка ключей ЦС Атрибуты: – Идентификатор центра сертификации
Ошибка при распаковке ключей ЦС	CAENV077	ERROR	Описание: Ошибка при распаковке ключей ЦС Атрибуты: – Идентификатор центра сертификации – Причина ошибки
Скачан контейнер PKCS#12	CAENV078	INFO	Описание: Скачан контейнер PKCS#12 Атрибуты: – Серийный номер сертификата в контейнере
Скачан сертификат	CAENV079	INFO	Описание: Скачан сертификат Атрибуты: – Идентификатор сертификата – Серийный номер сертификата – CN в сертификате
Скачана цепочка сертификатов	CAENV080	INFO	Описание: Скачана цепочка сертификата Атрибуты: –
Экспорт запроса на сертификат ЦС	CAENV081	INFO	Описание: Экспорт запроса на сертификат ЦС Атрибуты: – Идентификатор сертификата
Ошибка экспорта запроса на сертификат ЦС	CAENV082	ERROR	Описание: Ошибка экспорта запроса на сертификат ЦС Атрибуты: – Причина ошибки

Причина, вызвавшая запись в журнал	Код события	Категория события	Содержание описания в журнале
Ошибка экспорта контейнера PKCS#12	CAENV085	ERROR	Описание: Ошибка экспорта контейнера PKCS#12 Атрибуты: – Серийный номер сертификата в контейнере – Причина ошибки
Успешное создание резервной копии	CAENV086	INFO	Описание: Успешное создание резервной копии Атрибуты: – Путь к созданной резервной копии – Наличие БД в резервной копии
Ошибка создания резервной копии	CAENV087	ERROR	Описание: Ошибка создания резервной копии Атрибуты: – Причина ошибки
Успешное восстановление из резервной копии	CAENV088	INFO	Описание: Успешное восстановление из резервной копии Атрибуты: – Путь к использованной резервной копии – Восстановление БД
Ошибка восстановления из резервной копии	CAENV089	ERROR	Описание: Ошибка восстановления из резервной копии Атрибуты: – Причина ошибки
Ошибка синхронизации субъекта	CAENV090	ERROR	Описание: Ошибка синхронизации субъекта Атрибуты: – Идентификатор субъекта – DN субъекта – Идентификатор PC – Причина ошибки
Создание правила доступа	CAENV091	INFO	Описание: Создание правила доступа Атрибуты: – Категория правила доступа – Субъекты правила доступа – Объекты правила доступа – Операции правила доступа
Ошибка создания правила доступа	CAENV092	ERROR	Описание: Ошибка создания правила доступа Атрибуты: – Причина ошибки
Редактирование правила доступа	CAENV093	INFO	Описание: Редактирование правила доступа Атрибуты: – Субъекты правила доступа (Исходное значение; Конечное значение) – Объекты правила доступа (Исходное значение; Конечное значение) – Операции правила доступа (Исходное значение; Конечное значение)
Ошибка изменения правила доступа	CAENV094	ERROR	Описание: Ошибка изменения правила доступа Атрибуты: – Субъекты правила доступа – Объекты правила доступа – Операции правила доступа – Причина ошибки

Причина, вызвавшая запись в журнал	Код события	Категория события	Содержание описания в журнале
Удаление правила доступа	CAENV095	INFO	Описание: Удаление правила доступа Атрибуты: – Категория правила доступа: категория правила доступа, – Субъекты правила доступа – Объекты правила доступа – Операции правила доступа
Ошибка удаления правила доступа	CAENV096	ERROR	Описание: Ошибка удаления правила доступа Атрибуты: – Причина ошибки
Добавление Syslog-сервера	CAENV097	INFO	Описание: Добавление Syslog-сервера Атрибуты: – Хост – Порт – Протокол – Флаг отправки сообщения
Ошибка добавления Syslog-сервера	CAENV098	ERROR	Описание: Ошибка добавления Syslog-сервера Атрибуты: – Хост (может отсутствовать) – Порт (может отсутствовать) – Протокол (может отсутствовать) – Флаг отправки сообщения (может отсутствовать) – Причина ошибки
Изменение параметров Syslog-сервера	CAENV099	INFO	Описание: Изменение параметров Syslog-сервера Атрибуты: – Хост (может отсутствовать; исходное/конечное значение) – Порт (может отсутствовать; исходное/конечное значение) – Протокол (может отсутствовать; исходное/конечное значение) – Флаг отправки сообщения (может отсутствовать; исходное/конечное значение)
Ошибка изменения параметров Syslog-сервера	CAENV100	ERROR	Описание: Ошибка изменения параметров Syslog-сервера Атрибуты: – Хост (может отсутствовать; исходное/конечное значение) – Порт (может отсутствовать; исходное/конечное значение) – Протокол (может отсутствовать; исходное/конечное значение) – Флаг отправки сообщения (может отсутствовать; исходное/конечное значение) – Причина ошибки
Удаление Syslog-сервера	CAENV101	INFO	Описание: Удаление Syslog-сервера Атрибуты: – Хост – Порт – Протокол

Причина, вызвавшая запись в журнал	Код события	Категория события	Содержание описания в журнале
			– Флаг отправки сообщения
Ошибка удаления Syslog-сервера	CAENV102	ERROR	Описание: Ошибка удаления Syslog-сервера Атрибуты: – Хост (может отсутствовать) – Порт (может отсутствовать) – Протокол (может отсутствовать) – Флаг отправки сообщения (может отсутствовать) – Причина ошибки
Создание корневого ЦС	CAENV103	INFO	Описание: Создание корневого ЦС Атрибуты: – Отображаемое имя центра сертификации – CN корневого центра сертификации – Конфигурация криптопровайдеров центра сертификации – Срок действия – Алгоритм ключа – Длина ключа – Алгоритм хэш-суммы – Место хранения закрытого ключа
Ошибка создания корневого ЦС	CAENV104	ERROR	Описание: Ошибка создания корневого ЦС Атрибуты: – Отображаемое имя центра сертификации – Имя центра сертификации – Причина ошибки
Создание Подчинённого ЦС	CAENV105	INFO	Описание: Создание Подчинённого ЦС Атрибуты: – Отображаемое имя центра сертификации – CN запроса – Конфигурация криптопровайдеров – Срок действия – Алгоритм ключа – Длина ключа – Алгоритм хэш-суммы – Место хранения закрытого ключа
Ошибка создания Подчинённого ЦС	CAENV106	ERROR	Описание: Ошибка создания Подчинённого ЦС Атрибуты: – Отображаемое имя центра сертификации – Имя центра сертификации – Причина ошибки
Экспорт закрытого ключа ЦС	CAENV107	INFO	Описание: Экспорт закрытого ключа ЦС Атрибуты: – Идентификатор центра сертификации – Отображаемое имя центра сертификации – CN сертификата центра сертификации – Экспортирован из хранилища
Ошибка экспорта закрытого ключа ЦС	CAENV108	ERROR	Описание: Ошибка экспорта закрытого ключа ЦС Атрибуты: – Идентификатор центра сертификации – Отображаемое имя центра сертификации – Имя центра сертификации

Причина, вызвавшая запись в журнал	Код события	Категория события	Содержание описания в журнале
			– Хранилище – Причина ошибки
Скачан закрытый ключ ЦС	CAENV109	INFO	Описание: Скачан закрытый ключ ЦС Атрибуты: – Идентификатор центра сертификации – Отображаемое имя центра сертификации – CN сертификата центра сертификации
Ошибка скачивания закрытого ключа ЦС	CAENV110	ERROR	Описание: Ошибка скачивания закрытого ключа ЦС Атрибуты: – Идентификатор центра сертификации – Отображаемое имя центра сертификации – CN сертификата центра сертификации – Причина ошибки
Импорт закрытого ключа ЦС	CAENV111	INFO	Описание: Импорт закрытого ключа ЦС Атрибуты: – Идентификатор центра сертификации – Отображаемое имя центра сертификации – CN сертификат центра сертификации – Импортирован в хранилище
Ошибка импорта закрытого ключа ЦС	CAENV112	ERROR	Описание: Ошибка импорта закрытого ключа ЦС Атрибуты: – Идентификатор центра сертификации – Отображаемое имя центра сертификации – CN сертификата центра сертификации – Место хранения закрытого ключа – Причина ошибки
Создание ключевой пары	CAENV113	INFO	Описание: Создание ключевой пары Атрибуты: – Тип владельца – ID владельца – Алгоритм ключа – Длина ключа – Криптопровайдер – Место хранения закрытого ключа – Экспортируемость
Ошибка создания ключевой пары	CAENV114	ERROR	Описание: Ошибка создания ключевой пары Атрибуты: – Тип владельца (может отсутствовать) – ID владельца (может отсутствовать) – Алгоритм ключа (может отсутствовать) – Длина ключа (может отсутствовать) – Криптопровайдер (может отсутствовать) – Место хранения закрытого ключа (может отсутствовать) – Экспортируемость (может отсутствовать) – Причина ошибки
Удаление закрытого ключа ЦС	CAENV115	INFO	Описание: Удаление закрытого ключа ЦС Атрибуты: – Идентификатор центра сертификации

Причина, вызвавшая запись в журнал	Код события	Категория события	Содержание описания в журнале
			<ul style="list-style-type: none"> <li>– Отображаемое имя центра сертификации</li> <li>– CN центра сертификации</li> <li>– Место хранения закрытого ключа</li> </ul>
Ошибка удаления закрытого ключа ЦС	CAENV116	ERROR	<p>Описание: Ошибка удаления закрытого ключа ЦС</p> <p>Атрибуты:</p> <ul style="list-style-type: none"> <li>– Идентификатор центра сертификации (может отсутствовать)</li> <li>– Отображаемое имя центра сертификации (может отсутствовать)</li> <li>– CN центра сертификации (может отсутствовать)</li> <li>– Место хранения закрытого ключа (может отсутствовать)</li> <li>– Причина ошибки</li> </ul>
Создание корневого ЦС на основании контейнера PKCS#12	CAENV117	INFO	<p>Описание: Создание корневого ЦС на основании контейнера PKCS#12</p> <p>Атрибуты:</p> <ul style="list-style-type: none"> <li>– Отображаемое имя центра сертификации</li> <li>– CN центра сертификации</li> <li>– Конфигурация криптопровайдеров центра сертификации</li> <li>– Срок действия</li> <li>– Алгоритм ключа</li> <li>– Длина ключа</li> <li>– Алгоритм хэш-суммы</li> <li>– Место хранения закрытого ключа</li> </ul>
Ошибка создания корневого ЦС на основании контейнера PKCS#12	CAENV118	ERROR	<p>Описание: Ошибка создания корневого ЦС на основании контейнера PKCS#12</p> <p>Атрибуты:</p> <ul style="list-style-type: none"> <li>– Отображаемое имя центра сертификации (может отсутствовать)</li> <li>– CN центра сертификации (может отсутствовать)</li> <li>– Конфигурация криптопровайдеров центра сертификации (может отсутствовать)</li> <li>– Срок действия (может отсутствовать)</li> <li>– Алгоритм ключа (может отсутствовать)</li> <li>– Длина ключа (может отсутствовать)</li> <li>– Алгоритм хэш-суммы (может отсутствовать)</li> <li>– Место хранения закрытого ключа (может отсутствовать)</li> <li>– Причина ошибки</li> </ul>
Создание Подчинённого ЦС на основании контейнера PKCS#12	CAENV119	INFO	<p>Описание: Создание Подчинённого ЦС на основании контейнера PKCS#12</p> <p>Атрибуты:</p> <ul style="list-style-type: none"> <li>– Отображаемое имя центра сертификации</li> <li>– CN центра сертификации</li> <li>– Конфигурация криптопровайдеров центра сертификации</li> <li>– Срок действия</li> <li>– Алгоритм ключа</li> <li>– Длина ключа</li> </ul>

Причина, вызвавшая запись в журнал	Код события	Категория события	Содержание описания в журнале
			<ul style="list-style-type: none"> <li>– Алгоритм хэш-суммы</li> <li>– Место хранения закрытого ключа</li> </ul>
Ошибка создания Подчинённого ЦС на основании контейнера PKCS#12	CAENV120	ERROR	<p>Описание: Ошибка создания Подчинённого ЦС на основании контейнера PKCS#12</p> <p>Атрибуты:</p> <ul style="list-style-type: none"> <li>– Отображаемое имя центра сертификации (может отсутствовать)</li> <li>– CN центра сертификации (может отсутствовать)</li> <li>– Конфигурация криптопровайдеров центра сертификации (может отсутствовать)</li> <li>– Срок действия (может отсутствовать)</li> <li>– Алгоритм ключа (может отсутствовать)</li> <li>– Длина ключа (может отсутствовать)</li> <li>– Алгоритм хэш-суммы (может отсутствовать)</li> <li>– Место хранения закрытого ключа (может отсутствовать)</li> <li>– Причина ошибки</li> </ul>
Создание шаблона сертификата	CAENV121	INFO	<p>Описание: Создание шаблона сертификата</p> <p>Атрибуты:</p> <ul style="list-style-type: none"> <li>– Идентификатор шаблона</li> <li>– Наименование шаблона</li> <li>– Период действия сертификата</li> <li>– Центр сертификации</li> <li>– Тип субъекта</li> <li>– Опубликовать сертификат в ресурсную систему</li> <li>– Минимальная длина ключа RSA (может отсутствовать)</li> <li>– Минимальная длина ключа ECDSA (может отсутствовать)</li> <li>– Минимальная длина ключа ГОСТ Р 34.10-2012 (может отсутствовать)</li> <li>– Использование ключа</li> <li>– Считать критическим использование ключа</li> <li>– Расширенное использование ключа</li> <li>– Считать критическим расширенное использование ключа</li> <li>– Включать SID субъекта в сертификат</li> <li>– OID политики сертификата</li> <li>– Считать критическими OID политики сертификата</li> <li>– Политики выпуска PKCS#12</li> <li>– Включать сведения о средствах ЭП и УЦ издателя</li> <li>– Наименование средства ЭП (может отсутствовать, если в создаваемом шаблоне выключен чекбокс «Включать сведения о средствах ЭП и УЦ издателя»)</li> <li>– Реквизиты заключения о подтверждении соответствия средства ЭП (может отсутствовать, если в создаваемом шаблоне выключен чекбокс</li> </ul>

Причина, вызвавшая запись в журнал	Код события	Категория события	Содержание описания в журнале
			<p>«Включать сведения о средствах ЭП и УЦ издателя»)</p> <ul style="list-style-type: none"> <li>– Наименование средства УЦ (может отсутствовать, если в создаваемом шаблоне выключен чекбокс «Включать сведения о средствах ЭП и УЦ издателя»)</li> <li>– Реквизиты заключения о подтверждении соответствия средства УЦ (может отсутствовать, если в создаваемом шаблоне выключен чекбокс «Включать сведения о средствах ЭП и УЦ издателя»)</li> <li>– Включать сведения о средстве ЭП владельца сертификата</li> <li>– Используемое средство ЭП (может отсутствовать, если в создаваемом шаблоне выключен чекбокс «Включать сведения о средстве ЭП владельца сертификата»)</li> <li>– Отличительное имя субъекта</li> <li>– Альтернативное имя субъекта</li> <li>– Контроль соответствия полей в сертификате атрибутам субъекта</li> <li>– Короткоживущий (short-lived, throwaway) сертификат</li> </ul>
Ошибка создания шаблона сертификата	CAENV122	ERROR	<p>Описание: Ошибка создания шаблона сертификата</p> <p>Атрибуты:</p> <ul style="list-style-type: none"> <li>– Идентификатор шаблона (может отсутствовать)</li> <li>– Наименование шаблона (может отсутствовать)</li> <li>– Период действия сертификата (может отсутствовать)</li> <li>– Центр сертификации (может отсутствовать)</li> <li>– Тип субъекта (может отсутствовать)</li> <li>– Публиковать сертификат в ресурсную систему (может отсутствовать)</li> <li>– Минимальная длина ключа RSA (может отсутствовать)</li> <li>– Минимальная длина ключа ECDSA (может отсутствовать)</li> <li>– Минимальная длина ключа ГОСТ Р 34.10-2012 (может отсутствовать)</li> <li>– Использование ключа (может отсутствовать)</li> <li>– Считать критическим использование ключа (может отсутствовать)</li> <li>– Расширенное использование ключа (может отсутствовать)</li> <li>– Считать критическим расширенное использование ключа (может отсутствовать)</li> <li>– Включать SID субъекта в сертификат (может отсутствовать)</li> <li>– OID политики сертификата (может отсутствовать)</li> </ul>

Причина, вызвавшая запись в журнал	Код события	Категория события	Содержание описания в журнале
			<ul style="list-style-type: none"> <li>– Считать критическими OID политики сертификата (может отсутствовать)</li> <li>– Политики выпуска PKCS#12 (может отсутствовать)</li> <li>– Включать сведения о средствах ЭП и УЦ издателя</li> <li>– Наименование средства ЭП (может отсутствовать, если в создаваемом шаблоне выключен чекбокс «Включать сведения о средствах ЭП и УЦ издателя»)</li> <li>– Реквизиты заключения о подтверждении соответствия средства ЭП (может отсутствовать, если в создаваемом шаблоне выключен чекбокс «Включать сведения о средствах ЭП и УЦ издателя»)</li> <li>– Наименование средства УЦ (может отсутствовать, если в создаваемом шаблоне выключен чекбокс «Включать сведения о средствах ЭП и УЦ издателя»)</li> <li>– Реквизиты заключения о подтверждении соответствия средства УЦ (может отсутствовать, если в создаваемом шаблоне выключен чекбокс «Включать сведения о средствах ЭП и УЦ издателя»)</li> <li>– Включать сведения о средстве ЭП владельца сертификата</li> <li>– Используемое средство ЭП (может отсутствовать, если в создаваемом шаблоне выключен чекбокс «Включать сведения о средстве ЭП владельца сертификата»)</li> <li>– Отличительное имя субъекта (может отсутствовать)</li> <li>– Альтернативное имя субъекта (может отсутствовать)</li> <li>– Контроль соответствия полей в сертификате атрибутам субъекта (может отсутствовать)</li> <li>– Короткоживущий (short-lived, throwaway) сертификат (может отсутствовать)</li> <li>– Причина ошибки</li> </ul>
Изменение шаблона сертификата	CAENV123	INFO	<p>Описание: Изменение шаблона сертификата</p> <p>Атрибуты:</p> <ul style="list-style-type: none"> <li>– Идентификатор шаблона</li> <li>– Наименование шаблона (может отсутствовать, если данный параметр шаблона не менялся; для параметра указано исходное и конечное значение)</li> <li>– Период действия сертификата (может отсутствовать, если данный параметр шаблона не менялся; для параметра указано исходное и конечное значения)</li> </ul>

Причина, вызвавшая запись в журнал	Код события	Категория события	Содержание описания в журнале
			<ul style="list-style-type: none"> <li>– Центр сертификации (может отсутствовать, если данный параметр шаблона не менялся; для параметра указано исходное и конечное значения)</li> <li>– Тип субъекта (может отсутствовать, если данный параметр шаблона не менялся; для параметра указано исходное и конечное значения)</li> <li>– Опубликовать сертификат в ресурсную систему (может отсутствовать, если данный параметр шаблона не менялся; для параметра указано исходное и конечное значения)</li> <li>– Минимальная длина ключа RSA (может отсутствовать, если данный параметр шаблона не менялся; для параметра указано исходное и конечное значения)</li> <li>– Минимальная длина ключа ECDSA (может отсутствовать, если данный параметр шаблона не менялся; для параметра указано исходное и конечное значения)</li> <li>– Минимальная длина ключа ГОСТ Р 34.10-2012 (может отсутствовать, если данный параметр шаблона не менялся; для параметра указано исходное и конечное значения)</li> <li>– Использование ключа (может отсутствовать, если данный параметр шаблона не менялся; для параметра указано исходное и конечное значения)</li> <li>– Считать критическим использование ключа (может отсутствовать, если данный параметр шаблона не менялся; для параметра указано исходное и конечное значения)</li> <li>– Расширенное использование ключа (может отсутствовать, если данный параметр шаблона не менялся; для параметра указано исходное и конечное значения)</li> <li>– Считать критическим расширенное использование ключа (может отсутствовать, если данный параметр шаблона не менялся; для параметра указано исходное и конечное значения)</li> <li>– Включать SID субъекта в сертификат (может отсутствовать, если данный параметр шаблона не менялся; для параметра указано исходное и конечное значения)</li> <li>– OID политики сертификата (может отсутствовать, если данный параметр шаблона не менялся; для параметра указано исходное и конечное значения)</li> <li>– Считать критическими OID политики сертификата (может отсутствовать, если данный параметр шаблона не менялся; для параметра указано исходное и конечное значения)</li> <li>– Политики выпуска PKCS#12 (может отсутствовать, если данный параметр шаблона не</li> </ul>

Причина, вызвавшая запись в журнал	Код события	Категория события	Содержание описания в журнале
			<p>менялся; для параметра указано исходное и конечное значения)</p> <p>– Включать сведения о средствах ЭП и УЦ издателя (может отсутствовать, если данный параметр шаблона не менялся; для параметра указано исходное и конечное значения)</p> <p>– Наименование средства ЭП (может отсутствовать, если данный параметр шаблона не менялся; для параметра указано исходное и конечное значения)</p> <p>– Реквизиты заключения о подтверждении соответствия средства ЭП (может отсутствовать, если данный параметр шаблона не менялся; для параметра указано исходное и конечное значения)</p> <p>– Наименование средства УЦ (может отсутствовать, если данный параметр шаблона не менялся; для параметра указано исходное и конечное значения)</p> <p>– Реквизиты заключения о подтверждении соответствия средства УЦ (может отсутствовать, если данный параметр шаблона не менялся; для параметра указано исходное и конечное значения)</p> <p>– Включать сведения о средстве ЭП владельца сертификата (может отсутствовать, если данный параметр шаблона не менялся; для параметра указано исходное и конечное значения)</p> <p>– Используемое средство ЭП (может отсутствовать, если данный параметр шаблона не менялся; для параметра указано исходное и конечное значения)</p> <p>– Отличительное имя субъекта (может отсутствовать, если данный параметр шаблона не менялся; для параметра указано исходное и конечное значения)</p> <p>– Альтернативное имя субъекта (может отсутствовать, если данный параметр шаблона не менялся; для параметра указано исходное и конечное значения)</p> <p>– Контроль соответствия полей в сертификате атрибутам субъекта (может отсутствовать, если данный параметр шаблона не менялся; для параметра указано исходное и конечное значения)</p> <p>– Короткоживущий (short-lived, throwaway) сертификат (может отсутствовать, если данный параметр шаблона не менялся; для параметра указано исходное и конечное значения)</p>
Ошибка изменения шаблона сертификата	CAENV124	ERROR	<p>Описание: Ошибка изменения шаблона сертификата</p> <p>Атрибуты:</p> <p>– Идентификатор шаблона</p>

Причина, вызвавшая запись в журнал	Код события	Категория события	Содержание описания в журнале
			<ul style="list-style-type: none"> <li>– Наименование шаблона (может отсутствовать, если данный параметр шаблона не менялся; для параметра указано исходное и конечное значения)</li> <li>– Период действия сертификата (может отсутствовать, если данный параметр шаблона не менялся; для параметра указано исходное и конечное значения)</li> <li>– Центр сертификации (может отсутствовать, если данный параметр шаблона не менялся; для параметра указано исходное и конечное значения)</li> <li>– Тип субъекта (может отсутствовать, если данный параметр шаблона не менялся; для параметра указано исходное и конечное значения)</li> <li>– Публиковать сертификат в ресурсную систему (может отсутствовать, если данный параметр шаблона не менялся; для параметра указано исходное и конечное значения)</li> <li>– Минимальная длина ключа RSA (может отсутствовать, если данный параметр шаблона не менялся; для параметра указано исходное и конечное значения)</li> <li>– Минимальная длина ключа ECDSA (может отсутствовать, если данный параметр шаблона не менялся; для параметра указано исходное и конечное значения)</li> <li>– Минимальная длина ключа ГОСТ Р 34.10-2012 (может отсутствовать, если данный параметр шаблона не менялся; для параметра указано исходное и конечное значения)</li> <li>– Использование ключа (может отсутствовать, если данный параметр шаблона не менялся; для параметра указано исходное и конечное значения)</li> <li>– Считать критическим использование ключа (может отсутствовать, если данный параметр шаблона не менялся; для параметра указано исходное и конечное значения)</li> <li>– Расширенное использование ключа (может отсутствовать, если данный параметр шаблона не менялся; для параметра указано исходное и конечное значения)</li> <li>– Считать критическим расширенное использование ключа (может отсутствовать, если данный параметр шаблона не менялся; для параметра указано исходное и конечное значения)</li> <li>– Включать SID субъекта в сертификат (может отсутствовать, если данный параметр шаблона не менялся; для параметра указано исходное и конечное значения)</li> <li>– OID политики сертификата (может отсутствовать, если данный параметр шаблона не</li> </ul>

Причина, вызвавшая запись в журнал	Код события	Категория события	Содержание описания в журнале
			<p>менялся; для параметра указано исходное и конечное значения)</p> <ul style="list-style-type: none"> <li>– Считать критическими OID политики сертификата (может отсутствовать, если данный параметр шаблона не менялся; для параметра указано исходное и конечное значения)</li> <li>– Политики выпуска PKCS#12 (может отсутствовать, если данный параметр шаблона не менялся; для параметра указано исходное и конечное значения)</li> <li>– Включать сведения о средствах ЭП и УЦ издателя (может отсутствовать, если данный параметр шаблона не менялся; для параметра указано исходное и конечное значения)</li> <li>– Наименование средства ЭП (может отсутствовать, если данный параметр шаблона не менялся; для параметра указано исходное и конечное значения)</li> <li>– Реквизиты заключения о подтверждении соответствия средства ЭП (может отсутствовать, если данный параметр шаблона не менялся; для параметра указано исходное и конечное значения)</li> <li>– Наименование средства УЦ (может отсутствовать, если данный параметр шаблона не менялся; для параметра указано исходное и конечное значения)</li> <li>– Реквизиты заключения о подтверждении соответствия средства УЦ (может отсутствовать, если данный параметр шаблона не менялся; для параметра указано исходное и конечное значения)</li> <li>– Включать сведения о средстве ЭП владельца сертификата (может отсутствовать, если данный параметр шаблона не менялся; для параметра указано исходное и конечное значения)</li> <li>– Используемое средство ЭП (может отсутствовать, если данный параметр шаблона не менялся; для параметра указано исходное и конечное значения)</li> <li>– Отличительное имя субъекта (может отсутствовать, если данный параметр шаблона не менялся; для параметра указано исходное и конечное значения)</li> <li>– Альтернативное имя субъекта (может отсутствовать, если данный параметр шаблона не менялся; для параметра указано исходное и конечное значения)</li> <li>– Контроль соответствия полей в сертификате атрибутам субъекта (может отсутствовать, если данный параметр шаблона не менялся; для параметра указано исходное и конечное значения)</li> </ul>

Причина, вызвавшая запись в журнал	Код события	Категория события	Содержание описания в журнале
			<ul style="list-style-type: none"> <li>– Короткоживущий (short-lived, throwaway) сертификат (может отсутствовать, если данный параметр шаблона не менялся; для параметра указано исходное и конечное значения)</li> <li>– Причина ошибки</li> </ul>
Удаление шаблона сертификата	CAENV125	INFO	<p>Описание: Удаление шаблона сертификата</p> <p>Атрибуты:</p> <ul style="list-style-type: none"> <li>– Идентификатор шаблона</li> <li>– Наименование шаблона</li> <li>– Период действия сертификата</li> <li>– Центр сертификации</li> <li>– Тип субъекта</li> <li>– Публиковать сертификат в ресурсную систему</li> <li>– Минимальная длина ключа RSA</li> <li>– Минимальная длина ключа ECDSA</li> <li>– Минимальная длина ключа ГОСТ Р 34.10-2012</li> <li>– Использование ключа</li> <li>– Считать критическим использование ключа</li> <li>– Расширенное использование ключа</li> <li>– Считать критическим расширенное использование ключа</li> <li>– Включать SID субъекта в сертификат</li> <li>– OID политики сертификата</li> <li>– Считать критическими OID политики сертификата</li> <li>– Политики выпуска PKCS#12</li> <li>– Включать сведения о средствах ЭП и УЦ издателя</li> <li>– Наименование средства ЭП (может отсутствовать, если в создаваемом шаблоне выключен чекбокс «Включать сведения о средствах ЭП и УЦ издателя»)</li> <li>– Реквизиты заключения о подтверждении соответствия средства ЭП (может отсутствовать, если в создаваемом шаблоне выключен чекбокс «Включать сведения о средствах ЭП и УЦ издателя»)</li> <li>– Наименование средства УЦ (может отсутствовать, если в создаваемом шаблоне выключен чекбокс «Включать сведения о средствах ЭП и УЦ издателя»)</li> <li>– Реквизиты заключения о подтверждении соответствия средства УЦ (может отсутствовать, если в создаваемом шаблоне выключен чекбокс «Включать сведения о средствах ЭП и УЦ издателя»)</li> <li>– Включать сведения о средстве ЭП владельца сертификата</li> <li>– Используемое средство ЭП (может отсутствовать, если в создаваемом шаблоне</li> </ul>

Причина, вызвавшая запись в журнал	Код события	Категория события	Содержание описания в журнале
			<p>выключен чекбокс «Включать сведения о средстве ЭП владельца сертификата»)</p> <ul style="list-style-type: none"> <li>– Отличительное имя субъекта</li> <li>– Альтернативное имя субъекта</li> <li>– Контроль соответствия полей в сертификате атрибутам субъекта</li> <li>– Короткоживущий (short-lived, throwaway) сертификат</li> </ul>
Ошибка удаления шаблона сертификата	CAENV126	ERROR	<p>Описание: Ошибка удаления шаблона сертификата</p> <p>Атрибуты:</p> <ul style="list-style-type: none"> <li>– Идентификатор шаблона</li> <li>– Наименование шаблона (может отсутствовать)</li> <li>– Период действия сертификата (может отсутствовать)</li> <li>– Центр сертификации (может отсутствовать)</li> <li>– Тип субъекта (может отсутствовать)</li> <li>– Публиковать сертификат в ресурсную систему (может отсутствовать)</li> <li>– Минимальная длина ключа RSA (может отсутствовать)</li> <li>– Минимальная длина ключа ECDSA (может отсутствовать)</li> <li>– Минимальная длина ключа ГОСТ Р 34.10-2012 (может отсутствовать)</li> <li>– Использование ключа (может отсутствовать)</li> <li>– Считать критическим использование ключа (может отсутствовать)</li> <li>– Расширенное использование ключа (может отсутствовать)</li> <li>– Считать критическим расширенное использование ключа (может отсутствовать)</li> <li>– Включать SID субъекта в сертификат (может отсутствовать)</li> <li>– OID политики сертификата (может отсутствовать)</li> <li>– Считать критическими OID политики сертификата (может отсутствовать)</li> <li>– Политики выпуска PKCS#12 (может отсутствовать)</li> <li>– Включать сведения о средствах ЭП и УЦ издателя (может отсутствовать)</li> <li>– Наименование средства ЭП (может отсутствовать)</li> <li>– Реквизиты заключения о подтверждении соответствия средства ЭП (может отсутствовать)</li> <li>– Наименование средства УЦ (может отсутствовать)</li> <li>– Реквизиты заключения о подтверждении соответствия средства УЦ (может отсутствовать)</li> <li>– Включать сведения о средстве ЭП владельца сертификата (может отсутствовать)</li> </ul>

Причина, вызвавшая запись в журнал	Код события	Категория события	Содержание описания в журнале
			<ul style="list-style-type: none"> <li>– Используемое средство ЭП (может отсутствовать)</li> <li>– Отличительное имя субъекта (может отсутствовать)</li> <li>– Альтернативное имя субъекта (может отсутствовать)</li> <li>– Контроль соответствия полей в сертификате атрибутам субъекта (может отсутствовать)</li> <li>– Короткоживущий (short-lived, throwaway) сертификат (может отсутствовать)</li> <li>– Причина ошибки</li> </ul>
Добавление почтового сервера	CAENV127	INFO	<p>Описание: Добавление почтового сервера</p> <p>Атрибуты:</p> <ul style="list-style-type: none"> <li>– Идентификатор почтового сервера</li> <li>– Адрес хоста</li> <li>– Порт</li> <li>– Протокол</li> <li>– Почтовый адрес отправителя</li> <li>– Использовать SMTP-аутентификацию</li> <li>– Логин</li> <li>– Использовать TLS при подключении (STARTTLS)</li> <li>– Флаг отправки уведомлений</li> </ul>
Ошибка добавления почтового сервера	CAENV128	ERROR	<p>Описание: Ошибка добавления почтового сервера</p> <p>Атрибуты:</p> <ul style="list-style-type: none"> <li>– Идентификатор почтового сервера (может отсутствовать)</li> <li>– Адрес хоста (может отсутствовать)</li> <li>– Порт (может отсутствовать)</li> <li>– Протокол (может отсутствовать)</li> <li>– Почтовый адрес отправителя (может отсутствовать)</li> <li>– Использовать SMTP-аутентификацию (может отсутствовать)</li> <li>– Логин (может отсутствовать)</li> <li>– Использовать TLS при подключении (STARTTLS) (может отсутствовать)</li> <li>– Флаг отправки уведомлений</li> <li>– Причина ошибки</li> </ul>
Изменение параметров почтового сервера	CAENV129	INFO	<p>Описание: Изменение параметров почтового сервера</p> <p>Атрибуты:</p> <ul style="list-style-type: none"> <li>– Идентификатор почтового сервера</li> <li>– Адрес хоста (может отсутствовать). Исходное значение/ Конечное значение</li> <li>– Порт (может отсутствовать). Исходное значение/ Конечное значение</li> <li>– Протокол (может отсутствовать). Исходное значение/ Конечное значение</li> </ul>

Причина, вызвавшая запись в журнал	Код события	Категория события	Содержание описания в журнале
			<ul style="list-style-type: none"> <li>– Почтовый адрес отправителя (может отсутствовать). Исходное значение/ Конечное значение</li> <li>– Использовать SMTP-аутентификацию (может отсутствовать). Исходное значение/ Конечное значение</li> <li>– Логин (может отсутствовать). Исходное значение/ Конечное значение</li> <li>– Использовать TLS при подключении (STARTTLS) (может отсутствовать). Исходное значение/ Конечное значение</li> <li>– Флаг отправки уведомлений (может отсутствовать). Исходное значение/ Конечное значение</li> </ul>
Ошибка изменения параметров почтового сервера	CAENV130	ERROR	<p>Описание: Ошибка изменения параметров почтового сервера</p> <p>Атрибуты:</p> <ul style="list-style-type: none"> <li>– Идентификатор почтового сервера</li> <li>– Адрес хоста (может отсутствовать). Исходное значение/ Конечное значение</li> <li>– Порт (может отсутствовать). Исходное значение/ Конечное значение</li> <li>– Протокол (может отсутствовать). Исходное значение/ Конечное значение</li> <li>– Почтовый адрес отправителя (может отсутствовать). Исходное значение/ Конечное значение</li> <li>– Использовать SMTP-аутентификацию (может отсутствовать). Исходное значение/ Конечное значение</li> <li>– Логин (может отсутствовать). Исходное значение/ Конечное значение</li> <li>– Использовать TLS при подключении (STARTTLS) (может отсутствовать). Исходное значение/ Конечное значение</li> <li>– Флаг отправки уведомлений (может отсутствовать). Исходное значение/ Конечное значение</li> <li>– Причина ошибки</li> </ul>
Удаление почтового сервера	CAENV131	INFO	<p>Описание: Удаление почтового сервера</p> <p>Атрибуты:</p> <ul style="list-style-type: none"> <li>– Идентификатор почтового сервера</li> <li>– Адрес хоста</li> <li>– Порт</li> <li>– Протокол</li> <li>– Почтовый адрес отправителя</li> <li>– Использовать SMTP-аутентификацию</li> <li>– Логин</li> <li>– Использовать TLS при подключении (STARTTLS)</li> <li>– Флаг отправки уведомлений</li> </ul>

