



Центр сертификатов доступа

Aladdin Enterprise Certificate Authority Certified Edition

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

Издание	RU.АЛДЕ.03.01.020
Документ	RU.АЛДЕ.03.01.020 32 01-2
Версия	2.3
Листов	258
Дата	01.09.2025

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 резэкспорт продукта ограничения.

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

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

Лицензионное соглашение

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

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

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

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

Права и собственность

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

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

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

Лицензия

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

Соглашения:

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

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

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

Требования к использованию

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

Использование ПО

Пользователь вправе:

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

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

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

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

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

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

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

Обслуживание и поддержка

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

Ограниченная гарантия

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

Отказ от гарантии

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

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

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

Ограничение возмещения

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

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

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

Исключение косвенных убытков

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

Ограничение ответственности

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

Прекращение действия соглашения

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

После прекращения действия данного Лицензионного соглашения:

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

Применимое законодательство

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

Государственное регулирование и экспортный контроль

Вы соглашаетесь с тем, что ПО не будет Вами поставляться, передаваться или экспортироваться в какую-либо страну, а также использоваться каким-либо противоречащим закону и условиям настоящего соглашения образом. ПО является предметом дополнительного экспортного контроля, относящегося к Вам или Вашей юрисдикции. Вы гарантируете, что будете соблюдать накладываемые ограничения на экспорт и резкспорт 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»¹.

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»² 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.

¹ Далее по документу – программное средство, Центр сертификатов доступа

² Далее по документу – программа, Центр сертификации Aladdin eCA

СОДЕРЖАНИЕ

Аннотация	5
1 Роли управления.....	10
2 Режимы функционирования программы	13
3 Запуск и завершение программы	14
4 Лицензирование программы	17
4.1 Лицензионные ограничения	17
4.2 Первичное лицензирование	18
4.3 Продление срока действия лицензии	20
5 Начало работы с программой	22
5.1 Инициализация Центра сертификации с генерацией ключа	22
5.1.1 Инициализация корневого Центра сертификации с генерацией ключа	22
5.1.2 Инициализация подчиненного Центра сертификации с генерацией ключа.....	27
5.2 Инициализация Центра сертификации с импортом ключа.....	32
6 Доступ к программе	39
6.1 Аутентификация с использованием сертификата, перенесённого на жесткий диск.....	39
6.2 Аутентификация с использованием сертификата на ключевом носителе	42
6.2.1 Настройка СВТ для двухфакторной аутентификации администратора по сертификату на ключевом носителе	42
6.2.1.1 Установка Единого Клиента JaCarta	42
6.2.1.2 Настройка веб-браузера Firefox	42
6.2.1.3 Настройка веб-браузера Chromium для РЕД ОС, SberLinux OS Server и Альт Сервер	43
6.2.1.4 Настройка веб-браузера Chromium для Astra Linux Special Edition.....	43
6.2.2 Двухфакторная аутентификация администратора по сертификату на ключевом носителе.....	44
7 Безопасность соединения	45
7.1 Настройка доверенного соединения	45
8 Технологические составляющие программы.....	47
8.1 Назначение технологических составляющих	47
8.2 Установка и настройка технологических составляющих	47
8.3 Удаление технологических составляющих.....	48
8.4 Восстановление доступа к программе в случае некорректного удаления технологических составляющих и/или блокировки доступа	48
9 Функции управления программы	49
9.1 Верхняя панель	49
9.2 Боковая панель.....	50
9.3 Раздел «Центр сертификации»	52
9.3.1 Вкладка «Свои сертификаты»	53
9.3.1.1 Карточка сертификата центра сертификации	55
9.3.1.2 Создание корневого центра сертификации с генерацией ключа	58
9.3.1.3 Создание подчиненного центра сертификации с генерацией ключа	65
9.3.1.4 Создание центра сертификации с импортом внешнего ключа.....	65
9.3.1.5 Скачивание запроса на сертификат для центра сертификации в состоянии «Запрос»	65
9.3.1.6 Импорт сертификата подчиненного центра сертификации	65
9.3.1.7 Удаление центра сертификации	68
9.3.1.8 Экспорт закрытого ключа центра сертификации.....	69
9.3.1.9 Импорт закрытого ключа центра сертификации.....	71
9.3.2 Вкладка «Сертификаты Подчиненных центров».....	73
9.3.2.1 Карточка сертификата подчинённого центра сертификации	74
9.3.2.2 Подписание запроса в Корневом Центре сертификации	75
9.4 Раздел «Сертификаты».....	77

9.4.1	Выпуск сертификата	78
9.4.2	Поиск сертификатов	78
9.4.3	Сортировка сертификатов.....	79
9.4.4	Фильтрация сертификатов.....	79
9.4.4.1	Применение фильтров	79
9.4.4.2	Сброс применённых фильтров	80
9.4.5	Скачивание сертификатов	80
9.4.6	Статус сертификатов.....	81
9.4.7	Карточка сертификата	83
9.4.8	Экспорт списка выпущенных сертификатов.....	85
9.4.9	Массовые операции с сертификатами.....	86
9.5	Настройка уведомлений об истечении срока действия сертификата	88
9.5.1	Настройка параметров конфигурационного файла config.sh	88
9.5.2	Настройка шаблонов уведомлений об истечении срока действия сертификата.....	89
9.5.3	Настройка параметров почтового ящика пользователя	90
9.5.3.1	Настройка почтовой программы Яндекс.Почта	91
9.5.3.2	Настройка почтовой программы MS Exchange.....	92
9.6	Раздел «Учётные записи».....	93
9.6.1	Создание учётной записи пользователя локального ресурса	94
9.6.2	Создание учетной записи для подключенного субъекта	95
9.6.3	Изменение статуса учётной записи.....	95
9.6.4	Редактирование учётной записи.....	96
9.6.5	Назначение прав оператору	96
9.6.6	Удаление учётной записи.....	96
9.6.7	Выпуск сертификата для учетной записи	97
9.7	Раздел «Правила доступа»	97
9.7.1	Создание правила доступа	98
9.7.2	Редактирование правила доступа	102
9.7.3	Удаление правила доступа	104
9.8	Раздел «Субъекты».....	105
9.8.1	Просмотр субъектов ресурсных систем	106
9.8.2	Поиск субъектов	107
9.8.3	Сортировка субъектов.....	107
9.8.4	Карточка субъекта	107
9.8.4.1	Редактирование атрибутов субъекта	112
9.8.5	Субъекты локальной ресурсной системы.....	113
9.8.5.1	Создание нового субъекта локальной ресурсной системы	114
9.8.6	Субъекты внешнего ресурса.....	115
9.8.7	Создание сертификата для субъекта ресурсной системы.....	116
9.8.8	Создание учётной записи для субъекта.....	117
9.9	Раздел «Ресурсные системы».....	118
9.9.1	Регистрация точки подключения.....	119
9.9.2	Карточка ресурсной системы	124
9.9.3	Синхронизация ресурсных систем	125
9.9.3.1	Виды синхронизации ресурсных систем.....	125
9.9.3.2	Режимы синхронизации ресурсных систем	126
9.9.3.3	Полная синхронизация ресурсной системы в автоматизированном режиме	126
9.9.3.4	Частичная синхронизация точки подключения в автоматизированном режиме	126
9.9.4	Редактирование параметров точки подключения	127
9.9.5	Удаление зарегистрированной ресурсной системой.....	128

9.9.6 Удаление точки подключения к ресурсной системе	129
9.10 Раздел «Центры валидации».....	130
9.10.1 Настройка периодичности автоматического обновления CRL.....	130
9.10.2 Автоматизированная публикация списка отозванных сертификатов CRL	133
9.10.3 Экспорт актуального списка отозванных сертификатов CRL	133
9.10.4 Управление центрами валидации	134
9.10.5 Управление точками распространения.....	137
9.10.5.1 Создание пользовательской точки распространения.....	138
9.10.5.2 Редактирование пользовательской точки распространения.....	141
9.10.5.3 Редактирование автоматической точки распространения.....	142
9.10.5.4 Удаление пользовательской точки распространения	143
9.10.5.5 Создание кластера точек распространения	144
9.10.5.6 Просмотр состава кластера точек распространения	146
9.10.5.7 Редактирование кластера точек распространения	146
9.10.5.8 Удаление кластера точек распространения	148
9.10.6 Управление службами OCSP.....	148
9.10.6.1 Создание пользовательской службы OCSP	149
9.10.6.2 Редактирование пользовательской службы OCSP	150
9.10.6.3 Редактирование автоматической службы OCSP	151
9.10.6.4 Удаление пользовательской службы OCSP	151
9.10.6.5 Создание кластера служб OCSP.....	152
9.10.6.6 Просмотр состава кластера служб OCSP	154
9.10.6.7 Редактирование кластера служб OCSP.....	154
9.10.6.8 Удаление кластера служб OCSP.....	156
9.10.7 Получение файлов CRL, Delta CRL и AIA	157
9.10.7.1 Получение файлов посредством запуска скрипта из состава программы	157
9.10.7.2 Получение файлов посредством использования методов REST API	157
9.10.8 Параметры точек распространения в сертификате	159
9.11 Журнал событий	159
9.11.1 О журнале событий	159
9.11.2 Просмотр записей журнала событий	174
9.11.3 Просмотр карточки события.....	178
9.11.4 Экспорт записей журнала событий	179
9.11.5 Передача информации о событиях в сторонние системы по протоколу Syslog.....	179
9.12 Управление шаблонами сертификатов.....	182
9.12.1 Общие сведения о шаблонах сертификатов.....	182
9.12.2 Просмотр информации о шаблонах сертификатов.....	183
9.12.3 Просмотр карточки шаблона сертификата.....	185
9.12.4 Создание пользовательского шаблона	189
9.12.5 Удаление шаблонов сертификатов	198
9.12.6 Импорт шаблонов MS CS.....	201
9.13 Смена сертификата веб-сервера.....	202
9.14 Управление разрешёнными издателями.....	204
10 Поиск и устранение неисправностей	205
Приложение 1. Создание сертификата для субъекта	208
1.1 Способы создания сертификатов.....	208
1.2 Параметры криптографии сертификатов учётных записей пользователей и Центров сертификации	209
1.3 Публикация сертификата в ресурсную систему.....	209
1.4 Создание сертификата с закрытым ключом PKCS#12	210
1.5 Создание сертификата субъекта по запросу	214

1.5.1 Создание сертификата субъекта по запросу в разделе «Сертификаты»	214
1.5.2 Создание сертификата субъекта по запросу в разделе «Субъекты»	223
1.6 Создание сертификата субъекта на ключевом носителе	227
Приложение 2. Описание полей предустановленных шаблонов сертификатов	232
Приложение 3. Правила валидации значений полей по умолчанию предустановленных шаблонов сертификатов.....	243
Приложение 4. Описание предустановленных идентификаторов расширенного использования ключа.....	245
Приложение 5. Формат и правила записи значений в поля сертификата на бумажном носителе.....	247
5.1 Формат сертификата на бумажном носителе для физического лица.....	247
5.2 Формат сертификата на бумажном носителе для юридического лица.....	248
5.3 Правила записи значений в поля сертификата на бумажном носителе для физического лица	249
5.4 Правила записи значений в поля сертификата на бумажном носителе для юридического лица	251
5.5 Пример сертификата на бумажном носителе для физического лица	253
5.6 Пример сертификата на бумажном носителе для юридического лица	254
Обозначения и сокращения	255
Термины и определения	256

1 РОЛИ УПРАВЛЕНИЯ

В Центре сертификации Aladdin eCA определены следующие роли пользователей:

- Оператор

Пользователь с ролью «Оператор» имеет доступ к Центру сертификации Aladdin eCA 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 Центр сертификации Aladdin eCA, а также доступ через веб-интерфейс или программный интерфейс API к функциональным задачам и к функциям управления учетными 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 конфигурационной информации о уведомлениях об истечении срока действия сертификата	-	+
Внесение изменений в конфигурационную информацию о 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	-	+

Тип действия, осуществляемого пользователем, над объектом программы	Возможные роли пользователей	
	Оператор	Администратор
Подписание запроса на сертификат подчинённого центра сертификации	-	+
Импортирование сертификата центра сертификации (активация центра сертификации)	-	+
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	-	+

Тип действия, осуществляемого пользователем, над объектом программы	Возможные роли пользователей	
	Оператор	Администратор
Редактирование созданных шаблонов сертификатов	-	+
Удаление созданных шаблонов сертификатов	-	+
Просмотр идентификаторов расширенного использования ключа	-	+
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 Центра сертификации Aladdin eCA 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 Центра сертификации Aladdin eCA предусматривает автономный режим (Stand alone operation) или сетевой режим работы.

Сетевой режим работы Центра сертификации Aladdin eCA обеспечивает возможность кластеризации с целью отказоустойчивости.

3 ЗАПУСК И ЗАВЕРШЕНИЕ ПРОГРАММЫ

Центр сертификации Aladdin eCA запускается автоматически:

- В случае выполнения успешной установки программы.
- В случае выполнения успешного обновления программы.
- После запуска ОС.

Для проверки состояния Центра сертификации Aladdin eCA в терминале выполните команду с правами суперпользователя:

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

Возможные варианты ответа:

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

Для проверки автозагрузки программы выполните следующую команду с правами суперпользователя:

```
sudo systemctl is-enabled aeca-ca.service
```

Для добавления программы в автозагрузку выполните следующую команду с правами суперпользователя:

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

Для запуска программы выполните следующую команду с правами суперпользователя:

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

Для перезапуска программы выполните следующую команду с правами суперпользователя:

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

При запуске Центра сертификации Aladdin eCA выполняются следующие проверки:

- Проверка возможности подключения к базе данных. Если не удаётся подключиться к базе данных, то программа не запускается.
- Проверка соответствия номера своей сборки и значения номера сборки, указанной в базе данных:
 - Если в базе данных отсутствует номер сборки, то программа не запускается.
 - Если номер сборки не равен номеру сборки программы, то программа завершает запуск с ошибкой «Текущая версия схемы базы данных не позволяет выполнить запуск службы. Текущая версия схемы базы данных: X.X.X.X. Необходимая версия схемы базы данных: Y.Y.Y.Y.», где «X.X.X.X» – номер сборки указанный в базе данных, а «Y.Y.Y.Y» – номер сборки запускаемой программы.
- Проверка целостности контейнеров закрытого ключа всех Центров сертификации программы. Результат проверки целостности для каждого контейнера закрытого ключа записывается в журнал событий:
 - Событие с кодом CAENV076 – при успешной проверке целостности.
 - Событие с кодом CAENV077 – при неуспешной проверке целостности.

Модули Центра сертификации Aladdin eCA запускаются поочерёдно в порядке, приведенном в таблице 2.

Таблица 2 – Модули программы

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

Для завершения работы Центра сертификации Aladdin eCA выполните следующую команду с правами суперпользователя:

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

Центр сертификации Aladdin eCA при остановке отключает от веб-сервера свою конфигурацию. В результате отключения от веб-сервера конфигурации закрываются порты ¹, используемые для доступа к программе (определяются параметрами «http_port» и «http_port» конфигурационного файла /opt/aecaCa/scripts/config.sh), если данные порты не используются иными программами.

¹ Порты будут закрыты только в том случае, если они были открыты Центром сертификации Aladdin eCA.

4 ЛИЦЕНЗИРОВАНИЕ ПРОГРАММЫ

4.1 Лицензионные ограничения

Лицензию необходимо импортировать для каждого Центра сертификации Aladdin eCA.

Лицензия на право использования Центра сертификации Aladdin eCA 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 eVA, которые могут быть подключены.
- Максимальное количество подключаемых центров регистрации – лицензия ограничивает максимальное количество Центров регистрации Aladdin eRA, 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.

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».

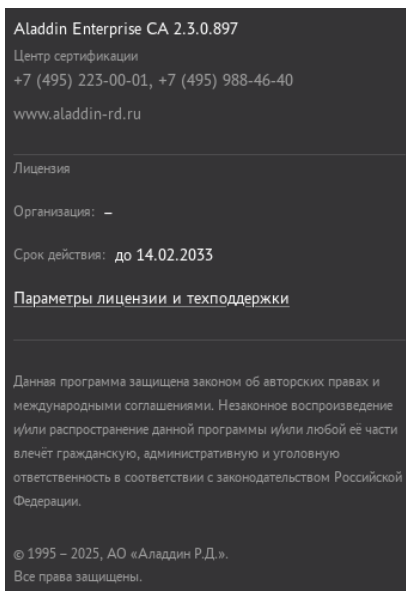


Рисунок 1 – Окно «О программе»

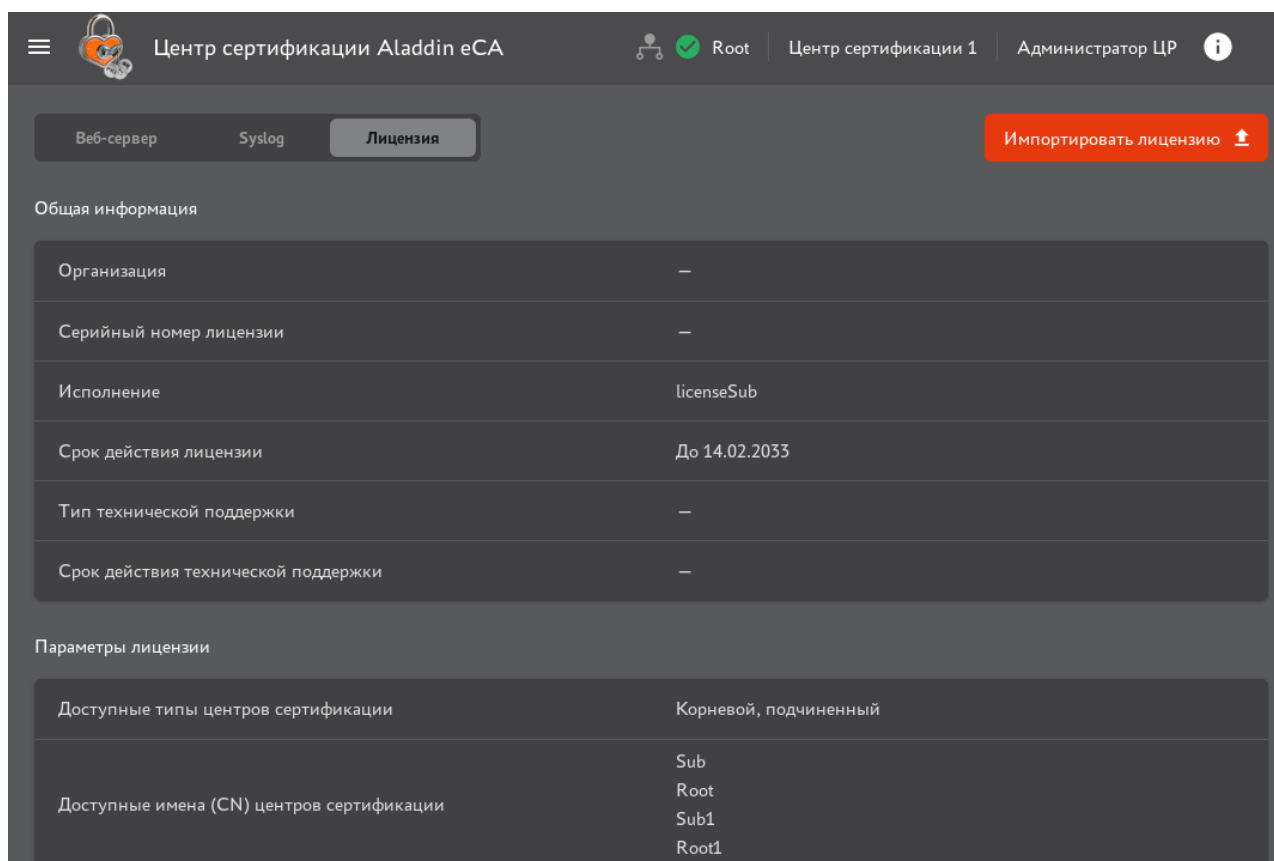


Рисунок 2 – Просмотр параметров лицензии

4.2 Первичное лицензирование

Порядок установки лицензии при первичной инициализации:

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

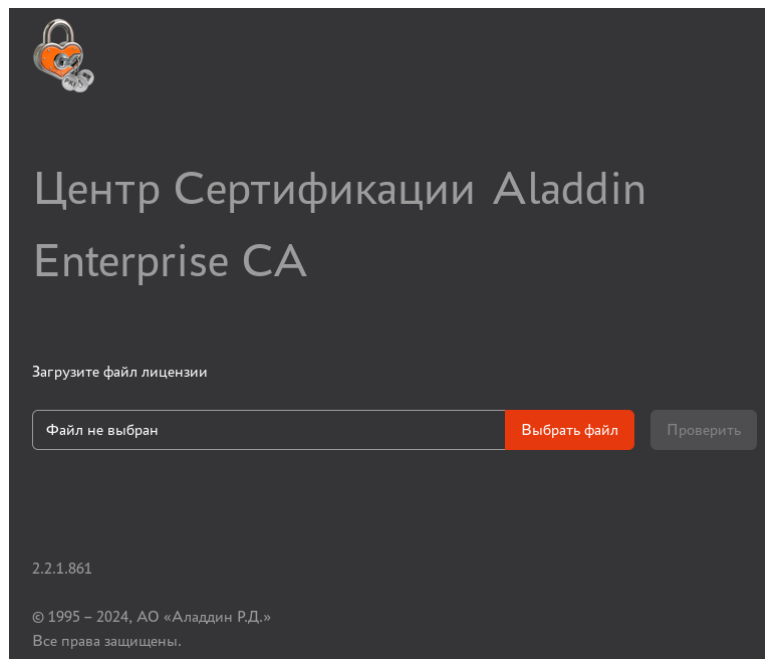


Рисунок 3 – Выбор файла с лицензией

- 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».

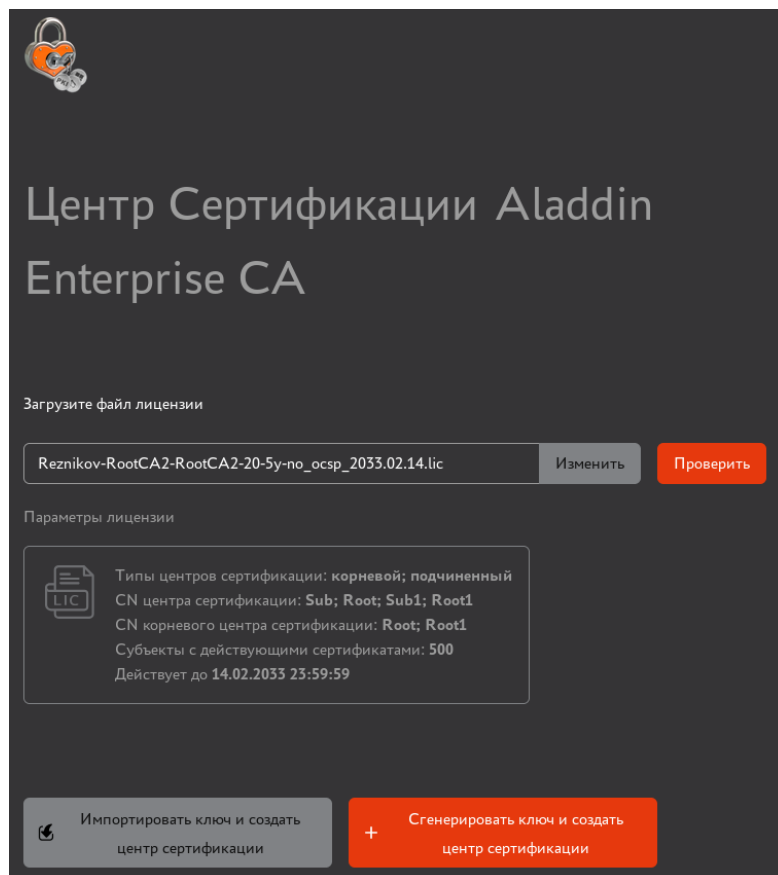


Рисунок 4 – Проверка лицензии выполнена успешно

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»¹.
- Перечень имен 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 5.1).
- Нажмите кнопку **<Импортировать ключ и создать центр сертификации>** для перехода к инициализации Центра сертификации с импортом ключа из контейнера PKCS#12 (см. раздел 5.2).

4.3 Продление срока действия лицензии

После истечения срока действия установленной лицензии доступ к функционалу Центра сертификации Aladdin eCA 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.

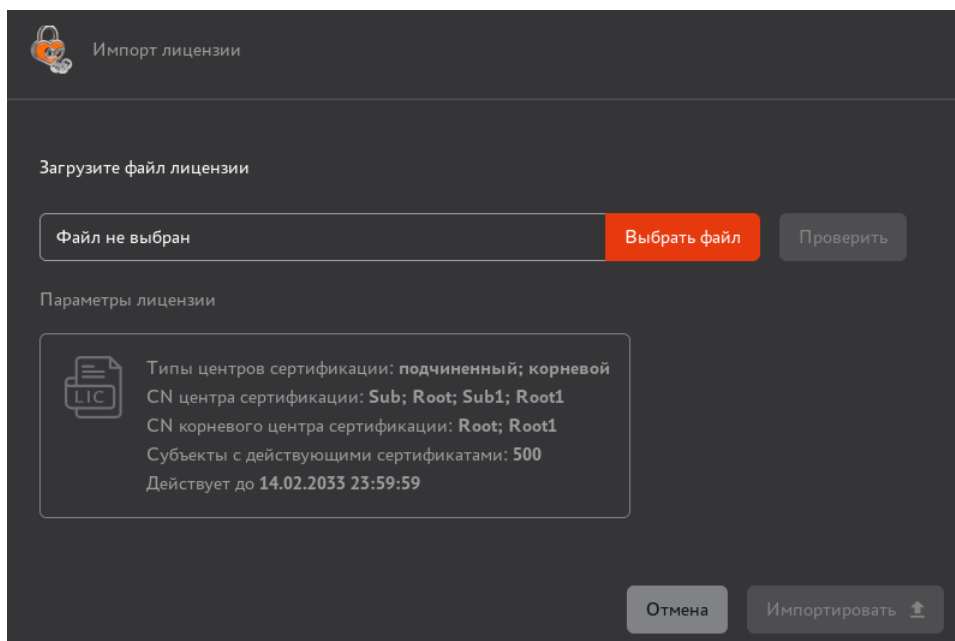


Рисунок 5 – Окно импорта лицензии

- 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:

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

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

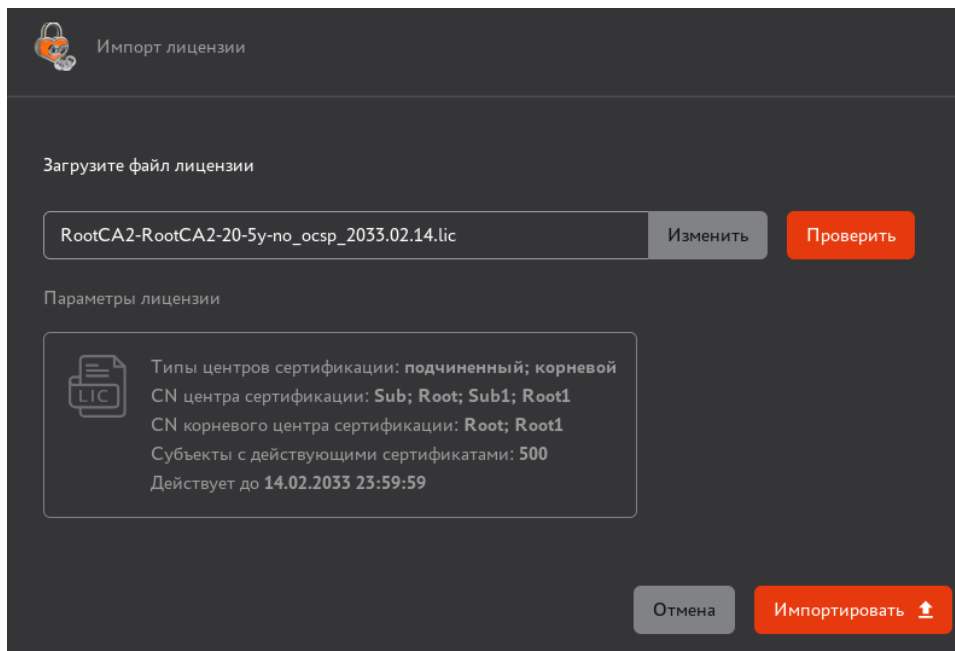


Рисунок 6 – Окно импорта лицензии после успешной проверки на валидность

- 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 объеме.
- При попытке импорта лицензии, в которой в перечень имен Центров сертификации не входят имена действующих ¹ Центров сертификации (учитывается комбинация имени Центра сертификации и корневого Центра сертификации) ², генерируется сообщение об ошибке «В импортируемой лицензии отсутствует имя действующего Центра сертификации».

¹ Имеющих статус «Активирован» или «Не активирован».

² Импортируемая лицензия позволяет повторно создать любой из действующих ЦС.

5 НАЧАЛО РАБОТЫ С ПРОГРАММОЙ

5.1 Инициализация Центра сертификации с генерацией ключа

5.1.1 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.

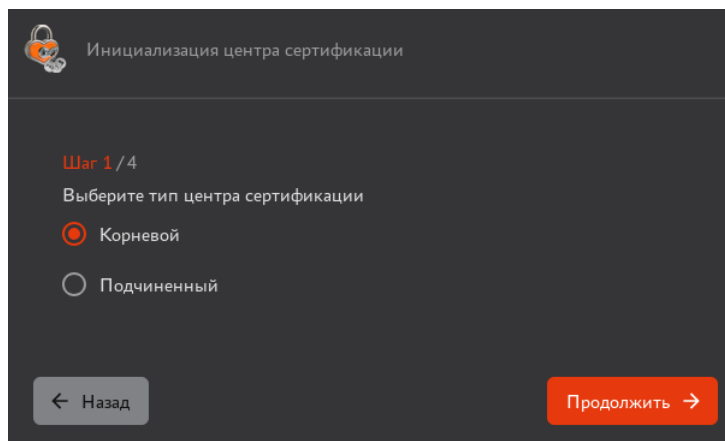


Рисунок 7 – Выбор типа создаваемого Центра сертификации

- 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 имен, 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 3.

Таблица 3 – 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

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

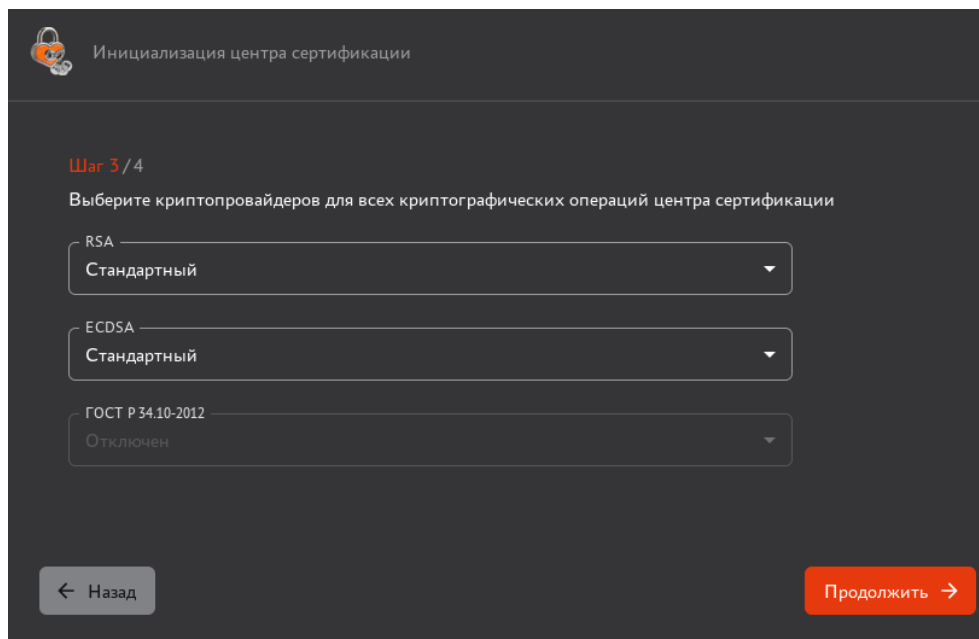


Рисунок 9 – Выбор криптопровайдеров

- «RSA» – список выбора криптопровайдера для алгоритма RSA:
 - Стандартный (по умолчанию).
 - КriptoПро CSP ¹ (доступен только при наличии активного и подключенного криптопровайдера СКЗИ «КriptoПро 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:
 - КriptoПро CSP (доступен только при наличии активного и подключенного криптопровайдера СКЗИ «КriptoПро 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» ², по которому будет выпущен сертификат.
 - В списке «Алгоритм ключа» (состав алгоритмов зависит от выбранных провайдеров) выберите алгоритм:
 - RSA;

¹ Подробная информация по настройке взаимодействия Центра сертификации Aladdin eCA с СКЗИ «КriptoПро 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».

² Информация про шаблон «Root CA» приведена в Приложении 2 «Описание полей предустановленных шаблонов сертификатов». Приложение 2. Описание полей предустановленных шаблонов сертификатов

- ECDSA;
- ГОСТ Р 34.10–2012.

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 установленное неизменяемое значение «Локальное хранилище Aladdin eCA».
- С помощью чек-бокса «Экспортируемый закрытый ключ» определите возможность экспорта ключа из хранилища.

В случае неудачной попытки создания Центра сертификации выводится одно из сообщений об ошибке, приведенных 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.																						
Ошибка. Ошибка атрибута attributeName: Значение не соответствует регулярному выражению: «regex»	<p>Ошибка валидации введенного значения атрибута различающегося имени¹. Возможные значения переменной «attributeName» и соответствующие им значения переменной «regex» представлены в таблице ниже:</p> <table border="1"> <thead> <tr> <th>attributeName</th><th>regex</th></tr> </thead> <tbody> <tr> <td>C</td><td>^[A-Za-z]{2}\$</td></tr> <tr> <td>DN</td><td>^[A-Za-z0-9''()+,\.V:=?]+\$</td></tr> <tr> <td>EMAILADDRESS</td><td>^[A-Za-zA-Яа-я0-9_ -]+@[A-Za-zA-Яа-я0-9_ -]+\$</td></tr> <tr> <td>SERIALNUMBER</td><td>^[A-Za-z0-9''()+,\.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>^(?:31\.(0[13578] 1[02]) (?:30 29)\.(0[13-9] 1[0-2]) (?:0[1-9] 1[0-9])\.(0[1-9] 1[0-2]))\.\d{4}29\.(02\.(?:\d{2}(?:0[48] [2468][048] 13579)[26]) (?:02468 [048][13579][26])0 0))\$</td></tr> </tbody> </table>	attributeName	regex	C	^[A-Za-z]{2}\$	DN	^[A-Za-z0-9''()+,\.V:=?]+\$	EMAILADDRESS	^[A-Za-zA-Яа-я0-9_ -]+@[A-Za-zA-Яа-я0-9_ -]+\$	SERIALNUMBER	^[A-Za-z0-9''()+,\.V:=?]+\$	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])\.(0[1-9] 1[0-2]))\.\d{4}29\.(02\.(?:\d{2}(?:0[48] [2468][048] 13579)[26]) (?:02468 [048][13579][26])0 0))\$
attributeName	regex																						
C	^[A-Za-z]{2}\$																						
DN	^[A-Za-z0-9''()+,\.V:=?]+\$																						
EMAILADDRESS	^[A-Za-zA-Яа-я0-9_ -]+@[A-Za-zA-Яа-я0-9_ -]+\$																						
SERIALNUMBER	^[A-Za-z0-9''()+,\.V:=?]+\$																						
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])\.(0[1-9] 1[0-2]))\.\d{4}29\.(02\.(?:\d{2}(?:0[48] [2468][048] 13579)[26]) (?:02468 [048][13579][26])0 0))\$																						
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:

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

¹ Правила валидации значений атрибутов представлены в Приложении 3 «Правила валидации значений полей по умолчанию предустановленных шаблонов сертификатов».

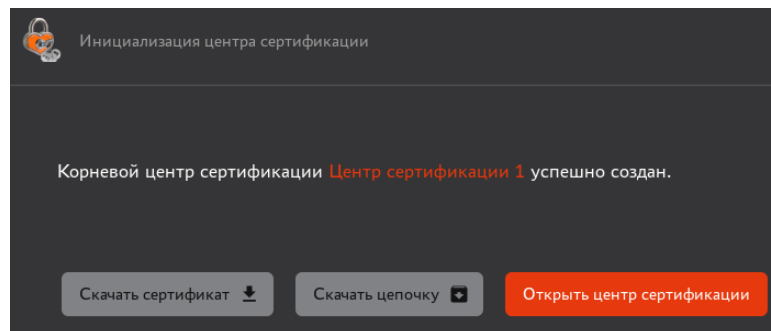


Рисунок 11 – Корневой Центр сертификации успешно создан

5.1.2 Инициализация подчиненного Центра сертификации с генерацией ключа

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

- На первом шаге мастера инициализации (см. Рисунок 7) выберите тип Центра сертификации «Подчиненный» 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 имен, 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 5.

Таблица 5 – 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

- На следующем шаге мастера инициализации (см. Рисунок 9) 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);

- КriptoПро CSP¹ (доступен только при наличии активного и подключенного криптопровайдера СКЗИ «КriptoПро 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:
 - КriptoПро CSP (доступен только при наличии активного и подключенного криптопровайдера СКЗИ «КriptoПро CSP»);
 - 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.

- На следующем шаге мастера инициализации выберите параметры криптографии (см. Рисунок 13) и нажмите кнопку <Создать ЦС>:
 - «Алгоритм ключа» (состав алгоритмов зависит от выбранных провайдеров):
 - RSA;
 - ECDSA;
 - ГОСТ Р 34.10–2012.
 - «Длина ключа» (по умолчанию выбирается наименьшая доступная длина ключа для выбранного алгоритма):
 - для RSA: 1024, 1536, 2048, 3072, 4096, 6144, 8192 (по умолчанию 3072);
 - для ECDSA: 256, 384, 521 (по умолчанию 256);
 - для ГОСТ Р 34.10–2012: 256, 512 (по умолчанию 256).
 - «Алгоритм хэш–суммы»:
 - для алгоритма ключа RSA или ECDSA: SHA1, SHA256, SHA384 (выбран по умолчанию), SHA512;
 - для алгоритма ключа ГОСТ Р 34.10–2012: ГОСТ Р 34.11–2012.
 - «Место хранения закрытого ключа»:
 - Доступные варианты выбора, если криптопровайдером выбранного алгоритма ключа является КriptoПро CSP:
 - Локальное хранилище Aladdin eCA (выбрано по умолчанию, требует заранее подготовленной на БДЧ криптопровайдера СКЗИ «КriptoПро CSP» гаммы);
 - КriptoПро CSP (HDIMAGE);
 - КriptoПро HSM (доступно только при наличии подключения криптопровайдера СКЗИ «КriptoПро CSP» к ПАКМ «КriptoПро HSM»).
 - Для других криптопровайдеров в данном поле указано неизменяемое значение «Локальное хранилище Aladdin eCA».

¹ Подробная информация по настройке взаимодействия Центра сертификации Aladdin eCA с СКЗИ «КriptoПро 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».

- 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.

Рисунок 13 – Указание срока действия Центра сертификации и параметров криптографии

- В случае неудачной попытки создания Центра сертификации будет отображено одно из сообщений об ошибке, приведенных в таблице 6.

Таблица 6 – 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»	<p>Ошибка валидации введенного значения атрибута различающегося имени¹. Возможные значения переменной «attributeName» и соответствующие им значения переменной «regex» представлены в таблице ниже:</p> <table> <tr> <th>attributeName</th><th>regex</th></tr> <tr> <td>C</td><td>^[A-Za-z]{2}\$</td></tr> <tr> <td>DN</td><td>^[A-Za-z0-9''()+,\.\/:=?]+\$</td></tr> <tr> <td>EMAILADDRESS</td><td>^[A-Za-zА-Яа-я0-9._-]+@[A-Za-zА-Яа-я0-9._-]+\$</td></tr> <tr> <td>SERIALNUMBER</td><td>^[A-Za-z0-9''()+,\.\/:=?]+\$</td></tr> <tr> <td>INN</td><td>^\d{12}\$</td></tr> <tr> <td>OGRN</td><td>^\d{13}\$</td></tr> <tr> <td>OGRNIP</td><td>^\d{15}\$</td></tr> <tr> <td>SNILS</td><td>^\d{11}\$</td></tr> <tr> <td>INNLE</td><td>^\d{10}\$</td></tr> <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\.(?:\d{2}(?:0[48] 2468)[048] 13579)[26]) (?:02468)[048]13579[26])0 0)\$</td></tr> </table>	attributeName	regex	C	^[A-Za-z]{2}\$	DN	^[A-Za-z0-9''()+,\.\/:=?]+\$	EMAILADDRESS	^[A-Za-zА-Яа-я0-9._-]+@[A-Za-zА-Яа-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\.(?:\d{2}(?:0[48] 2468)[048] 13579)[26]) (?:02468)[048]13579[26])0 0)\$
attributeName	regex																						
C	^[A-Za-z]{2}\$																						
DN	^[A-Za-z0-9''()+,\.\/:=?]+\$																						
EMAILADDRESS	^[A-Za-zА-Яа-я0-9._-]+@[A-Za-zА-Яа-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\.(?:\d{2}(?:0[48] 2468)[048] 13579)[26]) (?:02468)[048]13579[26])0 0)\$																						
Ошибка при создании Центра сертификации. Неизвестная ошибка	Внутренняя ошибка ПО																						

При успешном создании Подчиненного Центра сертификации и завершении инициализации Центра сертификации будет открыться соответствующее окно (см. Рисунок 14), 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 подчиненного ЦС.
- Заккрыть окно инициализации Подчиненного Центра сертификации.

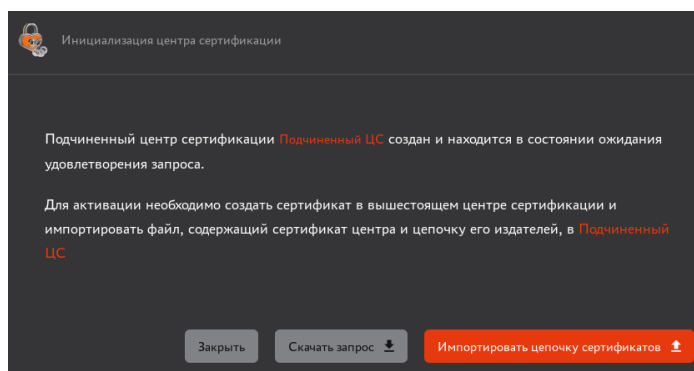


Рисунок 14 – Запрос на создание сертификата Подчиненного Центра сертификации создан

- Скачайте созданный запрос на сертификат Подчиненного Центра сертификации в формате **.csr**.
- На данном этапе Подчиненный Центр сертификации создан и отображается на вкладке «Свои сертификаты» и имеет статус «Запрос» (см. Рисунок 15).

¹ Правила валидации значений атрибутов представлены в Приложении 3 «Правила валидации значений полей по умолчанию предустановленных шаблонов сертификатов».

Для перевода Подчиненного Центра сертификации в состояние «Активирован» необходимо выполнить подписание запроса на Корневом Центре сертификации (см. раздел 9.3.2.2) и затем импортировать подписанный сертификат Подчиненного Центра сертификации и его цепочку сертификатов¹ (см. раздел 9.3.1.6).

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

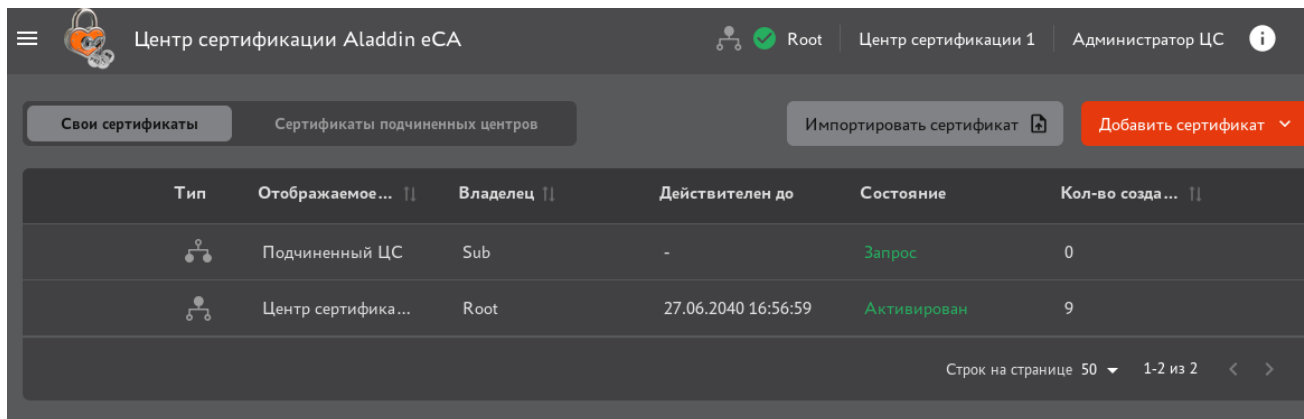


Рисунок 15 – Подчинённый Центр сертификации в состоянии «Запрос»

5.2 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 16) выберите файл контейнера ключей PKCS#12 и введите пароль от него.

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

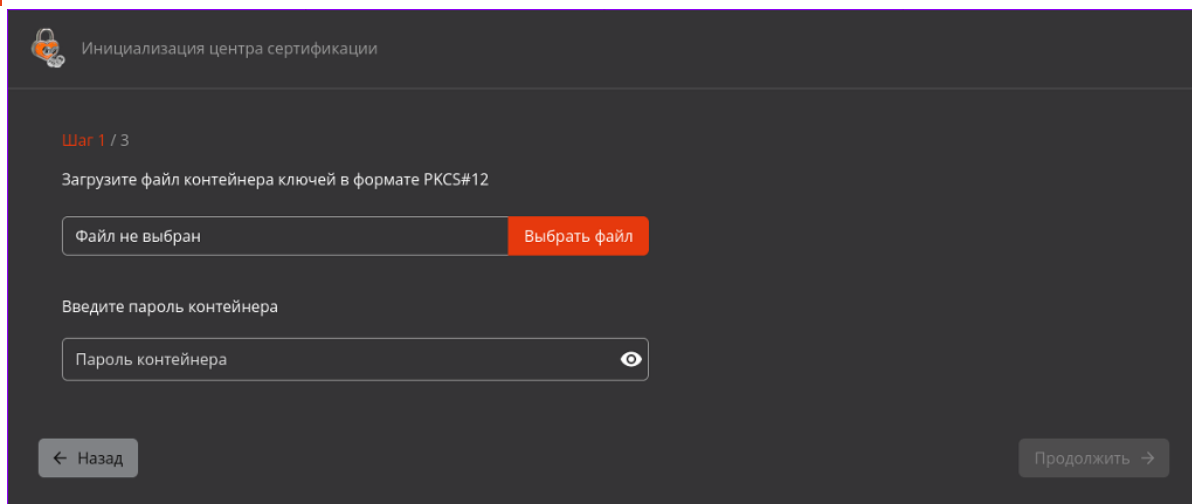


Рисунок 16 – Выбор контейнера ключей PKCS#12

- После выбора файла и ввода пароля необходимо нажать кнопку **<Проверить>**, которая появляется после их заполнения (см. Рисунок 17).

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

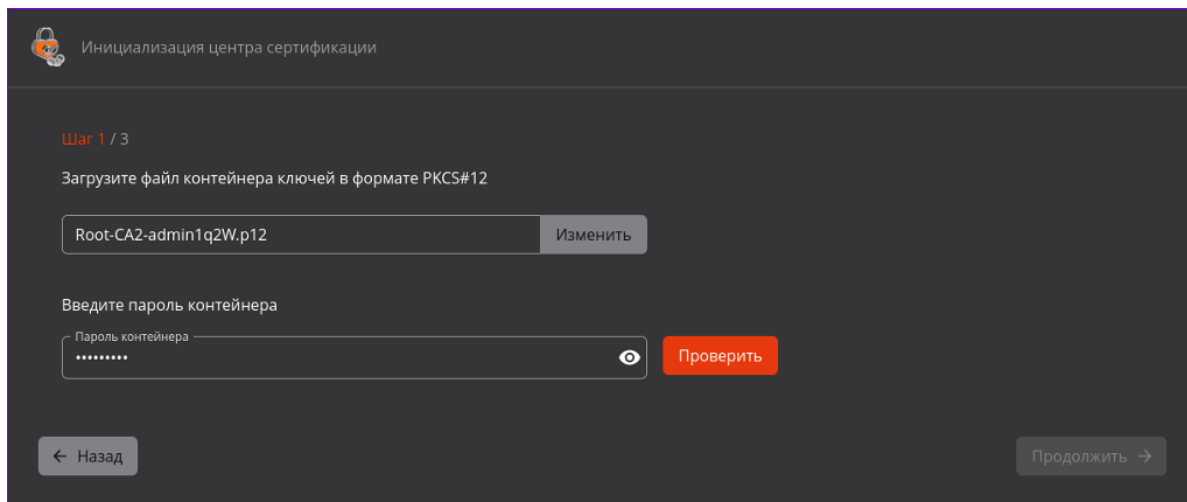


Рисунок 17 – Проверка сертификата

Список возможных ошибок, возникающих при проверке сертификата, приведен в таблице 7.

Таблица 7 – Возможные ошибки при проверке контейнера ключей PKCS#12

Ошибка	Причина
Формат файла	
Ошибка. Некорректный формат файла контейнера.	Формат файла контейнера не соответствует PKCS#12.
Ошибка. Неверный пароль контейнера.	Не удалось открыть контейнер с помощью указанного пароля.
Лицензионные ограничения	
Ошибка. Лицензионные ограничения не позволяют создать <Тип ЦС> ЦС.	Тип Центра сертификации из контейнера не входит в разрешенные 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.
Сертификат	
Ошибка. Срок действия сертификата истек.	Текущая дата превышает дату завершения срока действия сертификата, указанную в контейнере.
Ошибка. Срок действия сертификата <Имя> из цепочки истек.	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.
Параметры криптографии	
Ошибка. Неподдерживаемый алгоритм ключа: <Алгоритм> <Длина ключа>.	Неподдерживаемый алгоритм ключа или его длина.
Ошибка. Неподдерживаемый алгоритм хэш–суммы: <Алгоритм>.	Неподдерживаемый алгоритм хэш–суммы.
Прочее	
Ошибка. Неизвестная ошибка.	Внутренняя ошибка ПО.

После проверки данных контейнера PKCS#12 выводится следующая информация (см. Рисунок 18 и Рисунок 19) в информационном элементе «Сертификат» раздела «Параметры контейнера»:

- Наименование издателя.
- Наименование субъекта.

- Срок действия сертификата.
- Цепочка сертификатов.
- Алгоритм ключа.
- Длина ключа.

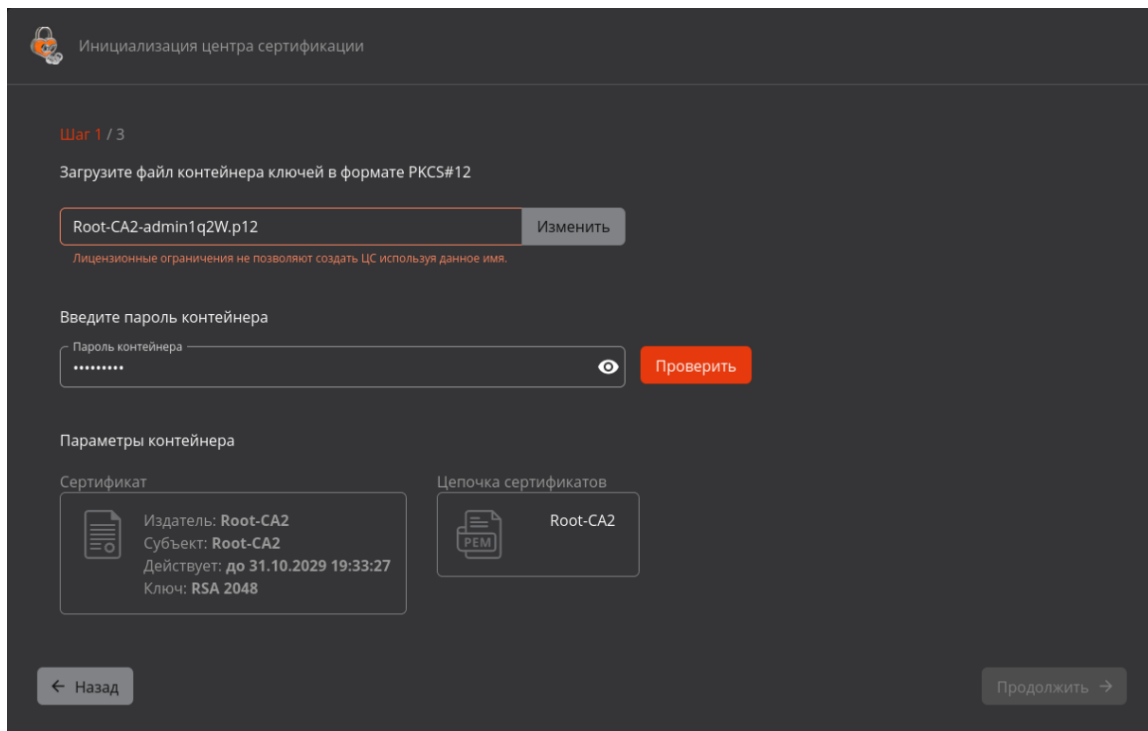


Рисунок 18 – Проверка сертификата выполнена с ошибкой

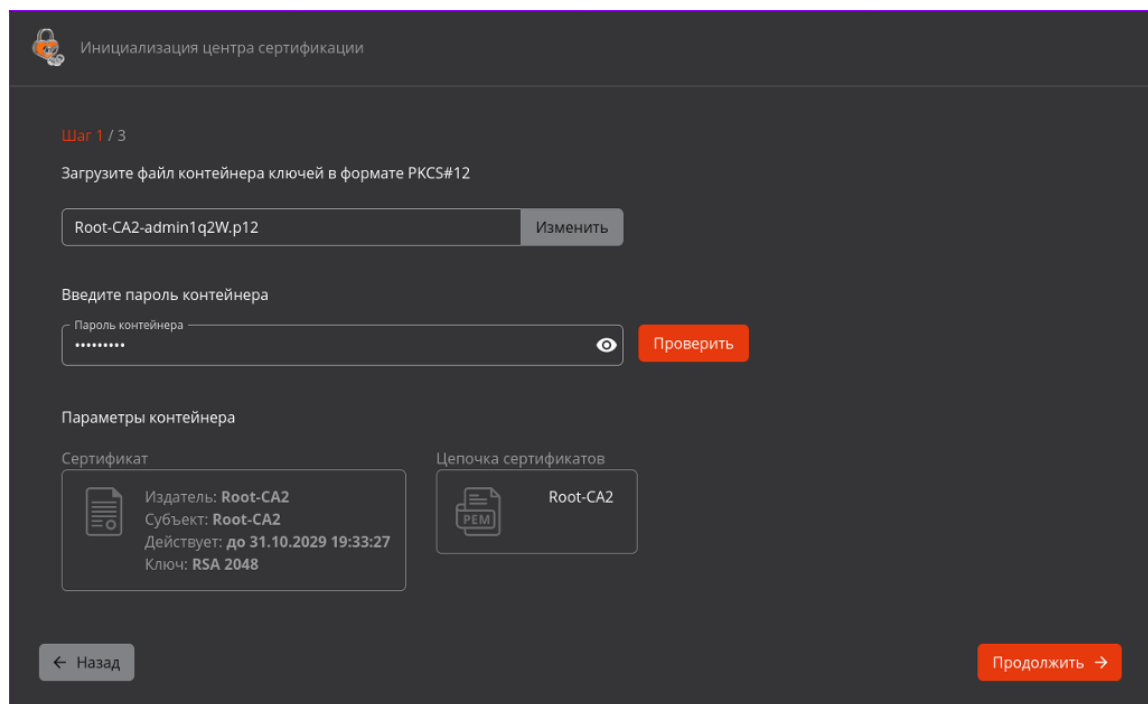


Рисунок 19 – Проверка сертификата выполнена успешно

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

Внимание! Тип Центра сертификации (Корневой или Подчиненный) 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 Центра сертификации Aladdin eCA. 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#12¹;
 - наличия активного криптопровайдера СКЗИ «КриптоПро CSP» на хосте Центра сертификации Aladdin eCA;
 - наличия подключения криптопровайдера СКЗИ «КриптоПро CSP» к ПАКМ «КриптоПро HSM».

Варианты мест хранения закрытого ключа представлены в таблице 8.

Таблица 8 – 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 Центра сертификации Aladdin eCA. КриптоПро HSM - при активном криптопровайдере СКЗИ «КриптоПро CSP» на хосте Центра сертификации Aladdin eCA 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 Центра сертификации Aladdin eCA. КриптоПро HSM - при активном криптопровайдере СКЗИ «КриптоПро CSP» на хосте Центра сертификации Aladdin eCA 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 Центра сертификации Aladdin eCA КриптоПро HSM - при активном криптопровайдере СКЗИ «КриптоПро CSP» на хосте Центра сертификации Aladdin eCA и подключении криптопровайдера СКЗИ «КриптоПро CSP» к ПАКМ «КриптоПро HSM».

¹ 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.

Инициализация центра сертификации

Шаг 2 / 3

Укажите отображаемое имя и место хранения закрытого ключа

Отображаемое имя
RootCA

Лимит 194 символов

Место хранения закрытого ключа центра сертификации

Место хранения
Локальное хранилище Aladdin eCA

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

Для данного ключа с криптопровайдером
Стандартный доступны следующие места
хранения: Локальное хранилище Aladdin eCA

← Назад

Продолжить →

Рисунок 20 – Окно инициализации Центра сертификации. Шаг 2/3

- Для перехода к следующему шагу нажмите кнопку **<Продолжить>**.
- На шаге 3/3 выберите криптопровайдеры для всех криптографических операций центра сертификации. Для выбора криптопровайдеров заполните следующие поля (см. Рисунок 21 и Рисунок 22):
 - «RSA» – поле выбора криптопровайдера для алгоритма RSA, допустимые варианты выбора:
 - Стандартный (по умолчанию);
 - КриптоПро CSP¹ (доступен только при наличии активного и подключенного 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 подключенного криптопровайдера СКЗИ «КриптоПро CSP»);
 - Отключен (по умолчанию).
 - поле «Алгоритм хэш–суммы»:
 - Для корневого Центра сертификации значение берется из контейнера PKCS#12 (см. Рисунок 21). При этом поле заблокировано. Поддерживаются следующие алгоритмы хэш–суммы ключа: SHA1, SHA256, SHA384, SHA512, SHA3–256, SHA3–384, SHA3–512, RSASSA–PSS.
 - Для подчиненного Центра сертификации необходимо возможно выбрать следующие значения (см. Рисунок 22):
 - для алгоритма ключа RSA или ECDSA: SHA1, SHA256, SHA384 (выбран по умолчанию), SHA512;

¹ Подробная информация по настройке взаимодействия Центра сертификации Aladdin eCA 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».

- для алгоритма ключа ГОСТ Р 34.10–2012: ГОСТ Р 34.11–2012.

Рисунок 21 – Выбор криптопровайдеров и параметров криптографии для Корневого Центра сертификации

Рисунок 22 – Выбор криптопровайдеров и параметров криптографии для Подчиненного 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 23 и Рисунок 24). 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».

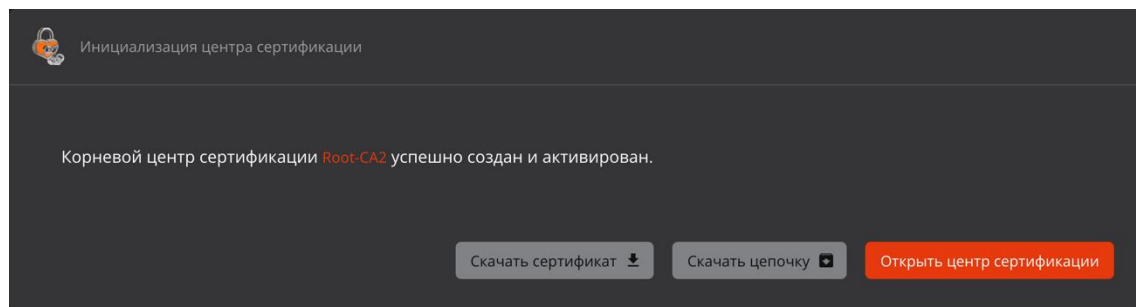


Рисунок 23 – Окно завершения инициализации корневого Центра сертификации

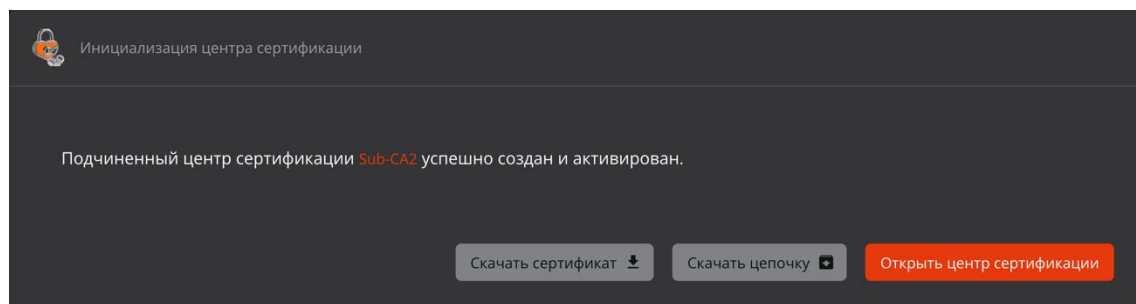


Рисунок 24 – Окно завершения инициализации подчиненного Центра сертификации

6 ДОСТУП К ПРОГРАММЕ

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

6.1 Аутентификация с использованием сертификата, перенесённого на жесткий диск

Полученный администратором контейнер сертификата доступа для аутентификации на веб–сервере Центра сертификации Aladdin eCA 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 25). Нажмите кнопку **<Просмотр сертификатов>**.

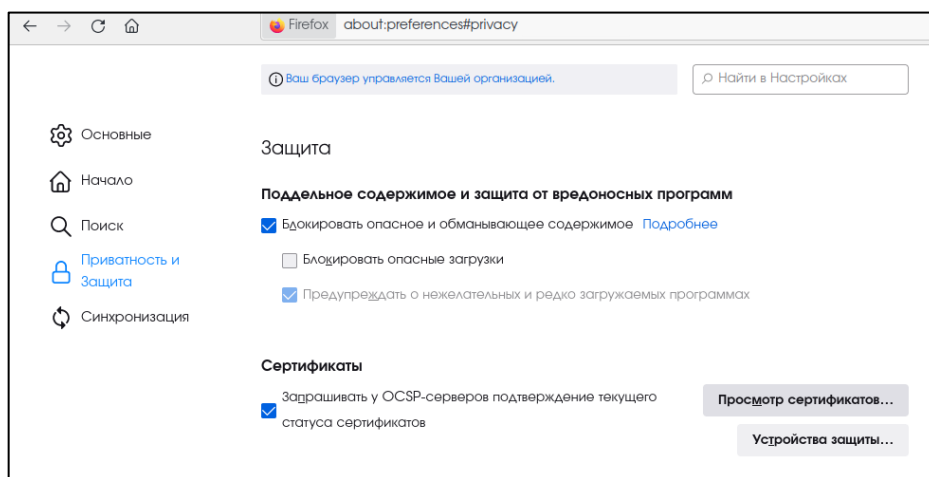


Рисунок 25 – Окно настроек веб-браузера

- Выберите вкладку «Ваши сертификаты», в открывшейся вкладке нажмите кнопку **<Импортировать>** (см. Рисунок 26).