Причина, вызвавшая запись в журнал	Код события	Категория события	Содержание описания в журнале
Ошибка удаления почтового сервера	CAENV132	ERROR	<p>Описание: Ошибка удаления почтового сервера</p> <p>Атрибуты:</p> <ul style="list-style-type: none"> <li>– Идентификатор почтового сервера (может отсутствовать)</li> <li>– Адрес хоста (может отсутствовать)</li> <li>– Порт (может отсутствовать)</li> <li>– Протокол (может отсутствовать)</li> <li>– Почтовый адрес отправителя (может отсутствовать)</li> <li>– Использовать SMTP-аутентификацию (может отсутствовать)</li> <li>– Логин (может отсутствовать)</li> <li>– Использовать TLS при подключении (STARTTLS) (может отсутствовать)</li> <li>– Флаг отправки уведомлений (может отсутствовать)</li> <li>– Причина ошибки</li> </ul>
Добавление шаблона рассылки уведомлений	CAENV133	INFO	<p>Описание: Добавление шаблона рассылки уведомлений</p> <p>Атрибуты:</p> <ul style="list-style-type: none"> <li>– Идентификатор шаблона рассылки уведомлений</li> <li>– Название шаблона рассылки уведомлений</li> <li>– Время до истечения сертификата</li> <li>– Тема письма</li> <li>– Флаг использования шаблона рассылки уведомлений</li> <li>– Объекты, о сертификатах которых должны рассылаться уведомления</li> <li>– Получатели уведомлений</li> </ul>
Ошибка добавления шаблона рассылки уведомлений	CAENV134	ERROR	<p>Описание: Ошибка добавления шаблона рассылки уведомлений</p> <p>Атрибуты:</p> <ul style="list-style-type: none"> <li>– Идентификатор шаблона рассылки уведомлений (может отсутствовать)</li> <li>– Название шаблона рассылки уведомлений (может отсутствовать)</li> <li>– Время до истечения сертификата (может отсутствовать)</li> <li>– Тема письма (может отсутствовать)</li> <li>– Флаг использования шаблона рассылки уведомлений (может отсутствовать)</li> <li>– Объекты, о сертификатах которых должны рассылаться уведомления (может отсутствовать)</li> <li>– Получатели уведомлений (может отсутствовать)</li> <li>– Причина ошибки</li> </ul>
Изменение параметров шаблона рассылки уведомлений	CAENV135	INFO	<p>Описание: Изменение параметров шаблона рассылки уведомлений</p> <p>Атрибуты:</p>

Причина, вызвавшая запись в журнал	Код события	Категория события	Содержание описания в журнале
			<ul style="list-style-type: none"> <li>– Идентификатор шаблона рассылки уведомлений (может отсутствовать). Исходное значение/ Конечное значение</li> <li>– Название шаблона рассылки уведомлений (может отсутствовать). Исходное значение/ Конечное значение</li> <li>– Время до истечения сертификата (может отсутствовать). Исходное значение/ Конечное значение</li> <li>– Тема письма (может отсутствовать). Исходное значение/ Конечное значение</li> <li>– Флаг использования шаблона рассылки уведомлений (может отсутствовать). Исходное значение/ Конечное значение</li> <li>– Объекты, о сертификатах которых должны рассылаться уведомления (может отсутствовать). Исходное значение/ Конечное значение</li> <li>– Получатели уведомлений (может отсутствовать). Исходное значение/ Конечное значение</li> </ul>
Ошибка изменения параметров шаблона рассылки уведомлений	CAENV136	ERROR	<p>Описание: Ошибка изменения параметров шаблона рассылки уведомлений</p> <p>Атрибуты:</p> <ul style="list-style-type: none"> <li>– Идентификатор шаблона рассылки уведомлений (может отсутствовать). Исходное значение/ Конечное значение</li> <li>– Название шаблона рассылки уведомлений (может отсутствовать). Исходное значение/ Конечное значение</li> <li>– Время до истечения сертификата (может отсутствовать). Исходное значение/ Конечное значение</li> <li>– Тема письма (может отсутствовать). Исходное значение/ Конечное значение</li> <li>– Флаг использования шаблона рассылки уведомлений (может отсутствовать). Исходное значение/ Конечное значение</li> <li>– Объекты, о сертификатах которых должны рассылаться уведомления (может отсутствовать). Исходное значение/ Конечное значение</li> <li>– Получатели уведомлений (может отсутствовать). Исходное значение/ Конечное значение</li> <li>– Причина ошибки</li> </ul>
Удаление шаблона рассылки уведомлений	CAENV137	INFO	<p>Описание: Удаление шаблона рассылки уведомлений</p> <p>Атрибуты:</p> <ul style="list-style-type: none"> <li>– Идентификатор шаблона рассылки уведомлений</li> <li>– Название шаблона рассылки уведомлений</li> <li>– Время до истечения сертификата</li> <li>– Тема письма</li> <li>– Флаг использования шаблона рассылки уведомлений</li> </ul>

Причина, вызвавшая запись в журнал	Код события	Категория события	Содержание описания в журнале
			<ul style="list-style-type: none"> <li>– Объекты, о сертификатах которых должны рассылаться уведомления</li> <li>– Получатели уведомлений</li> </ul>
Ошибка удаления шаблона рассылки уведомлений	CAENV138	ERROR	<p>Описание: Ошибка удаления шаблона рассылки уведомлений</p> <p>Атрибуты:</p> <ul style="list-style-type: none"> <li>– Идентификатор шаблона рассылки уведомлений (может отсутствовать)</li> <li>– Название шаблона рассылки уведомлений (может отсутствовать)</li> <li>– Время до истечения сертификата (может отсутствовать)</li> <li>– Тема письма (может отсутствовать)</li> <li>– Флаг использования шаблона рассылки уведомлений (может отсутствовать)</li> <li>– Объекты, о сертификатах которых должны рассылаться уведомления (может отсутствовать)</li> <li>– Получатели уведомлений (может отсутствовать)</li> <li>– Причина ошибки</li> </ul>
Переформирование сертификата Подчинённого ЦС	CAENV139	INFO	<p>Описание: Переформирование сертификата Подчинённого ЦС</p> <p>Атрибуты:</p> <ul style="list-style-type: none"> <li>– Идентификатор сертификата</li> <li>– Серийный номер сертификата (исходное и конечное значение)</li> <li>– Сведения о CRL DP (CRL, Delta CRL, AIA) и OCSP (исходное и конечное значение)</li> </ul>
Ошибка переформирования сертификата Подчинённого ЦС	CAENV140	ERROR	<p>Описание: Ошибка переформирования сертификата Подчинённого ЦС</p> <p>Атрибуты:</p> <ul style="list-style-type: none"> <li>– Идентификатор сертификата (может отсутствовать)</li> <li>– Серийный номер предыдущего сертификата (может отсутствовать)</li> <li>– Серийный номер нового сертификата (может отсутствовать)</li> <li>– Сведения о CRL DP и OCSP в предыдущем сертификате (может отсутствовать)</li> <li>– Сведения о CRL DP и OCSP в новом сертификате (может отсутствовать)</li> <li>– Причина ошибки</li> </ul>
Повторный импорт сертификата Подчинённого ЦС	CAENV141	INFO	<p>Описание: Переформирование сертификата Подчинённого ЦС</p> <p>Атрибуты:</p> <ul style="list-style-type: none"> <li>– Идентификатор сертификата</li> <li>– Серийный номер предыдущего сертификата</li> <li>– Серийный номер нового сертификата</li> <li>– Владелец</li> <li>– Издатель</li> </ul>

Причина, вызвавшая запись в журнал	Код события	Категория события	Содержание описания в журнале
Ошибка повторного импорта сертификата Подчинённого ЦС	CAENV142	ERROR	Описание: Ошибка переформирование сертификата Подчинённого ЦС Атрибуты: – Идентификатор сертификата (может отсутствовать) – Серийный номер предыдущего сертификата (может отсутствовать) – Серийный номер нового сертификата (может отсутствовать) – Владелец (может отсутствовать) – Издатель (может отсутствовать) – Причина ошибки
Создание правила сопоставления атрибутов	CAENV143	INFO	Описание: Создание правила сопоставления атрибутов Атрибуты: – Идентификатор правила – Тип ресурсной системы – Тип объекта – Атрибут объекта в ресурсной системе – Атрибут субъекта в еСА
Ошибка создания правила сопоставления атрибутов	CAENV144	ERROR	Описание: Ошибка создания правила сопоставления атрибутов Атрибуты: – Идентификатор правила (может отсутствовать) – Тип ресурсной системы (может отсутствовать) – Тип объекта (может отсутствовать) – Атрибут объекта в ресурсной системе (может отсутствовать) – Атрибут субъекта в еСА (может отсутствовать) – Причина ошибки
Изменение правила сопоставления атрибутов	CAENV145	INFO	Описание: Изменение правила сопоставления атрибутов Атрибуты: – Идентификатор правила. Исходное значение/ Конечное значение – Тип ресурсной системы – Тип объекта – Атрибут объекта в ресурсной системе (может отсутствовать). Исходное значение/ Конечное значение – Атрибут субъекта в еСА (может отсутствовать). Исходное значение/ Конечное значение
Ошибка изменения правила сопоставления атрибутов	CAENV146	ERROR	Описание: Ошибка изменения правила сопоставления атрибутов Атрибуты: – Идентификатор правила (может отсутствовать). Исходное значение/ Конечное значение – Тип ресурсной системы (может отсутствовать). Исходное значение/ Конечное значение

Причина, вызвавшая запись в журнал	Код события	Категория события	Содержание описания в журнале
			– Тип объекта (может отсутствовать). Исходное значение/ Конечное значение – Атрибут объекта в ресурсной системе (может отсутствовать). Исходное значение/ Конечное значение – Атрибут субъекта в еСА (может отсутствовать). Исходное значение/ Конечное значение – Причина ошибки
Удаление правила сопоставления атрибутов	CAENV147	INFO	Описание: Удаление правила сопоставления атрибутов Атрибуты: – Идентификатор правила – Тип ресурсной системы – Тип объекта – Атрибут объекта в ресурсной системе – Атрибут субъекта в еСА
Ошибка удаления правила сопоставления атрибутов	CAENV148	ERROR	Описание: Ошибка удаления правила сопоставления атрибутов Атрибуты: – Идентификатор правила (может отсутствовать) – Тип ресурсной системы (может отсутствовать) – Тип объекта (может отсутствовать) – Атрибут объекта в ресурсной системе (может отсутствовать) – Атрибут субъекта в еСА (может отсутствовать) – Причина ошибки
Выход пользователя	CAENV149	INFO	Описание: Выход пользователя Атрибуты: – Id пользователя – Отображаемое имя пользователя – Роль пользователя – IP адрес – Аутентификатор – Тип аутентификации
Применение параметров конфигурационного файла	CAENV150	INFO	Описание: Применение параметров конфигурационного файла Атрибуты: – Наличие изменений в конфигурационном файле – Параметры конфигурационного файла. В данном атрибуте присутствуют все параметры применённого конфигурационного файла еСА-СА в формате «ключ=значение», кроме параметра «database_password».
Создание субъекта	CAENV151	INFO	Описание: Создание субъекта Атрибуты: – Идентификатор субъекта – CN субъекта – Идентификатор ресурсной системы – Отображаемое имя ресурсной системы – Subject атрибуты

Причина, вызвавшая запись в журнал	Код события	Категория события	Содержание описания в журнале
			<p>– Subject Alternative Name атрибуты</p> <p><i>Примечание: журналирование события происходит только при создании локальных субъектов</i></p>
Ошибка создания субъекта	CAENV152	ERROR	<p>Описание: Ошибка создания субъекта</p> <p>Атрибуты:</p> <ul style="list-style-type: none"> <li>– CN субъекта (может отсутствовать)</li> <li>– Идентификатор ресурсной системы (может отсутствовать)</li> <li>– Отображаемое имя ресурсной системы (может отсутствовать)</li> <li>– Subject атрибуты (может отсутствовать)</li> <li>– Subject Alternative Name атрибуты (может отсутствовать)</li> <li>– Причина ошибки</li> </ul> <p><i>Примечание: журналирование события происходит только при ошибке создания локальных субъектов</i></p>
Изменение субъекта	CAENV153	INFO	<p>Описание: Изменение субъекта</p> <p>Атрибуты:</p> <ul style="list-style-type: none"> <li>– Идентификатор субъекта</li> <li>– CN субъекта (исходное/конечное значение)</li> <li>– Идентификатор ресурсной системы</li> <li>– Отображаемое имя ресурсной системы</li> <li>– Subject атрибуты (исходное/конечное значение)</li> <li>– Subject Alternative Name атрибуты (исходное/конечное значение)</li> </ul> <p><i>Примечание: журналирование события происходит только при ручном изменении субъекта</i></p>
Ошибка изменения субъекта	CAENV154	ERROR	<p>Описание: Ошибка изменения субъекта</p> <p>Атрибуты:</p> <ul style="list-style-type: none"> <li>– Идентификатор субъекта (может отсутствовать)</li> <li>– CN субъекта (может отсутствовать)</li> <li>– Идентификатор ресурсной системы (может отсутствовать)</li> <li>– Отображаемое имя ресурсной системы (может отсутствовать)</li> <li>– Subject атрибуты (может отсутствовать)</li> <li>– Subject Alternative Name атрибуты (может отсутствовать)</li> </ul> <p><i>Примечание: журналирование события происходит только при попытке ручного изменения субъекта</i></p>
Удаление субъекта	CAENV155	INFO	<p>Описание: Удаление субъекта</p> <p>Атрибуты:</p>

Причина, вызвавшая запись в журнал	Код события	Категория события	Содержание описания в журнале
			<ul style="list-style-type: none"> <li>– Идентификатор субъекта</li> <li>– CN субъекта</li> <li>– Идентификатор ресурсной системы</li> <li>– Отображаемое имя ресурсной системы</li> <li>– Subject атрибуты</li> <li>– Subject Alternative Name атрибуты</li> </ul>
Ошибка удаления субъекта	CAENV156	ERROR	<p>Описание: Ошибка удаления субъекта</p> <p>Атрибуты:</p> <ul style="list-style-type: none"> <li>– CN субъекта (может отсутствовать)</li> <li>– Идентификатор ресурсной системы (может отсутствовать)</li> <li>– Отображаемое имя ресурсной системы (может отсутствовать)</li> <li>– Subject атрибуты (может отсутствовать)</li> <li>– Subject Alternative Name атрибуты (может отсутствовать)</li> <li>– Причина ошибки</li> </ul>
Создание точки распространения	CAENV157	INFO	<p>Описание: Создание точки распространения</p> <p>Атрибуты:</p> <ul style="list-style-type: none"> <li>– Идентификатор точки распространения</li> <li>– Идентификатор центра сертификации</li> <li>– Отображаемое имя центра сертификации</li> <li>– Тип распространяемых данных</li> <li>– URL распространения</li> <li>– URL публикации (может отсутствовать)</li> <li>– Запись в сертификаты</li> <li>– Приоритет</li> <li>– Идентификатор центра валидации (может отсутствовать)</li> <li>– Адрес хоста центра валидации (может отсутствовать)</li> <li>– Дочерние точки распространения (может отсутствовать)</li> </ul>
Ошибка создания точки распространения	CAENV158	ERROR	<p>Описание: Ошибка создания точки распространения</p> <p>Атрибуты:</p> <ul style="list-style-type: none"> <li>– Идентификатор точки распространения (может отсутствовать)</li> <li>– Идентификатор центра сертификации (может отсутствовать)</li> <li>– Отображаемое имя центра сертификации (может отсутствовать)</li> <li>– Тип распространяемых данных (может отсутствовать)</li> <li>– URL распространения (может отсутствовать)</li> <li>– URL публикации (может отсутствовать)</li> <li>– Запись в сертификаты (может отсутствовать)</li> <li>– Приоритет (может отсутствовать)</li> </ul>

Причина, вызвавшая запись в журнал	Код события	Категория события	Содержание описания в журнале
			<ul style="list-style-type: none"> <li>– Идентификатор центра валидации (может отсутствовать)</li> <li>– Адрес хоста центра валидации (может отсутствовать)</li> <li>– Дочерние точки распространения (может отсутствовать)</li> <li>– Причина ошибки</li> </ul>
Изменение точки распространения	CAENV159	INFO	<p>Описание: Изменение точки распространения</p> <p>Атрибуты:</p> <ul style="list-style-type: none"> <li>– Идентификатор точки распространения</li> <li>– Идентификатор центра сертификации</li> <li>– Отображаемое имя центра сертификации</li> <li>– Тип распространяемых данных</li> <li>– URL распространения (может отсутствовать; будет присутствовать только при изменении данного параметра; исходное/конечное значение)</li> <li>– URL публикации (может отсутствовать; будет присутствовать только при изменении данного параметра; исходное/конечное значение)</li> <li>– Запись в сертификаты (может отсутствовать; будет присутствовать только при изменении данного параметра; исходное/конечное значение)</li> <li>– Приоритет (может отсутствовать; будет присутствовать только при изменении данного параметра; исходное/конечное значение)</li> <li>– Идентификатор центра валидации</li> <li>– Адрес хоста центра валидации</li> <li>– Дочерние точки распространения (может отсутствовать; будет присутствовать только при изменении данного параметра; исходное/конечное значение)</li> </ul>
Ошибка изменения точки распространения	CAENV160	ERROR	<p>Описание: Ошибка изменения точки распространения</p> <p>Атрибуты:</p> <ul style="list-style-type: none"> <li>– Идентификатор точки распространения (может отсутствовать)</li> <li>– Идентификатор центра сертификации (может отсутствовать)</li> <li>– Отображаемое имя центра сертификации (может отсутствовать)</li> <li>– Тип распространяемых данных (может отсутствовать)</li> <li>– URL распространения (может отсутствовать; будет присутствовать только при попытке изменения данного параметра; исходное/конечное значение)</li> <li>– URL публикации (может отсутствовать; будет присутствовать только при попытке изменения данного параметра; исходное/конечное значение)</li> <li>– Запись в сертификаты (может отсутствовать; будет присутствовать только при попытке</li> </ul>

Причина, вызвавшая запись в журнал	Код события	Категория события	Содержание описания в журнале
			<p>изменения данного параметра; исходное/конечное значение)</p> <ul style="list-style-type: none"> <li>– Приоритет (может отсутствовать; будет присутствовать только при попытке изменения данного параметра; исходное/конечное значение)</li> <li>– Идентификатор центра валидации</li> <li>– Адрес хоста центра валидации</li> <li>– Дочерние точки распространения (может отсутствовать; будет присутствовать только при попытке изменения данного параметра; исходное/конечное значение)</li> <li>– Причина ошибки</li> </ul>
Удаление точки распространения	CAENV161	INFO	<p>Описание: Удаление точки распространения</p> <p>Атрибуты:</p> <ul style="list-style-type: none"> <li>– Идентификатор точки распространения</li> <li>– Идентификатор центра сертификации</li> <li>– Отображаемое имя центра сертификации</li> <li>– Тип распространяемых данных</li> <li>– URL распространения</li> <li>– URL публикации (может отсутствовать)</li> <li>– Запись в сертификаты</li> <li>– Приоритет</li> <li>– Идентификатор центра валидации (может отсутствовать)</li> <li>– Адрес хоста центра валидации (может отсутствовать)</li> <li>– Дочерние точки распространения (может отсутствовать)</li> </ul>
Ошибка удаления точки распространения	CAENV162	ERROR	<p>Описание: Ошибка удаления точки распространения</p> <p>Атрибуты:</p> <ul style="list-style-type: none"> <li>– Идентификатор точки распространения (может отсутствовать)</li> <li>– Идентификатор центра сертификации (может отсутствовать)</li> <li>– Отображаемое имя центра сертификации (может отсутствовать)</li> <li>– Тип распространяемых данных (может отсутствовать)</li> <li>– URL распространения (может отсутствовать)</li> <li>– URL публикации (может отсутствовать)</li> <li>– Запись в сертификаты (может отсутствовать)</li> <li>– Приоритет (может отсутствовать)</li> <li>– Идентификатор центра валидации (может отсутствовать)</li> <li>– Адрес хоста центра валидации (может отсутствовать)</li> <li>– Дочерние точки распространения (может отсутствовать)</li> <li>– Причина ошибки</li> </ul>

Причина, вызвавшая запись в журнал	Код события	Категория события	Содержание описания в журнале
Создание службы OCSP	CAENV163	INFO	<p>Описание: Создание службы OCSP</p> <p>Атрибуты:</p> <ul style="list-style-type: none"> <li>– Идентификатор службы OCSP</li> <li>– Идентификатор центра сертификации</li> <li>– Отображаемое имя центра сертификации</li> <li>– URL службы OCSP</li> <li>– Запись в сертификаты</li> <li>– Приоритет</li> <li>– Идентификатор центра валидации (может отсутствовать)</li> <li>– Адрес хоста центра валидации (может отсутствовать)</li> <li>– Дочерние службы OCSP (может отсутствовать)</li> </ul>
Ошибка создания службы OCSP	CAENV164	ERROR	<p>Описание: Ошибка создания службы OCSP</p> <p>Атрибуты:</p> <ul style="list-style-type: none"> <li>– Идентификатор службы OCSP (может отсутствовать)</li> <li>– Идентификатор центра сертификации (может отсутствовать)</li> <li>– Отображаемое имя центра сертификации (может отсутствовать)</li> <li>– URL службы OCSP (может отсутствовать)</li> <li>– Запись в сертификаты (может отсутствовать)</li> <li>– Приоритет (может отсутствовать)</li> <li>– Идентификатор центра валидации (может отсутствовать)</li> <li>– Адрес хоста центра валидации (может отсутствовать)</li> <li>– Дочерние службы OCSP (может отсутствовать)</li> <li>– Причина ошибки</li> </ul>
Изменение службы OCSP	CAENV165	INFO	<p>Описание: Изменение службы OCSP</p> <p>Атрибуты:</p> <ul style="list-style-type: none"> <li>– Идентификатор службы OCSP</li> <li>– Идентификатор центра сертификации</li> <li>– Отображаемое имя центра сертификации</li> <li>– URL службы OCSP (может отсутствовать; будет присутствовать только при изменении данного параметра; исходное/конечное значение)</li> <li>– Запись в сертификаты (может отсутствовать; будет присутствовать только при изменении данного параметра; исходное/конечное значение)</li> <li>– Приоритет (может отсутствовать; будет присутствовать только при изменении данного параметра; исходное/конечное значение)</li> <li>– Идентификатор центра валидации</li> <li>– Адрес хоста центра валидации</li> <li>– Дочерние службы OCSP (может отсутствовать; будет присутствовать только при изменении данного параметра; исходное/конечное значение)</li> </ul>

Причина, вызвавшая запись в журнал	Код события	Категория события	Содержание описания в журнале
Ошибка изменения службы OSCP	CAENV166	ERROR	<p>Описание: Ошибка изменения службы OSCP</p> <p>Атрибуты:</p> <ul style="list-style-type: none"> <li>– Идентификатор службы OSCP (может отсутствовать)</li> <li>– Идентификатор центра сертификации (может отсутствовать)</li> <li>– Отображаемое имя центра сертификации (может отсутствовать)</li> <li>– URL службы OSCP (может отсутствовать; будет присутствовать только при попытке изменения данного параметра; исходное/конечное значение)</li> <li>– Запись в сертификаты (может отсутствовать; будет присутствовать только при попытке изменения данного параметра; исходное/конечное значение)</li> <li>– Приоритет (может отсутствовать; будет присутствовать только при попытке изменения данного параметра; исходное/конечное значение)</li> <li>– Идентификатор центра валидации (может отсутствовать)</li> <li>– Адрес хоста центра валидации (может отсутствовать)</li> <li>– Дочерние службы OSCP (может отсутствовать; будет присутствовать только при попытке изменения данного параметра; исходное/конечное значение)</li> <li>– Причина ошибки</li> </ul>
Удаление службы OSCP	CAENV167	INFO	<p>Описание: Удаление службы OSCP</p> <p>Атрибуты:</p> <ul style="list-style-type: none"> <li>– Идентификатор службы OSCP</li> <li>– Идентификатор центра сертификации</li> <li>– Отображаемое имя центра сертификации</li> <li>– URL службы OSCP</li> <li>– Запись в сертификаты</li> <li>– Приоритет</li> <li>– Идентификатор центра валидации (может отсутствовать)</li> <li>– Адрес хоста центра валидации (может отсутствовать)</li> <li>– Дочерние службы OSCP (может отсутствовать)</li> </ul>
Ошибка удаления службы OSCP	CAENV168	ERROR	<p>Описание: Ошибка удаления службы OSCP</p> <p>Атрибуты:</p> <ul style="list-style-type: none"> <li>– Идентификатор службы OSCP (может отсутствовать)</li> <li>– Идентификатор центра сертификации (может отсутствовать)</li> <li>– Отображаемое имя центра сертификации (может отсутствовать)</li> <li>– URL службы OSCP (может отсутствовать)</li> <li>– Запись в сертификаты (может отсутствовать)</li> <li>– Приоритет (может отсутствовать)</li> </ul>

Причина, вызвавшая запись в журнал	Код события	Категория события	Содержание описания в журнале
			– Идентификатор центра валидации (может отсутствовать) – Адрес хоста центра валидации (может отсутствовать) – Дочерние службы OCSP (может отсутствовать) – Причина ошибки
Удаление центра валидации	CAENV169	INFO	Описание: Удаление центра валидации Атрибуты: – Идентификатор центра валидации – Адрес хоста центра валидации – Идентификатор центра сертификации – Отображаемое имя центра сертификации
Ошибка удаления центра валидации	CAENV170	ERROR	Описание: Ошибка удаления центра валидации Атрибуты: – Идентификатор центра валидации (может отсутствовать) – Адрес хоста центра валидации (может отсутствовать) – Идентификатор центра сертификации (может отсутствовать) – Отображаемое имя центра сертификации (может отсутствовать) – Причина ошибки

## 8.10.2 Просмотр журнала событий

### 8.10.2.1 Просмотр записей, не помещённых в архив

Просмотр журнала событий доступен только пользователям с ролью «Администратор».

Для просмотра журнала событий:

1. Перейдите на вкладку «Журнал событий» (см. рисунок 192). При необходимости используйте прокрутку мышью.

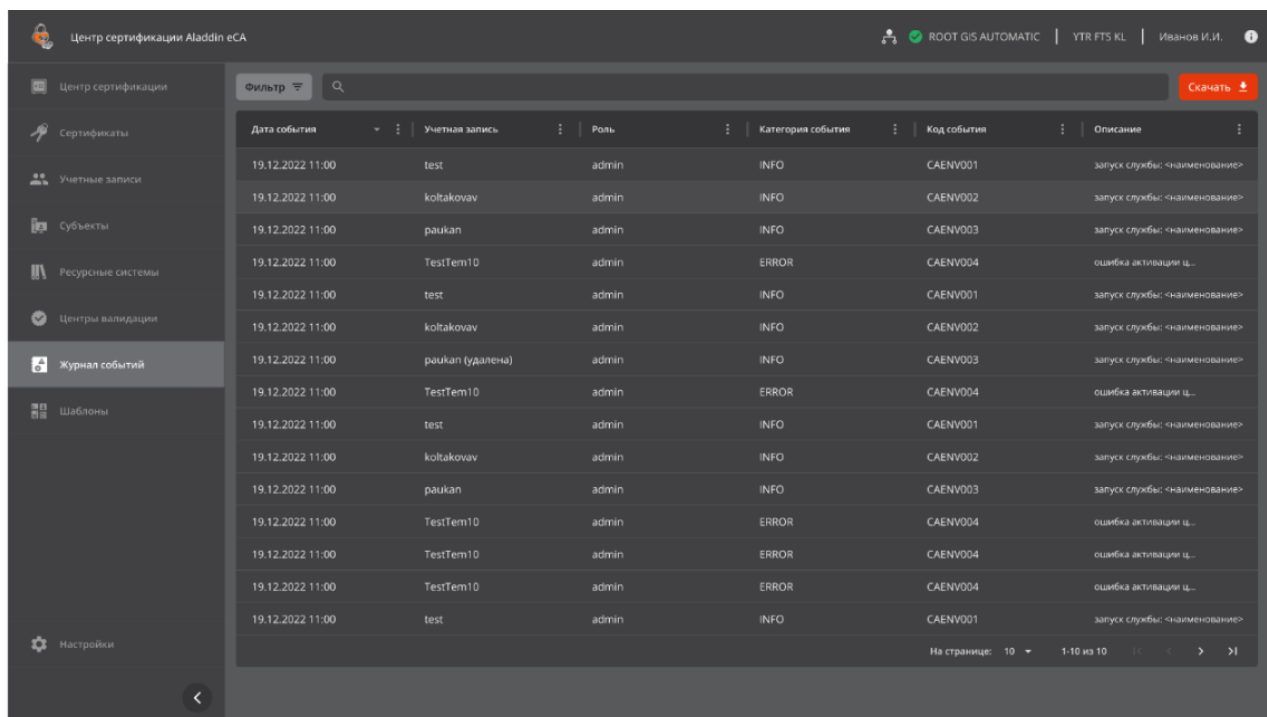





Рисунок 192 — Вкладка «Журнал событий»

2. Для перемещения по страницам списка используйте инструменты навигации (см. рисунок 193).



Рисунок 193 – Инструменты навигации

3. Для сортировки сведений используйте кнопку  в необходимом столбце таблицы сведений.
4. Для фильтрации сведений:
  - 4.1. Нажмите на кнопку «Фильтр»
  - 4.2. Выберите параметры фильтрации в выпадающих списках в колонках таблицы.
5. Для поиска записей по описанию события введите достаточную часть описания в поле .
6. Для просмотра подробных сведений о событии:
  - 6.1. Нажмите на строку записи этого события.
  - 6.2. В окне «Свойства события» (см. рисунок 194):
    - 6.2.1. Ознакомьтесь со сведениями о событии в полях раздела «Общие сведения»:
      - «Идентификатор события»;
      - «Дата и время события»;
      - «Учётная запись» — инициатор, логин учётной записи, действия которой повлекли событие (имя пользователя eCA-CA или «SYSTEM» для системных событий);
      - «Роль» — роль инициатора («администратор», «оператор»);
      - «IP-адрес источника» — IP-адрес инициатора события. Для системных событий значение в данном поле может отсутствовать;
      - «Категория события» — информационное или ошибка;
      - «Код События» (см. 8.10.1);
      - «Описание» — описание события с атрибутами (см. 8.10.1).
    - 6.2.2. Ознакомьтесь со сведениями о событии в полях раздела «Подробности». Состав полей раздела «Подробности» соответствует составу полей списка «Атрибуты» в столбце «Описание в журнале» таблиц, представленных в 8.10.1.
7. Для копирования информации о событии в буфер обмена нажмите кнопку  «Копировать» в окне «Свойства события».

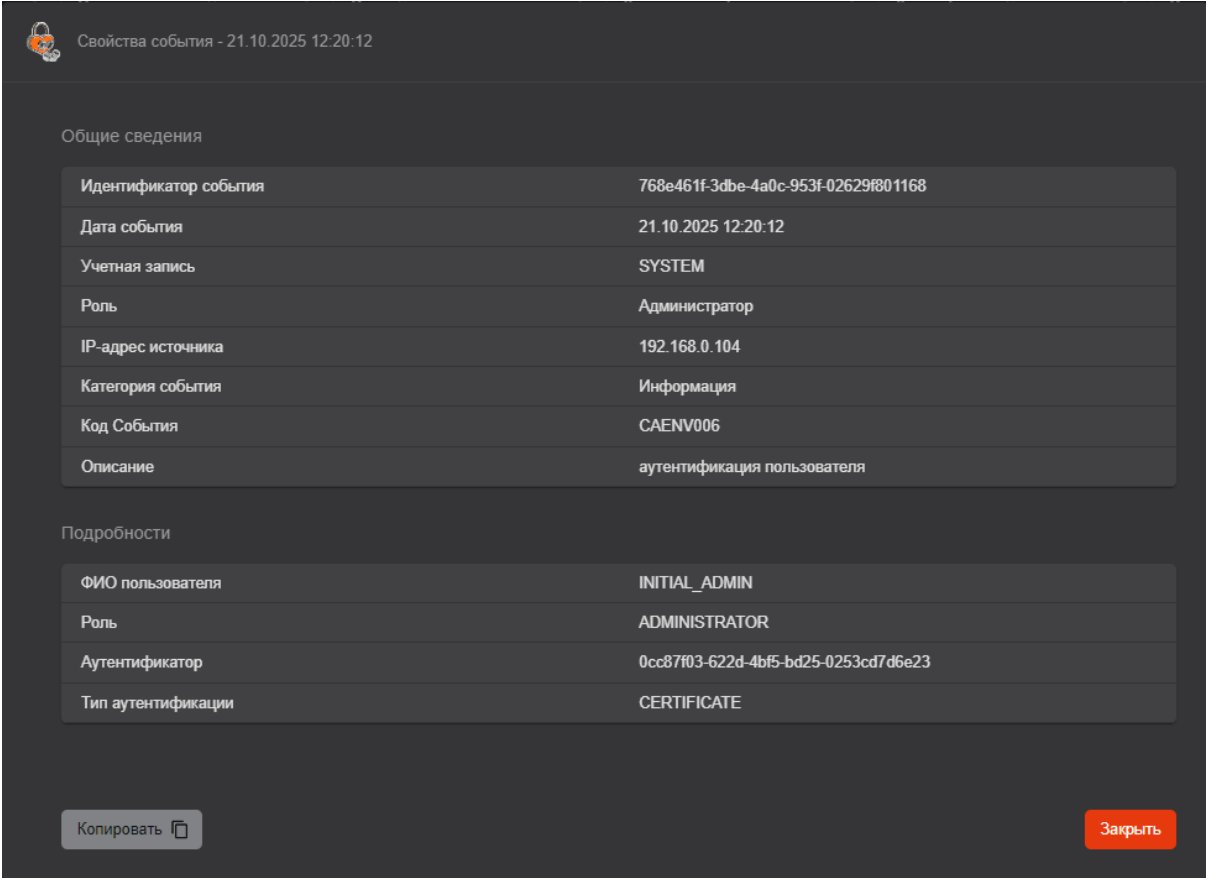


Рисунок 194 — Окно «Свойства события»

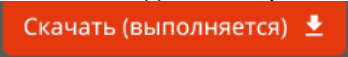
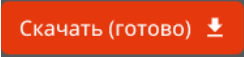
### 8.10.2.2 Просмотр записей, помещённых в архив

Для просмотра записей, помещённых в архив (см. 8.10.4), используйте любые средства работы с файлами формата CSV.

### 8.10.3 Экспорт журнала событий

Экспорт журнала событий производится в файл в формате CSV с учётом фильтрации и поиска. Используется кодировка UTF-8 с разделителем полей «;». Экспортируется часть журнала, не помещённая в архив (см. 8.10.4).

Для экспорта журнала событий:

1. Перейдите на вкладку «Журнал событий» (см. рисунок 192), при необходимости воспользуйтесь фильтром или строкой поиска для задания критериев отбора экспортируемых событий журнала (при отсутствии заданных в фильтре или строке поиска значений будут экспортированы все записи журнала событий),
2. Нажмите кнопку «Скачать». Начнётся подготовка файла экспорта и название кнопки измениться на «Скачать (выполняется)» .
3. Дождитесь пока кнопка «Скачать (выполняется)» сменит название на «Скачать (готово)» .
4. Нажмите кнопку «Скачать (готово)». Файл `log.csv` будет помещён в архив `logs.zip` и скачан в директорию «Загрузки» на тот компьютер, где была открыта вкладка «Журнал событий» на шаге1.<sup>1</sup>

### 8.10.4 Архивация журнала событий

По умолчанию при наступлении первого числа каждого месяца еCA-CA автоматически проверяет наличие записей в журнале событий старше 180 дней. Записи, попадающие под это условие, помещаются в csv-файл (имя файла «logs-date.csv», где «date» — дата и время создания архива) и архивируются в zip-

<sup>1</sup> Заданные по умолчанию имена файлов и директория для скачивания не могут быть изменены.

файл с именем «logs-date.zip», где «date» — дата и время создания архива в каталоге хранения (по умолчанию каталог хранения расположен по пути: `/opt/aecaCa/dist}/archive`).

Для изменения времени хранения записей в журнале до архивирования отредактируйте в конфигурационном файле параметр `archive_millis_ago`. Значение параметра `archive_millis_ago` указывается в миллисекундах.

Для изменения времени запуска архивации отредактируйте в конфигурационном файле параметр `archive_cron`. Значение параметра `archive_cron` указывается в формате CRON-выражения (по умолчанию – «0 0 0 1 \* \*»).

### 8.10.5 Передача информации о событиях в сторонние системы по протоколу Syslog

еCA-CA выполняет автоматическую отправку сообщений о зафиксированных событиях на Syslog-серверы из списка в разделе «Настройки» на вкладке «Syslog» (см. 8.16).

Значения полей отправляемых Syslog-сообщений о зарегистрированных событиях представлено в таблице 18.

Таблица 18 – Значения полей отправляемых Syslog-сообщений

Поле Syslog-сообщения	Описание	Значение
PRIVAL	Priority Value – значение, вычисляемое на основе категории и важности события	Для информационных событий: 14. Для ошибок: 11
VERSION	Версия используемого стандарта Syslog	1
TIMESTAMP	Временная метка в соответствии с RFC3339	Текущее время на хосте AECA-CA в формате ISO 8601: <code>YYYY-MM-DDThh:mm:ss[.SSS]</code>
HOSTNAME	Имя хоста, отправляющего сообщение	FQDN хоста AECA-CA
APP-NAME	Тег, указывающий приложение или процесс, создавшего сообщение	<code>AECA-CA</code>
PROCID	Идентификатор процесса (PID) приложения	PID сервиса, являющегося источником события
MSGID	Идентификатор сообщения	Код события
[STRUCTURED-DATA]	Структурированные данные	<pre>[aeca-ca eventId='eventId' actionCode='actionCode' category='category' id='id' serviceName='serviceName' system='system' username='username' role='role' ipAddress='ipAddress' attributes='attributes'],</pre> <p>где:</p> <ul style="list-style-type: none"> <li>– "eventId" – идентификатор события;</li> <li>– "actionCode" – код события;</li> <li>– "category" – категория события;</li> <li>– "id" – идентификатор типа события;</li> </ul>

Поле Syslog-сообщения	Описание	Значение
		<ul style="list-style-type: none"> <li>– "serviceName" – имя сервиса, в котором произошло событие;</li> <li>– "system" – флаг системного события;</li> <li>– "username" – логин учетной записи инициатора события;</li> <li>– "role" – роль инициатора события;</li> <li>– "ipAddress" – IP-адрес инициатора события;</li> <li>– "attributes" – расширенное описание события. Состав полей расширенного описания события соответствует составу описания события, указанному в столбце «Содержание описания в журнале» таблицы 17.</li> </ul> <p>Пример содержания "attributes" для ошибки CAENV055: <code>attributes="[CN: red; email: red@sambadc.host; шаблон: Рассылка об истечении срока действия сертификата через 1 день; причина ошибки: &lt;description&gt;]"</code></p>
MESSAGE	Строка, содержащая краткую информацию о событии	Краткое описание события (аналогично описанию события, отображаемому в списке событий в разделе «Журнал событий»).

## 8.11 Управление шаблонами сертификатов

### 8.11.1 Общие сведения о работе с шаблонами сертификатов

Раздел «Шаблоны» (см. рисунок 195) отображаться только для:

- пользователя с правами администратора;
- пользователя с правами оператора при наличии в программе правила доступа, по которому данному оператору предоставлены полномочия на просмотр и использование шаблонов.

Имя	Создано сертификатов	Дата создания	Центр сертификации	Тип субъекта
ALD PRO Domain Controller	0	05.06.2025 21:56:51	Любой	Устройство
ALD PRO Smartcard Logon	0	05.06.2025 21:56:51	Любой	Пользователь
Domain Controller	0	05.06.2025 21:56:51	Любой	Устройство
OCSP Signer	1	05.06.2025 21:56:51	Любой	Устройство
Root CA	2	05.06.2025 21:56:51	Любой	Корневой ЦС
SCEP Management	0	05.06.2025 01:34:05	Любой	Устройство
Smartcard Logon	0	05.06.2025 21:56:51	Любой	Пользователь
S/MIME	0	05.06.2025 21:56:51	Любой	Пользователь
Sub CA	0	05.06.2025 21:56:51	Любой	Подчиненный ЦС
User	2	05.06.2025 01:34:05	Любой	Пользователь
WEB-Client	0	05.06.2025 21:56:51	Любой	Пользователь
WEB-Server	1	05.06.2025 21:56:51	Любой	Устройство

Рисунок 195 — Раздел шаблоны

Пользователь с правами администратора имеет возможность выполнять через клиентский компонент следующие операции с шаблонами сертификатов:

- просмотр;
- клонирование;
- редактирование;
- удаление;
- выполнение массовых операций над шаблонами (удаление);
- отображение списка;
- импорт шаблонов сертификатов MS CS.

Пользователь с правами оператора имеет возможность выполнять через клиентский компонент просмотр шаблонов сертификатов. При этом доступен просмотр только тех шаблонов, на просмотр которых данному оператору предоставлены полномочия в соответствии с правилами доступа.


Шаблоны, установленные в системе по умолчанию, нельзя удалить или отредактировать.

В общем списке шаблоны по умолчанию выделяются символом «замок», при наведении курсора на который отображается всплывающее сообщение «Шаблон по умолчанию». Шаблоны, установленные по умолчанию:

- User;
- WEB-Client;
- WEB-Server;
- Domain Controller;
- Smartcard Logon;
- S/MIME;
- ALD PRO Domain Controller;
- ALD PRO Smartcard Logon;
- OCSP Signer;
- Root CA;
- Sub CA;
- SCEP Management;
- [Deprecated] ECA-Auth;
- [Deprecated] ECA-User;
- [Deprecated] Domain Controller;
- [Deprecated] Smartcard Logon;
- [Deprecated] WEB-Client;
- [Deprecated] WEB-Server;
- [Deprecated] ECA-WEB-Server;
- [Deprecated] S/MIME;
- [Deprecated] ALD PRO Domain Controller;
- [Deprecated] ALD PRO Smartcard Logon;
- [Deprecated] OCSP Signer;
- [Deprecated] Root CA;
- [Deprecated] Sub CA;
- [Deprecated] SCEP Management.

**Внимание!** После обновления eCA-CA до версии 2.4 все предустановленные в предыдущих версиях шаблоны сертификатов считаются устаревшими (в названиях таких шаблонов добавлена пометка «[Deprecated]»). В набор предустановленных шаблонов сертификатов добавлены копии устаревших шаблонов с измененными параметрами (за исключением шаблонов «ECA-WEB-Server» и «ECA-Auth»). Шаблон «ECA-User» переименован в «User». Параметры предустановленных шаблонов сертификатов представлены в приложении 2 «Описание полей предустановленных шаблонов сертификатов».




### 8.11.2 Просмотр информации о шаблонах сертификатов

Для просмотра информации о шаблонах подключитесь к веб-интерфейсу eCA-CA и перейдите в раздел  **Шаблоны** (см. рисунок 195).

Записи о шаблонах отображаются списком в табличном виде. В колонках таблицы отображаются следующие атрибуты шаблонов:

-  - в шаблоне выключен чекбокс «Контролировать соответствие полей в сертификате атрибутам субъекта».

**Внимание!** Использование таких шаблонов в информационных системах крайне не рекомендуется. При использовании таких шаблонов контроль соответствия значений в SDN и SAN полях сертификатов необходимо обеспечивать средствами внешней системы, и доступ к таким шаблонам должен быть строго ограничен.

- Условное обозначение типа шаблона:
  -  – предустановленные по умолчанию шаблоны.
  -  – пользовательские шаблоны.
  -  – импортированные из файла шаблоны MS CS.
- Имена (названия) шаблонов.
- Количество сертификатов, выпущенных по шаблону.
- Дата и время создания (клонирования) шаблона.
- Отображаемое имя Центра 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 по умолчанию выпуск сертификатов будет выполняться в активном на данный момент Центре сертификации. По предустановленным шаблонам выпуск сертификатов доступен в любом центре сертификации.

**Внимание!** При обновлении ПО до версии 2.4 всем шаблонам для параметра «Центр сертификации» устанавливается значение «Любой».

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

**Внимание!** При обновлении ПО до версии 2.4 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 предустановленных шаблонов «WEB-Server», [Deprecated] «WEB-Server», «ECA-WEB-Server», [Deprecated] «ECA-WEB-Server», «OCSP Signer», [Deprecated] «OCSP Signer», «Domain Controller», [Deprecated] «Domain Controller», «ALD PRO Domain Controller», [Deprecated] «ALD PRO Domain

**Controller», «SCEP Management», [Deprecated] «SCEP Management», для которых устанавливается значение типа субъекта «Устройство»).**

Записи о шаблонах выводятся постранично. Для перемещения по страницам списка используйте инструменты навигации.

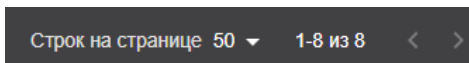


Рисунок 196 – Инструменты навигации

Описание инструментов навигации:

- — переход на следующую страницу списка.
- — переход на предыдущую страницу списка.
- — выбор количества записей, отображаемых на одной странице списка.

Для поиска шаблонов в списке вы можете выполнить сортировку (упорядочивание) записей по выбранному атрибуту, представленному в соответствующей колонке.

Сортировка (упорядочивание) записей о шаблонах возможна по следующим атрибутам (колонкам):

- По имени шаблона в алфавитном порядке.
- По дате и времени создания шаблона в порядке убывания или возрастания временных меток.
- По наименованию Центра сертификации, в котором разрешён выпуск сертификатов по шаблону, в алфавитном порядке.
- По типу субъекта, для которого может быть выпущен сертификат по шаблону, в алфавитном порядке.

По умолчанию сортировка записей в списке выполнена по имени шаблона (в порядке убывания в алфавитном порядке, начиная с латинских букв).

Чтобы выполнить сортировку записей о шаблонах по выбранному атрибуту, щёлкните в заголовке соответствующей колонки значок

Статусы выполненной сортировки отображаются в заголовках колонок следующими значками:

- – сортировка выполнена в порядке возрастания.
- – сортировка выполнена в порядке убывания.
- – сортировка не выполнена.

Менять порядок сортировки, а также отменять сортировку можно, последовательно щелкая на значок статуса сортировки или в колонке.

Чтобы выполнить выборку шаблонов по их именам, введите в поисковой строке, расположенной на панели инструментов, ключевое слово, содержащееся в имени шаблона. Для отмены выборки щёлкните в поисковой строке значок или удалите ключевое слово в поисковой строке.

Для фильтрации шаблонов по типу создания из выпадающего списка в элементе управления слева от поля поиска выберите: «Все типы шаблонов» (выбрано по умолчанию), «Предустановленные», «Клонированные» или «Импортированные».

Для фильтрации шаблонов по актуальности из выпадающего списка в элементе управления слева от поля поиска выберите: «Актуальные» (выбрано по умолчанию), «Устаревшие» или «Все шаблоны».

### 8.11.3 Просмотр карточки шаблона сертификата

Чтобы открыть карточку шаблона:

- Подключитесь к веб-интерфейсу eCA-CA и перейдите в раздел **Шаблоны**.
- Откройте карточку шаблона. Для этого найдите его в списке и щёлкните запись о нем.

В карточке шаблона (см. Рисунок 197) администратору доступны следующие инструменты и информация:

- Кнопка возврата на вкладку «Шаблоны».
- Кнопка для клонирования текущего шаблона.

- Кнопка **Сохранить** для записи изменений полей текущего шаблона, доступная для всех шаблонов, кроме предустановленных.
- Имя шаблона.
- Постоянный идентификатор шаблона.

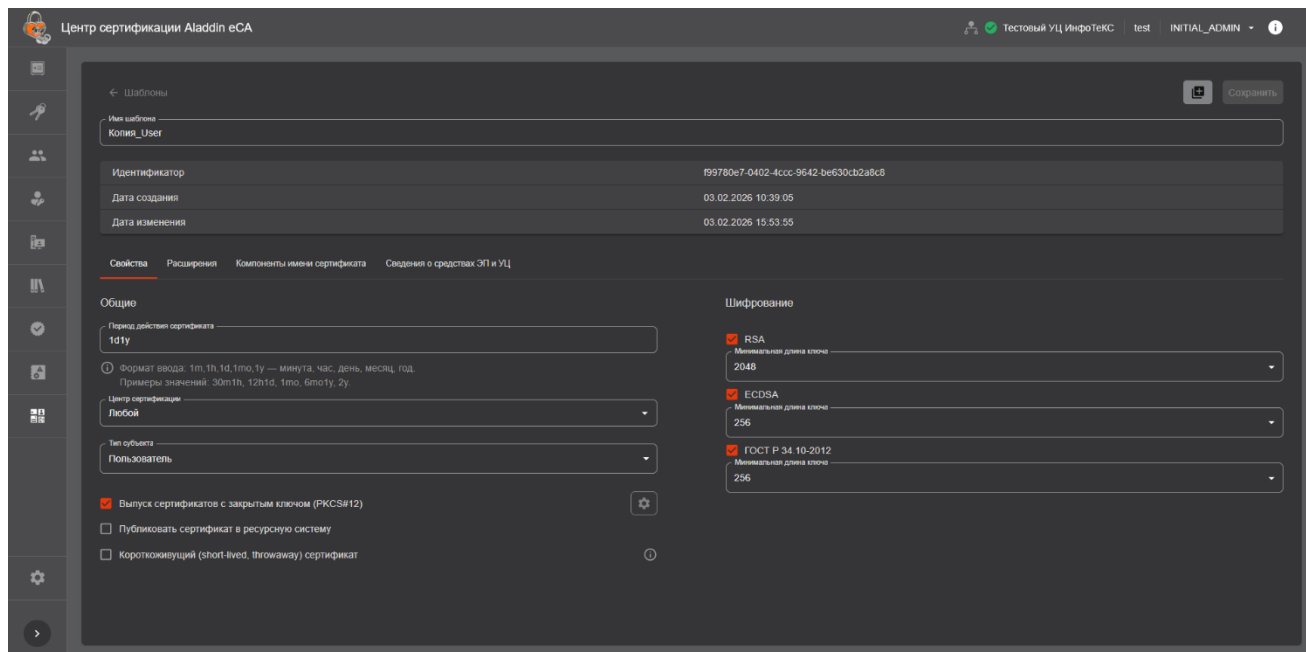


Рисунок 197 – «Карточка шаблона»

- Дата и время создания шаблона (для предустановленных шаблонов – это дата и время развёртывания или обновления Центра сертификации, для импортируемых шаблонов – это дата и время загрузки шаблонов в Центр сертификации, для новых пользовательских шаблонов – это дата и время клонирования шаблона).
- Дата и время изменения шаблона.
- Информация, сформированная в виде вкладок «Свойства», «Расширения», «Компоненты имени сертификата» и «Сведения о средствах ЭП».

На вкладке «Свойства» доступны (см. Рисунок 198):

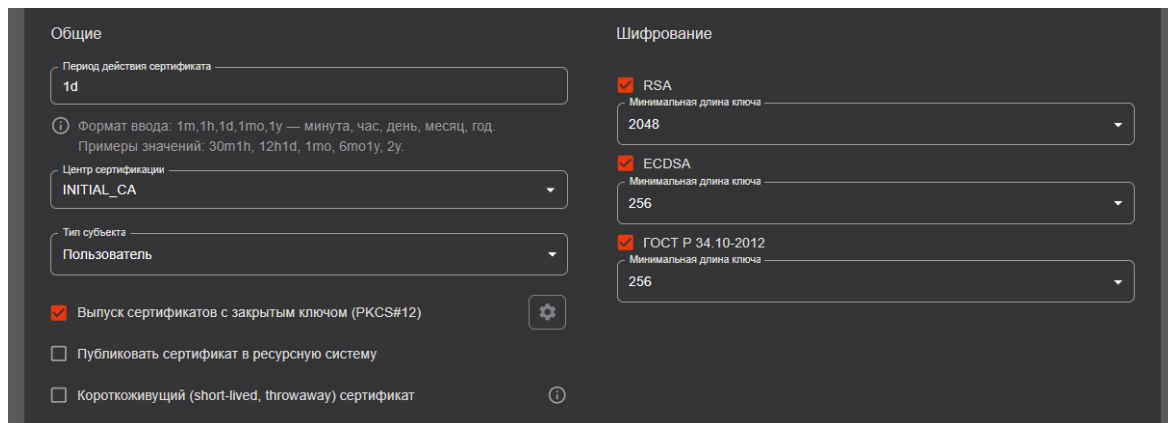



Рисунок 198 – Вкладка «Свойства» шаблона сертификата

- В разделе «Общие»:
  - Поле «Период действия сертификата». Формат ввода: 1m, 1h, 1d, 1mo, 1y – минута, час, день, месяц, год (примеры: 1d1y, 30m1h). Если включён чекбокс «Короткоживущий (short-lived, throwaway) сертификат», то период действия сертификата не может составлять более суток.
  - 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).
- чекбокс «Выпуск сертификатов с закрытым ключом (PKCS#12)». Для клонированных и импортированных шаблонов справа от данного чекбокса присутствует кнопка (пиктограмма «Настройка») для открытия окна «Настройка выпуска сертификатов с закрытым ключом (PKCS#12)» (см. 8.11.4).
- чекбокс «Публиковать сертификат в ресурсную систему»;
- чекбокс «Короткоживущий (short-lived, throwaway) сертификат». Справа от данного чекбокса присутствует пиктограмма «Информация», при наведении курсора на которую отображается всплывающее сообщение со справочным текстом.
- В разделе «Шифрование» (перечень доступных алгоритмов зависит от криптопровайдеров выбранного для данного шаблона Центра сертификации – издателя сертификатов):
  - RSA.
  - ECDSA.
  - ГОСТ Р 34.10–2012.

На вкладке «Расширения» доступны:

- Список с множественным выбором «Использование ключа»;
- Чекбокс «Считать это расширение критическим» для списка «Использование ключа».
- Список с множественным выбором «Расширенное использование ключа».
- Кнопка  рядом со списком «Расширенное использование ключа», которая позволяет создавать пользовательские идентификаторы расширенного использования ключа.
- Чек-бокс «Считать это расширение критическим» для списка «Расширенное использование ключа».
- Чек-бокс «Включить SID субъекта в сертификат». При включённой 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».

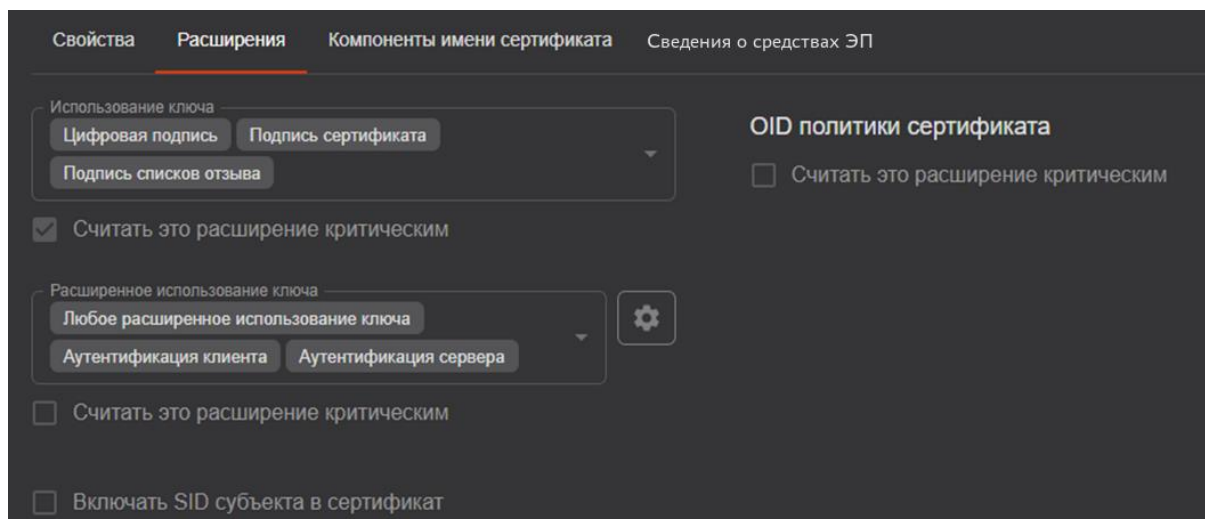


Рисунок 199 – Вкладка «Расширения» шаблона сертификата

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 200).

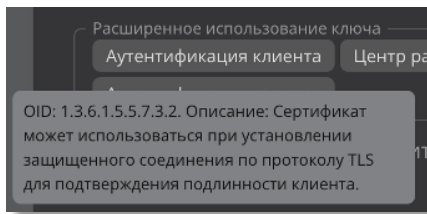


Рисунок 200 – Всплывающая подсказка значения расширенного использования ключа

На вкладке «Компоненты имени сертификата» доступны (см. Рисунок 201):

- Чек-бокс «Контролировать соответствие полей в сертификате атрибутам субъекта».
- Список атрибутов (типов полей) отличительного имени субъекта.
- Список атрибутов (типов полей) альтернативного имени субъекта.

Рисунок 201 – Карточка шаблона (вкладка «Компоненты имени сертификата»)

На вкладке «Сведения о средствах ЭП» доступны:

Рисунок 202 – Вкладка «Сведения о средствах ЭП»

- В разделе «Сведения о средствах ЭП и УЦ издателя» доступны:
  - Чек-бокс «Включать сведения о средствах ЭП и УЦ издателя» - при активации данной опции необходимо заполнить все поля данного подраздела, сведения из которых будут включены в сертификаты, выпущенные по данному шаблону.

- В разделе «Сведения о средстве ЭП владельца сертификата» доступен чек-бокс «Включать сведения о средстве ЭП владельца сертификата». При активации данной опции необходимо заполнить поле «Наименование средства ЭП владельца сертификата» данного подраздела, сведения из которого будут включены в сертификаты, выпущенные по данному шаблону.

#### 8.11.4 Настройка выпуска сертификатов с закрытым ключом (PKCS#12)

Для настройки выпуска сертификатов с закрытым ключом (PKCS#12):

1. Нажмите кнопку «Настройка» для чекбокса «Выпуск сертификатов с закрытым ключом (PKCS#12)» на вкладке «Свойства» карточки шаблона (см. рисунок 198).
2. В окне «Настройка выпуска сертификатов с закрытым ключом (PKCS#12)» (см. рисунок 203) задайте регулярное выражение и нажмите кнопку «Продолжить».

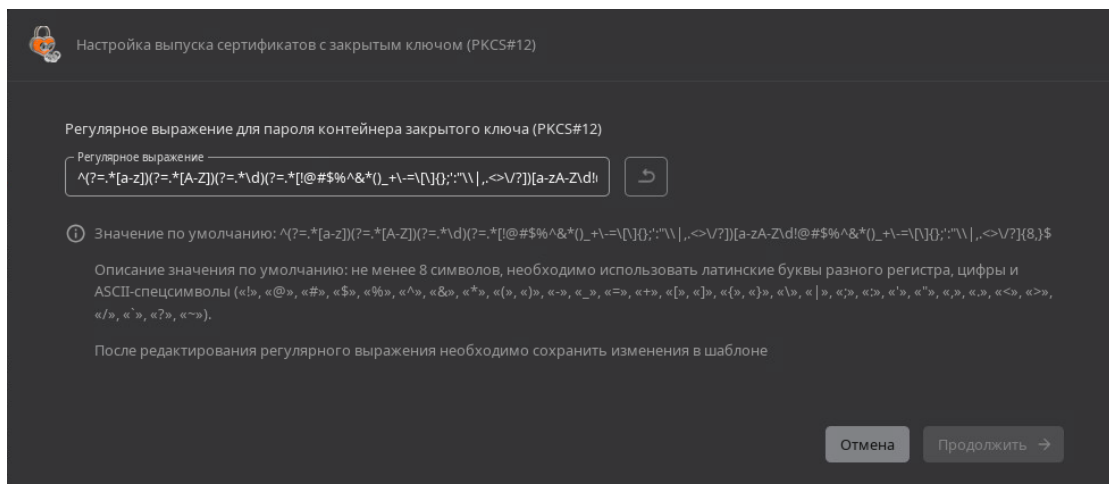





Рисунок 203 — Окно «Настройка выпуска сертификатов с закрытым ключом (PKCS#12)»

### 8.11.5 Создание пользовательского шаблона

Создание индивидуального шаблона возможно на базе предустановленных шаблонов и состоит из следующих этапов:

- Клонирования выбранного шаблона.
- Редактирование клонированного шаблона.

### Порядок клонирования шаблона:

- Подключитесь к веб-интерфейсу eCA-CA и перейдите в раздел  **Шаблоны**.
- Инициировать клонирования шаблона возможно двумя способами. Найдите в списке запись о шаблоне, который вы хотите клонировать, наведите указатель на запись о шаблоне в списке и нажмите появившуюся кнопку  или откройте карточку и нажмите аналогичную кнопку.
- В открывшемся окне действия (см. Рисунок 204) при необходимости отредактируйте имя нового пользовательского шаблона в соответствующем поле и нажмите кнопку . Имя шаблона должно быть уникальным. Длина имени шаблона не должна превышать 255 символов.

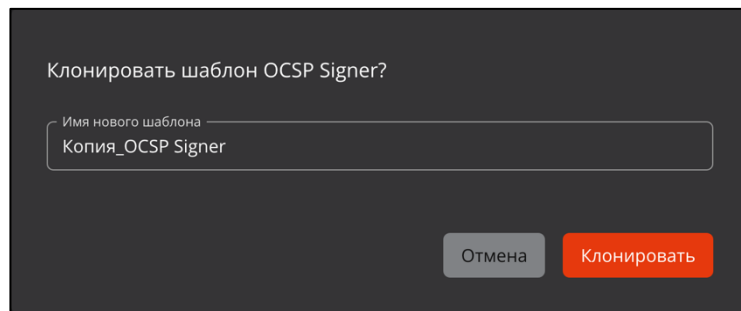


Рисунок 204 – Экран раздела меню «Шаблоны»

В случае успешного клонирования шаблона сертификата администратор будет уведомлен сообщением на экране «Шаблон успешно клонирован». В результате создаётся полная копия выбранного шаблона.

Редактировать можно только пользовательские и импортированные шаблоны.

**Внимание!** Шаблоны можно редактировать даже после выпуска по ним сертификатов.

Порядок редактирования шаблона:


- Подключитесь к веб-интерфейсу eCA-CA и перейдите в раздел  **Шаблоны**.
- Откройте карточку шаблона (см. Рисунок 205), редактирование которого вы хотите выполнить. Для этого найдите запись о нем в списке и выберите ее.

Рисунок 205 – Карточка шаблона (вкладка «Свойства»)

- При необходимости измените в поле «Имя шаблона» имя шаблона. Длина имени шаблона не должна превышать 255 символов.
- Перейдите на вкладку «Свойства» карточки шаблона (вкладка открывается по умолчанию при открытии карточки) и выполните редактирование необходимых полей и опции шаблона:
  - В разделе «Общие» в поле «Период действия сертификата» измените период действия сертификата, который будет выпущен по данному шаблону.

Формат ввода периода: 1m, 1h, 1d, 1mo, 1y – минута, час, день, месяц, год (примеры: 1d1y, 30m1h). Срок действия сертификата не должен быть больше 25 лет вне зависимости от единиц измерения времени, указанных в поле.

- В разделе «Общие» в списке «Центр сертификации» выберите Центр сертификации (по его отображаемому имени), в котором будет выполняться выпуск сертификатов по данному шаблону. Если выбрать значение «Любой», выпуск сертификатов по данному шаблону будет доступен в любом Центре сертификации. При этом по умолчанию выпуск сертификатов будет выполняться в активном на данный момент Центре сертификации.
- В разделе «Общие» списке «Тип субъекта» выберите тип субъекта, для которого предназначен данный шаблон.

Доступны следующие типы:

- Пользователь – для создания сертификата субъекта.
  - Устройство – для создания сертификата субъекта.
  - Корневой центр сертификации - для создания сертификата Центра сертификации.
  - Подчинённый центр сертификации - для создания сертификата Центра сертификации.
- Установите флажок «Публиковать сертификат в ресурсную систему» для автоматической публикации сертификата в ресурсную систему после его выпуска по данному шаблону.
- В разделе «Шифрование» с помощью флажков выберите криптографические алгоритмы, которые могут быть использованы при выпуске сертификатов по данному шаблону. Перечень доступных для выбора алгоритмов зависит от криптопровайдеров Центра сертификатов (издателя сертификатов), выбранного для данного шаблона в списке «Центр сертификации» раздела «Общие».

В общем случае доступны следующие алгоритмы:

- RSA.
- ECDSA.
- ГОСТ Р 34.10–2012.

Для каждого выбранного алгоритма в списках «Минимальная длина ключа» выберите минимальную длину ключа, доступную для выбора при выпуске сертификатов по данному шаблону.

Доступные для выбора длины ключей алгоритмов:

- RSA: 1024, 1536, 2048, 3072, 4096, 6144 или 8192 бит.
- ECDSA: 256, 384 или 521 бит.
- ГОСТ Р 34.10-2012: 256 или 512 бит.

- Перейдите на вкладку «Расширение» карточки шаблона (см. Рисунок 206) и при необходимости выполните редактирование (добавление, удаление) следующих полей и опций шаблона:

← Шаблоны

Имя шаблона  
A1\_MSCS\_Веб-сервер

Идентификатор: bc9e3a1e-f7bb-4a3c-8e8c-633f65cdb170

Дата создания: 23.10.2025 13:05:40

Дата изменения: 24.10.2025 14:53:43

Свойства   **Расширения**   Компоненты имени сертификата   Сведения о средствах ЭП и УЦ

Использование ключа  
Цифровая подпись   Шифрование ключей

☒ Считать это расширение критическим

Расширенное использование ключа  
Аутентификация сервера   Аутентификация клиента

☒ Считать это расширение критическим

☒ Включать SID субъекта в сертификат

OID политики сертификата  
OID \*: 1.3.6.1.4.1.9999.1

Добавить поле +

☐ Считать это расширение критическим

Рисунок 206 – Карточка шаблона (вкладка «Расширение»)

- В списке «Использование ключа» с помощью флажков определите обобщённое назначение открытого ключа сертификата, который будет выпущен по данному шаблону.

Возможные варианты использования открытого ключа:

- Цифровая подпись.
- Подтверждение подлинности.
- Шифрование ключей.
- Шифрование данных.
- Согласование ключей.
- Подпись сертификатов.
- Подпись списков отзыва.
- Только шифрование.
- Только расшифрование.
- В списке «Расширенное использование ключа» с помощью флажков определите уточнённое назначение открытого ключа сертификата, который будет выпущен по данному шаблону.



Перечень предустановленных <sup>1</sup> идентификаторов расширенного использования ключа:

- Любое расширенное использование ключа
- CSN 369791 TLS клиент.
- CSN 369791 TLS сервер.
- Аутентификация клиента.
- Подписание кода.
- EAP через LAN (EAPOL).
- EAP через PPP.
- Подписание ETSI TSL.
- Защита электронной почты.

<sup>1</sup> Описание предустановленных идентификаторов расширенного использования ключа приведено в приложении 4 «Описание предустановленных идентификаторов расширенного использования ключа».

- ICAO подписание списка отклонений.
- Управление Intel AMT.
- Интернет–обмен ключами для Ipsec.
- Аутентификация клиента Kerberos.
- Центр распространения ключей Kerberos.
- Подписание коммерческого MS кода.
- Подписание MS документа.
- Восстановление MS EFS.
- Зашифрованная MS файловая система.
- Подписание индивидуального MS кода.
- Вход с MS смарт–картой.
- OCSP подписант.
- Подписание Adobe PDF.
- Аутентификация PIV карты.
- SCVP клиент.
- SCVP сервер.
- Домен SIP.
- SSH клиент.
- SSH сервер.
- Аутентификация сервера.
- Отметка времени.
- ICAO подписание основного списка.

При необходимости вы можете создать пользовательские идентификаторы расширенного использования ключа. Для этого выполните следующие действия:

- Нажмите рядом со списком «Расширенное использование ключа» кнопку .
- В открывшемся окне (см. Рисунок 207) нажмите кнопку .

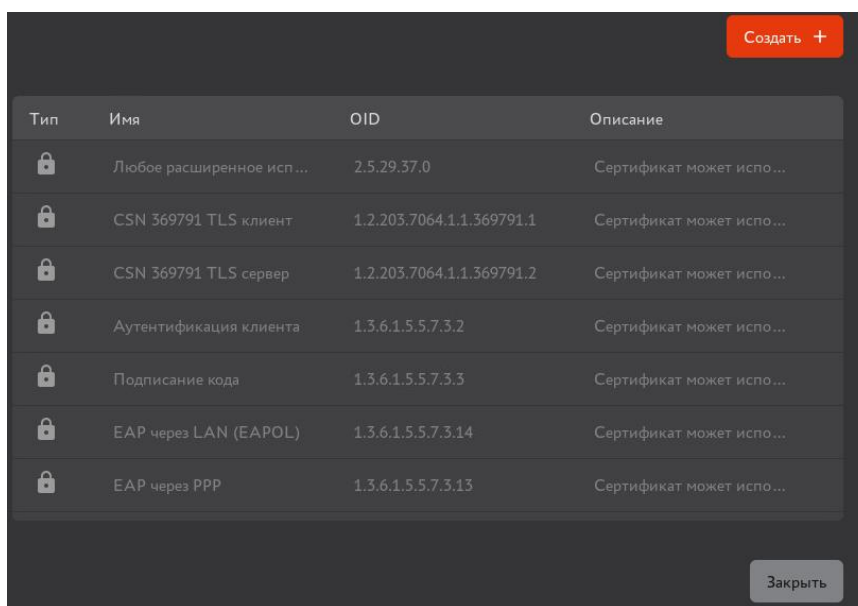


Рисунок 207 – Просмотр списка идентификаторов расширенного использования открытого ключа

- В открывшемся окне (см. Рисунок 208) в соответствующих поля укажите имя <sup>1</sup>, OID <sup>2</sup>, описание пользовательского идентификатора расширенного использования открытого ключа и нажмите кнопку

Создание идентификатора расширенного использования ключа

Укажите данные идентификатора расширенного использования ключа

Имя  
Новый идентификатор EKU



OID  
1.2.643.100.112


Описание  
Пользовательский ECU

Отмена Создать →

Рисунок 208 – Создание пользовательского идентификатора расширенного использования открытого ключа

В результате пользовательский идентификатор расширенного использования открытого ключа появится в списке в окне «Идентификаторы расширенного использования ключа» (см. Рисунок 207) и будет доступен для добавления в шаблон.