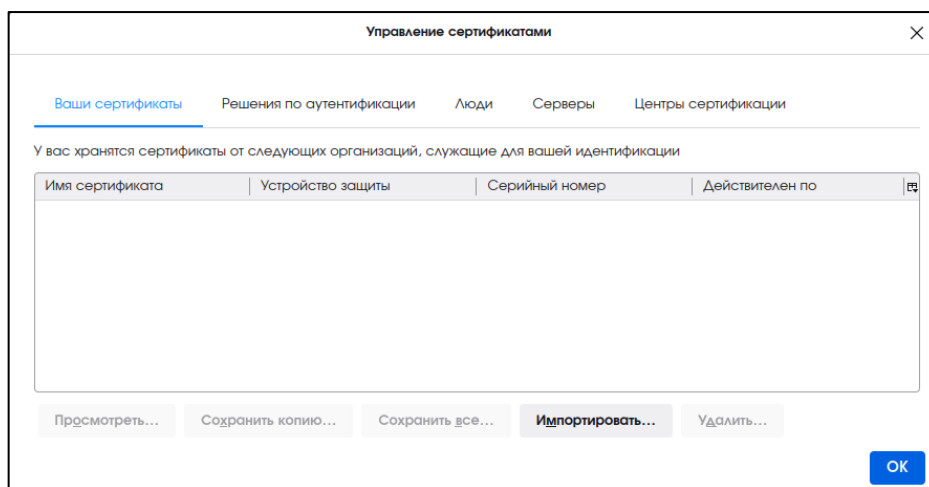


Рисунок 26 – Окно управления сертификатами

- Выберите контейнер .p12, содержащий закрытый ключ и сертификат доступа, перенесённый на жесткий диск, выпущенный для учётной записи пользователя (см. Рисунок 27).

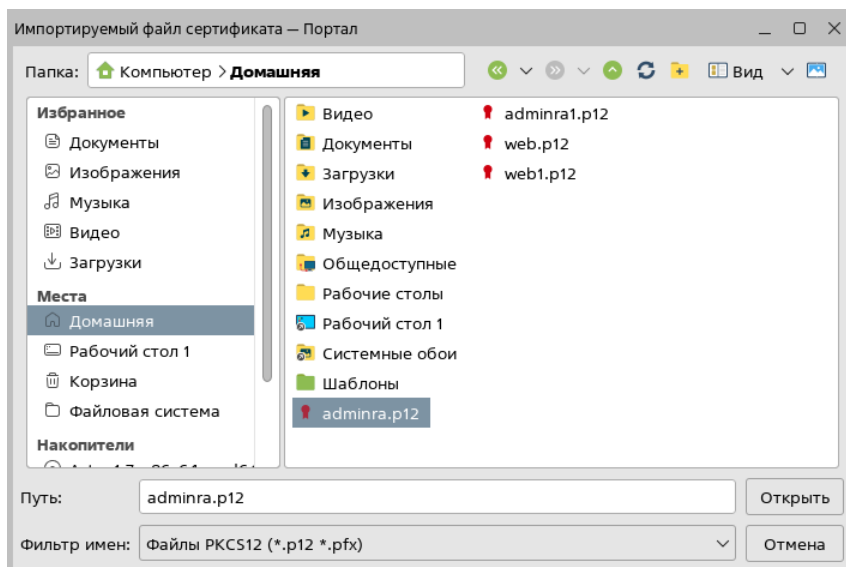


Рисунок 27 – Окно выбора импортируемого файла сертификата

- В открывшемся окне введите пароль от контейнера .p12 и нажмите кнопку **<Ок>** (см. Рисунок 28). Пароль от контейнера является атрибутом безопасности и должен быть передан администратором с контейнером закрытого ключа и сертификата.

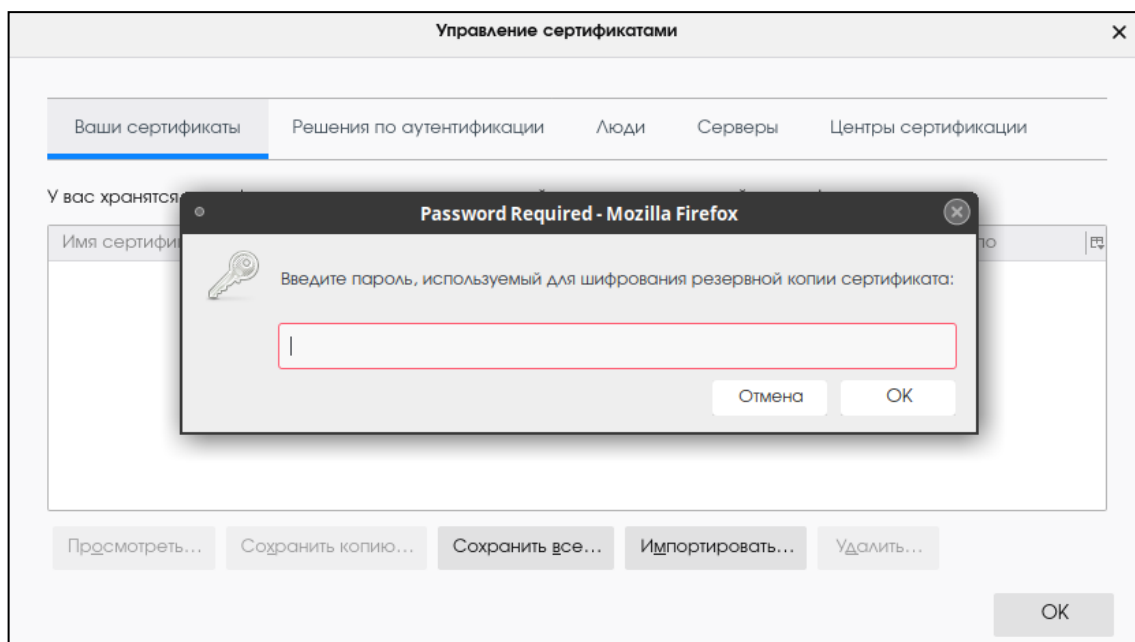


Рисунок 28 – Окно ввода пароля контейнера

- В адресной строке веб-браузера введите IP-адрес или полное доменное имя сервера, выдавшего импортированный сертификат доступа, на котором произведена установка Центра сертификации Aladdin eCA (например, <https://172.22.5.21>).
- В открывшемся окне выберите сертификат для аутентификации на веб-сервере Центра сертификации Aladdin eCA (см. Рисунок 29). Нажмите кнопку **<ОК>**.

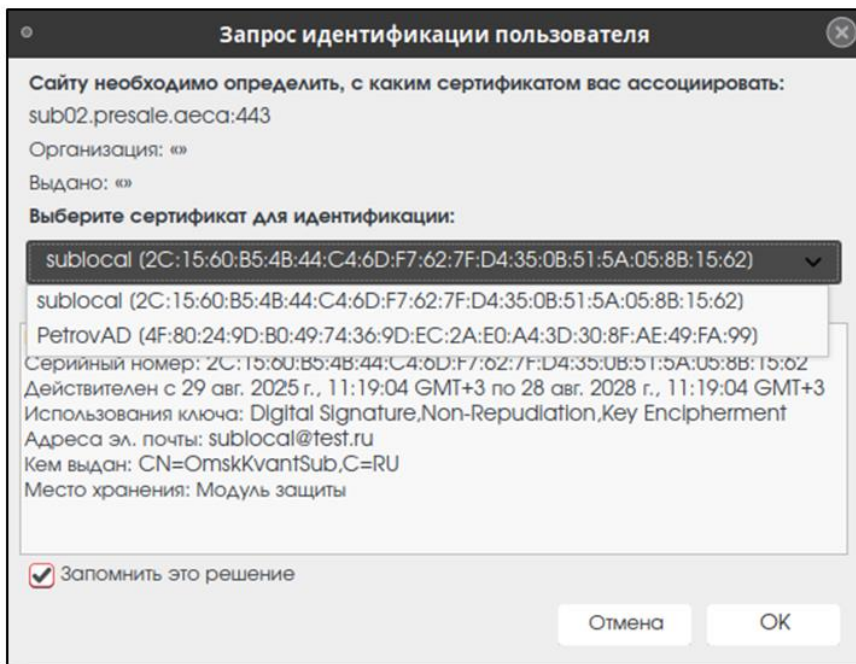


Рисунок 29 – Выбор сертификата для аутентификации

- Далее откроется страница с предупреждением системы безопасности (см. Рисунок 30). Нажмите кнопку **<Дополнительно>** и далее кнопку **<Принять риск и продолжить>**.

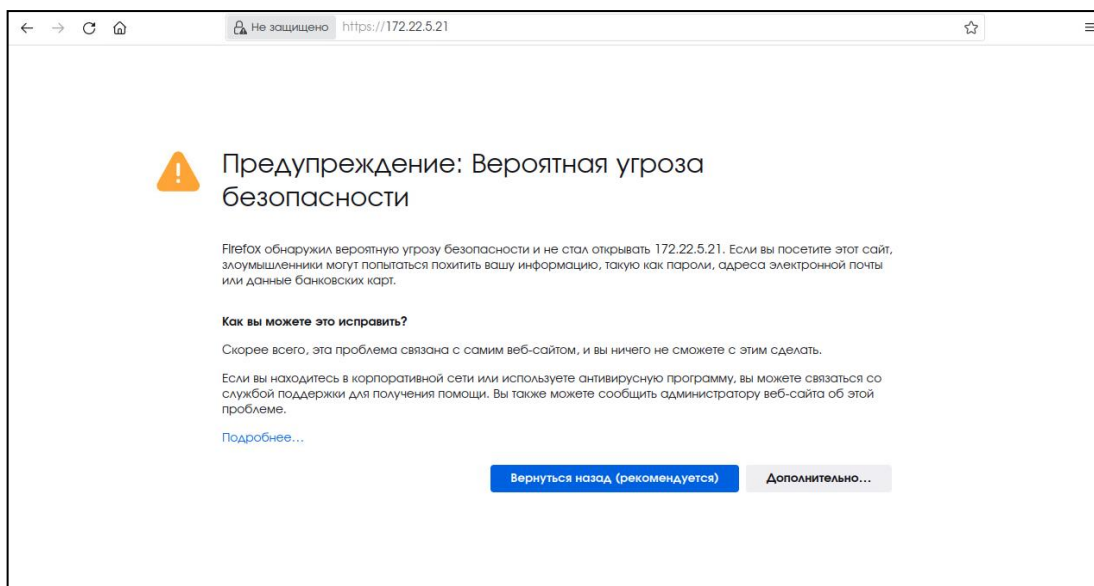


Рисунок 30 – Страница с предупреждением системы безопасности

В случае отказа в доступе к веб-интерфейсу Центра сертификации Aladdin eCA пользователь будет уведомлен 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 Центра сертификации Aladdin eCA 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» Центра сертификации Aladdin eCA.

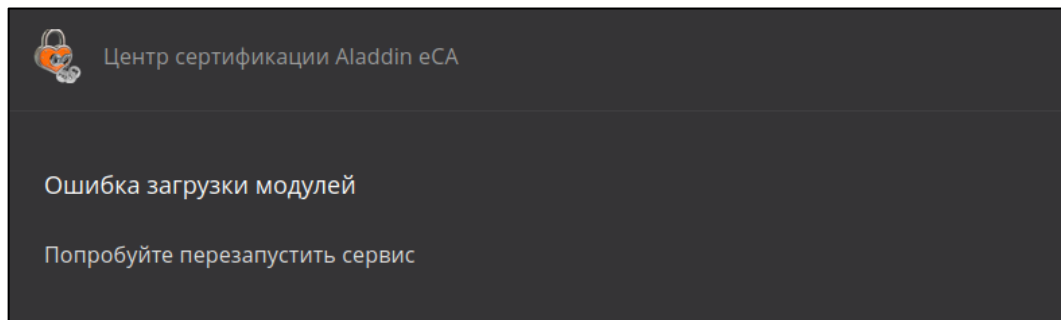


Рисунок 31 – Ошибка загрузки модулей

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

6.2 Аутентификация с использованием сертификата на ключевом носителе

6.2.1 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 6.2.1.2, настройку Chromium в зависимости от ОС см. в подразделах 6.2.1.3 и 6.2.1.4).

6.2.1.1 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**).

6.2.1.2 Настройка веб-браузера Firefox

Выполните настройку веб-браузера **Firefox**, если подключение к серверу Центра сертификации Aladdin eCA 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`¹ (см. Рисунок 32) и подтвердите загрузку модуля, нажав кнопку **<ОК>**;

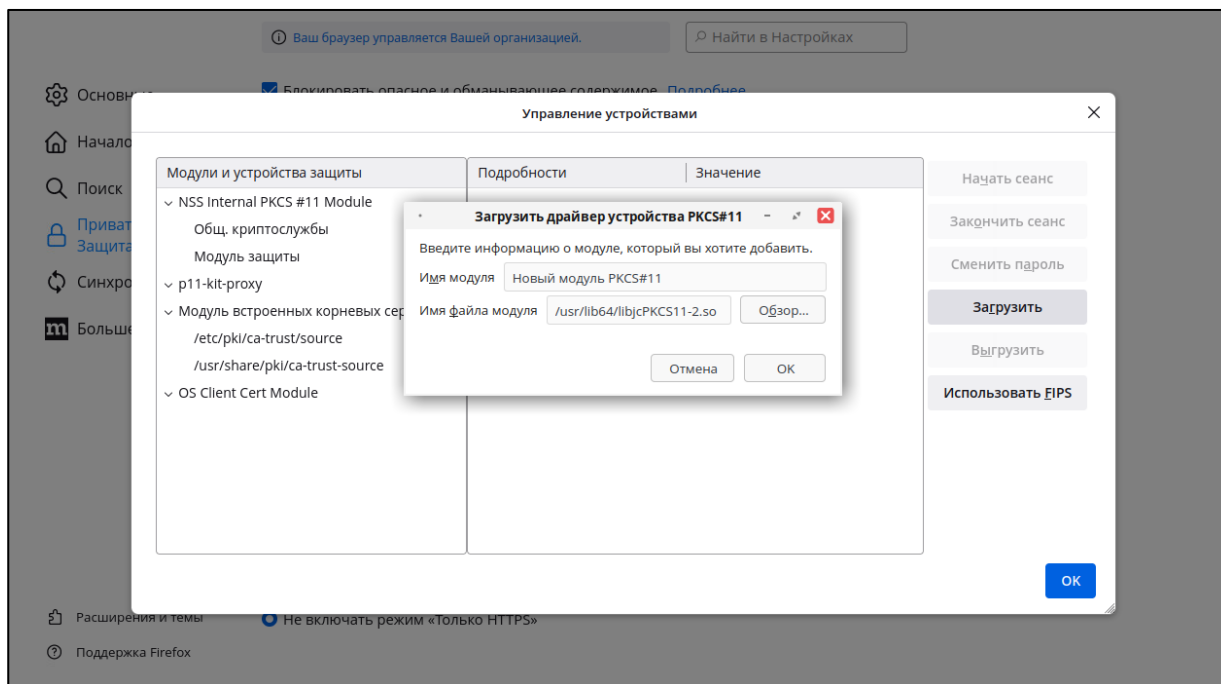


Рисунок 32 – Настройка веб-браузера Firefox

- перезапустите веб-браузер.

6.2.1.3 Настройка веб-браузера Chromium для РЕД ОС, SberLinux OS Server и Альт Сервер

Выполните настройку веб-браузера **Chromium**, если подключение к серверу Центра сертификации Aladdin eCA 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 ~/.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.

6.2.1.4 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**:

¹ Файл модуля `libjcpkcs11-2.so` создается при успешной установке Единого Клиента JaCarta (описание установки было выше в 6.2.1). 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 32).

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

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

- перезапустите веб-браузер.

6.2.2 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 Центра сертификации Aladdin eCA необходимо подключить в USB-порт предварительного настроенного СБТ – 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 6.2.1 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 Центра сертификации Aladdin eCA (например, <https://172.22.5.21>).
- В появившемся окне введите PIN-код ключевого носителя.

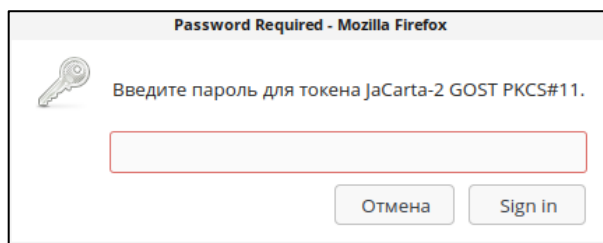


Рисунок 33 – Окно ввода PIN-кода ключевого носителя

- В появившемся окне выберите сертификат с подключенного ключевого носителя.

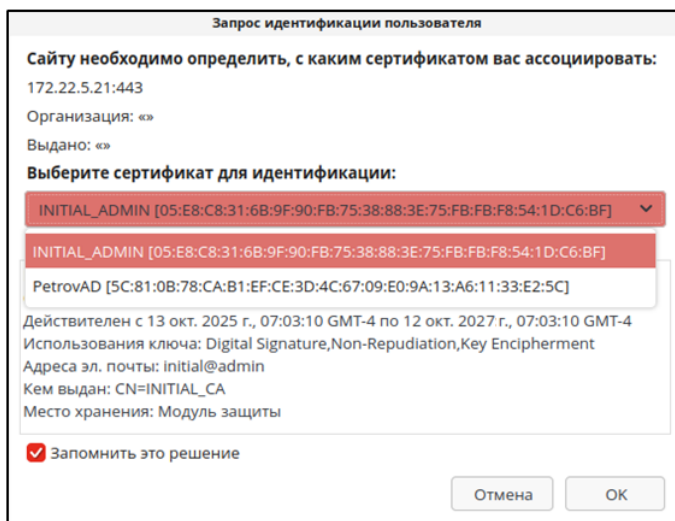


Рисунок 34 – Выбор сертификата пользователя для аутентификации на сервере

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 Центра сертификации Aladdin eCA.

7 БЕЗОПАСНОСТЬ СОЕДИНЕНИЯ

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

Протокол TLS позволяет авторизованным пользователям (администраторам/операторам) клиентской части программы проходить проверку подлинности серверов Центров сертификации Aladdin eCA, 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.

7.1 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 (см. раздел 9.3.1.1 настоящего руководства).
- 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 35). Нажмите кнопку **<Просмотр сертификатов>**.

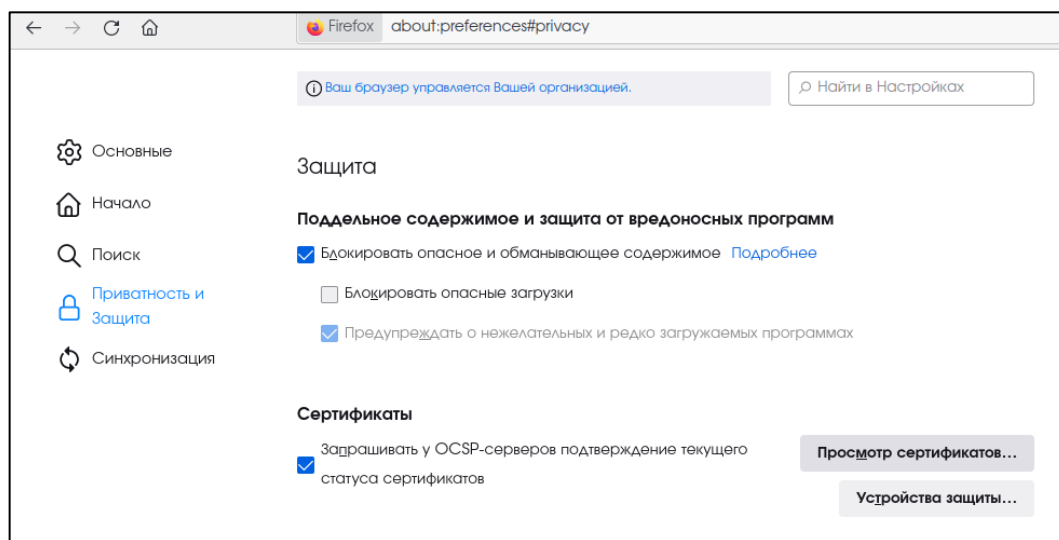


Рисунок 35 – Окно настроек веб-браузера

- 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». Поочерёдно импортируйте все сертификаты Центра сертификации, участвующие в построении цепочки доверия (см. Рисунок 36) или импортируйте цепочку сертификатов.

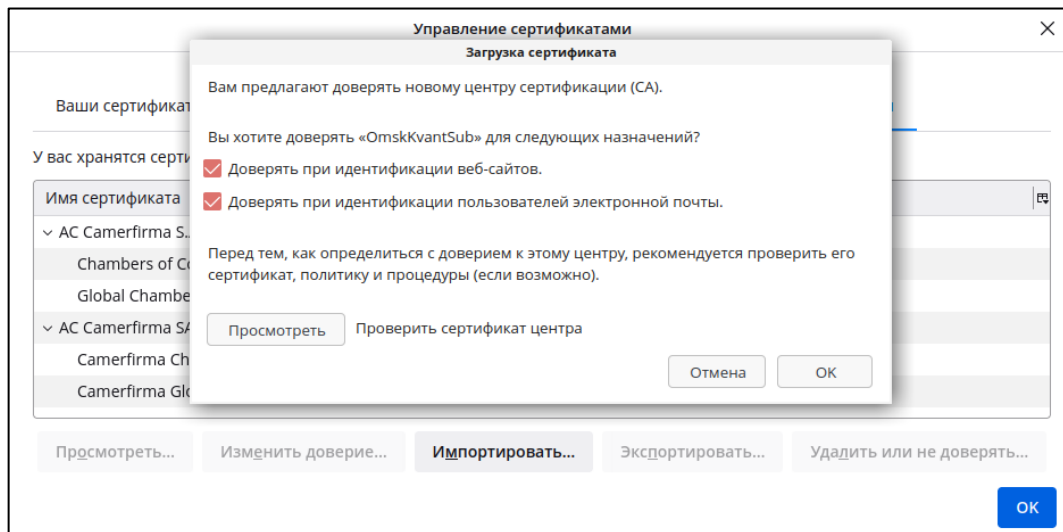


Рисунок 36 – Окно управления сертификатами

- Создать локальный субъект для веб-сервера, выпустите для него сертификат по шаблону «WEB-Server» (см. раздел 9.4.1) и установите сертификат (см. раздел 9.13), если это не сделано ранее.
- Перезапустите веб-браузер.
- Для безопасного доверенного соединения при обращении к серверу Центра сертификации Aladdin eCA используйте доменное имя (см. Рисунок 37), указанное в атрибуте DNS-name суффикса сервера Subject alternative name (SAN) сертификата веб-сервера (см. Рисунок 38) и соответственно указанное в конфигурационном файле `/etc/hosts/` сервера Центра сертификации Aladdin eCA.



Рисунок 37 – Адресная строка в веб-браузере

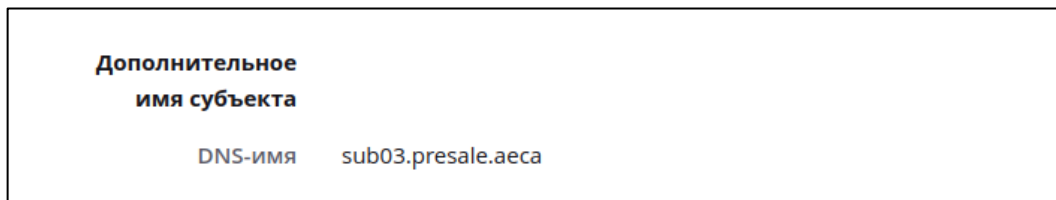


Рисунок 38 – Сертификат веб-сервера

8 ТЕХНОЛОГИЧЕСКИЕ СОСТАВЛЯЮЩИЕ ПРОГРАММЫ

8.1 Назначение технологических составляющих

Технологические составляющие создаются автоматически, с целью первичного запуска Центра сертификации Aladdin eCA.

Внимание! Технологический Центр сертификации использовать для выпуска сертификатов запрещено.

8.2 Установка и настройка технологических составляющих

Перед установкой Центра сертификации Aladdin eCA 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 Центра сертификации Aladdin eCA 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 Центра сертификации Aladdin eCA в каталоге `/opt/aecaCa/dist/certificates/account/` будет размещён сертификат администратора инициализации **INITIAL_ADMIN.p12**, необходимый для дальнейшей аутентификации на веб-сервере. Пароль от сертификата администратора, заданный по умолчанию в конфигурационном файле, **INITIAL**.

Первичная авторизация в открывшемся веб-интерфейсе установленного Центра сертификации Aladdin eCA 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 «Настройка».

8.3 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 Центру сертификации Aladdin eCA.

Для удаления технологических составляющих, необходимых для первичного запуска Центра сертификации Aladdin eCA, после развёртывания Центра сертификации Aladdin eCA 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 9.6.1 настоящего руководства).
- Выпустите сертификат для созданной учётной записи, сохранив контейнер с ключевой парой (сертификат и закрытый ключ) в формате PKCS#12 (см. раздел 9.6.7 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 9.4.1 настоящего руководства).
- Установите выпущенный сертификат веб-сервера через соответствующее меню раздела «Настройки» (см. раздел 9.13 настоящего руководства).
- Выключите проверку издателя технологического Центра сертификации (см. раздел 9.14) настоящего руководства).
- Удалите технологический Центр сертификации (см. раздел 9.3.1.7 настоящего руководства).

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

В случае блокировки доступа к Центру сертификации Aladdin eCA, 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»).

9 ФУНКЦИИ УПРАВЛЕНИЯ ПРОГРАММЫ

9.1 Верхняя панель

Верхняя панель (см. Рисунок 39) веб-интерфейса фиксирована и отображается на любом шаге или переходе между разделами.



Рисунок 39 – 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 Подчиненный);
- обозначение статуса Центра сертификации.

При отсутствии ошибок и предупреждений отображается активный статус:

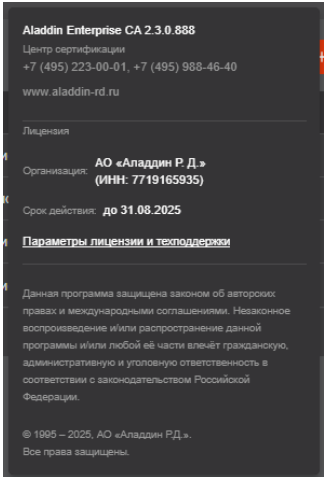
 - активный . При наведении курсора отображается всплывающее сообщение «Активный»;

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»;
 - истекает¹ срок действия сертификата текущего активного Центра сертификации . При наведении курсора отображается всплывающее сообщение «Истекает срок действия сертификата ЦС»;
 - закрытый ключ Центра сертификации недоступен² . 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);
- текущая авторизация учётной записи пользователя;

¹ До истечения остаётся менее 90 дней.



² При запуске серверного компонента Центра сертификации Aladdin eCA не удалось получить закрытый ключ данного ЦС, что может быть обусловлено удалением или повреждением локально хранимого контейнера закрытого ключа либо отсутствием доступа к криптопровайдеру алгоритма, по которому была создана ключевая пара данного ЦС.

- 

– сведения о текущей версии программы, контактная информация разработчика, информация о лицензии.

9.2 Боковая панель

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

- либо быть закрепленной 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 40) или компактном (см. Рисунок 41) 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).

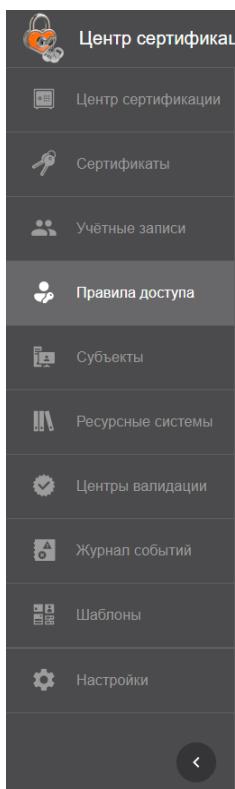


Рисунок 40 – Полный вид боковой панели



Рисунок 41 – 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 Подчиненного Центра сертификации;

- скачать цепочку сертификатов активного Центра сертификации;
- скачать сертификат Корневого и Подчиненного Центра сертификации в формате .pem;
- отозвать сертификат Подчиненного Центра сертификации;
- посмотреть карточку Центра сертификации;
- Раздел «Сертификаты» – в данном разделе возможно:
 - выпустить сертификат с закрытым ключом PKCS#12 для субъекта;
 - выпустить сертификат на основании запроса для субъекта;
 - выпустить сертификат на ключевом носителе для субъекта;
 - посмотреть список всех выпущенных сертификатов субъектов, выпущенных активным 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;
 - скачать сертификат субъекта в формате .pem;
 - скачать цепочку сертификатов;
 - скачивание бумажного сертификата (файл, содержащий сведения из сертификата).
 - скачать текущий CRL;
 - скачать список всех выпущенных сертификатов в формате .csv;
 - применить массовые операции к выбранным сертификатам (отзыв, приостановка, возобновление);
- Раздел «Учетные записи» – в данном разделе возможно:
 - создать новую учетную запись;
 - отредактировать существующую учетную запись;
 - заблокировать или активировать существующую учетную запись;
 - задать группы, на которые предоставляются права для управления сертификатами субъектов, для учетной записи, выполняющей роль «Оператор»;
 - выпустить сертификат для пользователя учётной записи;
- Раздел «Правила доступа» – в данном разделе возможно:
 - просмотреть существующие правила доступа;
 - создать новое правило доступа;
 - отредактировать правило доступа;
 - удалить правило доступа.
- Раздел «Субъекты» – в данном разделе возможно:
 - произвести поиск субъекта по его имени (или части имени);
 - обновить список групп и субъектов;
 - посмотреть существующие субъекты;
 - создать новый локальный субъект;
 - выпустить сертификат с закрытым ключом PKCS#12 для субъекта;
 - выпустить сертификат по запросу для субъекта;
 - выпустить сертификат на ключевом носителе для субъекта;
 - посмотреть все выпущенные сертификаты для каждого субъекта;
 - создать учётную запись для субъекта из группы «Users»;
 - посмотреть карточку субъекта;
 - опубликовать сертификат субъекта в ресурсную систему;
- Раздел «Ресурсная система» – в данном разделе возможно:

- подключить ресурсную систему для управления сертификатами доменных пользователей и других субъектов;
- обновить список субъектов ресурсной системы и их данных в ручном режиме.
- Раздел «Центры валидации» – в данном разделе возможно:
 - настроить параметры рассылки CRL/Delta CRL;
 - скачать CRL;
 - обновить CRL по нажатию кнопки;
 - просмотреть список уже зарегистрированных Центров валидации (далее – ЦВ);
 - зарегистрировать сторонние ЦВ;
 - объединить точки распространения или службы OCSP в кластер;
- Раздел «Журнал событий» – в данном разделе возможно:
 - посмотреть в интерактивном режиме полный или выборочный (с применением фильтров) журнал событий;
 - скачать журнал событий в формате .csv по выбранным параметрам экспорта.
- Раздел «Шаблоны» – в данном разделе отображены предустановленные шаблоны сертификатов. Возможно выполнение следующих операций с шаблонами сертификатов:
 - клонирование;
 - редактирование загруженных и созданных шаблонов сертификатов;
 - удаление шаблонов (кроме предустановленных);
 - отображение списка шаблонов;
 - загрузка шаблонов сертификатов MSCS.
- Раздел «Настройки» – в данном разделе производится:
 - настройка аутентификации при подключении к веб-серверу;
 - замена сертификата текущего веб-сервера;
 - управление списком подключенных Syslog-серверов;
 - просмотр информации о лицензии;
 - импорт новой лицензии.

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

9.3 Раздел «Центр сертификации»

Переход на экран управления центра сертификации осуществляется по выбору раздела «Центр сертификации» бокового меню, расположенного слева на главном экране (см. Рисунок 40).

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».

9.3.1 Вкладка «Свои сертификаты»

Вид раздела «Центр сертификации» – вкладка «Свои сертификаты» показан на рисунке ниже (Рисунок 42).

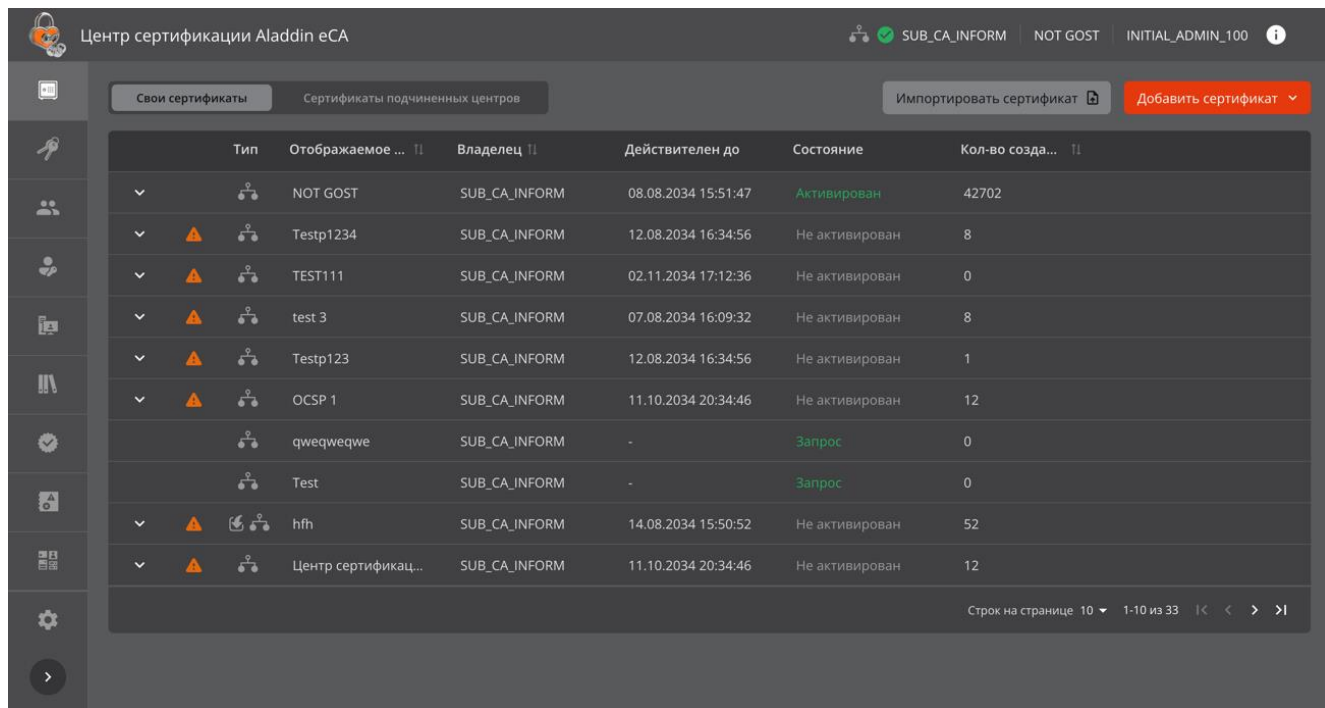


Рисунок 42 – Экран раздела «Центр сертификации» – вкладка «Свои сертификаты»

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

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 по умолчанию в каталоге `/opt/aeca/cryptotoken`, если не изменена конфигурация развёртывания в конфигурационном файле `/opt/aecaCa/scripts/config.sh`.

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

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 9;
- тип – тип центра сертификации:
 - – для корневого Центра сертификации;
 - – для подчиненного 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 9 – Причины отображения индикатора «Обратить внимание на ЦС»

Тип	Причина отображения
 Ошибка	Если истёк срок действия сертификата центра сертификации. При наведении курсора на индикатор отображается всплывающее сообщение «Истек срок действия сертификата ЦС»
 Ошибка	Если закрытый ключ центра сертификации недоступен. При запуске серверного компонента Центра сертификации Aladdin eCA не удалось получить закрытый ключ данного центра сертификации, что может быть обусловлено удалением или повреждением локально хранимого контейнера закрытого ключа либо отсутствием доступа к криптопровайдеру алгоритма, по которому была создана ключевая пара данного центра сертификации.
 Ошибка	Если закрытый ключ центра сертификации находится в состоянии «Ключ экспортирован». При наведении курсора на индикатор отображается всплывающее сообщение «Закрытый ключ центра сертификации недоступен».
 Ошибка	Если до истечения срока действия сертификата центра сертификации остается менее 90 дней. При наведении курсора на индикатор отображается всплывающее сообщение «Истекает срок действия сертификата ЦС».


Для управления Центром сертификации администратору доступны действия, приведённые в таблице 10.

Таблица 10 – 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

Операция	Состояние «Запрос»	Состояние «Активирован»	Состояние «Не активирован»	Необходимое действие для выполнения операции
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 ¹

Технологический Центр сертификации может быть удалён после выпуска и загрузки нового сертификата для текущего сервера (см. раздел 8.3 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 9.3.1.2);
- Для добавления сертификата Центра сертификации симпортом внешнего ключа из контейнера PKCS#12 выберите опцию «Импорт внешнего ключа» (подробнее см. раздел 9.3.1.2).

9.3.1.1 Карточка сертификата центра сертификации

Переход к экрану «Карточка сертификата ЦС» осуществляется при нажатии на строку сертификата таблицы на вкладке «Свои сертификаты» в состоянии «Активирован» или «Не активирован» (см. Рисунок 43 и Рисунок 44).

В карточке активного Центра сертификации доступны следующие действия (см. Рисунок 43):

- выгрузить сертификат, цепочку сертификатов или текущий список отозванных сертификатов по нажатию кнопки **<Скачать>**;
- удалить Центр сертификации по нажатию кнопки **<Удалить>**.

В карточке неактивного Центра сертификации доступны следующие действия (Рисунок 44):

- выгрузить сертификат, цепочку сертификатов или текущий список отозванных сертификатов по нажатию кнопки **<Скачать>**;
- удалить Центр сертификации по нажатию кнопки **<Удалить>**;
- активировать центр сертификации².

¹ При успешной активации центра сертификации в журнале событий регистрируется запись с кодом CAENV008.

² При успешной активации центра сертификации в журнале событий регистрируется запись с кодом CAENV008.

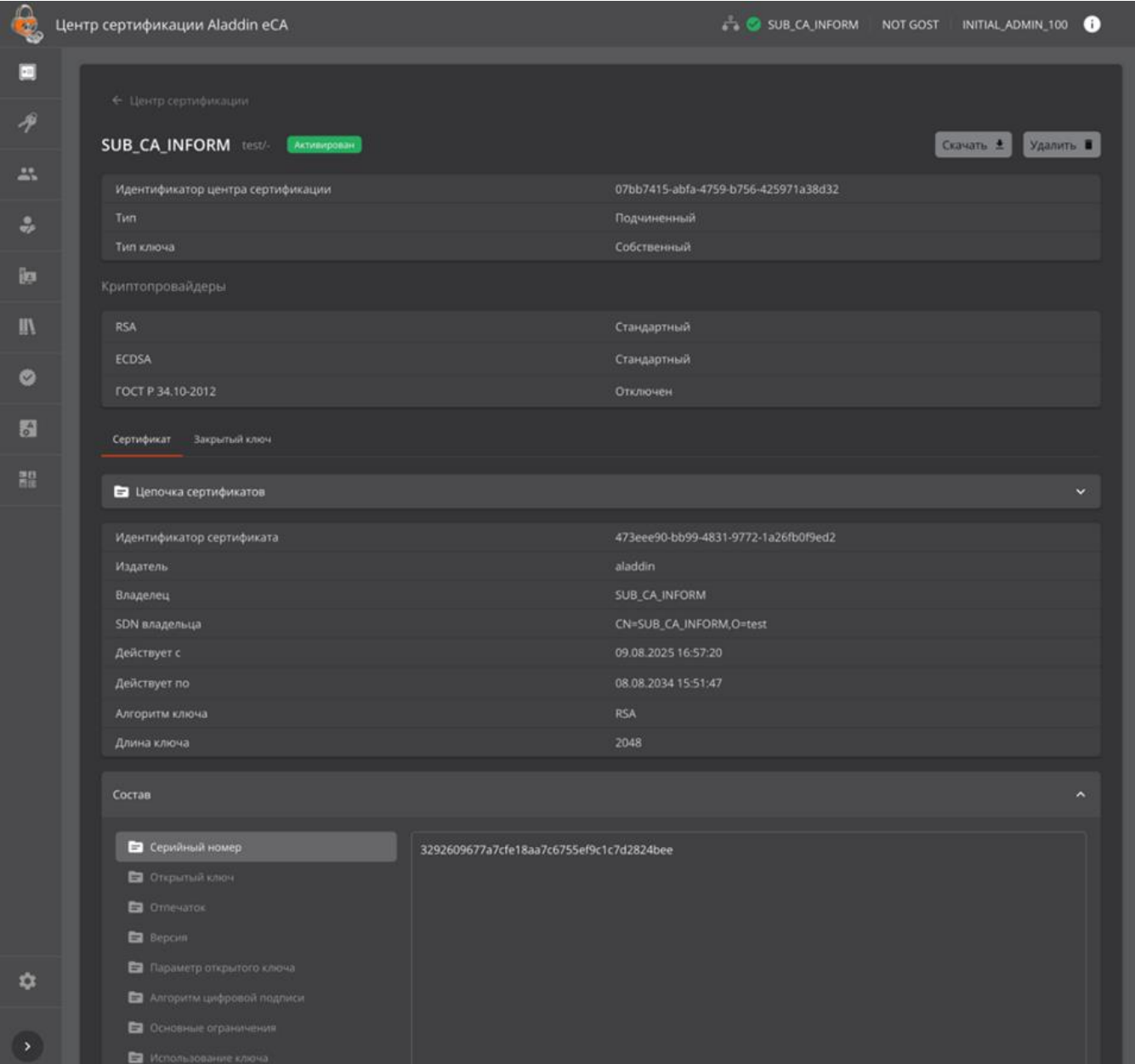


Рисунок 43 – Карточка Центра сертификации в состоянии «Активирован»

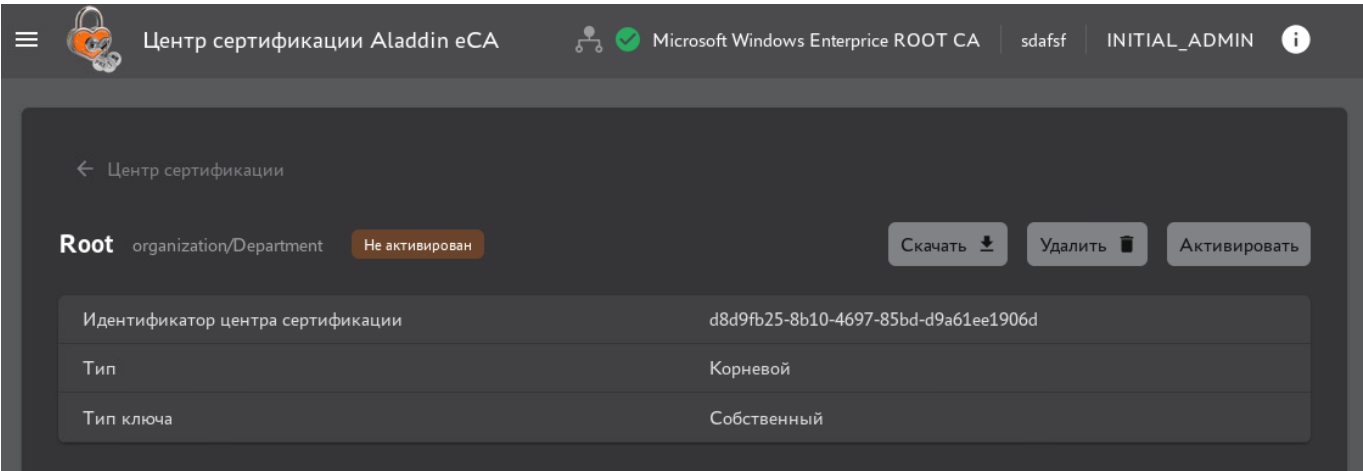




Рисунок 44 – Карточка Центра сертификации в состоянии «Не активирован»

В карточке Центра сертификации отображаются следующие сведения:

- В заголовке карточки:
 - Отображаемое имя Центра сертификации;

- Состояние Центра сертификации;
- Индикатор «Обратить внимание на ЦС» – отображается только при наличии проблем у данного Центра сертификации (Таблица 9).
- идентификатор Центра сертификации;
- тип – тип Центра сертификации (корневой или подчиненный);
- тип ключа:
 - собственный – ключевая пара была создана при инициализации Центра сертификации;
 - импортированный – ключевая пара была импортирована из контейнера PKCS#12;
- Подраздел «Криптопровайдеры», отображающий выбранных при создании данного Центра сертификации криптопровайдеров алгоритмов. В случае, если криптопровайдер недоступен, слева от его названия отображается индикация «треугольник с восклицательным знаком», при наведении на которую отображается всплывающее сообщение «Криптопровайдер недоступен»;
- Вкладка «Сертификат», содержащая:
 - Раскрывающийся список (дерево) «Цепочка сертификатов»;
 - Сведения о сертификате Центра сертификации в табличной форме, содержащие следующие строки в формате «ключ – значение»:
 - Идентификатор сертификата (значение в данном поле соответствует идентификатору сертификата данного Центра сертификации);
 - Издатель (поле «Issuer» сертификата);
 - Владелец (атрибут «CN» из поля «Subject» сертификата);
 - SDN издателя (значение поля «Subject» сертификата);
 - Действует с (атрибут «Not Before» из поля «Validity» сертификата);
 - Действует по (атрибут «Not After» из поля «Validity» сертификата);
 - если до истечения остается менее 90 дней, то цвет значения – оранжевый и рядом отображается индикатор , при наведении курсора отображается всплывающая подсказка «Осталось менее 90 дней до истечения»;
 - для истекших сертификатов цвет значения – красный и рядом отображается индикатор , при наведении курсора отображается всплывающая подсказка «Сертификат истек».
 - Алгоритм ключа (атрибут «Public Key Algorithm» из поля «Subject Public Key Info» сертификата);
 - Длина ключа (атрибут «Public Key Algorithm» из поля «Subject Public Key Info» сертификата);
 - Раскрывающийся список «Состав», содержащий следующую информацию о полях сертификата Центра сертификации:
 - Серийный номер (поле «Serial Number» сертификата);
 - Открытый ключ (поле «Subject Public Key Info»);
 - Отпечаток (вычисляемое значение, отсутствует в сертификате);
 - Версия (поле «Version» сертификата);
 - Параметр открытого ключа (всегда «X509»);
 - Алгоритм цифровой подписи (поле «Signature Algorithm»);
 - Основные ограничения (поле «X509v3 Basic Constraints»);
 - Использование ключа (поле «X509v3 Key Usage» сертификата);
 - Доступ к информации о центре сертификации (поле «Authority Information Access»);
 - Альтернативное имя субъекта (поле «X509v3 Subject Alternative Name» сертификата);


- Идентификатор ключа центра (поле «X509v3 Authority Key Identifier» сертификата);
- Идентификатор ключа субъекта (поле «X509v3 Subject Key Identifier» сертификата);
- Расширенное использование ключа (поле «X509v3 Extended Key Usage» сертификата).
- Вкладка «Закрытый ключ», содержащая:
 - Кнопку для экспорта/импорта закрытого ключа Центра сертификации;
 - Для Центра сертификации в состоянии «Не активирован» кнопка называется **<Экспортировать ключ>**, если в поле «Состояние» на вкладке «Закрытый ключ» указано значение «Доступен» и в поле «Экспорт ключа» указано значение «Разрешен»;
 - Для Центра сертификации с состоянием закрытого ключа «Ключ экспортирован» кнопка называется **<Импортировать ключ>**.
 - Иначе кнопка для экспорта/импорта закрытого ключа Центра сертификации не отображается на вкладке «Закрытый ключ».
 - Алгоритм ключа – название алгоритма ключевой пары Центра сертификации;
 - Длина ключа – длина закрытого ключа Центра сертификации;
 - Место хранения – место хранения закрытого ключа Центра сертификации:
 - Локальное хранилище Aladdin eCA.
 - КриптоПро CSP (HDIMAGE).
 - КриптоПро HSM.

Для центра сертификации с состоянием закрытого ключа «Ключ экспортирован» в данном поле указан прочерк (символ «–»).
 - Экспорт ключа – возможность экспорта закрытого ключа Центра сертификации:
 - Разрешен;
 - Запрещен.

Для центра сертификации в состоянии «Ключ экспортирован» в данном поле прочерк (символ «–»).
 - Состояние – состояние закрытого ключа Центра сертификации:
 - Доступен;
 - Недоступен;
 - Экспортирован.

9.3.1.2 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>** и в выпадающем списке выберите опцию «Создать ключ».
- Если текущая лицензия позволяет создание корневого и подчиненного Центров сертификации, то отобразится модальное окно «Окно инициализации корневого ЦС. Шаг 1/5» с шагом выбора лицензии (см. Рисунок 45). 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.

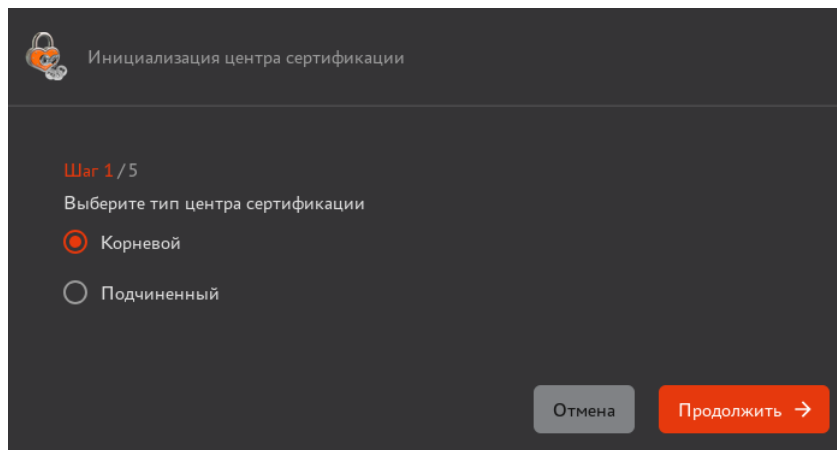


Рисунок 45 – Выбор типа центра сертификации

- На шаге 2/5 (см. Рисунок 46) заполните поля:

Рисунок 46 – Окно инициализации корневого центра сертификации. Шаг 2/5

- «Отображаемое имя» – введите имя создаваемого Центра сертификации, которое будет отображаться в интерфейсе Центра сертификации Aladdin eCA. Оно может содержать буквы латинского и/или кириллического алфавита, цифры от 0 до 9, символы таблицы ASCII, максимальная длина 200 символов;
- «Имя центра сертификации» (Common Name) – выберите имя создаваемого корневого Центра сертификации из перечня возможных имен в соответствии с параметрами лицензии;

- «Суффикс различающегося имени» – укажите суффикс различающегося имени корневого сертификата (формат ввода суффикса приведен справа от поля). Ограничители ввода между параметрами – запятые и запятые с пробелами. Длина вводимого суффикса различающегося имени не должна превышать 250 байт. Ввод атрибутов возможен в любом порядке, но в сертификате порядок атрибутов будет установлен в соответствии с номерами пунктов, указанных в таблице 11.

Таблица 11 – 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

- 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 47):

Рисунок 47 – Окно инициализации корневого центра сертификации. Шаг 3/5

- «RSA» – поле выбора криптопровайдера для алгоритма RSA, допустимые варианты выбора:
 - Стандартный (по умолчанию);
 - КриптоПро CSP¹ (доступен только при наличии активного и подключенного криптопровайдера СКЗИ «КриптоПро CSP», работающего на сервере совместно с Центром сертификации Aladdin eCA);
 - Отключен.
- «ECDSA» – поле выбора криптопровайдера для алгоритма ECDSA, допустимые варианты выбора:
 - Стандартный (по умолчанию);
 - Отключен.
- «ГОСТ Р 34.10–2012» – поле выбора криптопровайдера для алгоритма ГОСТ Р 34.10–2012, допустимые варианты выбора:
 - КриптоПро CSP (доступен только при наличии активного и подключенного криптопровайдера СКЗИ «КриптоПро CSP», работающего на сервере совместно с Центром сертификации Aladdin eCA);
 - 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 48).

¹ Подробная информация по настройке взаимодействия Центра сертификации Aladdin eCA 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».

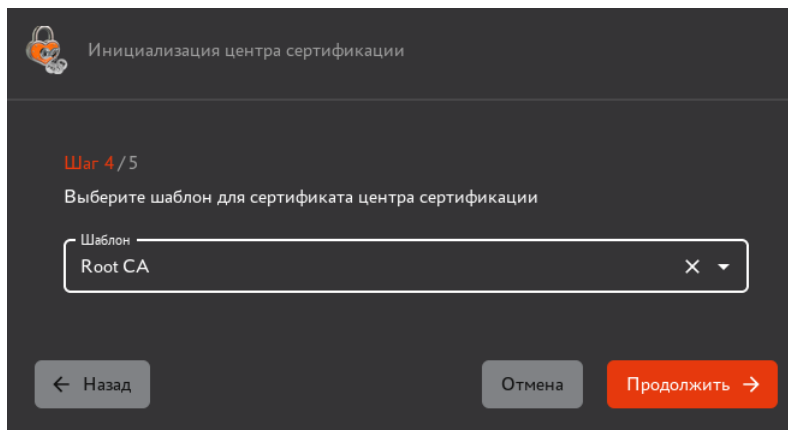



Рисунок 48 – Окно инициализации корневого центра сертификации. Шаг 4/5

- 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 49). Заполните следующие поля:
 - «Срок действия сертификата» – срок действия Корневого сертификата (по умолчанию – 15 лет). Ввод осуществляется вручную или выбором даты окончания действия сертификата в открывшемся календаре. Максимальный срок действия сертификата определяется шаблоном, выбранным на предыдущем шаге;
 - «Алгоритм ключа» (состав алгоритмов зависит от выбранных провайдеров и шаблоном, выбранным на предыдущем шаге):
 - RSA;
 - ECDSA;
 - ГОСТ Р 34.10–2012.
 - «Длина ключа» (доступные значения определяются шаблоном, выбранным на предыдущем шаге):
 - для RSA: 1024, 1536, 2048, 3072, 4096, 6144, 8192 (по умолчанию 4096);
 - для ECDSA: 256, 384, 521 (по умолчанию 384);
 - для ГОСТ Р 34.10–2012: 256, 512 (по умолчанию 512).
 - «Алгоритм хэш–суммы»:
 - для алгоритма ключа RSA или ECDSA: SHA1, SHA256, SHA384, SHA512 (выбран по умолчанию);
 - для алгоритма ключа ГОСТ Р 34.10–2012: ГОСТ Р 34.11–2012.
 - «Место хранения закрытого ключа»:
 - Доступные варианты выбора, если криптопровайдером выбранного алгоритма ключа является КриптоПро CSP:
 - Локальное хранилище Aladdin eCA (выбрано по умолчанию, требует заранее подготовленной на БДЧ криптопровайдера 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».
 - 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

25.12.2034

Максимальный срок действия ЦС определяется шаблоном

Параметры криптографии

Алгоритм ключа

RSA

Длина ключа

2048

Алгоритм хэш-суммы

SHA256

Место хранения закрытого ключа центра сертификации

Место хранения

Локальное хранилище Aladdin eCA

Убедитесь в наличии достаточного объема используемой внешней гаммы

☒ Экспортируемый закрытый ключ

← Назад

Отмена

Создать ЦС →

Рисунок 49 – 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, приведенных в таблице .

Таблица 12 – 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
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.

АО "Аладдин Р.Д.", 1995–2025 г.

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

Стр. 63 / 258

Текст ошибки	Причина																						
Ошибка. Ошибка атрибута attributeName: Значение не соответствует регулярному выражению: «regex»	<p>Ошибка валидации введенного значения атрибута различающегося имени¹. Возможные значения переменной «attributeName» и соответствующие им значения переменной «regex» представлены в таблице ниже:</p> <table> <tr> <th>attributeName</th><th>regex</th></tr> <tr> <td>C</td><td>^[A-Za-z]{2}\$</td></tr> <tr> <td>DN</td><td>^[A-Za-z0-9''()+,\.:=?]+\$</td></tr> <tr> <td>EMAILADDRESS</td><td>^[A-Za-zАа-яа-я0-9._-]+@[A-Za-zАа-яа-я0-9._-]+\$</td></tr> <tr> <td>SERIALNUMBER</td><td>^[A-Za-z0-9''()+,\.:=?]+\$</td></tr> <tr> <td>INN</td><td>^\d{12}\$</td></tr> <tr> <td>OGRN</td><td>^\d{13}\$</td></tr> <tr> <td>OGRNIP</td><td>^\d{15}\$</td></tr> <tr> <td>SNILS</td><td>^\d{11}\$</td></tr> <tr> <td>INNLE</td><td>^\d{10}\$</td></tr> <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''()+,\.:=?]+\$	EMAILADDRESS	^[A-Za-zАа-яа-я0-9._-]+@[A-Za-zАа-яа-я0-9._-]+\$	SERIALNUMBER	^[A-Za-z0-9''()+,\.:=?]+\$	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''()+,\.:=?]+\$																						
EMAILADDRESS	^[A-Za-zАа-яа-я0-9._-]+@[A-Za-zАа-яа-я0-9._-]+\$																						
SERIALNUMBER	^[A-Za-z0-9''()+,\.:=?]+\$																						
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																						

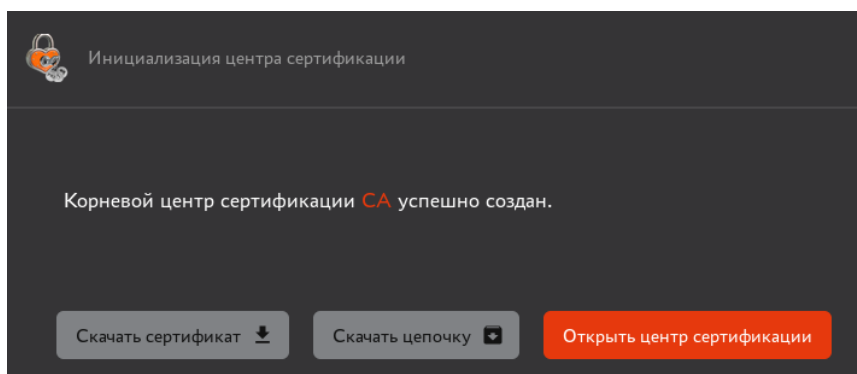


Рисунок 50 – Окно завершения инициализации корневого центра сертификации

При успешном создании Корневого Центра сертификации и завершении инициализации Центра сертификации будет отображено соответствующее окно (см. Рисунок 50). 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.

¹ Правила валидации значений атрибутов представлены в Приложении 3 «Правила валидации значений полей по умолчанию предустановленных шаблонов сертификатов».

9.3.1.3 Создание подчиненного 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 5.1.2 при создании сертификата подчиненного Центра сертификации;

Новый Центр сертификации будет создан на основании текущей лицензии.

9.3.1.4 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 5.2.

Новый Центр сертификации будет создан на основании текущей лицензии.

9.3.1.5 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 Подчиненный Центр сертификации в состоянии «Запрос» (см. Рисунок 51).

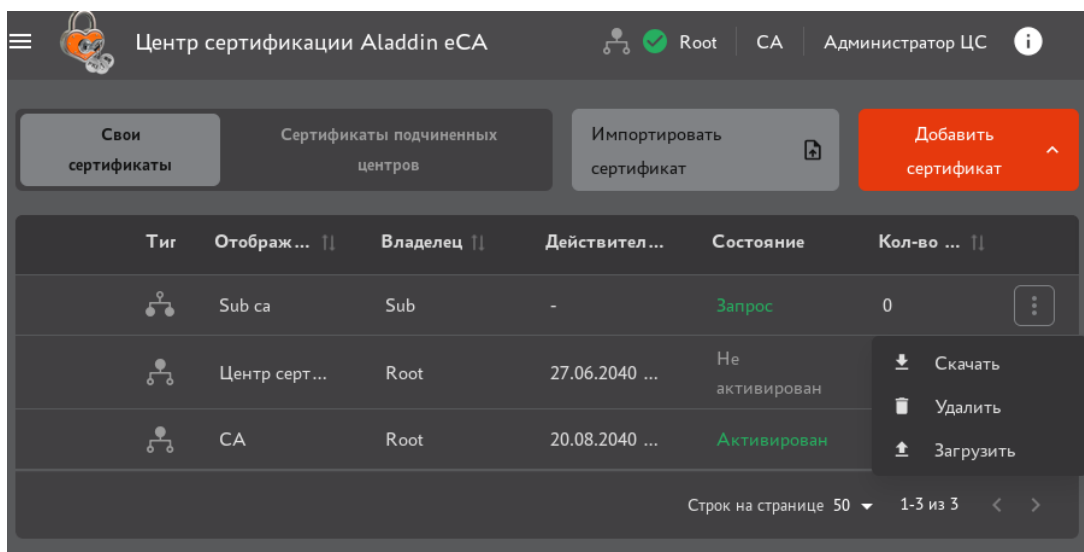



Рисунок 51 – Скачивание запроса на сертификат



- Нажать появившуюся в строке выбранного Центра сертификации кнопку  и скачать запрос в формате **.csr**.
- Далее следует подписать скаченный запрос на Корневом Центре сертификации согласно разделу 9.3.2.2 настоящего руководства администратора.

9.3.1.6 Импорт сертификата подчиненного 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 подчиненного 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 Подчиненный Центр сертификации в состоянии «Запрос», по запросу которого был сформирован сертификат и цепочка сертификатов в формате `.pem` или `.p7b` в разделе 9.3.1.5 данного руководства. Нажать кнопку  **<Загрузить>** (см. Рисунок 51) 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 52) выбрать скачанный ранее файл цепочки сертификата для загрузки в формате `.pem` или `.p7b`. Нажать кнопку **<Загрузить>**, активированную после выбора файла цепочки сертификатов.

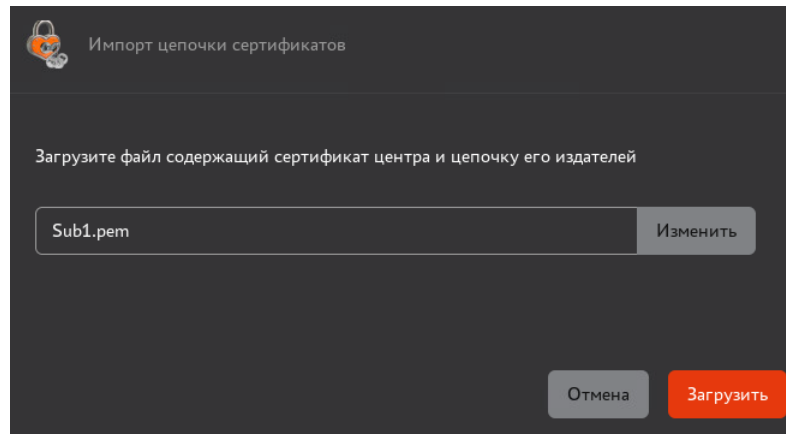


Рисунок 52 – Окно импорта цепочки сертификатов

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

- имени подчиненного Центра сертификации, указанного в импортируемом сертификате (компонент «Common name» в поле «Subject») на соответствие имени, указанному в лицензии подчиненного 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 подчиненного 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 Центре сертификации Aladdin eCA компоненты SDN в поле «Subject» расположены в следующем порядке:

- 1) EMAILADDRESS;
- 2) CN;
- 3) UID;
- 4) SERIALNUMBER;
- 5) OU;
- 6) O;
- 7) L;
- 8) ST;
- 9) DC;
- 10) C;
- 11) T;
- 12) SURNAME;
- 13) STREET;

- 14) INITIALS;
- 15) GIVENNAME;
- 16) UNSTRUCTUREDADDRESS;
- 17) UNSTRUCTUREDNAME;
- 18) POSTALCODE;
- 19) BUSINESSCATEGORY;
- 20) TELEPHONENUMBER;
- 21) PSEUDONYM;
- 22) POSTALADDRESS;
- 23) NAME;
- 24) DN;
- 25) DESCRIPTION;
- 26) INN;
- 27) OGRN;
- 28) OGRNIP;
- 29) SNILS;
- 30) INNLE.
- 31) DATEOFBIRTH;
- 32) PLACEOFBIRTH.