Пользовательские идентификаторы расширенного использования открытого ключа помечены в списке значком , предустановленные – значком .

Чтобы удалить пользовательский идентификатор расширенного использования открытого ключа, найдите его в списке и нажмите кнопку .

**Внимание! Удалить предустановленные или пользовательские идентификаторы расширенного использования открытого ключа, которые используются в других шаблонах, невозможно.**

После создание всех необходимых пользовательских идентификаторов расширенного использования открытого ключа нажмите в окне «Идентификаторы расширенного использования ключа» (см. Рисунок 207) кнопку

- При необходимости определите политики сертификатов, которые будут выпущены по данному шаблону.

Для этого в разделе «OID политики сертификата» выполните следующие действия:

- Нажмите кнопку
- В появившемся поле «OID\*» укажите идентификатор политики в соответствии с рекомендацией ITU X.660 (рекомендация определяет древовидную структуру, которая поддерживает международные OID).
- Чтобы добавить новый OID политики сертификаты, повторите действия настоящего сценария.

Чтобы удалить политику, нажмите рядом с полем «OID\*» выбранной политики кнопку .

<sup>1</sup> Имена идентификаторов расширенного использования открытого ключа должны быть уникальными. Если введенное имя принадлежит уже существующему идентификатору, система выводит сообщение об ошибке «Указанное имя уже используется».

<sup>2</sup> Идентификатор объекта (OID) должен соответствовать рекомендации ITU X.660 (рекомендация определяет древовидную структуру, которая поддерживает международные OID). OID идентификаторов расширенного использования открытого ключа должны быть уникальными. Если введенный OID принадлежит уже существующему идентификатору, система выводит сообщение об ошибке «Указанный OID уже используется».

- Чтобы при выпуске сертификата по данному шаблону расширения помечались как критические, установите флажки «Считать это расширение критическим» для выбранных типов расширений.

При обработке сертификата с расширениями, помеченными как критические:

- Системы, понимающие расширения, в зависимости от содержимого расширения принимают или отклоняют сертификат.
- Системы, не понимающие расширение, отклоняют сертификат.

При обработке сертификата с расширениями, не помеченными как критические:

- Системы, понимающие расширения, в зависимости от содержимого расширения принимают или отклоняют сертификат.
- Системы, не понимающие расширение, принимают сертификат.

Подробное описание приведено в RFC 5280.

- Чтобы при выпуске сертификата по данному шаблону в его состав был включен SID (идентификатор безопасности)<sup>1</sup> субъекта, установите флажок «Включать SID субъекта в сертификат».
- Перейдите на вкладку «Компоненты имени сертификата» карточки шаблона (см. рисунок 209) и при необходимости выполните редактирование (добавление, удаление) полей и опций шаблона.

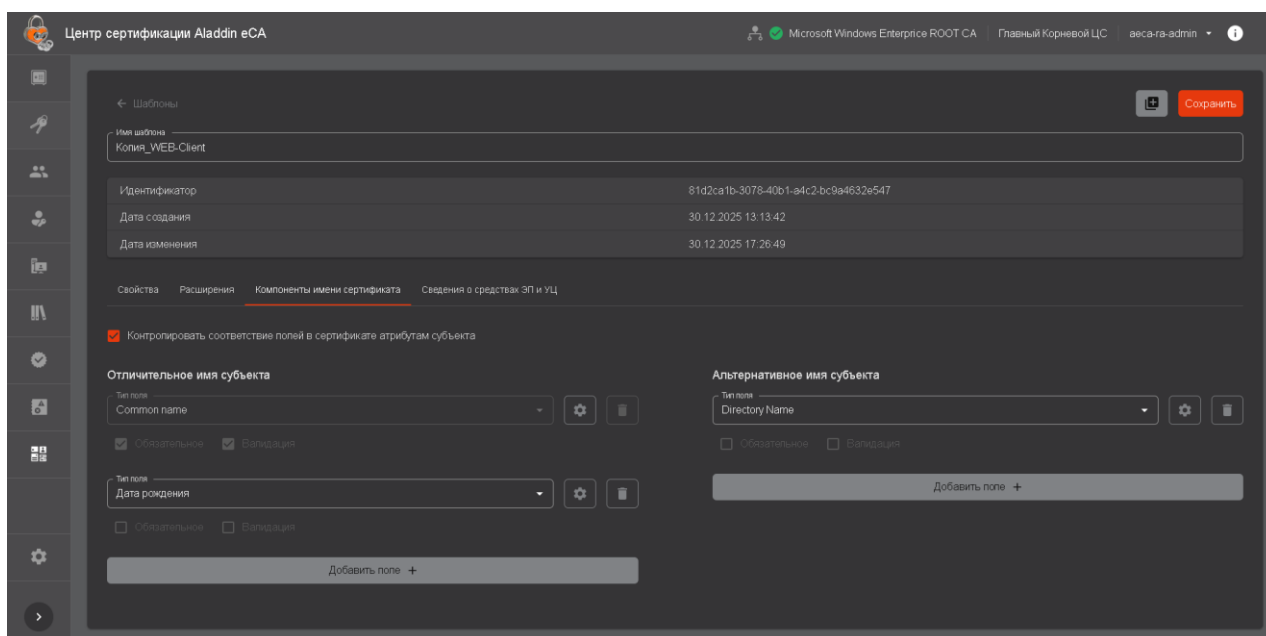


Рисунок 209 – Карточка шаблона (вкладка «Компоненты имени сертификата»)

- С помощью флажка «Контролировать соответствие полей в сертификате атрибутам субъекта» определите возможность выпуска по данному шаблону сертификатов без валидации соответствия атрибутов, передаваемых во входных параметрах (в CSR или в полях методов выпуска), атрибутам субъектов.

**Внимание!** Отключение данной опции в шаблоне позволяет записывать в поля сертификата любые (в соответствии с регулярными выражениями полей) значения, не соответствующие атрибутам субъекта. Контроль соответствия полей не выполняется только при выпуске сертификатов через REST API<sup>2</sup>. Использование таких шаблонов в информационных системах крайне не рекомендуется. При использовании таких шаблонов контроль соответствия значений в SDN и SAN полях сертификатов необходимо обеспечивать средствами внешней системы, и доступ к таким шаблонам должен быть строго ограничен.

<sup>1</sup> Атрибут SID может присутствовать только у субъектов ресурсных систем MS AD, SambaDC, РЕД АДМ и Альт Домен.

<sup>2</sup> Описание REST API приведено в документе «Центр сертификатов доступа Aladdin Enterprise Certificate Authority Certified Edition. Руководство администратора. Часть 3. Описание методов REST API «Центра сертификации Aladdin Enterprise Certification Authority».

При отключении контроля соответствия полей в сертификате атрибутам субъекта в открывшемся окне подтвердите данное действие.

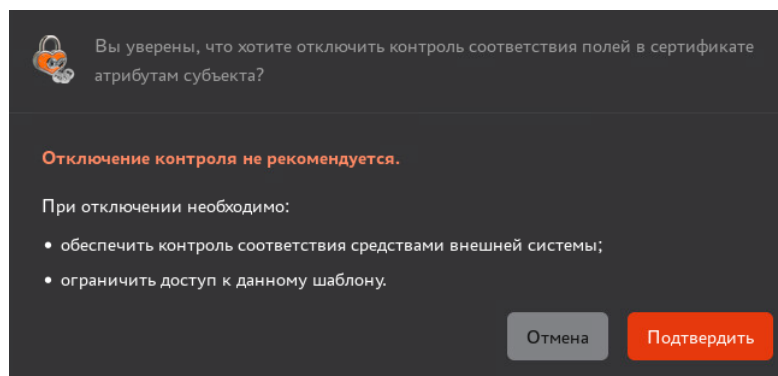


Рисунок 210 – Подтверждение отключения контроля соответствия полей в сертификате атрибутам субъекта

**Внимание!** После обновления ПО до версии 2.4 у всех имеющихся в программе шаблонов опция «Контролировать соответствия полей в сертификате атрибутам субъекта» включена по умолчанию.


- При необходимости определите атрибуты (типов полей) отличительного имени субъекта (SDN), которые будут включены в сертификат, выпущенный по данному шаблону.

Отличительное имя субъекта может содержать следующие атрибуты (типы полей):

- Common name.
- Unique Identifier (UID).
- Given name.
- Initials.
- Surname.
- Organizational Unit.
- Organization.
- Locality.
- State or Province.
- Domain Component.
- Country.
- Postal Code.
- Business Category.
- Telephone number.
- Pseudonym.
- Postal address.
- Street.
- Name.
- Title.
- Domain qualifier.
- Description.
- Role.
- Unstructured address.
- Unstructured name.
- Email Address (E).

- Serial number.
- Дата рождения.
- Место рождения.
- ИНН.
- ОГРН.
- ОГРНИП.
- СНИЛС.
- ИНН ЮЛ.

Чтобы добавить атрибут (тип поля)<sup>1</sup> в отличительное имя субъекта, в разделе «Отличительное имя субъекта» (см. рисунок 209) выполните следующие действия:

- Нажмите кнопку .
- В появившемся списке «Тип поля» выберите атрибут (тип поля) отличительного имени субъекта, который будет включён в сертификат.


Для поиска атрибута введите в поле списка ключевые слова, содержащиеся в названии атрибута.

- Чтобы добавить следующий атрибут (тип поля), повторите действия настоящего сценария.
- При необходимости определите состав атрибутов (типы полей) альтернативного имени субъекта (SAN), которое будет включено в сертификат, выпущенный по данному шаблону.

Альтернативное имя субъекта может содержать следующие атрибуты (типы полей):

- RFC 822 Name.
- DNS Name.
- IP address.
- Directory Name.
- Uniform resource identifier.
- Registered Identifier (OID).
- MS UPN, User Principal Name.
- MS GUID, Globally Unique Identifier.
- Kerberos KPN, Kerberos 5 Principal Name.
- Permanent Identifier.
- Xmpp address.
- Service Name.
- Subject Identification Method.



Чтобы добавить атрибут (тип поля) в альтернативное имя субъекта в разделе «Альтернативное имя субъекта» (см. рисунок 209) выполните следующие действия:

- Нажмите кнопку .
- В появившемся списке «Тип поля» выберите тип поля альтернативного имени субъекта, который будет включён в сертификат.

Для поиска атрибута введите в поле списка ключевые слова, содержащиеся в названии атрибута.

- Чтобы добавить следующий атрибут (тип поля), повторите действия настоящего сценария.

<sup>1</sup> Тип поля «Common Name» является обязательным для отличительного имени субъекта в шаблонах. Удалить данный тип поля нельзя.

- Если чекбокс «Обязательное» для атрибута (типа поля) отличительного или альтернативного имени субъекта не включён, то такой атрибут является необязательными. И выпуск сертификата по данному шаблону для субъекта будет возможен, даже если у субъекта отсутствует данный атрибут. Для управления чекбоксом «Обязательное»:
  - Нажмите на кнопку «Настройки»  для поля шаблона (см. рисунок 209).
  - Воспользуйтесь чекбоксом «Обязательное».
  - Нажмите кнопку «Продолжить» для подтверждения изменений, иначе нажмите «Отмена».
- Если чекбокс «Валидация» для атрибута (тип поля) отличительного или альтернативного имени субъекта отключён, то необходимость его валидации при выпуске сертификата отключена. И выпуск сертификата по такому шаблону для субъекта будет возможен, даже если значение данного атрибута у субъекта не соответствует правилам валидации. Вы можете для атрибутов отличительного или альтернативного имени определить необходимость обязательной валидации значений атрибутов субъектов при выпуске сертификата с помощью флажков «Валидация». Для управления валидацией (проверкой записываемого в поле значения на соответствие регулярному выражению):
  - Нажмите на кнопку «Настройки»  для поля шаблона (см. рисунок 209).
  - Воспользуйтесь чекбоксом «Валидация».
  - Если на предыдущем шаге был включён чекбокс «Валидация», то задайте регулярное выражение в поле «Регулярное выражение» (см. рисунок 211).

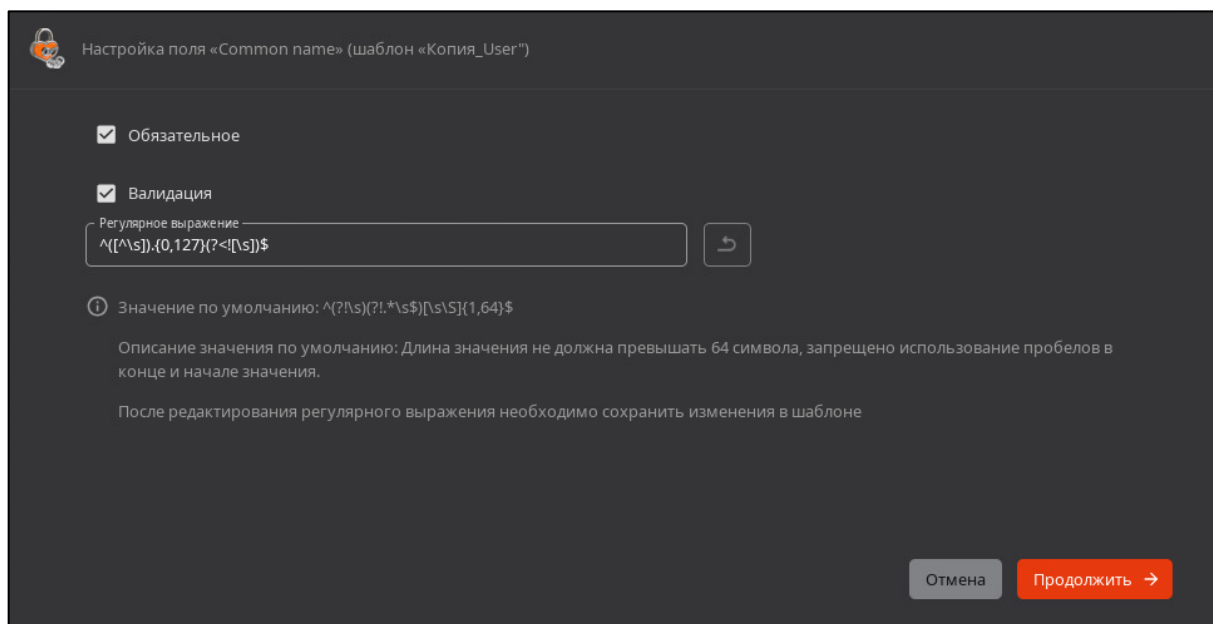



Рисунок 211 — Окно «Настройка поля шаблона»

- Для возврата значения регулярного выражения по умолчанию (при его наличии для данного поля) нажмите кнопку .
- Нажмите кнопку «Продолжить» для подтверждения изменений, иначе нажмите «Отмена».
- Перейдите на вкладку «Сведения о средствах ЭП и УЦ издателя» (см. рисунок 212) карточки шаблона и при необходимости выполните редактирование (добавление) следующих полей и опций шаблона:
  - Чтобы добавить в шаблон сведения о средствах ЭП и УЦ издателя в разделе «Сведения о средствах ЭП и УЦ издателя» установите флажок «Включать сведения о средствах ЭП и УЦ издателя» и обязательно в порядке заполните следующие поля:



- Наименование средства ЭП издателя.
  - Заключение на средство ЭП - номер и дата выдачи заключения на средство ЭП УЦ издателя.
  - Наименование средства УЦ издателя.
  - Заключение на средство УЦ - номер и дата выдачи заключения на средство УЦ издателя.
- Чтобы добавить в шаблон сведения о средствах ЭП владельца сертификата в разделе «Сведения о средстве ЭП владельца сертификата» установите флажок «Включать сведения о средстве ЭП владельца сертификата» и заполните поле «Наименование средства ЭП владельца сертификата».

Рисунок 212 – Карточка шаблона (вкладка «Сведения о средствах ЭП и УЦ издателя»)

- Для сохранения изменений, внесённых в шаблон, нажмите кнопку .

### 8.11.6 Удаление шаблонов сертификатов

Удалить можно только пользовательские и импортированные шаблоны.  
Удалять можно как один выбранный шаблон, так и несколько шаблоном одновременно.  
Порядок удаление одного выбранного шаблона:

- Подключитесь к веб-интерфейсу eCA-CA и перейдите в раздел  **Шаблоны**.
- Найдите в списке запись о шаблоне, который вы хотите удалить.
- Наведите указатель на запись о шаблоне в списке и нажмите появившуюся кнопку .

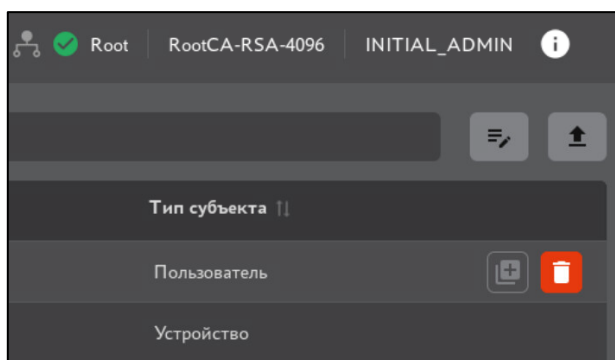



Рисунок 213 – Инициализация процесса удаления шаблона

- В открывшемся окне нажмите кнопку .

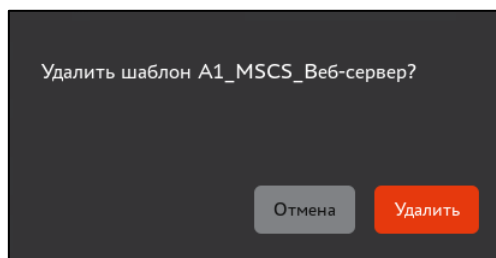







Рисунок 214 – Окно подтверждения удаления шаблона сертификата

После удаления шаблона сертификаты, выпущенные по нему, остаются действительными.  
Порядок одновременного удаления нескольких шаблонов:

- Подключитесь к веб-интерфейсу eCA-CA и перейдите в раздел  **Шаблоны**.
- На панели инструментов нажмите кнопку .
- В открывшемся окне (см. Рисунок 215) выполните следующие действия:
  - В списке «Выбрать» с помощью флажков выберите шаблоны, которые необходимо удалить, и щёлкните значок . В результате выбранные шаблоны будут перемещены в список «Выбрано».
  - Чтобы изменить список удаляемых шаблонов, в списке «Выбрано» с помощью флажков выберите шаблоны, исключаемые из списка удаляемых, и щёлкните значок . В результате выбранные шаблоны будут перемещены в список «Выбрать».
  - Чтобы найти шаблон в списках, используйте поля поиска.
  - Нажмите кнопку .

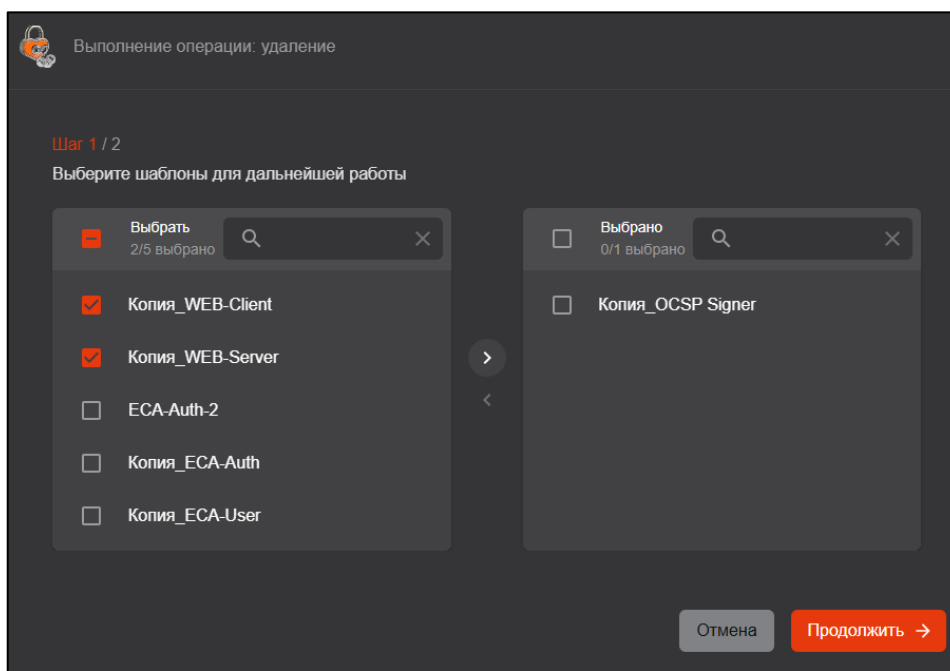


Рисунок 215 – Выбор шаблонов для удаления

- В открывшемся окне подтвердите действие, нажав кнопку **<Применить>** (см. Рисунок 216).

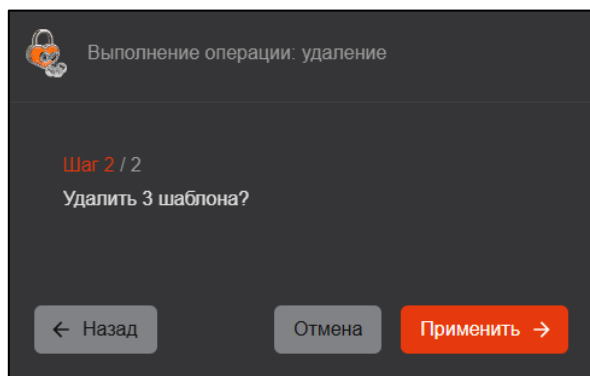


Рисунок 216 – Окно выполнения массовых операций. Шаг 3

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

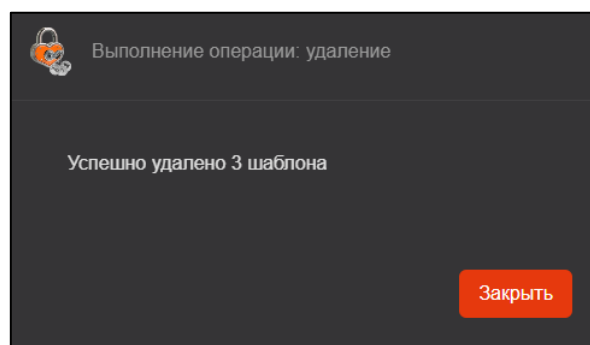


Рисунок 217 – Окно выполнения массовых операций. Шаг 4

### 8.11.7 Импорт шаблонов MS CS



Перед импортом шаблонов MS CS в eCA-CA необходимо предварительно экспортировать их из MS CS.

Для экспорта шаблонов запустите скрипт **mscs2aeca.ps1** (файл расположен в каталоге `/opt/aecaCa/scripts/external`) из консоли «Windows PowerShell», запущенной от имени администратора на хосте Центра сертификации MS CS. Скрипт запускается как консольное приложение и работает в режиме командной строки. Графический интерфейс не предусмотрен.

**Внимание!** Для успешного выполнения скрипта необходимо интернет-соединение. Для успешного выполнения скрипта в оффлайн-режиме требуется предварительно скачать и установить пакет NuGet.

Шаблоны экспортируются в файл формата CSV с разделителем «;». Файл с шаблонами расположен в каталог `C:\temp\` на хосте Центра сертификации MS CS.

Порядок импорта шаблонов MS CS в eCA-CA из файла:

- Подключитесь к веб-интерфейсу eCA-CA и перейдите в раздел  **Шаблоны**.
- На панели инструментов нажмите кнопку .
- В открывшемся окне укажите путь к CSV-файлу с шаблонами MS CS и нажмите кнопку **<Открыть>**.

В результате шаблоны MS CS будут импортированы, и администратор будет уведомлён сообщением на экране «XX шаблонов успешно загружено», где «XX» – количество успешно загруженных шаблонов (см. Рисунок 218).

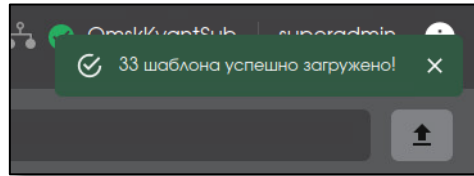


Рисунок 218 – Уведомление об успешной загрузке шаблонов MSCS

В случае, если шаблоны не были импортированы, администратор будет уведомлён сообщением «Невозможно загрузить шаблоны» (см. Рисунок 218).

При импорте шаблона из MS CS к названию шаблона добавляется префикс «MSCS\_». Если в системе уже существует шаблон, совпадающий с именем импортируемого, то к имени импортируемого добавляется суффикс «\_1» и т.д. (счётчик копий).

Поля, загружаемые из CSV-файла с шаблонами MS CS, приведены в таблице 19.

Таблица 19 – 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, CritExts	Расширенное использование ключа	Расширенное использование ключа; флажок «считать это расширение критическим»
Polices, CritExts	Политики	OID политики сертификата; флажок «считать это расширение критическим»

При импорте шаблонов из MS CS 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 «Подчинённый ЦС».

При импорте шаблонов из MS CS для параметра «Центр сертификации» импортируемого шаблона будет установлено значение «Любой».

При повторной загрузке файла шаблонов MS CS, все шаблоны будут загружены повторно. Имя шаблона будет сформировано из значения, записанного в поле шаблона «TmplName», и присвоением порядкового номера (счетчик копий).

## 8.12 Смена сертификата веб-сервера

Предварительно выпустите по шаблону WEB–Server сертификат для субъекта локальной ресурсной системы (см. приложение 1 «Создание сертификата для субъекта»). У субъекта должны присутствовать следующие атрибуты:


- Common name – имя веб–сервера, отображаемое в веб-интерфейсе (рекомендуется указать имя сервера, на котором развернут «Центр сертификации Aladdin Enterprise Certification Authority» .
- DNS Name – имя хоста, на котором развёрнут eCA-CA (должно совпадать с именем, указанным в файле `/etc/hosts`).

Импортируемый сертификат должен отвечать следующим требованиям:

- должен быть действительным;
- должен содержать идентификатор расширенного использования ключа «Server Authentication» (OID 1.3.6.1.5.5.7.3.1);

- если используется веб-сервер Cppnginx, алгоритм ключа в импортируемом сертификате не должен быть отличен от ГОСТ Р 34.10-2012. При попытке импорта сертификата с иным алгоритмом ключа будет отображаться уведомление об ошибке «При использовании cppnginx установка сертификата с алгоритмом ключа, отличным от ГОСТ Р 34.10-2012, недоступна».

Для смены сертификата веб-сервера выполните следующие действия:

- Подключитесь к веб-интерфейсу eCA-CA и перейдите в раздел  **Настройки > Веб-сервер** (Рисунок 219).

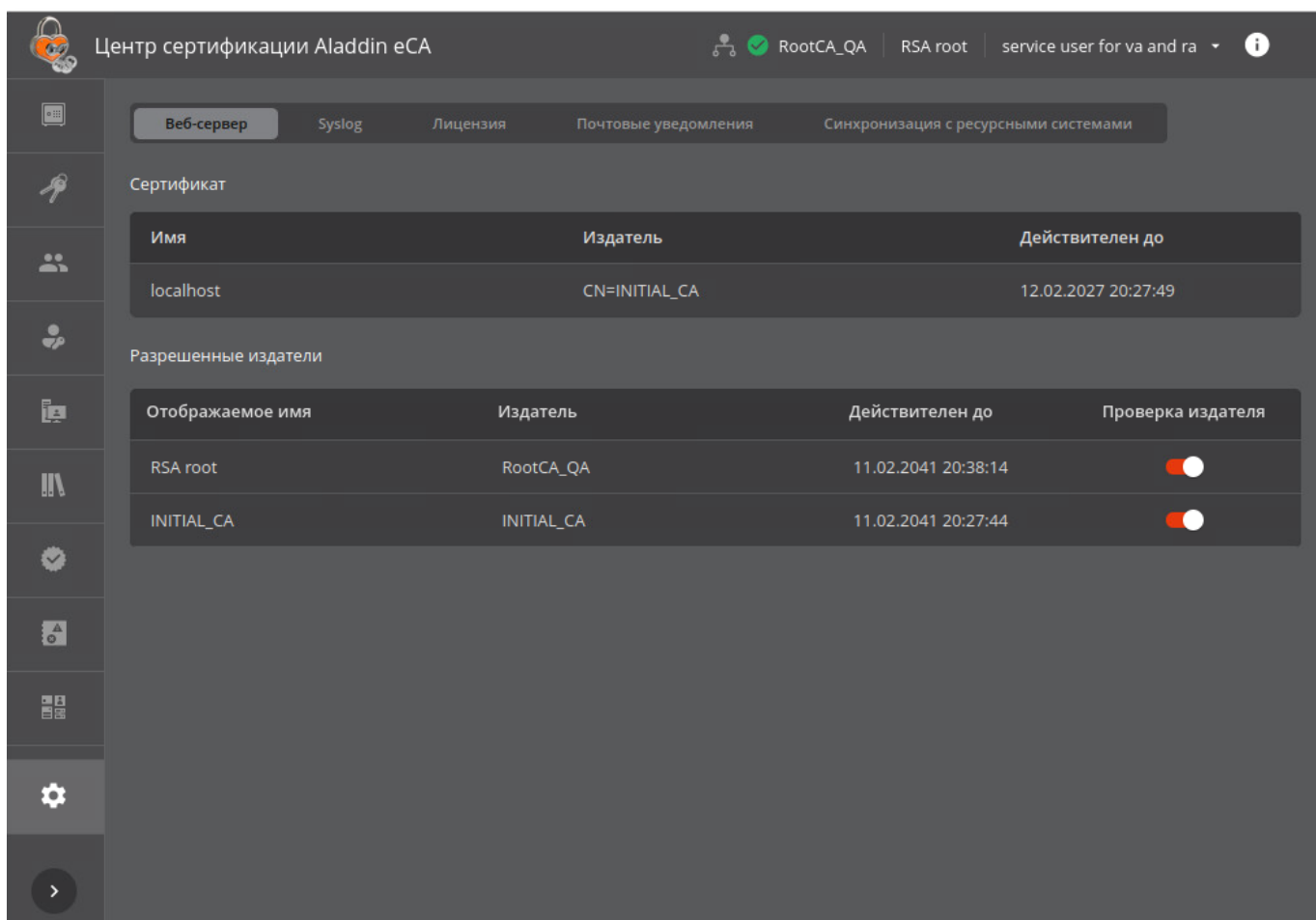




Рисунок 219 – Экран раздела «Настройки»

Информация об установленном сертификате отображается в разделе «Сертификат» в табличном виде и содержит:

- «Имя» – CN, указанный в сертификате.
- «Издатель» – SDN издателя сертификата.
- «Действителен до» – дата окончания действия сертификата.
- Наведите на запись о веб-сервере и нажмите появившуюся кнопку .
- В появившемся окне (см. Рисунок 220) выберите файл сертификата и введите пароль от контейнера.
- Нажмите кнопку .

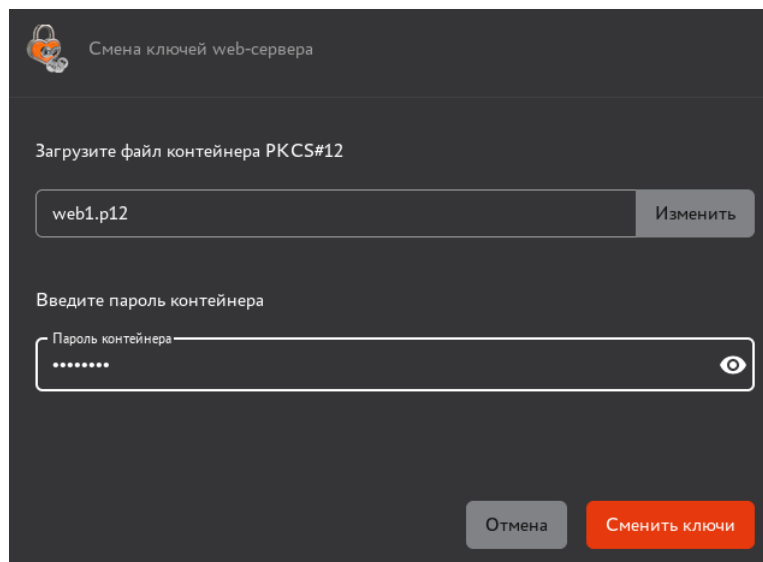



Рисунок 220 – Смена ключей веб-сервера

- В открывшемся окне с сообщением об успешной смене ключей нажмите кнопку .


В результате будет выполнена автоматическая перезагрузка веб-сервера. В результате перезагрузки веб-сервера в журнале событий будет зарегистрировано событие с кодом CAENV040 в случае успешной перезагрузки веб-сервера или событие с кодом CAENV041 в случае ошибки в процессе перезагрузки веб-сервера.

### 8.13 Управление разрешёнными издателями

Для доступа пользователей с ролями «Администратор» и «Оператор» к текущему веб-серверу необходимо, чтобы для издателя (Центра сертификации) сертификата учётной записи была включена проверка (издатель включен в список разрешённых). С сертификатом, выпущенным исключённым из списка разрешённых издателем, аутентификация пользователя будет невозможна.

Для просмотра списка разрешённых издателей подключитесь к веб-интерфейсу eCA-CA и перейдите в раздел  **Настройки > Веб-сервер** (Рисунок 219).

Информация о разрешённых издателях отображается в разделе «Разрешённые издатели» списком в табличном виде и содержит:

- «Отображаемое имя» – отображаемое имя Центра сертификации.
- «Издатель» – CN, указанный в сертификате Центра сертификации.
- «Действителен до» – дата окончания действия сертификата Центра сертификации.
- Для каждого издателя в списке в столбце «Проверка издателя» присутствует переключатель , позволяющий включить или исключить Центр сертификации из списка разрешённых издателей.

### 8.14 Управление правилами сопоставления атрибутов

По умолчанию используются следующие правила преобразования атрибутов субъектов из ресурсной системы при сохранении (обновлении) загруженных данных в базу субъектов ПО AECA-CA.

Атрибут субъекта AECA-CA	Поле в MS AD, SambaDC, RED ADM, Альт Домен		Поле в ALD PRO, FreeIPA, Dynamic Directory		
	Тип субъекта		Тип субъекта		
	Пользователь	Компьютер	Пользователь	Компьютер	Сервис
Id *	ObjectGUID	ObjectGUID	ipaUniqueID	ipaUniqueID	ipaUniqueID
Common name	cn	cn	cn	cn	krbPrincipalName
			uid		
Initials	-	-	initials	-	-

Атрибут субъекта AECA-CA	Поле в MS AD, SambaDC, RED ADM, Альт Домен		Поле в ALD PRO, FreeIPA, Dynamic Directory		
	Тип субъекта		Тип субъекта		
	Пользователь	Компьютер	Пользователь	Компьютер	Сервис
Surname	sn	-	sn	-	-
Given Name	givenName	-	givenName	-	-
Organization	-	-	krbPrincipalName	krbPrincipalName	krbPrincipalName
Name	name	name	-	serverHostName	-
MS GUID	-	ObjectGUID	-	-	-
Description	description	-	-	-	-
DNS Name	-	dNSHostName	-	fqdn	-
Email Address (Mail)	mail	-	mail	-	-
	userPrincipalName	-	krbPrincipalName	krbPrincipalName	krbPrincipalName
RFC 822 NAME	mail	-	mail	-	-
	userPrincipalName	-	krbPrincipalName	krbPrincipalName	krbPrincipalName
MS UPN	userPrincipalName	-	krbPrincipalName	krbPrincipalName	krbPrincipalName
Unique Identifier (UID)	-	-	uid	-	-
Kerberos KPN, Kerberos 5 Principal	-	-	-	krbPrincipalName	-
SID *	objectSid	objectSid	-	-	-

\* - правила сопоставления для атрибутов Id (идентификатор субъекта) и SID (SID субъекта) будут отсутствовать в списке правил сопоставления в разделе «Настройки» на вкладке «Синхронизация с ресурсными системами». Данными правилами сопоставления нельзя управлять в eCA-CA.

#### 8.14.1 Создание правила сопоставления атрибутов

Для создания правила сопоставления атрибутов:

1. В eCA-CA перейдите в раздел «Настройки» на вкладку «Синхронизация с ресурсными системами».
2. В подразделе «Правила сопоставления атрибутов» нажмите на кнопку «Создать».
3. В окне «Создание правила сопоставления атрибутов» (см. рисунок 221) укажите параметры правила сопоставления атрибутов:
  - «Тип ресурсной системы». В данном поле доступен выбор значения из списка: «Samba DC», «ALD PRO», «FreeIPA», «MS AD», «RED ADM», «Альт Домен» и «ROSA Dynamic Directory».
  - «Тип объекта». В данном поле доступен выбор значения из списка: «Пользователь», «Компьютер», «Сервис» (только если в поле «Тип ресурсной системы» выбрано значение «ALD PRO», «FreeIPA» или «ROSA Dynamic Directory»).
  - «Атрибут объекта в ресурсной системе». В данном поле доступен ввод названия атрибута объекта в ресурсной системе, значение которого должно записываться в атрибут(-ы) субъекта в eCA-CA. Значение, указываемое в данном поле, должно быть уникальным в рамках правил сопоставления атрибутов для данного типа объекта данного типа ресурсной системы. Допускается указание только латинских символов, цифр и дефиса.

- «Атрибут субъекта в еСА». В данном поле доступен выбор атрибутов (одного или нескольких), в которые должно записываться значение указанного в поле «Атрибут объекта в ресурсной системе» атрибута объекта данного типа при синхронизации с РС данного типа.
- Нажмите кнопку «Создать».

Рисунок 221 — Окно «Создание правила сопоставления атрибутов»

### 8.14.2 Редактирование правила сопоставления атрибутов

Для редактирования правила сопоставления атрибутов:

1. В еСА-СА перейдите в раздел «Настройки» на вкладку «Синхронизация с ресурсными системами».
2. В подразделе «Правила сопоставления атрибутов» в строке правила нажмите кнопку «Редактировать».
3. Отредактируйте параметры. Для редактирования доступны параметры «Атрибут объекта в ресурсной системе» и «Атрибут субъекта в еСА».
4. Для сохранения результатов редактирования нажмите кнопку «Сохранить изменения», иначе нажмите «Отмена».

### 8.14.3 Удаление правила сопоставления атрибутов

1. В еСА-СА перейдите в раздел «Настройки» на вкладку «Синхронизация с ресурсными системами».
2. В подразделе «Правила сопоставления атрибутов» в строке правила нажмите кнопку «Удалить».
3. В диалоговом окне подтвердите удаление при помощи кнопки «Удалить», иначе нажмите кнопку «Отмена».

## 8.15 Управление параметрами рассылки уведомлений об истечении срока действия сертификатов субъектов

### 8.15.1 Добавление почтового сервера

Для добавления почтового сервера:

1. В еСА-СА перейдите в раздел «Настройки» на вкладку «Почтовые уведомления» (см. рисунок 222).

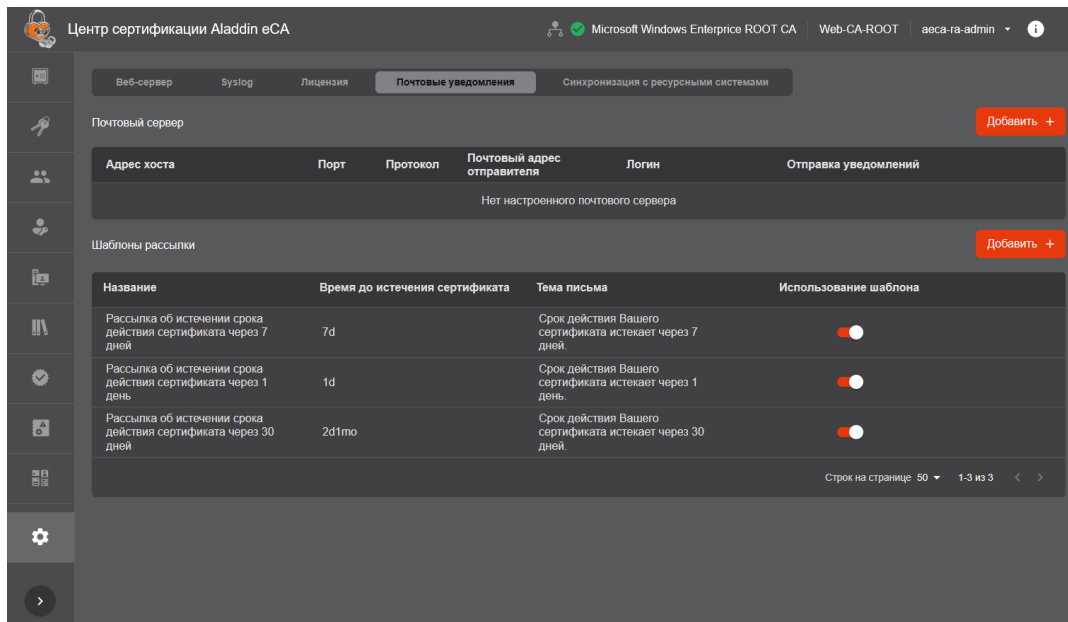


Рисунок 222 — Вкладка «Почтовые уведомления» раздела «Настройки» до добавления почтового сервера

2. В подразделе «Почтовые серверы» нажмите на кнопку «Добавить» (данная кнопка будет отображаться только при отсутствии добавленного почтового сервера).
3. В окне «Добавление почтового сервера» (см. рисунок 223) укажите следующие параметры почтового сервера:
  - 3.1. «Адрес хоста». В данном поле укажите адрес хоста почтового сервера (доступно указание IP-адреса или DNS-имени). Если адрес хоста не указан, то в данном поле ввода будет отображаться сообщение об ошибке «Обязательно к заполнению» (кнопка «Добавить» будет недоступна для нажатия).
  - 3.2. «Порт». В данном поле укажите порт для подключения к почтовому серверу. Формат ввода – число от 1 до 65535. Если порт не указан, то в данном поле ввода будет отображаться сообщение об ошибке «Обязательно к заполнению» (кнопка «Добавить» будет недоступна для нажатия).
  - 3.3. «Протокол». В данном поле по умолчанию указано значение «SMTP» без возможности редактирования.
  - 3.4. «Почтовый адрес отправителя».
  - 3.5. Чекбокс «Использовать SMTP-аутентификацию». По умолчанию данный чек-бокс включён. Если данный чекбокс включён, то отображаются следующие поля ввода:
    - 3.5.1. «Логин». В данном поле укажите логин пользователя, от имени которого будет выполняться подключение к почтовому серверу.
    - 3.5.2. «Пароль». В данном поле укажите пароль пользователя, от имени которого будет выполняться подключение к почтовому серверу.
  - 3.6. Чекбокс «Использовать TLS при подключении (STARTTLS)». Данный чекбокс позволяет управлять состоянием директивы STARTTLS при подключении к почтовому серверу.

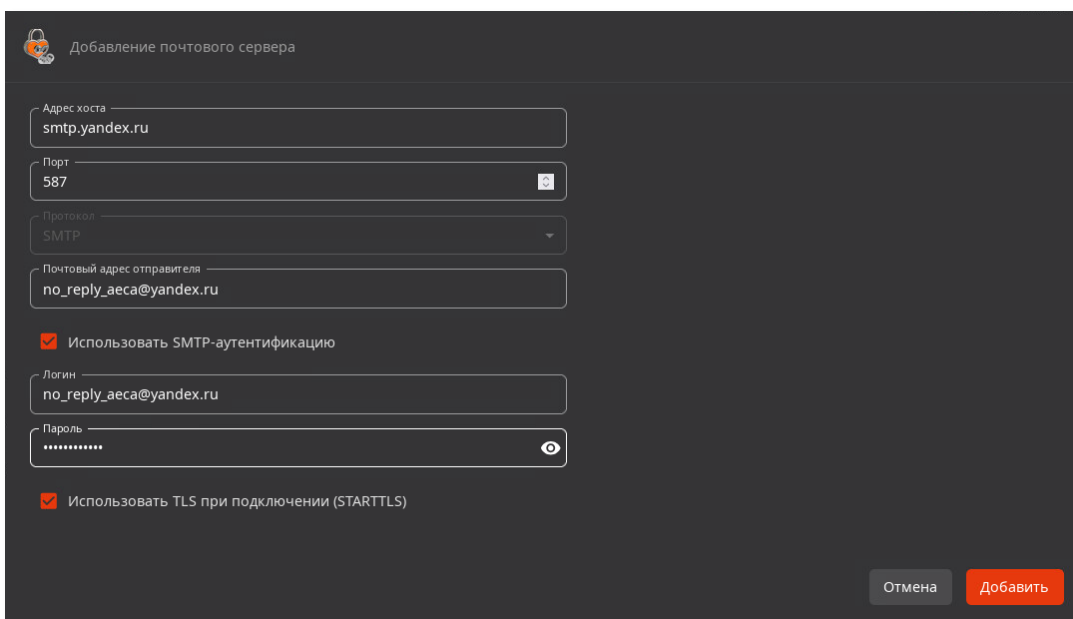


Рисунок 223 — Окно «Добавление почтового сервера»

4. Нажмите кнопку «Добавить».

### 8.15.2 Редактирование параметров почтового сервера

Для редактирования параметров почтового сервера:

1. В еСА-СА перейдите в раздел «Настройки» на вкладку «Почтовые уведомления» (см. рисунок 224).

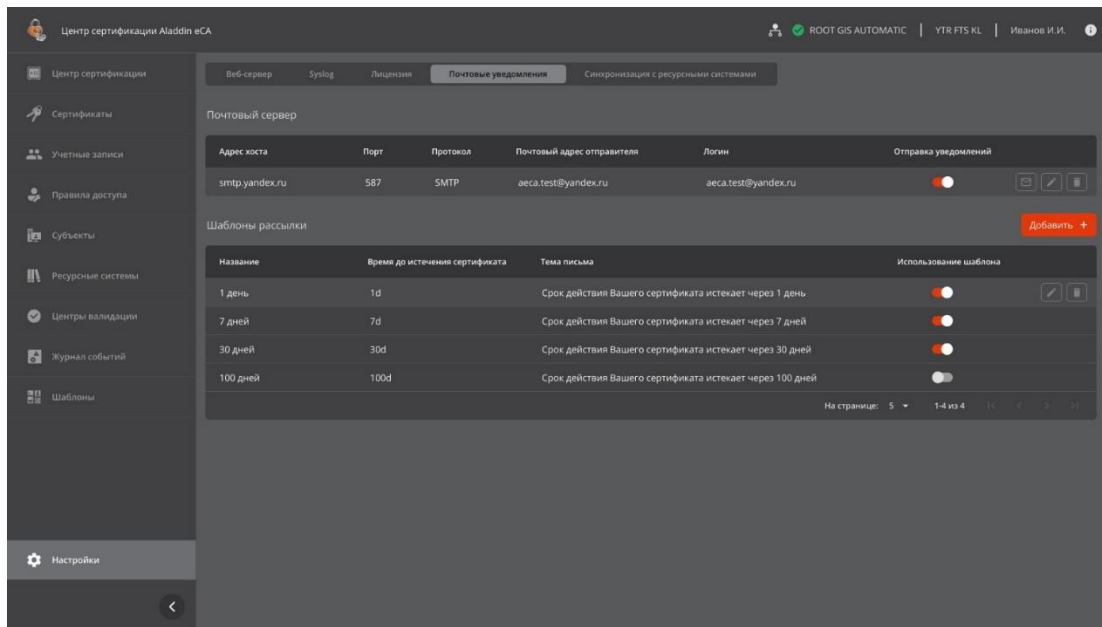


Рисунок 224 — Вкладка «Почтовые уведомления» раздела «Настройки» после добавления почтового сервера

2. В подразделе «Почтовые серверы» нажмите на кнопку «Редактировать» для почтового сервера.
3. В окне «Редактирование почтового сервера» отредактируйте параметры почтового сервера (параметры аналогичны параметрам, указываемым при добавлении почтового сервера).
4. Нажмите на кнопку «Сохранить изменения».

### 8.15.3 Удаление почтового сервера

Для удаления почтового сервера:

1. В еСА-СА перейдите в раздел «Настройки» на вкладку «Почтовые уведомления».
2. В подразделе «Почтовые серверы» нажмите кнопку «Удалить» для почтового сервера.
3. В диалоговом окне (см. рисунок 225) нажмите кнопку «Удалить».

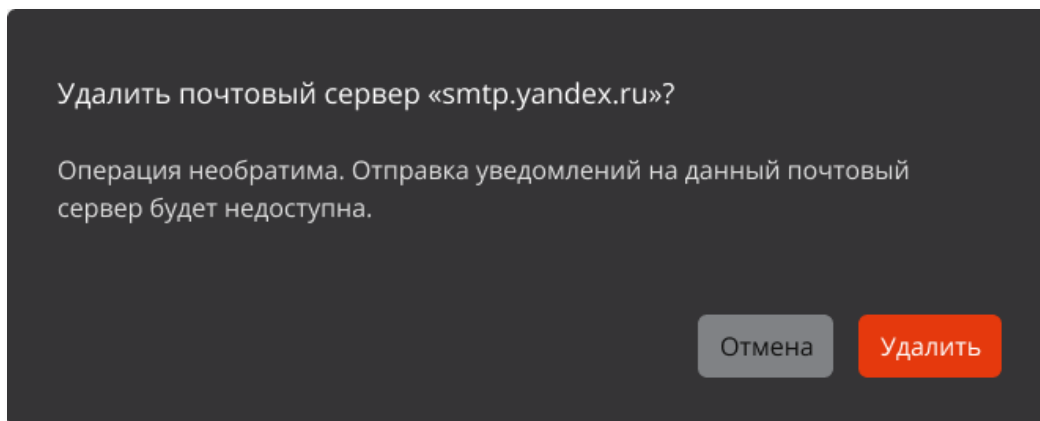


Рисунок 225 — Диалоговое окно удаления почтового сервера

### 8.15.4 Добавление шаблона рассылки

Для добавления шаблона рассылки:

1. В еСА-СА перейдите в раздел «Настройки» на вкладку «Почтовые уведомления».
2. В подразделе «Шаблоны рассылки» нажмите на кнопку «Добавить».
3. В окне «Добавление шаблона рассылки» на шаге 1 мастера добавления шаблона рассылки (см. рисунок 226) укажите следующие параметры шаблона рассылки:
  - 3.1. «Название». В данном поле укажите название шаблона рассылки. Максимальная длина названия – 100 символов.
  - 3.2. «Время до истечения сертификата». В данном поле укажите остаток времени действия сертификата, при достижении которого сертификат будет считаться соответствующим шаблону рассылки. Формат ввода: 1m, 1h, 1d, 1mo, 1y — минута, час, день, месяц, год.
  - 3.3. «Тема письма». В данном поле укажите тему письма, которое будет отправляться в соответствии с данным шаблоном рассылки. Максимальная длина темы письма – 200 символов.

Рисунок 226 — Окно «Добавление шаблона рассылки» на шаге 1 мастера добавления шаблона рассылки

4. В окне «Добавление шаблона рассылки» на шаге 2 мастера добавления шаблона рассылки (см. рисунок 227) выберите тип объектов, о сертификатах которых должны рассылаться уведомления.

Рисунок 227 — Окно «Добавление шаблона рассылки» на шаге 2 мастера добавления шаблона рассылки

5. В окне «Добавление шаблона рассылки» на шаге 3 мастера добавления шаблона рассылки выберите объекты, о сертификатах которых должны рассылаться уведомления:
  - 5.1. Если на шаге 2 мастера добавления шаблона рассылки был выбран вариант «Субъекты», на шаге 3 присутствуют следующие варианты выбора (см. рисунок 228):
    - 5.1.1. «Все субъекты».
    - 5.1.2. «Выбрать субъектов или группы». При выборе данного варианта доступен выбор отдельных субъектов и групп субъектов. При выборе данной опции в столбце «Выбрано» должен присутствовать хотя бы один элемент.

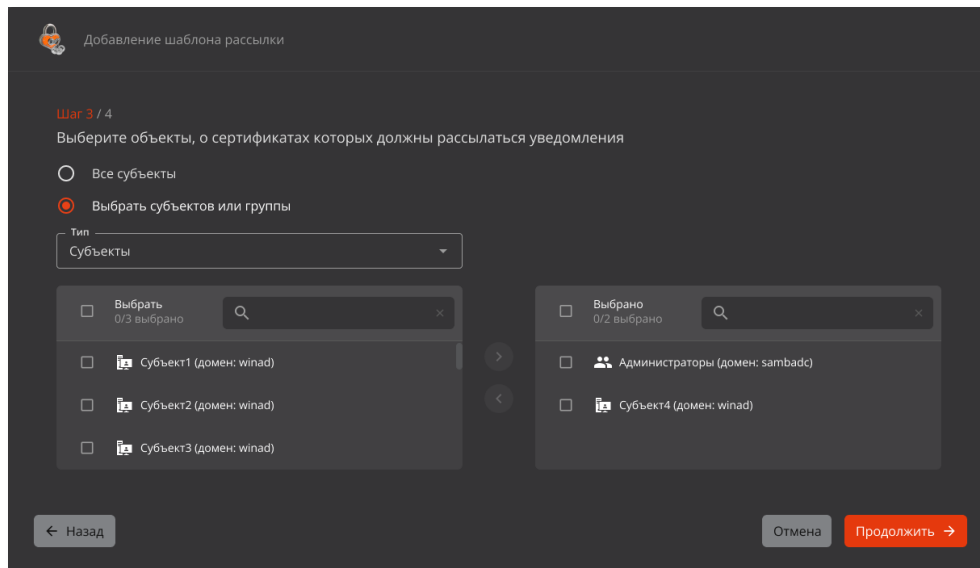


Рисунок 228 — Окно «Добавление шаблона рассылки» на шаге 3 мастера добавления шаблона рассылки.  
Вариант «Субъекты»

- 5.2. Если на шаге 2 мастера добавления шаблона рассылки выбран вариант «Учётные записи», то на шаге 3 присутствуют следующие варианты выбора (см. рисунок 229):
- 5.2.1. «Все учётные записи».
- 5.2.2. «Выбрать учётные записи». При выборе данного варианта доступен выбор отдельных учётных записей. В столбце «Выбрано» должен присутствовать хотя бы один элемент.

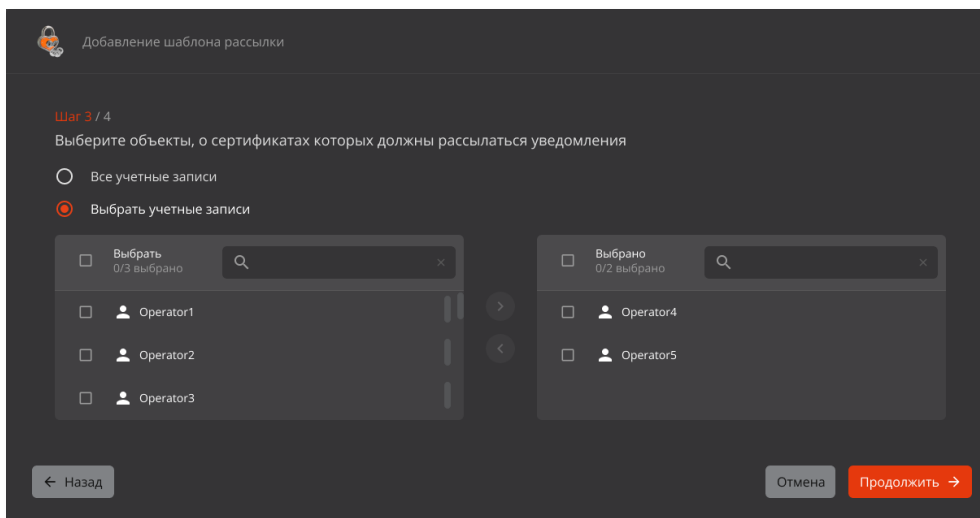


Рисунок 229 — Окно «Добавление шаблона рассылки» на шаге 3 мастера добавления шаблона рассылки.  
Вариант «Учётные записи»

6. В окне «Добавление шаблона рассылки» на шаге 4 мастера добавления шаблона рассылки выберите получателей уведомлений:
- 6.1. Если на шаге 2 мастера добавления шаблона рассылки выбран вариант «Субъекты», то на шаге 4 (см. рисунок 230):
- 6.1.1. Для выбора получателей по атрибуту включите чекбокс «Владелец сертификата. Определять его почту по» и выберите необходимый атрибут из выпадающего списка.
- 6.1.2. Для выбора получателей по адресам электронной почты включите чекбокс «Список адресов электронной почты» и укажите адреса электронной почты получателей. Доступно указание не более 10 адресов электронной почты. Должен быть задан как минимум один адрес электронной почты.

Рисунок 230 — Окно «Добавление шаблона рассылки» на шаге 4 мастера добавления шаблона рассылки.  
Вариант «Субъекты»

- 6.2. Если на шаге 2 2 мастера добавления шаблона рассылки был выбран вариант «Учётные записи», то на шаге 4 (см. рисунок 231) введите адреса электронной почты получателей. Доступно указание не более 10 адресов электронной почты. Должен быть задан как минимум один адрес электронной почты.

Рисунок 231 — Окно «Добавление шаблона рассылки» на шаге 4 мастера добавления шаблона рассылки.  
Вариант «Учётные записи»

7. Нажмите кнопку «Добавить».

### 8.15.5 Редактирование шаблона рассылки

Для редактирования шаблона рассылки:

1. В еСА-СА перейдите в раздел «Настройки» на вкладку «Почтовые уведомления».
2. В подразделе «Шаблоны рассылки» нажмите на кнопку «Редактировать» для любого шаблона рассылки в списке.
3. В окне «Редактирование шаблона рассылки» отредактируйте параметры шаблона рассылки (параметры аналогичны параметрам, указываемым при добавлении шаблона рассылки, за исключением невозможности изменения значения на шаге 2 мастера добавления шаблона рассылки).
4. Нажмите кнопку «Сохранить изменения».

### 8.15.6 Удаление шаблона рассылки

Для удаления шаблона рассылки:

1. В еСА-СА перейдите в раздел «Настройки» на вкладку «Почтовые уведомления».
2. В подразделе «Шаблоны рассылки» нажмите на кнопку «Удалить» для любого шаблона рассылки в списке.
3. В диалоговом окне (см. рисунок 232) нажмите кнопку «Удалить».

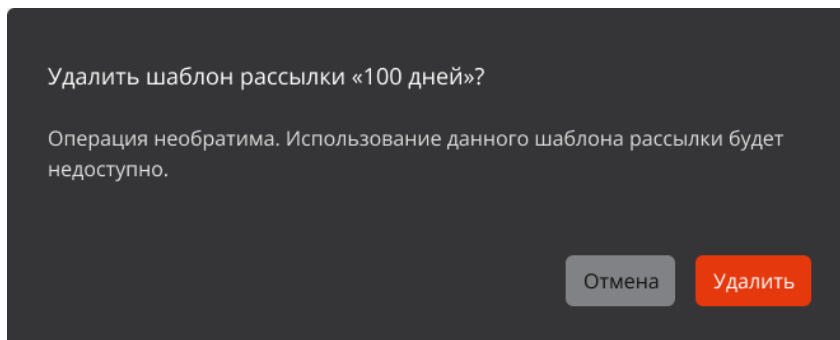


Рисунок 232 — Диалоговое окно удаления шаблона рассылки

### 8.15.7 Отправка тестового уведомления

Для отправки тестового уведомления:

1. В еСА-СА перейдите в раздел «Настройки» на вкладку «Почтовые уведомления».
2. В подразделе «Почтовые серверы» нажмите кнопку «Отправить тестовое уведомление» (пиктограмма «Письмо») для почтового сервера (см. рисунок 233).

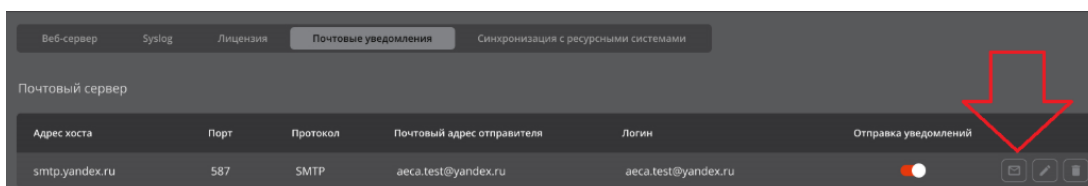


Рисунок 233 — Расположение пиктограммы «Письмо»

3. В окне «Отправка тестового почтового уведомления» (см. рисунок 234) укажите Email получателя (обязательный параметр), тему и текст письма (необязательные параметры).

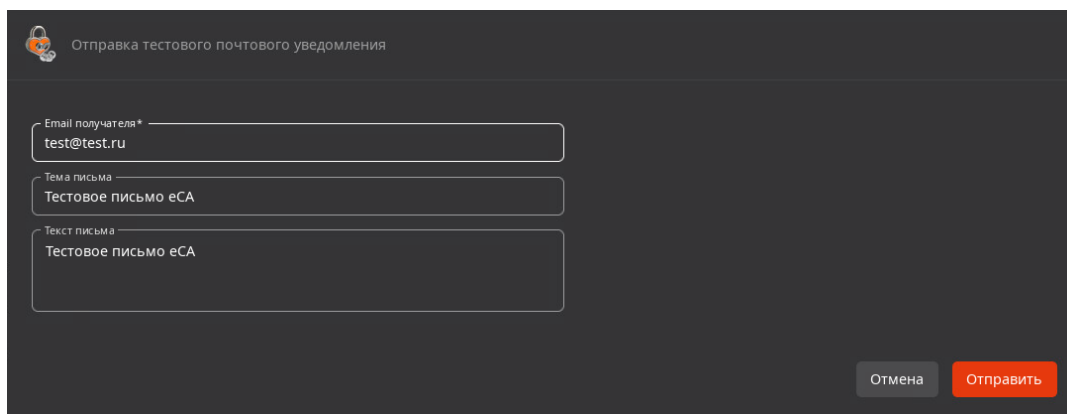


Рисунок 234 — Окно «Отправка тестового почтового уведомления»

4. Нажмите кнопку «Отправить».

## 8.16 Управление рассылкой Syslog-сообщений

### 8.16.1 Добавление Syslog-сервера

**Внимание!** Данная возможность доступна только пользователю с ролью «Администратор».

**Внимание!** Количество Syslog-серверов в списке не может превышать 10.

Для добавления Syslog-сервера:

1. Перейдите в раздел «Настройки» на вкладку «Syslog» (см. рисунок 235).
2. В подразделе «Syslog серверы» нажмите кнопку «Добавить».

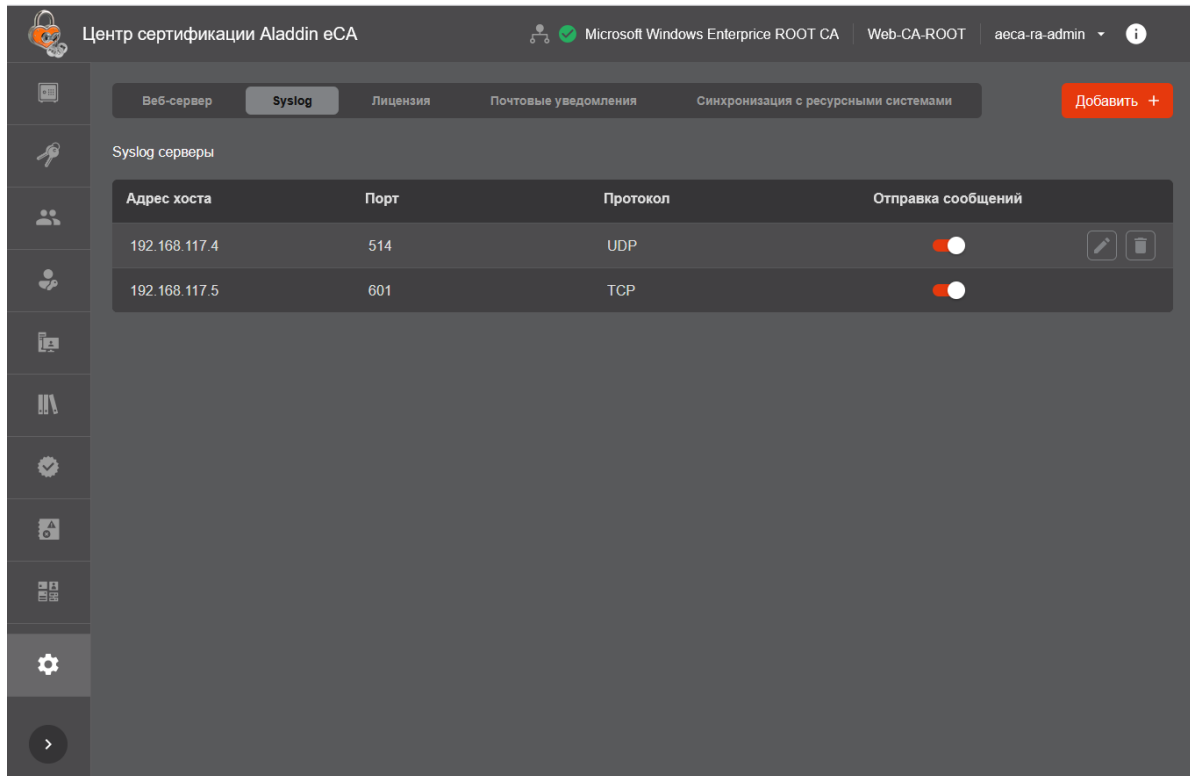


Рисунок 235 — Вкладка «Syslog»

3. В окне «Добавление Syslog-сервера» (см. рисунок 236) укажите следующие параметры добавляемого Syslog-сервера:
  - 3.1. «Адрес хоста». В данном поле укажите адрес хоста Syslog-сервера. Формат ввода – IPv4 или FQDN <sup>1</sup>.
  - 3.2. «Порт». В данном поле укажите порт Syslog-сервера. Формат ввода – число от 1 до 65535.
  - 3.3. «Протокол». Допустимые варианты выбора: UDP (указан по умолчанию), TCP, TCP (TLS).
4. Нажмите кнопку «Добавить».

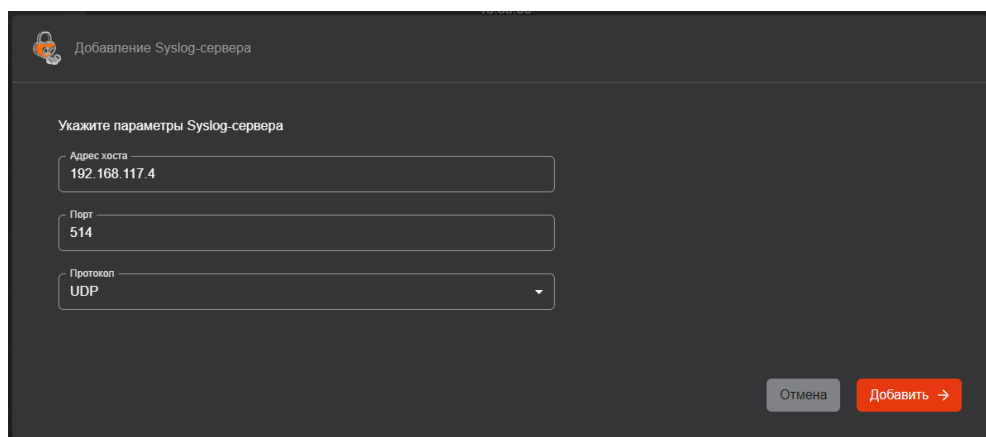


Рисунок 236 – Окно «Добавление Syslog-сервера»

Если в качестве протокола используется TCP (как с TLS, так и без него), то при добавлении Syslog-сервера будет осуществляться попытка подключения к нему. При невозможности подключения новый Syslog-сервер не будет добавлен.

### 8.16.2 Редактирование параметров Syslog-сервера

**Внимание!** Данная возможность доступна только пользователю с ролью «Администратор».

Для редактирования параметров Syslog-сервера:

1. Перейдите в раздел «Настройки» на вкладку «Syslog».

<sup>1</sup> Регулярное выражение для параметра «Адрес хоста»: `^(25[0-5]|2[0-4][0-9]|1[0-9][0-9]|1[0-9][0-9][0-9])\.{3}(25[0-5]|2[0-4][0-9]|1[0-9][0-9]|1[0-9][0-9][0-9])$` `^(\?=, {1,253}$) ([a-zA-Z0-9- ]{0,61}[a-zA-Z0-9- ]?)?\.[a-zA-Z]{2,}$`

2. В строке необходимого Syslog-сервера нажмите кнопку «Редактировать».
3. В окне «Редактирование Syslog-сервера» (см. рисунок 237) отредактируйте необходимые параметры.
4. Нажмите на кнопку «Сохранить изменения».

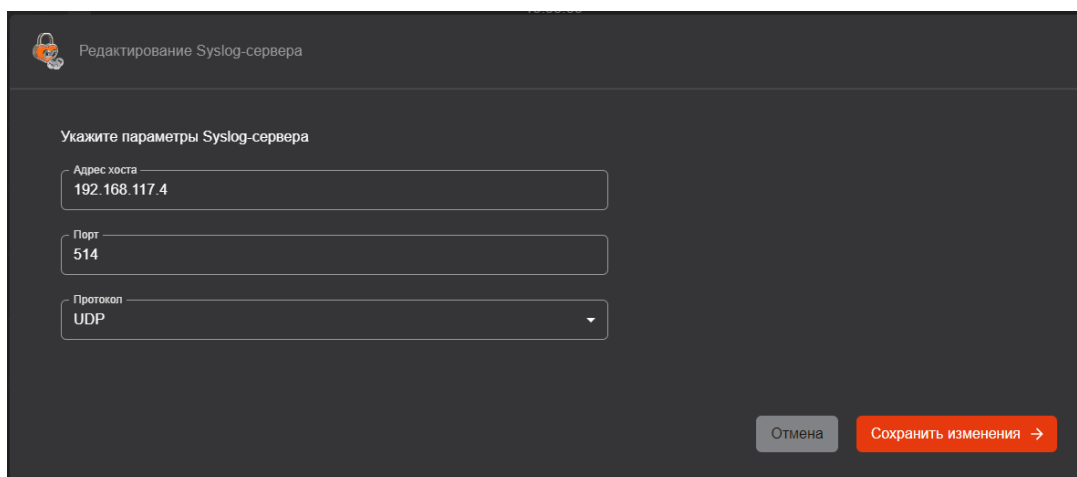


Рисунок 237 – Окно «Редактирование Syslog-сервера»

Если в качестве протокола используется TCP (как с TLS, так и без него), то при изменении параметров Syslog-сервера будет осуществляться попытка подключения к нему. При невозможности подключения параметры Syslog-сервера не будут изменены.