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 приведен в таблице 13. При этом в журнале событий будет зарегистрировано событие с кодом CAENV013.

Таблица 13 – Перечень сообщений в случае неудачной попытки импорта сертификата

Текст ошибки	Причина
Ошибка. Недействительный сертификат.	Ошибка истечения срока действия сертификата, входящего в состав цепочки.
Ошибка. Поле отсутствует в шаблоне.	Ошибка указания в запросе на сертификат подчиненного ЦС компонента суффикса различающегося имени, отсутствующего в выбранном шаблоне.
Ошибка. Проверка публичного ключа сертификата не удалась.	Ошибка прохождения проверки соответствия открытого ключа закрытому ключу.
Ошибка. Имя подчиненного ЦС, указанное в сертификате, не соответствует лицензии.	Ошибка несоответствия имени подчиненного Центра сертификации, указанного в его сертификате (компонент «Common name» в поле «Subject» сертификата подчиненного Центра сертификации) имени (перечню имен), указанному в лицензии.
Ошибка. Имя корневого ЦС, указанное в сертификате, не соответствует лицензии.	Ошибка несоответствия имени корневого Центра сертификации, указанного в его сертификате (компонент «Common name» в поле «Subject» сертификата корневого Центра сертификации) имени (перечню имен) корневого Центра сертификации, указанному в лицензии.
Ошибка. Сертификат ЦС содержит некорректный порядок компонентов суффикса различающегося имени.	Сертификат Центра сертификации содержит некорректный порядок компонентов суффикса различающегося имени.
Ошибка. Загружаемая цепочка сертификатов содержит сертификат (CN=«CN сертификата»), не являющийся сертификатом ЦС	Указанный в ошибке сертификат из цепочки не является сертификатом Центра сертификации (флаг <code>isCA=false</code> , а должен быть <code>isCA=true</code>).
Ошибка. Неизвестная ошибка.	Внутренняя ошибка ПО.

После успешной загрузки цепочки сертификатов открывается окно с уведомлением об успешной загрузке сертификата (см. Рисунок 53) 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.

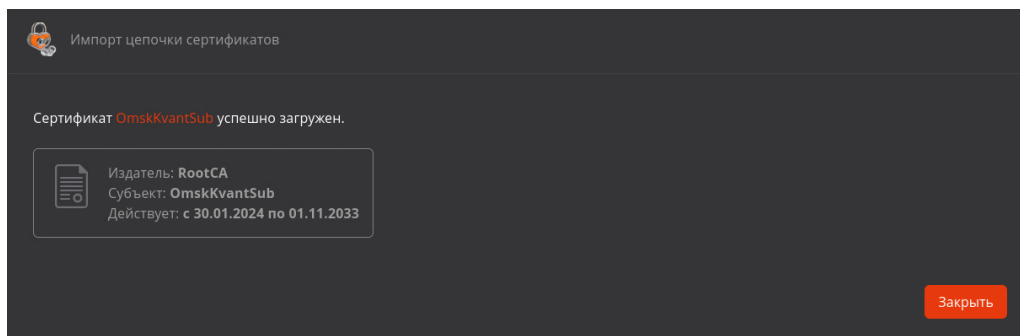


Рисунок 53 – Окно уведомления об успешном загрузке сертификата

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

9.3.1.7 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 Подчиненный Центр сертификации был активным, необходимо восстановить доступ к программе в соответствии с инструкцией, приведенной 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 54);


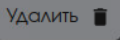
SubCA	OmskKvantSub	01.11.2033 18:18:21	RSA	2048	Не активирован	7
-------	--------------	---------------------	-----	------	----------------	---

Рисунок 54 – Раздел «Центр сертификации» – Вкладка «Свои сертификаты» – Состояние удаляемого Центра сертификации

- выключена проверка издателя – удаляемого Центра сертификации (см. Рисунок 55, раздел 9.14 настоящего руководства).

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 55 – 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 56).

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.

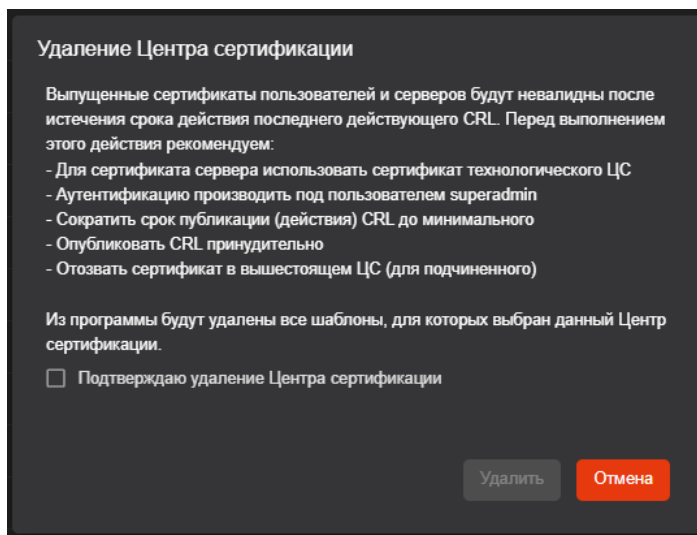


Рисунок 56 – Окно подтверждения удаления Центра сертификации

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>**.

В результате удаления Центра сертификации в журнал событий будут зарегистрированы записи с кодами:

- CAENV059;
- CAENV038 (изменение списка издателей);
- CAENV060.

9.3.1.8 Экспорт закрытого ключа центра сертификации

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

- В разделе «Центр сертификации» перейти на вкладку «Свои сертификаты», затем перейдите в карточку Центра сертификации с состоянием «Не активирован» и с разрешенным экспортом закрытого ключа.
- В открывшейся карточке Центра сертификации перейдите на вкладку «Закрытый ключ». На данной вкладке нажмите на кнопку **<Экспортировать ключ>** (см. Рисунок 57).

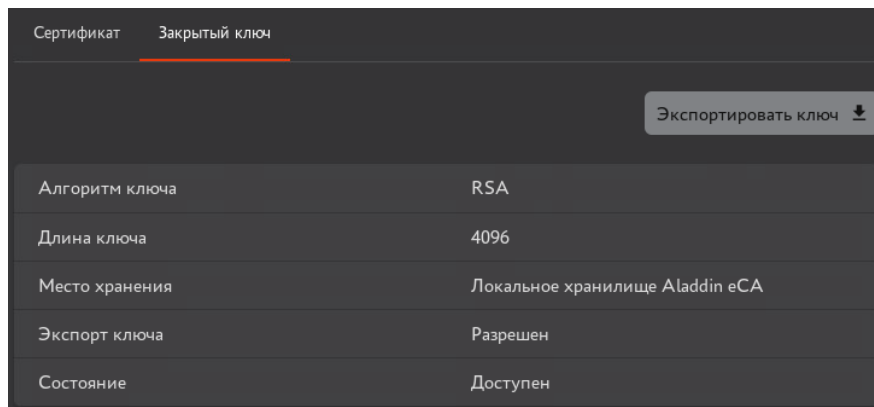


Рисунок 57 – Вкладка «Закрытый ключ» с возможностью экспорта закрытого ключа

- 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 58).

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

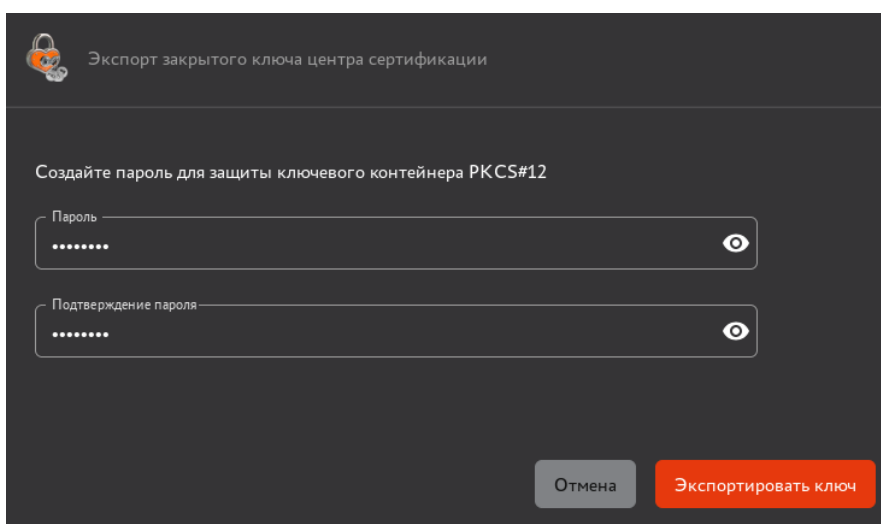


Рисунок 58 – Создание пароля для контейнера PKCS#12 при экспорте закрытого ключа

- 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 59).

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.

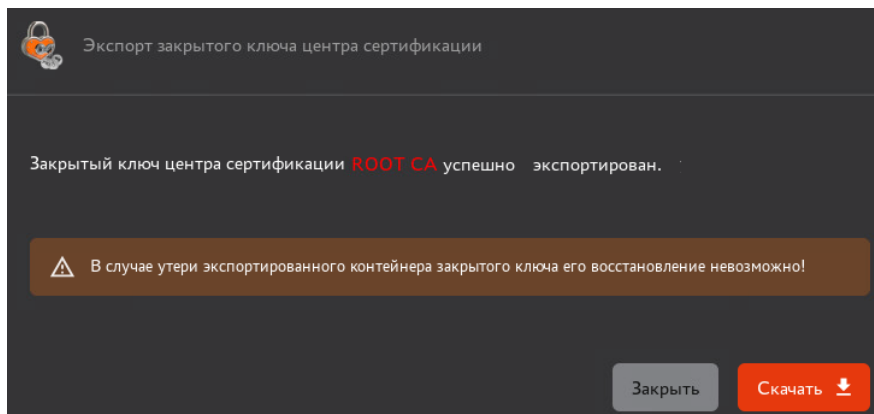


Рисунок 59 – Окно с успешным результатом экспорта закрытого ключа Центра сертификации

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.

9.3.1.9 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 60).

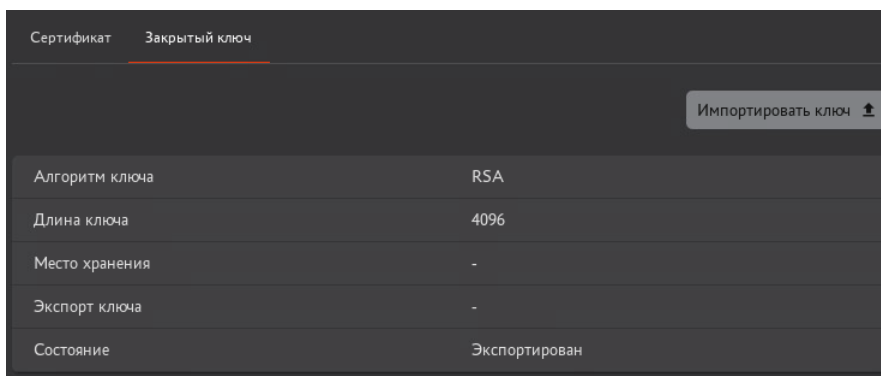


Рисунок 60 – Вкладка «Закрытый ключ» с возможностью импорта закрытого ключа

- В отобразившемся окне «Импорт закрытого ключа центра сертификации» на шаге 1 необходимо выбрать место хранения для закрытого ключа Центра сертификации (см. Рисунок 61).

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».

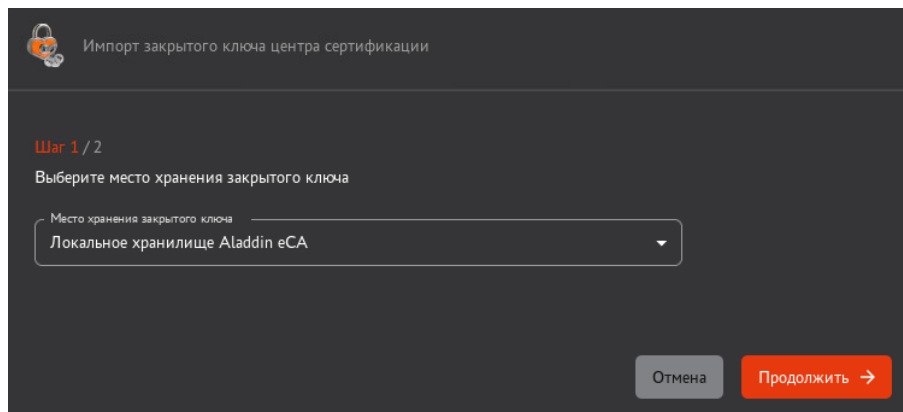


Рисунок 61 – Окно «Импорт закрытого ключа центра сертификации». Шаг 1/2

- Для перехода к следующему шагу нажмите на кнопку **<Продолжить>**.
- На шаге 2 загрузите файл контейнера закрытого ключа и введите пароль от него (см. Рисунок 62). Допустимое расширение для загружаемых файлов – **.p12**. При загрузке файла с иным расширением в поле загрузки файла будет отображено сообщение об ошибке «Некорректный формат файла».

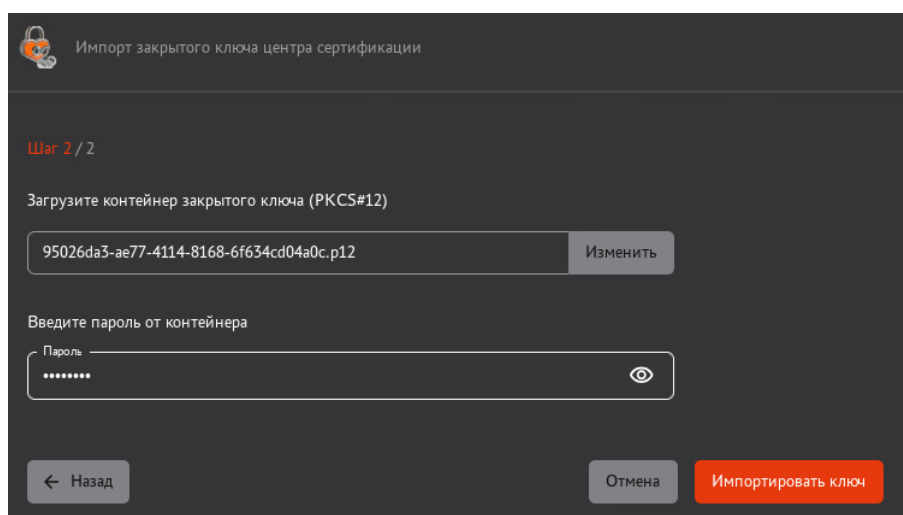


Рисунок 62 – Окно «Импорт закрытого ключа центра сертификации». Шаг 2/2

- 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 14.

Таблица 14 – 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 63).

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

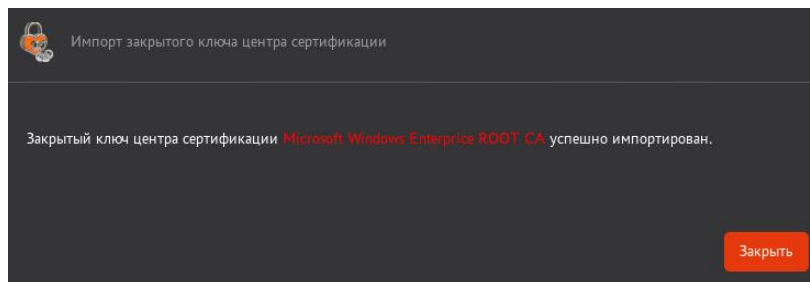


Рисунок 63 – Окно с успешным результатом импорта закрытого ключа Центра сертификации

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»;
- В журнале событий будет зафиксировано событие с кодом CAENV107.

9.3.2 Вкладка «Сертификаты Подчиненных центров»

Вкладка «Сертификаты Подчиненных центров» (см. Рисунок 64) 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 15 – Действия над сертификатами Подчиненных центров

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

Нажатие на кнопку **<Подписать запрос>** запускает сценарий подписи запроса Подчиненного Центра сертификации из категории «Сертификаты Подчиненных центров».

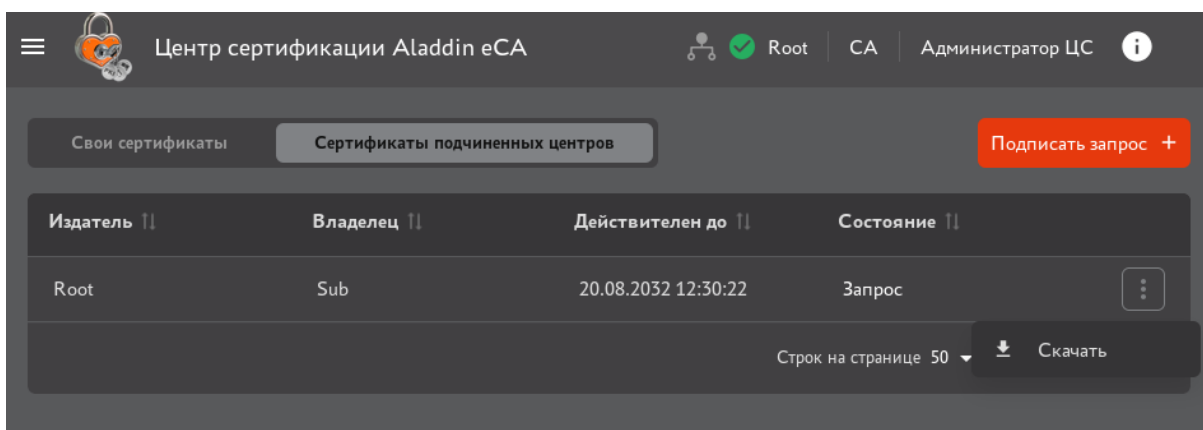


Рисунок 64 – Экран «Сертификаты Подчиненных центров»

Информационные элементы экрана «Сертификаты Подчиненных центров» – неуправляемые табличные поля:

- издатель;
- владелец;
- действителен до (дата);

- алгоритм ключа;
- длина ключа;
- состояние (варианты состояний: действительный, отозван, истёк срок).

Управляемые поля. В соответствии с состоянием Подчиненного сертификата при помощи кнопок управления, расположенных на табличных полях, возможны действия, приведенные в таблице ниже (Таблица 15).

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

9.3.2.1 Карточка сертификата подчинённого центра сертификации

- Переход к экрану «Карточка сертификата ЦС» осуществляется при нажатии на строку сертификата таблицы на вкладке «Свои сертификаты» (см. Рисунок 43).

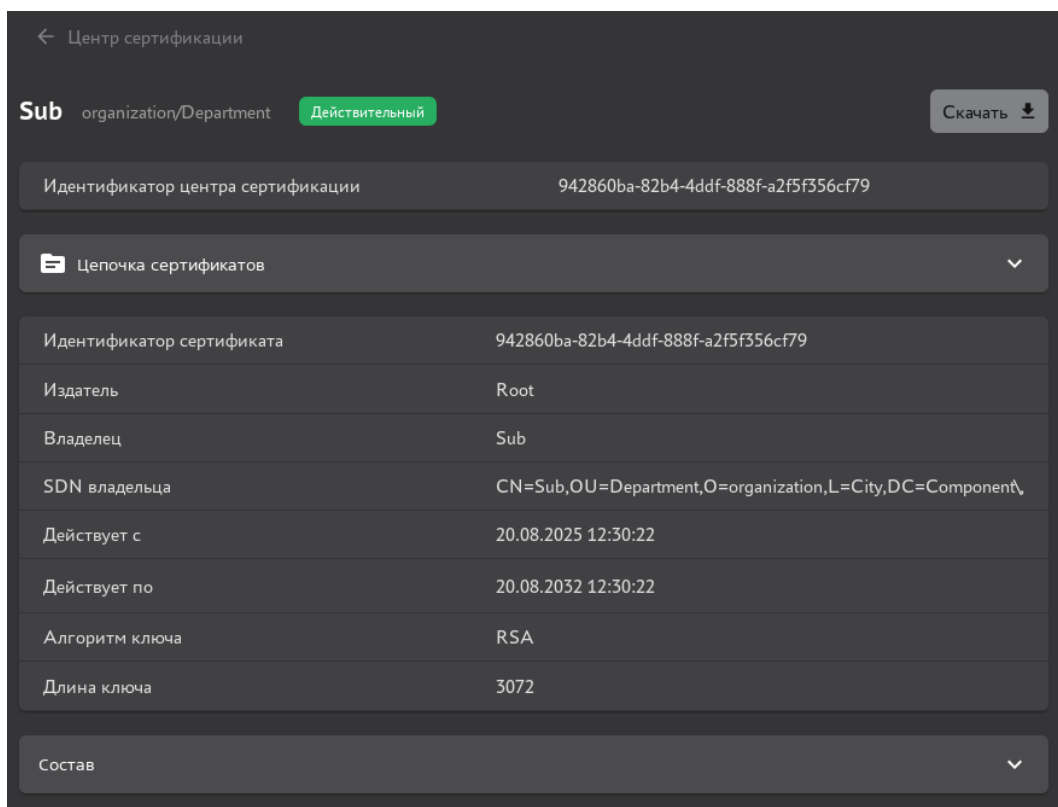


Рисунок 65 – Экран карточки сертификата Подчинённого Центра сертификации в состоянии «Действительный»

Доступные действия в карточке сертификата Центра сертификации со статусом «Действительный» возможно:

- выгрузить сертификат по нажатию кнопки **<Скачать>**.
- отозвать сертификат Центра сертификации по нажатию кнопки **<Отозвать>**.

Набор кнопок в карточке Центра сертификации в зависимости от статуса сертификата Центра сертификации соответствует приведённым действиям в таблице 15.

В карточке Центра сертификации отображаются следующие сведения:

- идентификатор Центра сертификации;
- цепочка сертификатов;
- идентификатор сертификата;
- издатель;
- владелец;
- SDN владельца;

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

9.3.2.2 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 66).

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.

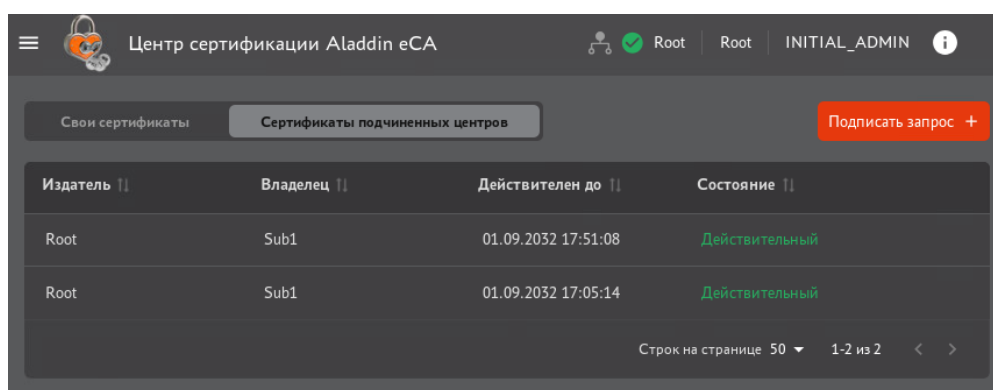


Рисунок 66 – Окно «Сертификаты Подчиненных ЦС»

- В открывшемся окне загрузите файл-запрос в формате **.csr**, нажав кнопку «Выбрать файл» (см. Рисунок 67).
- Выберите шаблон сертификата Подчинённого Центра сертификации (например, предварительно подготовленный шаблон путём редактирования клонированного предустановленного шаблона Центра сертификации в разделе «Шаблоны»).

Срок действия сертификата Подчиненного Центра сертификации определяется шаблоном «Sub CA»¹, но не превышает срок действия сертификата Корневого Центра сертификации.

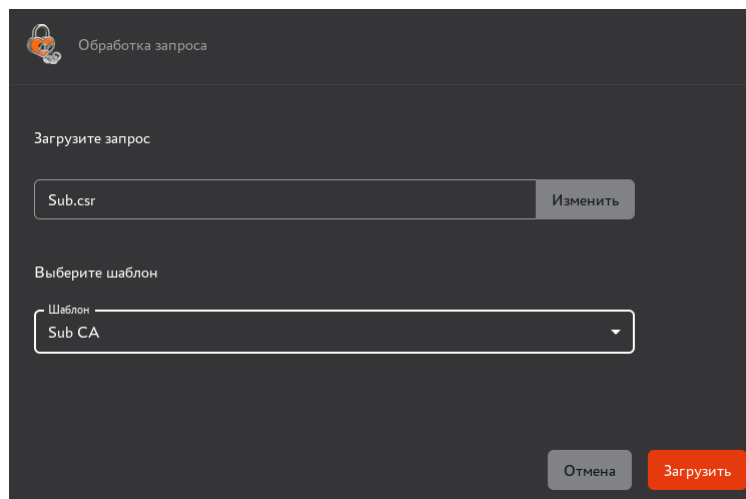


Рисунок 67 – Окно выбора файла запроса

На текущем шаге, после выбора файла запроса, возможно изменить выбор, нажав кнопку **<Изменить>** (см. Рисунок 67).

- Нажмите кнопку **<Загрузить>** (см. Рисунок 67).

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 Подчиненного Центра сертификации успешно сформирован и подписан Корневым Центром сертификации (см. Рисунок 68).

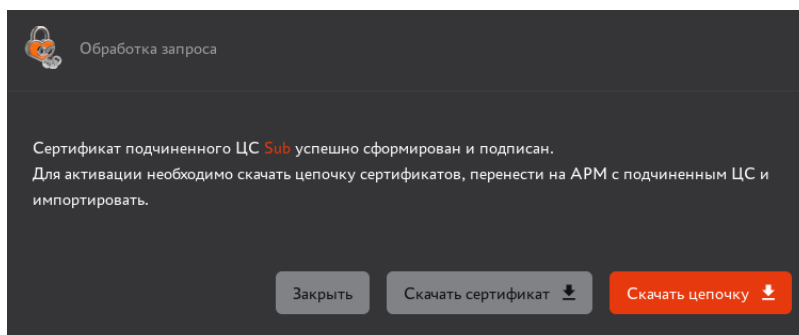



Рисунок 68 – Окно успешного формирования и подписи сертификата

- 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 Подчиненных 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 9.3.1.6 настоящего руководства.

¹ Про шаблон «Sub CA» см. в Приложении 2 «Описание полей предустановленных шаблонов сертификатов».

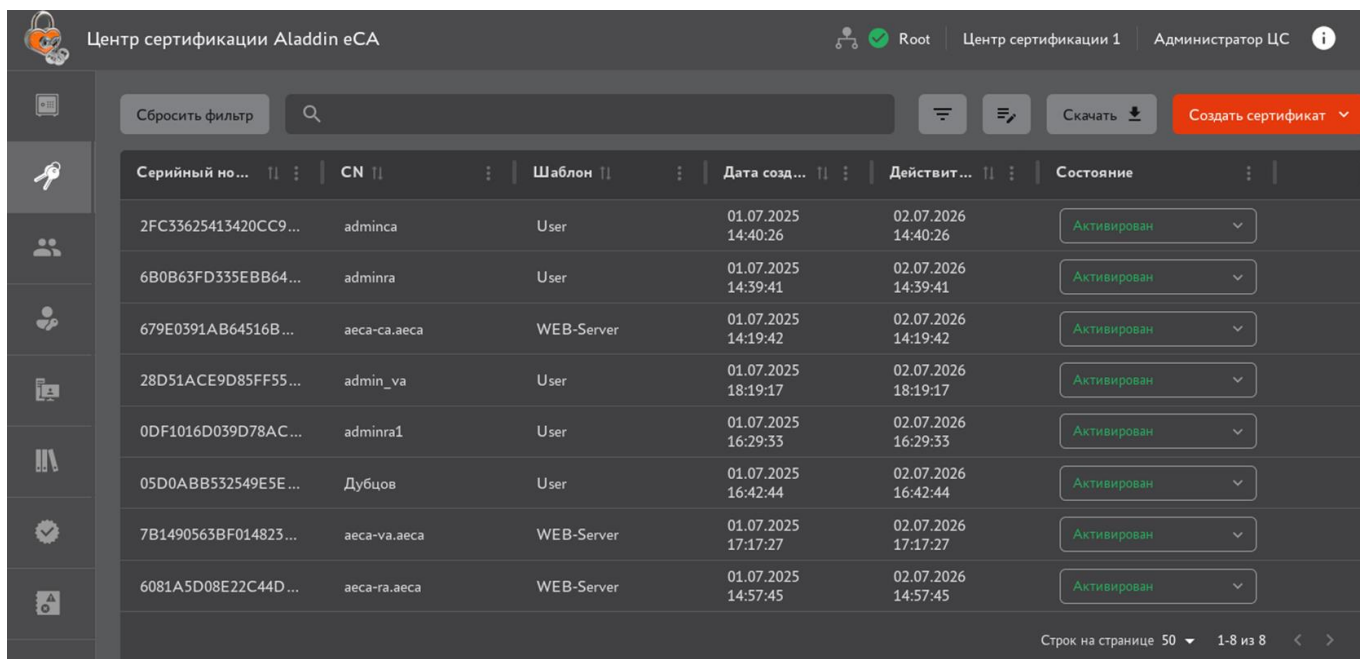
9.4 Раздел «Сертификаты»

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 40).

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



Центр сертификации Aladdin eCA

Root | Центр сертификации 1 | Администратор ЦС

Сбросить фильтр

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 69 – 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.

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.

9.4.1 Выпуск сертификата

Для выпуска сертификата для существующего или нового субъекта нажмите кнопку **<Создать сертификат>** и выберите способ создания из выпадающего списка (см. Рисунок 70):

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

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

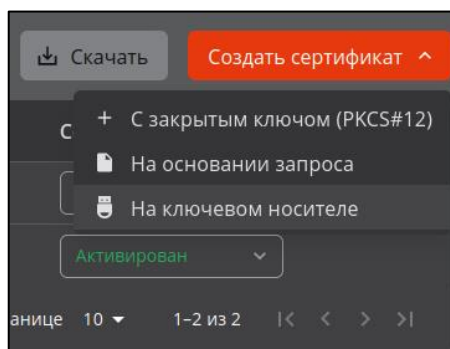


Рисунок 70 – Выпуск сертификата в разделе «Сертификаты»

9.4.2 Поиск сертификатов

Строка поиска (см. Рисунок 71) 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.

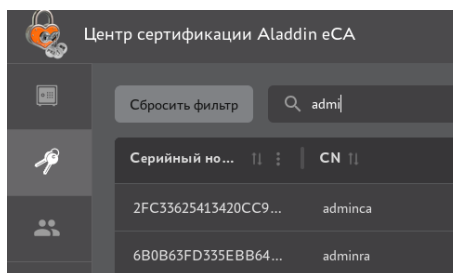



Рисунок 71 – Поисковая строка в разделе «Сертификаты»

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

9.4.3 Сортировка сертификатов

Средства сортировки выпущенных сертификатов представлены элементами выбора направления сортировки в заголовке таблицы экранной формы (см. Рисунок 72):

- «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.

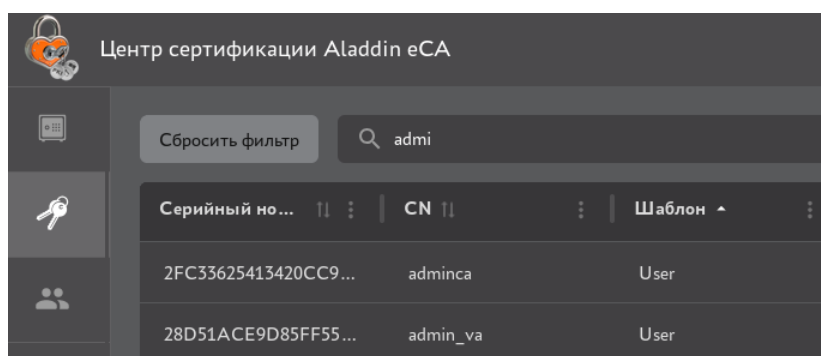




Рисунок 72 – Сортировка сертификатов

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 74).


9.4.4 Фильтрация сертификатов


9.4.4.1 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 73):

- 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 .

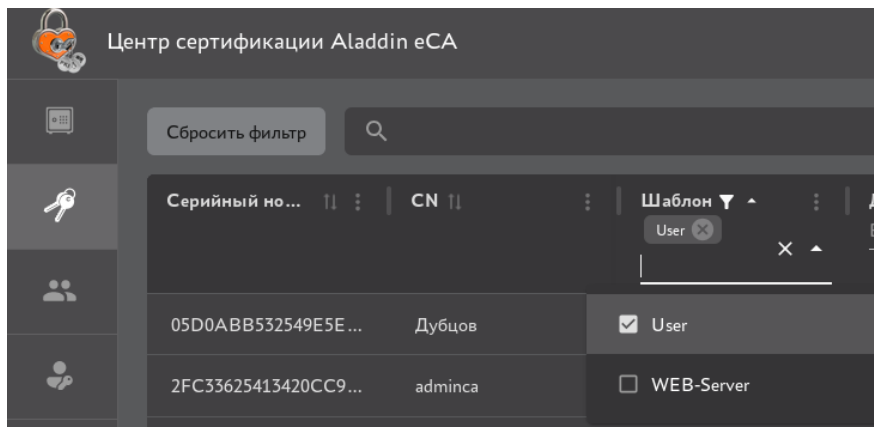



Рисунок 73 – Поля фильтра заголовков экранной таблицы

9.4.4.2 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 74);

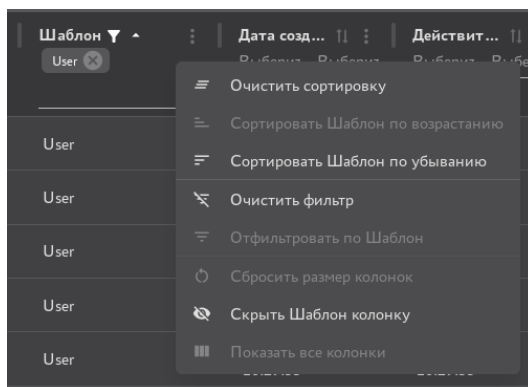
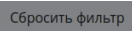



Рисунок 74 – Кнопка <Очистить> фильтр

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

9.4.5 Скачивание сертификатов

Для скачивания наведите указатель мыши на выбранный сертификат в экранной таблице, нажмите появившуюся кнопку  (см. Рисунок 69) и в раскрывшемся меню выберите пункт **<Скачать сертификат>** или **<Скачать цепочку>** в формате `.pem` (см. Рисунок 75).

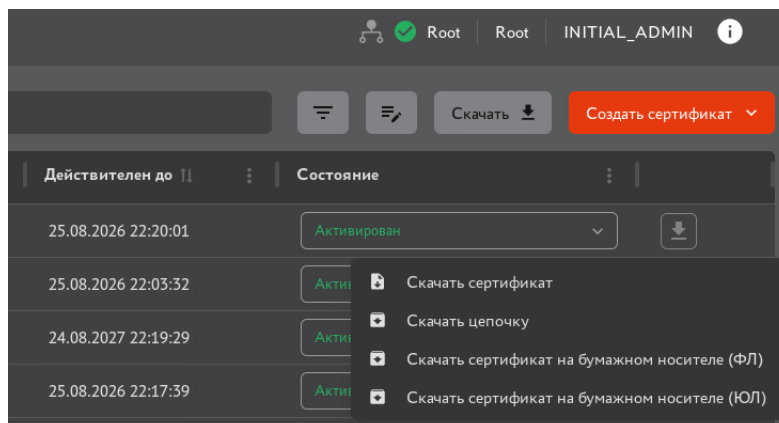



Рисунок 75 – Скачивание сертификата и цепочки сертификатов

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.

9.4.6 Статус сертификатов

Возможные варианты состояния и доступные действия над сертификатами в зависимости от состояния приведены в таблице 16.

Таблица 16 – 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 76).

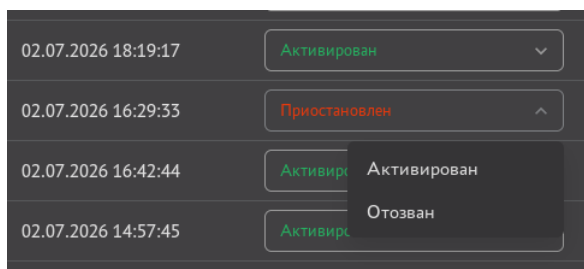


Рисунок 76 – Выпадающее меню смены состояния сертификата

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 77)

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».

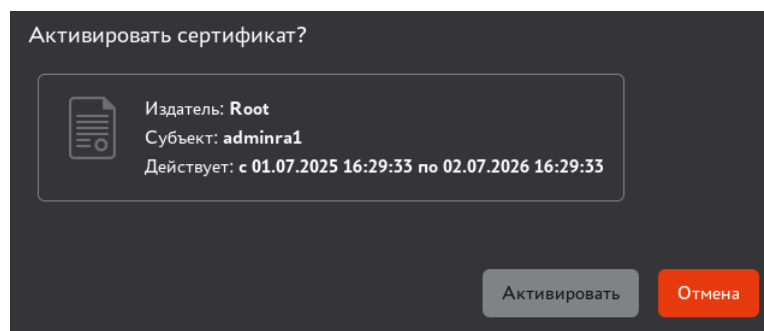


Рисунок 77 – Окно активации сертификата

- отзыв (см. Рисунок 78);

Внимание! Данную операцию нельзя отменить.

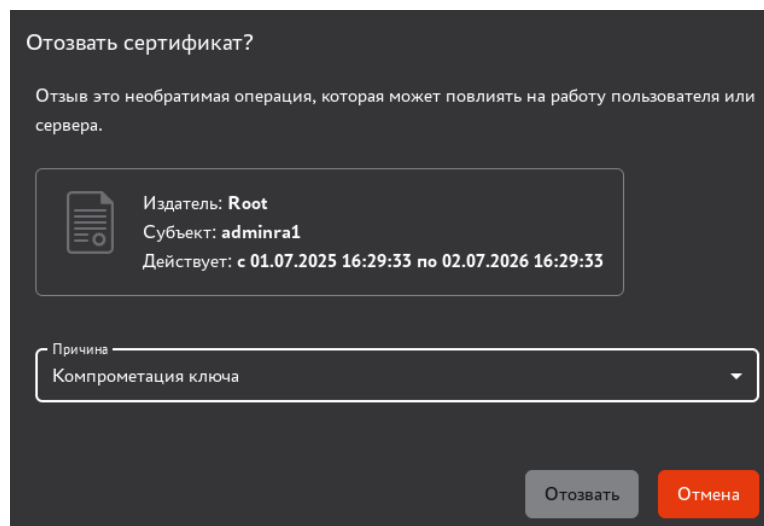


Рисунок 78 – Окно отзыва сертификата

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 79):

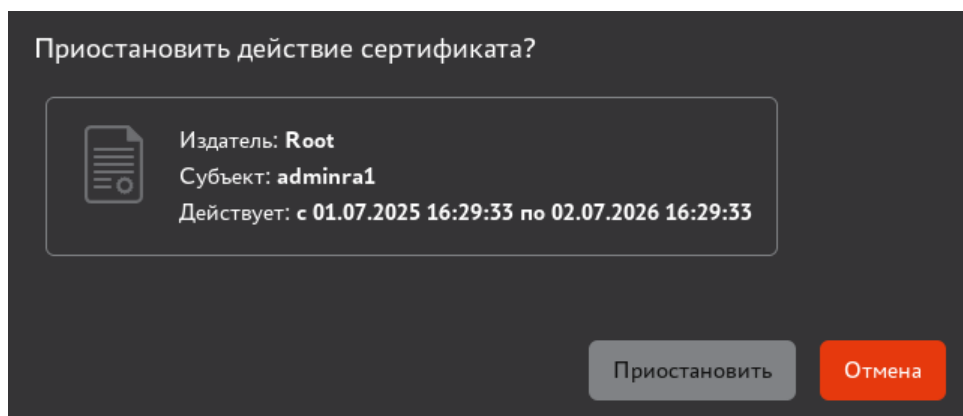


Рисунок 79 – Окно приостановки действия сертификата

9.4.7 Карточка сертификата

Просмотр данных сертификата возможен посредством страницы «Карточка сертификата».

Переход к экрану «Карточка сертификата» (см. Рисунок 80) осуществляется при нажатии на строку сертификата таблицы главного экрана раздела «Сертификаты» (см. Рисунок 69).

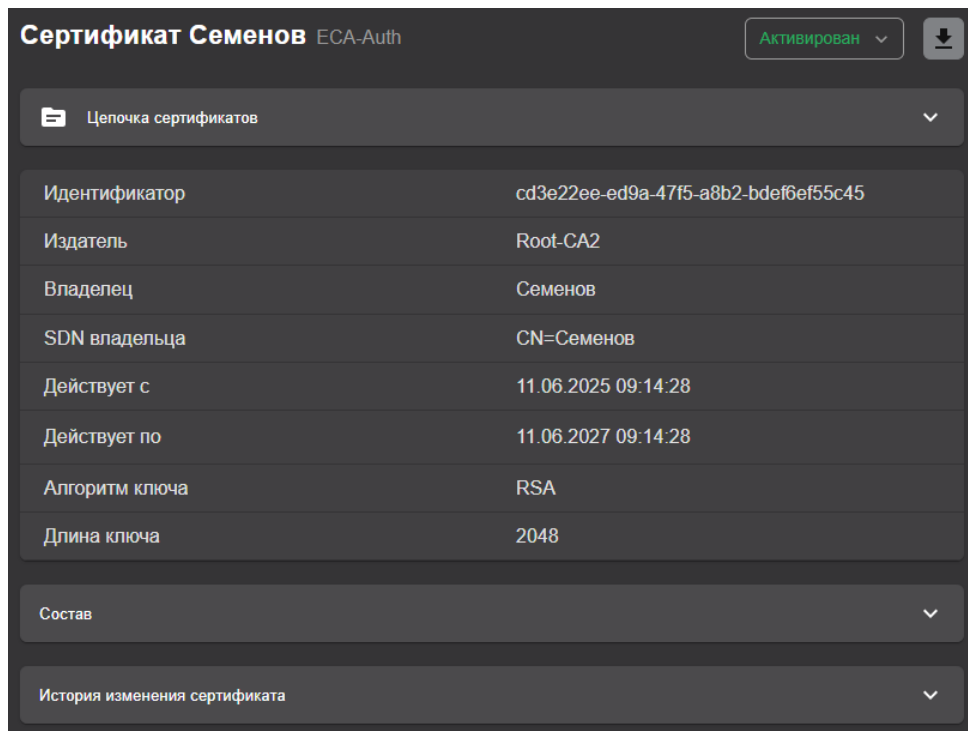


Рисунок 80 – Окно «Карточка сертификата»

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

16.

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 81) выберите <Скачать сертификат> субъекта или <Скачать цепочку сертификатов>.

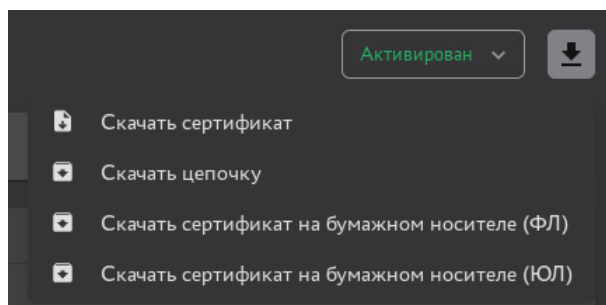




Рисунок 81 – Скачивание сертификата

Для изготовления и экспорта документа, содержащего значения полей данного сертификата (далее – сертификат на бумажном носителе) нажмите кнопку  и во всплывающем меню (см. Рисунок 81) 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 82).

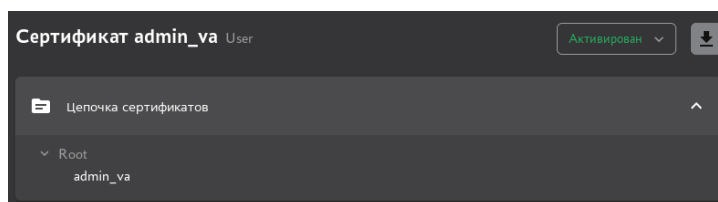



Рисунок 82 – Окно карточки сертификата. Подменю «Цепочка сертификатов»

- «Состав». Раскройте вкладку, нажав в строке с именем вкладки символ . На раскрывшемся экране отображены следующие поля (см. Рисунок 83):

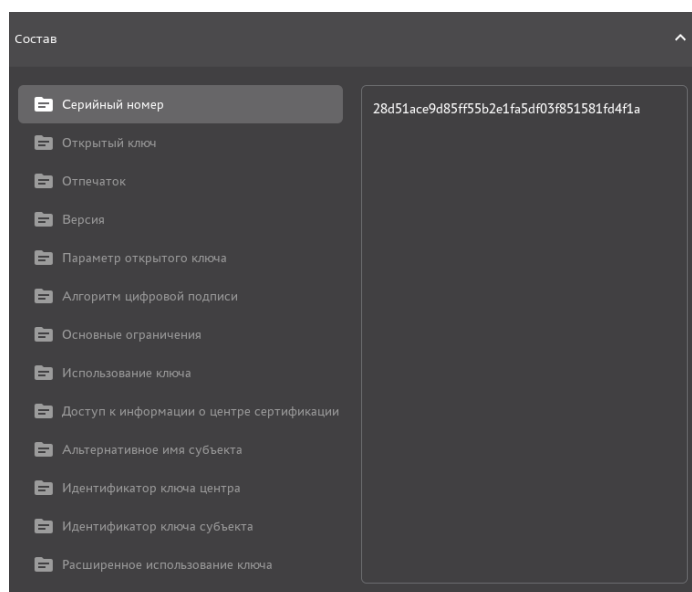



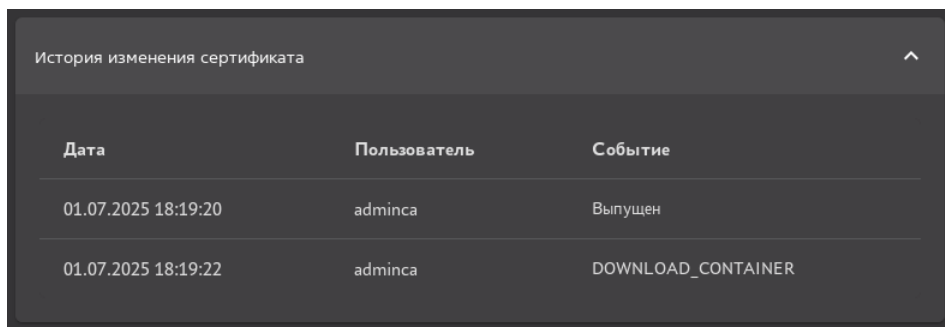
Рисунок 83 – Окно карточки сертификатов. Вкладка «Состав»

– 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 84):
 - дата – дата совершенного действия;
 - пользователь – учётная запись, под которой было совершено данное действие;
 - событие – действие, совершённое над сертификатом.



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


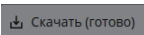
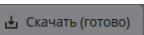
Рисунок 84 – Окно карточки сертификатов. Вкладка «История изменения сертификата»

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

9.4.8 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 . Происходит формирование списка сертификатов, по завершению действия и готовности к выгрузке списка сертификатов кнопка переходит в состояние . Нажмите кнопку  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.

9.4.9 Массовые операции с сертификатами

Порядок выполнения массовых операций с сертификатами:

- Для запуска мастера массовых операции с сертификатов нажмите кнопку  **<Массовые операции>** (см. Рисунок 85).

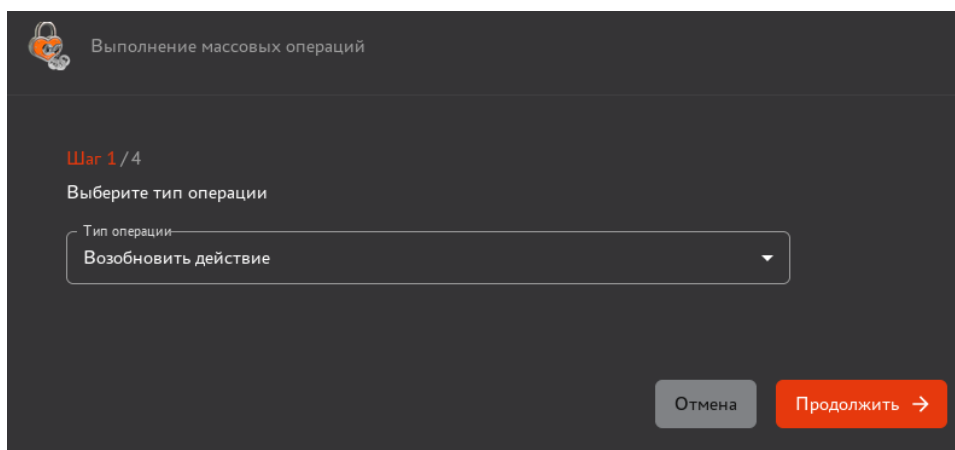




Рисунок 85 – Окно выполнения массовых операций. Шаг 1

- Выберите необходимую операцию из раскрывающегося списка и нажмите кнопку **<Продолжить>**.
Доступны следующие типы операций:
 - возобновление действия;
 - приостановить;
 - отозвать.

При выборе операции «Отозвать» дополнительно необходимо будет указать причину отзыва из выпадающего списка.
- На следующем шаге, до применения поиска в левом столбце окна будут отображены первые 100 сертификатов с соответствующим статусом (в зависимости от выбранной операции на шаге 1) в алфавитном порядке по атрибуту Common Name. В случае, если найдено более 100 сертификатов соответствующего выбранной операции статуса, то требуется уточнить параметры поиска сертификатов.

Также возможно осуществить поиск сертификатов по отличительному имени субъекта Subject Distinguished Names, для которых требуется применить выбранную операцию, в левом столбце окна Шаг 2 (см. Рисунок 86). Поиск сертификатов производится с учётом текущего статуса сертификата и выбранного типа операции на шаге 1, отображается не более 100 результатов поиска, для выбора более 100 сертификатов требуется уточнить и повторить поиск.

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

- Выберите, найденные сертификаты, отметив их флажками .
- Перенесите отмеченные флажками сертификаты в правую часть окна, нажав кнопку , которая находится между правой и левой частью окна выполнения операции.

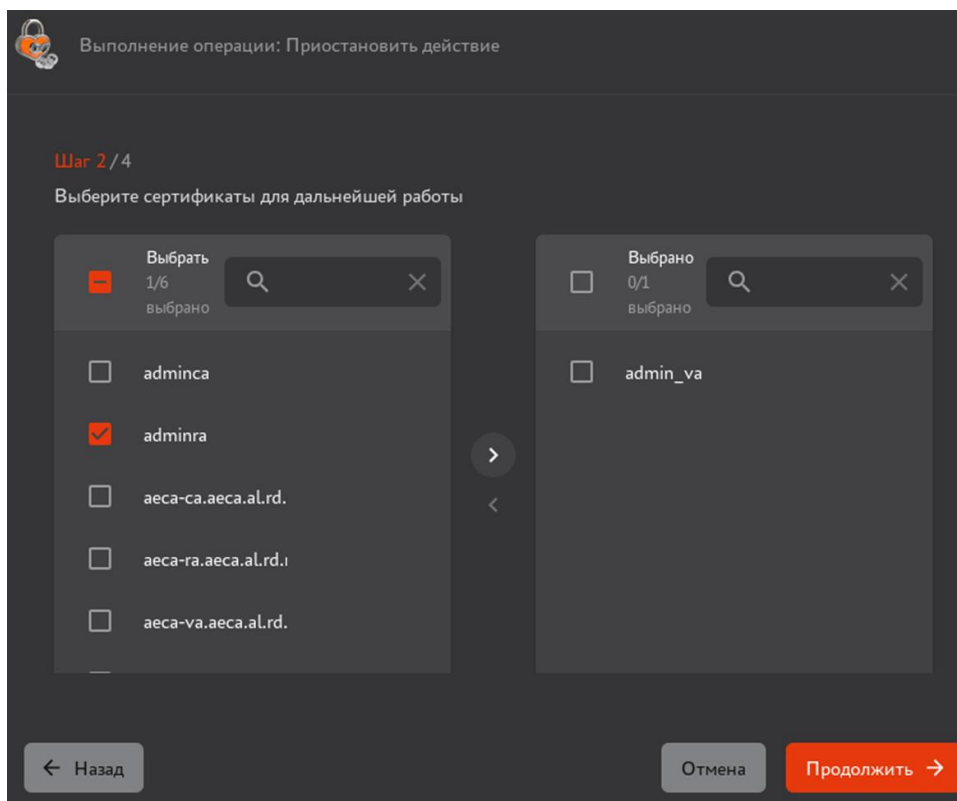



Рисунок 86 – Окно выполнения массовых операций. Шаг 2. Создание списка выбранных сертификатов

- В случае необходимости исключения из выбранных сертификатов, к которым будет применена массовая операция, отметьте флажками сертификата из списка в правой части окна, и нажмите кнопку .
- Для перехода на следующий шаг нажмите кнопку **<Продолжить>**.
- В открывшемся окне подтвердите действие, нажав кнопку **<Применить>** (см. Рисунок 87).

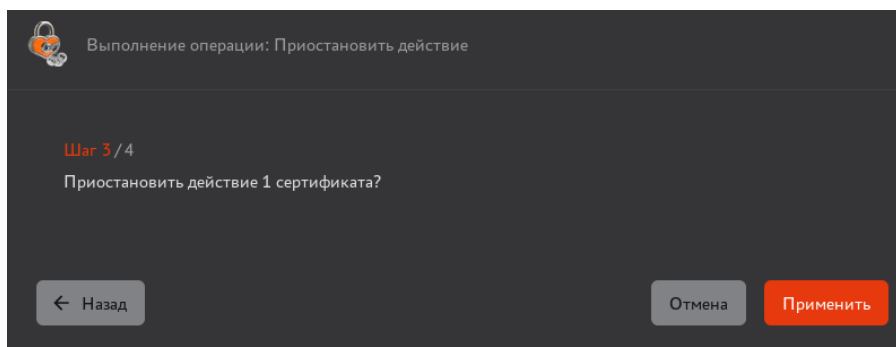


Рисунок 87 – Окно выполнения массовых операций. Шаг 3

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

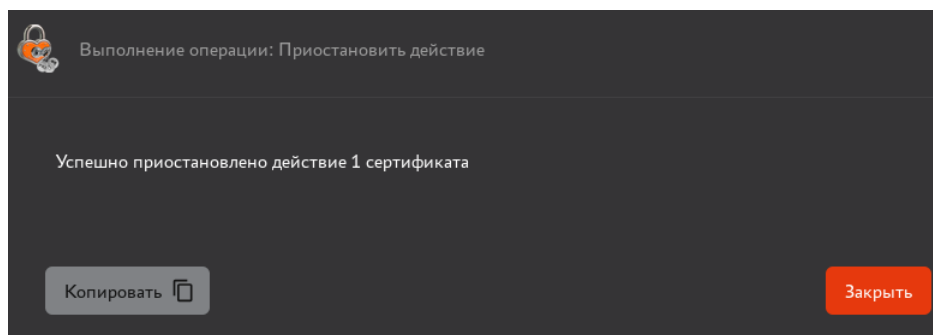


Рисунок 88 – Окно выполнения массовых операций. Шаг 4

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

9.5 Настройка уведомлений об истечении срока действия сертификата

Центр сертификации Aladdin eCA поддерживает возможность уведомления пользователей (субъектов ресурсных систем) по электронной почте об истечении срока действия их сертификатов.

Отправка уведомлений об истечении срока действия сертификата фиксируется в Журнале событий с кодом CAENV054 «Отправка уведомления на почту».

При использовании настроек по умолчанию программа однократно отправит электронные письма с уведомлением по следующему расписанию:

- 30 дней до истечения срока;
- 7 дней до истечения срока;
- 1 день до истечения срока.

По умолчанию уведомления отправляются на адреса электронной почты, указанные в атрибуте «RFC 822 Name» субъекта ресурсной системы, срок действия сертификата которых истекает. Если в атрибуте «RFC 822 Name» адрес электронной почты не указан, письма отправляются на адрес, указанный в атрибуте «MS UPN, UserPrincipalName».

Условия выполнения уведомления об истечении срока действия сертификата субъекта:

- Статус сертификата, срок которого истекает – активный.
- Для субъекта, сертификат которого истекает, определен адрес электронной почты в атрибуте «RFC 822 Name» или «MS UPN, UserPrincipalName».
- Выполнена настройка параметров конфигурационного файла `event-delivery.env`, расположенного в каталоге `/opt/aecaCa/dist/environment/`, настройка которого выполняется посредством настройки конфигурационного файла `/opt/aecaCa/scripts/config.sh`.
- Выполнена настройка почтовой программы.
- Создан и настроен хотя бы один шаблон уведомлений.

9.5.1 Настройка параметров конфигурационного файла `config.sh`

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

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

Описание параметров конфигурационного файла для настройки уведомлений об истечении срока действия сертификата приведено в таблице 17.

Таблица 17 – Переменные окружения для настройки почтовых уведомлений

Параметр	Значение параметра по умолчанию	Описание
email_host	127.0.0.1	Укажите ip-адрес почтового сервера
email_port	25	Укажите порт почтового сервера
email_login	aeca	Укажите логин пользователя, под которым производится авторизация в почтовом сервере
email_password	aeca	Введите пароль пользователя, под которым производится авторизация в почтовом сервере
email_from	no_reply@aeca.kg	Укажите адрес почты, с которой будет производиться рассылка уведомлений
email_schedule	'0 0 12 * * *'	Укажите период проверки в виде CRON-выражения, по которому будет выполняться проверка сроков действия сертификатов и рассылка уведомлений (по умолчанию – каждый день в полдень (12:00))
email_enabled	true	Флаг отправки почтовых уведомлений, если выкл. То сообщения не отправляются, но помечаются, как отправленные
email_protocol	smtp	Протокол подключения к почтовому серверу
email_smtp_auth	false	Флаг: использование SMTP-авторизации
email_start_tls	false	Флаг: использование директивы start tls при подключении к почтовому серверу

Для применения внесенных настроек следует запустить сценарий обновления, выполнив команду с правами суперпользователя:

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

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

9.5.2 Настройка шаблонов уведомлений об истечении срока действия сертификата

В базе данных в таблице «`delivery.delivery_template`» хранится набор шаблонов рассылки уведомлений. Каждый шаблон определяет следующие параметры отправки уведомления:

- Наименование шаблона.
- Признак необходимости уведомления по этому шаблону.
- Отслеживание времени окончания срока действия сертификата, для отправки уведомлений в установленный в шаблоне срок.
- Тему письма, указанную при отправке уведомления.

По умолчанию созданы шаблоны, описанные в таблице 18.

Таблица 18 – Шаблоны, настроенные по умолчанию

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

Уведомление формируется по следующим правилам:

- тема письма в соответствии с указанной в шаблоне;
- текст письма в соответствии с данными сертификата в следующем формате:

```
Здравствуйте, {certificate.username}!
Время действия сертификата истекает {certificate.expire_date}
Фингерпринт сертификата: {certificate.fingerprint}
Серийный номер сертификата: {certificate.serial_number}
```

Для просмотра списка существующих шаблонов уведомлений выполните команду:

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

Для редактирования шаблона выполните команду:

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

где:

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

Пример редактирования шаблона уведомления:

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

Для создания нового шаблона уведомлений выполните команду:

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

где:

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

Пример создания нового шаблона уведомлений:

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

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

(4 строки)

Для применения внесенных настроек перезапустите сервис, выполнив команду:

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

9.5.3 Настройка параметров почтового ящика пользователя

Указанный в конфигурационном файле почтовый ящик пользователя, должен иметь следующие настройки:

- Разрешен доступ к почтовому ящику с помощью почтовых клиентов.
- Отключить автоматическое удаление писем, помеченных в IMAP как удалённые.
- Разрешить доступ по протоколу POP3.

9.5.3.1 Настройка почтовой программы Яндекс.Почта

Настройка почтовой программы показана на примере настройки Яндекс.Почта (см. Рисунок 89):

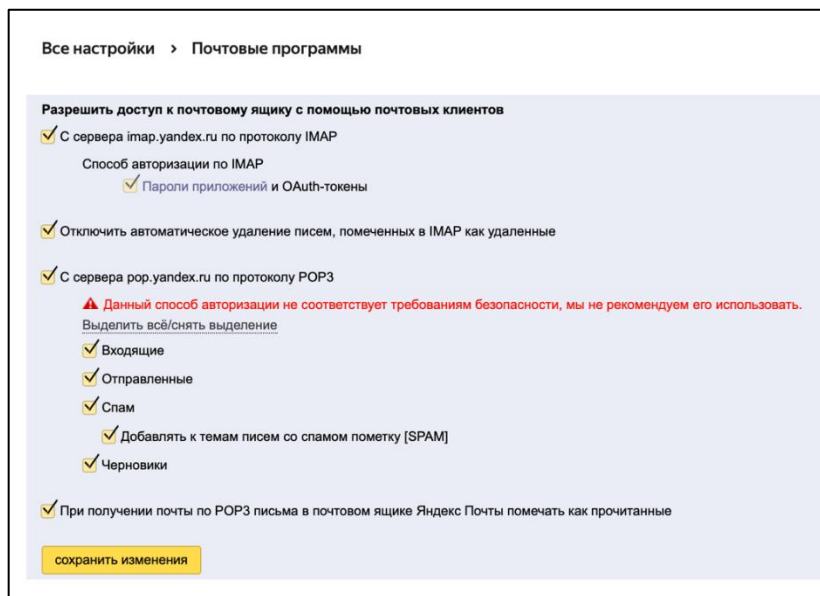


Рисунок 89 – Настройки почтового ящика Яндекс.Почта для получения уведомления

1. В настройках аккаунта Яндекс.Почты выберете пункт меню «Безопасность» (см. Рисунок 234).

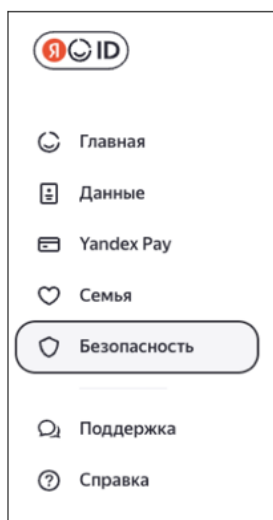


Рисунок 90 – Раздел «Безопасность» аккаунта почтового ящика Yandex

- Перейдите в раздел «Доступ к вашим данным» (см. Рисунок 91).

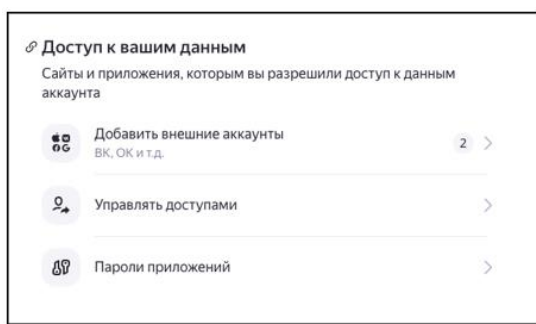


Рисунок 91 – Подраздел «Доступ к вашим данным» аккаунта почтового ящика Yandex

- Перейдите в подраздел «Пароли приложений» (см. Рисунок 92).

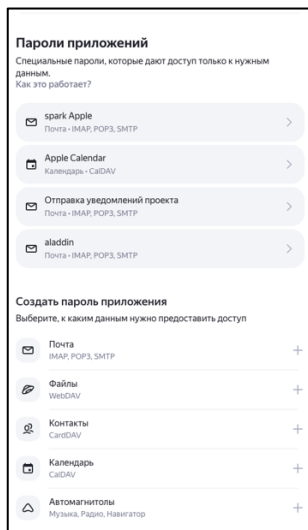


Рисунок 92 – Подраздел «Пароли приложений» аккаунта почтового ящика Yandex

- Перейдите в подраздел «Почта», «Создать пароль приложения» (см. Рисунок 93).