### 8.16.3 Удаление Syslog-сервера

**Внимание!** Данная возможность доступна только пользователю с ролью «Администратор».

Для удаления Syslog-сервера:

1. Перейдите в раздел «Настройки» на вкладку «Syslog».
2. В строке необходимого Syslog-сервера нажмите кнопку «Удалить».
3. В окне подтверждения удаления (см. рисунок 238) нажмите кнопку «Удалить».

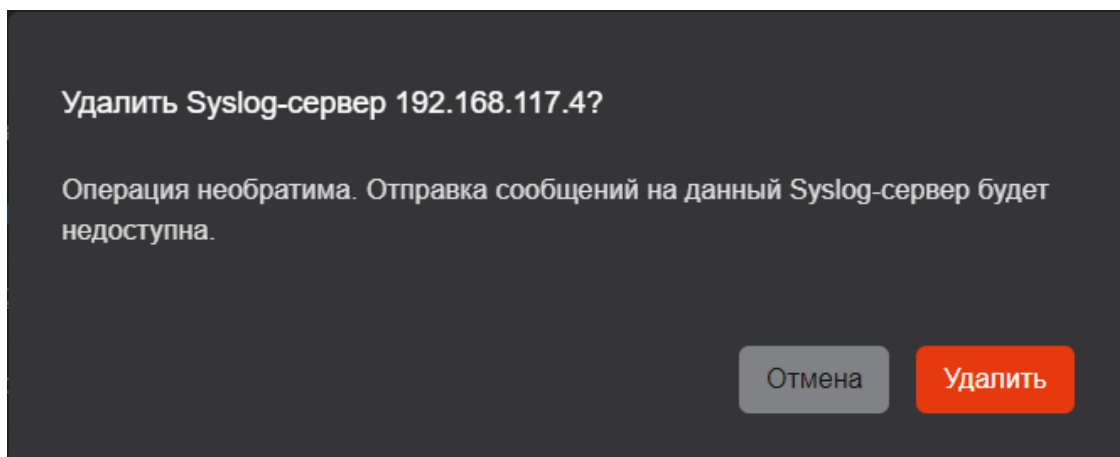


Рисунок 238 – Окно подтверждения удаления Syslog-сервера

## 8.17 Просмотр сведений о лицензии и её импорт

Сведений о лицензии и её импорт доступны на вкладке «Лицензия» в разделе «Настройки». Импорта лицензии выполняется при помощи кнопки «Импортировать лицензию».

## 9 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
П002	Прекращение установки или обновление ПО	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 Руководства администратора. Также проверьте и при необходимости переключите текущую версию java-компонентов, выполнив команды с правами суперпользователя: update-alternatives —config java update-alternatives —config javac update-alternatives —config javap
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> : <code>ldap server require strong auth = no</code>
		2. Проверить подключение к контроллеру домена Samba	Проверьте подключение к контроллеру домена, используя инструмент <code>ldapsearch</code> : – получение списка пользователей <code>ldapsearch -D «Administrator@pki-test.local» -w «Qwerty1234» -b «DC=pki-test,DC=local» -H «ldap://192.168.111.148» «(objectCategory=user)»</code> – получение списка компьютеров <code>ldapsearch -D «Administrator@pki-test.local» -w «Qwerty1234» -b «DC=pki-test,DC=local» -H «ldap://192.168.111.148» «(objectCategory=computer)»</code> – получение списка групп безопасности <code>ldapsearch -D «Administrator@pki-test.local» -w «Qwerty1234» -b «DC=pki-test,DC= pki-test» -H «ldap://192.168.111.148» «(objectCategory=group)»</code> 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.

Ид.	Проблема	Возможная причина	Способы решения
		3. Проверить подключение к контроллеру домена ALD PRO	<p>Проверьте подключение к контроллеру домена, используя инструмент ldapsearch:</p> <ul style="list-style-type: none"> <li>– получение списка пользователей  <code>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=x-ald-user)"</code></li> <li>– получение списка компьютеров  <code>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)"</code></li> <li>– получение списка групп безопасности  <code>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)"</code></li> </ul> <p>где:  <code>users, accounts</code>  <code>Qwerty1234</code> – пароль администратора домена;  <code>domain, local</code> – доменное имя;  <code>192.168.111.148</code> – 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 ЦС с выпущенным сертификатом невозможен в веб-браузере Chromium	Веб-браузер Chromium не поддерживает сертификаты с алгоритмом шифрования ECDSA512	Использовать другой веб-браузер
П005	Вход в интерфейс ЦС невозможен в веб-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 веб-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 ЦС невозможен. Ошибка 500	Удалён сертификат технологического ЦС	<p>Проверить файл <code>opt/aeca/p12/truststore.jks</code> на предмет содержания записи о сертификате технологического ЦС, созданного при установке ПО Aladdin eCA.</p> <p>Запись о сертификате технологического ЦС следующего вида:  <code>keytool -import -alias managementca -file cert.pem -keystore ./truststore.jks</code>  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> <code>openssl pkcs12 -in superadmin.p12 -out cert.pem -nodes -clcerts</code> Пароль контейнера сертификата технологического ЦС указан в файле <code>/opt/aeca/generated_passwords.txt</code>

Ид.	Проблема	Возможная причина	Способы решения
П007	Невозможно подключиться к токену для выпуска сертификата после установки JC–WebClient. Сообщение «ПО JCWebClient не установлено»	Требуется разрешить ПО JC–WebClient доступ к ресурсу	В адресную строку веб-браузера введите: https://localhost:24738/admin/token_manager.html 2. Во всплывающем окне предупреждения веб-браузера подтвердите действия.
П008	Пустой файл шаблонов по завершению работы скрипта msocs2aeca.ps1экспорта шаблонов MSCS	Требуется настройка tls	Откройте Powershell от имени администратора и задайте версию протокола безопасности, выполнив команду: [Net.ServicePointManager]::SecurityProtocol = [Net.SecurityProtocolType]::Tls12
П009	Невозможно применить выпущенный ЦС сертификат в ОС Windows (в частности, WinServer2012/2016)	Сертификат доступа сгенерирован с использованием алгоритма хеширования sha256, и операционная система Windows не поддерживает данный алгоритм	Конвертируйте сертификат, сгенерированный с использованием алгоритма хеширования sha256, в формате .p12 в формат .pem с помощью openssl: openssl pkcs12 -in <имя контейнера>.p12 -out <имя декодированного файла>.pem openssl pkcs12 -keypbe PBE-SHA1-3DES -certpbe PBE-SHA1-3DES -export -in <имя декодированного файла>.pem -out <имя контейнера>.p12
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 веб-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	На клиенте выполнить команды с правами суперпользователя: kinit <администратор домена> ipa-certupdate И повторить попытку авторизации.
П013	Периодическая остановка или падение службы aecaservice	Недостаток оперативной памяти на хосте	Проверьте потребление оперативной памяти на хосте с помощью команды <code>top</code> : – в <code>MiB Mem</code> значение <code>total</code> – это общий объем оперативной памяти; – в <code>MiB Mem</code> значение <code>free</code> – это свободная оперативная память; – в строке таблицы <code>USER=aeca</code> значение в колонке <code>RES</code> – это потребляемая ЦС оперативная память. Для корректной работы ЦС сумма <code>free</code> и <code>RES</code> должна быть не менее 10 Гб <sup>1</sup> . 2. Если полученное значение меньше 10 Гб, то при исчерпании свободной оперативной памяти <code>oom-killer</code> останавливает ЦС. В данном случае рекомендуется проанализировать состав стороннего ПО на хосте и его потребление памяти, например, с помощью команд <code>top</code> или <code>htop</code> . 3. После этого следует либо добавить необходимое количество оперативной памяти, либо удалить с хоста стороннее ПО, освободив этим оперативную память.

<sup>1</sup> Браузер Требования к аппаратному обеспечению см. «Руководство 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. 8.7.3 настоящего руководства) или подключенных ресурсных систем (см. 8.7.4 настоящего руководства)!

Создание сертификата субъекта по запросу, возможно как для существующего предварительно созданного локального субъекта (см. 8.7.3.1 настоящего руководства) или субъекта внешней ресурсной системы (см. 8.7.4 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 239):

- с закрытым ключом для существующего субъекта;
- на основании запроса;
- на ключевом носителе.

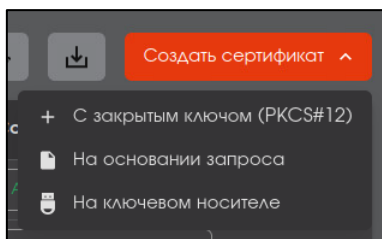


Рисунок 239 – Кнопка «Создать сертификат» на вкладке «Сертификаты»

На вкладке «Учётные записи» при выделении строки учётной записи и нажатии кнопки <Создать сертификат> доступен выпуск сертификата для учётной записи (см. Рисунок 240):

- с закрытым ключом (PKCS#12);
- 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 240 – Кнопка «Создать сертификат» на вкладке «Учётные записи»

На вкладке «Субъекты» при выделении строки субъекта и нажатии кнопки **<Создать сертификат>** доступен выпуск сертификата (см. Рисунок 241):

- с закрытым ключом;
- на основании запроса;
- на ключевом носителе.

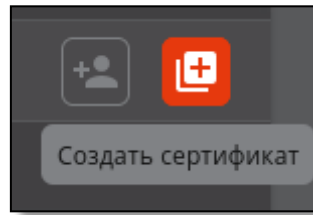


Рисунок 241 – Кнопка «Создать сертификат» на вкладке «Субъекты»

В результате нажатия на кнопку создания сертификата появится окно создания сертификата.

Предусмотрена возможность выпуска сертификатов при помощи API (см. документ «Центр сертификатов доступа Aladdin Enterprise Certificate Authority Certified Edition. Руководство администратора. Часть 3. Описание методов REST API»).

## 1.2 Параметры криптографии сертификатов учётных записей пользователей и Центров сертификации

В таблице ниже 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 Центра сертификации Aladdin eCA.

Таблица 20 – Успешные комбинации сертификатов Центра сертификации и учётной записи пользователя при аутентификации

Операционная система	Алгоритм и длина ключа сертификата ЦС	Алгоритм и длина ключа сертификата учётной записи пользователя
Astra Linux Special Edition	RSA: 2048–4096, SHA256–SHA512	RSA: 2048–8196. ECDSA: 256–521 ГОСТ Р 34.10–2012: 256–512
	ECDSA: 256–521, SHA256–SHA512	
	ГОСТ Р 34.10–2012: 256–512, ГОСТ Р 34.11–2012	
РЕД ОС, РОСА «ХРОМ» 12 Сервер и SberLinux OS Server	RSA: 2048–4096, SHA1–SHA512	RSA: 1024–8196. ECDSA: 256–521 ГОСТ Р 34.10–2012: 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: 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, подключённого к ресурсной системе;
- сертификат создан по шаблону, в котором включена публикация сертификата в ресурсную систему.

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

eCA-CA выполняет автоматическую публикацию сертификатов, требующих публикации при включённом 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, Dynamic Directory и FreeIPA) выбранного субъекта ресурсной системы, для которого выпущен сертификат, путём добавления, а не перезаписи атрибута.

### 1.4 Создание сертификата с закрытым ключом PKCS#12

**Внимание!** Создание сертификата возможно только для существующего субъекта! Предварительно создайте локальный субъект (см. 8.7.3.1) или выберите субъект внешней ресурсной системы (см. 8.7.4).

Для создания сертификата с закрытым ключом PKCS#12:

1. В разделе «Сертификаты» или в карточке субъекта, или в списке субъектов нажмите кнопку «Создать сертификат» и выберите из выпадающего списка функцию «С закрытым ключом (PKCS#12)». Если кнопки «Создать сертификат» и «С закрытым ключом (PKCS#12)» Вы нажали в карточке субъекта или в списке субъектов, то перейдите на п. 2 данного сценария (нумерация шагов при выполнении сценария, а также их общее количество в этом случае меньше на 1).
2. В окне шага 1 мастера создания сертификата (см. рисунок 242) выберите субъект и нажмите кнопку продолжить.

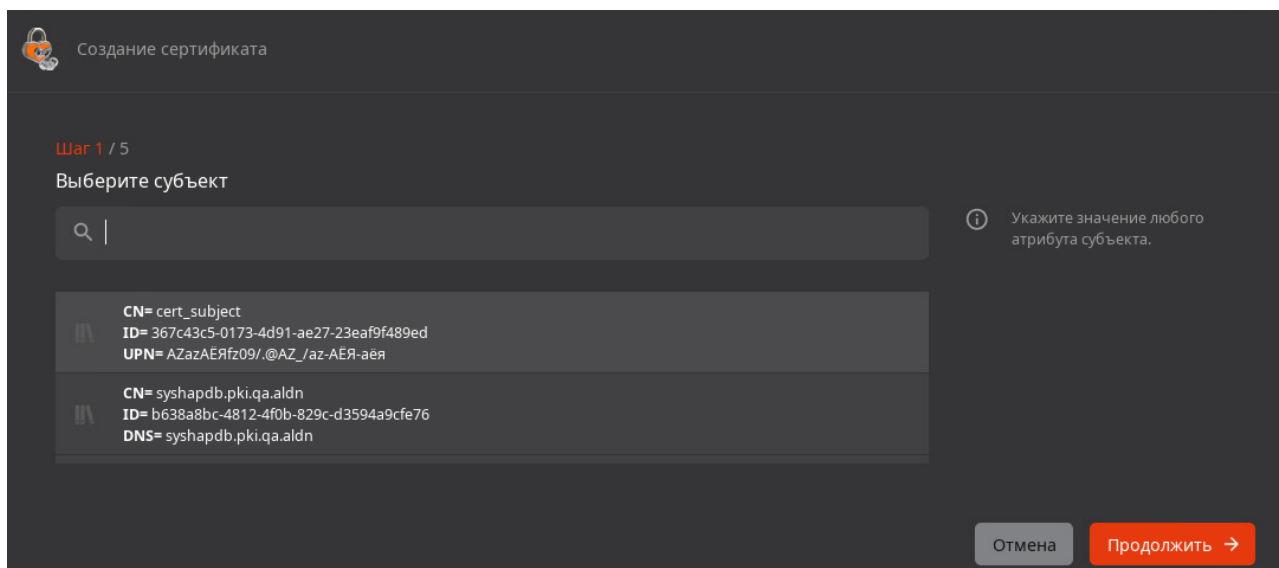


Рисунок 242 —Шаг 1 мастера создания сертификата

3. В окне шага 2 мастера создания сертификатов (см. рисунок 243) выберите шаблон сертификата<sup>1</sup> и нажмите кнопку «Продолжить».

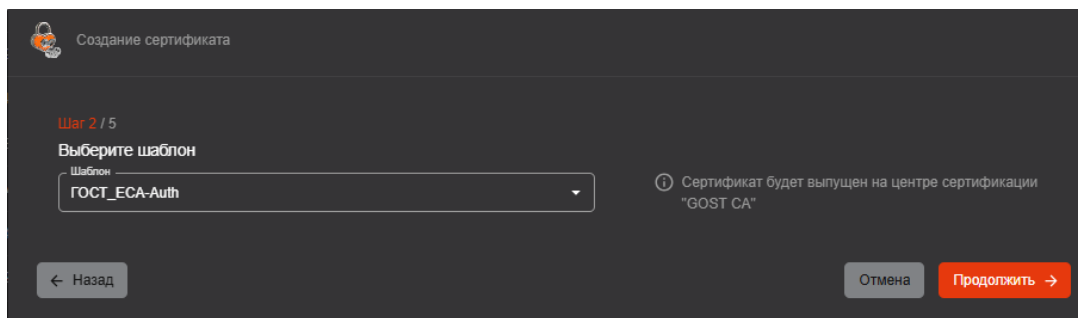



Рисунок 243 — Шаг 2 мастера создания сертификата

4. В окне шага 3 мастера создания сертификата (см. рисунок 244) значения атрибутов заполняются автоматически в соответствии с данными в карточке субъекта (см. 8.7.2) и изменению не подлежат. Если у субъекта несколько значений в атрибуте, то при необходимости выберите нужное из выпадающего списка или добавьте дополнительное значение при помощи кнопки . Затем нажмите кнопку «Продолжить».

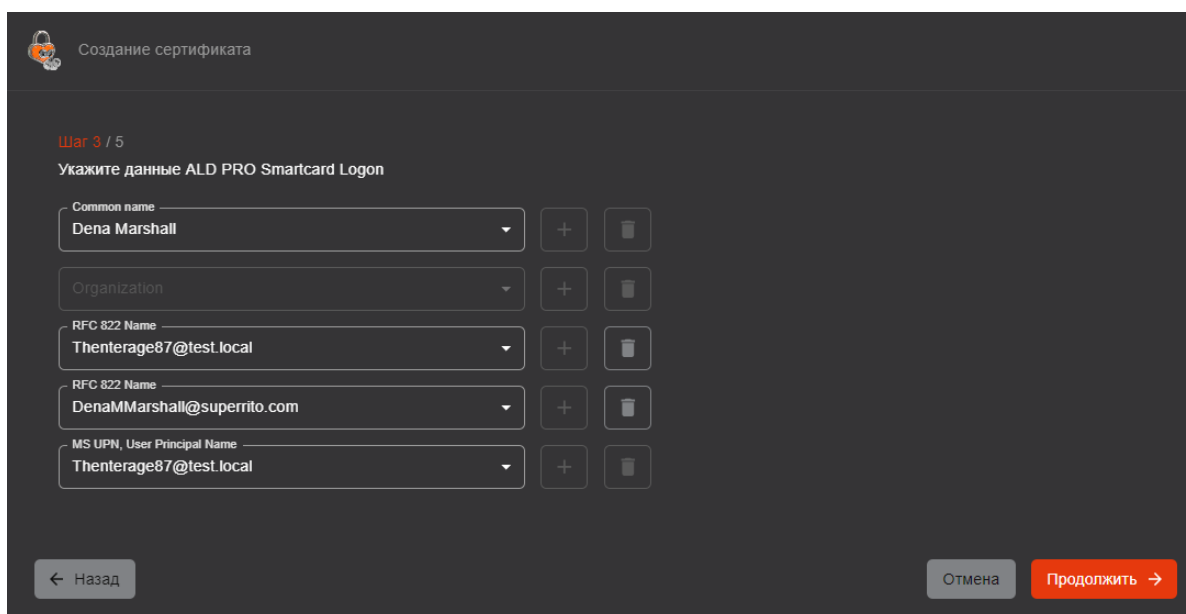


Рисунок 244 — Окно «Создание сертификата». Шаг 3 мастера создания сертификата

5. В окне шага 4 мастера создания сертификата (см. рисунок 245):
  - 5.1. Укажите пароль для контейнера PKCS#12 в полях «Пароль» и «Подтверждение пароля».
  - 5.2. Нажмите кнопку «Продолжить».

<sup>1</sup> В данном списке будут отсутствовать шаблоны, у которых выключена опция «Выпуск сертификатов с закрытым ключом (PKCS#12)».

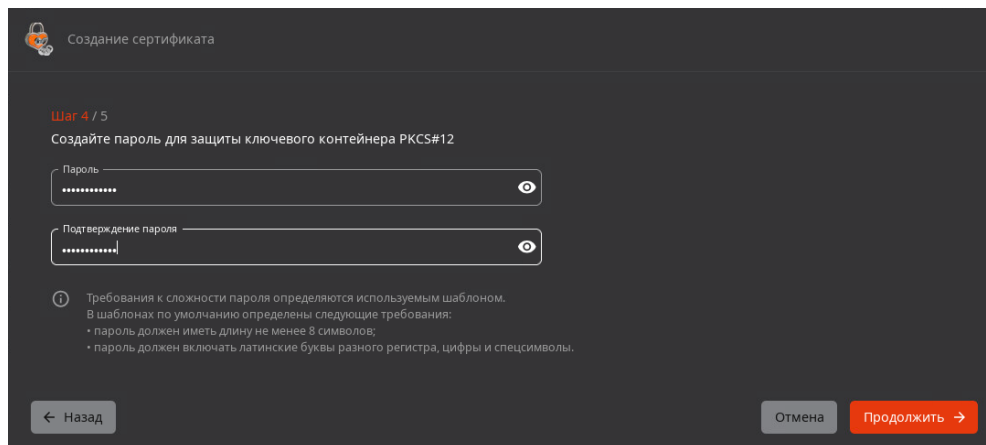


Рисунок 245 — Шаг 4 мастера создания сертификата

6. На шаге 5 мастера создания сертификата (см. рисунок 246):
  - 6.1. Выберите алгоритм генерации ключевой пары и длину ключа.
  - 6.2. Нажмите кнопку «Создать сертификат».

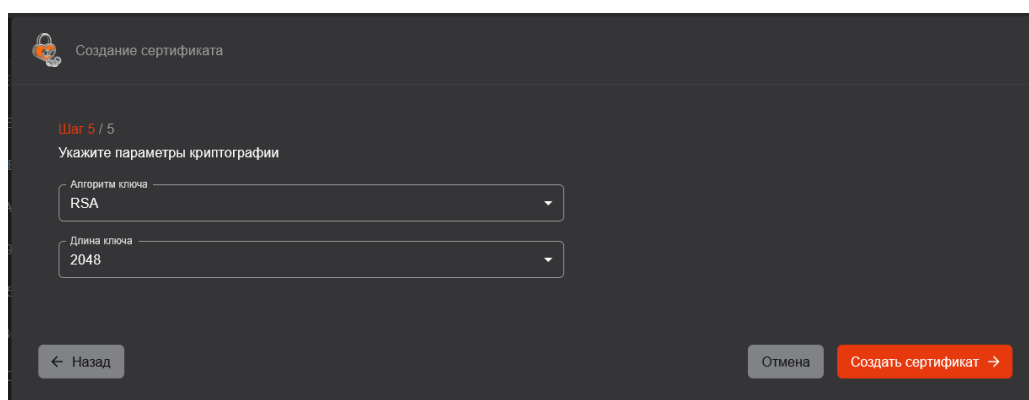


Рисунок 246 — Шаг 5 мастера создания сертификата

Если сертификат создан для субъекта, подключённого к ресурсной системе, или создан по шаблону, в котором включена публикация сертификата в ресурсную систему, то сертификат публикуется в ресурсную систему и выводится сообщение «Сертификат успешно опубликован в ресурсную систему».

7. В финальном окне мастера создания сертификата (см. рисунок 247):
  - 7.1. Ознакомьтесь со сведениями о созданном сертификате.
  - 7.2. Скачайте сертификат в контейнере PKCS#12.<sup>1</sup>
  - 7.3. Нажмите кнопку «Заккрыть».

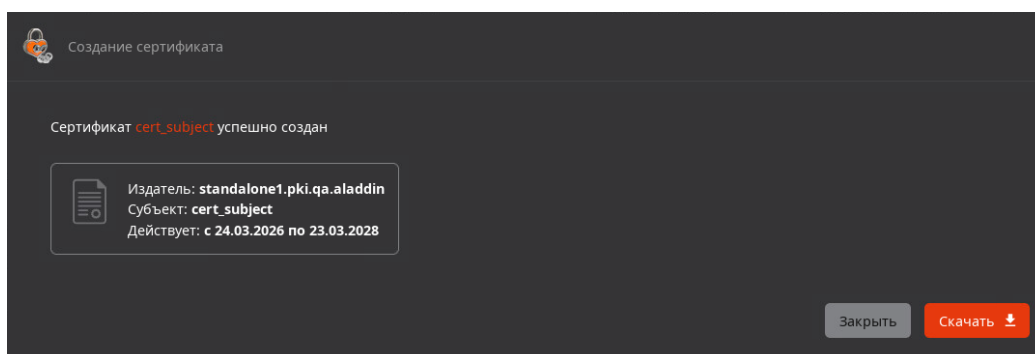


Рисунок 247 — финальное окно мастера создания сертификата

<sup>1</sup> После закрытия настоящего окна сертификат возможно скачать только в формате «.pem».

## 1.5 Создание сертификата субъекта по запросу

**Внимание!** Создание сертификата возможно как для существующего предварительно созданного локального субъекта (см. раздел 8.7.3.1 настоящего руководства) или субъекта внешней ресурсной системы (см. раздел 8.7.4 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 еСА-СА. 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»

Порядок создания 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 248) загрузите файл–запрос (загружается по кнопке **<Выбрать файл>**) и нажмите кнопку **<Продолжить>**.

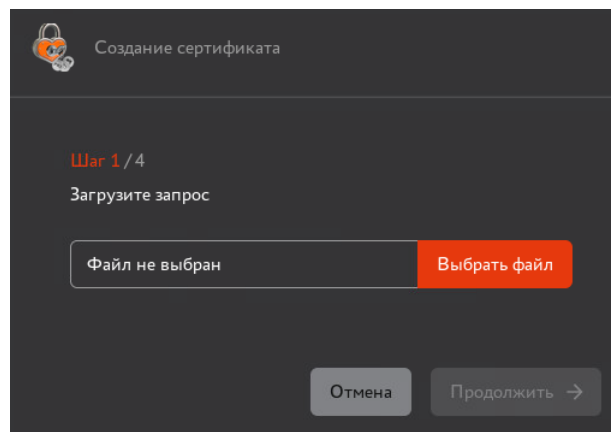


Рисунок 248 – Окно создания сертификата по запросу в разделе «Сертификаты». Шаг 1. Загрузка запроса

- 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 249):
    - «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.

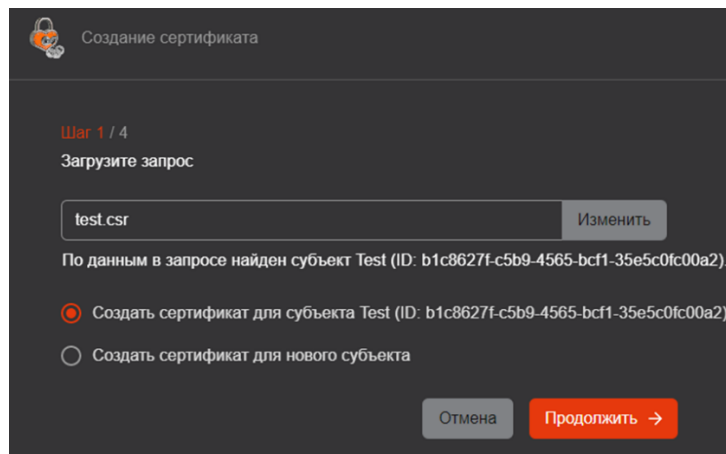


Рисунок 249 – Окно создания сертификата по запросу в разделе «Сертификаты». Шаг 1. Загрузка запроса.

- 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 250):
  - «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>1</sup>;
  - «Создать сертификат для нового субъекта». Выберите данную опцию, чтобы создать сертификат для нового субъекта, который будет создан на основании данных запроса.

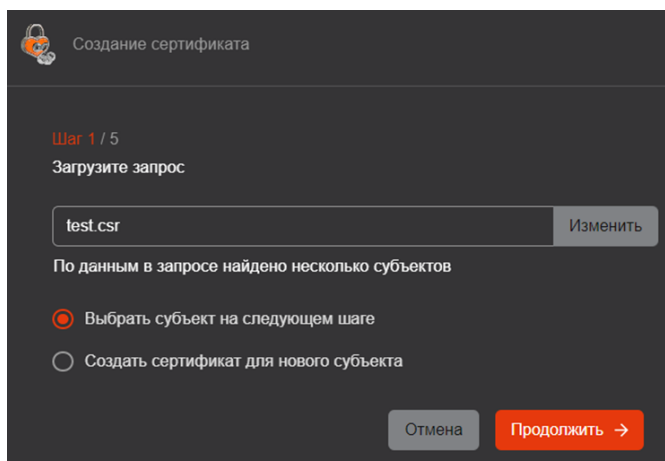


Рисунок 250 – Окно создания сертификата по запросу в разделе «Сертификаты». Шаг 1. Загрузка запроса. Найдено несколько субъектов

- 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 251). Далее по сценарию сертификат будет создаваться для нового субъекта, который будет создан на основании данных запроса;

<sup>1</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.

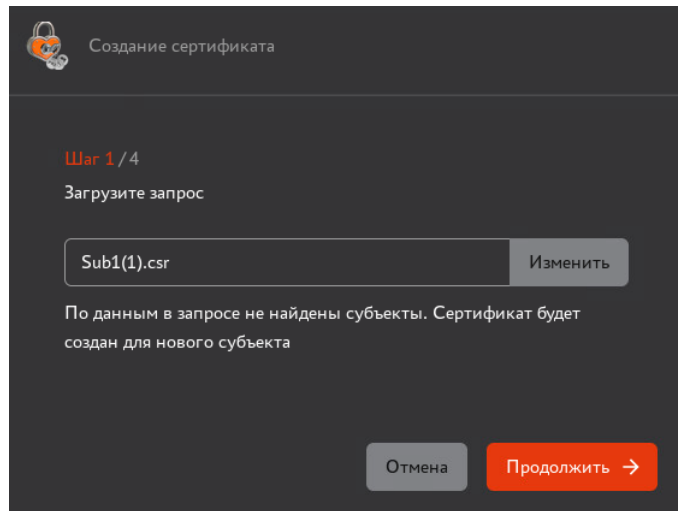



Рисунок 251 – Окно создания сертификата по запросу в разделе «Сертификаты». Шаг 1. Загрузка запроса.  
Не найден ни один субъект

- 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>1</sup>. Нажмите кнопку **<Продолжить>** для перехода к следующему шагу.
- (Шаг 2/5) В появившемся окне (см. Рисунок 252):
  - 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;
  - 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 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 следующему шагу;

<sup>1</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.

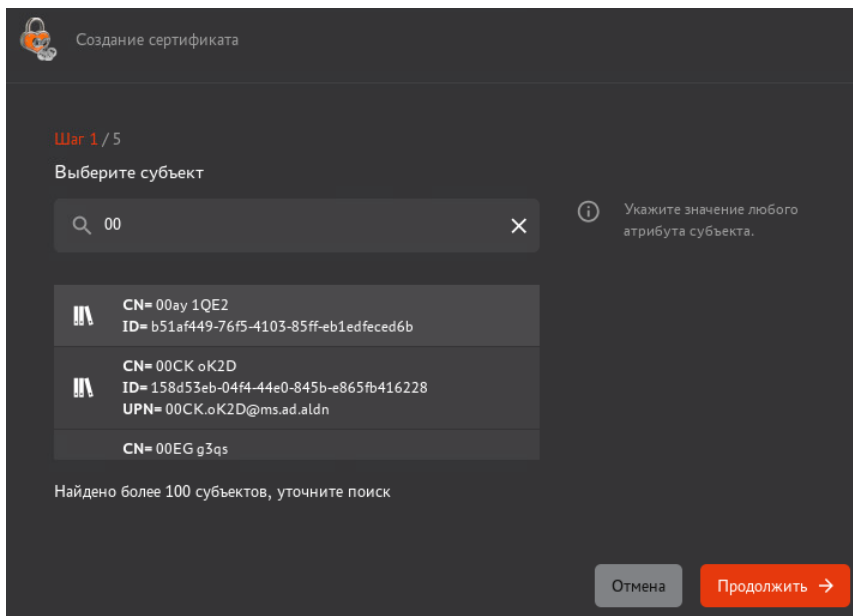


Рисунок 252 – Окно создания сертификата по запросу в разделе «Сертификаты». Шаг 2. Выбор субъекта

- (Шаг 2/4 или 3/5) В появившемся окне (см. Рисунок 253) 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. 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.

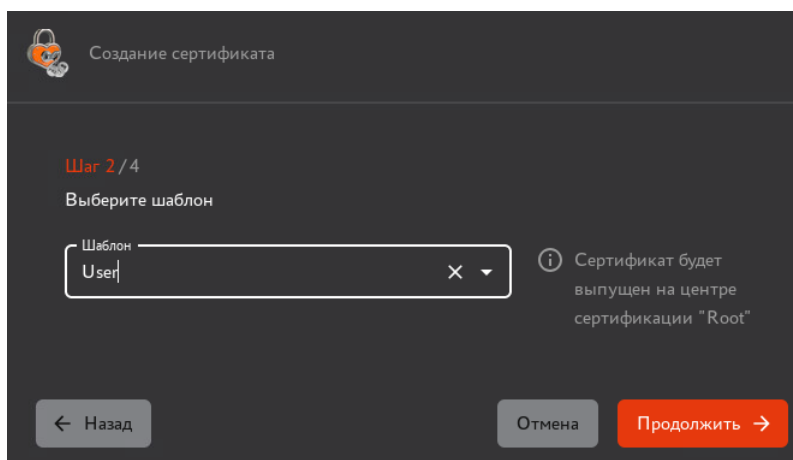


Рисунок 253 – Окно создания сертификата по запросу в разделе «Сертификаты». Шаг 3. Выбор шаблона

- 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 таблице 21. Проверка является регистронезависимой.

При этом в случае, если в процессе выпуска сертификата по запросу создаётся новый субъект, то валидация значений из полей запроса на соответствие атрибутам субъекта не выполняется (возможность возникновения ошибки №4 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 254 и Рисунок 255).

Перечень возможных ошибок представлен в таблице 22.

Таблица 21 – Соответствие полей запроса шаблону выпускаемого сертификата

Поле в шаблоне	Значение поля в запросе	Атрибут субъекта	Возможность создания сертификата	Поле в сертификате	Возможные ошибки*
<b>Правила проверки соответствия SDN полей</b>					
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
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	–
<b>Правила проверки соответствия SAN полей</b>					
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 (путём

Поле в шаблоне	Значение поля в запросе	Атрибут субъекта	Возможность создания сертификата	Поле в сертификате	Возможные ошибки*
					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	–
Нет	Есть	Нет	Да	Отсутствует	Ошибка №3
Нет	Нет	Нет	Да	Отсутствует	–
Нет	Есть	Есть	Да	Отсутствует	Ошибка №3
Нет	Нет	Есть	Да	Отсутствует	–

Таблица 22 – Перечень возможных ошибок обработки запроса


Ошибка	Сообщение
Ошибка №1	«Отсутствует обязательное поле» <sup>1</sup>
Ошибка №2	«Значение в поле не соответствует регулярному выражению: \»%s\»», где \»%s\» <sup>2</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 учётом выявленных при сверке ошибок и перезагрузить файл–запрос, вернувшись на предыдущие шаги по нажатию кнопки **<Назад>**.

<sup>1</sup> Описание полей предустановленных шаблонов см. в приложении 2 «Описание полей предустановленных шаблонов сертификатов».

<sup>2</sup> Правила валидации значений полей предустановленных шаблонов см. в приложении 3 «Правила валидации значений полей по умолчанию предустановленных шаблонов сертификатов».

 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	<b>⚠ Значение в поле не соответствует значению атрибута субъекта</b>
Альтернативное имя субъекта			
RFC822NAME		email@address.com	<b>⚠ Значение в поле не соответствует значению атрибута субъекта</b>
DNS_NAME		www.domain.com	<b>⚠ Поле отсутствует в шаблоне</b>
MS_UPN		email@address.com	<b>⚠ Значение в поле не соответствует значению атрибута субъекта</b>
MS_GUID		e4134486122d452495c771503eabf73f	<b>⚠ Поле отсутствует в шаблоне</b>

← Назад Отмена Продолжить →

Рисунок 254 – Окно создания сертификата по запросу в разделе «Сертификаты». Шаг 4. Результат обработки запроса с ошибкой в поле различающегося имени субъекта

 Создание сертификата

Шаг 3 / 4

Загружен запрос на сертификат для <common name>.