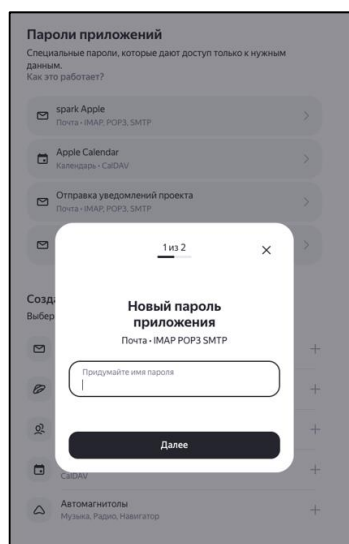


Рисунок 93 – Создание пароля приложения

Новый пароль необходимо сохранить. При потере восстановление невозможно. Возможен сброс и создание нового. Данный пароль необходимо внести в конфигурационный файл `config.sh` в параметр `email_password`

9.5.3.2 Настройка почтовой программы MS Exchange

- Настройка почтовой программы показана на примере настройки MS Exchange (см. Рисунок 94). Убедитесь, что настроен протокол SMTP в настройках MS Exchange.

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

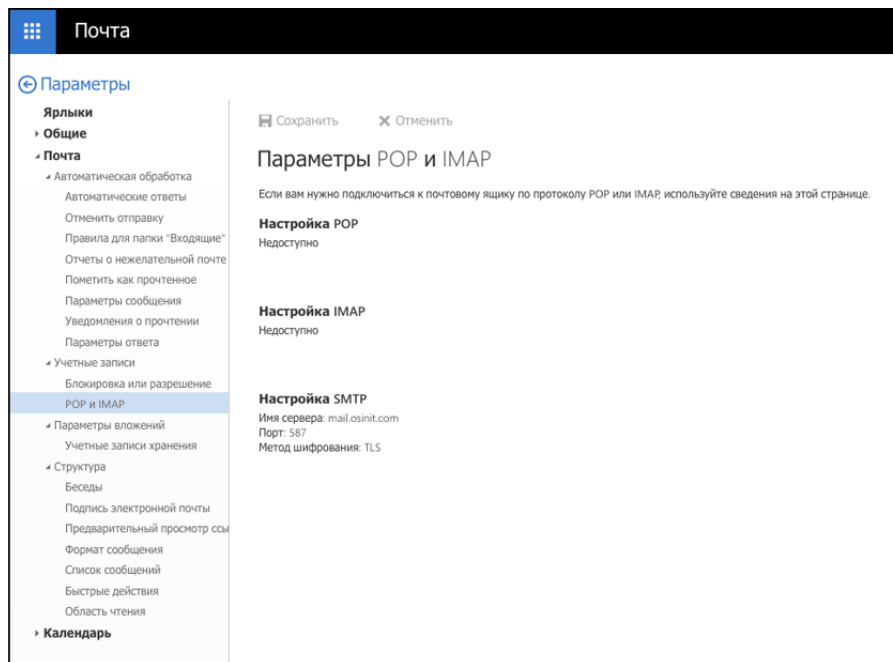


Рисунок 94 – Настройки почтового ящика MS Exchange для получения уведомления

9.6 Раздел «Учётные записи»

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

Переход к разделу «Учётные записи» осуществляется по выбору раздела «Учётные записи» бокового меню, расположенного слева на главном экране (см. Рисунок 95).

На экране раздела «Учётные записи» отображены следующие поля:

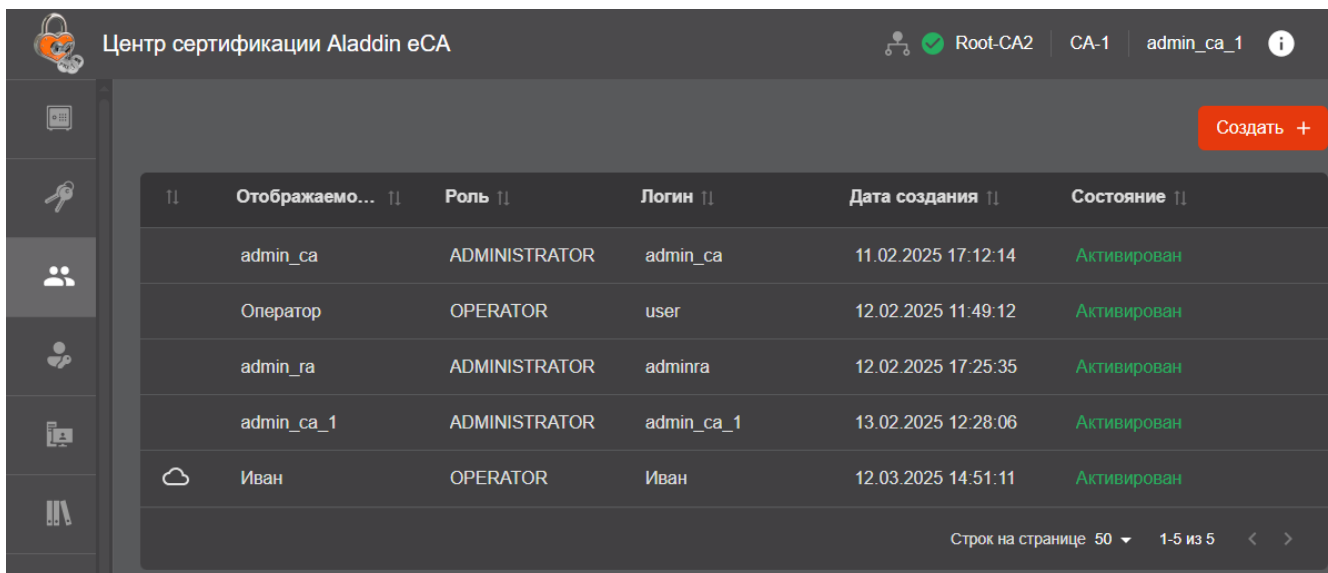



Рисунок 95 – Экран раздела меню «Учётные записи»

-  – соответствующий символ обозначает, что данная учётная запись создана для субъекта внешней (подключенной) ресурсной системы;
- отображаемое имя – идентифицирует владельца учетной записи, соответствует полю «Отображаемое имя» в окне создания учётной записи;
- роль – указывает набор дискретных прав. Возможные роли:

- Оператор – обладает правами на работу с субъектами группы, над которой он может осуществлять свои ролевые права, и принадлежащими им сертификатами (выпуск, отзыв, приостановка и возобновление сертификата), имеет полномочия запуска обновления списка субъектов. Таким образом оператору доступны следующие разделы:
 - «Сертификаты», где доступны сертификаты субъектов, на которые оператору предоставлены права в соответствии с правилами доступа.
 - «Субъекты», где доступны субъекты ресурсных систем, на которые оператору предоставлены права в соответствии с правилами доступа, и принадлежащим им сертификатам, без прочих ограничений.
 - «Ресурсные системы», где доступен запуск синхронизации субъектов ресурсной системы, на которую оператору предоставлены права в соответствии с правилами доступа.
 - «Шаблоны», где доступен просмотр шаблонов, на которые оператору предоставлены права в соответствии с правилами доступа.
- Администратор – обладает неограниченными возможностями, в том числе имеет доступ к управлению учетными записями и может делегировать полномочия Оператору на просмотр и использование шаблонов при создании сертификатов для субъектов, а также на работу с субъектами групп безопасности ресурсных систем;
- логин – показывает параметр учетной записи для авторизации, содержит Common Name субъекта. Логины учетных записей должны быть уникальными;
- дата создания – показывает дату создания учётной записи;
- состояние – отображает состояние учётной записи (активирован или заблокирован).

Вход под учётной записью пользователя на сервер осуществляется при помощи сертификата, выпущенного с использованием шаблона «Web-client». Подробнее о настройке аутентификации для входа в учётную запись см. раздел 6 настоящего руководства.

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


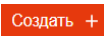
- успешная аутентификация, включая аутентификацию в Центре регистрации Aladdin eRA;
- успешное обновление маркера доступа, включая его обновление в Центре регистрации Aladdin eRA.

Центр сертификации Aladdin eCA автоматически блокирует учетные записи пользователей с ролью «Оператор», период пассивности которых превысил значение, указанное в параметре `block_inactive_account_delay`¹ 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`² конфигурационного файла.

Внимание! При обновлении ПО с версии 2.1.2 до версии 2.3 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.

9.6.1 Создание учётной записи пользователя локального ресурса

Порядок создания учетной записи для пользователя Центра сертификации Aladdin eCA:

- На панели слева выберите раздел «Учетные записи» .
- Нажмите кнопку  (см. Рисунок 95).
- В открывшемся окне выполните следующие действия (см. Рисунок 96):
 - выберите роль учетной записи;

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

² По умолчанию – каждую полночь.

- укажите имя, которое отображается на верхней панели веб-интерфейса после авторизации пользователя;
- логин – имя учетной записи (данные для поля «Common Name» при выпуске сертификата пользователя).

Внимание! Логин (имена) учетных записей должны быть уникальными.

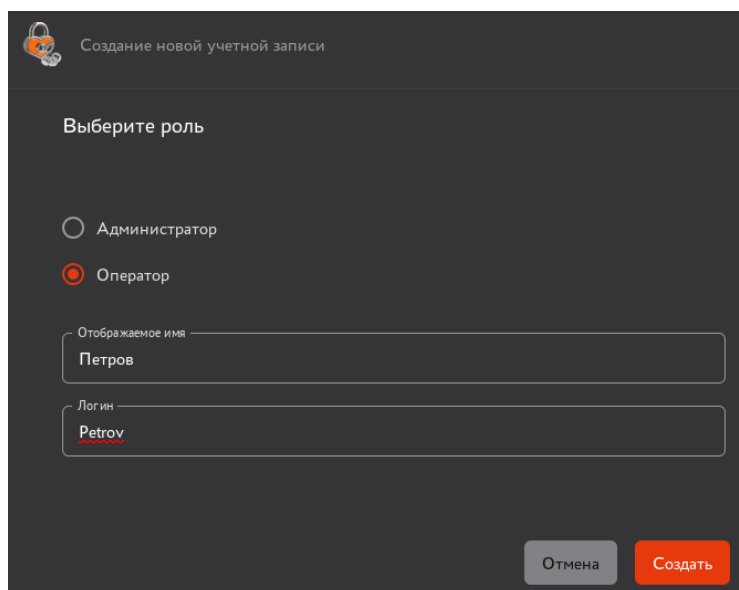


Рисунок 96 – Окно создания новой учётной записи локального пользователя

- Нажмите кнопку **Создать**.

Для созданной учетной записи пользователя с ролью «Оператор» создайте правила доступа шаблонам и субъектам (см. раздел 9.6.5).

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

9.6.2 Создание учетной записи для подключенного субъекта

Для создания учётной записи доменного пользователя перейдите в раздел «Субъекты» и создайте учётную запись в соответствии с разделом 9.8.8 настоящего руководства.

9.6.3 Изменение статуса учётной записи

При наведении курсора на строку с данными выбранной учётной записи отображаются инструменты управления учетной записью (возможность управления статусом текущей учётной записи) (см. Рисунок 97):

- 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.

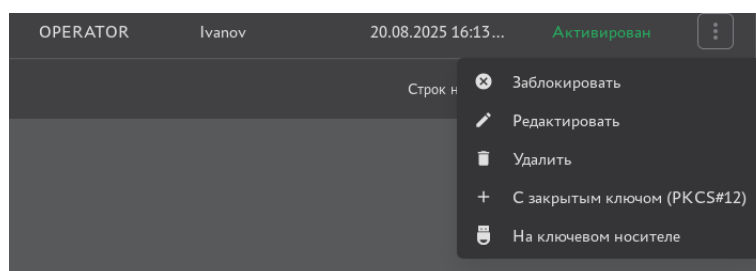

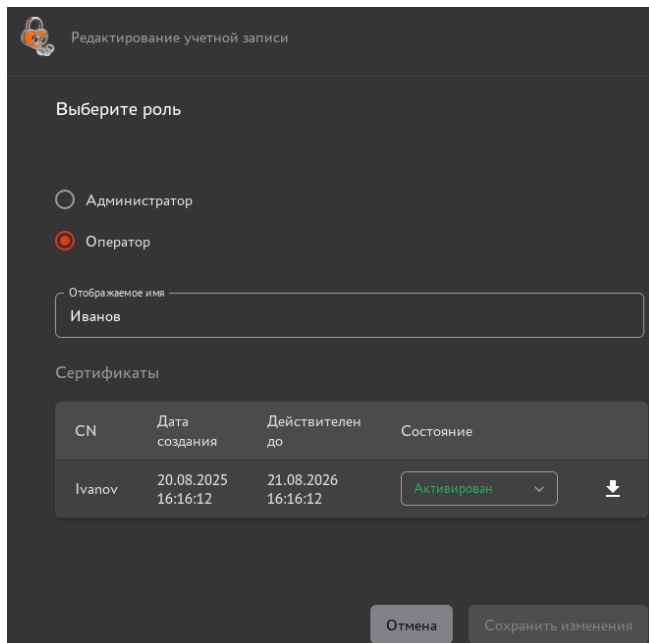


Рисунок 97 – Доступные действия над учетными записями

9.6.4 Редактирование учётной записи

По нажатию на кнопку **<Редактировать>**  (в строке учётной записи) открывается карточка учётной записи, содержащая следующие поля (см. Рисунок 98):



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

Рисунок 98 – 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 16), 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.

9.6.5 Назначение прав оператору

Для назначения прав оператору перейдите в раздел «Правила доступа» и произведите назначение прав в соответствии с разделом 9.7 настоящего руководства.

9.6.6 Удаление учётной записи

По нажатию на кнопку **<Удалить>**  (в строке учётной записи) открывается окно подтверждения удаления учётной записи (см. Рисунок 99)

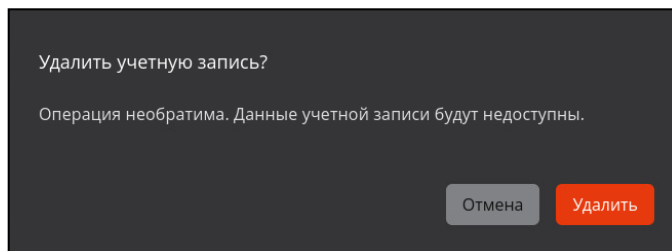



Рисунок 99 – Окно подтверждения удаления учётной записи

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

9.6.7 Выпуск сертификата для учётной записи

По нажатию на кнопку **<Создать сертификат>**  (в строке учётной записи) в выпадающем меню выберите способ выпуска (см. Рисунок 100):

- с закрытым ключом;
- на ключевом носителе.

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

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

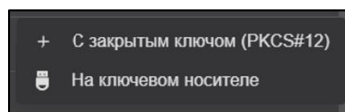


Рисунок 100 – Раздел «Учетные записи». Кнопка выпуска сертификата

9.7 Раздел «Правила доступа»

Раздел «Правила доступа» обеспечивает возможность предоставления пользователям с ролью «Оператор», а также группам безопасности зарегистрированных ресурсных систем¹ доступа на:

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

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

Переход в раздел «Правила доступа» осуществляется через боковое меню, расположенное слева на главном экране (см. Рисунок 40).

В данном разделе отображаются все существующие правила доступа (см. Рисунок 101).

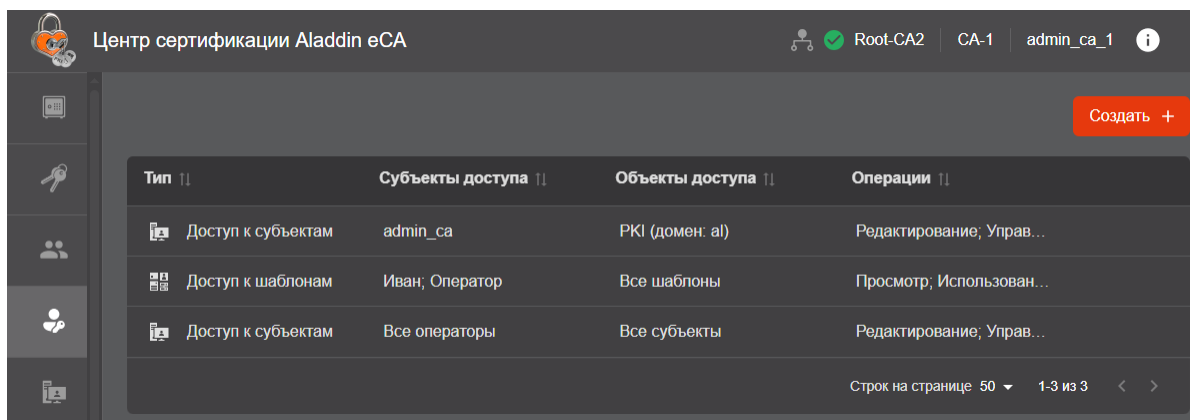


Рисунок 101 – Экран раздела меню «Правила доступа»

На экране раздела «Правила доступа» отображены информационные элементы (табличные поля):

¹ Назначение правил доступа группам безопасности зарегистрированных ресурсных систем предназначено обеспечивать возможность для наследования данных правил операторами, учетные записи которых созданы на основе субъектов данных групп безопасности.

- поле «Тип», отображающее тип правила доступа. Допустимые варианты значений в данном поле:
 - Доступ к шаблонам;
 - Доступ к субъектам.
- поле «Субъекты доступа», содержащее перечень пользователей с ролью «Оператор», а также групп безопасности зарегистрированных ресурсных систем, которым предоставлен доступ в соответствии с правилом;
- поле «Объекты доступа», содержащее перечень объектов доступа в соответствии с данным правилом. Объектами доступа в зависимости от типа правила могут являться шаблоны или группы безопасности;
- поле «Операции», содержащее перечень допустимых операций, которые могут выполнять субъекты доступа с объектами доступа.

Доступны следующие операции по работе с правилами доступа:

- просмотр списка правил доступа;
- создание нового правила доступа;
- редактирование правила доступа;
- удаление правила доступа.

Внимание! При обновлении Aladdin eCA CE с версии 2.1.2 на 2.3 в правилах доступа субъекты или объекты доступа, являющиеся подразделениями зарегистрированных ресурсных систем, будут удалены. Если в правиле доступа все субъекты или объекты доступа являются подразделениями зарегистрированных ресурсных систем, то такое правило будет удалено. Субъекты локальной ресурсной системы перестают быть членами подразделения «Local». Все субъекты локальной ресурсной системы становятся членами группы «Локальные субъекты».

9.7.1 Создание правила доступа

Порядок создания правила доступа:

- По нажатию кнопки **<Создать +>** на главном экране раздела «Правила доступа» происходит запуск сценария создания правила доступа.
- В открывшемся окне «Создание правила доступа» на шаге 1 выберите тип правила доступа из следующих вариантов (см. Рисунок 102):
 - Доступ к шаблонам (выбран по умолчанию);
 - Доступ к субъектам.

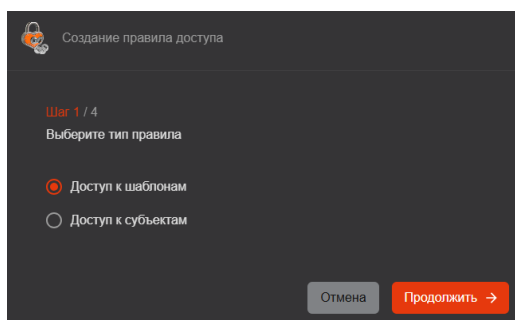


Рисунок 102 – Шаг 1 окна «Создание правила доступа»

- На шаге 2 окна «Создание правила доступа» выберите субъекты доступа. Допустимые варианты выбора субъектов доступа:
 - выбор перечня субъектов доступа вручную при включении режима «Выбрать операторов или группы» (см. Рисунок 103). При выборе данного режима доступен выбор типа субъектов доступа (оператор или группа) для отображения. В поле «Выбрать» необходимо выбрать субъекты доступа, при необходимости воспользовавшись поиском, затем перенести их в поле «Выбрано» путем нажатия на стрелку вправо. В поле «Выбрано» будут присутствовать все ранее добавленные в него субъекты доступа вне зависимости от того, какой тип для отображения субъектов доступа выбран для поля «Выбрать». Для исключения субъектов доступа из поля «Выбрано» необходимо выделить

их и перенести обратно в поле «Выбрать» путем нажатия на стрелку влево. В случае, если в поле «Выбрано» не добавлен ни один субъект доступа, переход на следующий шаг недоступен;

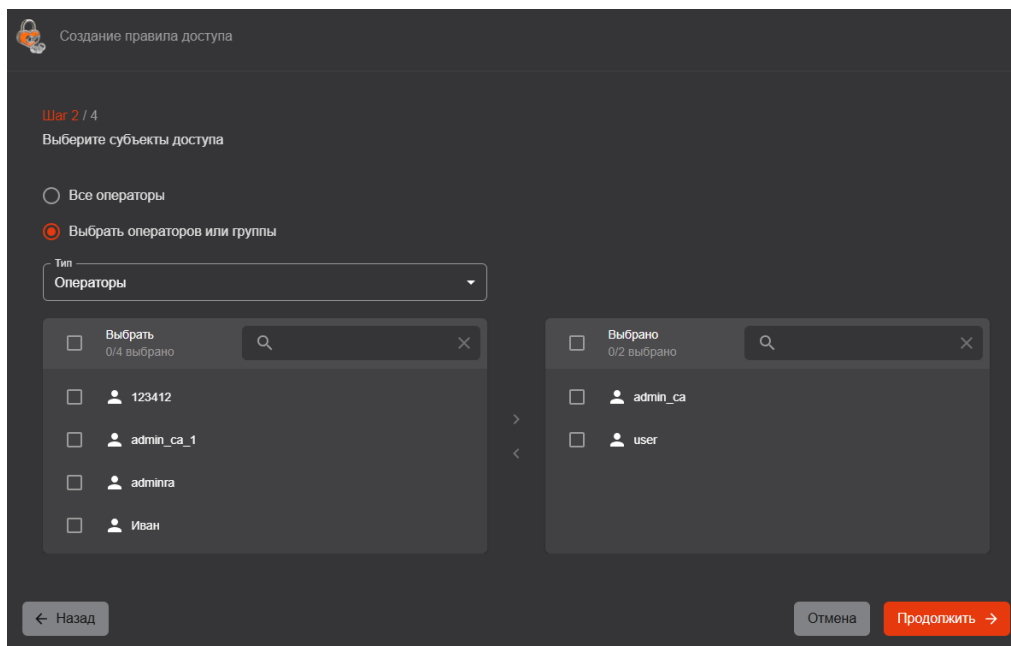


Рисунок 103 – Шаг 2 окна «Создание правила доступа» при выборе режима «Выбрать операторов или группы»

- выбор всех операторов или групп при включении режима «Все операторы» (см. Рисунок 104). При выборе данного режима субъектами доступа будут являться все пользователи с ролью «Оператор», а также все группы безопасности зарегистрированных ресурсных систем (в том числе те, которые будут созданы или получены из ресурсной системы позднее). В данном режиме указание отдельных операторов или групп на данном шаге недоступно.

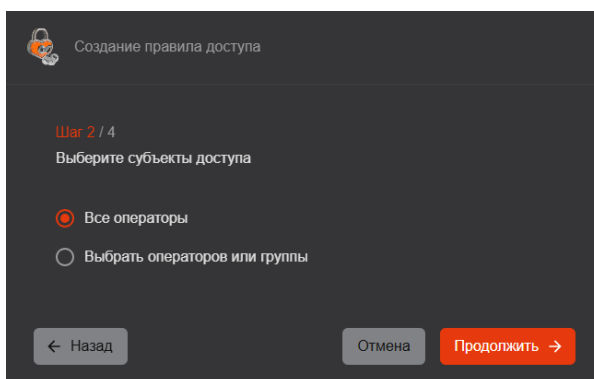


Рисунок 104 – Шаг 2 окна «Создание правила доступа» при выборе режима «Все операторы»

- Переход на следующий шаг осуществляется по ставшей активной кнопке **<Продолжить>** после выбора субъектов доступа.
- В окне «Создание правила доступа» на шаге 3 выберите объекты доступа.
- Если на шаге 1 был выбран тип «Доступ к шаблонам», то необходимо выбрать шаблоны, на просмотр и использование которых необходимо предоставить полномочия. Допустимые варианты выбора объектов доступа:
 - выбор шаблонов вручную при включении режима «Выбрать шаблоны» (см. Рисунок 105). В поле «Выбрать» необходимо выбрать шаблоны, при необходимости воспользовавшись поиском, затем перенести их в поле «Выбрано» путем нажатия на стрелку вправо. Для исключения шаблонов из поля «Выбрано» необходимо выделить их и перенести обратно в поле «Выбрать» путем нажатия на стрелку влево. В случае, если в поле «Выбрано» не добавлен ни один шаблон, переход на следующий шаг недоступен;

- выбор всех шаблонов при включении режима «Все шаблоны» (см. Рисунок 106). При выборе данного режима объектами доступа будут являться все шаблоны (в том числе те, которые будут созданы позднее). При выборе режима «Все шаблоны» указание отдельных шаблонов на данном шаге будет недоступно.

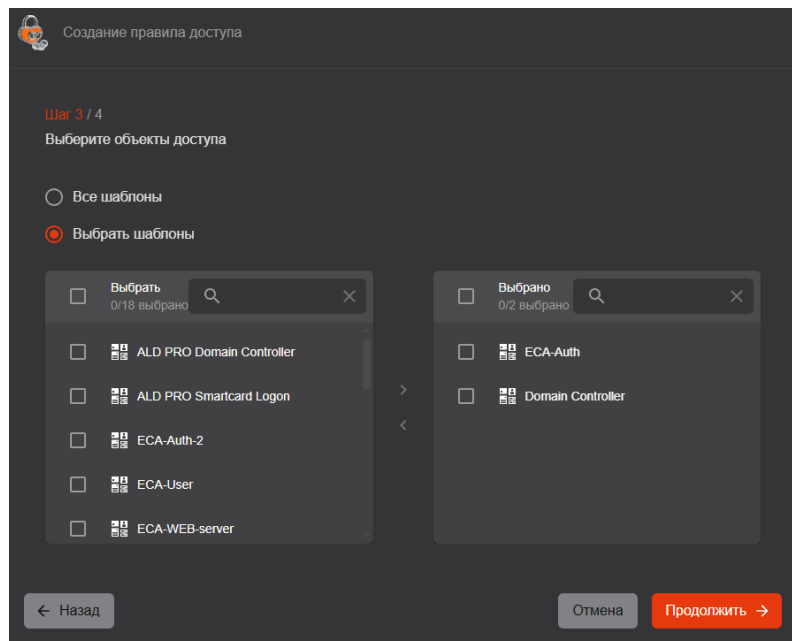


Рисунок 105 – Шаг 3 окна «Создание правила доступа» при выборе режима «Выбрать шаблоны»

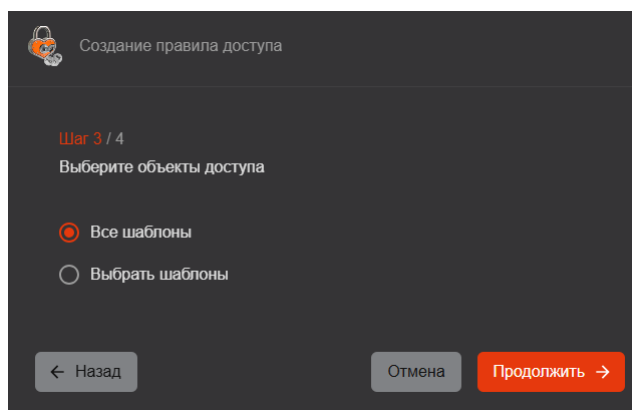


Рисунок 106 – Шаг 3 окна «Создание правила доступа» при выборе режима «Все шаблоны»

- Если на шаге 1 был выбран тип «Доступ к субъектам», то необходимо выбрать субъекты, на просмотр и использование которых необходимо предоставить полномочия. Допустимые варианты выбора объектов доступа:
 - выбор субъектов вручную при включении режима «Выбрать группы» (см. Рисунок 107). В поле «Домен» необходимо выбрать ресурсную систему. В поле «Выбрать» необходимо выбрать группы безопасности, при необходимости воспользовавшись поиском, затем перенести их в поле «Выбрано» путем нажатия на стрелку вправо. Для исключения групп безопасности из поля «Выбрано» необходимо выделить их и перенести обратно в поле «Выбрать» путем нажатия на стрелку влево. В случае, если в поле «Выбрано» не добавлены ни одна группа безопасности или ни один оператор, переход на следующий шаг недоступен;
 - выбор всех субъектов при включении режима «Все субъекты» (см. Рисунок 108). При выборе данного режима объектами доступа будут являться все субъекты зарегистрированных ресурсных систем (в том числе те, которые будут созданы позднее). При выборе режима «Все субъекты» указание отдельных групп безопасности зарегистрированных ресурсных систем на данном шаге будет недоступно.

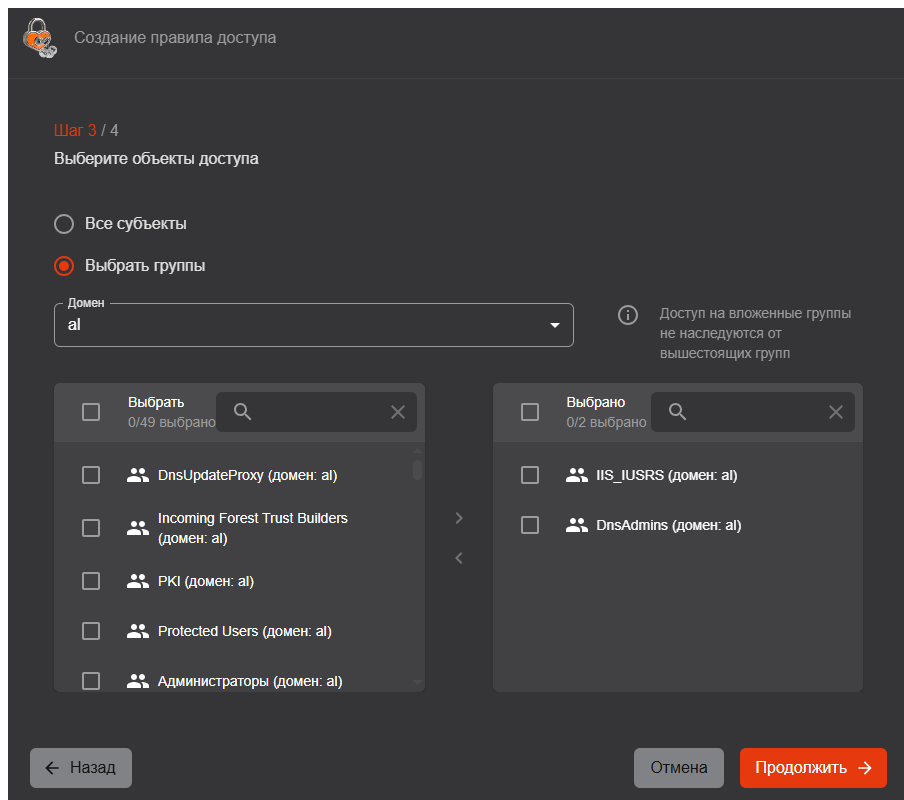


Рисунок 107 – Шаг 3 окна «Создание правила доступа» при выборе режима «Выбрать группы»

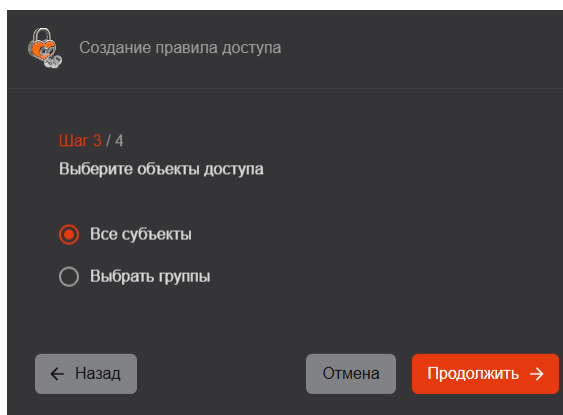


Рисунок 108 – Шаг 3 окна «Создание правила доступа» при выборе режима «Все субъекты»

- Переход на следующий шаг осуществляется по ставшей активной кнопке **<Продолжить>** после выбора объектов доступа.
- На шаге 4 окна «Создание правила доступа» будет отображена информация о создаваемом правиле доступа, включающая в себя: тип правила, перечень выбранных ранее субъектов доступа и объектов доступа и операции (см. Рисунок 109).

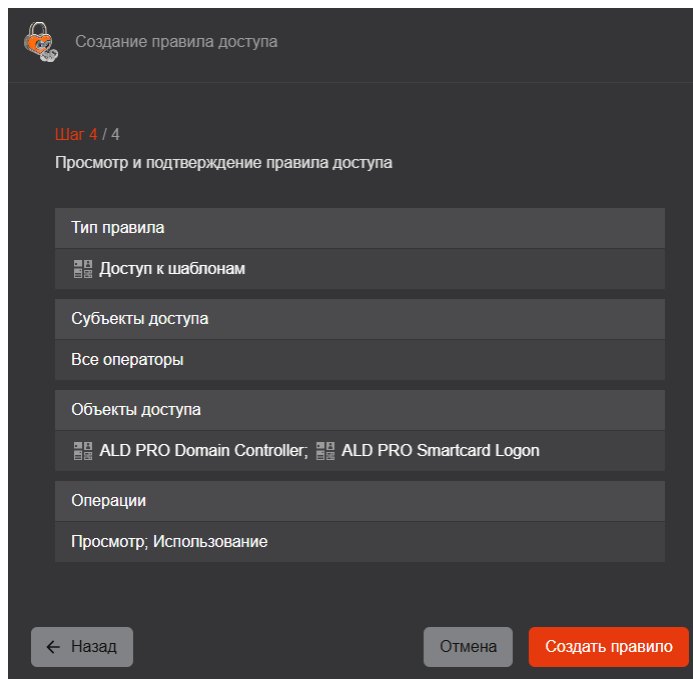



Рисунок 109 – Шаг 4 окна «Создание правила доступа» – «Просмотр и подтверждение правила доступа»

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

9.7.2 Редактирование правила доступа

После создания правила доступа, при наведении курсора на строку добавленного правила доступа появляется возможность его редактирования – при нажатии на кнопку **<Редактировать>**  (см. Рисунок 110) открывается окно «Редактирование правила доступа» для редактирования перечня субъектов доступа и объектов доступа, указанных при создании правила доступа (см. Рисунок 111, Рисунок 112, Рисунок 113, Рисунок 114). Управление составом субъектов доступа и объектов доступа в правиле доступа при его редактировании осуществляется аналогично их выбору при создании правила доступа.

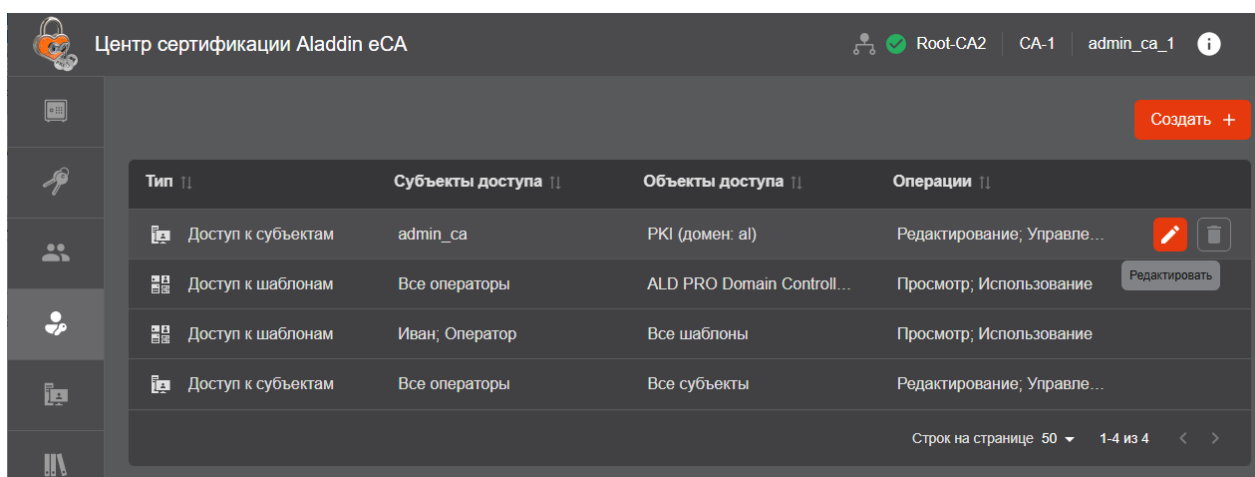


Рисунок 110 – Кнопка редактирования правила доступа

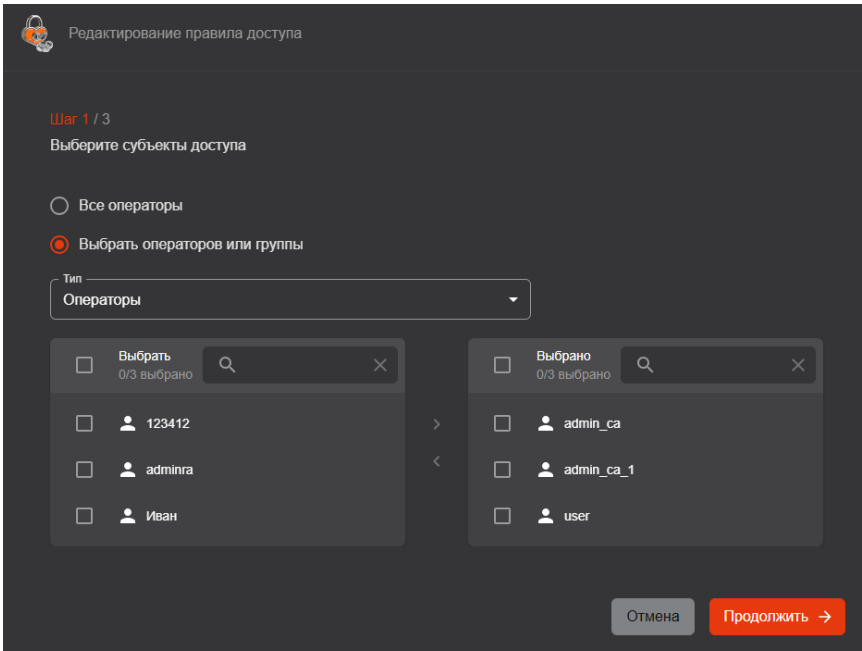


Рисунок 111 – Окно «Редктирование правила доступа», шаг 1

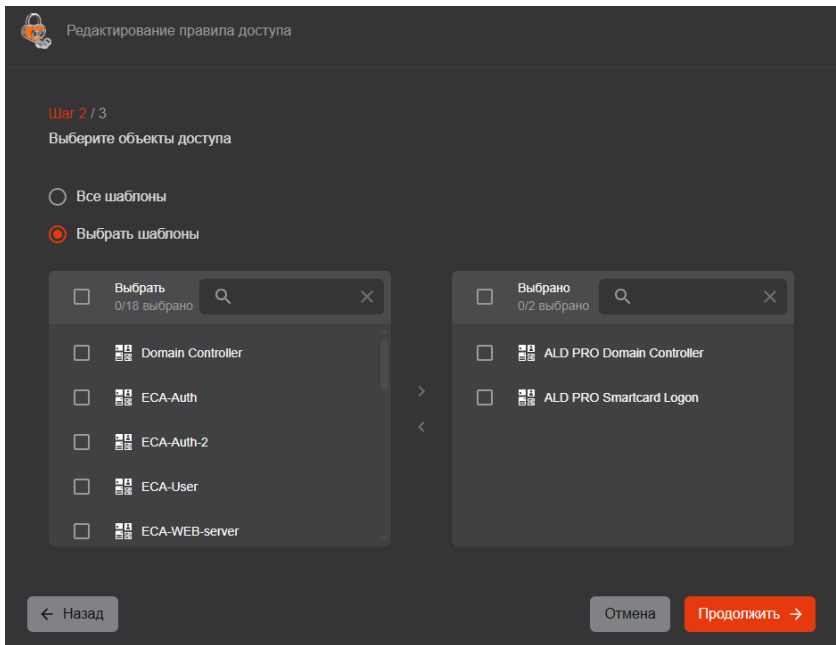


Рисунок 112 – Окно «Редктирование правила доступа», шаг 2, тип правила – «Доступ к шаблонам»

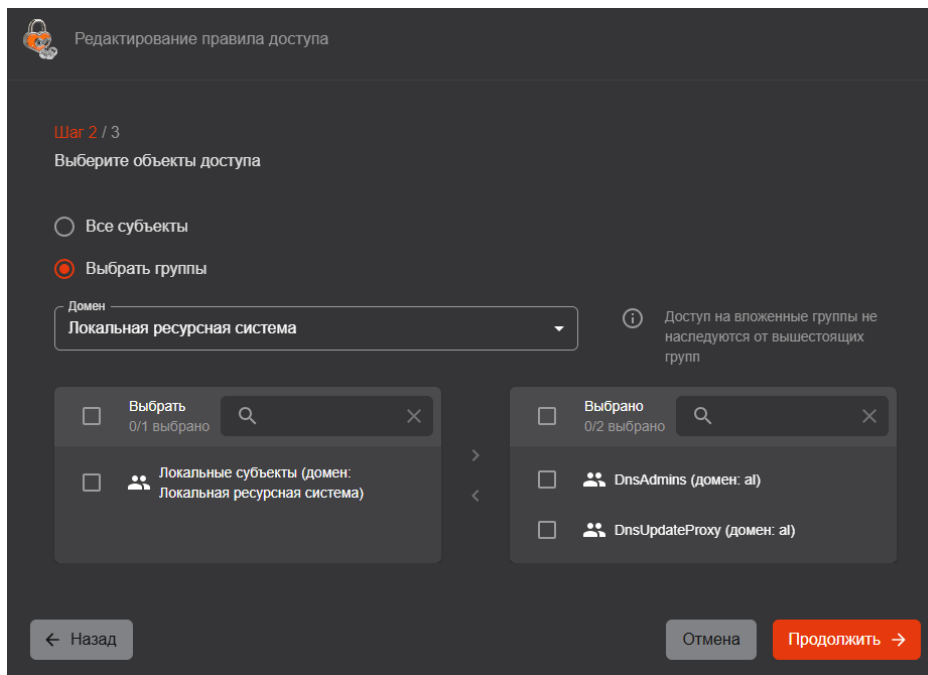


Рисунок 113 – Окно «Редактирование правила доступа», шаг 2, тип правила – «Доступ к группам»

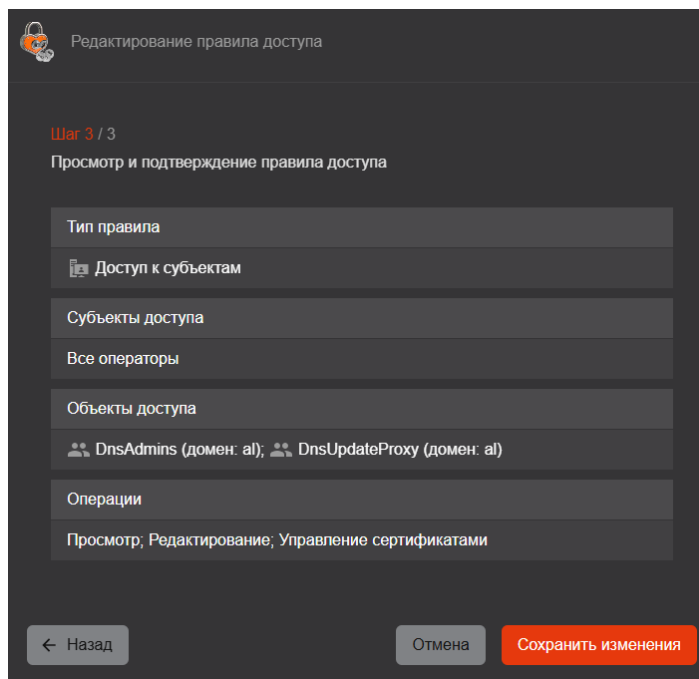



Рисунок 114 – Окно «Редактирование правила доступа», шаг 3

Изменение типа правила доступа недоступно. При редактировании правила доступа исключение всех субъектов доступа или объектов доступа из правила доступа недоступно.

После нажатия на кнопку **<Сохранить изменения>** правило доступа будет изменено.

9.7.3 Удаление правила доступа

После добавления правила доступа, при наведении курсора на строку добавленного правила доступа появляется возможность его удаления – при нажатии на кнопку **<Удалить>**  (см. Рисунок 115) на экран будет выведено окно подтверждения выбранного действия (см. Рисунок 116).

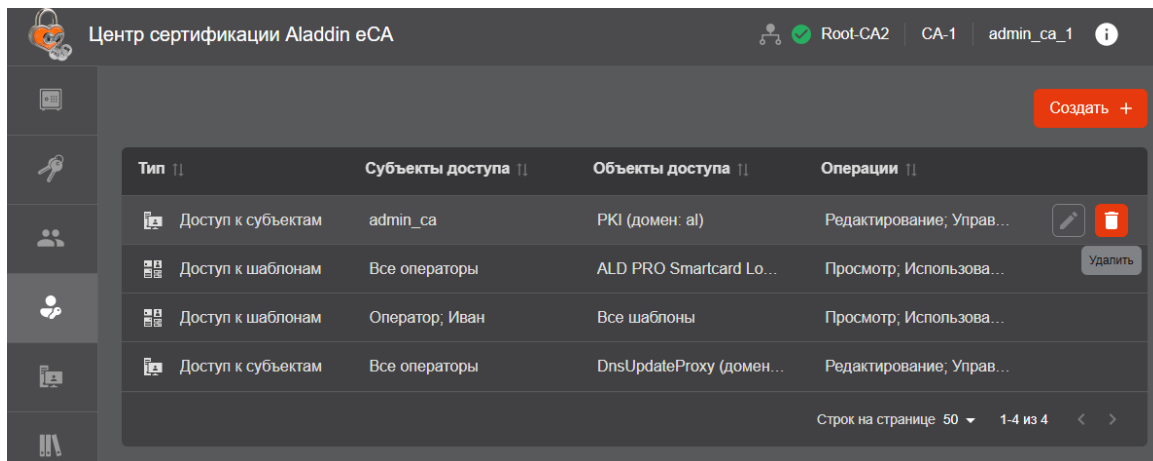


Рисунок 115 – Кнопка удаления правила доступа

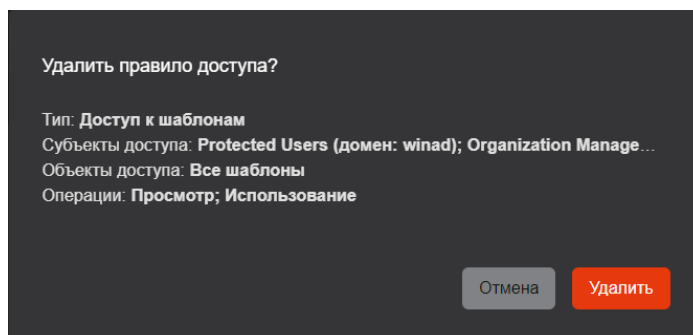


Рисунок 116 – Окно удаления правила доступа

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

9.8 Раздел «Субъекты»

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

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

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

Переход в раздел «Субъекты» осуществляется через боковое меню, расположенное слева на главном экране (см. Рисунок 117).

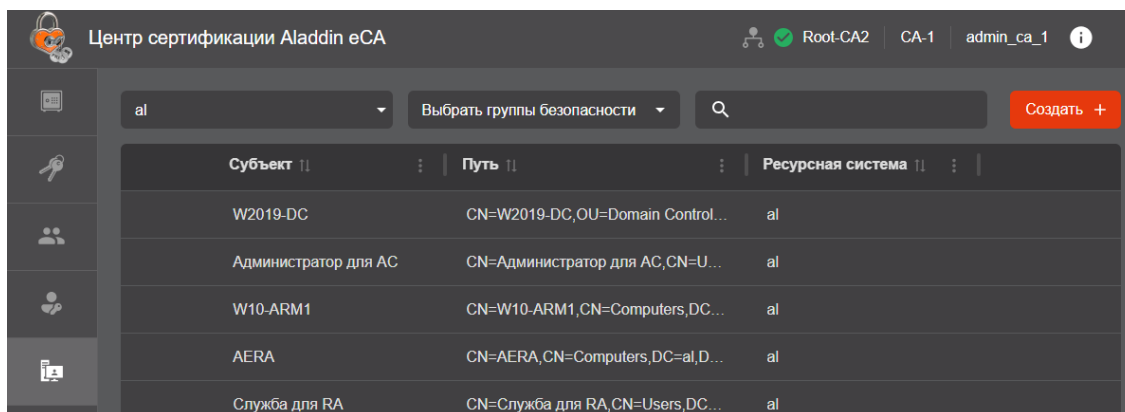



Рисунок 117 – Экран раздела «Субъекты»

В разделе доступны следующие элементы:

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

В разделе «Субъекты» доступны следующие действия:

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

Идентификация локальных и подключенных субъектов в Центре сертификации осуществляется по атрибуту

UUID.

9.8.1 Просмотр субъектов ресурсных систем

Просмотр субъектов осуществляется посредством выбора источника:

- все внешние ресурсы – подключенные службы каталогов;
- локальный ресурс – появляется в случае, если в локальной базе данных присутствует хотя бы один субъект;
- внешний ресурс, отображаемое имя которого соответствует имени контроллера домена.

В разделе «Субъекты» в верхней панели расположены элементы выбора ресурса и фильтрации (см. Рисунок 118):

- поле «Ресурсная система», по нажатию на которое в выпадающем меню выберите локальную ресурсную систему, подключенный ресурс или все внешние ресурсы для отображения всех субъектов внешних ресурсных систем;

- поле «Выбрать группы безопасности», для отображения на экране субъектов определенной группы нажмите на поле и в выпадающем меню выберите необходимую группу. В случае если группа безопасности не выбрана, то будут отображены все субъекты выбранного источника. Для локального ресурса группы безопасности отсутствуют. В списке «Выбрать группу безопасности» отображаются только те группы безопасности, которые содержат один или более субъектов. Группы безопасности, не имеющие членов, не будут показаны в списке и не доступны для выбора;

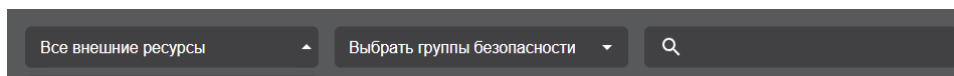


Рисунок 118 – Верхняя панель экранной формы вкладки «Субъекты»

9.8.2 Поиск субъектов

В разделе «Субъекты» в верхней панели расположен элемент поиска (см. Рисунок 118). Поле поиска предназначено для поиска субъектов по компонентам SubjectDN и SubjectAltName в выбранной ресурсной системе. Для поиска начните ввод имени субъекта в строке, поиск начинается автоматически через 1 секунду после прекращения ввода с клавиатуры. Для сброса поиска и отображения всех субъектов выбранной ресурсной системы очистите строку поиска.

9.8.3 Сортировка субъектов

Средства сортировки субъектов выбранной ресурсной системы представлены элементами выбора направления сортировки в заголовке таблицы экранной формы (см. Рисунок 119):

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


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



Рисунок 119 – Поля сортировки содержимого экрана раздела «Субъекты»

9.8.4 Карточка субъекта

Просмотр данных субъекта возможен посредством страницы «Карточка субъекта».

Переход к экрану «Карточка субъекта» (см. Рисунок 121) осуществляется при нажатии на строку субъекта главного экрана раздела «Субъекты» (см. Рисунок 117).

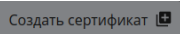
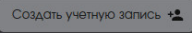
Карточка субъекта включает в себя следующие информационные поля:

- сведения о субъекте:
 - из какой ресурсной системы получен субъект;
 - статус пользователя в ресурсной системе;
 - идентификатор UUID;
 - SID (идентификатор безопасности) ¹;
- атрибуты SAN и SDN (Таблица 19);
- сведения обо всех сертификатах субъекта, ранее выпущенных Центром сертификации:
 - серийный номер;
 - Common Name владельца сертификата;

¹ SID может быть получен для субъекта только из ресурсных систем MS AD, SambaDC, РЕД АДМ и Альт Домен. Для субъектов ресурсных систем FreeIPA и ALD PRO данный атрибут отсутствует.

- шаблон;
- дата создания;
- дата окончания действия;
- дата публикации в ресурсную систему;
- состояние сертификата.

Доступные действия в карточке субъекта:

- создать сертификат для выбранного субъекта с закрытым ключом, на основании запроса или на ключевом носителе по нажатию на кнопку **<Создать сертификат>**  (см. раздел 9.8.7, настоящего руководства);
- создание учётной записи для текущего субъекта по нажатию на кнопку . Только для субъекта типа «Пользователь»;
- выбрать набор атрибутов SDN и SAN, отображаемых в карточке субъекта, в выпадающем меню (см. Рисунок 120);

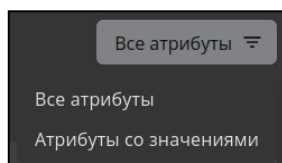




Рисунок 120 – Фильтрация отображаемых атрибутов в карточке субъекта

- опубликовать сертификат в ресурсную систему (только для подключенных субъектов). По нажатию на кнопку  происходит запись сертификата в формате LDIF в атрибут `userCertification` выбранного субъекта ресурсной системы, для которого выпущен сертификат. Если атрибут `userCertification` заполнен, то происходит перезапись содержимого;
- экспорт сертификата выбранного субъекта по указанному для сохранения файла по указанному пути по кнопке  **<Скачать>**;
- переход в карточку сертификата;
- изменить статус сертификатов, выпущенных для данного субъекта в соответствии с таблицей 16 в поле сертификата «Состояние».

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

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

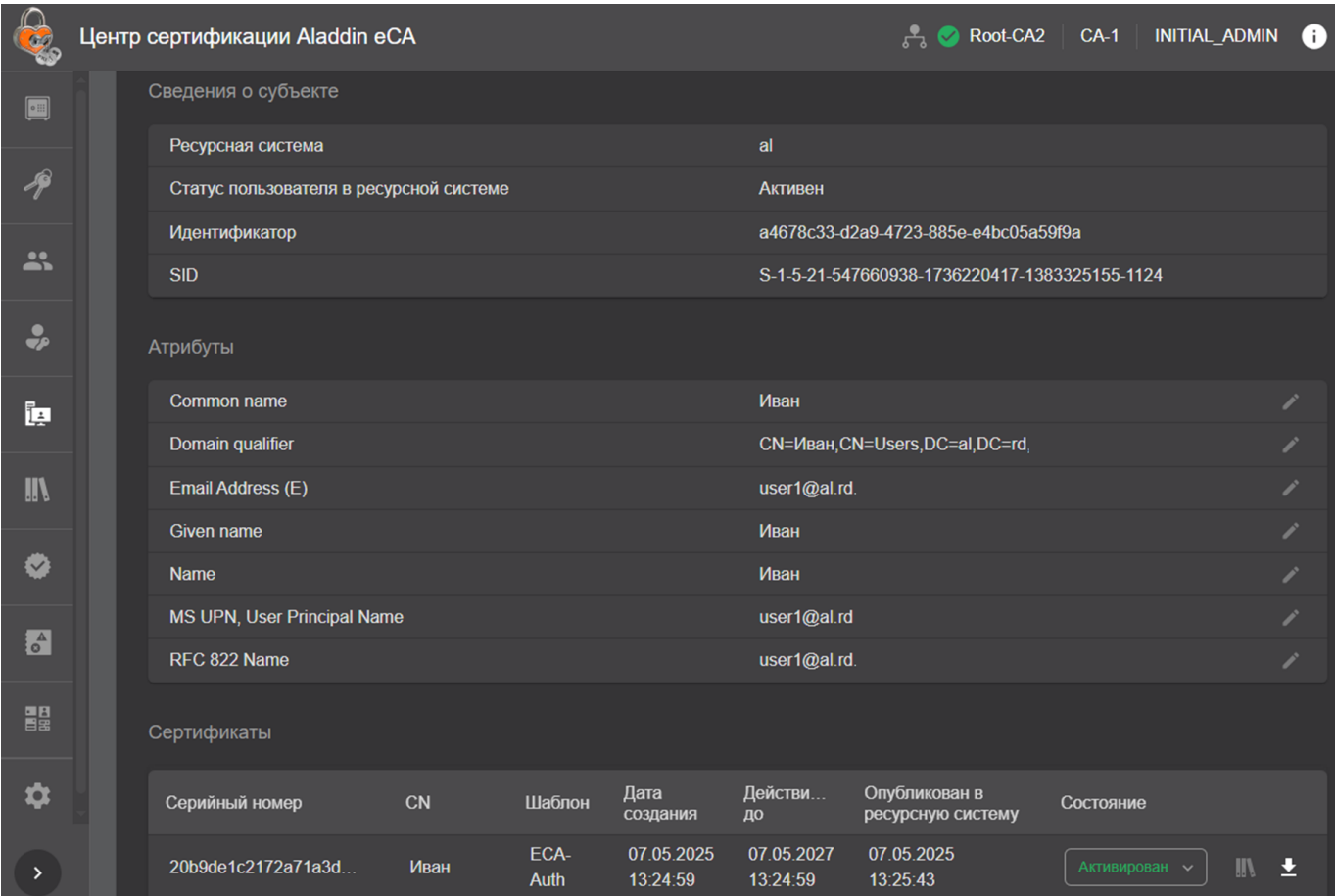


Рисунок 121 – Окно просмотра карточки подключенного субъекта (включено отображение «Атрибуты со значениями»)

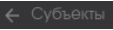
- Выход из карточки субъекта осуществляется по кнопке **<Возврат>**  в раздел «Субъекты» и по кнопкам разделов боковой панели.

Таблица 19 – Атрибуты субъекта

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

Атрибут	Возможные значения	Представление в API	Представление в клиентском компоненте
Расположение субъекта в структуре PC	Строка	«distinguishedName»	Поле «Путь» в списке субъектов в разделе «Субъекты»
Время обновления субъекта	Дата в формате ISO 8601	«updated»	–
Время создания субъекта	Дата в формате ISO 8601	«created»	–
SID ¹	Строка	«sid»	Поле «SID» карточки субъекта
Атрибуты SDN			
Common name	Список строк	«CN»	Поле «Common name» в карточке субъекта
Unique Identifier (UID)	Список строк	«UID»	Поле «Unique Identifier (UID)» в карточке субъекта
Email Address (Mail)	Список строк	«EMAILADDRESS»	Поле «Email Address (E)» в карточке субъекта
Serial number	Список строк	«SN»	Поле «Serial number» в карточке субъекта
Given name	Список строк	«GIVENNAME»	Поле «Given name» в карточке субъекта
Initials	Список строк	«INITIALS»	Поле «Initials» в карточке субъекта
Surname	Список строк	«SURNAME»	Поле «Surname» в карточке субъекта
Organizational unit	Список строк	«OU»	Поле «Organizational unit» в карточке субъекта
Organization	Список строк	«O»	Поле «Organization» в карточке субъекта
Locality	Список строк	«L»	Поле «Locality» в карточке субъекта
State or province	Список строк	«ST»	Поле «State or province» в карточке субъекта
Domain component	Список строк	«DC»	Поле «Domain component» в карточке субъекта
Country	Список строк	«C»	Поле «Country» в карточке субъекта
Unstructured address	Список строк	«UNSTRUCTUREDADDRESS»	Поле «Unstructured address» в карточке субъекта
Unstructured name	Список строк	«UNSTRUCTUREDNAME»	Поле «Unstructured name» в карточке субъекта
Postalcode	Список строк	«POSTALCODE»	Поле «Postal code» в карточке субъекта
Business category	Список строк	«BUSINESSCATEGORY»	Поле «Business category» в карточке субъекта
Telephone number	Список строк	«TELEPHONENUMBER»	Поле «Telephone number» в карточке субъекта
Pseudonym	Список строк	«PSEUDONYM»	Поле «Pseudonym» в карточке субъекта
Postal address	Список строк	«POSTALADDRESS»	Поле «Postal address» в карточке субъекта
Street	Список строк	«STREET»	Поле «Street» в карточке субъекта

¹ SID может быть получен для субъекта только из ресурсных систем MS AD, SambaDC, РЕД АДМ и «Альт Домен».

Атрибут	Возможные значения	Представление в API	Представление в клиентском компоненте
Name	Список строк	«NAME»	Поле «Name» в карточке субъекта
Title	Список строк	«T»	Поле «Title» в карточке субъекта
Domain Qualifier	Список строк	«DN»	Поле «Domain Qualifier» в карточке субъекта
Description	Список строк	«DESCRIPTION»	Поле «Description» в карточке субъекта
Дата рождения	Список строк	«DATEOFBIRTH»	Поле «Дата рождения» в карточке субъекта
Место рождения	Список строк	«PLACEOFBIRTH»	Поле «Место рождения» в карточке субъекта
ИНН	Список строк	«INN»	Поле «ИНН» в карточке субъекта
ОГРН	Список строк	«OGRN»	Поле «ОГРН» в карточке субъекта
ОГРНИП	Список строк	«OGRNIP»	Поле «ОГРНИП» в карточке субъекта
СНИЛС	Список строк	«SNILS»	Поле «СНИЛС» в карточке субъекта
ИНН ЮЛ	Список строк	«INNLE»	Поле «ИНН ЮЛ» в карточке субъекта
Атрибуты SAN			
MS GUID, Globally Unique Identifier	string(\$uuid)	«MS_GUID»	Поле «MS GUID, Globally Unique Identifier» в карточке субъекта
RFC 822 NAME	Список строк	«RFC822NAME»	Поле «RFC 822 NAME» в карточке субъекта
MS UPN, UserPrincipalName	Список строк	«MS_UPN»	Поле «MS UPN, UserPrincipalName» в карточке субъекта
DNS Name	Список строк	«DNS_NAME»	Поле «DNS Name» в карточке субъекта
IP address	Список строк	«IPADDRESS»	Поле «IP address» в карточке субъекта
Directory Name	Список строк	«DIRECTORY_NAME»	Поле «Directory Name» в карточке субъекта
Uniform resource identifier	Список строк	«UNIFORM_RESOURCE_ID»	Поле «Uniform resource identifier» в карточке субъекта
Registered identifier	Список строк	«REGISTERED_ID»	Поле «Registered identifier» в карточке субъекта
Kerberos KPN, Kerberos 5 Principal	Список строк	«KRB5PRINCIPAL»	Поле «Kerberos KPN, Kerberos 5 Principal» в карточке субъекта
Permanent identifier	Список строк	«PERMANENT_IDENTIFIER»	Поле «Permanent identifier» в карточке субъекта
Xmpp address	Список строк	«XMPP_ADDR»	Поле «Xmpp address» в карточке субъекта
Service Name	Список строк	«SRV_NAME»	Поле «Service Name» в карточке субъекта
Subject Identification Method	Список строк	«SUBJECT_IDENTIFICATION_METHOD»	Поле «Subject Identification Method» в карточке субъекта

9.8.4.1 Редактирование атрибутов субъекта

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

Для субъектов подключенной ресурсной системы редактирование атрибутов SDN или SAN, значения которых получены Центром сертификации из ресурсной системы, недоступно. Все остальные атрибуты SDN или SAN доступны для редактирования.


Для субъектов любой ресурсной системы редактирование сведений о субъектах в их карточках (поля «Получен из ресурсной системы», «Статус в ресурсной системе», «UUID») недоступны для редактирования.


При вводе/редактировании значений атрибутов, указанных в таблице 20, осуществляется валидация. Для всех остальных атрибутов субъекта валидация отсутствует.

Таблица 20 – Допустимые значения атрибутов

Атрибут	Правило валидации
Country	Допустимые символы: «А»–«Z», «а»–«z». Длина значения должна составлять 2 символа.
Domain qualifier	Допустимые символы: «А»–«Z», «а»–«z», «0»–«9», «'», «(», «)», «+», «,», «-», «.», «/», «:», «=», «?», пробел.
Email Address (E)	Допустимые символы: «А»–«Z», «а»–«z», «А»–«Я», «а»–«я», «0»–«9», «.», «@», «_», «-». Формат значения: «text@text».
Serial number	Допустимые символы: «А»–«Z», «а»–«z», «0»–«9», «'», «(», «)», «+», «,», «-», «.», «/», «:», «=», «?», пробел.
RFC 822 Name	Допустимые символы: «А»–«Z», «а»–«z», «0»–«9», «.», «@», «_», «-». Если необходимо использовать кириллицу, то кириллицу необходимо преобразовать в латиницу с помощью Punycode (подробнее см. RFC 3492) и ввести полученное значение в поле. При этом преобразовывать можно только доменную часть. Формат значения: «text@text».
DNS Name	Допустимые символы: «А»–«Z», «а»–«z», «0»–«9», «-», «.», «*». Если необходимо использовать кириллицу, то кириллицу необходимо преобразовать в латиницу с помощью Punycode (подробнее см. RFC 3492) и ввести полученное значение в поле.
IP address	Допустимые символы: «А»–«F», «а»–«f», «0»–«9», «.», «:». Формат значения: Ipv4–адрес или Ipv6–адрес.
Directory Name	Формат значения: последовательность идентификаторов относительных отличительных имен (RDN) и их значений, отделенных запятой или запятой с пробелом (например, O=organization, OU=Department, L=City, DC=Component...). 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: «А»–«Z», «а»–«z», «А»–«Я», «а»–«я», «ё», «Ё», «0»–«9», «.», «@», «_», «-», «/». Формат значения: «text@text».
MS GUID, Globally Unique Identifier	Допустимые символы: «А»–«F», «а»–«f», «0»–«9». Длина значения должна составлять 32 символа.
Kerberos KPN, Kerberos 5 Principal Name	Допустимые символы: «А»–«Z», «а»–«z», «А»–«Я», «а»–«я», «ё», «Ё», «0»–«9», «.», «@», «_», «-», «/». Формат значения: «text@text».
Permanent Identifier	Формат значения: «value/OID», где «value» – любая последовательность символов, а «OID» – OID в соответствии с рекомендацией ITU X.660. Допускается отсутствие значения «text», например, «/1.2.2.3.4.5».
Xmpp address	Допустимые символы: «А»–«Z», «а»–«z», «А»–«Я», «а»–«я», «ё», «Ё», «0»–«9», «.», «@», «_», «-», «/». Формат значения: «text@text».
Subject Identification Method	Формат значения: «OID::text::text», где «OID» – OID в соответствии с рекомендацией ITU X.660, а «text» – любая последовательность символов.

Атрибут	Правило валидации
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 122).

- Для добавления значения атрибута (будет указано в поле атрибута через запятую) нажмите кнопку **<Добавить значение +>**;
- Для удаления значения атрибута нажмите кнопку **<Удалить значение атрибута>** . При этом у атрибута «Common name» нельзя удалить последнее значение;
- Для сохранения результата нажмите кнопку **<Сохранить>**;
- Для выхода из режима редактирования без сохранения изменений или нажмите кнопку **<Заккрыть>**.
- При синхронизации отредактированное поле атрибута будет заменено значением соответствующего атрибута субъекта синхронизированной ресурсной системы, если оно заполнено для этого доменного субъекта в ресурсной системе!

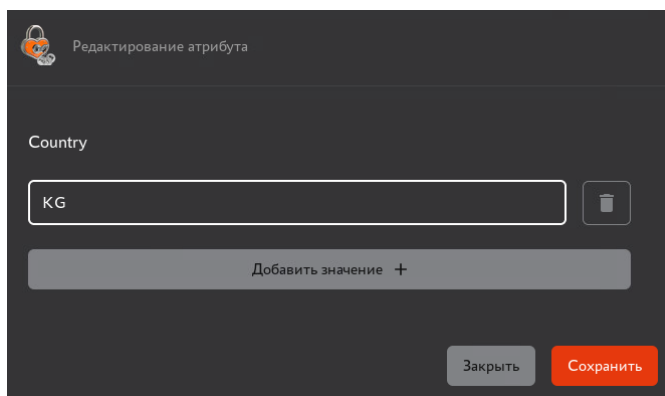


Рисунок 122 – Окно редактирования значения атрибута в карточке субъекта

9.8.5 Субъекты локальной ресурсной системы

Локальную базу субъектов формируют:

- субъекты, созданные Администратором путём вызова метода API (см. документ «Центр сертификатов доступа Aladdin Enterprise Certificate Authority Certified Edition. Руководство администратора. Часть 3. Описание методов REST API Центра сертификации Aladdin Enterprise Certification Authority»);
- субъекты отключенной ресурсной системы (удалённой ранее зарегистрированной ресурсной системы), атрибут субъекта «isBlocked» принимает значение «false». В случае повторного подключения ресурсной системы связи субъектов с группами будут восстановлены, обновлены атрибуты в соответствии с данными из ресурсной системы;
- субъекты, загруженные в базу данных Центра сертификации Aladdin eCA при подключении ресурсной системы, но отсутствующие в списке субъектов, полученном по результатам выполнения полной синхронизации ресурсной системы. Атрибут субъекта «isBlocked» принимает значение «false»;
- субъект веб-сервера, автоматически созданный при развёртывании Центра сертификации Aladdin eCA, с параметрами, указанными в конфигурационном файле `/opt/aecaCa/scripts/config.sh`:

- параметр `hostname` задаёт значение атрибутов «Common name» и «DNS Name» локального субъекта;
- параметры `initial_server_key_algorithm` и `initial_server_key_bits` задают значения криптографических параметров сертификата веб-сервера;
- параметр `initial_server_password` задаёт значение пароля контейнера сертификата веб-сервера.

Локальный субъект отключенной ресурсной системы при подключении ресурсной системы, где существует данный субъект, будет перенесён из базы локальной ресурсной системы (атрибут субъекта «isConnected» примет значение «true»). При этом будет выполнено обновление атрибутов субъекта в соответствии с его атрибутами из ресурсной системы (Таблица 21), остальные текущие атрибуты (то есть те, которые не были получены из ресурсной системы) не изменятся.

Проверка субъектов осуществляется по атрибуту «id».

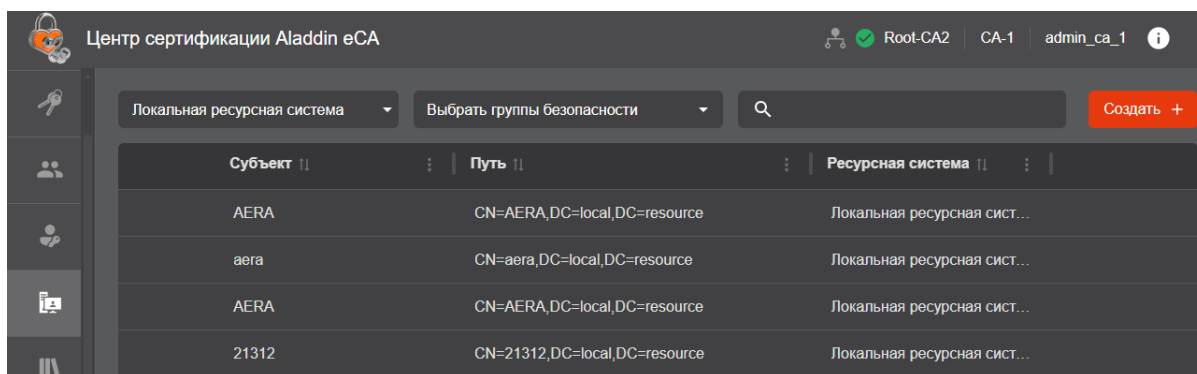


Рисунок 123 – Экран раздела меню «Субъекты». Локальный ресурс

9.8.5.1 Создание нового субъекта локальной ресурсной системы

Доступно только пользователю с ролью «Администратор». Для создания нового локального субъекта нажмите кнопку **<Создать>** (см. Рисунок 123), в открывшемся окне (см. Рисунок 124) введите имя создаваемого субъекта (CN), добавьте необходимые атрибуты и задайте им значения.

Для добавления атрибута нажмите кнопку **<Добавить атрибут +>** и выберите атрибут в списке возможных атрибутов SDN и SAN (см. Рисунок 125). При необходимости воспользуйтесь поиском и прокруткой списка.

Полный список доступных атрибутов приведён в таблице выше (Таблица 19).

Далее укажите значения выбранным атрибутам или удалите атрибуты, нажав кнопку **<Удалить>**.

При отсутствии значения в поле «Common name» или несоответствии введенного значения допустимому формату создание субъекта запрещено.

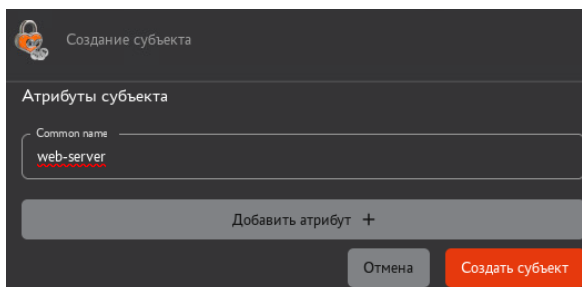


Рисунок 124 – Создание субъекта

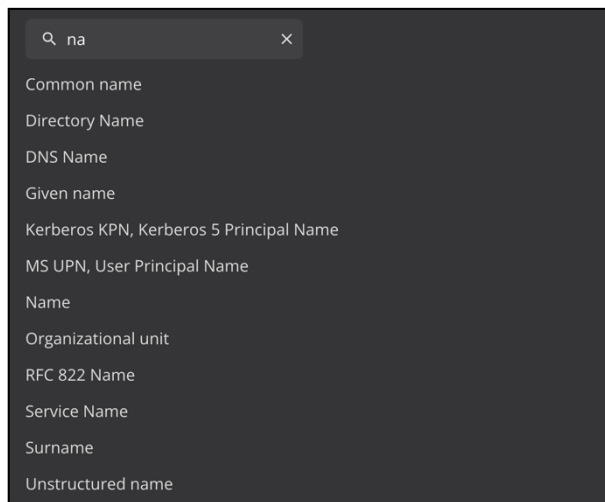


Рисунок 125 – Добавление атрибута субъекта

После корректного заполнения всех выбранных полей атрибутов будет доступно создание субъекта по нажатию на кнопку **<Создать субъект>**.

При создании локального субъекта Центра сертификации автоматически назначает новому субъекту идентификатор (UUID).

В результате создания субъекта администратор будет уведомлён всплывающим сообщением об успешном создании субъекта.

9.8.6 Субъекты внешнего ресурса

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

Подключенный ресурс будет отображен только после регистрации ресурсной системы на вкладке «Ресурсная система» (см. раздел 9.9.1 настоящего руководства).

Обновление списков и данных субъектов ресурсной системы происходит по правилам, приведённым в разделе 9.9.3 настоящего руководства.

После подключения внешней ресурсной системы, обновления и выбора источника в поле «Ресурсная система», субъекты будут отображены в виде списка в окне вкладки «Субъекты». Возможно настроить отображение определенной группы безопасности или вывести полный список, упорядочив субъекты в алфавитном порядке по имени (CommonName) (см. Рисунок 126).

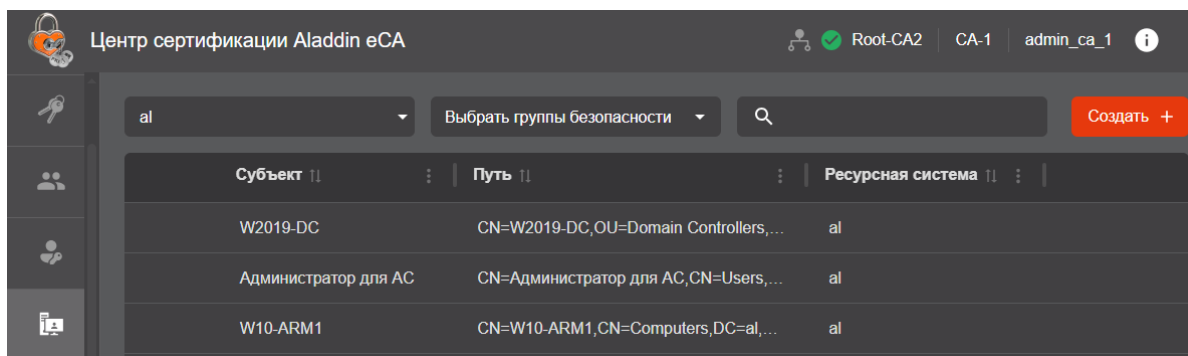


Рисунок 126 – Экран раздела меню «Субъекты». Подключенный ресурс

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

Для каждого загруженного пользователя и компьютера будет создан субъект и подгружены все поля, относящиеся к SubjectDN и SubjectAltName. Преобразование содержимого записи LDAP в поля базы субъектов ресурсной системы происходит в соответствии с таблицей 21.


Таблица 21 – Преобразование данных субъектов ресурсной системы

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

Если данные поля отсутствуют в описании субъекта в подключенном домене, то в шаблоне при выпуске сертификата соответствующие поля заполняются пустыми значениями.

Идентификация подключенных субъектов в Центре сертификации осуществляется по атрибуту **Id**.

9.8.7 Создание сертификата для субъекта ресурсной системы

Выберите субъект, для которого необходимо создать сертификат, нажмите появившуюся кнопку  **<Создать сертификат>** и выберите способ создания из выпадающего списка (см. Рисунок 127):

- 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.

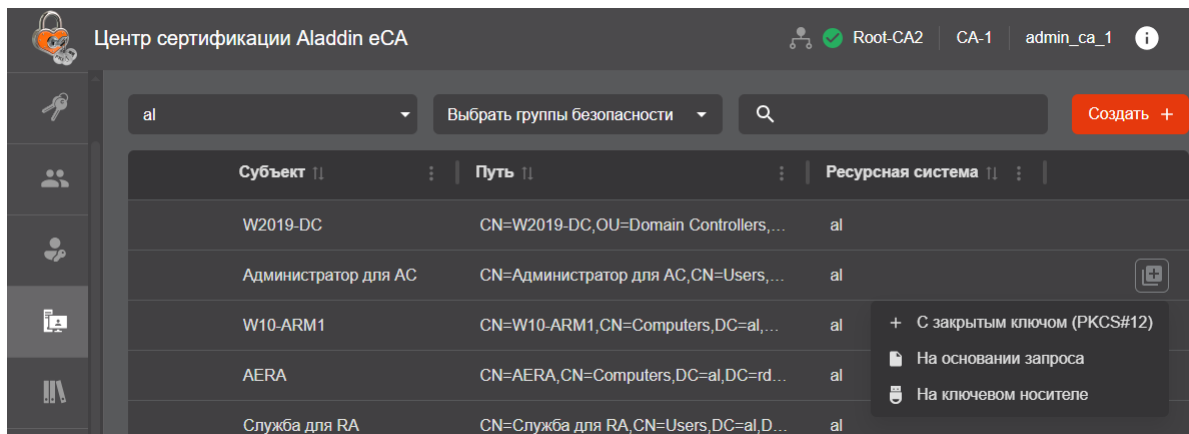


Рисунок 127 – Окно выпуска сертификата для субъекта ресурсной системы

При выпуске сертификатов для субъектов внешних (подключенных) ресурсных систем возможно публиковать сертификат в формате LDIF в атрибут `userCertification` субъекта ресурсной системы (путём добавления, а не перезаписи атрибута), проставив флаг в чек-боксе «Публиковать сертификат в ресурсную систему» окна выпуска сертификата. По умолчанию флаг выполнения публикации сертификата включен.

После выбора шаблона субъекта ресурсной системы на следующем шаге поля автоматически заполняются данными субъекта в соответствии с таблицей 21.

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».

9.8.8 Создание учётной записи для субъекта

Выберите субъект локальной или подключенной ресурсной системы, для которого необходимо создать учетную запись и нажмите кнопку в строке выбранного пользователя **<Создать учетную запись>** (см. Рисунок 128).

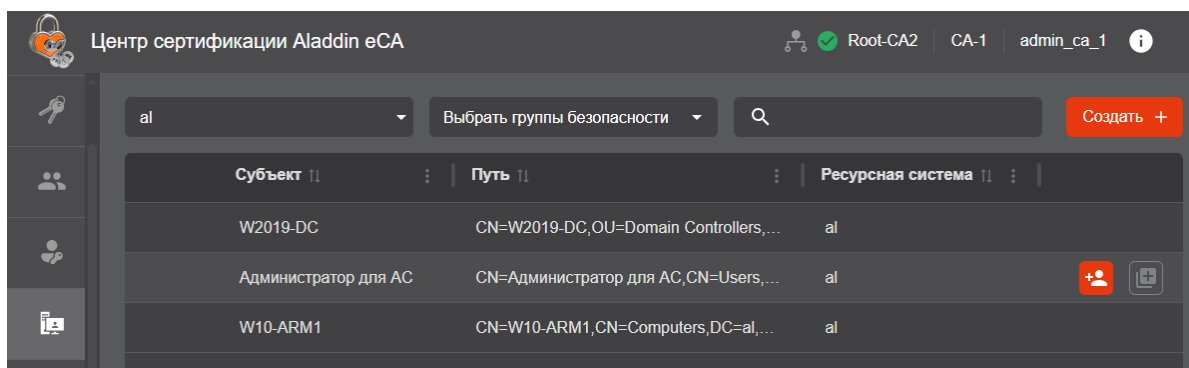


Рисунок 128 – Выбор субъекта для создания учётной записи

В открывшемся окне создания новой учетной записи (см. Рисунок 129) поле «Отображаемое имя» автоматически заполнено данными атрибута «Common Name» субъекта, но доступно для редактирования, и соответствует полю «ФИО» в разделе «Учётные записи». Поле «Логин» не отображается в окне создания новой учётной записи и заполняется по умолчанию в соответствии со значением атрибута «Common Name» выбранного субъекта.

Выберите роль, применяемую к создаваемой учетной записи, и нажмите кнопку **<Создать>** для создания учетной записи для субъекта.

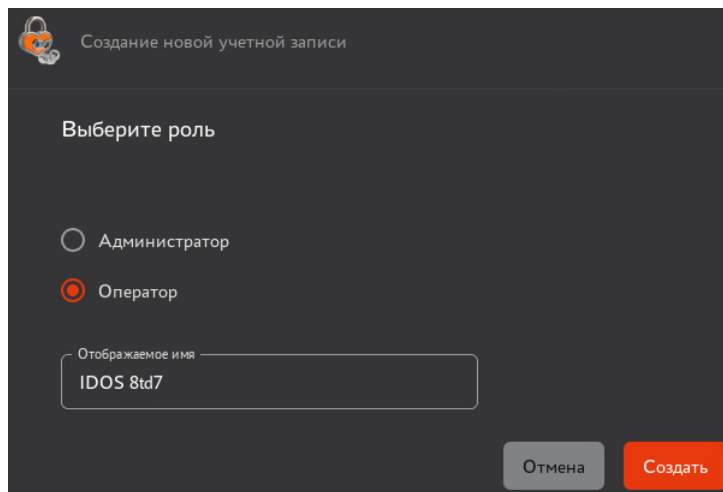


Рисунок 129 – Окно создания новой учётной записи

- Для созданной учетной записи с ролью «Оператор» произведите настройку прав доступа к группам и объектам ресурсной системы в соответствии с разделом 9.6.5 настоящего руководства¹.

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

9.9 Раздел «Ресурсные системы»

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

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


Переход в раздел «Ресурсные системы» осуществляется через боковое меню, расположенное слева на главном экране (см. Рисунок 130).

На основном экране раздела «Ресурсные системы» отображены следующие информационные поля (см. Рисунок 130):

- имя домена – домен подключенной ресурсной системы;
- последнее обновление – дата и время последней синхронизации с базой субъектов ресурсной системы;
- статус – статус ресурсной системы, который назначается в соответствии с критериями, приведенными в таблице 22.

Таблица 22 – 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.

¹ 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.

Ресурсным системам возможно назначить выполнение следующих задач:

- полная синхронизация ресурсной системы (см. раздел 9.9.3.3);
- частичная синхронизация ресурсной системы (синхронизация точки подключения ресурсной системы) (см. раздел 9.9.3.4);
- удаление зарегистрированной ресурсной системы (см. Раздел 9.9.5);
- удаление точки подключения зарегистрированной ресурсной системы (см. раздел 9.9.6).

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

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

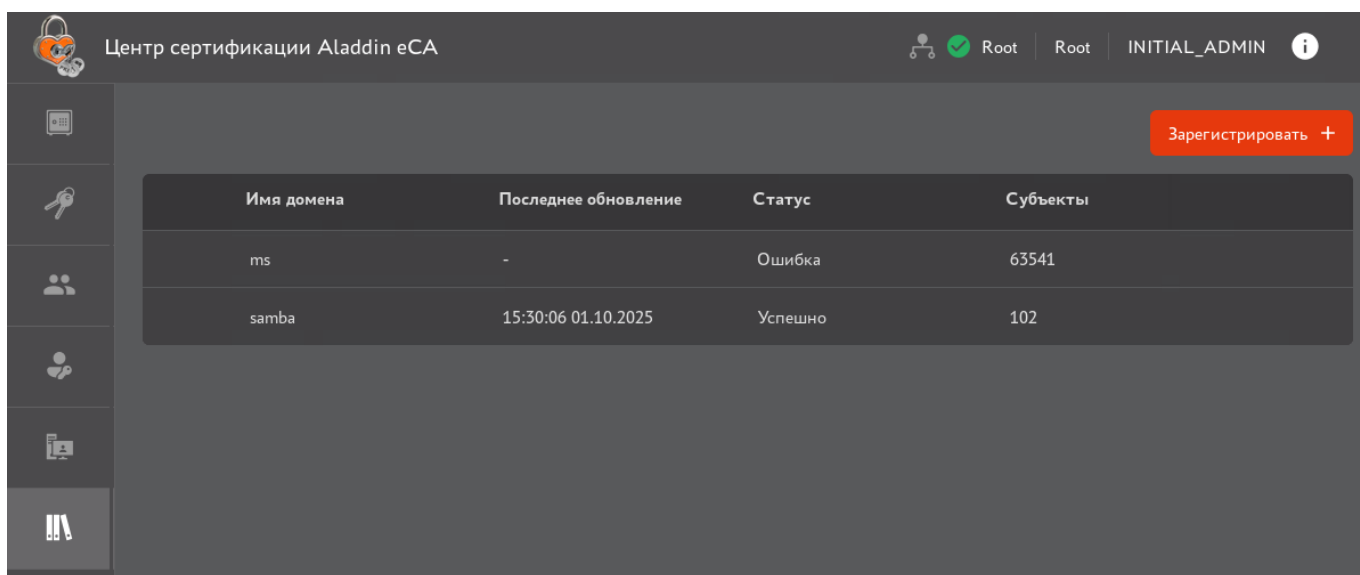


Рисунок 130 – Экран раздела «Ресурсные системы»

Центр сертификации Aladdin eCA позволяет взаимодействовать с несколькими ресурсными системами: Samba DC, РЕД АДМ, MS AD, FreeIPA, ALD PRO и Альт Домен:

- список субъектов (пользователей, компьютеров и сервисов (только для ALD PRO и FreeIPA)), их атрибуты и сертификаты;
- список и состав групп безопасности.

Идентификация загружаемых субъектов ресурсной системы производится по их атрибуту «id».

В разделе «Ресурсные системы» доступны следующие возможности:

- регистрация (подключение) ресурсной системы для выпуска сертификатов и учётных записей субъектам служб каталогов (см. раздел 9.9.1);
- переход в карточку ресурсной системы (см. раздел 9.9.2);
- запуск полной синхронизации ресурсной системы (см. раздел 9.9.3.3);
- удаление зарегистрированной ресурсной системы (см. раздел 9.9.5).

9.9.1 Регистрация точки подключения

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

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

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

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

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

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

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

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

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

- наличие роли «Service Role» для подключения к ресурсной системе;
- наличие роли «helpdesk» или роли «User Administrator» для публикации сертификатов пользователей;
- наличие роли «Enrollment Administrator» для публикации сертификатов контроллеров домена.

Для подключения к ресурсной системе Samba DC, Альт Домен, РЕД АДМ или MS AD необходимо создать учетную запись на контроллере домена с правами, позволяющими получить данные (наличие ролей «Domain Users» и «Cert Publishers» для публикации сертификатов пользователей).

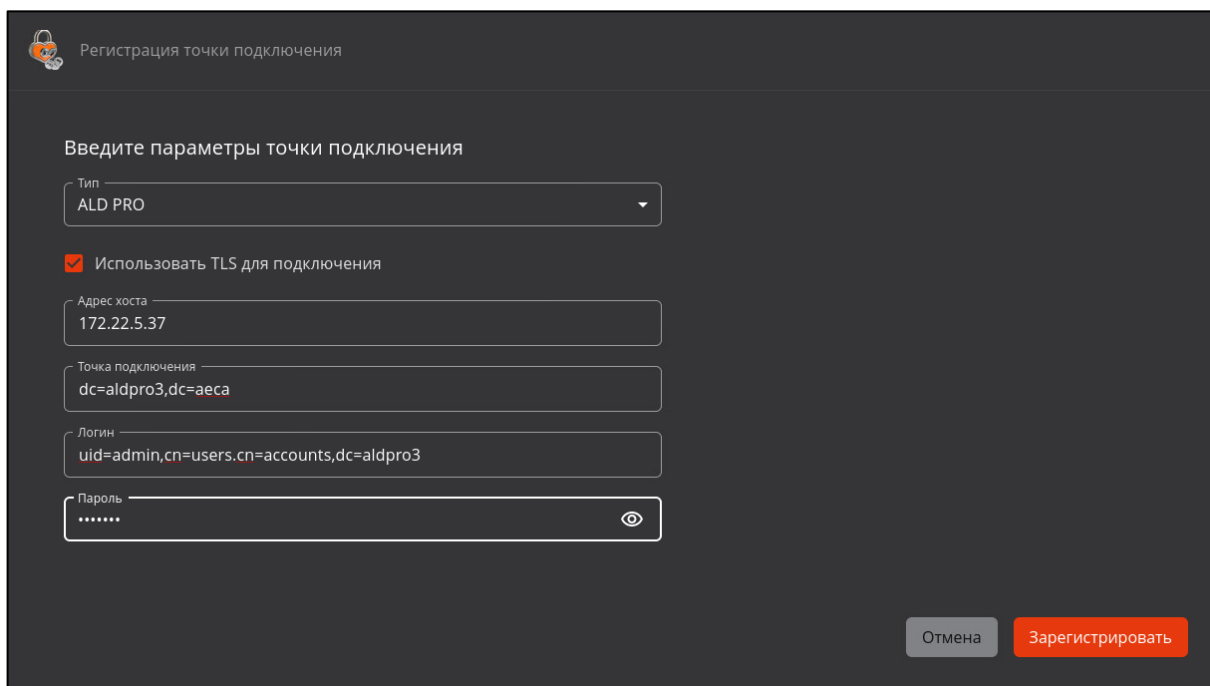
Порядок регистрации точки подключения:

- 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, 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 незащищённого соединения снимите отметку чек-бокса;
 - адрес хоста – укажите полное доменное имя или IP-адрес точки подключения ресурсной системы;
 - точка подключения – укажите точку подключения в формате:
 DC={первое доменное имя}, DC={второе доменное имя} и т.д.;
 - логин – укажите имя учетной записи администратора контроллера домена:
 - для Samba DC, Альт Домен, РЕД АДМ и MS AD имя учетной записи администратора указывается в формате RFC822Name;
 - для ALD PRO и FreeIPA имя учетной записи администратора указывается в формате Distinguished Names.
 - пароль – укажите пароль учетной записи администратора контроллера домена.

Пароль хранится в базе данных в зашифрованном по алгоритму AES256 виде (конфигурация базы данных указана в конфигурационном файле `/opt/aecaCa/scripts/config.sh`).

Примеры заполненных полей при подключении ресурсной системы для разных типов источников приведены на соответствующих рисунках (см. Рисунок 131, Рисунок 132, Рисунок 133, Рисунок 134, Рисунок 135, Рисунок 136).

- 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

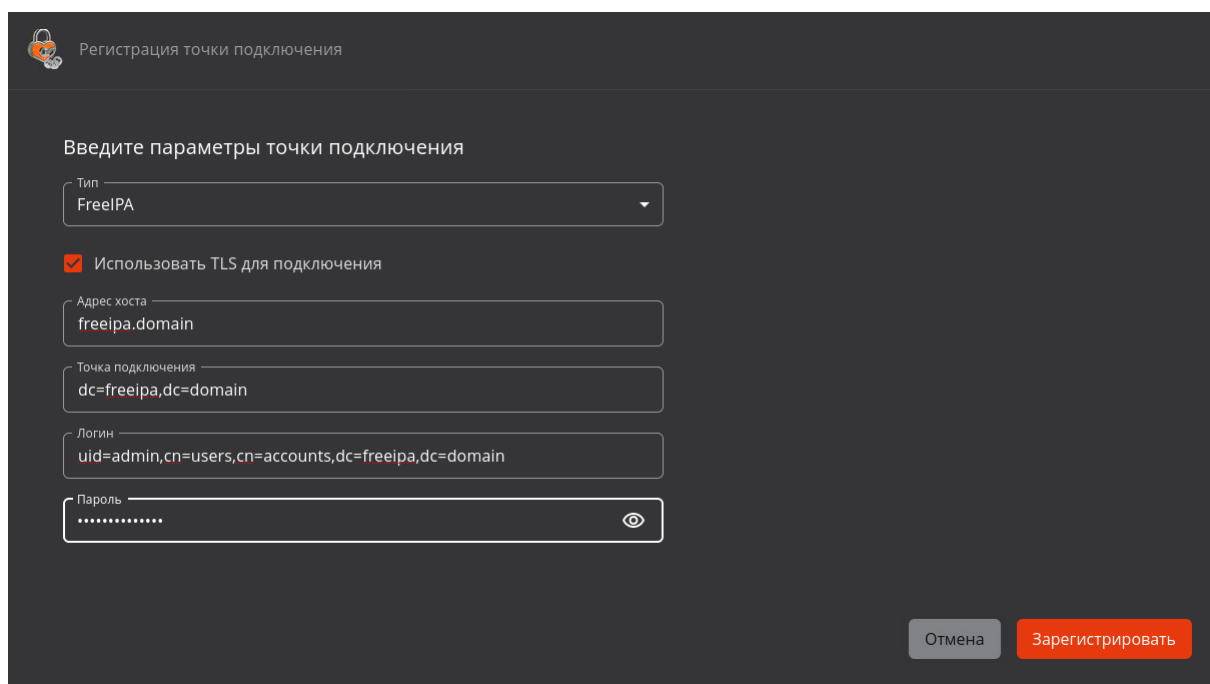
Точка подключения
dc=aldpro3,dc=aeca

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

Пароль
.....

Отмена Зарегистрировать

Рисунок 131 – Пример регистрации ресурсной системы ALD PRO



Регистрация точки подключения

Введите параметры точки подключения

Тип
FreeIPA

☒ Использовать TLS для подключения

Адрес хоста
freeipa.domain

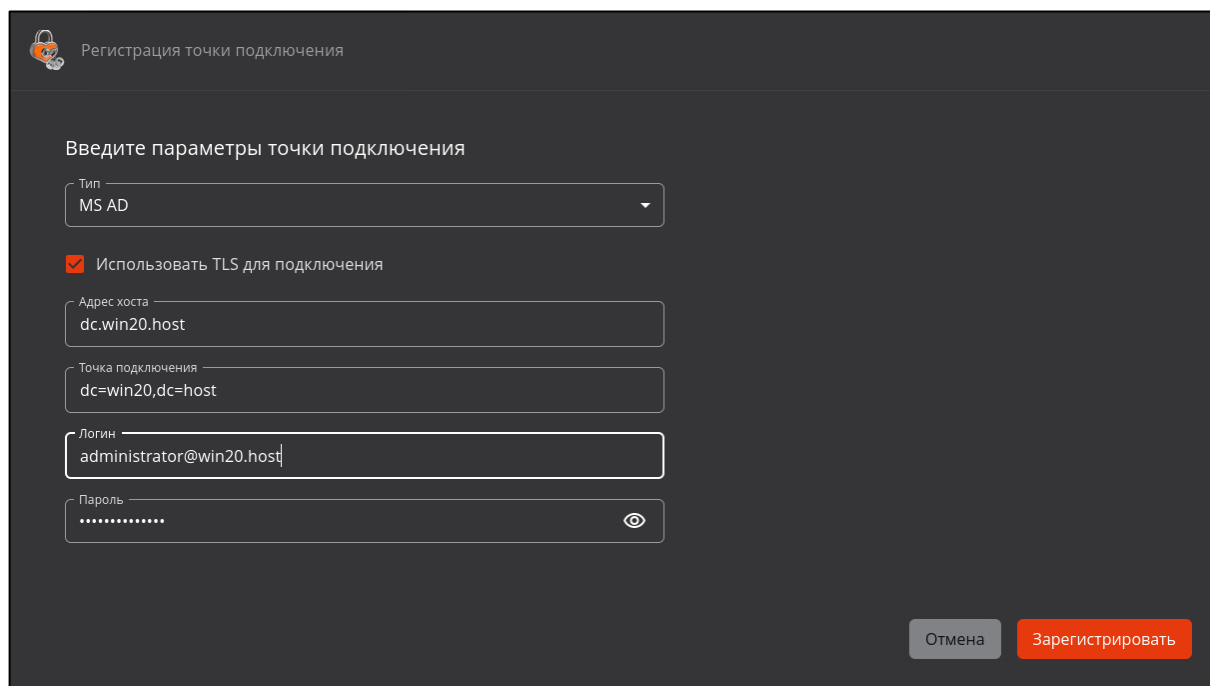
Точка подключения
dc=freeipa,dc=domain

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

Пароль
.....

Отмена Зарегистрировать

Рисунок 132 – Пример регистрации ресурсной системы FreeIPA



Регистрация точки подключения

Введите параметры точки подключения

Тип
MS AD

☒ Использовать TLS для подключения

Адрес хоста
dc.win20.host

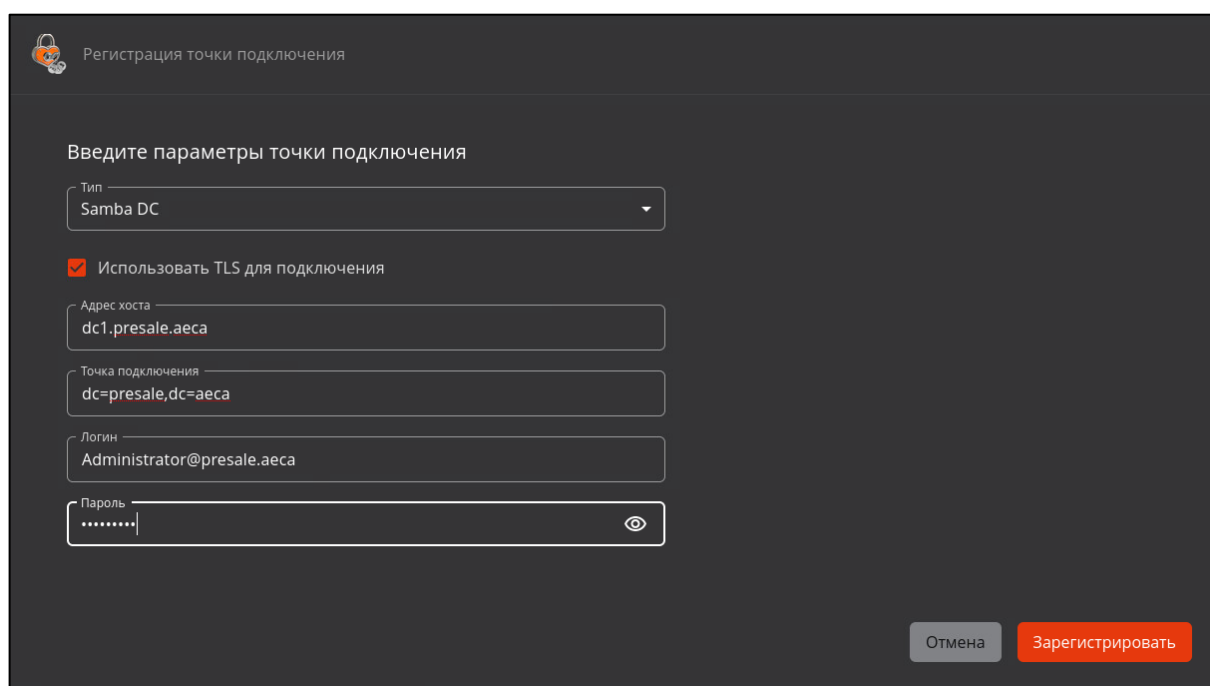
Точка подключения
dc=win20,dc=host

Логин
administrator@win20.host

Пароль
.....

Отмена Зарегистрировать

Рисунок 133 – 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 134 – Пример регистрации ресурсной системы Samba DC

Рисунок 135 – Пример регистрации ресурсной системы Альт Домен

Рисунок 136 – 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 137).

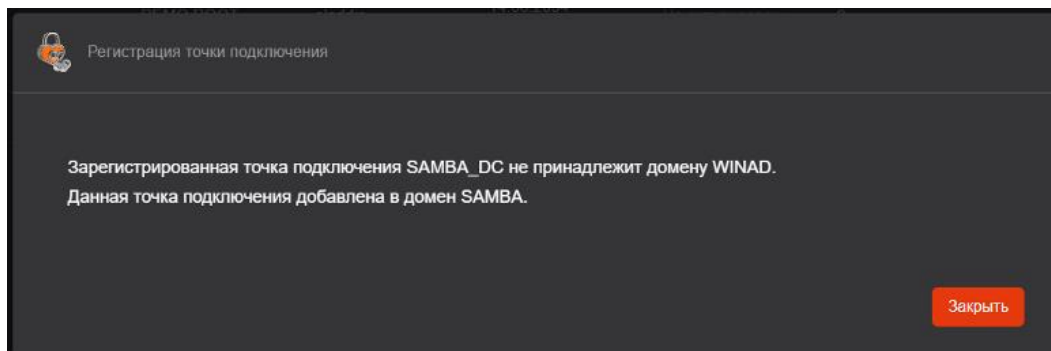


Рисунок 137 – Модальное окно с информацией о принадлежности регистрируемой точки подключения другой ресурсной системе

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

9.9.2 Карточка ресурсной системы

Просмотр информации о ресурсной системе возможен в ее карточке. Переход к «Карточке ресурсной системы» (см. Рисунок 138) осуществляется при нажатии на строку ресурсной системы в разделе «Ресурсные системы» (см. Рисунок 130).

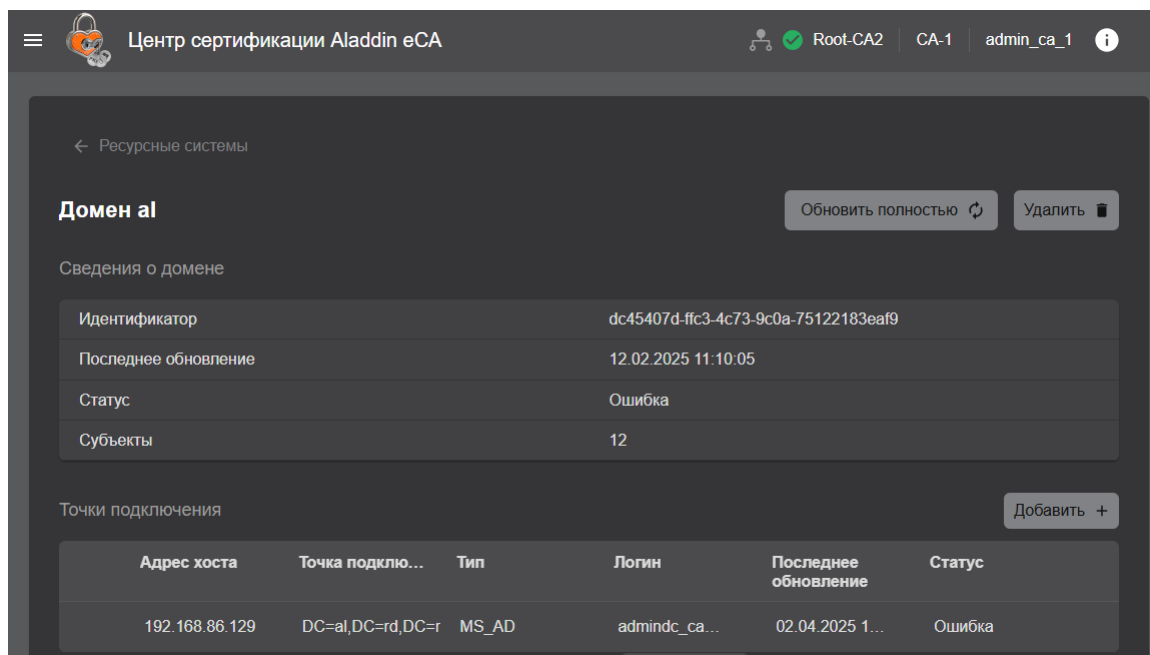


Рисунок 138 – Карточка ресурсной системы


В карточке ресурсной системы представлена следующая информация:

- имя домена;
- уникальный идентификатор ресурсной системы;
- дата и время последней попытки полной синхронизации ресурсной системы;
- статус ресурсной системы, который назначается в соответствии с критериями, приведенными в таблице выше (Таблица 22);
- количество субъектов, полученных из ресурсной системы.

- информация о точках подключения ресурсной систем:
 - адрес хоста – полное доменное имя или IP–адрес точки подключения ресурсной системы;
 - точка подключения – Base DN (Distinguished Name) уникальный идентификатор корневого объекта в LDAP–каталоге, который содержит в своем DN–объекты, получаемые из точки подключения;
 - тип – тип ресурсной системы: SambaDC, Альт домен, ALD PRO, MS_AD, FreeIPA, RED ADM.
 - логин (имя) учетной записи администратора контроллера домена;
 - дата и время последней попытки синхронизации точки подключения;
 - статус точки подключения, который назначается в соответствии с критериями, приведенными в таблице ниже (Таблица 23);

Таблица 23 – 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 9.9.3.4);
- удаление точки подключения зарегистрированной ресурсной системы (см. раздел 9.9.6).

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

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

В карточке ресурсной системы доступны следующие действия:

- запуск полной синхронизации ресурсной системы (см. раздел 9.9.3.3);
- удаление зарегистрированной ресурсной системы (см. Раздел 9.9.5);
- регистрация новой точки подключения к ресурсной системе (см. раздел 9.9.1);
- запуск частичной синхронизации точки подключения (см. раздел 9.9.3.4);
- изменение параметров, указанные при регистрации точки подключения (см. раздел 9.9.4);
- удаление точки подключения (см. раздел 9.9.6).

9.9.3 Синхронизация ресурсных систем

9.9.3.1 Виды синхронизации ресурсных систем

Центр сертификации Aladdin eCA поддерживает следующие виды синхронизации:

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

- Частичная.

При частичной синхронизации выполняется синхронизация всех данных выбранных точек подключения к ресурсной системе, полученных при полной синхронизации, за исключением сведений об удалении субъектов и групп безопасности из ресурсной системы.

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

Синхронизация ресурсной системы производится постранично¹. 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`.

9.9.3.2 Режимы синхронизации ресурсных систем

- Автоматический режим синхронизации.

В данном режиме синхронизация всех зарегистрированных точек подключения к ресурсным системам выполняется по расписанию в соответствии с CRON-выражением, указанным в конфигурационном файле `/opt/aecaCa/scripts/config.sh`:

- для задания расписания полной синхронизации укажите значение CRON-выражения для параметра `ldap_synch_resource` (значение по умолчанию `'0 0 0 * * *'` – запуск полной синхронизации каждую полночь);
- для задания расписания частичной синхронизации укажите значение CRON-выражения для параметра `ldap_synch_connection_point` (значение по умолчанию `'0 */30 * * * *'` – запуск частичной синхронизации каждые полчаса).

- Автоматизированный режим синхронизации.

В данном режиме запуск синхронизации выполняется по команде пользователя с ролью «Администратор»:

- запуск полной синхронизации выбранных ресурсных систем (см. раздел 9.9.3.3).
- запуск частичной синхронизации выбранных точек подключения к ресурсным системам (см. раздел 9.9.3.4)

9.9.3.3 Полная синхронизация ресурсной системы в автоматизированном режиме

Запуск полной синхронизации ресурсной системы может осуществляться путем нажатия на кнопку **<Обновить>** для ресурсной системы в разделе «Ресурсные системы» (см. Рисунок 139) или путем нажатия на кнопку **<Обновить полностью>** в карточке ресурсной системы (см. Рисунок 138).

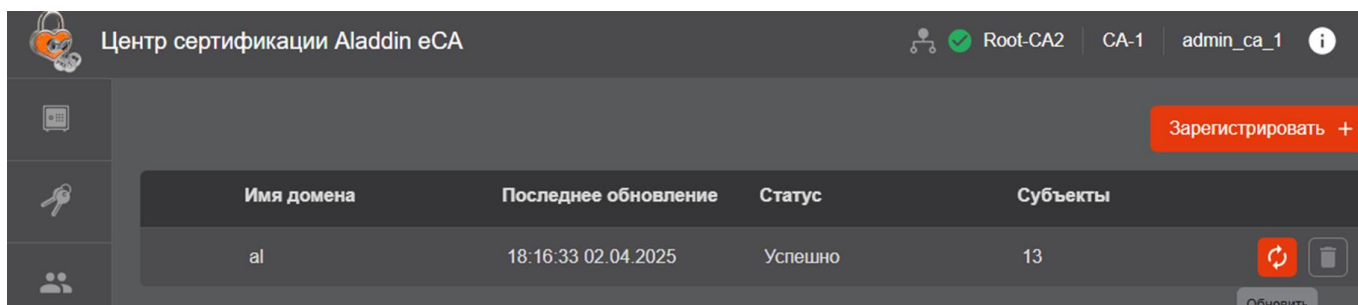


Рисунок 139 – Запуск полной синхронизации ресурсной системы из раздела «Ресурсные системы»

9.9.3.4 Частичная синхронизация точки подключения в автоматизированном режиме

Запуск частичной синхронизации точки подключения осуществляется путем нажатия на кнопку **<Обновить>** для выбранной точки подключения в карточке ресурсной системы (см. Рисунок 140).

¹ Центр сертификации Aladdin eCA получает данные из ресурсной системы частями, выполняя несколько запросов с ограничением на максимальное количество выдаваемых объектов вместо одного запроса на выгрузку сразу всех данных.

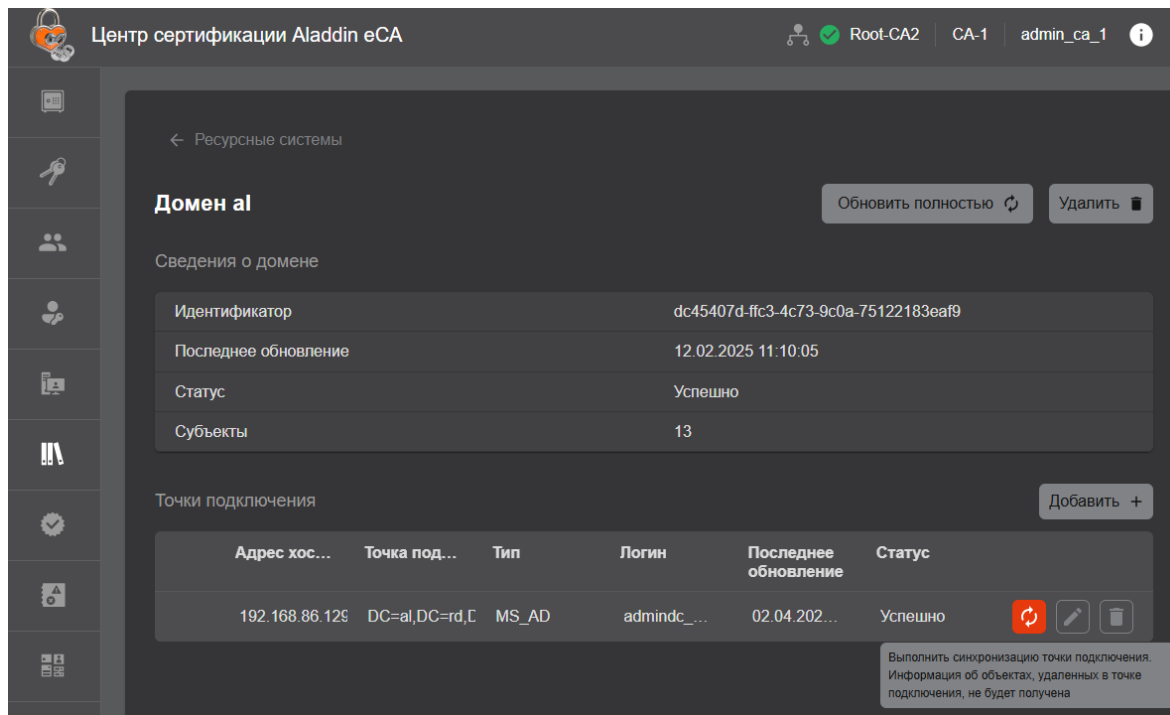



Рисунок 140 – Запуск частичной синхронизации точки подключения

9.9.4 Редактирование параметров точки подключения

Для редактирования параметров точки подключения необходимо в карточке ресурсной системы нажать на кнопку **<Редактировать>**  около точки подключения (см. Рисунок 141).

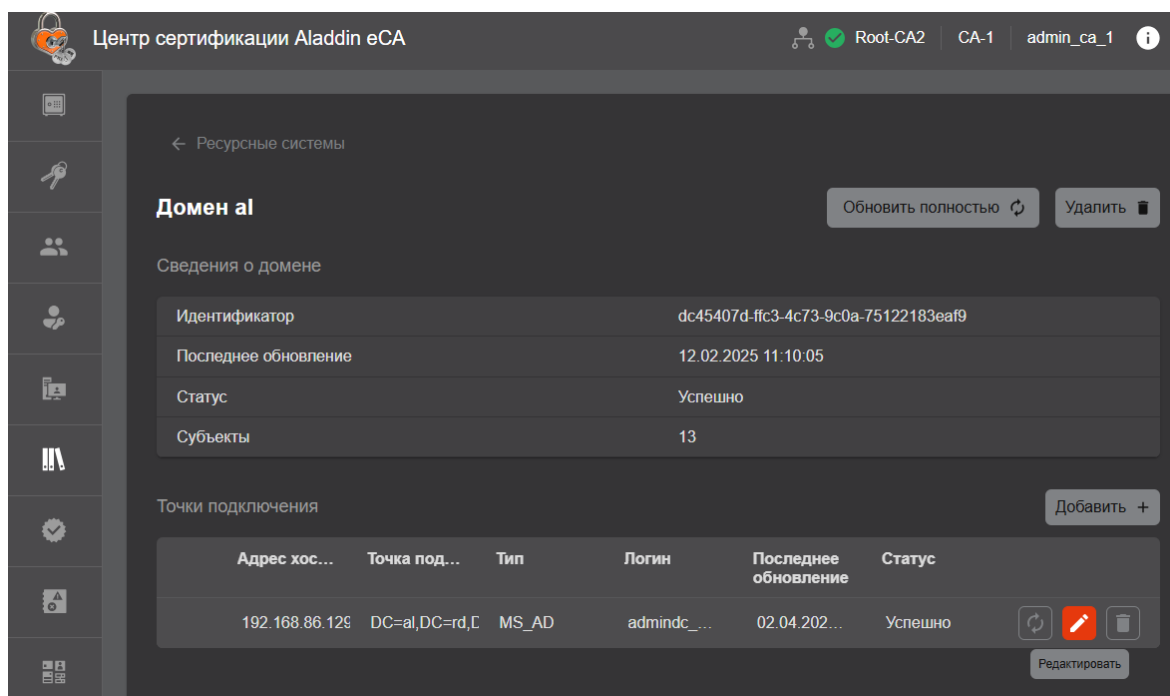


Рисунок 141 – Окно раздела «Ресурсная система». Кнопка редактирования РС

После этого открывается окно для редактирования полей, заполненных при создании точки подключения. Тип подключаемого ресурса изменить невозможно (см. Рисунок 142).

Рисунок 142 – Окно редактирования подключения к РС

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

9.9.5 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 143) или путем нажатия на кнопку **<Удалить>** в карточке ресурсной системы (см. Рисунок 138).

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

Рисунок 143 – Удаление ресурсной системы из раздела «Ресурсные системы»

- После этого отобразится окно подтверждения выбранного действия (см. Рисунок 144).

Рисунок 144 – 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.

9.9.6 Удаление точки подключения к ресурсной системе

Удаление точки подключения осуществляется путем нажатия на кнопку **<Удалить>** для точки подключения в карточке ресурсной системы (см. Рисунок 145).

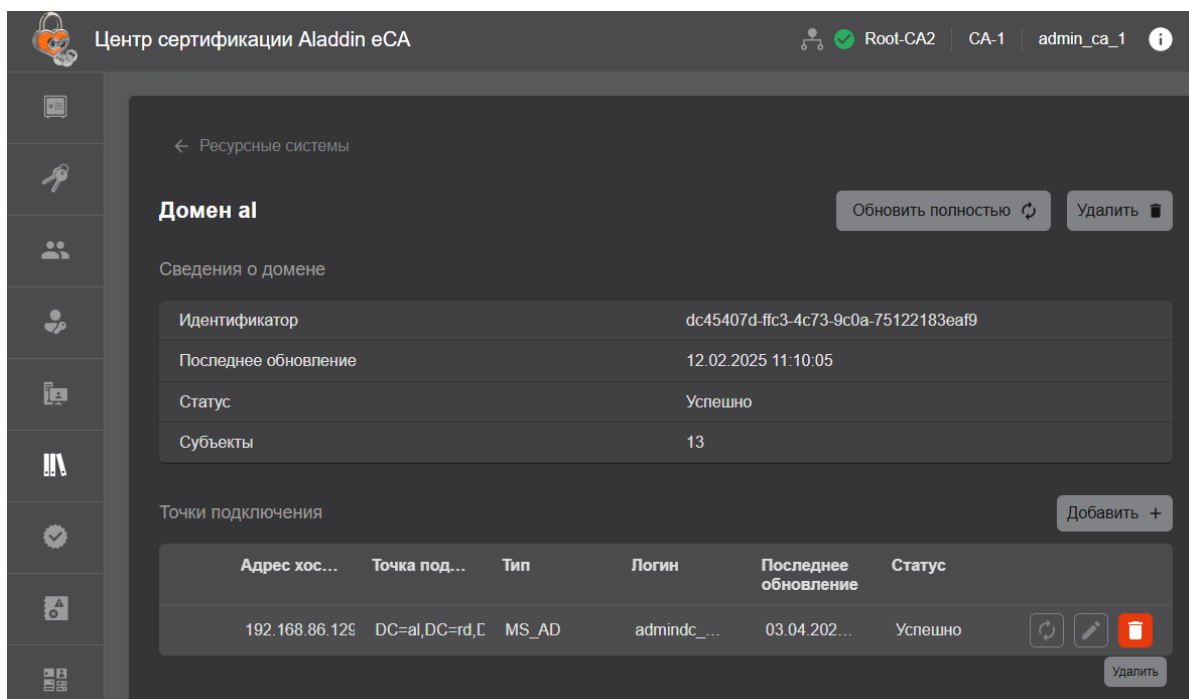


Рисунок 145 – Удаление ресурсной системы из карточки ресурсной системы

После этого отобразится окно подтверждения выбранного действия (см. Рисунок 146).

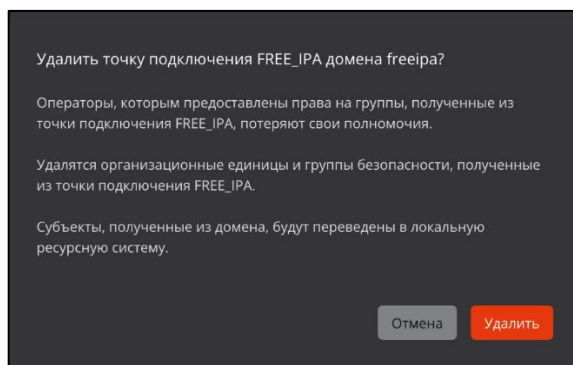


Рисунок 146 – Окно подтверждения удаления точки подключения

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.

9.10 Раздел «Центры валидации»

Переход в раздел «Центры валидации» выполняется через боковое меню, расположенное слева на главном экране (см. Рисунок 147). Данный раздел доступен только для пользователя с ролью «Администратор».

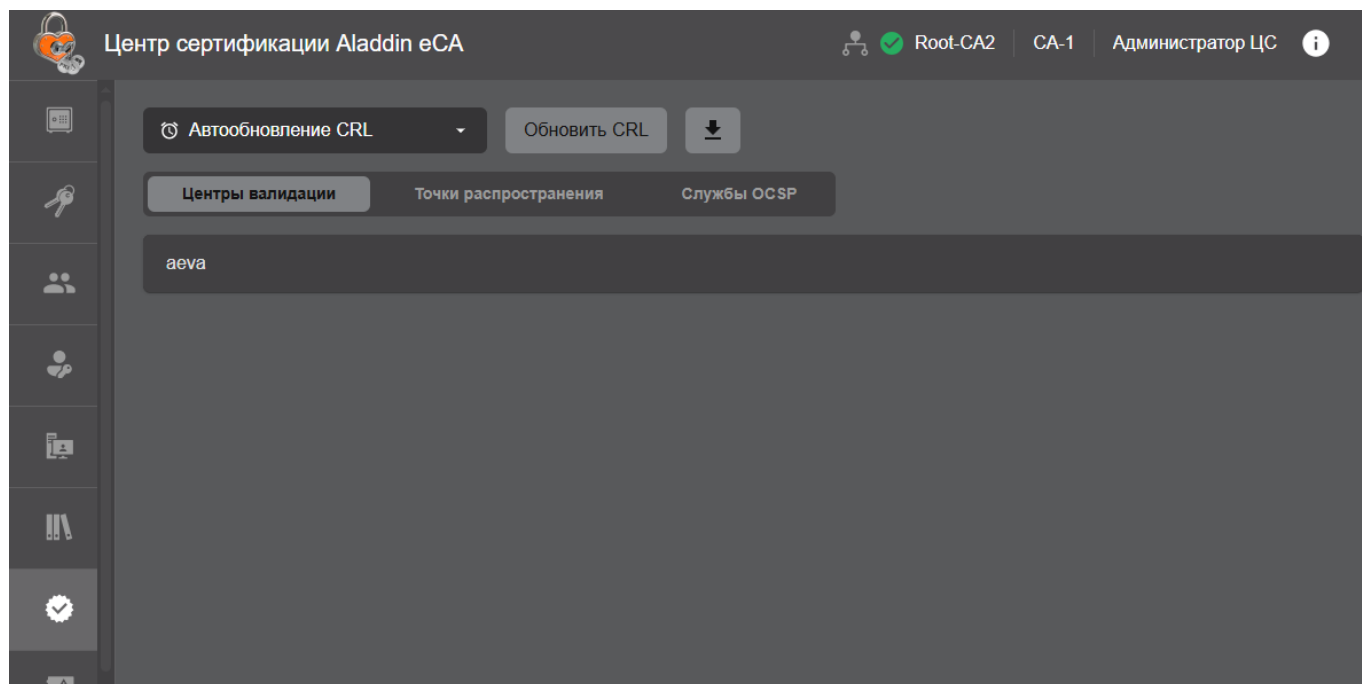


Рисунок 147 – Раздел «Центр валидации»

Раздел «Центры валидации» предназначен для выполнения следующих сценариев:

- Автоматизированная 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.

9.10.1 Настройка периодичности автоматического обновления CRL

Чтобы настроить периодичность автоматического обновления CRL и формирования Delta CRL, на верхней панели раздела «Центр валидации» раскройте список **<Автообновление CRL>** (см. Рисунок 148).

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.

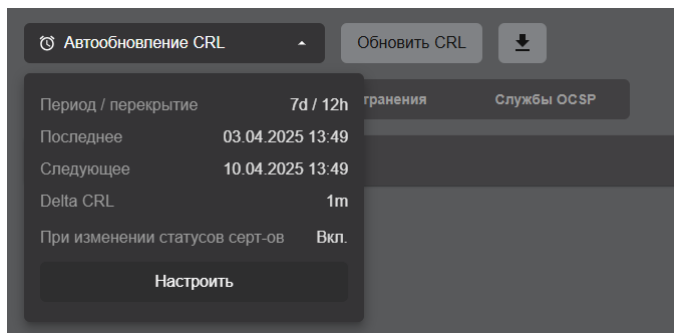


Рисунок 148 – Просмотр настроек автоматического обновления CRL

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 148).
- В открывшемся окне выполните настройку следующих параметров автоматического обновления CRL (см. Рисунок 149):

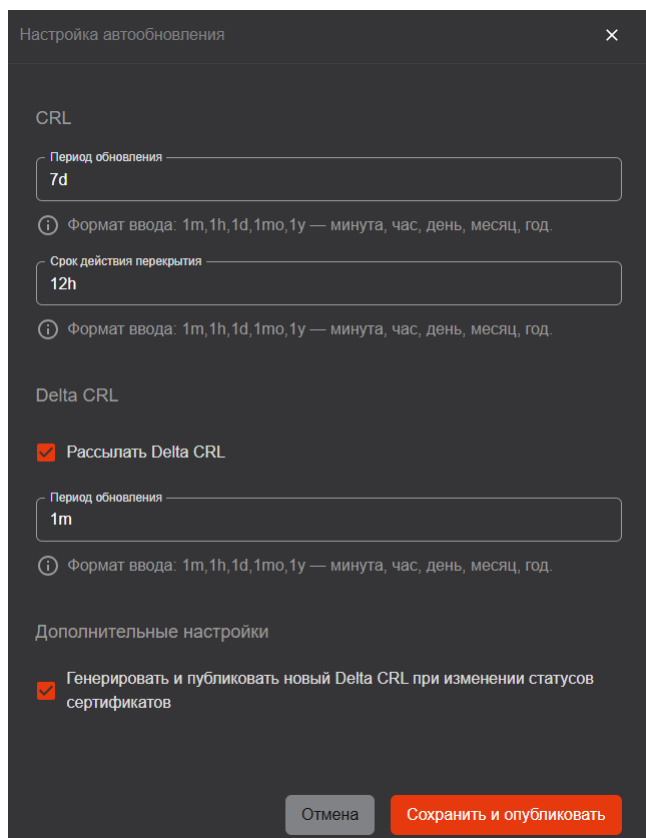


Рисунок 149 – Настройка автоматического обновления CRL

- 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 включенной рассылке Delta CRL).

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

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, приведенные ниже.
- Срок действия перекрытия (crlOverlapTime) не должен быть больше периода обновления Delta CRL (deltacrlperiod), если выполняется следующее условие, приведенное ниже.
- Срок действия перекрытия (crlOverlapTime) не должен быть меньше 1/5 от интервала рассинхронизации времени в сети (обычная рассинхронизация составляет не более 10 мин).

Файлы CRL содержат следующие данные, указывающие на время действия списка отозванных сертификатов:

- <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.

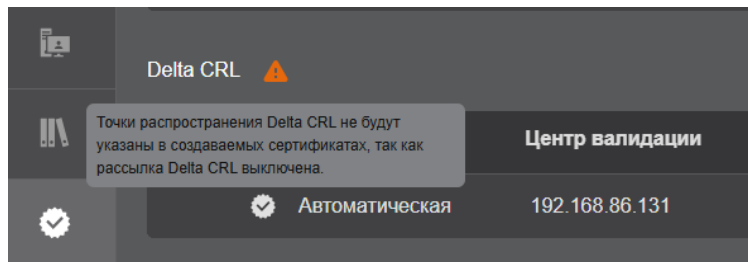


Рисунок 150 – Индикация точки распространения Delta CRL при выключенной рассылке Delta CRL

9.10.2 Автоматизированная публикация списка отозванных сертификатов CRL

Список отозванных сертификатов может быть обновлен внепланово по команде уполномоченного пользователя с ролью «Администратор». Для этого на верхней панели вкладки «Центры валидации» раздела «Центры валидации» нажмите кнопку **<Обновить CRL>** (см. Рисунок 151). 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`).