Поля	В шаблоне	Значение из запроса	Значение в сертификате
Различающееся имя субъекта			
Общее имя	✓	123	123
Домен	✓	—	—
Отдел	✓	—	—
Организация	✓	—	—
Адрес	✓	—	—
Район	✓	—	—
Область, край	✓	—	—
Страна	✓	KG	KG
Альтернативное имя субъекта			
RFC 822 NAME	✓	—	<b>⚠ Отсутствует обязательное поле</b>
DNS NAME	✓	—	—
MS GUID	✓	3252345	<b>⚠ Значение в поле не соответствует регулярному выражению: \"%s\"</b>
IP Address	✓	192.168.11.15	<b>⚠ Значение в поле не соответствует значению атрибута субъекта</b>

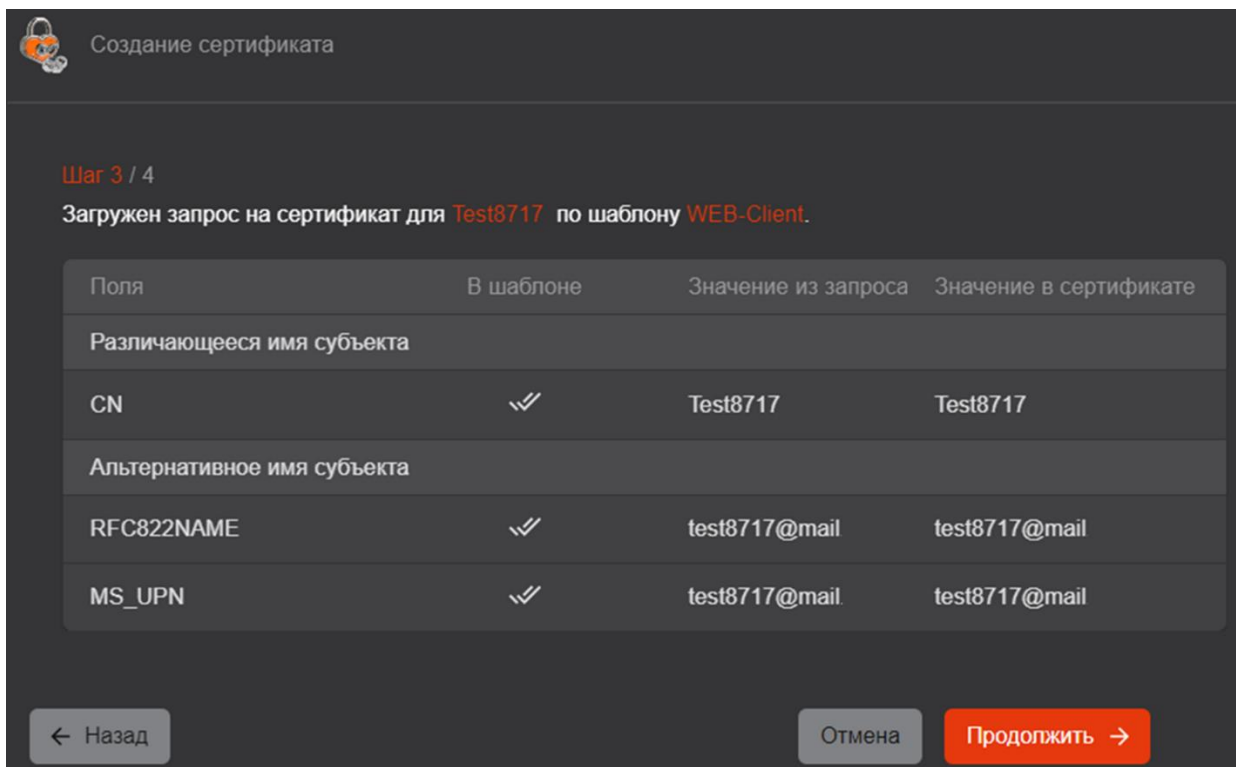
← Назад Отмена Продолжить →

Рисунок 255 – Окно создания сертификата по запросу в разделе «Сертификаты». Шаг 4. Результат обработки запроса с ошибками в полях альтернативного имени субъекта

В результате успешной обработки запроса на сертификат субъекта на следующем шаге отображается (см. Рисунок 256):

- 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>1</sup>, то они идентифицируются по параметру OID.



Создание сертификата

Шаг 3 / 4

Загружен запрос на сертификат для **Test8717** по шаблону **WEB-Client**.



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	test8717@mail
MS_UPN	<input checked="" type="checkbox"/>	test8717@mail	test8717@mail

← Назад      Отмена      Продолжить →

Рисунок 256 – 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>1</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>1</sup>. Значение атрибутов заполняется автоматически в соответствии с данными в карточке субъекта<sup>2</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 257).

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.

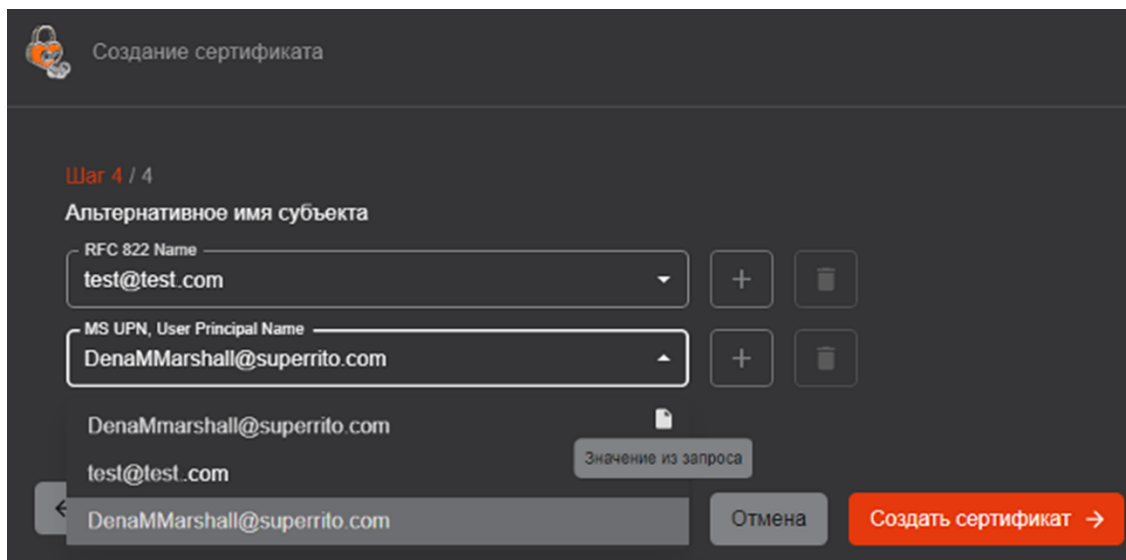


Рисунок 257 – Окно создания сертификата по запросу в разделе «Сертификаты». Шаг 5. Атрибуты сертификата

- Далее по нажатию кнопки **<Создать сертификат>** открывается финальное окно создания сертификата и отображается краткая информация о созданном сертификате (см. Рисунок 258). 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>1</sup> Подробное описание полей предустановленных шаблонов см. в приложении 2 «Описание полей предустановленных шаблонов сертификатов».

<sup>2</sup> Подробнее см. раздел 8.7.2 настоящего руководства.

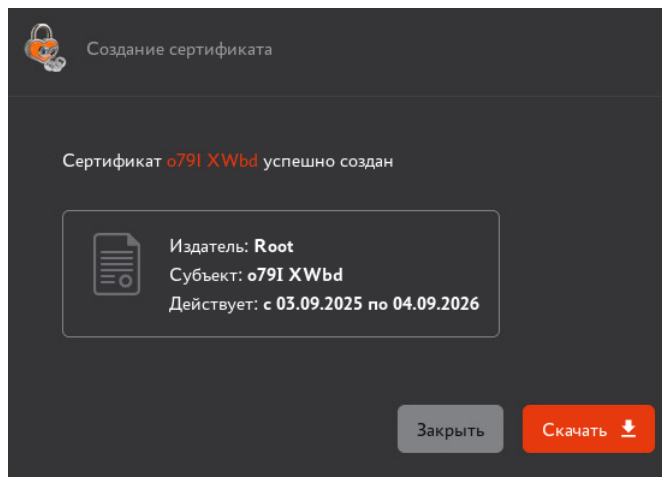


Рисунок 258 – Окно создания сертификата по запросу в разделе «Сертификаты».

Результат успешного создания сертификата

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

### 1.5.2 Создание сертификата субъекта по запросу в разделе «Субъекты»

Порядок создания сертификата 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 загрузите 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. раздел 8.11 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>**.

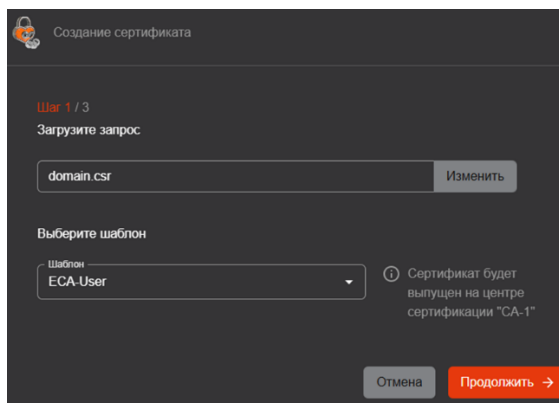


Рисунок 259 – Окно создания сертификата по запросу в разделе «Субъекты». Шаг 1. Загрузка запроса и выбор шаблона

Программа проверяет запрос на соответствие полей запроса на сертификат и атрибутов субъекта по правилам, приведённым в таблице 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 260 и Рисунок 261).

Перечень возможных ошибок представлен в таблице 29.

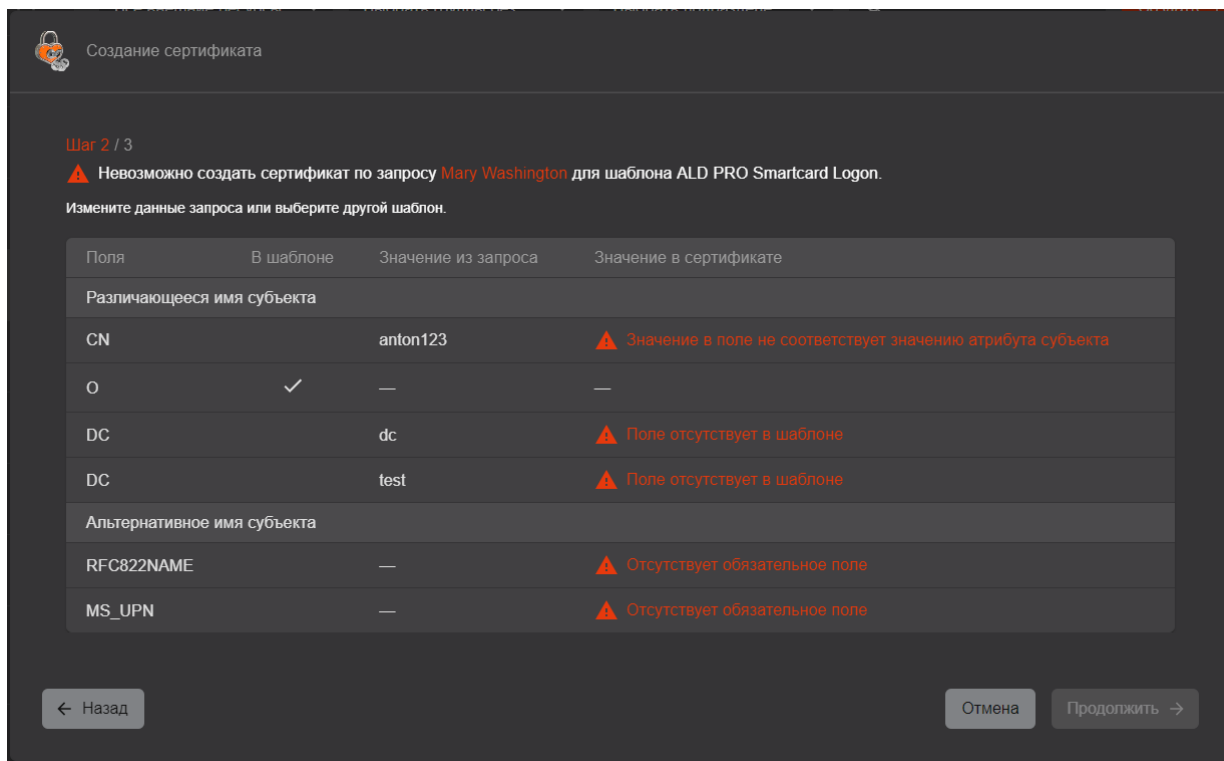


Рисунок 260 – Окно создания сертификата по запросу в разделе «Субъекты». Шаг 2. Результат обработки запроса с ошибкой в поле различающегося имени субъекта

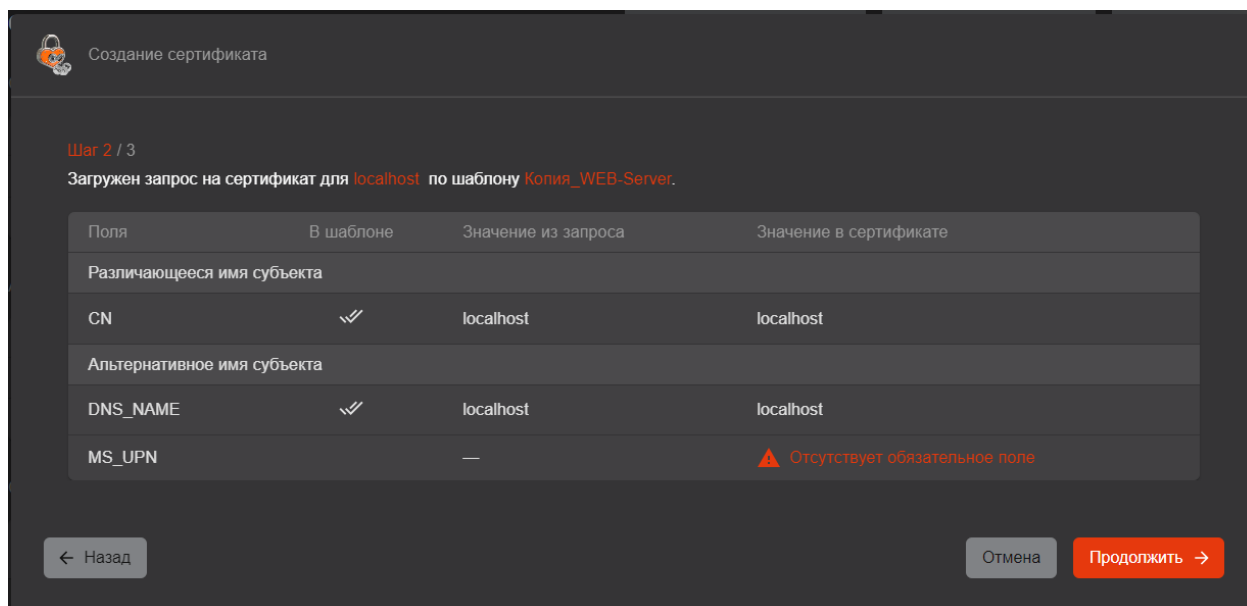




Рисунок 261 – Окно создания сертификата по запросу в разделе «Субъекты». Шаг 2. Результат обработки запроса с ошибками в полях альтернативного имени субъекта

Если создание сертификата невозможно, то существует две возможности:

- вернуться на предыдущий шаг и сменить шаблон на подходящий;
- пересоздать файл-запрос с учётом 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 262):
  - 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 разделены 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>1</sup>, то они идентифицируются по параметру OID.

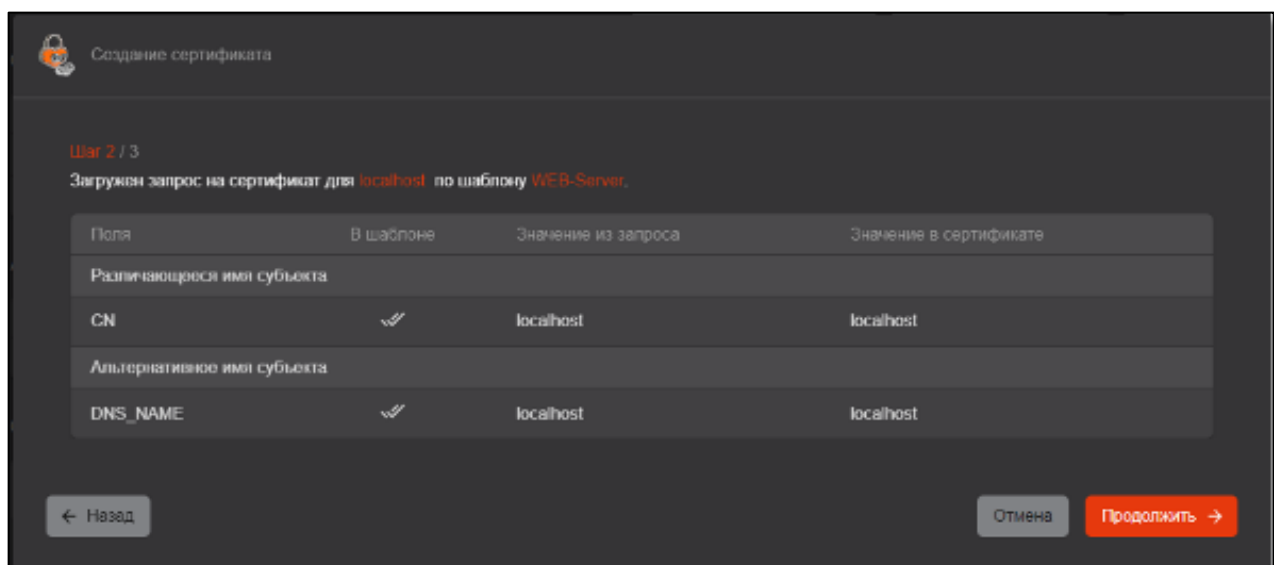





Рисунок 262 – Окно создания сертификата по запросу в разделе «Субъекты». Шаг 2. Результат успешной обработки запроса

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.

<sup>1</sup> Для справки – <https://www.alvestrand.no/objectid/2.5.4.html>, раздел Subdirectory references.

- В открывшемся окне указаны атрибуты в соответствии с шаблоном сертификата (подробное описание полей предустановленных шаблонов см. в приложении 2 «Описание полей предустановленных шаблонов сертификатов». Значение атрибутов заполняется автоматически в соответствии с данными в карточке субъекта (см. раздел 8.7.2 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 263).

Перечень доступных для выбора значений в полях SAN включает в себя:

- значения соответствующего полю атрибута субъекта;
- значения данного поля из запроса, если у субъекта в соответствующем атрибуте есть аналогичное значение, отличающееся от значения в запросе только регистрами символов (такие значения отмечены пиктограммой «Запрос» ).

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

Необязательные поля могут оставаться незаполненными.

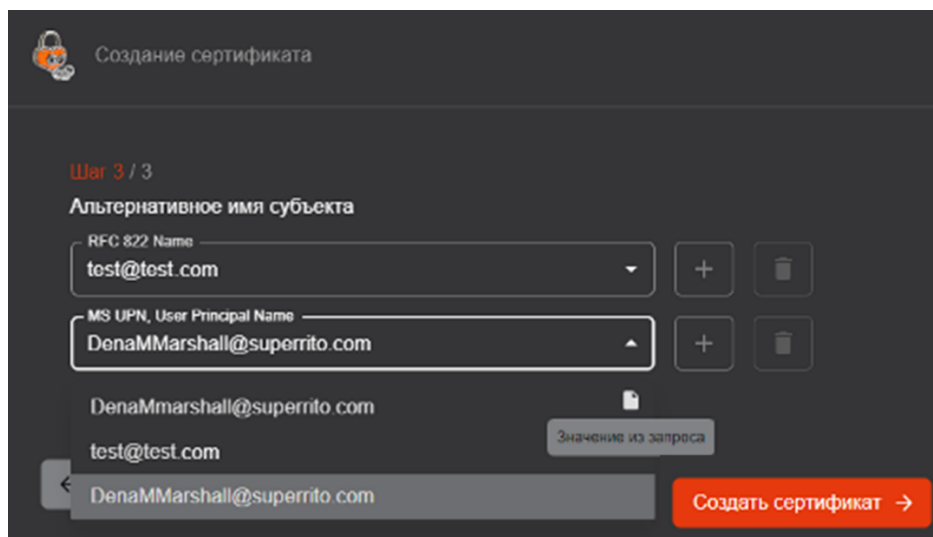


Рисунок 263 – Окно создания сертификата по запросу в разделе «Субъекты». Шаг 4. Атрибуты сертификата

- Далее по нажатию кнопки **<Создать сертификат>** открывается финальное окно создания сертификата и отображается краткая информация о созданном сертификате (см. Рисунок 264). 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.

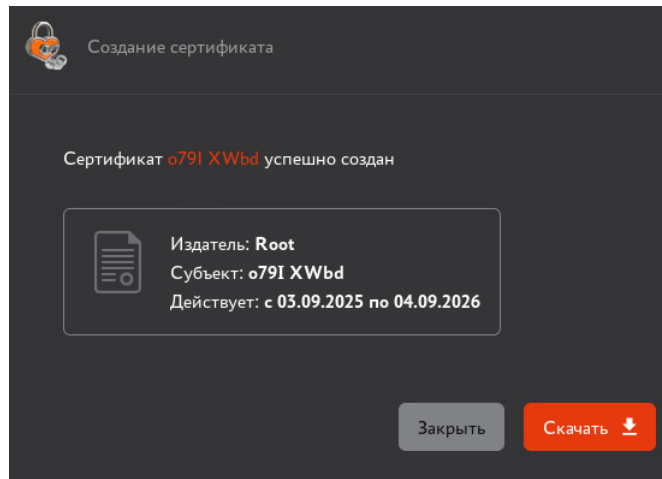


Рисунок 264 – Окно создания сертификата по запросу в разделе «Субъекты». Шаг 4. Информирование об успешном создании сертификата

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

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

## 1.6 Создание сертификата субъекта на ключевом носителе

**Внимание!** Создание сертификата возможно только для существующего субъекта! Предварительно создайте локальный субъект (см. раздел 8.7.3.1 настоящего руководства) или выберите субъект внешней ресурсной системы (см. раздел 8.7.4 настоящего руководства).

eCA-CA поддерживает следующие виды ключевых носителей для создания сертификата:

- JaCarta:
  - JaCarta PKI.
  - JaCarta PRO.
  - JaCarta-2 PKI/ГОСТ.
  - JaCarta-2 ГОСТ.
  - JaCarta-3.
- Рутокен<sup>1</sup>:
  - Рутокен ЭЦП 3.0.
  - Рутокен ЭЦП 2.0.
  - Рутокен ЭЦП 2.0 Flash.
  - Рутокен ЭЦП PKI.

Для работы с ключевыми носителями JaCarta используется приложение JC-WebClient. Рекомендуется использовать приложение последней версии для 64-битных систем.

Для работы с ключевыми носителями Рутокен используется ПО «Рутокен Плагин» и его браузерное расширение «Адаптер Рутокен Плагин».

Порядок установки ПО приведён в документе «Центр сертификатов доступа Aladdin Enterprise Certificate Authority Certified Edition. Руководство администратора. Часть 1. Установка и обслуживание «Центра сертификации Aladdin Enterprise Certification Authority».

**Внимание!** Выпуск сертификатов с алгоритмом ключа ГОСТ Р 34.10-2012 и длиной ключа 512 возможен только на ключевых носителях JaCarta-3.

<sup>1</sup> Возможность использования ключевых носителей Рутокен может быть ограничена лицензией.

**Внимание!** Ограничения по возможностям генерации для ключевых носителей Рутокен приведены на [официальном сайте производителя](#).

Предварительные условия выполнения сценария:

- На компьютере, с которого выполняется подключение к веб-интерфейсу eCA-CA, должно быть установлено приложение JC-WebClient или ПО «Рутокен Плагин».

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 265):
  - «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 266).

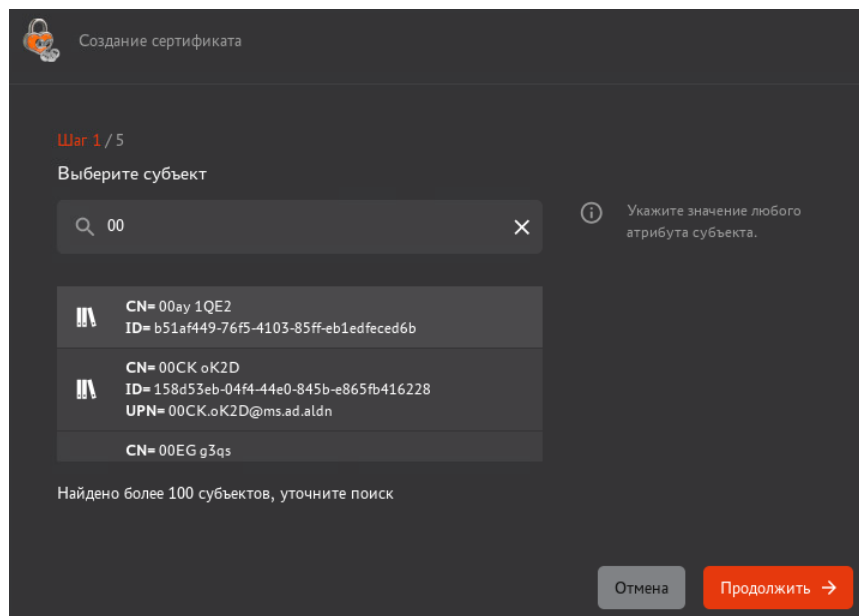


Рисунок 265 – Окно создания сертификата на электронном ключе в разделе «Сертификаты». Шаг 1

- В открывшемся окне (см. Рисунок 266) 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. раздел 8.11 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 заполнения всех полей.

Рисунок 266 – 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 приложении 2 «Описание полей предустановленных шаблонов сертификатов»). Значение атрибутов заполняется автоматически в соответствии с данными в карточке субъекта (см. раздел 8.7.2 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 267). Необязательные поля могут оставаться незаполненными.

Рисунок 267 – 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 267).

- Далее необходимо выбрать параметры криптографии (см. Рисунок 268):
  - 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>**.

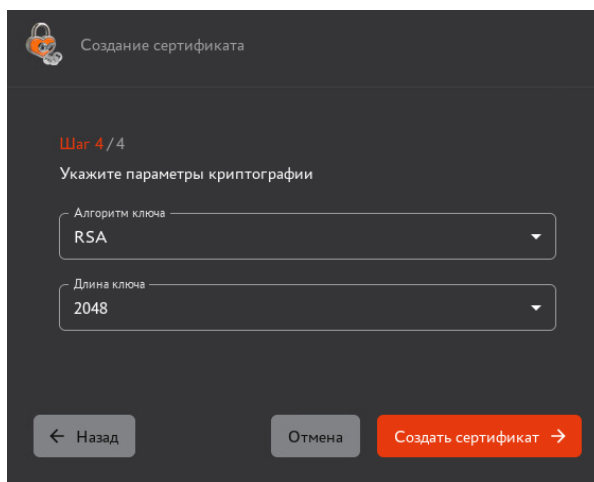


Рисунок 268 – Окно создания сертификата на электронном ключе. Шаг 4

- 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>**..

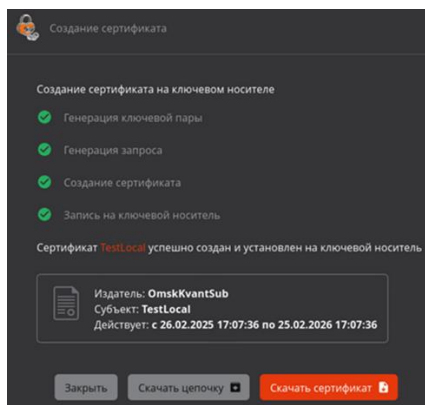


Рисунок 269 – Окно успешного создания сертификата субъекта на электронном ключе

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

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

Сообщения об ошибках при создании сертификата на ключевом носителе:

- В случае, если ПО JC–WebClient или ПО «Рутокен Плагин» предварительно не установлено, то администратор будет уведомлен об этом информационным сообщением (см. Рисунок 270). Для выпуска сертификата на электронном ключе установите ПО JC–WebClient или «Рутокен Плагин».

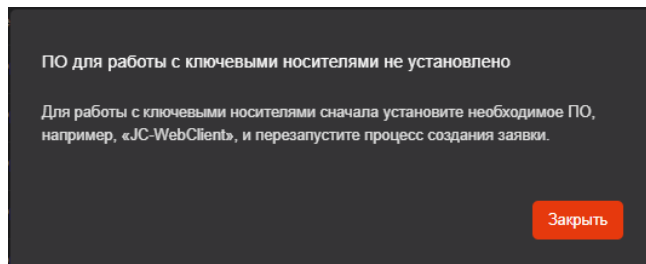


Рисунок 270 – ПО для работы с ключевыми носителями не установлено

- В случае, если электронный носитель не подключен, то администратор будет уведомлен об этом информационным сообщением (см. Рисунок 271). Для выпуска сертификата подключите электронный ключ и перезапустите мастер создания сертификата.

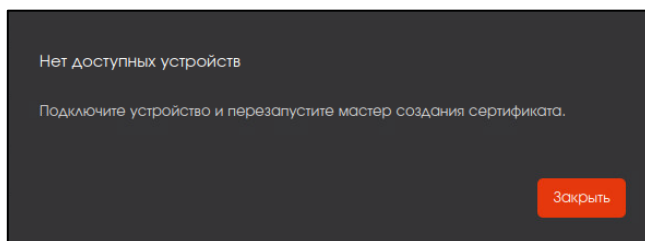


Рисунок 271 – Окно информационного сообщения «Нет доступных устройств»

- В случае, если выбранный для выпуска сертификата алгоритм не поддерживается выбранной моделью ключевого носителя, администратор будет уведомлён об этом информационным сообщением.

## 1.7 Создание короткоживущего сертификата

Под короткоживущими (short-lived, throwaway) сертификатами подразумеваются сертификаты, отвечающие следующим требованиям:

- сертификат после его выпуска не сохраняется в базе данных eCA-CA;
- период действия сертификата не превышает 1 сутки;
- сертификат не содержит записей о точках распространения CRL, Delta CRL и службах OCSP, однако может содержать записи о точках AIA;
- у сертификата отсутствует владелец-субъект, и, как следствие, данный сертификат не влияет на лицензируемое количество субъектов с действующими сертификатами.

Выпуск короткоживущих (short-lived, throwaway) сертификатов доступен только через методы публичного API v3 и v4.