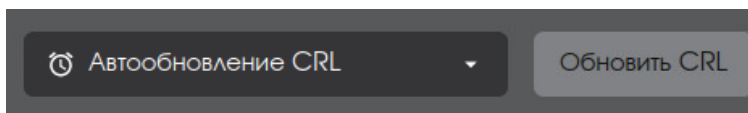



Рисунок 151 – Обновление CRL по команде администратора

9.10.3 Экспорт актуального списка отозванных сертификатов CRL

Для выгрузки списка отозванных сертификатов CRL выполните следующие действия:

- На верхней панели вкладки «Центры валидации» раздела «Центры валидации» нажмите кнопку **<Скачать CRL>** .
- В открывшемся окне в зависимости от текущего состояния Центра сертификации Aladdin eCA выполните одно из следующих действий:
 - Если в Центре сертификации Aladdin eCA не зарегистрирован ни один ЦВ и CRL ранее не публиковался, то опубликуйте и выгрузите новый CRL (см. Рисунок 152). Для этого в соответствующем поле укажите срок действия CRL и нажмите кнопку **<Сгенерировать и скачать>**.

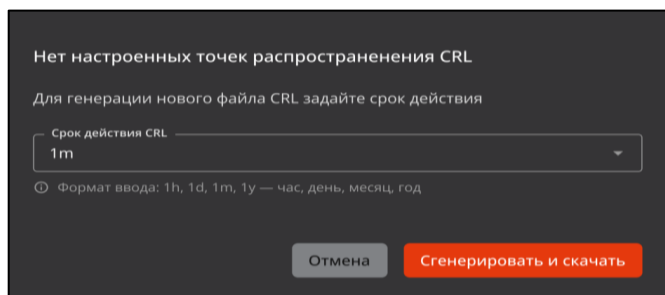


Рисунок 152 – Публикация и выгрузка нового CRL

- Если в Центре сертификации Aladdin eCA не зарегистрирован ни один ЦВ, а CRL ранее публиковался, то выполните одно из следующих действий (см. Рисунок 153):

- 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 153 – Выгрузка последнего опубликованного CRL

- Если в Центре сертификации Aladdin eCA зарегистрирован хотя бы один ЦВ, скачайте последний опубликованный CRL, нажав кнопку **<Скачать последний>** (см. Рисунок 154).

Рисунок 154 – Выгрузка последнего опубликованного CRL

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

9.10.4 Управление центрами валидации

Процесс регистрации ЦВ заключается в активации служб AIA и CRL DP. Создание ЦВ выполняется уполномоченным администратором в Центре валидации Aladdin eVA. Порядок создания ЦВ приведен в документе «Центр сертификатов доступа Aladdin Enterprise Certificate Authority Certified Edition. Руководство администратора. Часть 4. Центр валидации Aladdin Enterprise Validation Authority». После регистрации ЦВ создаются службы CRL DP и AIA, а в карточке центра валидации Центра сертификации появляются их адреса.

Для просмотра карточки центра валидации (см. Рисунок 155) перейдите на вкладку «Центры валидации» раздела «Центры валидации» и щелкните в списке строку с выбранным центром валидации.

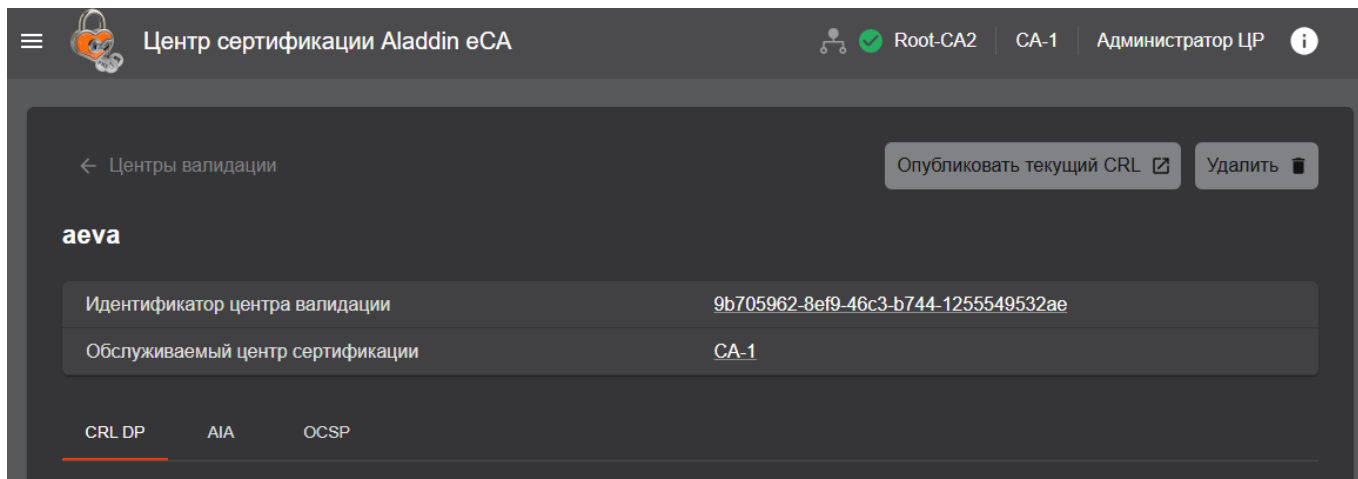





Рисунок 155 – Карточка зарегистрированного центра валидации

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 156) подтвердите удаление, нажав кнопку .

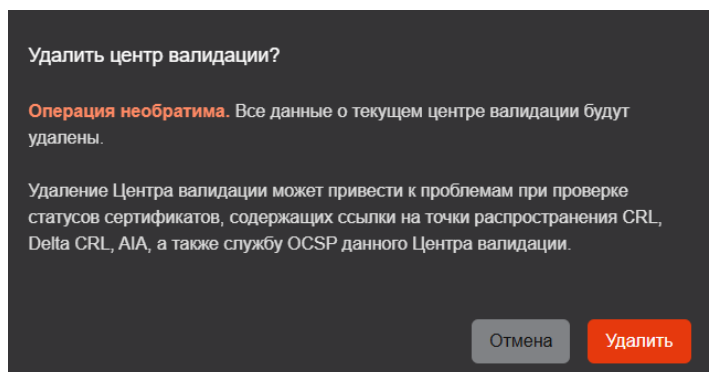



Рисунок 156 –Подтверждение удаления центра валидации

- Для службы CRL DP на вкладке «CRL DP» (см. Рисунок 157) 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. 9.10.8). Чтобы скопировать URL в буфер обмена, щелкните рядом с URL значок .

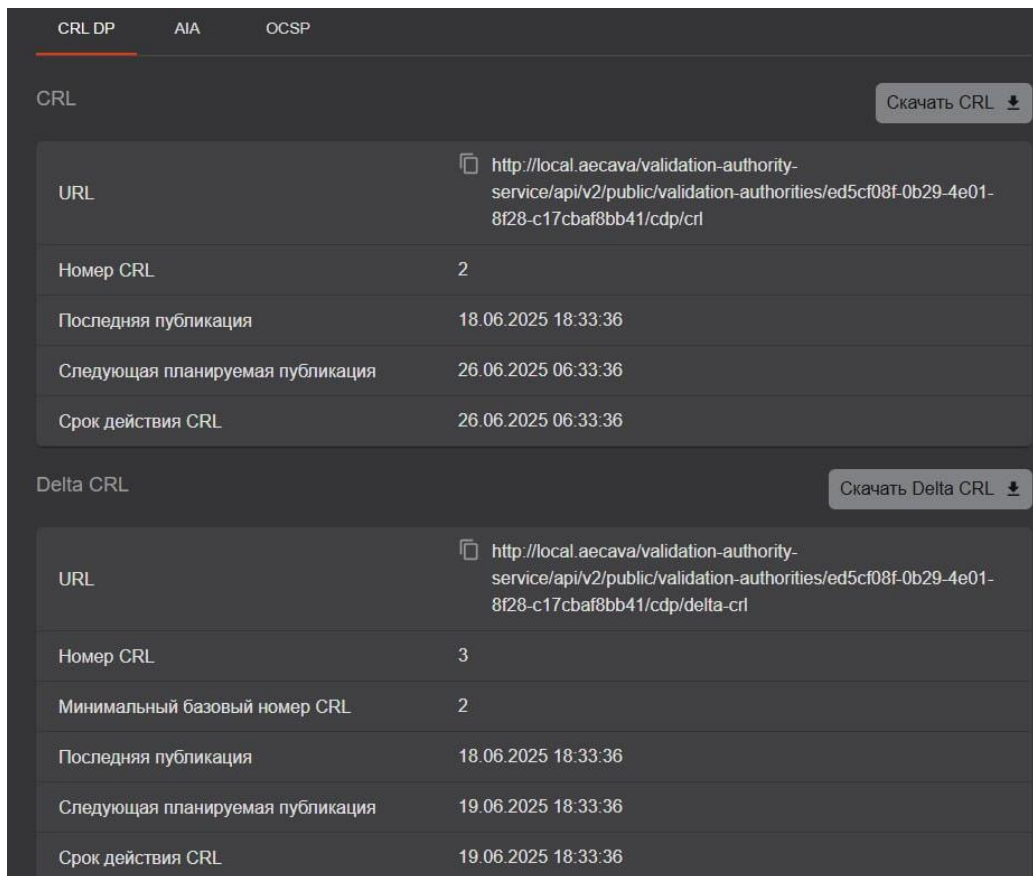


Рисунок 157 – Вкладка «CRL» карточки центра валидации

- Просмотр URL выгрузки DELTA CRL, который будет включаться в выпускаемые сертификаты (см. 9.10.8). Чтобы скопировать URL в буфер обмена, щелкните 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 158) 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 9.10.8). Чтобы скопировать URL в буфер обмена, щелкните 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 159) доступны следующие действия:
 - Просмотр URL OCSP-сервера. URL будет включаться в выпускаемые сертификаты (см. раздел 9.10.8). Чтобы скопировать URL в буфер обмена, щелкните рядом с адресом OCSP значок .
 - Просмотр статуса OCSP-службы.

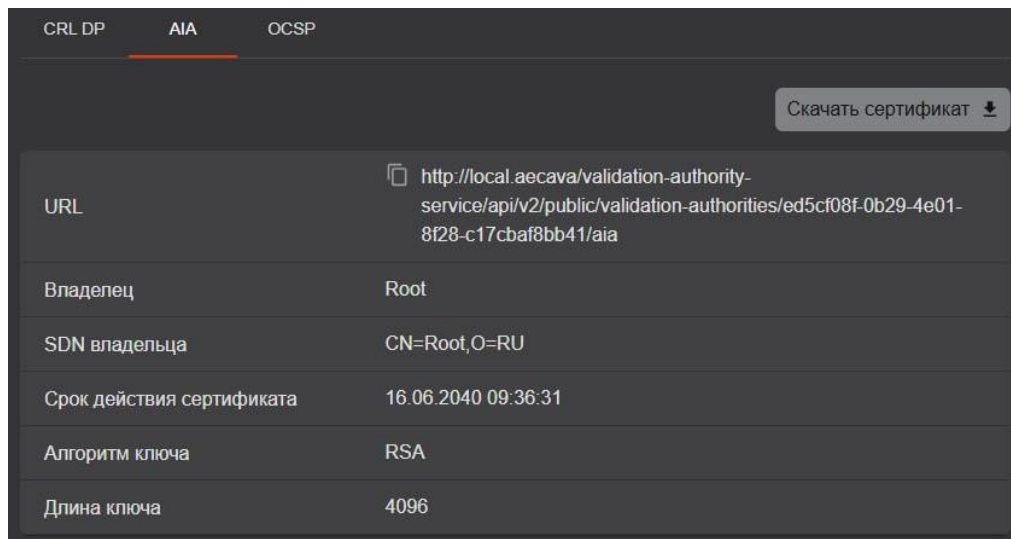


Рисунок 158 – Вкладка «AIA» карточки центра валидации

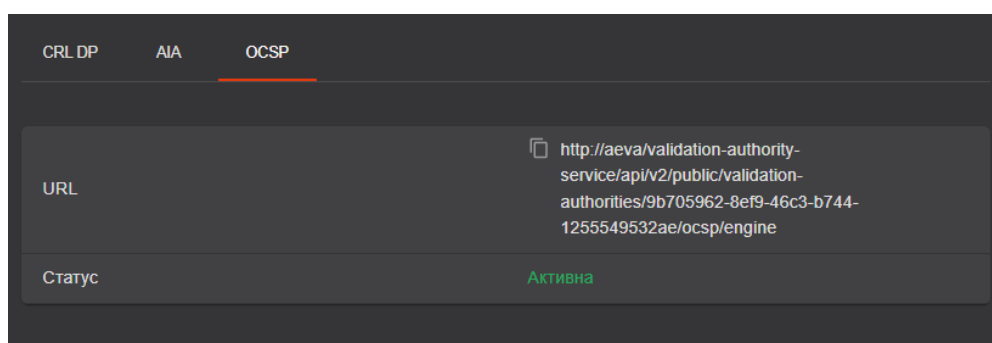




Рисунок 159 – Вкладка «OCSP» карточки центра валидации

9.10.5 Управление точками распространения

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

- Просмотра URL точек распространения CRL, Delta CRL и AIA, подключенных Центров валидации Aladdin eCA, образующих **автоматические точки распространения**. Данные точки распространения обозначены в списках значком  (поле «Тип»).
- Регистрации, редактирования и удаления внешних точек распространения CRL, Delta CRL и AIA, образующих **пользовательские точки распространения**. Данные точки распространения обозначены в списках значком  (поле «Тип»);
- Управления режимом публикации CRL, Delta CRL и AIA в LDAP–каталог ресурсных систем (доменные службы каталогов) пользовательских точек распространения.
- Управления записью точек распространения в выпускаемые сертификаты.
- Управления приоритетами точек распространения. Приоритет определяет очерёдность записи URL точек распространения в сертификаты субъектов (см. раздел 9.10.8).
- 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 160):

- Тип – тип точки распространения (автоматическая или пользовательская).
- Центр валидации – IP–адрес или полное доменное имя компьютера с установленным Центром валидации Aladdin eCA (только для автоматических точек распространения).
- URL – адрес сервера точки распространения.
- Приоритет – числовое значение от 0 до 1000.

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

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

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

Рисунок 160 – 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.

9.10.5.1 Создание пользовательской точки распространения

Пользовательские точки предназначены для распространения:

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

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

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

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

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

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

Пример URL для точки распространения CRL:

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

Пример URL для точки распространения Delta CRL:

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

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

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

Порядок создания пользовательской точки распространения:

- Перейдите на вкладку «Точки распространения» раздела «Центры валидации».
- Нажмите кнопку **Создать** и выберите в списке «Пользовательская».
- В открывшемся окне (см. Рисунок 161) выполните следующие действия:

Рисунок 161 – 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 162) выполните следующие действия:

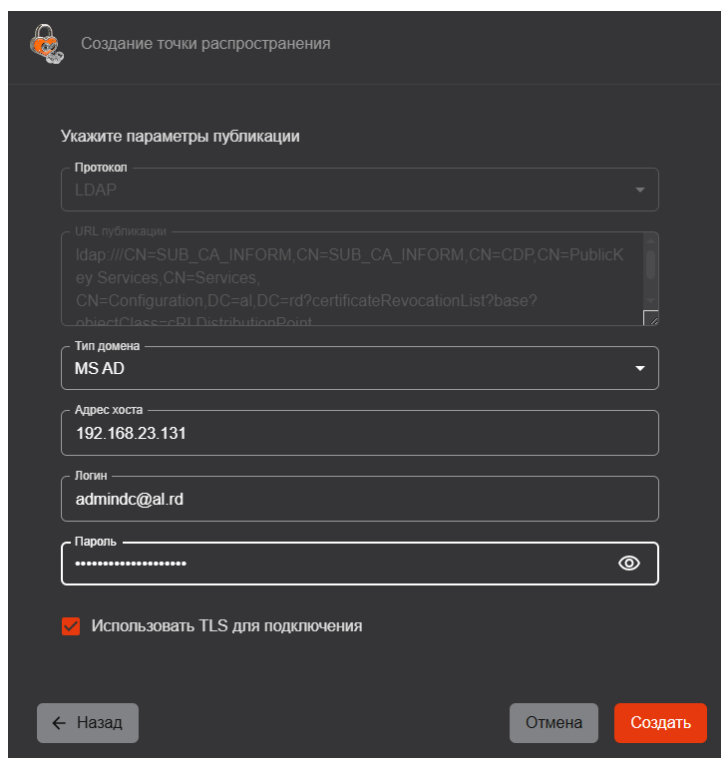



Рисунок 162 – Указание параметров публикации для точки распространения

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

9.10.5.2 Редактирование пользовательской точки распространения

Порядок редактирования пользовательской точки распространения:

- Перейдите на вкладку «Точки распространения» раздела «Центры валидации».
- Наведите указателем мыши на выбранную службу в списке и нажмите кнопку  **<Редактировать>** (см. Рисунок 163).

CRL









Тип	Центр ва...	URL	Приоритет	Дата изм...	Публикац...	Дата пуб...	Запись в сертификаты	
	—	https://ae...	15	07.05.20...	Ошибка	18.06.20...		 
	aeva	http://aev...	0	07.05.20...	Ошибка	18.06.20...		 Редактировать


Рисунок 163 – Инициализация процесса редактирования пользовательской точки распространения

- В открывшемся окне (см. Рисунок 164) выполните следующие действия:

 Редактирование точки распространения

URL точки распространения

Приоритет

 Формат ввода: число от 0 до 1000

☐ Публиковать CRL в точку распространения



 

Рисунок 164 – Редактирование пользовательской точки распространения

- При необходимости в соответствующих полях измените URL и приоритет точки распространения (описание и правила заполнения полей см. в разделе 9.10.5.1).
- Если режим публикации распространяемых данных в LDAP–каталог ресурсной системы выключен, а вы не хотите его включать, то нажмите кнопку **<Сохранить изменения>** для завершения процесса редактирования.
- Если режим публикации распространяемых данных в LDAP–каталог ресурсной системы включен, а вы хотите его выключить, снимите флажок **<Публиковать CRL в точку распространения>** (при редактировании точки распространения CRL), **<Публиковать Delta CRL в точку распространения>** (при редактировании точки распространения Delta CRL), **<Публиковать AIA в точку распространения>** (при редактировании точки распространения сертификатов издающих Центров сертификации) и нажмите кнопку **<Сохранить изменения>** для завершения процесса редактирования.
- Если режим публикации распространяемых данных в LDAP–каталог ресурсной системы включен, а вы не хотите его выключать, то нажмите кнопку **<Продолжить>** для изменения параметров публикации точки распространения.

- Если режим публикации распространяемых данных в LDAP–каталог ресурсной системы выключен, а вы хотите его включить, установите флажок **<Публиковать CRL в точку распространения>** (при редактировании точки распространения CRL), **<Публиковать Delta CRL в точку распространения>** (при редактировании точки распространения Delta CRL), **<Публиковать AIA в точку распространения>** (при редактировании точки распространения сертификатов издающих Центров сертификации) и нажмите кнопку **<Продолжить>** для указания параметров публикации точки распространения.
- В открывшемся окне (см. Рисунок 165) выберите тип доменной службы, укажите адрес контроллера домена, имя и пароль учетной записи администратора контроллера домена (описание и правила заполнения полей см. в разделе 9.10.5.1) и нажмите кнопку **<Сохранить изменения>**.

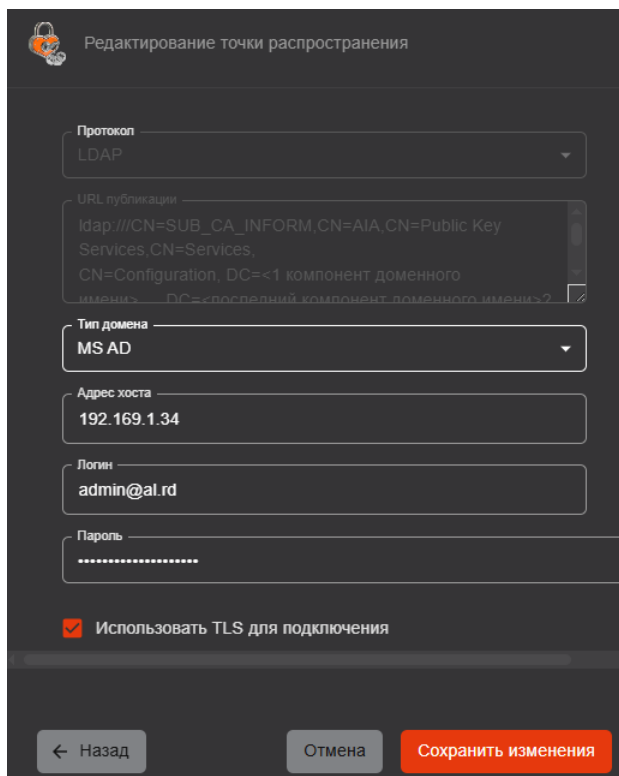



Рисунок 165 – Редактирование параметров публикации пользовательской точки распространения

9.10.5.3 Редактирование автоматической точки распространения

Для редактирования параметров автоматической точки распространения выполните следующие действия:

- Перейдите на вкладку «Точки распространения» раздела «Центры валидации».
- Наведите указателем мыши на выбранную автоматическую точку распространения в списке и нажмите кнопку  **<Редактировать>** (см. Рисунок 163).
- В открывшемся окне (см. Рисунок 166) в соответствующем поле измените приоритет автоматической точки распространения (описание и правила заполнения полей см. в разделе 9.10.5.1). После этого нажмите кнопку **<Продолжить>**.

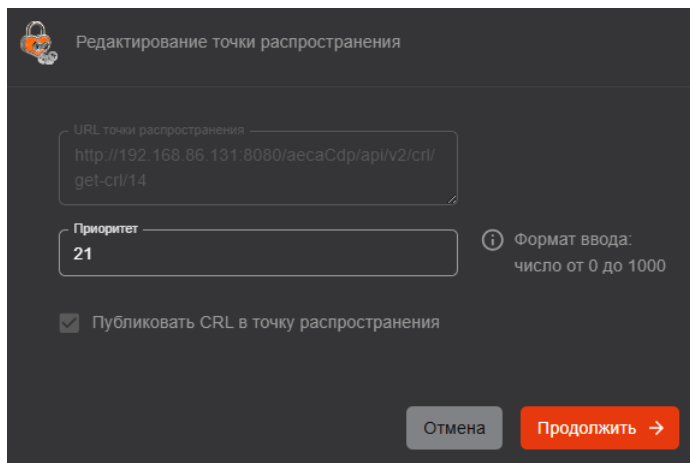


Рисунок 166 – Редактирование автоматической точки распространения

- В открывшемся окне (см. Рисунок 167) нажмите кнопку **<Сохранить изменения>**.

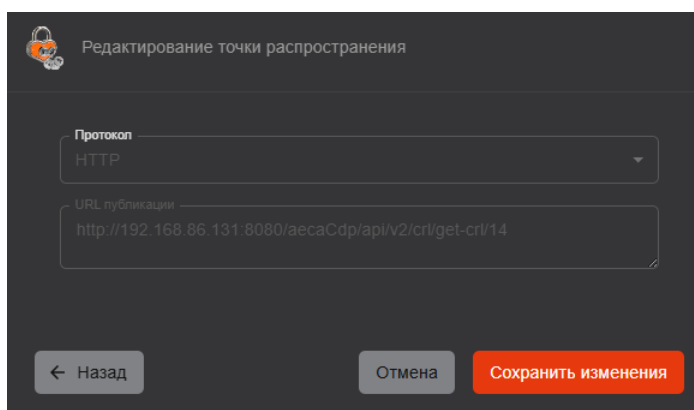



Рисунок 167 – Редактирование автоматической точки распространения

9.10.5.4 Удаление пользовательской точки распространения

Для удаления пользовательской точки распространения выполните следующие действия:

- Перейдите на вкладку «Точки распространения» раздела «Центры валидации».
- Наведите указателем мыши на выбранную автоматическую точку распространения в списке и нажмите кнопку  **<Удалить>** (см. Рисунок 168).











CRL								
	Тип	Центр валид...	URL	Приоритет	Дата изменен...	Публикация	Дата публика...	Запись в серти...
		—	https://aeca/v...	15	07.05.2025 1...	Ошибка	20.05.2025 1...	   
		aeva	http://aeva:80...	0	07.05.2025 1...	Ошибка	20.05.2025 1...	    Удалить

Рисунок 168 –Инициализация процесса удаления точки распространения

- В открывшемся окне (см. Рисунок 169) подтвердите удаление точки распространения, нажав кнопку **<Удалить>**.

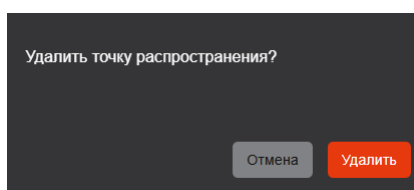


Рисунок 169 – Подтверждение удаления пользовательской точки распространения

9.10.5.5 Создание кластера точек распространения

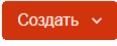
Объединения точек распространения в кластеры может потребоваться для проксирования доступа к ним с целью распределения нагрузки.

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

Создание кластера возможно двумя способами:

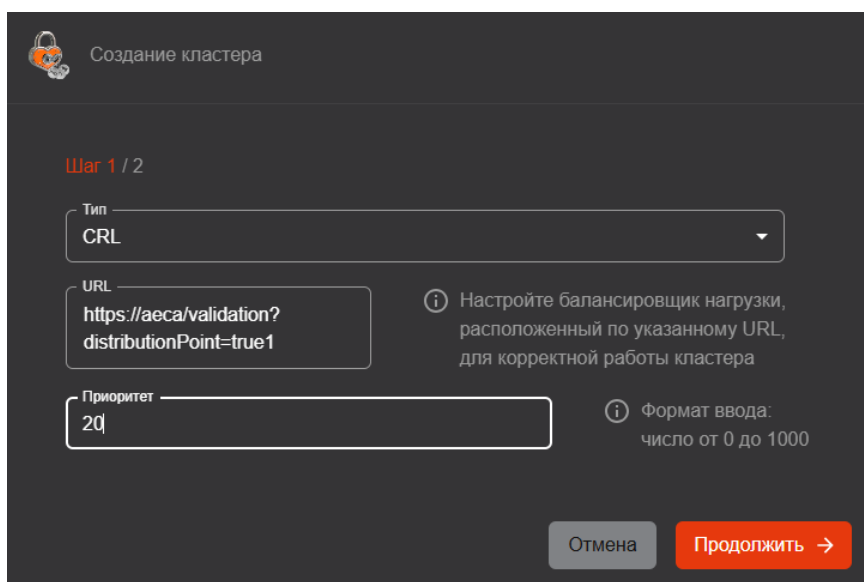
- Путем создания нового кластера и добавления в него уже существующих точек распространения.
- Путем создания кластера на базе ранее созданной точки распространения.

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

- Перейдите на вкладку «Точки распространения» раздела «Центры валидации».
- Нажмите кнопку  и выберите в списке «Кластер».
- В открывшемся окне (см. Рисунок 170) 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>**.



Создание кластера

Шаг 1 / 2

Тип: CRL

URL: `https://aeca/validation?distributionPoint=true1`



Приоритет: 20

Настройте балансировщик нагрузки, расположенный по указанному URL, для корректной работы кластера

Формат ввода: число от 0 до 1000

Отмена Продолжить →

Рисунок 170 – Создание кластера точек распространения. Шаг 1

- В открывшемся окне (см. Рисунок 171) выполните следующие действия:
 - В списке «Выбрать» с помощью флажков выберите URL точек распространения, которые необходимо объединить в кластер, и щелкните значок . В результате выбранные точки распространения будут перемещены в список «Выбрано».
 - Чтобы изменить список точек распространения, объединяемых в кластер, в списке «Выбрано» с помощью флажков выберите URL точек распространения, исключаемых из кластера, и щелкните значок . В результате выбранные точки распространения будут перемещены в список «Выбрать».
 - Чтобы найти точки распространения в списках, используйте поля поиска.
 - Нажмите кнопку **<Создать кластер>**.

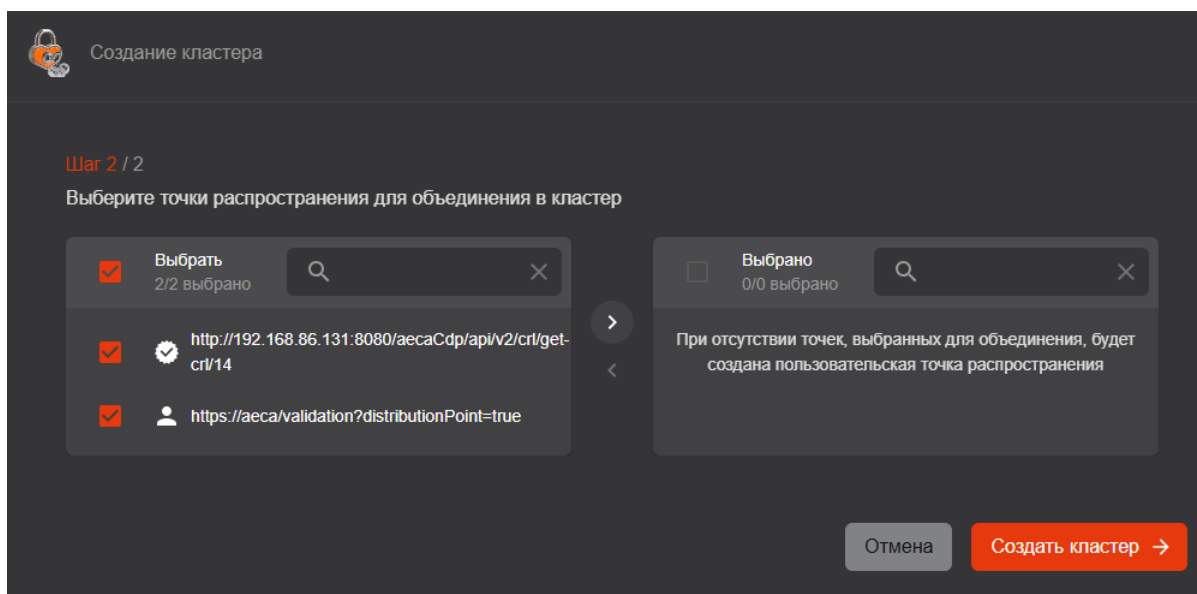



Рисунок 171 – Создание кластера точек распространения. Шаг 2

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 172).

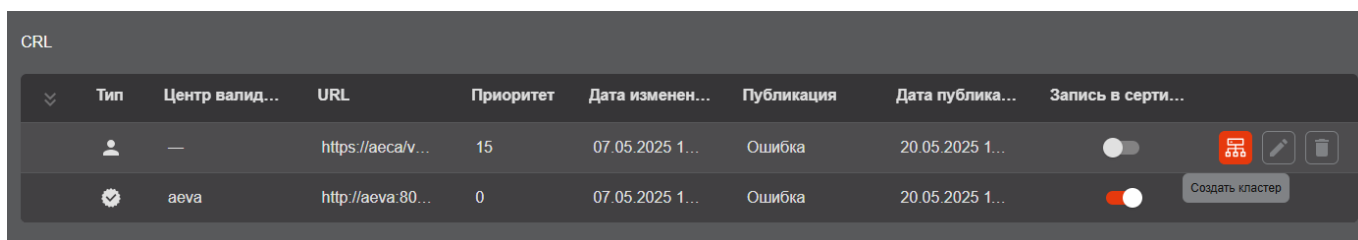





Рисунок 172 – Создание кластера на основе зарегистрированной точки распространения

- В открывшемся окне (см. Рисунок 171) выполните следующие действия:
 - В списке «Выбрать» с помощью флажков выберите URL точек распространения, которые необходимо объединить в кластер, и щелкните значок . В результате выбранные точки распространения будут перемещены в список «Выбрано».
 - Чтобы изменить список точек распространения, объединяемых в кластер, в списке «Выбрано» с помощью флажков выберите URL точек распространения, исключаемых из кластера, и щелкните значок .
 - Чтобы найти точки распространения в списках, используйте поля поиска.
 - Нажмите кнопку **<Создать кластер>**.

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

9.10.5.6 Просмотр состава кластера точек распространения

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

- Перейдите на вкладку «Точки распространения» раздела «Центры валидации».
- Раскройте состав кластер в списке. Для этого в строке выбранного кластера щелкните значок  (см Рисунок 173).

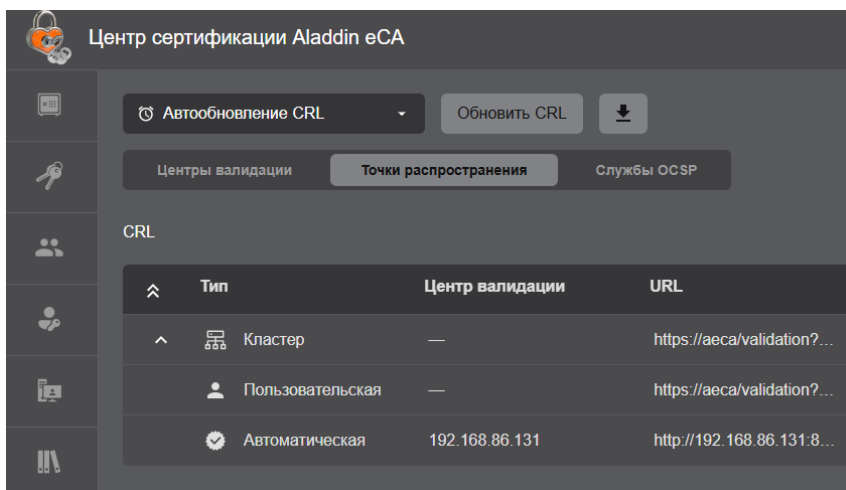




Рисунок 173 – Просмотр состава кластера точек распространения

- Чтобы скрыть состав кластера, щелкните значок .

9.10.5.7 Редактирование кластера точек распространения

Для редактирования состава кластера точек распространения выполните следующие действия:

- Перейдите на вкладку «Точки распространения» раздела «Центры валидации».
- Наведите указателем мыши на выбранный кластер в списке и нажмите кнопку  **<Редактировать кластер>** (см. Рисунок 174).

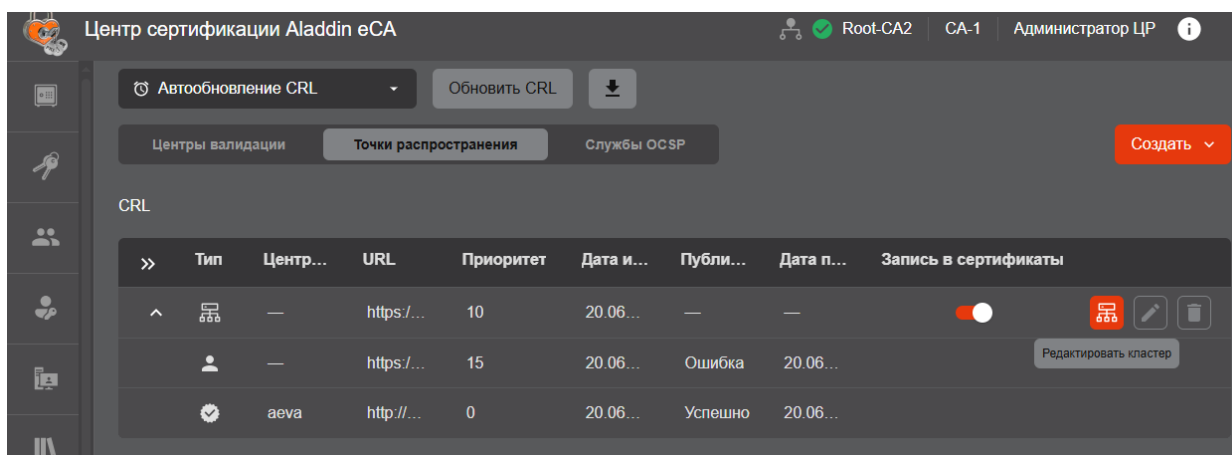


Рисунок 174 – Инициализация процесса редактирования кластера

- В открывшемся окне управления кластером (см. Рисунок 175) измените состав кластера и нажмите кнопку **<Сохранить изменения>**.

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

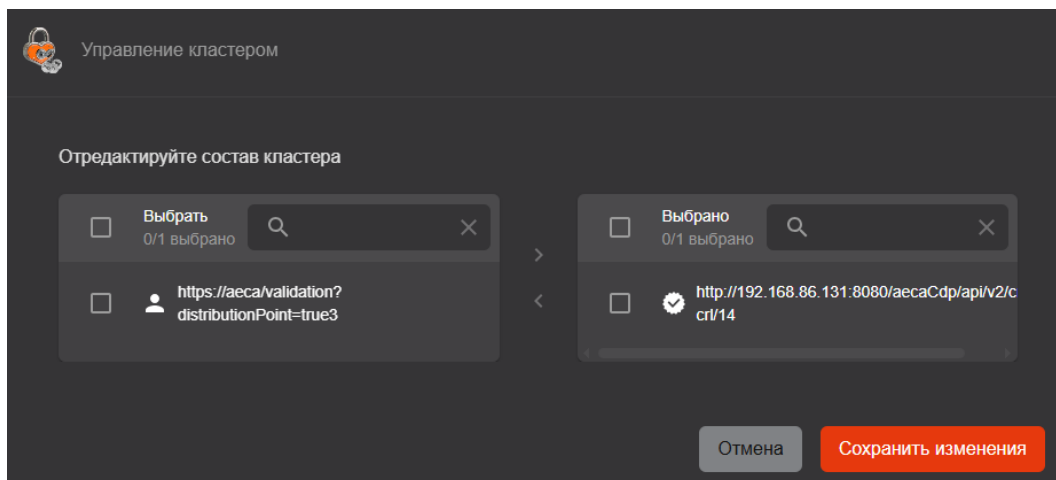



Рисунок 175 – Редактирование состава кластера

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 176).

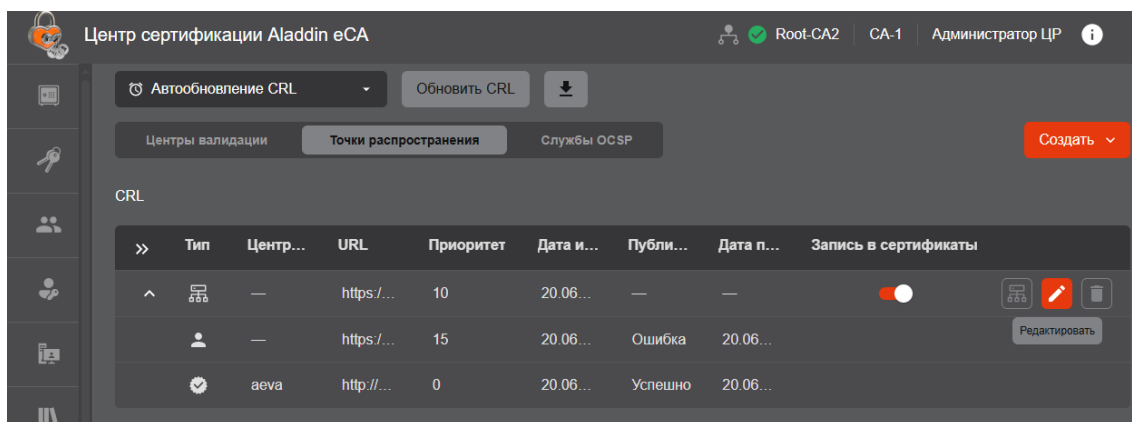


Рисунок 176 – Инициализация процесса редактирования параметров кластера

- В открывшемся окне (см. Рисунок 177) в соответствующих полях измените URL, приоритет кластера точек распространения и нажмите кнопку **«Сохранить изменения»**.

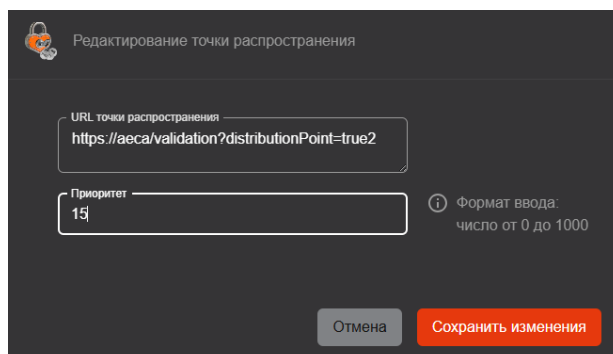



Рисунок 177 – Редактирование кластера точек распространения

9.10.5.8 Удаление кластера точек распространения

Для удаления кластера точек распространения выполните следующие действия:

- Перейдите на вкладку «Точки распространения» раздела «Центры валидации».
- Наведите указателем мыши на выбранный кластер в списке и нажмите кнопку  **<Удалить>** (см. Рисунок 178).

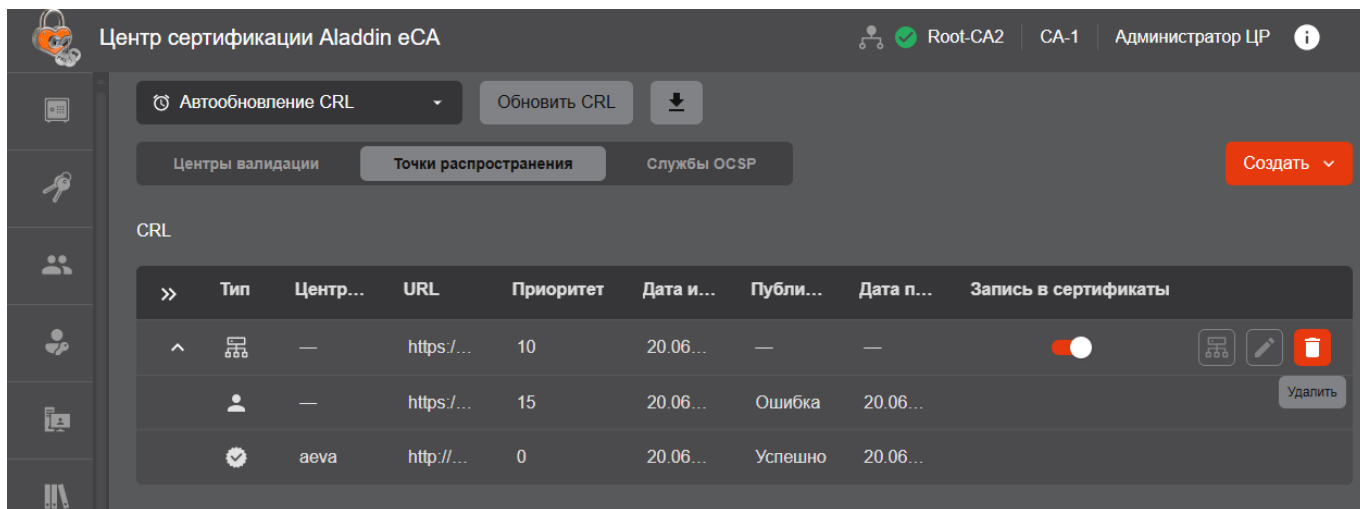


Рисунок 178 – Инициализация процесса удаления кластера

- В открывшемся окне (см. Рисунок 179) подтвердите удаление, нажав кнопку **<Удалить>**.

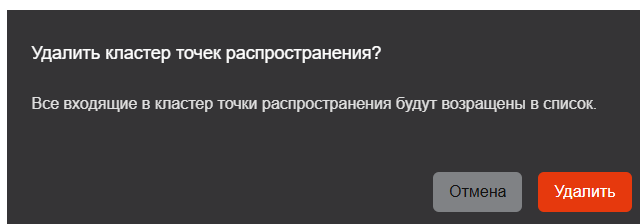




Рисунок 179 – Подтверждение удаления кластера

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

9.10.6 Управление службами OCSP

Управление службами OCSP предполагает:

- Просмотр URL служб OCSP, созданных в Центрах валидации Aladdin eVA, 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 eVA. 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 развертываемых 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 9.10.8).
- 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 Центром валидации Aladdin eVA (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.

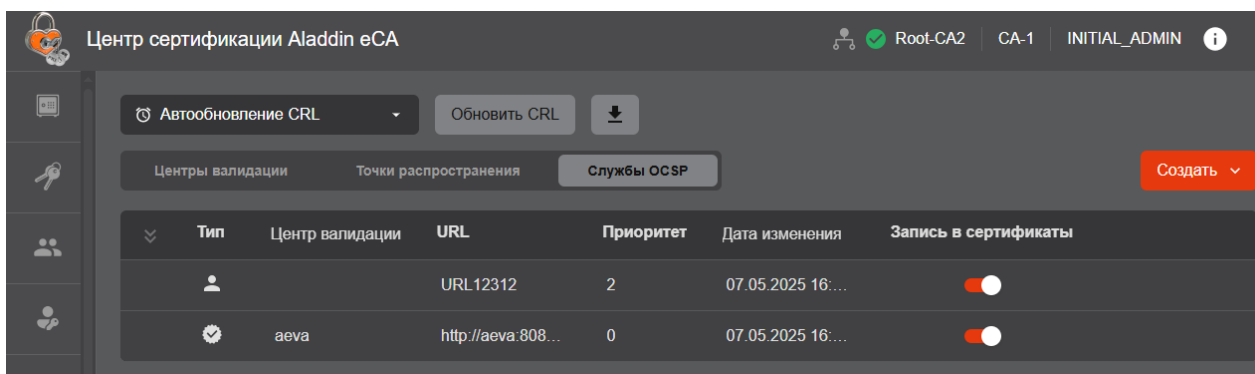


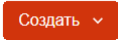
Рисунок 180 –Список служб OCSP

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.

9.10.6.1 Создание пользовательской службы OCSP

Порядок создания пользовательской службы OCSP:

- Перейдите на вкладку «Службы OCSP» раздела «Центры валидации».
- Нажмите кнопку  и выберите в списке «Пользовательская».
- В открывшемся окне (см. Рисунок 181) выполните следующие действия:
 - В поле «URL» укажите URL службы OCSP.

При указании URL возможны следующие сообщения об ошибках:

- «Указан URL существующей службы OCSP» – введенный URL совпадает с URL ранее зарегистрированной службы OCSP.
- «Некорректный ввод» – введенный URL содержит один и несколько пробелов.
- В поле «Приоритет» укажите приоритет службы OCSP (числовое значение от 0 до 1000).

Службы OCSP располагаются в списке в порядке убывания назначенного им приоритета. Если приоритеты служб OCSP совпадают, то выше в списке будет располагаться служба OCSP, в параметры которой изменения были внесены позднее, начиная с момента ее создания.


Рисунок 181 – Создание службы OSCP

- Нажмите кнопку **<Создать>**.

В результате будет создана пользовательская служба OSCP.

9.10.6.2 Редактирование пользовательской службы OSCP

Для редактирования параметров пользовательской службы OSCP выполните следующие действия:

- Перейдите на вкладку «Службы OSCP» раздела «Центры валидации».
- Наведите указателем мыши на выбранную службу в списке и нажмите кнопку  **<Редактировать>** (см. Рисунок 182).

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


Рисунок 182 –Инициализация процесса редактирования службы OSCP

- В открывшемся окне (см. Рисунок 183) в соответствующих полях измените URL и приоритет службы OSCP (описание и правила заполнения полей см. в разделе 9.10.6.1). После этого нажмите кнопку **<Сохранить изменения>**.

Рисунок 183 – Редактирования пользовательской службы OSCP

9.10.6.3 Редактирование автоматической службы OCSP

Для редактирования параметров автоматической службы OCSP выполните следующие действия:

- Перейдите на вкладку «Службы OCSP» раздела «Центры валидации».
- Наведите указателем мыши на выбранную автоматическую службу в списке и нажмите кнопку  **<Редактировать>** (см. Рисунок 182).
- В открывшемся окне (см. Рисунок 184) в соответствующем поле измените приоритет автоматической службы OCSP (описание и правила заполнения полей см. в разделе 9.10.6.1). После этого нажмите кнопку **<Сохранить изменения>**.

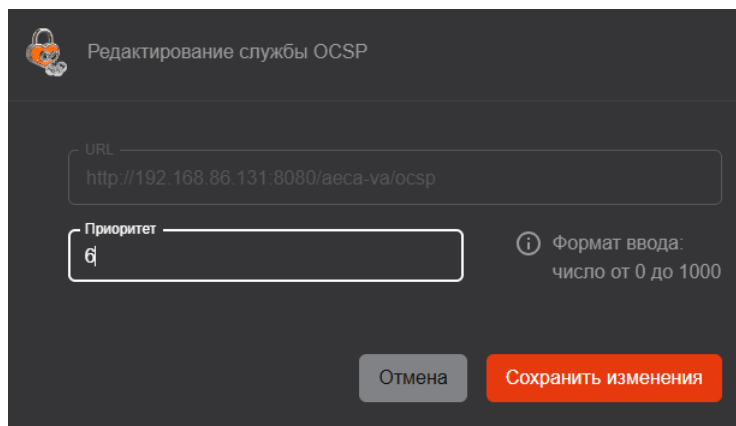



Рисунок 184 – Окно редактирования автоматической службы OCSP

9.10.6.4 Удаление пользовательской службы OCSP

Для удаления пользовательской службы OCSP выполните следующие действия:

- Перейдите на вкладку «Службы OCSP» раздела «Центры валидации».
- Наведите указателем мыши на выбранную службу в списке и нажмите кнопку  **<Удалить>** (см. Рисунок 185).

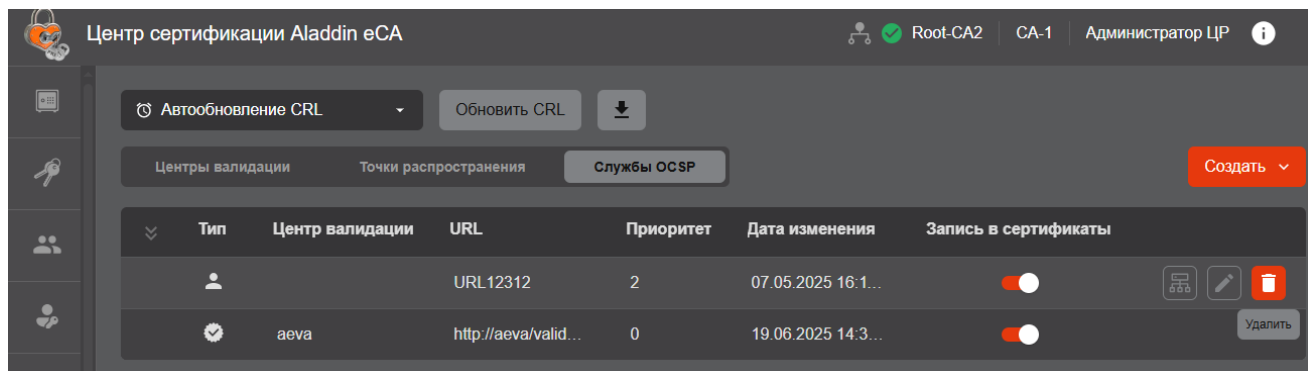


Рисунок 185 –Инициализация процесса удаления службы OCSP

- В открывшемся окне (см. Рисунок 186) подтвердите удаление службы, нажав кнопку **<Удалить>**.

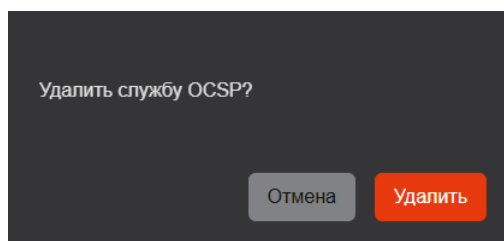


Рисунок 186 – Подтверждение удаления пользовательской службы OCSP

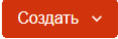
9.10.6.5 Создание кластера служб OCSP

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

Создание кластера возможно двумя способами:

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

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

- Перейдите на вкладку «Службы OCSP» раздела «Центры валидации».
- Нажмите кнопку  и выберите в списке «Кластер».
- В открывшемся окне (см. Рисунок 187) выполните следующие действия:
 - В поле «URL» укажите URL балансировщика нагрузки.

При указании URL возможны следующие сообщения об ошибках:

- «Указан URL существующей службы OCSP» – введенный URL совпадает с URL существующей (ранее зарегистрированной) точки распространения.
- «Некорректный ввод» – введенный URL содержит один и несколько пробелов.
- В поле «Приоритет» укажите приоритет кластера (числовое значение от 0 до 1000).

Кластеры и службы OCSP располагаются в списках в порядке убывания назначенного им приоритета. Если приоритеты кластеров и/или служб OCSP совпадают, то выше в списке будет располагаться кластер и/или служба, в параметры которых изменения были внесены позднее, начиная с даты создания.

- Нажмите кнопку **<Продолжить>**.

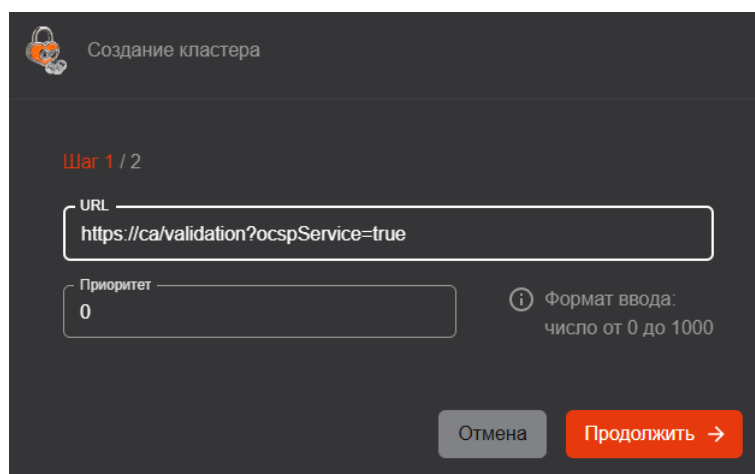




Рисунок 187 – Создание кластера служб OCSP. Шаг 1

- В открывшем окне (см. Рисунок 188) выполните следующие действия:
 - В списке «Выбрать» с помощью флажков выберите URL служб OCSP, которые необходимо объединить в кластер, и щелкните значок . В результате выбранные службы будут перемещены в список «Выбрано».
 - Чтобы изменить список служб OCSP, объединяемых в кластер, в списке «Выбрано» с помощью флажков выберите URL служб, исключаемых из кластера, и щелкните значок . В результате выбранные службы будут перемещены в список «Выбрать».
 - Чтобы найти службу в списках, используйте поля поиска.
 - Нажмите кнопку **<Создать кластер>**.

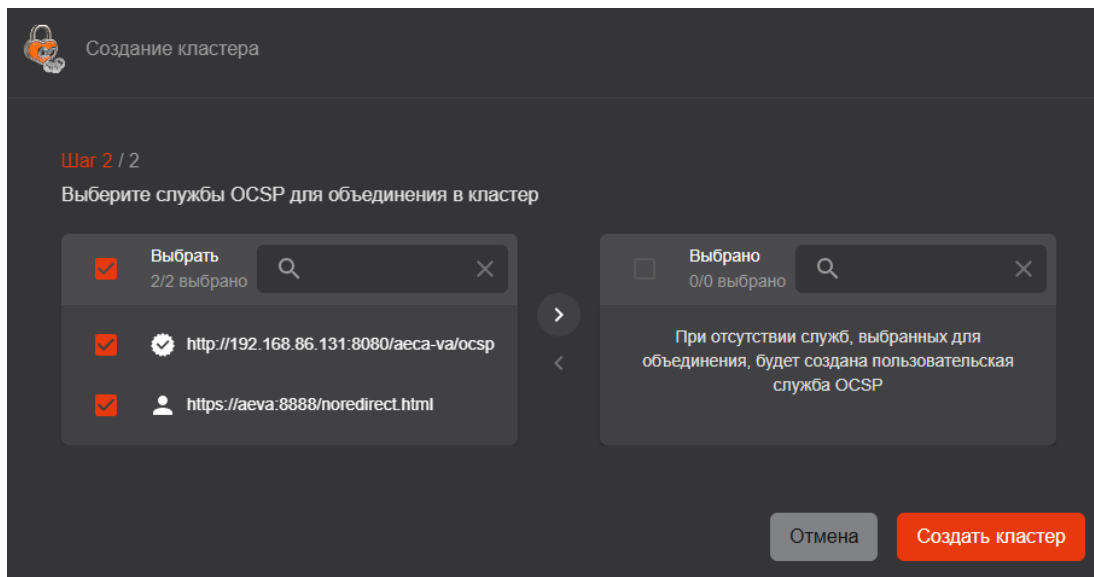


Рисунок 188 – Создание кластера служб OCSP. Шаг 2

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 189).

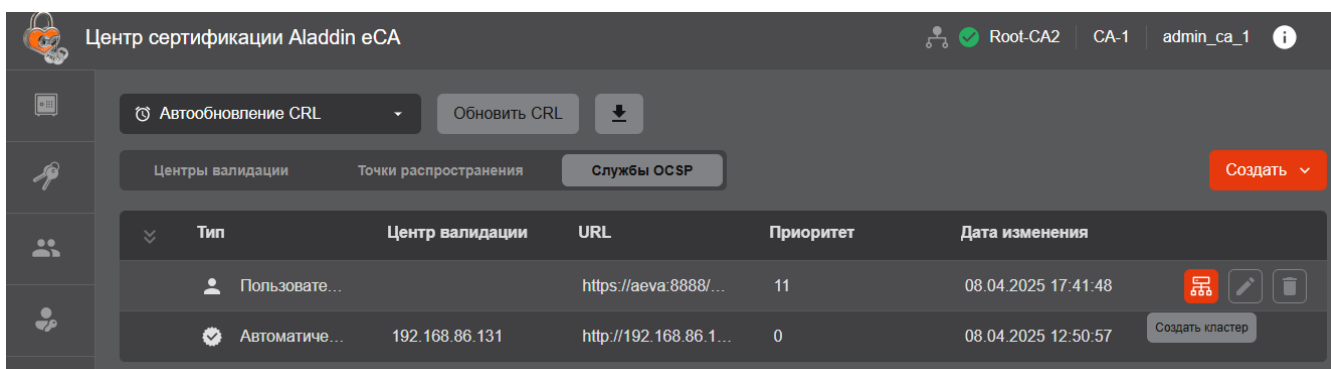


Рисунок 189 – Инициализация процесса создания кластера служб OCSP

- В открывшемся окне создания кластера (см. Рисунок 190) выполните следующие действия:

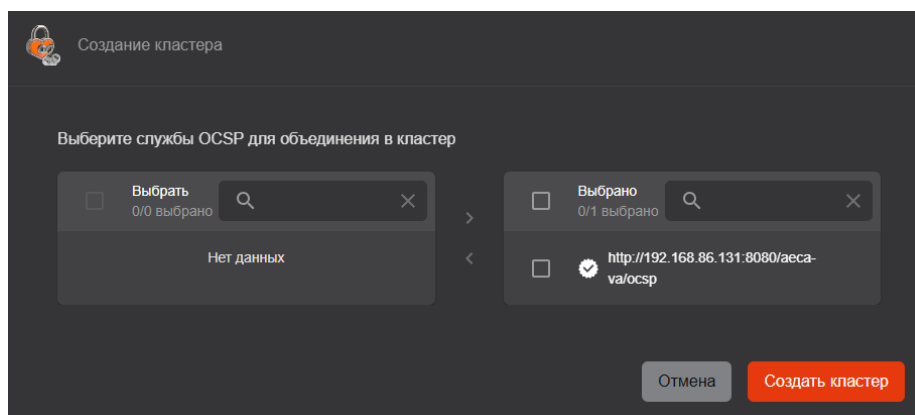



Рисунок 190 – Создание кластера из пользовательской службы OCSP


- В списке «Выбрать» с помощью флажков выберите URL служб OCSP, которые необходимо объединить в кластер, и щелкните значок . В результате выбранные службы будут перемещены в список «Выбрано».

- Чтобы изменить список служб OCSP, объединяемых в кластер, в списке «Выбрано» с помощью флажков выберите URL служб, исключаемых из кластера, и щелкните значок .
- Чтобы найти службу в списках, используйте поля поиска.
- Нажмите кнопку **<Создать кластер>**.

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

9.10.6.6 Просмотр состава кластера служб OCSP

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

- Перейдите на вкладку «Службы OCSP» раздела «Центры валидации».
- Раскройте состав кластер в списке. Для этого в строке выбранного кластера щелкните значок  (см. Рисунок 191).

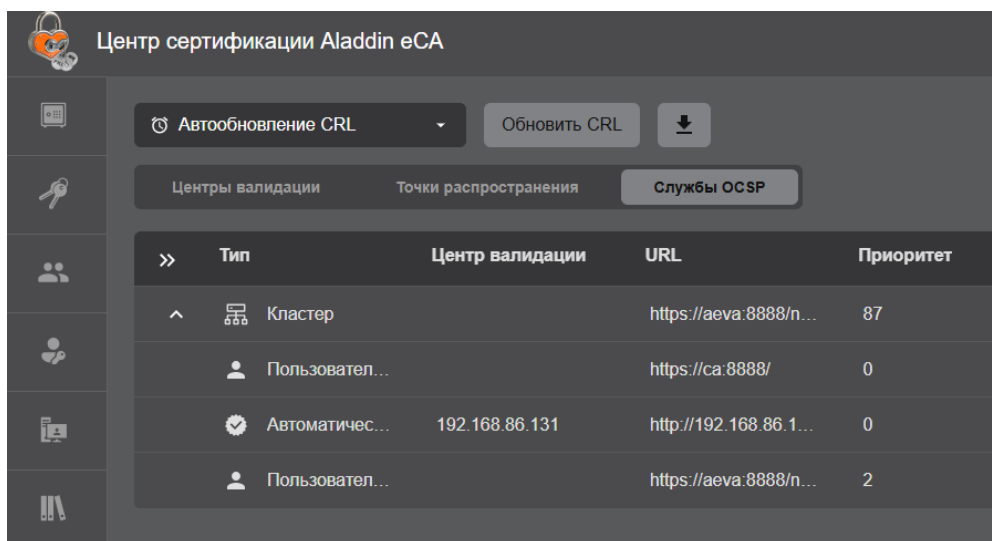




Рисунок 191 –Просмотр состава кластера служб OCSP

- Чтобы скрыть состав кластера, щелкните значок .

9.10.6.7 Редактирование кластера служб OCSP

Для редактирования состава кластера служб OCSP выполните следующие действия:

- Перейдите на вкладку «Службы OCSP» раздела «Центры валидации».
- Наведите указателем мыши на выбранный кластер в списке и нажмите кнопку  **<Редактировать кластер>** (см. Рисунок 192).

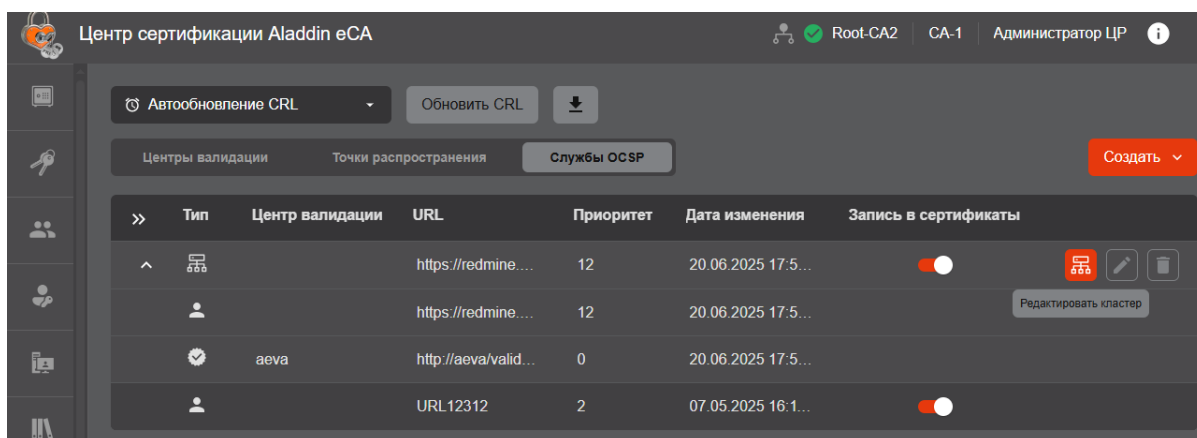


Рисунок 192 – Инициализация процесса редактирования состава кластера

- В открывшем окне управления кластером (см. Рисунок 193) измените состав кластера и нажмите кнопку **<Сохранить изменения>**.
 - Чтобы добавить службы OCSP в кластер, выберите URL служб в списке «Выбрать» с помощью флажков и щелкните значок ➤. В результате выбранные службы будут перемещены в список «Выбрано».
 - Чтобы исключить службы OCSP из кластера, выберите URL служб в списке «Выбрано» с помощью флажков и щелкните значок ◀. В результате выбранные службы будут перемещены в список «Выбрать».
 - Чтобы найти службу в списках, используйте поля поиска.

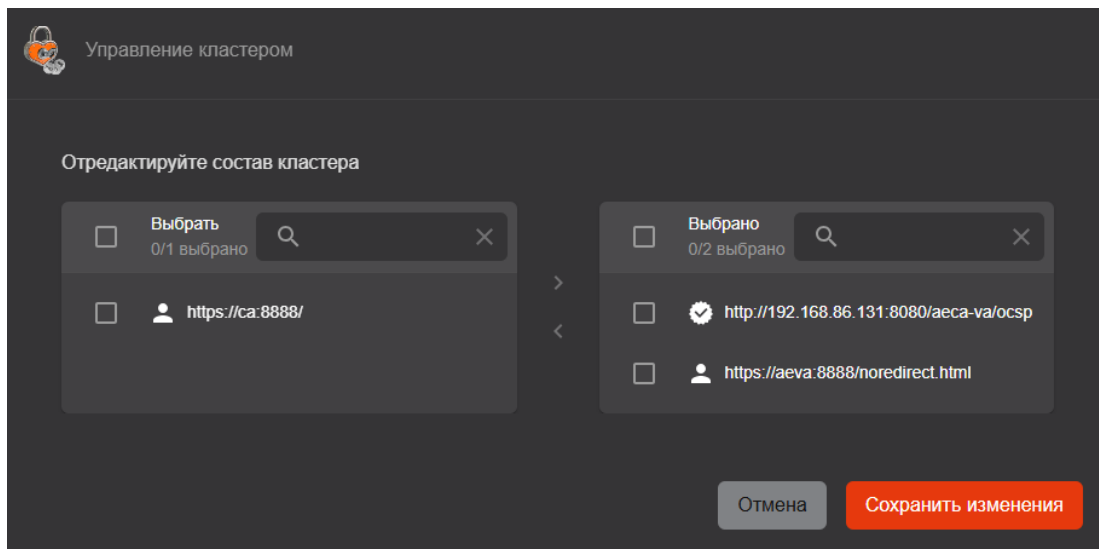



Рисунок 193 – Редактирование состава кластера служб OCSP

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 194).

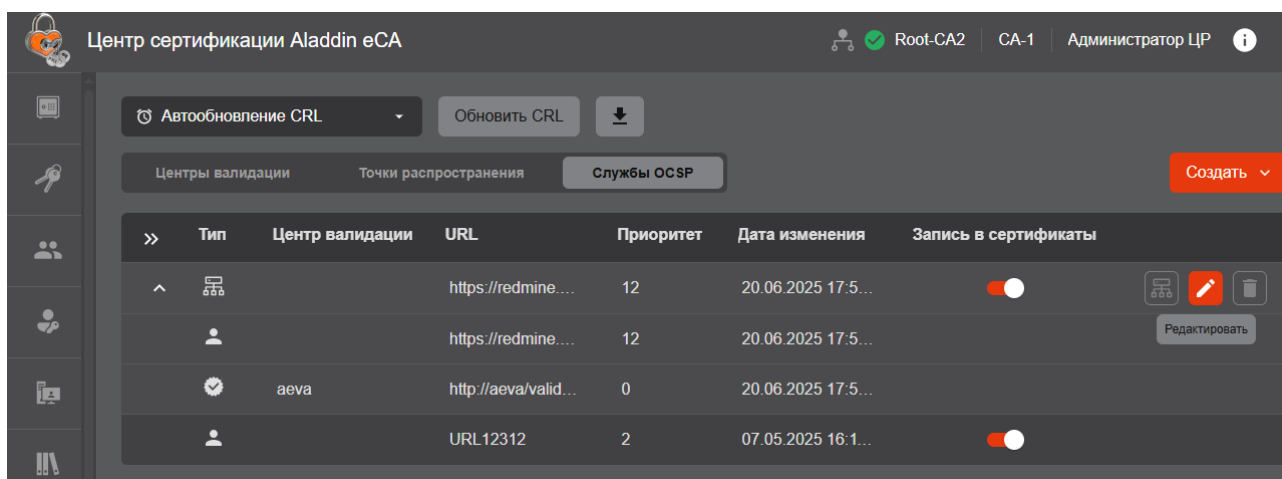


Рисунок 194 – Инициализация процесса редактирования параметров кластера

- В открывшемся окне (см. Рисунок 195) в соответствующих полях измените URL, приоритет кластера служб OCSP и нажмите кнопку **<Сохранить изменения>** (описание и правила заполнения полей см. в разделе 9.10.6.5).

Редактирование службы OSCP

URL
https://cadp:8888/noredirect

Приоритет
100


Формат ввода:
число от 0 до 1000

Отмена Сохранить изменения

Рисунок 195 – Редактирование параметров кластера службы OSCP

9.10.6.8 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 196).

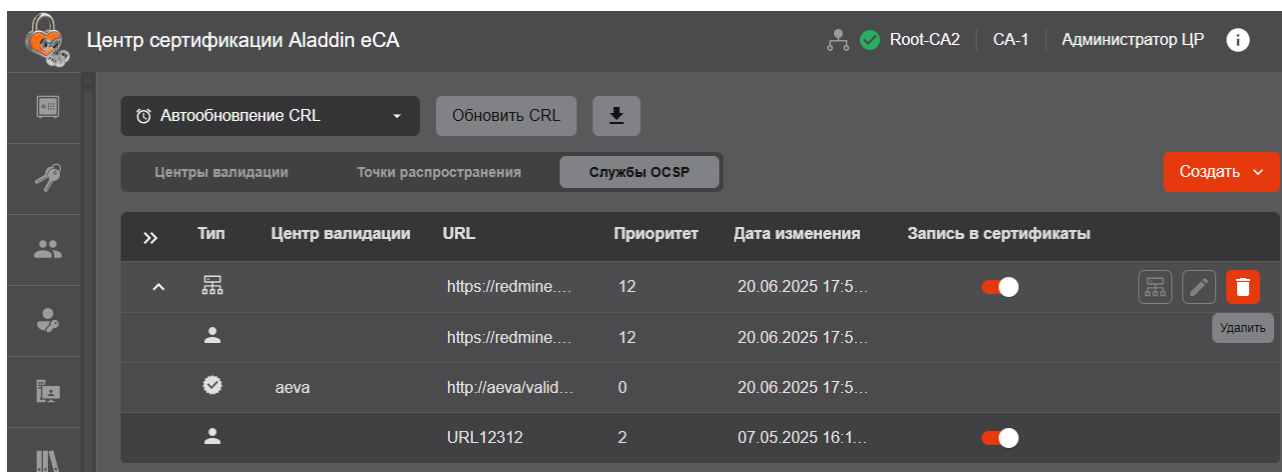


Рисунок 196 – Инициализация процесса удаления кластера служб OSCP

- В открывшемся окне (см. Рисунок 197) подтвердите удаление, нажав кнопку **<Удалить>**.

Удалить кластер служб OSCP?

Все входящие в кластер службы OSCP будут возвращены в список.

Отмена Удалить

Рисунок 197 – 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.

9.10.7 Получение файлов CRL, Delta CRL и AIA

9.10.7.1 Получение файлов посредством запуска скрипта из состава программы

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

```
sudo nano /opt/aecaCa/scripts/export-ca-data.sh
```

Внесите актуальные значения следующих параметров:

- идентификатор Центра сертификации, файлы CRL, Delta CRL и AIA которого будут экспортированы (параметр `CA_ID` можно выделить, как крайний параметр URL Центра сертификации, например: **https://sub01.presale.aeca/access-certificates/4a660253-09bf-4cc6-a363-871a9c4cbd8c**, где **4a660253-09bf-4cc6-a363-871a9c4cbd8c** – идентификатор 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 или sudo):

```
sudo bash /opt/aecaCa/scripts/export-ca-data.sh
```

В результате успешного выполнения скрипта в каталог, указанный в параметре `DOWNLOAD_PATH`, будут экспортированы файлы CRL, Delta CRL и AIA, а также архив «certificates.zip» со списком сертификатов, выпущенных Центром сертификации, идентификатор которого указан в параметре `CA_ID`.

9.10.7.2 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.eyJzZXNzaW9uSWQiOiI2Njc3NGU1ZS1jODkzLTRmOWQtODM4Yy1lMzQzZGQ1MGE3ZjUiLCJpYXQiOiE3MTAzMTIzODAsImV4cCI6MTMxMDMxMjU2MH0.MyyCQr89HeahIsnsn_vUXxeSqwFVlWRJUtPIkVMTbxq7BrzjG1cjFNJ9rEXx9jGKeSaTMbuwhmjX4aODGnPWCSFc18DUCqFA-85BTYgvGL5ns5kXfCe2Wxmr7oPj-7XMAZBI98JydXkLEbmRx7F10teNW1ZY3JkwKvi9yFxbWrojB3yNq2ak39cvNj4AFKCEBF0nE8UxKPoyXKDXegC0xEv2UK8mhF7Um4od9B1LW1CuNqKExyqTGr1DDKJcYjowBh49pQFAC3mG_bv7pBtTY7_vwuVNAelBAqj1kUm_sca_l-gARbh-oaU_ZTGXNe-zpXKIiTDM-uFXLTuImZXRA'
```

где:

192.168.111.100 – IP-адрес хоста Центра сертификации Aladdin eCA;

e5291624-fac6-4d5f-ae7-d57be0372489 – идентификатор Центра сертификации (может быть получен из URL карточки Центра сертификации);

eyJhbGciOiJSUzUxMiJ9.eyJzZXNzaW9uSWQoOiI2Njc3NGU1ZS1jODkzLTRmOWQtODM4Yy1lMzQzZGQ1MGE3ZjU1LkUpYXQoOiJEMTMtMTIzODAsImV4cCI6MTcxMDMxMjU2MH0.MyyCqR89HeahIsnsn_vUXxeSqwFVlWRJUtpIkVMtbxq7BrzjG1cjFNJ9rEXx9jGKeSaTMbuwhmjX4aODGnPWCSFc18DUCqFA-85BTYgvGL5ns5kXfCe2Wxmr7oPj-7XMAzBI98JydXkLEbmRx7F10teNW1ZY3JkwKvi9yFxbWrojB3yNq2ak39cvNj4AFKCEBF0nE8UxKPoyXKDXegC0xEv2UK8mhF7Um4od9B1LWlCuNqKEXyqTGr1DDKJcYjoWBh49pQFAc3mG_bv7pBtTY7_vwuVNAelBAqj1kUm_scA_1-gARBh-oaU_ZTGXNe-zpXKIiTDM-uFXLTuImZXRA - маркер доступа, полученный в результате аутентификации.

Полученный ответ на обращение к методу (при отсутствии ошибок) необходимо сохранить в файл с расширением **crl**.

Для получения файла 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.eyJzZXNzaW9uSWQoI2Njc3NGU1ZS1jODkzLTRmOWQtODM4Yy1lMzQzZGQlMGExZ3UiLCJpYXQiOjE5MTAzMTIzODAsImV4cCI6MTcxMDMxMjU2MH0.MyyCqR89HeahIsns_n_vUXxeSqwFVLWRJUtpIkVMtbxq7BrzjG1cjFNJ9rEXx9jgKeSaTMbuwhmjX4aODGnPWCSFc18DUCqFA-85BTYgvGL5ns5kXfCe2WxmR7oPj-7XMAzBI98JydXkLEbmRx7F10tenNW1ZY3JkwKvi9yFxbWrojb3ynQ2ak39cvNj4AFKCEBF0nE8UXKPoyXKDXegC0xEv2UK8mhF7Um4od9B1LWLcuNqKExyqTGr1DDKJcyJoWBh49pQFAC3mGbv7pBtTY7vwuVNAelBAqjlUm_sCA_l-gARBh-oaUZTGXNe-zpXKIiTDM-uFXLTuImZXRA'
```

где:

192.168.111.100 – IP-адрес хоста Центра сертификации Aladdin eCA;

e5291624-fac6-4d5f-ae7-d57be0372489 – идентификатор Центра сертификации (может быть получен из URL карточки ЦС)

eyJhbGciOiJSUzUxMiJ9.eyJzZXNzaW9uSWQoOiI2Njc3NGU1ZS1jODkzLTRmOWQtODM4Yy1lMzQzZGQ1MGE3ZjUiLCJpYXQiOiJEMTAzMtIzODAsImV4cCI6MTcxMDMxMjU2MH0.MyyCqR89HeahIsnsn_vUXxeSqwFVlWRJUtPIkVMTbxq7BrzjG1cjFNJ9rEXx9jGKeSaTMbuwhmjX4aODGnPWCSFc18DUCqFA-85BTYgvGL5ns5kXfCe2Wxmr7oPj-7XMAZBI98JydXkLEbmRx7F10teNW1ZY3JkwKvi9yFxbWroJB3yNq2ak39cvNj4AFKCEBF0nE8UxKPoyXKDXegC0xEv2UK8mhF7Um4od9B1LWlCuNqKEXyqTGr1DDKJcYjowBh49pQFAc3mG_bv7pBtTY7_vwuVNAelBAqj1kUm_scA_1-gARBh-oaU_ZTGXNe-zpXKIiTDM-uFXLTuImZXRA - маркер доступа, полученный в результате аутентификации.

Полученный ответ на обращение к методу (при отсутствии ошибок) необходимо сохранить в файл с расширением **crl**.