ПРИЛОЖЕНИЕ 2. ОПИСАНИЕ ПОЛЕЙ ПРЕДУСТАНОВЛЕННЫХ ШАБЛОНОВ СЕРТИФИКАТОВ

Имя шаблона	Идентификатор	Период действия сертификата	Тип субъекта	Центр сертификации	Выпуск сертификатов с закрытым ключом (PKCS#12)	Публиковать сертификат в ресурсную систему	Короткое имя (short-lived, throwaway) сертификат	Шифрование		Использование ключа		Расширенное использование ключа		Включать SID субъекта в сертификат	Контролировать соответствие полей в сертификате атрибутам субъекта	Компоненты имени сертификата						Сведения о средствах ЭП и УЦ
																Отличительное имя субъекта			Альтернативное имя субъекта			
								Алгоритм	Минимальная длина ключа	Значения	Крит.	Значения	Крит.			Поле	Обязат.	Вал. и дац.	Поле	Обязат.	Вал. и дац.	
[Deprecated] ECA-Auth	8ecba810-7f48-4c4e-b803-99a97146e2ba	2y	Пользователь	Любой	+	-	-	RSA	1024	• Цифровая подпись • Подтверждение подлинности • Шифрование ключей	+	• Аутентификация клиента • Защита электронной почты	-	-	+	Common name	+	+	-			-
								ECD SA	256													
								ГОСТ Р 34.10-2012	Выключен													
[Deprecated] ECA-User	e97d92b1-2e6e-4ed2-943f-6508113feac6	2y	Пользователь	Любой	+	-	-	RSA	1024	• Цифровая подпись • Подтверждение подлинности • Шифрование ключей	+	• Аутентификация клиента • Защита электронной почты	-	-	+	Common name	+	+	-			-
								ECD SA	256													
								ГОСТ Р 34.10-2012	256													
[Deprecated] Domain Controller	bf2dac0a-f05f-49dd-95b4-e50691489b6a	2y	Устройство	Любой	+	-	-	RSA	1024	• Цифровая подпись • Подтверждение подлинности • Шифрование ключей	+	• Аутентификация клиента • Центр распространения ключей Kerberos • SSH сервер	-	-	+	Common name	+	+	DNS name	+	+	-
								ECD SA	256										MS GUID	+	+	
								ГОСТ Р 34.10-2012	Выключен													
[Deprecated]	aa03e458-50cd-	2y	Пользователь	Любой	+	-	-	RSA	1024		+		-	-	+	Common name	+	+	MS UPN	+	+	-

Smartcard Logon	46b8-82cd-d5612ed3b647							ECD SA	256	• Цифровая подпись • Подтверждение подлинности • Шифрование ключей • Шифрование данных		• Аутентификация клиента • Защита электронной почты • Вход с MS смарт-картой								RFC 822 Name	+	+	
								ГОСТ Р 34.10-2012	Выключен														
[Deprecated] WEB-Client	059a38f5-f345-4275-b79f-e7e6cc3cbb68	2y	Пользователь	Любой	+	-	-	RSA	1024	• Цифровая подпись • Подтверждение подлинности • Шифрование ключей	+	• Аутентификация клиента • Защита электронной почты	-	-	+	Common name	+	+	MS UPN	+	+	-	
								ECD SA	256														
								ГОСТ Р 34.10-2012	Выключен														RFC 822 Name
[Deprecated] WEB-Server	08c66f99-218a-46ef-bdee-6a2b3b26a4f1	2y	Устройство	Любой	+	-	-	RSA	1024	• Цифровая подпись • Шифрование ключей	+	Аутентификация сервера	-	-	+	Common name	+	+	DNS name	+	+	-	
								ECD SA	256														
								ГОСТ Р 34.10-2012	Выключен														
[Deprecated] ECA-WEB-Server	076f61dc-5ff4-43cc-8cf9-6b833adf1092	2y	Устройство	Любой	+	-	-	RSA	1024	• Цифровая подпись • Шифрование ключей	+	Аутентификация сервера	-	-	+	Common name	+	+	DNS name	+	+	-	
								ECD SA	256														
								ГОСТ Р 34.10-2012	256														
[Deprecated] S/MIME	0c234243-18cf-4c05-b699-537731b2436f	2y	Пользователь	Любой	+	-	-	RSA	1024	• Цифровая подпись • Подтверждение подлинности	+	• Аутентификация клиента • Защита электронной почты	-	-	+	Common name	+	+	RFC 822 Name	+	+	-	
								ECD SA	256														
								ГОСТ Р 34.10-2012	Выключен														

Cmp. 249 / 275

Cmp. 250 / 275

																Pseudo nym	-	+				
																Postal address	-	+				
																Street	-	+				
																Name	-	+				
																Title	-	+				
																Domain qualifie r	-	+				
																Descrip tion	-	+				
																Unstruc tured address	-	+				
																Unstruc tured name	-	+				
																Email Address (E)	-	+				
																Serial number	-	+				
																Organiz ation	-	+				
																ИНН	-	+				
																ОГРН	-	+				
																ОГРНИ П	-	+				
																СНИЛ С	-	+				
																ИНН ЮЛ	-	+				
[Depre cated]	af3b0355- 1798- 4c64-	25y	Подчин ённый ЦС	Любой	+	-	-	RSA	1024	• Цифров ая подпись	+	• Любое расширен ное	-	-	+	Commo n name	+	+	RFC 822 Name	-	+	-

Sub CA	98f7- a9c70407 db1c									• Подпис ь сертифик ата • Подпис ь списка отзыва	использо вание ключа • Аутенти фикация клиента • Аутенти фикация сервера							Unique Identifi er (UID)	-	+	DNS name	-	+	
								ECD SA	256									Given name	-	+	MS UPN	-	+	
								ГОС Т Р 34.10 -2012	256															
																		Initials	-	+	MS GUID	-	+	
																		Surnam e	-	+	IP address	-	+	
																		Organiz ational unit	-	+	Directo ry Name	-	+	
																		Locality	-	+	Unifor m resourc e identifi er	-	+	
																		State or provinc e	-	+	Registe red Identifi er (OID)	-	+	
																		Domain compon ent	-	+	Perma nent identifi er	-	+	
																		Country	-	+	Xmpp address	-	+	
																		Postal code	-	+	Service Name	-	+	
																		Busines s categor y	-	+	Subject Identifi cation Metho d	-	+	
																		Telepho ne number	-	+	Kerber os KPN	-	+	

																Pseudo nym	-	+				
																Postal address	-	+				
																Street	-	+				
																Name	-	+				
																Title	-	+				
																Domain qualifie r	-	+				
																Descrip tion	-	+				
																Unstruc tured address	-	+				
																Unstruc tured name	-	+				
																Email Address (E)	-	+				
																Serial number	-	+				
																Organiz ation	-	+				
																ИНН	-	+				
																ОГРН	-	+				
																ОГРНИ П	-	+				
																СНИЛ С	-	+				
																ИНН ЮЛ	-	+				
		25y		Любой	+	-	-	RSA	1024		+	-	-	-	+		+	-		-		-

[Depre- cated] SCEP Manag- ement	3e5df3d4- 683c- 4252- b862- 467589c2 225b		Устрой- ство					ECD SA	256	• Цифров ая подпись • Шифро вание ключей • Шифро вание данных						Commo n name						
								ГОС Т Р 34.10 -2012	256													
User	25862d3b- 8904- 407f- 9d36- 356dde84 a293	1y	Пользо- ватель	Любой	+	-	-	RSA	2048	• Цифров ая подпись • Подтвер ждение подлинно сти • Шифро вание ключей	+	• Аутенти фикация клиента • Защита электронн ой почты	-	-	+	Commo n name	+	+	-			-
								ECD SA	256													
								ГОС Т Р 34.10 -2012	256													
Domai- n Contro- ller	3da2ce13- 8494- 47d1- 8afc- 59048d9f e0b6	1y	Устрой- ство	Любой	+	-	-	RSA	2048	• Цифров ая подпись • Подтвер ждение подлинно сти • Шифро вание ключей	+	• Аутенти фикация клиента • Центр распростр анения ключей Kerberos • Аутенти фикация сервера	-	-	+	Commo n name	+	+	DNS name	+	+	-
								ECD SA	256										MS GUID	+	+	
								ГОС Т Р 34.10 -2012	256													
Smartc- ard Logon	adbb089c- 9868- 4188- b0ce- 9631eec0 7c1e	1y	Пользо- ватель	Любой	+	-	-	RSA	2048	• Цифров ая подпись • Подтвер ждение подлинно сти • Шифро вание ключей • Шифро вание данных	+	• Аутенти фикация клиента • Защита электронн ой почты • Вход с MS смарт- картой	-	-	+	Commo n name	+	+	MS UPN	+	+	-
								ECD SA	256										RFC 822 Name	+	+	
								ГОС Т Р 34.10 -2012	256													
WEB- Client	0044967a- f269- 477b- 97b6-	1y	Пользо- ватель	Любой	+	-	-	RSA	2048	• Цифров ая подпись • Подтвер ждение	+	• Аутенти фикация клиента	-	-	+	Commo n name	+	+	MS UPN	+	+	-
								ECD SA	256											+	+	

	b5d1f1e6923e							ГОСТ Р 34.10-2012	256	подлинности • Шифрование ключей		• Защита электронной почты							RFC 822 Name			
WEB-Server	1ed0d903-5f8c-4a6b-b881-6c8cbd61070b	1y	Устройство	Любой	+	-	-	RSA	2048	• Цифровая подпись • Шифрование ключей	+	Аутентификация сервера	-	-	+	Common name	+	+	DNS name	+	+	-
								ECD SA	256													
								ГОСТ Р 34.10-2012	256													
S/MIME	e7ec9d66-6d97-4f30-9d93-92a5dd101bb0	1y	Пользователь	Любой	+	-	-	RSA	2048	• Цифровая подпись • Подтверждение подлинности • Шифрование ключей • Шифрование данных	+	• Аутентификация клиента • Защита электронной почты • Вход с MS смарт-картой	-	-	+	Common name	+	+	RFC 822 Name	+	+	-
								ECD SA	256													
								ГОСТ Р 34.10-2012	256													
ALD PRO Domain Controller	3d1d2fd5-1134-49ea-8473-65017e7bf7b	1y	Устройство	Любой	+	-	-	RSA	2048	• Цифровая подпись • Подтверждение подлинности • Шифрование ключей • Шифрование данных	+	• Аутентификация клиента • Центр распространения ключей Kerberos • Аутентификация сервера	-	-	+	Common name	+	+	MS UPN	+	+	-
								ECD SA	256							Organization	-	+	Kerberos KPN	+	+	
								ГОСТ Р 34.10-2012	256													
ALD PRO Smartcard Logon	3866ec41-9407-4862-aeb6-5980e951e825	1y	Пользователь	Любой	+	-	-	RSA	2048	• Цифровая подпись • Подтверждение подлинности	+	• Аутентификация клиента • Центр распространения ключей Kerberos	-	-	+	Common name	+	+	MS UPN	+	+	-
								ECD SA	256							Organization	-	+	RFC 822 Name	+	+	
								ГОСТ Р 34.10-2012	256													

Cmp. 256 / 275

[illegible]

																Serial number	-	+				
																Organization	-	+				
																Role	-	+				
																Дата рождения	-	+				
																Место рождения	-	+				
																ИНН	-	+				
																ОГРН	-	+				
																ОГРНИП	-	+				
																СНИЛС	-	+				
																ИНН ЮЛ	-	+				
Sub CA	04ca3e95-376a-48f2-95fa-37711f3c43b3	7y	Подчинённый ЦС	Любой	+	-	-	RSA	3072	• Цифровая подпись • Подпись сертификата • Подпись списка отзыва	+	• Любое расширенное использование ключа • Аутентификация клиента • Аутентификация сервера	-	-	+	Common name	+	+	RFC 822 Name	-	+	-
								Unique Identifier (UID)	-							+	DNS name	-	+			
								Given name	-							+	MS UPN	-	+			
								Initials	-							+	MS GUID	-	+			
								Surname	-							+	IP address	-	+			
								Organizational unit	-							+	Directory Name	-	+			
								Locality	-							+	Uniform	-	+			

																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																					</
--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	----

																Unstruc tured address	-	+				
																Unstruc tured name	-	+				
																Email Address (E)	-	+				
																Serial number	-	+				
																Organiz ation	-	+				
																Role	-	+				
																Дата рожден ия	-	+				
																Место рожден ия	-	+				
																ИНН	-	+				
																ОГРН	-	+				
																ОГРНИ П	-	+				
																СНИЛ С	-	+				
																ИНН ЮЛ	-	+				
SCEP Manag ement	f6097cd0- b1aa- 47e8- 8b8d- fe75c127 384a	25y	Устрой ство	Любой	+	-	-	RSA	2048	• Цифров ая подпись • Шифро вание ключей • Шифро вание данных	+	-	-	-	+	Commo n name	+	-	-		-	
								ECD SA	256													
								ГОС Т Р 34.10 -2012	256													

## ПРИЛОЖЕНИЕ 3. 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 или 14 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 или 14 символов.
Postal code	Допускается любая последовательность символов, в которой отсутствуют непарные двойные кавычки ("").
Дата рождения	Формат значения: дата в формате «DD.MM.YYYY».
<b>Поля SAN</b>	
RFC 822 Name	Допустимые символы: "A"—"Z", "a"—"z", "0"—"9", ".", "@", "_", "-". Формат значения: "text@text". Пример заполнения: «ivanova@example.com».
DNS Name	Допустимые символы: "A"—"Z", "a"—"z", "0"—"9", "-", ".", "*". Пример значения: «dc1.presale.aeca».
IP address	Допустимые символы: "A"—"F", "a"—"f", "0"—"9", ".", ":". Формат значения: IPv4—адрес или IPv6—адрес.
Directory Name	Формат значения: последовательность идентификаторов относительных отличительных имён (RDN) и их значений, отделенных запятой или запятой с пробелом (например, O=organization, OU=Department, L=City, DC=Component..). Допускается использование следующих идентификаторов RDN: EMAILADDRESS, CN, UID, SERIALNUMBER, OU, O, L, ST, C, T, SURNAME, STREET, INITIALS, GIVENNAME, DC, UNSTRUCTUREDADDRESS, UNSTRUCTUREDNAME, POSTALCODE, BUSINESSCATEGORY, TELEPHONENUMBER, PSEUDONYM, POSTALADDRESS, NAME, DN, DESCRIPTION. В качестве идентификатора RDN допускается указание OID (формат OID должен соответствовать рекомендации ITU X.660).
Registered Identifier (OID)	Допустимые символы: "0"—"9", ".". Формат значения: OID в соответствии с рекомендацией ITU X.660.
MS UPN, User Principal Name	Допустимые символы: "A"—"Z", "a"—"z", "A"—"Я", "a"—"я", "ё", "Ё", "0"—"9", ".", "@", "_", "-", "/", "\"". Формат значения: "text@text". Пример заполнения: «krbtgt/ald.pro@ald.pro».
MS GUID, Globally Unique Identifier	Допустимые символы: "A"—"F", "a"—"f", "0"—"9". Длина значения должна составлять 32 символа. Пример значения: «92625ee510e248479554779d1f43f751».

Поле	Правило валидации
Kerberos KPN, Kerberos 5 Principal Name	Допустимые символы: "A"–"Z", "a"–"z", "A"–"Я", "a"–"я", "ё", "Ё", "0"–"9", ".", "@", "_", "–", "/", ".". Формат значения: «text@text». Пример заполнения: «krbtgt/ald.pro@ald.pro».
Permanent Identifier	Формат значения: "value/OID", где "value" – любая последовательность символов, а "OID" – OID в соответствии с рекомендацией ITU X.660. Допускается отсутствие значения "text", например, "/1.2.2.3.4.5".
Xmpp address	Допустимые символы: "A"–"Z", "a"–"z", "A"–"Я", "a"–"я", "ё", "Ё", "0"–"9", ".", "@", "_", "–", "/", ".". Формат значения: "text@text".
Subject Identification Method	Формат значения: "OID::text::text", где "OID" – OID в соответствии с рекомендацией ITU X.660, а "text" – любая последовательность символов.

## ПРИЛОЖЕНИЕ 4. 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.

Имя	OID	Описание
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.

## ПРИЛОЖЕНИЕ 5. ФОРМАТ И ПРАВИЛА ЗАПИСИ ЗНАЧЕНИЙ В ПОЛЯ СЕРТИФИКАТА НА БУМАЖНОМ НОСИТЕЛЕ

### 5.1 Формат сертификата на бумажном носителе для физического лица

<b>Сертификат ключа проверки электронной подписи</b>	
1.	Номер квалифицированного сертификата: _____
2.	Действие квалифицированного сертификата: с _____ по _____
3.	Сведения о владельце квалифицированного сертификата
	- Фамилия, имя, отчество: _____
	- ПИН: _____
4.	Сведения об издателе квалифицированного сертификата
	- Наименование УЦ: _____
	- Место нахождения УЦ: _____
	- Доверенное лицо УЦ: _____
5.	Номер квалифицированного сертификата УЦ: _____
6.	Наименование средства ЭП: _____
7.	Реквизиты заключения о подтверждении соответствия средства ЭП: _____
8.	Наименование средства УЦ: _____
9.	Реквизиты заключения о подтверждении соответствия средства УЦ: _____
10.	Сведения о ключе проверки ЭП
	- Используемый алгоритм: _____
	- Используемое средство ЭП: _____
	- Область использования ключа: _____
	- Значение ключа: _____
11.	ЭП под квалифицированным сертификатом
	- Используемый алгоритм: _____
	- Значение ЭП: _____
Подпись уполномоченного лица _____ / _____ /	

### 5.2 Формат сертификата на бумажном носителе для юридического лица

<b>Сертификат ключа проверки электронной подписи</b>	
1.	Номер квалифицированного сертификата: _____
2.	Действие квалифицированного сертификата: с _____ по _____
3.	Сведения о владельце квалифицированного сертификата
	- Наименование юридического лица: _____
	- ИНН: _____
—	

- Место нахождения юридического лица: \_\_\_\_\_

- Уполномоченный представитель юридического лица: \_\_\_\_\_

- ПИН: \_\_\_\_\_

---

4. Сведения об издателе квалифицированного сертификата

- Наименование УЦ: \_\_\_\_\_

- Место нахождения УЦ: \_\_\_\_\_

- Доверенное лицо УЦ: \_\_\_\_\_

5. Номер квалифицированного сертификата УЦ: \_\_\_\_\_

6. Наименование средства ЭП: \_\_\_\_\_

7. Реквизиты заключения о подтверждении соответствия средства ЭП: \_\_\_\_\_

8. Наименование средства УЦ: \_\_\_\_\_

9. Реквизиты заключения о подтверждении соответствия средства УЦ: \_\_\_\_\_

10. Сведения о ключе проверки ЭП

- Используемый алгоритм: \_\_\_\_\_

- Используемое средство ЭП: \_\_\_\_\_

- Область использования ключа: \_\_\_\_\_

- Значение ключа: \_\_\_\_\_

11. ЭП под квалифицированным сертификатом

- Используемый алгоритм: \_\_\_\_\_

- Значение ЭП: \_\_\_\_\_

Подпись уполномоченного лица \_\_\_\_\_ / \_\_\_\_\_ /

### 5.3 Правила записи значений в поля сертификата на бумажном носителе для физического лица

Поле	Значение
1. Номер квалифицированного сертификата	Серийный номер сертификата
2. Действие квалифицированного сертификата	

Поле	Значение
с	Дата и время начала действия сертификата в формате «ДД.ММ.ГГГГ ЧЧ:ММ:СС (UTC)»
по	Дата и время окончания действия сертификата в формате «ДД.ММ.ГГГГ ЧЧ:ММ:СС (UTC)»
3. Сведения о владельце квалифицированного сертификата	
Фамилия, имя, отчество	CN в сертификате
ПИН	INN в сертификате
4. Сведения об издателе квалифицированного сертификата	
Наименование УЦ	CN в сертификате ЦС, издавшего данный сертификат
Место нахождения УЦ	Строка вида «{поле «С» в сертификате ЦС}, {поле «ST» в сертификате ЦС}, {поле «L» в сертификате ЦС}, {поле «STREET» в сертификате ЦС}»
Доверенное лицо УЦ	Строка вида «{поле «Т» в сертификате ЦС} {поле «SURNAME» в сертификате ЦС} {поле «GIVENNAME» в сертификате ЦС}»
5. Номер квалифицированного сертификата УЦ	Серийный номер сертификата ЦС
6. Наименование средства ЭП	issuerSignTool.signTool (1.2.643.100.112 [0]) из сертификата
7. Реквизиты заключения о подтверждении соответствия средства ЭП	issuerSignTool.signToolCert (1.2.643.100.112 [2]) из сертификата
8. Наименование средства УЦ	issuerSignTool.cATool (1.2.643.100.112 [1]) из сертификата
9. Реквизиты заключения о подтверждении соответствия средства УЦ	issuerSignTool.cAToolCert (1.2.643.100.112 [3]) из сертификата
10. Сведения о ключе проверки ЭП	
Используемый алгоритм	Алгоритм ключа в сертификате
Используемое средство ЭП	subjectSignTool (1.2.643.100.111) из сертификата
Область использования ключа	Список keyUsage
Значение ключа	Открытый ключ (hex; разделитель - пробелы)
11. ЭП под квалифицированным сертификатом	
Используемый алгоритм	Алгоритм подписи сертификата
Значение ЭП	Подпись (hex; разделитель - пробелы)

Поле	Значение
<p>Примечания:</p> <p>1 В случае, если для поля сертификата на бумажном носителе в преобразуемом сертификате отсутствуют значения (в случае составных полей – для всех компонентов составного поля отсутствуют значения), то для данного поля в качестве значения указан прочерк «-».</p> <p>2 Формат значения в поле «Используемый алгоритм» в разделе «Сведения о ключе проверки ЭП»:          &lt;Название алгоритма&gt; (&lt;длина ключа&gt;)          Примеры:          - RSA (2048)          - ECDSA (384)          - ГОСТ Р 34.10-2012 (256)</p> <p>3 Формат значения в поле «Используемый алгоритм» в разделе «ЭП под квалифицированным сертификатом»:          - «Алгоритм хеш-суммы» «Алгоритм ключа» - для подписи, формируемой с помощью RSA или ECDSA ключа.          Примеры:          - SHA512RSA          - SHA512ECDSA          - ГОСТ Р 34.11-2012/34.10-2012 (длина ключа)» - для подписи, формируемой с помощью ГОСТ ключа.          Примеры:          - ГОСТ Р 34.11-2012/34.10-2012 (256)          - ГОСТ Р 34.11-2012/34.10-2012 (512)</p>	

#### 5.4 Правила записи значений в поля сертификата на бумажном носителе для юридического лица

Поле	Значение
1. Номер квалифицированного сертификата	Серийный номер сертификата
2. Действие квалифицированного сертификата	
с	Дата и время начала действия сертификата в формате «ДД.ММ.ГГГГ ЧЧ:ММ:СС (UTC)»
по	Дата и время окончания действия сертификата в формате «ДД.ММ.ГГГГ ЧЧ:ММ:СС (UTC)»
3. Сведения о владельце квалифицированного сертификата	
Наименование юридического лица	CN в сертификате
ИНН	INNLE в сертификате
Место нахождения юридического лица	Строка вида «{поле «С» в сертификате}, {поле «ST» в сертификате}, {поле «L» в сертификате}, {поле «STREET» в сертификате}»
Уполномоченный представитель юридического лица	Строка вида «{поле «Т» в сертификате} {поле «SURNAME» в сертификате} {поле «GIVENNAME» в сертификате}»
ПИН	INN в сертификате
4. Сведения об издателе квалифицированного сертификата	
Наименование УЦ	CN ЦС
Место нахождения УЦ	Строка вида «{поле «С» в сертификате ЦС}, {поле «ST» в сертификате ЦС}, {поле «L» в сертификате ЦС}, {поле «STREET» в сертификате ЦС}»
Доверенное лицо УЦ	Строка вида «{поле «Т» в сертификате ЦС} {поле «SURNAME» в сертификате ЦС} {поле «GIVENNAME» в сертификате ЦС}»
5. Номер квалифицированного сертификата УЦ	Серийный номер сертификата ЦС
6. Наименование средства ЭП	issuerSignTool.signTool (1.2.643.100.112 [0]) из сертификата

Поле	Значение
7. Реквизиты заключения о подтверждении соответствия средства ЭП	issuerSignTool.signToolCert (1.2.643.100.112 [2]) из сертификата
8. Наименование средства УЦ	issuerSignTool.cATool (1.2.643.100.112 [1]) из сертификата
9. Реквизиты заключения о подтверждении соответствия средства УЦ	issuerSignTool.cAToolCert (1.2.643.100.112 [3]) из сертификата
10. Сведения о ключе проверки ЭП	
Используемый алгоритм	Алгоритм ключа в сертификате
Используемое средство ЭП	subjectSignTool (1.2.643.100.111) из сертификата
Область использования ключа	Список keyUsage
Значение ключа	Открытый ключ (hex; разделитель - пробелы)
11. ЭП под квалифицированным сертификатом	
Используемый алгоритм	Алгоритм подписи сертификата
Значение ЭП	Подпись (hex; разделитель - пробелы)
<p>Примечания:</p> <p>1 В случае, если для поля сертификата на бумажном носителе в преобразуемом сертификате отсутствуют значения (в случае составных полей – для всех компонентов составного поля отсутствуют значения), то для данного поля в качестве значения указан прочерк «-».</p> <p>2 Формат значения в поле «Используемый алгоритм» в разделе «Сведения о ключе проверки ЭП»: &lt;Название алгоритма&gt; (&lt;длина ключа&gt;) Примеры: - RSA (2048) - ECDSA (384) - ГОСТ Р 34.10-2012 (256)</p> <p>3 Формат значения в поле «Используемый алгоритм» в разделе «ЭП под квалифицированным сертификатом»: - «Алгоритм хеш-суммы» «Алгоритм ключа» - для подписи, формируемой с помощью RSA или ECDSA ключа. Примеры: - SHA512RSA - SHA512ECDSA - ГОСТ Р 34.11-2012/34.10-2012 (длина ключа) - для подписи, формируемой с помощью ГОСТ ключа. Примеры: - ГОСТ Р 34.11-2012/34.10-2012 (256) - ГОСТ Р 34.11-2012/34.10-2012 (512)</p>	

## 5.5 Пример сертификата на бумажном носителе для физического лица

Сертификат ключа проверки электронной подписи	
1.	Номер квалифицированного сертификата: 1389df28647548cd880ebfa2ad6c22ddff14f6da
2.	Действие квалифицированного сертификата: с 02.09.2025 14:16:23 UTC по 03.09.2026 14:16:23 UTC
3.	Сведения о владельце квалифицированного сертификата <ul style="list-style-type: none"> <li>- Фамилия, имя, отчество: Иванов Иван Иванович</li> <li>- ПИН: 01234567891234</li> </ul>
4.	Сведения об издателе квалифицированного сертификата <ul style="list-style-type: none"> <li>- Наименование УЦ: Root</li> <li>- Место нахождения УЦ: Страна, Область, Город, Ул. Тест 3, д. 123</li> <li>- Доверенное лицо УЦ: Директор Петров Петр Петрович</li> </ul>
5.	Номер квалифицированного сертификата УЦ: 3afef9c1f4b24b4d9afd0e0bb5f9befd24c1d65e
6.	Наименование средства ЭП: КриптоПро HSM
7.	Реквизиты заключения о подтверждении соответствия средства ЭП: Заключение на КриптоПро HSM
8.	Наименование средства УЦ: КриптоПро УЦ
9.	Реквизиты заключения о подтверждении соответствия средства УЦ: Заключение на КриптоПро УЦ
10.	Сведения о ключе проверки ЭП <ul style="list-style-type: none"> <li>- Используемый алгоритм: RSA (2048)</li> </ul>

- Используемое средство ЭП: КриптоПро CSP
- Область использования ключа: Цифровая подпись, Подтверждение подлинности, Шифрование ключей
- Значение ключа: 30 82 01 22 30 0D 06 09 2A 86 48 86 F7 0D 01 01 01 05 00 03 82 01 0F 00 30 82 01 0A 02 82 01 01 00 BC C2 E8 BC 6E 23 B5 42 35 88 57 1E 18 8B BE D4 99 87 8B A3 C9 12 C8 8A 89 91 D6 07 37 B9 98 90 4B 90 97 A7 07 81 E8 CC 69 EF EC B4 03 D4 41 DA 16 FD 3E 0F BA D0 5A 52 4F 4B D7 0E CB 42 7E AD 73 8B 52 7C E7 71 AE 84 D0 DD 92 1B 4A F6 1E 3C F4 55 59 FA 1B E8 60 03 40 CB 6A 68 E1 54 01 34 ED 61 5E CA 10 B4 83 5E 02 99 E5 3F C6 69 43 19 6D AF 4E B1 0F D3 40 2A B6 53 6F 70 64 26 07 15 5F 94 BD 2F CF 0C 00 4B 71 61 43 8C 8D 9D E3 4C 11 9C 94 E3 B8 4F 85 14 3F 15 DF EA 9B 8F 3F 48 57 22 36 E3 FE 40 19 9B 90 1F A1 19 E5 12 41 31 98 B2 97 F0 0C 74 74 CD BF D9 C3 20 1A 42 9C 1B 4A A7 FA D1 DA C9 31 23 55 A6 EB 30 8D 34 0E D4 38 3A EB 36 A2 3B 56 A2 0F 0C 03 AC 1A DD 54 C5 5B 09 D0 F0 00 CB 2B E1 DD 67 03 CB 52 C0 73 C1 0F 14 9B 7D C8 EB 2D 69 6B 82 B0 10 95 D9 55 B3 02 03 01 00 01

11. ЭП под квалифицированным сертификатом

- Используемый алгоритм: SHA512RSA
- Значение ЭП: 76 4C C2 F3 6A 78 81 03 2B F9 CF 99 76 BB 4F 03 82 FC 89 7C 48 66 94 9A 6B E0 5A 6B E5 55 C4 A4 78 FC DC 2B DB 5A 9B CB DE 95 89 AD CB 30 23 A8 F3 31 6F F4 AD 85 B8 71 9B FB 44 ED AB B3 78 39 F3 75 03 3B 8B 92 48 C2 39 D1 FB CF E5 79 53 52 77 77 FD 2B 2A D2 E6 5E BA 0C B8 FE 2F 13 32 0F A6 5D B9 77 46 8D C3 A4 65 5E 52 07 D8 42 AF 72 11 F2 F6 03 4D 82 4F 36 A5 6E C1 3E 8F 16 B0 D9 C2 A7 EA 8D 91 79 EB D8 26 CA DF 96 67 99 5A 73 E2 70 AC B3 D3 ED 4F E8 B9 B5 62 A4 5F 9E FE 4A 20 F5 27 38 7A 48 ED C4 BA C3 59 6D 67 C9 08 3C 5F 82 81 C8 AE 4B 20 88 87 C1 79 BC EF 77 F5 FA 44 E0 25 1B B9 20 38 9B 6A B6 AB 27 D8 19 33 04 52 47 5A A9 8D 06 C4 38 3B E3 DB FD 00 3B F7 F1 BA 66 65 8D 26 C6 02 E4 8C 5C E7 CC 24 7A A2 32 CD B9 FD BA 22 A5 4B 84 14 BB 97 DA 28 B9 4E F1 CF 1E 73 E7 A8 11 8E 75 B2 F6 3A 27 5C D4 67 55 03 5E F3 B6 E3 B9 26 65 34 DB 51 87 4D 9B 07 D3 83 41 D7 3F 18 21 94 DF C4 FA 23 6A 4D A0 1F 86 3E D3 D4 A8 9F FA 1C 15 5C 49 35 38 CD 02 CB 2F C5 F7 10 B2 66 A4 CE 40 F8 2B 17 0A EE 7F 37 66 C8 5F 38 86 0F 11 CD 8A 38 FF 23 B2 3B B1 62 E6 16 6E 69 C2 43 86 11 EE B9 64 4A 1C FD 6F 03 1B 10 E5 95 73 82 CF 37 EA B1 FB 72 EA D6 2A 45 99 F7 01 A4 EA 53 27 C9 C4 D1 2C 2C AE 9C 50 27 EC E2 B7 1B 61 60 A8 63 7A 4B B3 D9 8F C8 19 C0 B6 9A C1 6C 02 FB 81 0D 79 3C 87 37 FA 17 37 B2 E7 15 58 D0 F8 05 57 79 BA 57 C2 66 56 78 40 B5 EA 8F C3 4C 31 5B D7 8F 53 B5 C0 7E 0C 8B 73 0F 74 17 0F D2 FC 67 3B 23 3B 9A C8 FB A0 69 80 48 2B F0 C6 55 C4 C0 56 1D 93 DE 5E 69 2A 8B 05 B3 D5 D2 CB DC E9 95 72 84 90 AD 7B 8B BC 41 4F 2A 2D

Подпись уполномоченного лица \_\_\_\_\_ / \_\_\_\_\_ /

## 5.6 Пример сертификата на бумажном носителе для юридического лица

### Сертификат ключа проверки электронной подписи

1. Номер квалифицированного сертификата: 5b4d309e9baee870703354096d6580c9bbf11f10
2. Действие квалифицированного сертификата: с 02.09.2025 14:15:16 UTC по 03.09.2026 14:15:16 UTC
3. Сведения о владельце квалифицированного сертификата
  - Наименование юридического лица: ОсОО Тест
  - ИНН: 01234567891234
  - Место нахождения юридического лица: Страна, Область, Город, Пер. Тест 32 д. 456
  - Уполномоченный представитель юридического лица: Директор Антонов Антон Антонович
  - ПИН: 01234567891234
4. Сведения об издателе квалифицированного сертификата
  - Наименование УЦ: Root
  - Место нахождения УЦ: Страна, Область, Город, Пер. Тест 32 д. 123
  - Доверенное лицо УЦ: Директор Петров Петр Петрович
5. Номер квалифицированного сертификата УЦ: 3afef9c1f4b24b4d9afd0e0bb5f9befd24c1d65e
6. Наименование средства ЭП: КриптоПро HSM
7. Реквизиты заключения о подтверждении соответствия средства ЭП: Заключение на КриптоПро HSM
8. Наименование средства УЦ: КриптоПро УЦ
9. Реквизиты заключения о подтверждении соответствия средства УЦ: Заключение на КриптоПро УЦ
10. Сведения о ключе проверки ЭП
  - Используемый алгоритм: RSA (2048)
  - Используемое средство ЭП: КриптоПро CSP
  - Область использования ключа: Цифровая подпись, Подтверждение подлинности, Шифрование ключей
  - Значение ключа: 30 82 01 22 30 0D 06 09 2A 86 48 86 F7 0D 01 01 05 00 03 82 01 0F 00 30 82 01 0A 02 82 01 01 00 AF 2E 5F 8A 22 28 4B 1C 8E 71 EC 96 BD E4 F6 2E 14 73 AE FC 1D 1E 13 88 BA E4 B8 DD 54 05 0E 14 48 CD C4 A8 68 81 7F 18 22 D6 B4 4C 7B 17 EA 1A 60 50 12 41 11 70 BC 60 04 B8 61 03 2C 5F 67 17 D0 33 55 DF 65 59 E7 EE 53 82 91 D6 BC 81 02 BB DF 2C 06 74 07 6A AC 18 91 E9 5D 3C CC 6C 11 A1 19 D1 6F BE A7 57 B2 14 FE E3 A2 C1 C8 8F 42 DA 1B 88 C8 B6 62 EE EE 78 7E 1F 75 99 D9 5E AE 9D CC 75 C5 34 2A AF 9D 4D D4 27 B5 9A 75 4E AE D3 95 E2 CF 3C DD 6D 36 7C AC 98 6D 99 D1 DE FB AF 60 B6 92 DF 97 17 AC 2C 18 B1 47 3C D7 C4 D0 6A E7 50 26 DF 8D F7 7A 72 45 AA 74 B2 09 22 9F C0 1A 77 2A D1 4A 2D A2 3D D6 85 E2 BE FD 25 3B 20 FF 1D 0A A4 13 91 E3 70 C9 62 5B FB 57 0E 39 B1 B5 18 3C C2 4D A6 35 06 86 57 FC F4 9E 80 AC 59 82 B7 6B 2F A5 7B 9B 7C 82 CC B2 6A 59 79 31 F5 02 03 01 00 01
11. ЭП под квалифицированным сертификатом
  - Используемый алгоритм: SHA512RSA
  - Значение ЭП: 86 A5 1D 7E 93 F2 43 FB 4A C4 59 38 C5 69 C9 B0 46 23 16 AF EE A2 2C 4F 9F BD D8 EE 1A 3B B5 DF 22 5D 3F 22 FC AF 4F C4 BD C2 50 B7 F5 AB 1C E9 BA A1 FF 40 03 32 5A E6 09 CF FF 79 90 ED 68 38 DD C5 84 A9 43 A0 5B 73 80 C6 48 BD D4 55 86 79 09 9B 07 50 06 7F 61 DD E5 2F A9 F8 3B BC C1 B5 C1 2A F5 85 74 87 42 60 F2 BB F4 47 9E E7 9C 7C 2D 0D DD 3D 14 5C B2 82 5C A6 DB 50 43 0A 06 F2 FF C8 2F 31 95 68 01 64 3C 78 9E B6 A3 9F 42 0F 9C D0 20 0F FC 17 95 08 59 74 45 22 A0 09 18 80 3B 36 27 A2 29 70 DC 7F 90 38 48 73 68 9F 2E 04 34 24 09 91 A9 17 FC 7E 5E 90 20 6C 61 C7 7B 38 8E 8B 6B 7C 55 6C 76 02 EB 96 BA 8F 59 34 22 95 E0 B4 30 3F 02 C3 CE EA 63 EA 50 49 7B 83 2A 0A 16 58 6F 4F EB 30 BD 1E 4A BF 95 D1 A9 44 99 1C 0E B8 08 0A 90 97 B2 A4 9A 61 F7 A3 05 E0 61 29 9A 3C A1 F3 83 9B AE 3B 5B 1D 06 C5 47 CE FB 7D B1 BE 3D 9C 0A 09 33 DE 37 BA 3E A6 87 9C 2E 44 26 42 F9 11 9A 03 6F EB B3 C0 9F CC 46 23 0D D1 14 04 4E BE C7 BA B1 2D 94 E6 FD A9 BF AB E3 E8 5C 99 74 FC 0C 52 F3 5E F6 7A 63 83 9F 50 FD 94 E2 F0 F1 6E 0B 75 0A F4 8D 03 97 0F E8 42 1D CF 80 51 35 19 C4 E3 91 19 58 5D C2 A9 FE 15 A2 B3 07 7F 85 52 60 DA 55 F2 B9 09 9C D8 C1 B5 E2 26 7F DC DF 5E 5B A3 86 A0 01 18 94 B4 22 53 FA 95 9D 7B 5C C0 B0 D6 DB 4E 5B 36 BD F8 D0 AC 57 BF EF 93 6C 98 65 1A 3E FB 63 7F 6C 10 59 F2 EC C0 50 A9 07 F6 61 65 C0 F8 FD 28 98 7F EE 2D 43 9E F2 08 26 EC FC B4 6F 68 29 A0 8E 1A 61 A8 4C BE 9F 32 91 C1 08 BD EC C5 57 8B 48 B8 7E A2 22 E9 0F F4 69 62 B7 61 83 93 D9 9C 76 B8 78 80 88 D1 28 38 8A 04 F2 75 F7 F2 CF 05 CC 0B 77 C7 30 17

Подпись уполномоченного лица \_\_\_\_\_ / \_\_\_\_\_ /

## ОБОЗНАЧЕНИЯ И СОКРАЩЕНИЯ

ОС	– Операционная система
ПО	– Программное обеспечение
СУБД	– Система управления базами данных
УЦ	– Удостоверяющий центр
ЦС	– Центр сертификатов
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 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 развертываемой 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».

**Регулярное выражение** — (англ. *regular expressions*) — формальный язык, используемый в компьютерных программах, работающих с текстом, для поиска и осуществления манипуляций с подстроками в тексте. В eCA–CA используется нотация, приведенная в описании класса Pattern пакета java.util.regex.

**Разрешенные издатели** – это список Центров сертификации, сертификаты которых клиент может использовать для авторизации на сервере, на котором развернут Центр сертификации с актуальным списком разрешенных 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 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 eCA-CA, 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 eCA-CA.

**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. eCA-CA 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]