Для получения файла AIA необходимо использовать метод получения сертификата Центра сертификации по идентификатору Центра сертификации (см. описание метода в 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.eyJzZXNzaW9uSWQiOiI2Njc3NGU1ZS1jODkzLTRmOWQtODM4Yy1lMzQzZGQ1MGE3ZjUiLCJpYXQiOiJlMzUxMTAzMTIzODAsImV4cCI6MTcxMDMxMjU2MH0.MyycCqr89HeahIsnnsn_vUXxeSqwFVlWRJUTPIkVMTbxq7BrzjG1cjFNJ9rEXx9jGKeSaTMbuwhmjX4aODGnPWCSFc18DUCqFA-85BTYgvGL5ns5kXfCe2Wxmr7oPj-7XMAzBI98JydXkLEbmRx7F1OteNW1ZY3JkwKvi9yFxbWrojB3yNq2ak39cvNj4AFKCEBF0nE8UxKPoyXKDXegC0xEv2UK8mhF7Um4od9B1LWlCuNqKExyqTGr1DDKJcYjoWBh49pQFAc3mGbv7pBtTY7vwuVNAelBAqj1kUm_sCa_l-qARBh-oaU_ZTGXNe-zpXKIiTDM-uFXLTuImZXRA'
```

где:

192.168.111.100 – IP-адрес хоста Центра сертификации Aladdin eCA;

e5291624-fac6-4d5f-ae7-d57be0372489 – идентификатор Центра сертификации (может быть получен из URL карточки Центра сертификации);

eyJhbGciOiJSUzUxMiJ9.eyJzZXNzaW9uSWQoI2Njc3NGU1ZS1jODkzLTRmOWQtODM4Yy1lMzQzZGQ1MGE3ZjUiLCJpYXQiOiE3MTAzMTIzODAsImV4cCI6MTcxMDMxMjU2MH0.MyycCqr89HeahIsnsn_vUXxeSqwFVlWRJUtPIkVMtbxq7BrzjGlcjFNJ9rEXx9jGKeSaTMbuwhmjX4aODGnPWCSFc18DUCqFA-85BTYgvGL5ns5kXfCe2Wxmr7oPj-7XMAzBI98JyDXkLEbmRx7F10teNW1ZY3JkwKvi9yFxbWrojB3yNq2ak39cvNj4AFKCEBF0nE8UxKPoyXKDXegC0xEv2UK8mhF7Um4od9B1LWlCuNqKEXyqTGr1DDKJcYjowBh49pQFAc3mG_bv7pBtTY7_vwuVNAelBAqjlKUm_sca_1-gARbh-oaU_ZTGXNe-zpXKIiTDM-uFXLTuImZXRA - маркер доступа, полученный в результате аутентификации.

Ответ на обращение к методу (при отсутствии ошибок) необходимо сохранить в файл с расширением «ret».

9.10.8 Параметры точек распространения в сертификате

В создаваемых Центром сертификации Aladdin eSA 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.

9.11 Журнал событий

9.11.1 О журнале событий

Журнал событий предназначен для выявления случаев нарушения политики безопасности при эксплуатации Центра сертификации Aladdin eCA. В журнале аудита регистрируются системные события, связанные с работой ПО, а также события, связанные с изменениями настроек и действиями пользователей. Записи журнала событий хранятся в базе данных.

Каждая запись в журнале событий содержит следующую информацию:

- Дата и время регистрации с точностью до секунды.
- Имя учетной записи – пользователь, инициировавший событие (для системных событий – SYSTEM).
- Роль («Администратор» или «Оператор») – роль пользователя, инициировавшего событие.
- IP-адрес источника – IP-адрес узла, с которого была выполнена аутентификация инициатора события.
- Категория событий («Ошибка» или «Информация»).
- Код события в формате: CAENV[номер события].
- Описание – краткое описание события.
- Причина ошибки (только для событий категорий «Ошибка»).
- Подробное описание события.

Перечень событий с их кодами, категориями и подробным описанием приведен в таблице 24.

Таблица 24 – Сообщения журнала событий

Описание события	Код события	Категория события	Подробное описание события
Запуск службы	CAENV000	Информация	Описание: запуск службы
Остановка службы	CAENV001	Информация	Описание: остановка службы
Импорт лицензии	CAENV002	Информация	Описание: импорт лицензии <ul style="list-style-type: none"> Атрибуты: Срок действия CN сертификата ЦС CN сертификата корневого ЦС
Ошибка импорта лицензии	CAENV003	Ошибка	Описание: ошибка импорта лицензии <ul style="list-style-type: none"> Атрибуты: Срок действия CN сертификата ЦС CN сертификата корневого ЦС Причина ошибки
Проверка лицензии	CAENV004	Информация	Описание: проверка лицензии
Ошибка проверка лицензии	CAENV005	Ошибка	Описание: ошибка проверка лицензии Атрибуты: причина ошибки
Аутентификация пользователя	CAENV006	Информация	Описание: Аутентификация пользователя Атрибуты: <ul style="list-style-type: none"> Id пользователя Отображаемое имя пользователя Роль пользователя IP-адрес Аутентификатор Тип аутентификации
Ошибка аутентификации	CAENV007	Ошибка	Описание: Ошибка аутентификации пользователя Атрибуты: <ul style="list-style-type: none"> Id пользователя Отображаемое имя пользователя Роль пользователя IP-адрес Аутентификатор Тип аутентификации Причина ошибки
Активация центра сертификации	CAENV008	Информация	Описание: активация центра сертификации Атрибуты: <ul style="list-style-type: none"> CN сертификата ЦС Subject Alternative Name сертификата ЦС
Ошибка активации	CAENV009	Ошибка	Описание: ошибка активации Атрибуты: <ul style="list-style-type: none"> CN сертификата ЦС Subject Alternative Name сертификата ЦС Причина ошибки
Создание запроса на сертификат ЦС	CAENV010	Информация	Описание создание запроса на сертификат ЦС Атрибуты: <ul style="list-style-type: none"> CN запроса Subject Alternative Name запроса
Ошибка создания запроса	CAENV011	Ошибка	Описание: ошибка создания запроса Атрибуты: <ul style="list-style-type: none"> CN запроса Subject Alternative Name запроса Причина ошибки
Импорт сертификата центра сертификации	CAENV012	Информация	Описание: импорт сертификата центра сертификации Атрибуты:

Описание события	Код события	Категория события	Подробное описание события
			<ul style="list-style-type: none"> • CN сертификата ЦС • CN сертификата корневого ЦС
Ошибка импорта сертификата центра сертификации	CAENV013	Ошибка	<p>Описание: ошибка импорта сертификата центра сертификации</p> <ul style="list-style-type: none"> • Атрибуты: • CN сертификата ЦС • CN сертификата корневого ЦС • Причина ошибки
Выпуск сертификата	CAENV014	Информация	<p>Описание: выпуск сертификата</p> <p>Атрибуты:</p> <ul style="list-style-type: none"> • CN сертификата • Subject Alternative Name сертификата • Идентификатор шаблона • Вид операции • Сценарий • Контроль соответствия полей в сертификате атрибутам субъекта
Ошибка выпуска сертификата	CAENV015	Ошибка	<p>Описание: ошибка выпуска сертификата</p> <p>Атрибуты:</p> <ul style="list-style-type: none"> • CN сертификата • Subject Alternative Name сертификата • Идентификатор шаблона • Вид операции • Сценарий • Причина ошибки • Контроль соответствия полей в сертификате атрибутам субъекта
Регистрация центра валидации	CAENV016	Информация	<p>Описание: регистрация центра валидации</p> <p>Атрибуты: адрес центра валидации</p>
Ошибка регистрации	CAENV017	Ошибка	<p>Описание: ошибка регистрации</p> <p>Атрибуты:</p> <ul style="list-style-type: none"> • Адрес центра валидации • Причина ошибки
Активация OCSP центра валидации	CAENV018	Информация	<p>Описание: активация OCSP центра валидации</p> <p>Атрибуты: адрес центра валидации</p>
Ошибка активации	CAENV019	Ошибка	<p>Описание: ошибка активации</p> <p>Атрибуты: причина ошибки</p>
Настройка периода CRL	CAENV020	Информация	<p>Описание: настройка периода CRL</p>
Ошибка настройки	CAENV021	Ошибка	<p>Описание: Ошибка настройки периода CRL</p> <p>Атрибуты:</p> <ul style="list-style-type: none"> • периода CRL • перекрытие CR • период DeltaCRL • Причина ошибки
Публикация CRL	CAENV022	Информация	<p>Описание: публикация CRL</p> <p>Атрибуты:</p> <ul style="list-style-type: none"> • Номер CRL • Срок действия • Адрес точки публикации • Идентификатор ЦС
Ошибка публикации	CAENV023	Ошибка	<p>Описание: ошибка публикации</p> <p>Атрибуты:</p> <ul style="list-style-type: none"> • Номер CRL • Срок действия • Адрес точки публикации

Описание события	Код события	Категория события	Подробное описание события
			<ul style="list-style-type: none"> Идентификатор ЦС Причина ошибки
Добавление ресурсной системы	CAENV024	Информация	Описание: добавление ресурсной системы Атрибуты: <ul style="list-style-type: none"> Наименование ресурса Тип ресурса IP-адрес Точка подключения
Ошибка добавления	CAENV025	Ошибка	Описание: ошибка добавления Атрибуты: <ul style="list-style-type: none"> Наименование ресурса Тип ресурса IP-адрес Точка подключения Причина ошибки
Изменение ресурсной системы	CAENV026	Информация	Описание: изменение ресурсной системы Атрибуты: <ul style="list-style-type: none"> Наименование Тип Адрес Точка Служебный логин
Ошибка изменения	CAENV027	Ошибка	Описание: ошибка изменения ресурсной системы Атрибуты: <ul style="list-style-type: none"> Наименование Тип Адрес Точка Служебный логин Причина ошибки
Синхронизация ресурса	CAENV028	Информация	<ul style="list-style-type: none"> Описание: синхронизация ресурса Атрибуты: <ul style="list-style-type: none"> Наименование ресурса Количество субъектов
Ошибка синхронизации	CAENV029	Ошибка	Описание: ошибка синхронизации Атрибуты: <ul style="list-style-type: none"> Наименование ресурса Количество субъектов Причина ошибки
Создание учетной записи	CAENV030	Информация	Описание: создание учетной записи Атрибуты: <ul style="list-style-type: none"> Логин ФИО пользователя Роль
Ошибка создания	CAENV031	Ошибка	Описание: ошибка создания Атрибуты: <ul style="list-style-type: none"> Логин ФИО пользователя Роль Причина ошибки
Изменение учетной записи	CAENV032	Информация	Описание: изменение учетной записи Атрибуты: ФИО пользователя (исходное значение; конечное значение)
Ошибка изменения прав	CAENV033	Ошибка	Описание: ошибка изменения учетной записи Атрибуты: <ul style="list-style-type: none"> Логин

Описание события	Код события	Категория события	Подробное описание события
			<ul style="list-style-type: none"> Роль Серийный номер сертификата Причина ошибки
Сохранение прав оператора	CAENV034	Информация	Описание: ввод прав оператора Атрибуты: <ul style="list-style-type: none"> Лог.имя [список прав]
Ошибка сохранения	CAENV035	Ошибка	Описание: ошибка сохранения прав оператора Атрибуты: <ul style="list-style-type: none"> Лог.имя [список прав] Причина ошибки
Установка сертификата веб-сервера	CAENV036	Информация	Описание: установка сертификата веб-сервера Атрибуты: серийный номер сертификата
Ошибка установки	CAENV037	Ошибка	Описание: ошибка установки сертификата веб-сервера Атрибуты: <ul style="list-style-type: none"> Серийный номер сертификата Причина ошибки
Изменение списка издателей	CAENV038	Информация	<ul style="list-style-type: none"> Описание: изменение списка издателей Атрибуты: список идентификаторов активных издателей (Исходное значение; Конечное значение)
Ошибка изменения	CAENV039	Ошибка	Описание: ошибка изменения списка разрешенных издателей Атрибуты: <ul style="list-style-type: none"> Имя издателя "добавлен" или "удален" Причина ошибки
Подключение к ключевому носителю	CAENV042	Информация	<ul style="list-style-type: none"> Описание: подключение к ключевому носителю Атрибуты: маркировка носителя
Ошибка подключения	CAENV043	Ошибка	Описание: ошибка подключения Атрибуты: <ul style="list-style-type: none"> Маркировка носителя Причина ошибки
Создание контейнера на ключевом носителе	CAENV044	Информация	Описание: создание контейнера на ключевом носителе Атрибуты: маркировка носителя
Ошибка создания	CAENV045	Ошибка	Описание: ошибка создания Атрибуты: <ul style="list-style-type: none"> Маркировка носителя Причина ошибки
Запись сертификата на ключевой носитель	CAENV046	Информация	Описание: запись сертификата на ключевой носитель Атрибуты: маркировка носителя
Ошибка записи	CAENV047	Ошибка	Описание: Ошибка записи сертификата на ключевой носитель Атрибуты: <ul style="list-style-type: none"> Маркировка носителя ID-сертификата Причина ошибки
Публикация сертификата в ресурсной системе	CAENV048	Информация	Описание: публикация сертификата в ресурсной системе Атрибуты: <ul style="list-style-type: none"> Идентификатор субъекта DN субъекта Идентификатор РС Серийный номер сертификата
Ошибка публикации	CAENV049	Ошибка	Описание: ошибка публикации

Описание события	Код события	Категория события	Подробное описание события
			Атрибуты: <ul style="list-style-type: none"> Идентификатор субъекта DN субъекта Идентификатор PC Серийный номер сертификата Причина ошибки
Сохранение журнала в CSV	CAENV050	Информация	Описание: сохранение журнала в CSV Атрибуты: <ul style="list-style-type: none"> Фильтр: дата и время фиксации события (начиная с указанной включительно) Фильтр: дата и время фиксации события (до включительно) Фильтр: категории события (полное соответствие) Фильтр: учетные записи (полное соответствие) Фильтр: системные события
Ошибка сохранения	CAENV051	Ошибка	Описание: Ошибка сохранения журнала в CSV Атрибуты: <ul style="list-style-type: none"> Фильтр Причина ошибки
Генерация CRL	CAENV052	Информация	Описание: генерация CRL Атрибуты: <ul style="list-style-type: none"> Номер CRL Срок действия CRL
Ошибка генерации	CAENV053	Ошибка	Описание: ошибка генерации Атрибуты: <ul style="list-style-type: none"> Срок действия CRL Причина ошибки
Отправка уведомления на почту	CAENV054	Информация	Описание: отправка уведомления на почту Атрибуты: <ul style="list-style-type: none"> CN Email Шаблон
Ошибка отправки	CAENV055	Ошибка	Описание: ошибка отправки Атрибуты: <ul style="list-style-type: none"> CN Email Шаблон Причина ошибки
Отзыв сертификата	CAENV056	Информация	Описание: Отзыв сертификата: Атрибуты: <ul style="list-style-type: none"> Серийный номер сертификата Идентификатор сертификата Код причины отзыва Причина отзыва
Приостановка сертификата	CAENV057	Информация	Описание: Приостановка сертификата Атрибуты: <ul style="list-style-type: none"> Серийный номер сертификата Идентификатор сертификата Код причины отзыва Причина отзыва
Реактивация сертификата	CAENV058	Информация	Описание: Реактивация сертификата Атрибуты: <ul style="list-style-type: none"> Серийный номер сертификата Идентификатор сертификата Код причины отзыва Причина отзыва

Описание события	Код события	Категория события	Подробное описание события
Начало удаления центра сертификации	CAENV059	Информация	Описание: Начало удаления центра сертификации Атрибуты: <ul style="list-style-type: none"> • CN сертификата ЦС • CN сертификата корневого ЦС • Subject Alternative Name сертификата ЦС
Окончание удаления центра сертификации	CAENV060	Информация	Описание: окончание удаления центра сертификации Атрибуты: <ul style="list-style-type: none"> • CN сертификата ЦС • CN сертификата корневого ЦС • Subject Alternative Name сертификата ЦС
Ошибка при удалении центра сертификации	CAENV061	Ошибка	Описание: ошибка удаления центра сертификации Атрибуты: <ul style="list-style-type: none"> • CN сертификата ЦС • CN сертификата корневого ЦС • Subject Alternative Name сертификата ЦС • Причина ошибки
Начало очистки журнала событий	CAENV064	Информация	Описание: начало очистки журнала событий
Окончание очистки журнала событий	CAENV065	Информация	Описание: окончание очистки журнала событий
Ошибка при очистке журнала событий	CAENV066	Ошибка	Описание: Ошибка очистки журнала события Атрибуты: <ul style="list-style-type: none"> • Фильтр • Причина ошибки
Начало архивации журнала событий	CAENV067	Информация	Описание: начало архивации журнала событий
Окончание архивации журнала событий	CAENV068	Информация	Описание: окончание архивации журнала событий
Ошибка при архивации журнала событий	CAENV069	Ошибка	Описание: Ошибка архивации журнала события Атрибуты: <ul style="list-style-type: none"> • Фильтр • Причина ошибки
Добавить шаблон сертификата в «Центр регистрации»	CAENV070	Информация	Описание: добавить шаблон сертификата в «Центр регистрации» Атрибуты: <ul style="list-style-type: none"> • Идентификатор шаблона • Наименование шаблона
Ошибка при добавлении шаблона сертификата в «Центр регистрации»	CAENV071	Ошибка	Описание: Ошибка при добавлении шаблона сертификата в «Центр регистрации» Атрибуты: <ul style="list-style-type: none"> • Наименование шаблона • Причина ошибки
Убрать шаблон сертификата в «Центр регистрации»	CAENV072	Информация	Описание: Убрать шаблон сертификата в «Центр регистрации» Атрибуты: наименование шаблона
Ошибка при уборке шаблона сертификата в «Центр регистрации»	CAENV073	Ошибка	Описание: Ошибка при уборке шаблона сертификата в «Центр регистрации» Атрибуты: <ul style="list-style-type: none"> • Наименование шаблона • Причина ошибки
Успешная проверка контрольных сумм	CAENV074	Информация	Описание: Успешная проверка целостности исполняемых файлов
Неуспешная проверка контрольных сумм	CAENV075	Ошибка	Описание: Проверка целостности исполняемых файлов прошла неуспешно Атрибуты:

Описание события	Код события	Категория события	Подробное описание события
			<ul style="list-style-type: none"> Список файлов, которые не удалось проверить Причина ошибки
Распаковка ключей ЦС	CAENV076	Информация	Описание: распаковка ключей ЦС Атрибуты: идентификатор ЦС
Ошибка при распаковке ключей ЦС	CAENV077	Ошибка	Описание: ошибка при распаковке ключей ЦС Атрибуты: <ul style="list-style-type: none"> Идентификатор ЦС Причина ошибки
Скачан контейнер PKCS#12	CAENV078	Информация	Описание: скачан контейнер PKCS#12 Атрибуты: серийный номер сертификата в контейнере
Скачан сертификат	CAENV079	Информация	Описание: скачан сертификат
Скачена цепочка сертификата	CAENV080	Информация	Описание: скачана цепочка сертификата
Экспорт запроса на сертификат ЦС	CAENV081	Информация	Описание: экспорт запроса на сертификат ЦС Атрибуты: идентификатор сертификата
Ошибка экспорта запроса на сертификат ЦС	CAENV082	Ошибка	Описание: Неуспешный экспорт запроса на сертификат центра сертификации за пределы программы Атрибуты: причина ошибки
Ошибка экспорта контейнера PKCS#12	CAENV085	Ошибка	Описание: Ошибка экспорта контейнера закрытого ключа за пределы программы Атрибуты: <ul style="list-style-type: none"> Серийный номер сертификата в контейнере Причина ошибки
Успешное создание резервной копии	CAENV086	Информация	Описание: Успешное создание резервной копии Атрибуты: путь к созданной резервной копии
Ошибка создания резервной копии	CAENV087	Ошибка	Описание: Ошибка создания резервной копии Атрибуты: причина ошибки
Успешное восстановление из резервной копии	CAENV088	Информация	Описание: Успешное восстановление из резервной копии Атрибуты: путь к использованной резервной копии
Ошибка восстановления из резервной копии	CAENV089	Ошибка	Описание: Ошибка восстановления из резервной копии Атрибуты: причина ошибки
Ошибка синхронизации субъекта	CAENV090	Ошибка	Описание: Ошибка синхронизации субъекта: текущее значение Атрибуты: <ul style="list-style-type: none"> Идентификатор субъекта DN субъекта Идентификатор РС Причина ошибки
Создание правила доступа	CAENV091	Информация	Описание: создание правила доступа Атрибуты: <ul style="list-style-type: none"> Категория правила доступа Субъекты правила доступа Объекты правила доступа Операции правила доступа
Ошибка создания правила доступа	CAENV092	Ошибка	Описание: Ошибка создания правила доступа Атрибуты: причина ошибки
Редактирование правила доступа	CAENV093	Информация	Описание: редактирование правила доступа Атрибуты: <ul style="list-style-type: none"> Субъекты правила доступа (Исходное значение; Конечное значение) Объекты правила доступа (Исходное значение; Конечное значение)

Описание события	Код события	Категория события	Подробное описание события
			<ul style="list-style-type: none"> Операции правила доступа (Исходное значение; Конечное значение)
Ошибка изменения правила доступа	CAENV094	Ошибка	<p>Описание: ошибка изменения правила доступа</p> <p>Атрибуты:</p> <ul style="list-style-type: none"> Субъекты правила доступа Объекты правила доступа Операции правила доступа Причина ошибки
Удаление правила доступа	CAENV095	Информация	<p>Описание: удаление правила доступа: текущее значение:</p> <p>Атрибуты:</p> <ul style="list-style-type: none"> Категория правила доступа: категория правила доступа, Субъекты правила доступа Объекты правила доступа Операции правила доступа
Ошибка удаления правила доступа	CAENV096	Ошибка	<p>Описание: Ошибка удаления правила доступа</p> <p>Атрибуты: причина ошибки</p>
Добавление Syslog-сервера	CAENV097	Информация	<p>Описание: добавление Syslog-сервера</p> <p>Атрибуты:</p> <ul style="list-style-type: none"> Хост Порт Протокол Флаг отправки сообщения
Ошибка добавления Syslog-сервера	CAENV098	Ошибка	<p>Описание: Ошибка добавления Syslog-сервера</p> <p>Атрибуты: причина ошибки</p>
Изменение параметров Syslog-сервера	CAENV099	Информация	<p>Описание: изменение параметров Syslog-сервера</p> <p>Атрибуты: флаг отправки сообщения</p>
Ошибка изменения параметров Syslog-сервера	CAENV100	Ошибка	<p>Описание: Ошибка изменения параметров Syslog-сервера</p> <p>Атрибуты: причина ошибки</p>
Удаление Syslog-сервера	CAENV101	Информация	<p>Описание: удаление Syslog-сервера</p> <p>Атрибуты:</p> <ul style="list-style-type: none"> Хост Порт Протокол Флаг отправки сообщения
Ошибка удаления Syslog-сервера	CAENV102	Ошибка	<p>Описание: ошибка удаления Syslog-сервера</p> <p>Атрибуты:</p> <ul style="list-style-type: none"> Хост Порт Протокол Флаг отправки сообщения Причина ошибки
Создание корневого ЦС	CAENV103	Информация	<p>Описание: Создание корневого ЦС</p> <p>Атрибуты:</p> <ul style="list-style-type: none"> Отображаемое имя ЦС CN корневого ЦС Конфигурация криптопровайдеров ЦС Срок действия Алгоритм ключа Длина ключа Алгоритм хэш-суммы Место хранения закрытого ключа
Ошибка создания корневого ЦС	CAENV104	Ошибка	<p>Описание: Ошибка создания корневого ЦС</p> <p>Атрибуты:</p> <ul style="list-style-type: none"> Отображаемое имя ЦС

Описание события	Код события	Категория события	Подробное описание события
			<ul style="list-style-type: none"> Имя ЦС Причина ошибки
Создание подчиненного ЦС	CAENV105	Информация	<p>Описание: Создание подчиненного ЦС</p> <p>Атрибуты:</p> <ul style="list-style-type: none"> Отображаемое имя ЦС CN запроса Конфигурация криптопровайдеров Срок действия Алгоритм ключа Длина ключа Алгоритм хэш-суммы Место хранения закрытого ключа
Ошибка создания подчиненного ЦС	CAENV106	Ошибка	<p>Описание: Ошибка создания подчиненного ЦС</p> <p>Атрибуты:</p> <ul style="list-style-type: none"> Отображаемое имя ЦС Имя ЦС Причина ошибки
Экспорт закрытого ключа ЦС	CAENV107	Информация	<p>Описание: Экспорт закрытого ключа ЦС</p> <p>Атрибуты:</p> <ul style="list-style-type: none"> Идентификатор ЦС Отображаемое имя ЦС CN сертификата ЦС Экспортирован из хранилища
Ошибка экспорта закрытого ключа ЦС	CAENV108	Ошибка	<p>Описание: Ошибка экспорта закрытого ключа ЦС</p> <p>Атрибуты:</p> <ul style="list-style-type: none"> Идентификатор ЦС Отображаемое имя ЦС Имя ЦС Хранилище Причина ошибки
Скачан закрытый ключ ЦС	CAENV109	Информация	<p>Описание: Скачан закрытый ключ ЦС</p> <p>Атрибуты:</p> <ul style="list-style-type: none"> Идентификатор ЦС Отображаемое имя ЦС CN сертификата ЦС
Ошибка скачивания закрытого ключа ЦС	CAENV110	Ошибка	<p>Описание: Ошибка скачивания закрытого ключа ЦС</p> <p>Атрибуты:</p> <ul style="list-style-type: none"> Идентификатор ЦС Отображаемое имя ЦС CN сертификата ЦС Причина ошибки
Импорт закрытого ключа ЦС	CAENV111	Информация	<p>Описание: Импорт закрытого ключа ЦС</p> <p>Атрибуты:</p> <ul style="list-style-type: none"> Идентификатор ЦС Отображаемое имя ЦС CN сертификата ЦС Импортирован в хранилище
Ошибка импорта закрытого ключа ЦС	CAENV112	Ошибка	<p>Описание: Ошибка импорта закрытого ключа ЦС</p> <p>Атрибуты:</p> <ul style="list-style-type: none"> Идентификатор ЦС Отображаемое имя ЦС CN сертификата ЦС Место хранения закрытого ключа Причина ошибки
Создание ключевой пары	CAENV113	Информация	<p>Описание: Создание ключевой пары</p> <p>Атрибуты:</p>

Описание события	Код события	Категория события	Подробное описание события
			<ul style="list-style-type: none"> • Тип владельца • ID владельца • Алгоритм ключа • Длина ключа • Криптопровайдер • Место хранения закрытого ключа • Экспортируемость
Ошибка создания ключевой пары	CAENV114	Ошибка	<p>Описание: Ошибка создания ключевой пары</p> <p>Атрибуты:</p> <ul style="list-style-type: none"> • 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	Информация	<p>Описание: Удаление закрытого ключа ЦС</p> <p>Атрибуты:</p> <ul style="list-style-type: none"> • Идентификатор ЦС • Отображаемое имя ЦС • CN ЦС • Место хранения закрытого ключа
Ошибка удаления закрытого ключа ЦС	CAENV116	Ошибка	<p>Описание: Ошибка удаления закрытого ключа ЦС</p> <p>Атрибуты:</p> <ul style="list-style-type: none"> • Идентификатор ЦС (может отсутствовать) • Отображаемое имя ЦС (может отсутствовать) • CN ЦС (может отсутствовать) • Место хранения закрытого ключа (может отсутствовать) • Причина ошибки
Создание корневого ЦС на основании контейнера PKCS#12	CAENV117	Информация	<p>Описание: Создание корневого ЦС на основании контейнера PKCS#12</p> <p>Атрибуты:</p> <ul style="list-style-type: none"> • Отображаемое имя ЦС • CN ЦС • Конфигурация криптопровайдеров ЦС • Срок действия • Алгоритм ключа • Длина ключа • Алгоритм хэш-суммы • Место хранения закрытого ключа
Ошибка создания корневого ЦС на основании контейнера PKCS#12	CAENV118	Ошибка	<p>Описание: Ошибка создания корневого ЦС на основании контейнера PKCS#12</p> <p>Атрибуты:</p> <ul style="list-style-type: none"> • Отображаемое имя ЦС (может отсутствовать) • CN ЦС (может отсутствовать) • Конфигурация криптопровайдеров ЦС • Срок действия (может отсутствовать) • Алгоритм ключа (может отсутствовать) • Длина ключа (может отсутствовать) • Алгоритм хэш-суммы (может отсутствовать) • Место хранения закрытого ключа (может отсутствовать) • Причина ошибки
Создание подчиненного ЦС на основании контейнера PKCS#12	CAENV119	Информация	<p>Описание: Создание подчиненного ЦС на основании контейнера PKCS#12</p>

Описание события	Код события	Категория события	Подробное описание события
			<p>Атрибуты:</p> <ul style="list-style-type: none"> • Отображаемое имя ЦС • CN ЦС • Конфигурация криптопровайдеров ЦС • Срок действия • Алгоритм ключа • Длина ключа • Алгоритм хэш-суммы • Место хранения закрытого ключа
Ошибка создания подчиненного ЦС на основании контейнера PKCS#12	CAENV120	Ошибка	<p>Описание: Ошибка создания подчиненного ЦС на основании контейнера PKCS#12</p> <p>Атрибуты:</p> <ul style="list-style-type: none"> • Отображаемое имя ЦС (может отсутствовать) • CN ЦС (может отсутствовать) • Конфигурация криптопровайдеров ЦС (может отсутствовать) • Срок действия (может отсутствовать) • Алгоритм ключа (может отсутствовать) • Длина ключа (может отсутствовать) • Алгоритм хэш-суммы (может отсутствовать) • Место хранения закрытого ключа (может отсутствовать) • Причина ошибки
Создание шаблона сертификата	CAENV121	INFO	<p>Описание: Создание шаблона сертификата</p> <p>Атрибуты:</p> <ul style="list-style-type: none"> • Идентификатор шаблона • Наименование шаблона • Период действия сертификата • Центр сертификации • Тип субъекта • Чек-бокс «Публиковать сертификат в ресурсную систему» • Минимальная длина ключа RSA (может отсутствовать) • Минимальная длина ключа ECDSA (может отсутствовать) • Минимальная длина ключа ГОСТ Р 34.10-2012 (может отсутствовать) • Использование ключа • Чек-бокс «Считать это расширение критическим» для списка использования ключа • Расширенное использование ключа • Чек-бокс «Считать это расширение критическим» для списка расширенного использования ключа • Чек-бокс «Включать SID субъекта в сертификат» • OID политики сертификата • Чек-бокс «Считать это расширение критическим» для списка OID политики сертификата • Чек-бокс «Контролировать соответствие полей в сертификате атрибутам субъекта» • DN субъекта • Альтернативное имя субъекта • Чек-бокс «Сведения о средствах ЭП и УЦ издателя» • Наименование средства ЭП • Заключение на средство ЭП • Наименование средства УЦ • Заключение на средство УЦ • Чек-бокс «Сведения о средстве ЭП владельца сертификата» • Наименование средства ЭП владельца сертификата

Описание события	Код события	Категория события	Подробное описание события
Ошибка создания шаблона сертификата	CAENV122	ERROR	<p>Описание: Ошибка создания шаблона сертификата</p> <p>Атрибуты:</p> <ul style="list-style-type: none"> Идентификатор шаблона (может отсутствовать) Наименование шаблона (может отсутствовать) Период действия сертификата (может отсутствовать) Центр сертификации (может отсутствовать) Тип субъекта (может отсутствовать) Чек-бокс «Публиковать сертификат в ресурсную систему» Минимальная длина ключа RSA (может отсутствовать) Минимальная длина ключа ECDSA (может отсутствовать) Минимальная длина ключа ГОСТ Р 34.10-2012 (может отсутствовать) Использование ключа (может отсутствовать) Чек-бокс «Считать это расширение критическим» для списка использования ключа Расширенное использование ключа (может отсутствовать) Чек-бокс «Считать это расширение критическим» для списка расширенного использования ключа Чек-бокс «Включать SID субъекта в сертификат» OID политики сертификата (может отсутствовать) Чек-бокс «Считать это расширение критическим» для списка OID политики сертификата Чек-бокс «Контролировать соответствие полей в сертификате атрибутам субъекта» DN субъекта (может отсутствовать) Альтернативное имя субъекта (может отсутствовать) Чек-бокс «Сведения о средствах ЭП и УЦ издателя» (может отсутствовать) Наименование средства ЭП (может отсутствовать) Заключение на средство ЭП (может отсутствовать) Наименование средства УЦ (может отсутствовать) Заключение на средство УЦ (может отсутствовать) Чек-бокс «Сведения о средстве ЭП владельца сертификата» (может отсутствовать) Наименование средства ЭП владельца сертификата (может отсутствовать) Причина ошибки
Изменение шаблона сертификата	CAENV123	INFO	<p>Описание: Изменение шаблона сертификата</p> <p>Атрибуты:</p> <ul style="list-style-type: none"> Идентификатор шаблона Наименование шаблона: Исходное значение/ Конечное значение Период действия сертификата: Исходное значение/ Конечное значение Тип субъекта: Исходное значение/ Конечное значение Центр сертификации: Исходное значение/ Конечное значение Включение SID субъекта в сертификат: Исходное значение/ Конечное значение Параметры алгоритма RSA: Исходное значение/ Конечное значение Параметры алгоритма ECDSA: Исходное значение/ Конечное значение Параметры алгоритма ГОСТ Р 34.10-2012: Исходное значение/ Конечное значение

Описание события	Код события	Категория события	Подробное описание события
			<ul style="list-style-type: none"> Использование ключа: Исходное значение/ Конечное значение Расширенное использование ключа: Исходное значение/ Конечное значение OID политики сертификата: Исходное значение/ Конечное значение Чек-бокс «Контролировать соответствие полей в сертификате атрибутам субъекта» DN субъекта: Исходное значение/ Конечное значение Альтернативное имя субъекта: Исходное значение/ Конечное значение Публикация сертификата в ресурсную систему: Исходное значение/ Конечное значение Чек-бокс «Сведения о средствах ЭП и УЦ издателя»: Исходное значение/ Конечное значение Наименование средства ЭП: Исходное значение/ Конечное значение Заключение на средство ЭП: Исходное значение/ Конечное значение Наименование средства УЦ: Исходное значение/ Конечное значение Заключение на средство УЦ: Исходное значение/ Конечное значение Чек-бокс «Сведения о средстве ЭП владельца сертификата»: Исходное значение/ Конечное значение Наименование средства ЭП владельца сертификата: Исходное значение/ Конечное значение
Ошибка изменения шаблона сертификата	CAENV124	ERROR	<p>Описание: Ошибка изменения шаблона сертификата</p> <p>Атрибуты:</p> <ul style="list-style-type: none"> Идентификатор шаблона Наименование шаблона: Исходное значение/ Конечное значение (может отсутствовать) Период действия сертификата: Исходное значение/ Конечное значение (может отсутствовать) Тип субъекта: Исходное значение/ Конечное значение (может отсутствовать) Центр сертификации: Исходное значение/ Конечное значение (может отсутствовать) Включение SID субъекта в сертификат: Исходное значение/ Конечное значение Параметры алгоритма RSA: Исходное значение/ Конечное значение (может отсутствовать) Параметры алгоритма ECDSA: Исходное значение/ Конечное значение (может отсутствовать) Параметры алгоритма ГОСТ Р 34.10-2012: Исходное значение/ Конечное значение (может отсутствовать) Использование ключа: Исходное значение/ Конечное значение (может отсутствовать) Расширенное использование ключа: Исходное значение/ Конечное значение (может отсутствовать) OID политики сертификата: Исходное значение/ Конечное значение (может отсутствовать) Чек-бокс «Контролировать соответствие полей в сертификате атрибутам субъекта» DN субъекта: Исходное значение/ Конечное значение (может отсутствовать) Альтернативное имя субъекта: Исходное значение/ Конечное значение (может отсутствовать) Публикация сертификата в ресурсную систему: Исходное значение/ Конечное значение

Описание события	Код события	Категория события	Подробное описание события
			<ul style="list-style-type: none"> Чек-бокс «Сведения о средствах ЭП и УЦ издателя» (может отсутствовать). Исходное значение/ Конечное значение Наименование средства ЭП (может отсутствовать). Исходное значение/ Конечное значение Заключение на средство ЭП (может отсутствовать). Исходное значение/ Конечное значение Наименование средства УЦ (может отсутствовать). Исходное значение/ Конечное значение Заключение на средство УЦ (может отсутствовать). Исходное значение/ Конечное значение Чек-бокс «Сведения о средстве ЭП владельца сертификата» (может отсутствовать). Исходное значение/ Конечное значение Наименование средства ЭП владельца сертификата (может отсутствовать). Исходное значение/ Конечное значение Причина ошибки
Удаление шаблона сертификата	CAENV125	INFO	<p>Описание: Удаление шаблона сертификата</p> <p>Атрибуты:</p> <ul style="list-style-type: none"> Идентификатор шаблона Наименование шаблона Период действия сертификата Центр сертификации Тип субъекта Чек-бокс «Публиковать сертификат в ресурсную систему» Минимальная длина ключа Минимальная длина ключа ECDSA Минимальная длина ключа ГОСТ Р 34.10-2012 (может отсутствовать) Использование ключа Чек-бокс «Считать это расширение критическим» для списка использования ключа Расширенное использование ключа Чек-бокс «Считать это расширение критическим» для списка расширенного использования ключа Чек-бокс «Включать SID субъекта в сертификат» OID политики сертификата Чек-бокс «Считать это расширение критическим» для списка OID политики сертификата Чек-бокс «Контролировать соответствие полей в сертификате атрибутам субъекта» Отличительное имя субъекта Альтернативное имя субъекта Чек-бокс «Сведения о средствах ЭП и УЦ издателя» Наименование средства ЭП Заключение на средство ЭП Наименование средства УЦ Заключение на средство УЦ Чек-бокс «Сведения о средстве ЭП владельца сертификата» Наименование средства ЭП владельца сертификата
Ошибка удаления шаблона сертификата	CAENV126	ERROR	<p>Описание: Ошибка удаления шаблона сертификата</p> <p>Атрибуты:</p> <ul style="list-style-type: none"> Идентификатор шаблона Наименование шаблона (может отсутствовать) Период действия сертификата (может отсутствовать) Центр сертификации (может отсутствовать) Тип субъекта (может отсутствовать)

Описание события	Код события	Категория события	Подробное описание события
			<ul style="list-style-type: none"> Чек-бокс «Публиковать сертификат в ресурсную систему» Минимальная длина ключа RSA (может отсутствовать) Минимальная длина ключа ECDSA (может отсутствовать) Минимальная длина ключа ГОСТ Р 34.10-2012 (может отсутствовать) Использование ключа (может отсутствовать) Чек-бокс «Считать это расширение критическим» для списка использования ключа Расширенное использование ключа (может отсутствовать) Чек-бокс «Считать это расширение критическим» для списка расширенного использования ключа Чек-бокс «Включать SID субъекта в сертификат» OID политики сертификата (может отсутствовать) Чек-бокс «Считать это расширение критическим» для списка OID политики сертификата Чек-бокс «Контролировать соответствие полей в сертификате атрибутам субъекта» Отличительное имя субъекта (может отсутствовать) Альтернативное имя субъекта (может отсутствовать) Чек-бокс «Сведения о средствах ЭП и УЦ издателя» (может отсутствовать) Наименование средства ЭП (может отсутствовать) Заключение на средство ЭП (может отсутствовать) Наименование средства УЦ (может отсутствовать) Заклучение на средство УЦ (может отсутствовать) Чек-бокс «Сведения о средстве ЭП владельца сертификата» (может отсутствовать) Наименование средства ЭП владельца сертификата (может отсутствовать) Причина ошибки


Время хранения записей в журнале событий по умолчанию составлять 180 дней с момента регистрации. Время хранения регулируется с помощью параметра `archive_millis_ago` конфигурационного файла. Записи со сроком давности большим или равным времени хранения архивируются и удаляются из журнала событий. Режим архивации событий по умолчанию включен (параметр `archive_enabled` – флаг управления режимом архивации).

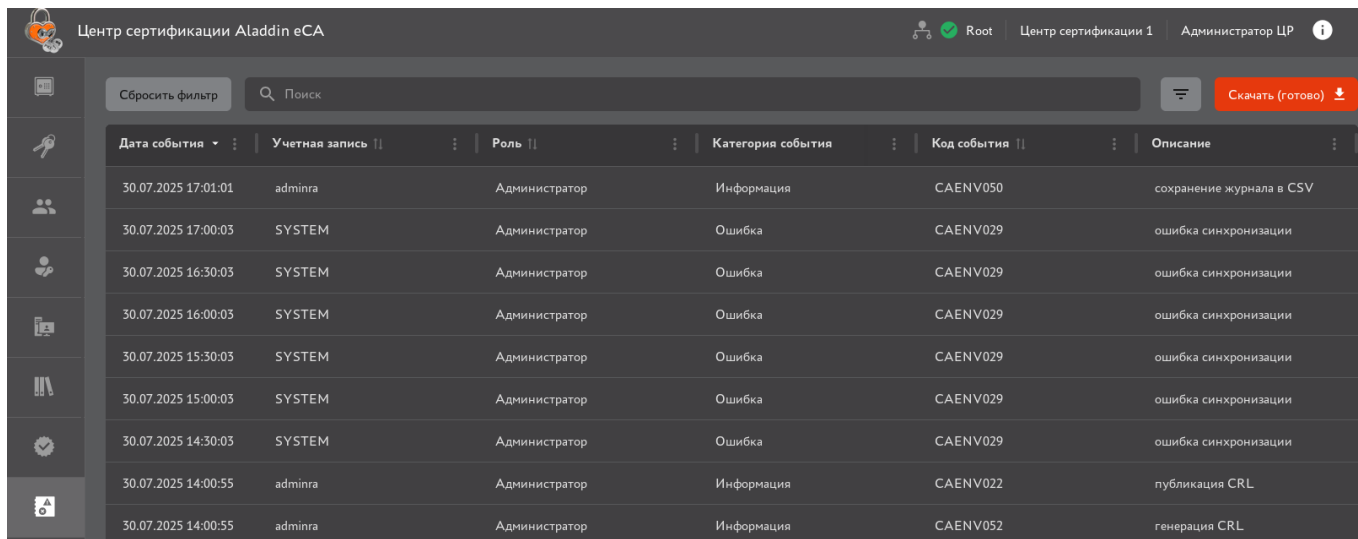
Периодичность запуска архивации регулируется параметром `archive_cron` конфигурационного файла. Значение указывается в формате CRON–выражения (значение по умолчанию – '0 0 0 1 * *'). По умолчанию процесс архивации запускается при наступлении первого числа каждого месяца.

Архив в формате `.zip`, содержащий `.csv` файл, с именем `logs-<дата создания архива>.zip` будет сохранён в каталог, указанный в параметре `archive_path` конфигурационного файла (по умолчанию `/opt/aecaCa/dist/archive`).

9.11.2 Просмотр записей журнала событий

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

Для просмотра записей журнала событий подключитесь к веб-интерфейсу Центра сертификации Aladdin eCA и перейдите в раздел  **Журнал событий**.



Дата события	Учетная запись	Роль	Категория события	Код события	Описание
30.07.2025 17:01:01	adminra	Администратор	Информация	CAENV050	сохранение журнала в CSV
30.07.2025 17:00:03	SYSTEM	Администратор	Ошибка	CAENV029	ошибка синхронизации
30.07.2025 16:30:03	SYSTEM	Администратор	Ошибка	CAENV029	ошибка синхронизации
30.07.2025 16:00:03	SYSTEM	Администратор	Ошибка	CAENV029	ошибка синхронизации
30.07.2025 15:30:03	SYSTEM	Администратор	Ошибка	CAENV029	ошибка синхронизации
30.07.2025 15:00:03	SYSTEM	Администратор	Ошибка	CAENV029	ошибка синхронизации
30.07.2025 14:30:03	SYSTEM	Администратор	Ошибка	CAENV029	ошибка синхронизации
30.07.2025 14:00:55	adminra	Администратор	Информация	CAENV022	публикация CRL
30.07.2025 14:00:55	adminra	Администратор	Информация	CAENV052	генерация CRL

Рисунок 198 – Просмотр записей журнала событий

Записи о событиях отображаются списком в табличном виде.

По умолчанию в колонках таблицы отображаются следующие атрибуты событий:




- Дата события.
- Учетная запись.
- Роль.
- Категория события.
- Код события.
- Описание.





Записи о событиях выводятся постранично. Для перемещения по страницам списка используйте инструменты навигации (см. Рисунок 199).



Рисунок 199 – Инструменты навигации

Описание инструментов навигации:

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

Для удобства анализа записей в списке вы можете управлять видимостью колонок таблицы. Чтобы скрыть отображение выбранной колонки, щелкните в ее заголовке значок  **<Действие колонки>** и в открывшемся списке ¹ выберите  **<Скрыть [название колонки] колонку>** (см. Рисунок 200). Чтобы вернуть в таблице отображение скрытых колонок, щелкните в заголовке любой колонки значок  **<Действие колонки>** и в открывшемся списке выберите  **<Показать все колонки>** (см. Рисунок 200).

¹ Набор действий колонок отличается в зависимости от атрибута события, представленного в данной колонке.

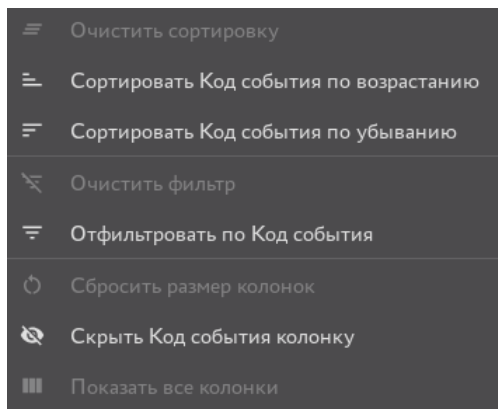



Рисунок 200 – Список действий с колонкой **[Код события]**



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

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




- По дате и времени регистрации события в порядке убывания или возрастания временных меток.
- По имени учетной записи инициатора события в алфавитном порядке.
- По роли инициатора события в алфавитном порядке.
- По коду события в порядке возрастания или убывания номера, содержащегося в коде.



По умолчанию сортировка записей в списке выполнена по дате и времени регистрации события (в порядке убывания временных меток).

Чтобы выполнить сортировку записей о событиях по выбранному атрибуту, щелкните в заголовке соответствующей колонки значок  **<Действие колонки>** и в открывшемся списке ¹ (см. Рисунок 200) выберите:

- Для упорядочивания по возрастанию –  **<Сортировать [название колонки] по возрастанию>**.
- Для упорядочивания по убыванию –  **<Сортировать [название колонки] по убыванию>**.

Статусы выполненной сортировки отображаются в заголовках колонок следующими значками ²:

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

Чтобы отменить сортировку записей по выбранному атрибуту, щелкните в заголовке соответствующей колонки значок  **<Действие колонки>** и в открывшемся списке выберите  **<Очистить сортировку>**.




Для поиска событий в списке вы можете выполнить выборку записей с помощью фильтров, расположенных в заголовках колонок. Каждый фильтр предназначен для выборки информации по атрибуту события, представленному в данной колонке. Возможно выполнить выборку информации, применив одновременно несколько фильтров.


Выборку записей о событиях возможно выполнить с помощью фильтров по следующим атрибутам:

- По дате события.
- По имени учетной записи.
- По роли.
- По категории события.
- По коду события.

¹ Набор действий колонок отличается в зависимости от атрибута события, представленного в данной колонке.

² Менять порядок сортировки, а также отменять сортировку можно, последовательно щелкая на значок статуса сортировки по колонке.

По умолчанию фильтры скрыты. Чтобы использовать фильтры, нажмите на панели инструментов кнопку  **<Фильтр>** или щелкните в заголовке колонок **[Сценарий]**, **[Дата обработки]** или **[Статус]** значок  **<Действие колонки>** и в открывшемся списке выберите  **<Отфильтровать по [название колонки]>** (см. Рисунок 201).

Чтобы скрыть фильтры, нажмите на панели инструментов кнопку  **<Фильтр>**. При этом выборка записей, выполненная с помощью фильтров, сохраняется.

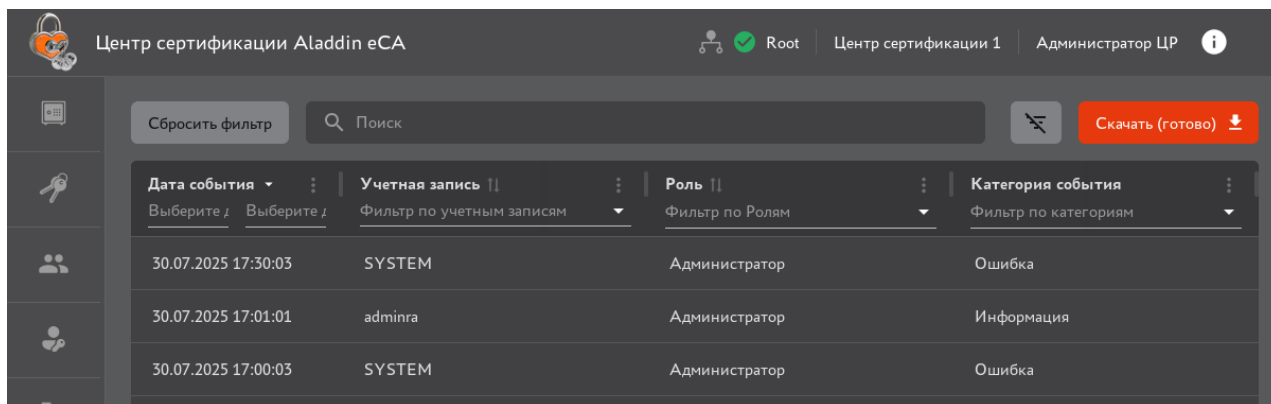



Рисунок 201 – Отображение фильтров в заголовках колонок включено

Чтобы выполнить выборку информации с помощью фильтра (открыть окно фильтра), щелкните название фильтра в заголовке колонки.

Фильтры по атрибутам событий, представленный в колонках **[Учетная запись]** (см. Рисунок 202а), **[Роль]** (см. Рисунок 202б), **[Категория события]** (см. Рисунок 202в) и **[Код события]** (см. Рисунок 202г) обеспечивают выборку информации по выбранным атрибутам. Выбор атрибутов выполняется установкой флажков для соответствующих значений атрибутов. Фильтр по атрибуту события, представленном в колонке **[Дата события]** (см. Рисунок 202д), обеспечивает выборку информации за указанный временной интервал. Начало и конец временного интервала (дата и время) задаются с помощью календарей и списков.

Заданные фильтрами критерии выборки отображаются в заголовках соответствующих колонок. Признаком применения фильтра является значок  в заголовке соответствующей колонки (см. Рисунок 202).

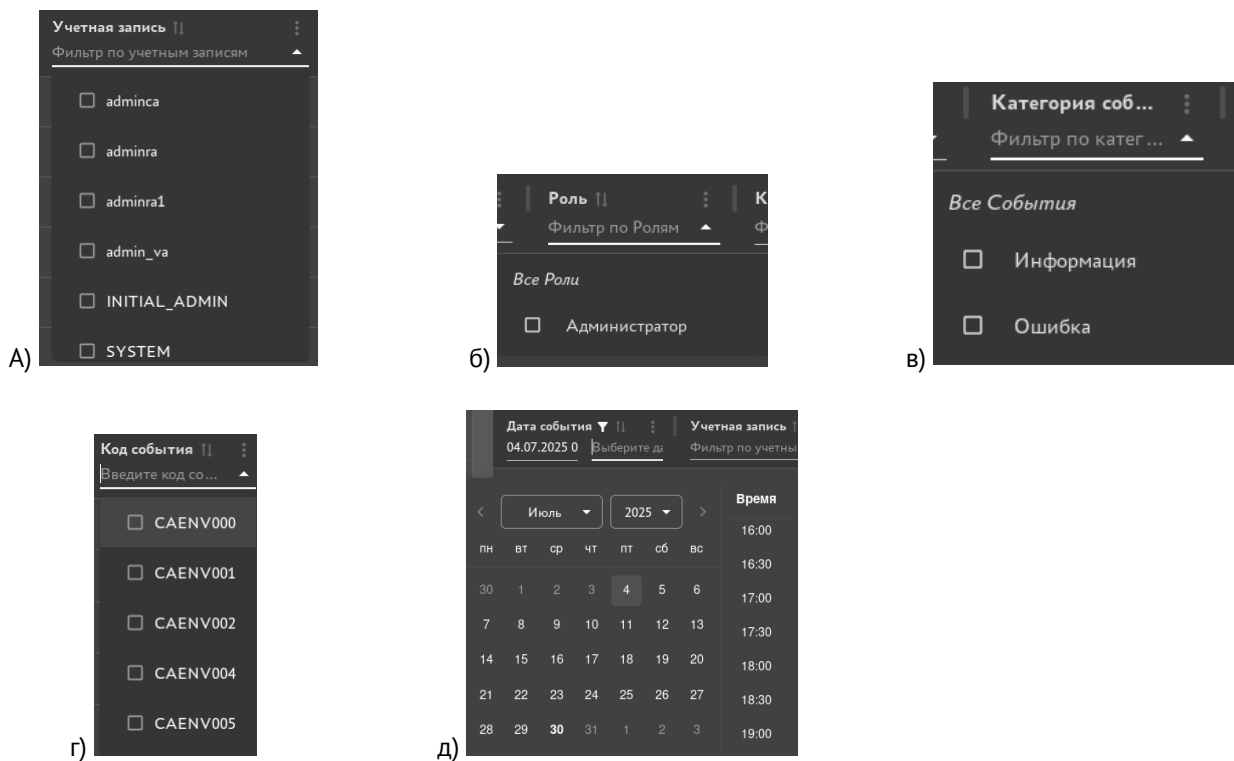






Рисунок 202 – Указание критериев выборки в фильтрах

Чтобы отменить действие определенного фильтра, щелкните в заголовке колоноки значок  **<Действие колоноки>** и в открывшемся списке выберите  **<Очистить фильтр>** или щелкните в заголовке колоноки значок .

Чтобы отменить действие всех фильтров, нажмите на панели инструментов кнопку  **Сбросить фильтр**.

Чтобы выполнить выборку событий по их описанию (в том числе и подробному) и причинам, введите в поисковой строке, расположенной на панели инструментов, ключевое слово, содержащееся в описании или причине события (см. Рисунок 203). Для отмены выборки щелкните в поисковой строке значок .

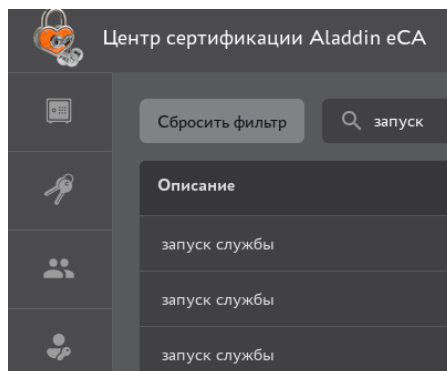



Рисунок 203 – Выборка событий по описанию с помощью поисковой строки

9.11.3 Просмотр карточки события

Карточка события содержит представленную в удобном для анализа виде подробную информацию о событии (описание атрибутов события см. в разделе 9.11.1).

Чтобы открыть карточку события:

- Подключитесь к веб-интерфейсу Центра сертификации Aladdin eCA и перейдите в раздел  **Журнал событий**.
- Найдите нужное событие и щелкните запись о нем в списке (см. Рисунок 204).

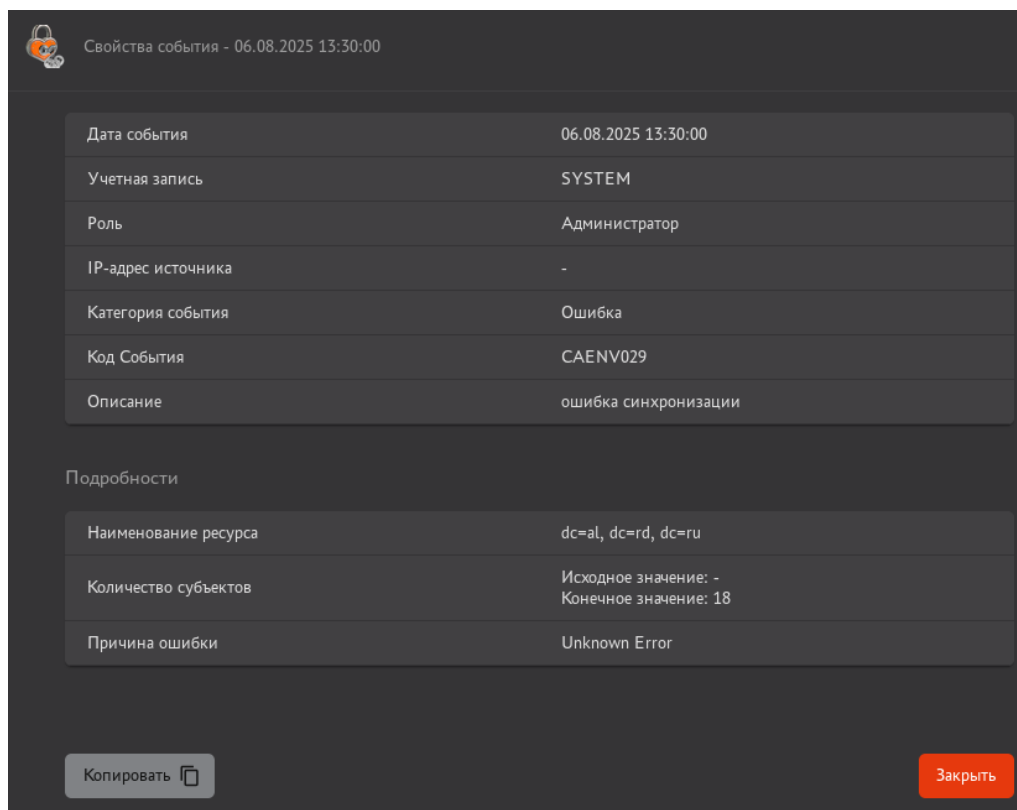
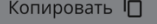


Рисунок 204 – Окно «Свойства события» (карточка события)

Для копирования информации о событии в буфер обмена нажмите кнопку . Содержимое события из буфера обмена можно вставить, например, в текстовый файл (см. Рисунок 205).

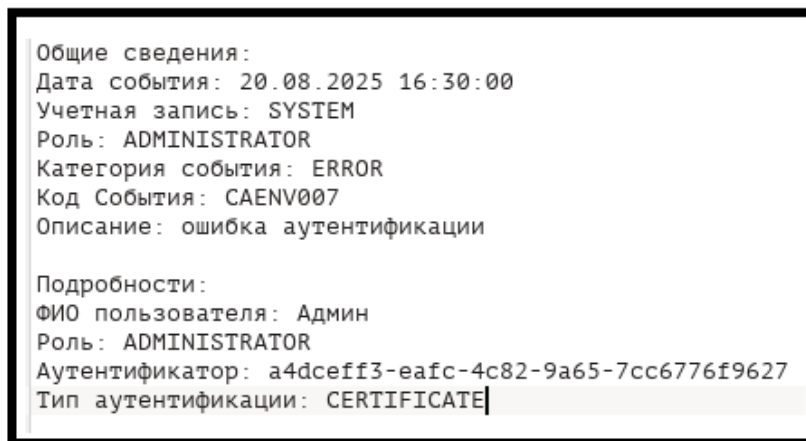


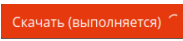
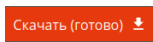


Рисунок 205 – Пример копирования события в текстовый файл

9.11.4 Экспорт записей журнала событий

Вы можете выгрузить записи журнала событий в файл формата `.csv` (кодировка UTF-8 с разделителем «;»), помещенный в архив в формате `.zip`. Записи списка экспортируются в файл в объеме выборки, сделанной с помощью фильтров и строки поиска.

Порядок экспорта журнала событий:

- Подключитесь к веб-интерфейсу Центра сертификации Aladdin eCA и перейдите в раздел  **Журнал событий**.
- Запустите процесс подготовки файла с событиями, нажав на панели инструментов кнопку . В результате кнопка меняет свое состояние на  (начинается подготовка файла, содержащего записи журнала событий).
- После подготовки файла для экспорта журнала нажмите кнопку .

9.11.5 Передача информации о событиях в сторонние системы по протоколу Syslog


Мониторинг событий аудита может выполняться в сторонних SIEM-системах. Передача информации о событиях на принимающие серверы SIEM-систем выполняется по протоколу Syslog (в соответствии с рекомендацией RFC5424). В качестве транспортного протокола для передачи данных может использоваться UDP или TCP. Использование протокола UDP не гарантирует доставку данных принимающей стороне. Максимально возможно добавить и отправлять сообщения на 10 Syslog-серверов.

Значения полей отправляемых Syslog-сообщений о зарегистрированных событиях представлено в таблице 25.

Таблица 25 – 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 Центра регистрации в формате ISO 8601: YYYY-MM-DDThh:mm:ss[.SSS]
HOSTNAME	Имя хоста, отправляющего сообщение	FQDN хоста Центра сертификации Aladdin eCA

Поле Syslog-сообщения	Описание	Значение
APP-NAME	Тег, указывающий приложение или процесс, создавшего сообщение	AECA-CA
PROCID	Идентификатор процесса (PID) приложения	PID сервиса, являющегося источником события
MSGID	Идентификатор сообщения	Код события
[STRUCTURED-DATA]	Структурированные данные	<p>[aeca-ca actionCode="actionCode" category="category" id="id" serviceName="serviceName" system="system" username="username" role="role" ipAddress="ipAddress" attributes="attributes"]</p> <p>где:</p> <ul style="list-style-type: none"> "actionCode" – код события; "category" – категория события; "id" – идентификатор типа события; "serviceName" – имя сервиса, в котором произошло событие; "system" – флаг системного события; "username" – логин учетной записи инициатора события; "role" – роль инициатора события; "ipAddress" – IP-адрес инициатора события; "attributes" – расширенное описание события. <p>Состав полей расширенного описания события соответствует составу полей описания события, указанному в таблице 24. Для категории события «ERROR» (ошибка) передается значение поля «description» (причина ошибки). Пример содержания "attributes" для ошибки CAENV055:</p> <p>attributes=>[CN: red; email: red@sambadc.host; шаблон: Рассылка об истечении срока действия сертификата через 1 день; причина ошибки: <description>]»].</p>
MESSAGE	Строка, содержащая описание события	Описание события

Чтобы просмотреть созданные в Центре сертификации Aladdin eCA Syslog-серверы, подключитесь к веб-интерфейсу Центра сертификации Aladdin eCA и перейдите в раздел  **Настройка > Syslog**.

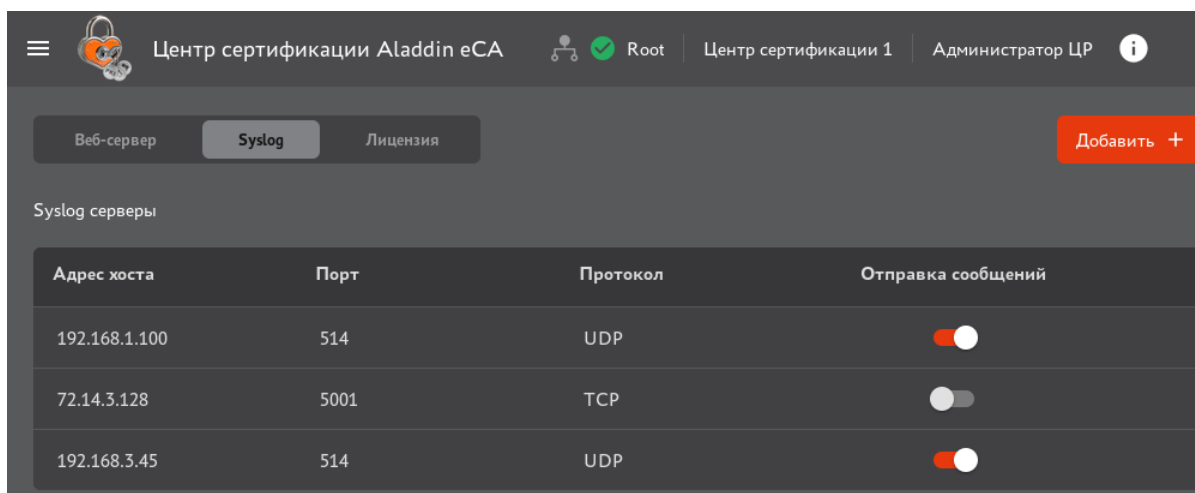



Рисунок 206 – Список Syslog-серверов


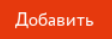
Записи о Syslog-серверах отображаются списком в табличном виде. По умолчанию в колонках таблицы отображаются следующие атрибуты Syslog-серверов:

- Адрес хоста – IP-адрес или доменное имя Syslog-сервера.

- Входящий порт Syslog-сервера, на который отправляются сообщения (число в диапазоне от 0 до 65535).
- Транспортный протокол, по которому выполняется передача данных.

После добавления нового Syslog-сервера отправка сообщений на него по умолчанию включена. Чтобы управлять передачей данных на Syslog-серверы, используйте переключатель  в колонке **[Отправка сообщений]**.

Порядок добавления Syslog-сервера:

- На панели инструментов нажмите кнопку .
- В открывшемся окне (см. Рисунок 207) выполните следующие действия:
 - В поле «Адрес хоста» укажите IP-адрес или доменное имя Syslog-сервера.
 - В поле «Порт» укажите входящий порт Syslog-сервера, на который будут отправляться сообщения (число в диапазоне от 0 до 65535).
 - В списке «Протокол» выберите транспортный протокол, по которому будет выполняться передача данных.
 - Нажмите кнопку .

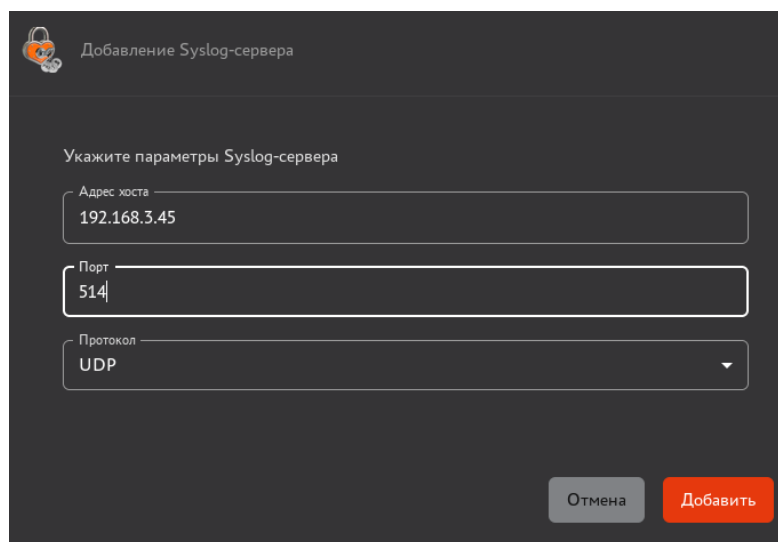




Рисунок 207 – Добавление Syslog-сервера

Чтобы изменить настройки Syslog-сервера в строке с записью о выбранном Syslog-сервере щелкните значок  **<Выбрать действие>**, выберите в списке  **<Редактировать>** (Рисунок 208) и в открывшемся окне измените параметры Syslog-сервера.

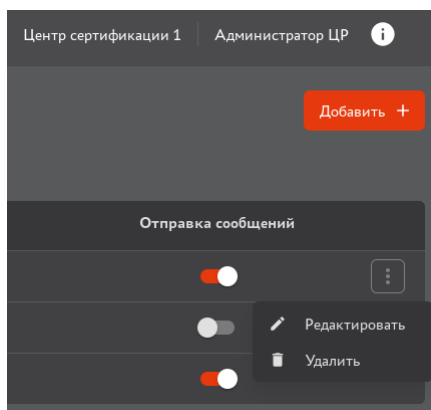




Рисунок 208 – Выбор действия с Syslog-сервером

Чтобы удалить Syslog-сервера в строке с записью о выбранном Syslog-сервере щелкните значок  **<Выбрать действие>**, выберите в списке  **<Удалить>** (Рисунок 208) и в открывшемся окне подтвердите Syslog-сервера.

9.12 Управление шаблонами сертификатов

9.12.1 Общие сведения о шаблонах сертификатов

Расширить возможности Центра сертификации возможно путем создания пользовательских шаблонов сертификатов.

В Центра сертификации Aladdin eCA различают следующие типы шаблонов сертификатов:

- Предустановленные шаблоны – шаблоны, созданные по умолчанию при установке Центра сертификации Aladdin eCA.

Предустановленные шаблоны нельзя удалять и редактировать.

- Импортированные шаблоны – шаблоны, созданные в Microsoft Certificate Services (далее – MS CS) и импортированные в Центр сертификации Aladdin eCA из файла формата CSV.

Подробная информация об экспорте шаблонов сертификатов из MS CS в файл и их последующем импорте в Центр сертификации Aladdin eCA представлена в разделе 9.12.6).

Импортированные шаблоны можно редактировать и удалять.

- Пользовательские шаблоны – шаблоны, созданные уполномоченным пользователем путем клонирования и последующего редактирования существующих в Центре сертификации Aladdin eCA шаблонов любого типа.

Пользовательские шаблоны можно редактировать и удалять.

Пользователь с ролью «Администратор» может выполнять любые операции с шаблонами. Пользователь с ролью «Оператор» может просматривать параметры тех шаблонов, на которые ему предоставлены права в соответствии с правилами доступа, назначенными пользователем с ролью «Администратор» (см. подробнее в разделе 9.7).

Перечень предустановленных в Центре сертификации Aladdin eCA шаблонов сертификатов:

- 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 Центра сертификации Aladdin eCA до версии 2.3 все предустановленные в версии 2.1.2 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».

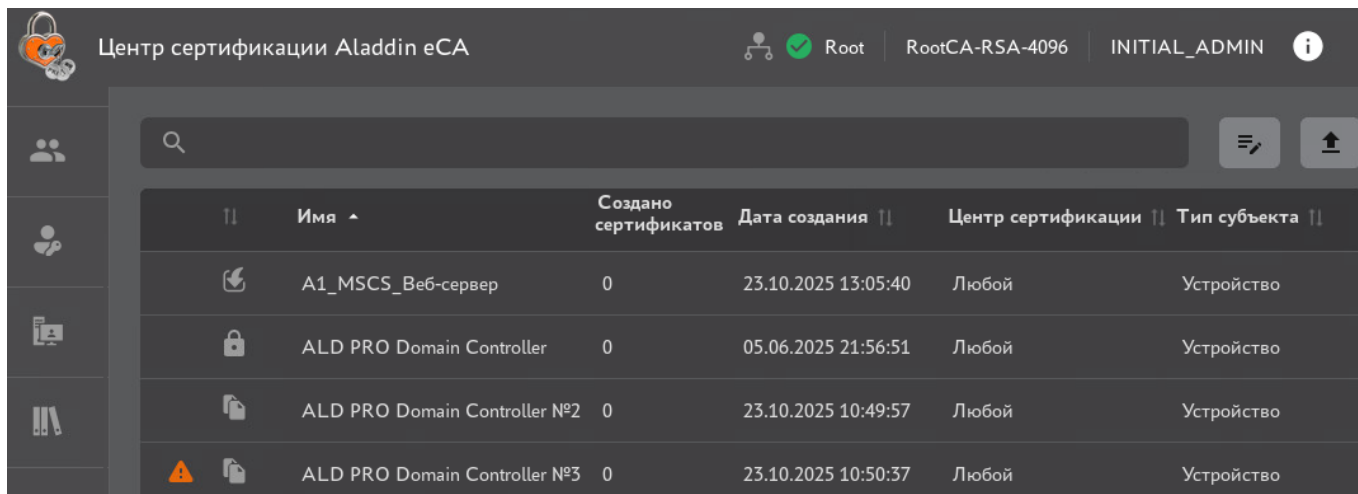
Действия, доступные с шаблонами сертификатов:

- Просмотр списка шаблонов сертификатов.
- Просмотр характеристик и полей шаблона сертификатов.
- Импорт шаблонов сертификатов MS CS из CSV-файла.
- Создание пользовательских шаблонов путем клонирования и последующего редактирования существующих шаблонов любого типа.
- Удаление пользовательских и импортированных шаблонов (в том числе одновременное удаление нескольких шаблонов).

Шаблоны доступны для использования при выпуске сертификатов на вкладке «Сертификаты» и «Субъекты» (см. раздел 9.4 и 9.7 настоящего руководства).

9.12.2 Просмотр информации о шаблонах сертификатов


Для просмотра информации о шаблонах подключитесь к веб-интерфейсу Центра сертификации Aladdin eCA и перейдите в раздел  **Шаблоны** (см. Рисунок 209).






Имя	Создано сертификатов	Дата создания	Центр сертификации	Тип субъекта
A1_MSCS_Веб-сервер	0	23.10.2025 13:05:40	Любой	Устройство
ALD PRO Domain Controller	0	05.06.2025 21:56:51	Любой	Устройство
ALD PRO Domain Controller №2	0	23.10.2025 10:49:57	Любой	Устройство
ALD PRO Domain Controller №3	0	23.10.2025 10:50:37	Любой	Устройство

Рисунок 209 – Просмотр информации о шаблонах

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

-  - Приznak отсутствия контроля соответствия полей в сертификате атрибутам субъекта при выпуске сертификата по данному шаблону, что позволяет записывать в поля сертификата любые (в соответствии с регулярными выражениями полей) значения, не соответствующие 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 в Центре сертификатов Aladdin eCA должен быть строго ограничен.

- Условное обозначение типа шаблона:
 -  – предустановленные по умолчанию шаблоны.
 -  – пользовательские шаблоны.
 -  – импортированные из файла шаблоны MS CS.

расположенным рядом с обозначением вида шаблона.

- 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 с версии 2.1.2 до версии 2.3 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 с версии 2.1.2 до версии 2.3 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.

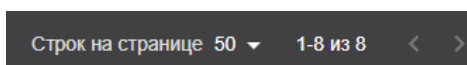





Рисунок 210 – Инструменты навигации

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 разрешен 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, щелкните 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 щелкните в поисковой строке значок  или удалите ключевое слово в поисковой строке.

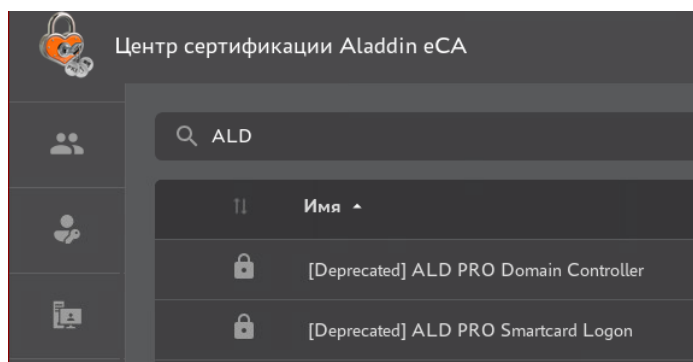





Рисунок 211 – Выборка шаблонов по их именам с помощью поисковой строки

9.12.3 Просмотр карточки шаблона сертификата

Чтобы открыть карточку шаблона:

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

В карточке шаблона (см. Рисунок 212) администратору доступны следующие инструменты и информация:

- Кнопка возврата на вкладку «Шаблоны».
- Кнопка  для клонирования текущего шаблона.
- Кнопка  для записи изменений полей текущего шаблона, доступная для всех шаблонов, кроме предустановленных.
- Имя шаблона.
- Постоянный идентификатор шаблона.

Центр сертификации Aladdin eCA

← Шаблоны

Имя шаблона: ECA-Auth-2

Идентификатор: 98b5967c-c666-4e3c-a5ae-f817e79f7135

Дата создания: 05.03.2025 15:24:38

Дата изменения: 05.03.2025 15:24:38

Свойства | Расширения | Компоненты имени сертификата | Сведения о средствах ЭП

Общие

Период действия сертификата: 2y

Формат ввода: 1m,1h,1d,1mo,1y — минута, час, день, месяц, год.
Примеры значений: 30m1h, 12h1d, 1mo, 6mo1y, 2y.

Центр сертификации: Любой

Тип субъекта: Пользователь

☐ Публиковать сертификат в ресурсную систему

Шифрование

☒ RSA
Минимальная длина ключа: 1024

☒ ECDSA
Минимальная длина ключа: 256

☐ ГОСТ Р 34.10-2012
Минимальная длина ключа: 256

Рисунок 212 – 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 Центре 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 213):

Свойства | Расширения | Компоненты имени сертификата | Сведения о средствах ЭП

Общие

Период действия сертификата: 1d1y

Формат ввода: 1m,1h,1d,1mo,1y — минута, час, день, месяц, год.
Примеры значений: 30m1h, 12h1d, 1mo, 6mo1y, 2y.

Центр сертификации: Любой

Тип субъекта: Пользователь

☐ Публиковать сертификат в ресурсную систему

Шифрование

☒ RSA
Минимальная длина ключа: 2048


☒ ECDSA
Минимальная длина ключа: 256

☒ ГОСТ Р 34.10-2012
Минимальная длина ключа: 256

Рисунок 213 – 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).
 - Поле «Центр сертификации» – Центр сертификации, в котором возможен выпуск сертификатов по данному шаблону.
 - Поле «Тип субъекта» – определяет тип субъекта, для которого предназначен данный шаблон (корневой Центр сертификации, подчинённый Центр сертификации, устройство, пользователь).
 - чек-бокс «Публиковать сертификат в ресурсную систему».
- 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»;
- Чек-бокс «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 включенной опции в поле сертификата субъекта с OID 1.3.6.1.4.1.311.25.2 будет записан его SID (при наличии данного атрибута у субъекта). SID может быть получен только для субъектов ресурсных систем MS AD, SambaDC, РЕД АДМ и Альт Домен.
- Список с возможностью удаления и добавления элементов «OID политики сертификата».
- Чек-бокс «Считать это расширение критическим» для списка «OID политики сертификата».

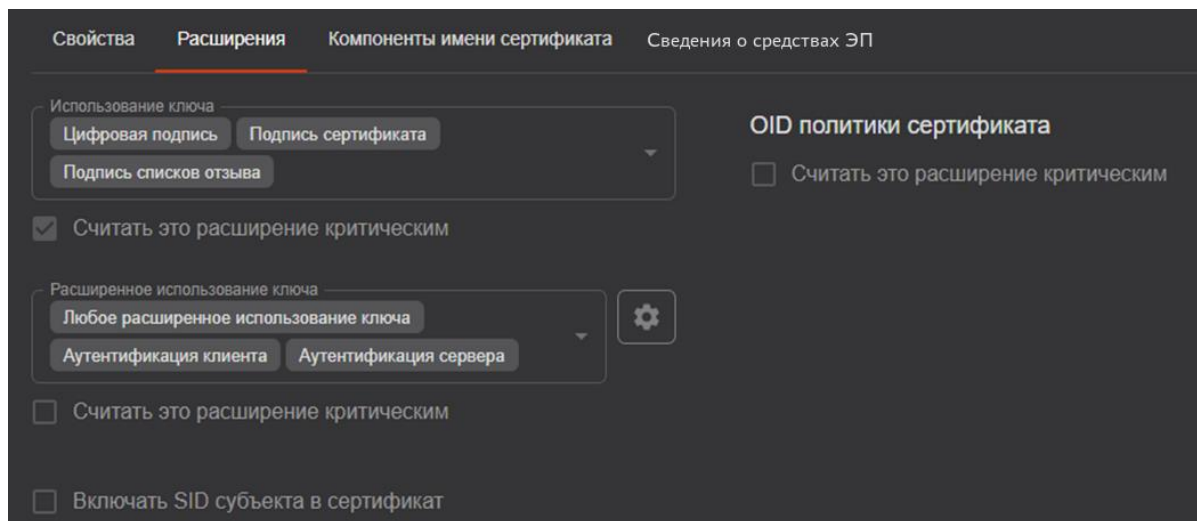


Рисунок 214 – Вкладка «Расширения» шаблона сертификата

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 215).

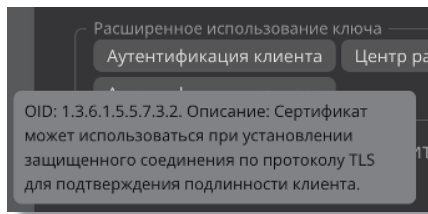


Рисунок 215 – Всплывающая подсказка значения расширенного использования ключа

На вкладке «Компоненты имени сертификата» доступны (см. Рисунок 216):

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

Рисунок 216 – Карточка шаблона (вкладка «Компоненты имени сертификата»)

На вкладке «Сведения о средствах ЭП» доступны:

Рисунок 217 – 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.
 - Поле «Наименование средства ЭП» - в поле указывается наименование средства ЭП удостоверяющего центра (далее -УЦ) издателя.
 - Поле «Заключение на средство ЭП» - в поле указывается номер и дата выдачи заключения на средство ЭП удостоверяющего центра издателя.
 - «Наименование средства УЦ» - в поле указывается наименование средства УЦ издателя.
 - «Заключение на средство УЦ» - в поле указывается номер и дата выдачи заключения на УЦ издателя.
- 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.

9.12.4 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 Центра сертификации Aladdin eCA 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 218) при необходимости отредактируйте имя нового пользовательского шаблона в соответствующем поле и нажмите кнопку  **Клонировать**.
- Имя шаблона должно быть уникальным. Длина имени шаблона не должна превышать 255 символов.

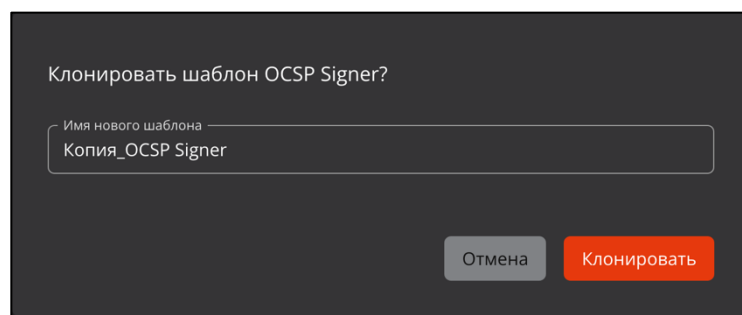


Рисунок 218 – Экран раздела меню «Шаблоны»

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 Центра сертификации Aladdin eCA и перейдите в раздел  **Шаблоны**.

- Откройте карточку шаблона (см. Рисунок 219), редактирование которого вы хотите выполнить. Для этого найдите запись о нем в списке и выберите ее.

← Шаблоны + Сохранить

Имя шаблона
A1_MSCS_Веб-сервер

Идентификатор	bc9e3a1e-f7bb-4a3c-8e8c-633f65cdb170
Дата создания	23.10.2025 13:05:40
Дата изменения	23.10.2025 16:06:07

Свойства Расширения Компоненты имени сертификата Сведения о средствах ЭП и УЦ

Общие

Период действия сертификата
2y

Формат ввода: 1m, 1h, 1d, 1mo, 1y — минута, час, день, месяц, год.
Примеры значений: 30m1h, 12h1d, 1mo, 6mo1y, 2y.

Центр сертификации
Любой

Тип субъекта
Пользователь

☐ Публиковать сертификат в ресурсную систему

Шифрование

☒ RSA
Минимальная длина ключа
2048

☐ ECDSA
Минимальная длина ключа
256

☒ ГОСТ Р 34.10-2012
Минимальная длина ключа
512

Рисунок 219 – 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.
- Подчиненный 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 220) и при необходимости выполните редактирование (добавление, удаление) следующих полей и опций шаблона:

Рисунок 220 – 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 уточненное назначение открытого ключа сертификата, который будет выпущен по данному шаблону.



Перечень предустановленных ¹ 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.
- 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.

¹ Описание предустановленных идентификаторов расширенного использования ключа приведено в Приложении 4 «Описание предустановленных идентификаторов расширенного использования ключа».

- 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 221) нажмите кнопку .

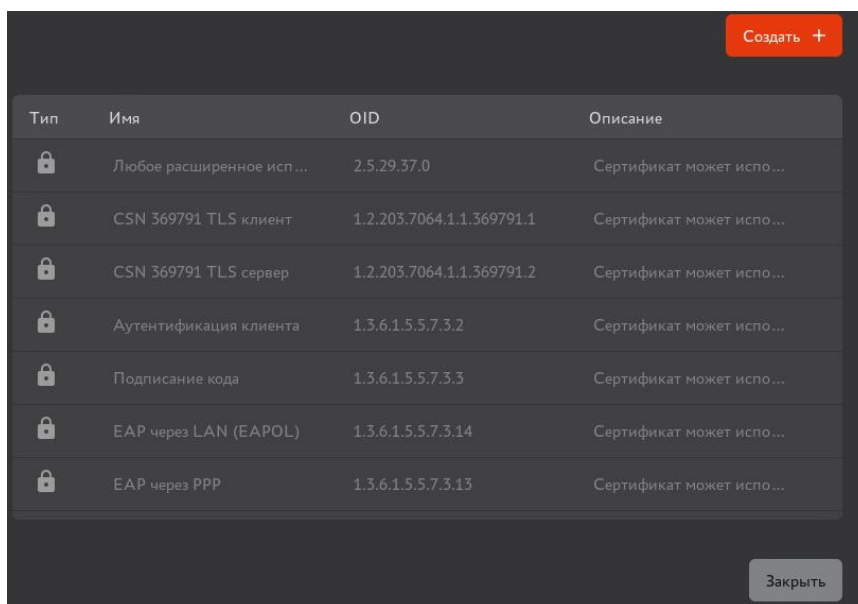

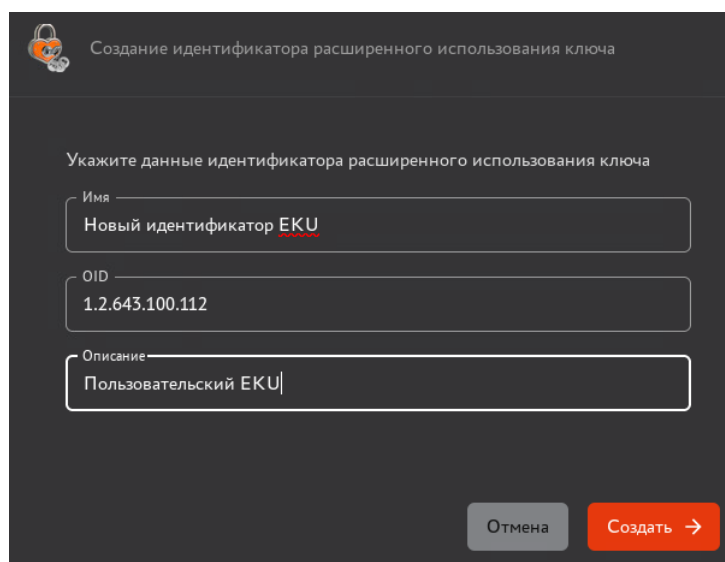


Рисунок 221 – Просмотр списка идентификаторов расширенного использования открытого ключа

- В открывшемся окне (см. Рисунок 222) в соответствующих поля укажите имя¹, OID², описание пользовательского идентификатора расширенного использования открытого ключа и нажмите кнопку .



Создание идентификатора расширенного использования ключа

Укажите данные идентификатора расширенного использования ключа

Имя
Новый идентификатор ECU

OID
1.2.643.100.112

Описание
Пользовательский ECU



Отмена Создать →


Рисунок 222 – Создание пользовательского идентификатора расширенного использования открытого ключа

¹ 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».


² 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».

В результате пользовательский идентификатор расширенного использования открытого ключа появится в списке в окне «Идентификаторы расширенного использования ключа» (см. Рисунок 221) 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 221) 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 .

- 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) ¹ субъекта, установите флажок «Включать SID субъекта в сертификат».
- Перейдите на вкладку «Компоненты имени сертификата» карточки шаблона (см. Рисунок 223) и при необходимости выполните редактирование (добавления, удаления) следующих полей и опций шаблона:

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

Рисунок 223 – 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 ¹. 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 в Центре сертификатов Aladdin eCA должен быть строго ограничен.

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

Рисунок 224 – Подтверждение отключения контроля соответствия полей в сертификате атрибутам субъекта

Внимание! После обновления ПО до версии 2.3 у всех имеющихся в программе шаблонов опция «Контролировать соответствия полей в сертификате атрибутам субъекта» включена по умолчанию.

¹ 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 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.
- Unstructured address.
- Unstructured name.
- Email Address (E).
- Serial number.
- Дата рождения.
- Место рождения.
- ИНН.
- ОГРН.
- ОГРНИП
- СНИСЛ
- ИНН ЮЛ

Чтобы добавить атрибут (тип поля) ¹ в отличительное имя субъекта, в разделе «Отличительное имя субъекта» выполните следующие действия:

- Нажмите кнопку .


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

- В появившемся списке «Тип поля» выберите атрибут (тип поля) отличительного имени субъекта, который будет включен 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» выполните следующие действия:

- Нажмите кнопку .
- В появившемся списке «Тип поля» выберите тип поля альтернативного имени субъекта, который будет включен 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.
- По умолчанию после добавления атрибут (тип поля) отличительного или альтернативного имени субъекта является необязательными. То есть выпуск сертификата по такому шаблону для субъекта будет возможен, даже если у субъекта отсутствует добавленный атрибут. Вы можете определить обязательные атрибуты отличительного и альтернативного имен субъекта с помощью флажков «Обязательное». При этом при отсутствии обязательных атрибутов у субъекта выпуск сертификатов по данному шаблону для субъекта будет невозможен.
- По умолчанию после добавления в шаблон атрибута (тип поля) отличительного или альтернативного имени субъекта необходимость его валидации ¹ при выпуске сертификата по умолчанию отключена. То есть 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».

¹ Правила валидации значений атрибутов представлены в Приложении 3 «Правила валидации значений полей по умолчанию предустановленных шаблонов сертификатов»

- Перейдите на вкладку «Сведения о средствах ЭП и УЦ издателя» (см. Рисунок 225) 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 обязательном 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 средстве 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 225 – Карточка шаблона (вкладка «Сведения о средствах ЭП и УЦ издателя»)



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

9.12.5 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 Центра сертификации Aladdin eCA 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 .

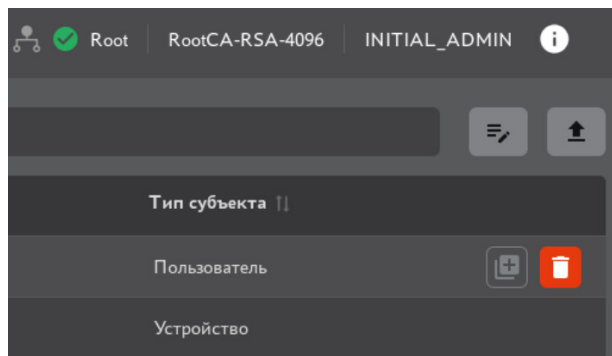


Рисунок 226 – Инициализация процесса удаления шаблона

- В открывшемся окне нажмите кнопку **Удалить**.

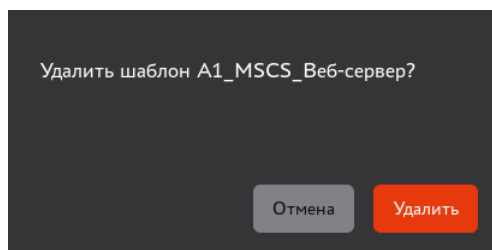







Рисунок 227 – Окно подтверждения удаления шаблона сертификата

После удаления шаблона сертификаты, выпущенные по нему, остаются действительными.

Порядок одновременного удаления нескольких шаблонов:

- Подключитесь к веб-интерфейсу Центра сертификации Aladdin eCA и перейдите в раздел  **Шаблоны**.
- На панели инструментов нажмите кнопку .
- В открывшемся окне (см. Рисунок 228) выполните следующие действия:
 - В списке «Выбрать» с помощью флажков выберите шаблоны, которые необходимо удалить, и щелкните 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 щелкните значок . В результате выбранные шаблоны будут перемещены в список «Выбрать».
 - Чтобы найти шаблон в списках, используйте поля поиска.
 - Нажмите кнопку **Продолжить** .

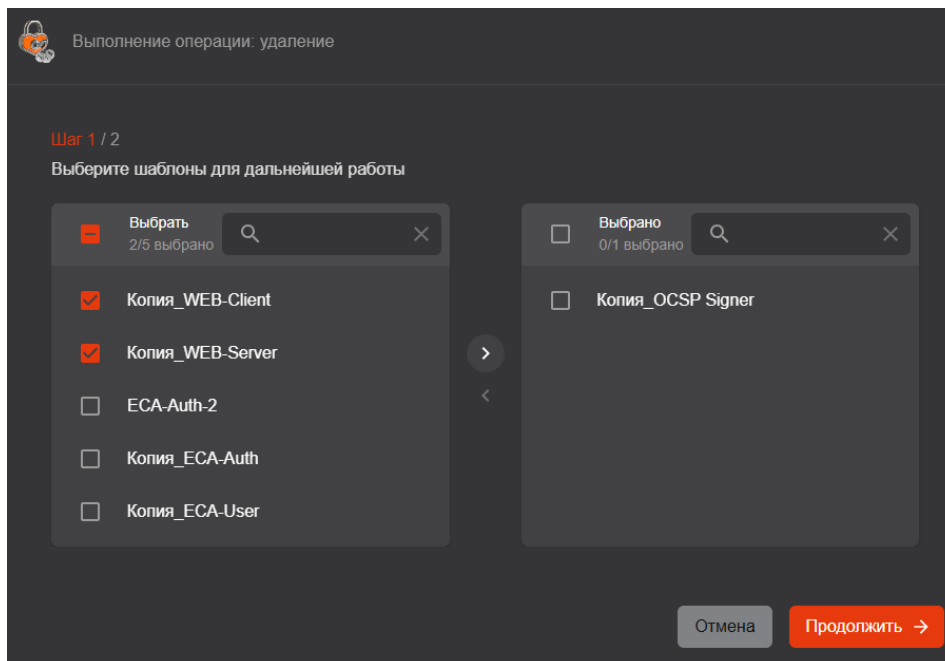


Рисунок 228 – Выбор шаблонов для удаления

- В открывшемся окне подтвердите действие, нажав кнопку **<Применить>** (см. Рисунок 229).

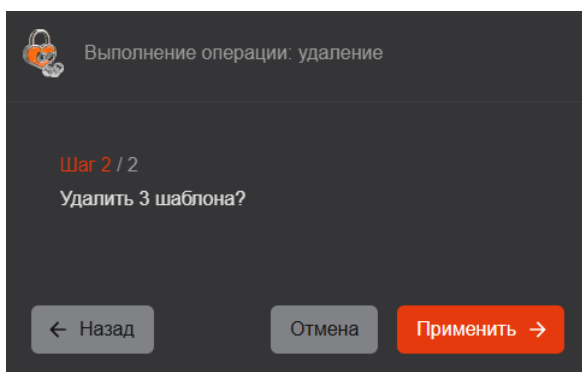


Рисунок 229 – Окно выполнения массовых операций. Шаг 3

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

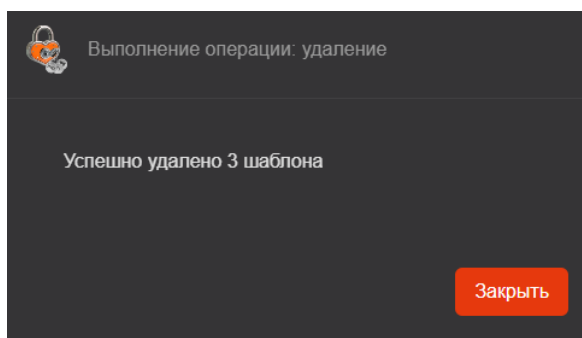


Рисунок 230 – Окно выполнения массовых операций. Шаг 4

9.12.6 Импорт шаблонов MS CS



Перед импортом шаблонов MS CS в Центр сертификации Aladdin eCA необходимо предварительно экспортировать их из MS CS.

Для экспорта шаблонов запустите скрипт **mcs2aeca.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 Центр Сертификации Aladdin eCA из файла:

- Подключитесь к веб-интерфейсу Центра сертификации Aladdin eCA 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 уведомлен сообщением на экране «XX шаблонов успешно загружено», где «XX» – количество успешно загруженных шаблонов (см. Рисунок 231).

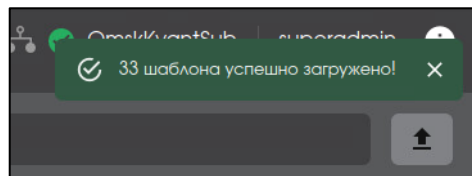


Рисунок 231 – Уведомление об успешной загрузке шаблонов MSCS

В случае, если шаблоны не были импортированы, администратор будет уведомлен сообщением «Невозможно загрузить шаблоны» (см. Рисунок 231).

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. (счетчик копий).

Поля, загружаемые из CSV-файла с шаблонами MS CS, приведены в таблице 26.

Таблица 26 – 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»

Название поля в файле	Описание	Название поле в АЕСА
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 «Подчиненный 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 «TplName», и присвоением порядкового номера (счетчик копий).

9.13 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 eCA.
- DNS Name – имя хоста, на котором развернут Центр сертификации Aladdin eCA (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 Csrnginx, 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 csrnginx 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 Центра сертификации Aladdin eCA и перейдите в раздел  **Настройка > Веб-сервер** (Рисунок 232).

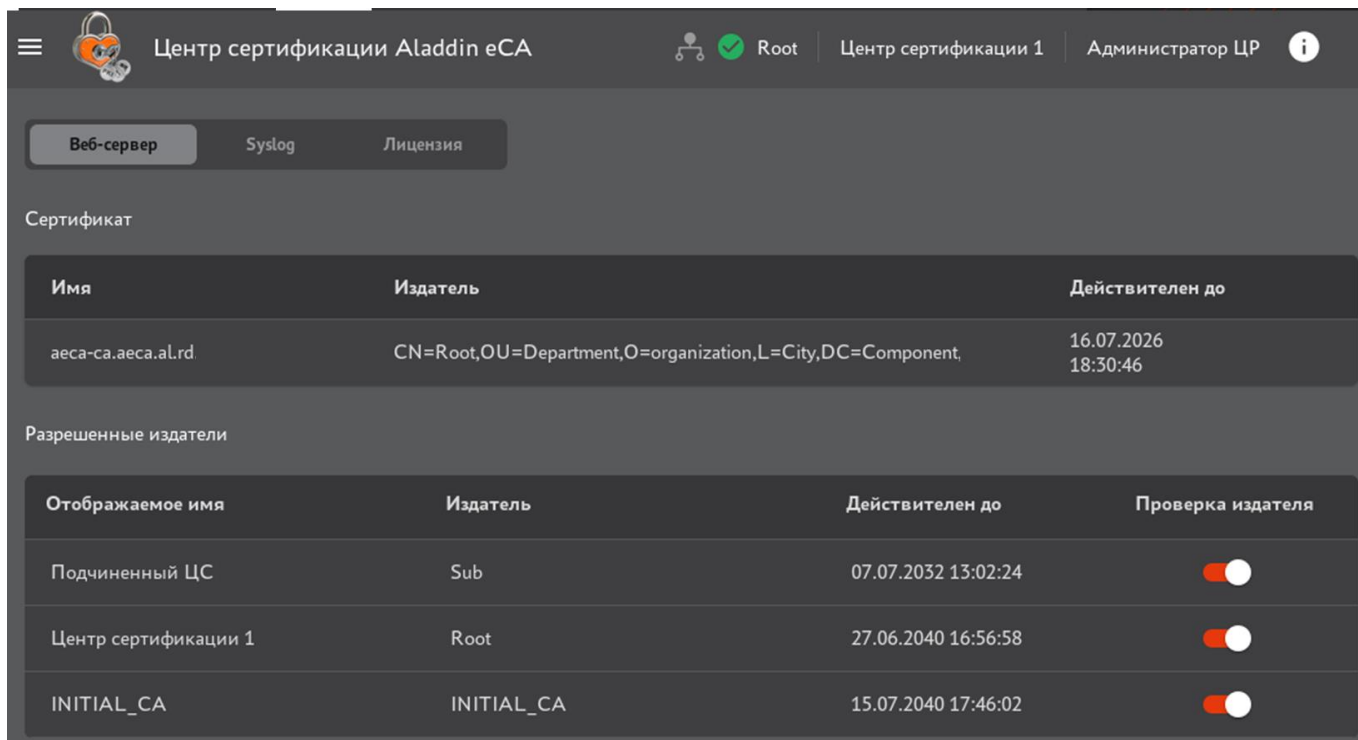




Рисунок 232 – Экран раздела «Настройки»

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 233) выберите файл сертификата и введите пароль от контейнера.
- Нажмите кнопку .

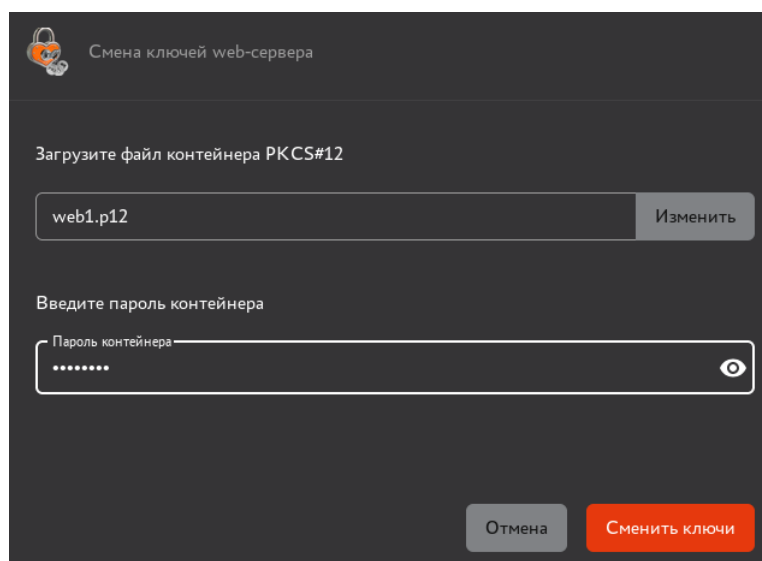



Рисунок 233 – Смена ключей веб-сервера

- 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.

9.14 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 разрешенных). С сертификатом, выпущенным исключённым из списка разрешенных издателем, аутентификация пользователя будет невозможна.

Для просмотра списка разрешенных издателей подключитесь к веб-интерфейсу Центра сертификации Aladdin eCA и перейдите в раздел  **Настройка > Веб-сервер** (Рисунок 232).

Информация о разрешенных издателях отображается в разделе «Разрешенные 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 разрешенных издателей.

10 ПОИСК И УСТРАНЕНИЕ НЕИСПРАВНОСТЕЙ

Ид.	Проблема	Возможная причина	Способы решения
П001	Заблокированы кнопки выпуска сертификатов	Истёк срок действия лицензии или исчерпан лимит доступных для выпуска сертификатов	Проверьте в окне «О программе» срок действия лицензии и количество доступных для выпуска сертификатов (см. раздел 3.1)
П002	Прекращение установки 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: sudo update-alternatives --config java sudo update-alternatives --config javac sudo 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</code> , <code>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"> – 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> – 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> – 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> <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"> 1. Firefox получает сертификат веб-сервера от сервера 2. После этого выполняет поиск в хранилище сертификатов ОС сертификата ЦС по SDN издателя сертификата 3. И далее выполняет проверку цепочки по открытым ключам 	<ol style="list-style-type: none"> 1. Проверьте состав сертификатов доверенных ЦС в хранилище ОС 2. В случае несоответствия установите сертификат издателя сертификата веб-сервера
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:</p> <pre>keytool -import -alias managementca -file cert.pem -keystore ./truststore.jks</pre> <p>где <code>cert.pem</code> – сертификат технологического ЦС, может быть получен в результате конвертации контейнера PKCS#12 <code>opt/aeca/p12/superadmin.p12</code>:</p> <pre>openssl pkcs12 -in superadmin.p12 -out cert.pem -nodes -clcerts</pre> <p>Пароль контейнера сертификата технологического ЦС указан в файле <code>/opt/aeca/generated_passwords.txt</code></p>

Ид.	Проблема	Возможная причина	Способы решения
П007	Невозможно подключиться к токenu для выпуска сертификата после установки JC-WebClient. Сообщение «ПО JCWebClient не установлено»	Требуется разрешить ПО JC-WebClient доступ к ресурсу	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 mscs2aeca.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/FreelPA. Сообщение: «Не удалось проверить цепочку сертификатов»	Клиент вводился в домен до обновления конфигурации сертификатов домена	На клиенте выполнить команды: sudo kinit <администратор домена> sudo ipa-certupdate И повторить попытку авторизации.
П013	Периодическая остановка или падение службы аеаса.service	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 ¹ . 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.

¹ Браузер Требования к аппаратному обеспечению см. в разделе 2.2 Руководства администратора. Часть 1. Установка и обслуживание Центра сертификации Aladdin Enterprise Certification Authority.

ПРИЛОЖЕНИЕ 1. СОЗДАНИЕ СЕРТИФИКАТА ДЛЯ СУБЪЕКТА

Внимание! Создание сертификата с закрытым ключом PKCS#12 и создание сертификата на ключевом носителе возможны только для существующего субъекта локальной (см. подраздел 9.8.5 настоящего руководства) или подключенных ресурсных систем (см. подраздел 9.8.6 настоящего руководства)!

Создание сертификата субъекта по запросу, возможно как для существующего предварительно созданного локального субъекта (см. подраздел 9.8.5.1 настоящего руководства) или субъекта внешней ресурсной системы (см. подраздел 9.8.6 настоящего руководства), так и субъекта, создаваемого в процессе выпуска сертификата. При этом субъект на основании запроса будет создан только при успешном создании для него сертификата создаваемого в процессе выпуска сертификата.

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

1.1 Способы создания сертификатов

На вкладке «Сертификаты» при нажатии на кнопку <Создать сертификат> доступен выпуск сертификата (см. Рисунок 234):

- с закрытым ключом для существующего субъекта;
- на основании запроса;
- на ключевом носителе.

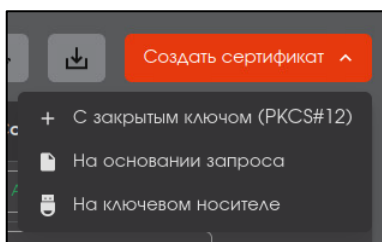


Рисунок 234 – Кнопка «Создать сертификат» на вкладке «Сертификаты»

На вкладке «Учётные записи» при выделении строки учётной записи и нажатии кнопки <Создать сертификат> доступен выпуск сертификата для учётной записи (см. Рисунок 235):

- с закрытым ключом;
- на основании запроса;
- на ключевом носителе.

Сертификат будет создан с использованием внутреннего шаблона ECA-Auth. Значение поля «Common Name» будет заполнено автоматически и соответствовать логину учетной записи, для которой выпускается сертификат.

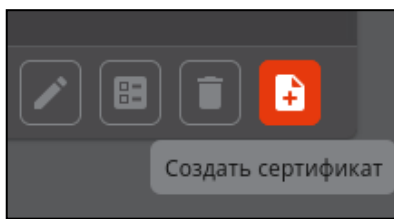


Рисунок 235 – Кнопка «Создать сертификат» на вкладке «Учётные записи»

На вкладке «Субъекты» при выделении строки субъекта и нажатии кнопки **<Создать сертификат>** доступен выпуск сертификата (см. Рисунок 236):

- с закрытым ключом;
- на основании запроса;
- на ключевом носителе.

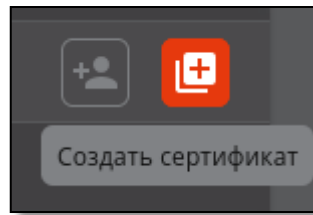


Рисунок 236 – Кнопка «Создать сертификат» на вкладке «Субъекты»

В результате нажатия на кнопку создания сертификата появится окно создания сертификата.

1.2 Параметры криптографии сертификатов учётных записей пользователей и Центров сертификации

В таблице 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 27 – 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 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, подключенного к ресурсной системе;

- сертификат создан по шаблону, в котором включена публикация сертификата в ресурсную систему (см. чек-бокс «Публиковать сертификат в ресурсную систему» в разделе **Ошибка! Источник ссылки не найден.**).

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.

Центр сертификации Aladdin eCA выполняет автоматическую публикацию сертификатов, требующих публикации при включенном флаге `ldap_automatically_certificates_publication_enable` по расписанию, заданному в параметре `ldap_automatically_certificates_publication_cron` (в конфигурационном файле `/opt/aecaCa/scripts/config.sh`). Также для выполнения публикации необходимо, чтобы владельцем сертификата являлся подключенный к ресурсной системе субъект.

При успешной публикации с сертификата снимается пометка, что он требует публикации.

Сертификат публикуется в формате LDIF в атрибут `userCertificate` (для ресурсных систем Samba DC, Альт Домен и MS AD) и `userCertificate;binary` (для ресурсных систем ALD Pro и FreeIPA) выбранного субъекта ресурсной системы, для которого выпущен сертификат, путём добавления, а не перезаписи атрибута.

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

- наличие роли «Service Role» для подключения к ресурсной системе;
- наличие роли «helpdesk» или роли «User Administrator» для публикации сертификатов пользователей;
- наличие роли «Enrollment Administrator» для публикации сертификатов контроллеров домена.

1.4 Создание сертификата с закрытым ключом PKCS#12

Внимание! Создание сертификата возможно только для существующего субъекта! Предварительно создайте локальный субъект (см. раздел 9.8.5.1 настоящего руководства) или выберите субъект внешней ресурсной системы (см. подраздел 9.8.6 настоящего руководства).

Порядок создания сертификата субъекта с закрытым ключом PKCS#12:


- В разделе «Сертификаты» после нажатия на кнопку **<Создать сертификат>** в выпадающем списке выберите функцию «На основании запроса» и в появившемся окне (см. Рисунок 237):

- при выпуске сертификата в разделе «Сертификаты» необходимо на шаге 1 ввести частичное или полное значение любого атрибута субъекта, для которого будет выпущен сертификат;

Поиск субъектов выполняется по значениям в их атрибутах и является регистронезависимым.

В результате будут отображены найденные субъекты с указанием краткой информации:

- «CN» – значение атрибута «Common Name» субъекта;
- «ID» – идентификатор субъекта;
- «UPN» – значение атрибута «MS UPN, User Principal Name» субъекта;
- «DNS» – значение атрибута «DNS Name» субъекта;

Пиктограммы наличия подключения субъекта к ресурсной системе  (см. Рисунок 237).

В результате поиска в полях «CN», «UPN» и «DNS» отображаются все значения соответствующего полю атрибута субъекта, разделитель значений в поле – запятая с пробелом.

В результате поиска поля «CN», «UPN» и «DNS» не отображаются, если в соответствующем данному полю атрибуте у субъекта отсутствуют значения.

Выберите субъект и нажмите кнопку **<Продолжить>** для перехода к шагу 1.

При выпуске сертификата в разделах «Субъекты» и «Учётные записи» шаг 1 не требуется и первым шагом будет выбор шаблона для выпуска сертификата (см. Рисунок 238).

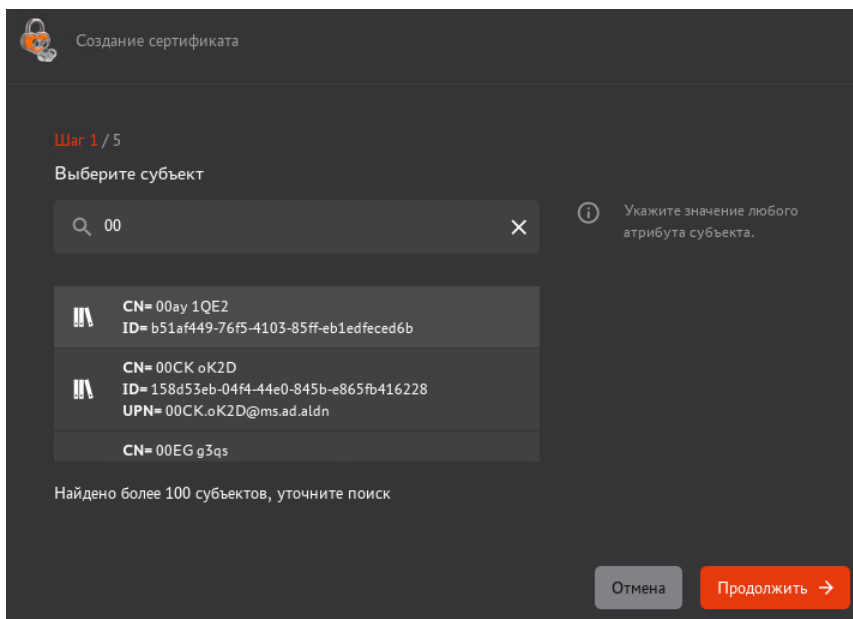


Рисунок 237 – Окно создания сертификата PKCS#12. Шаг 1. Поиск субъекта

- В открывшемся окне (см. Рисунок 238) необходимо выбрать шаблон из выпадающего списка в поле «Выберите шаблон» для выпуска сертификата. После выбора шаблона в окне отображается информация о Центре сертификации, в котором будет выпущен сертификат. Центр сертификации, в котором будет выпущен сертификат, определяется при создании шаблона (см. раздел 9.12 настоящего руководства). Если в шаблоне в качестве Центра сертификации выбрано значение «Любой», то выпуск сертификатов по данному шаблону доступен в любом Центре сертификации. При этом для выпуска сертификатов будет использован активный в данный момент Центр сертификации.

При выпуске сертификата из раздела «Учётные записи» шаблон будет определён по умолчанию и выбору не подлежит. Переход на следующий шаг осуществляется по ставшей активной кнопке **<Продолжить>** после выбора шаблона.

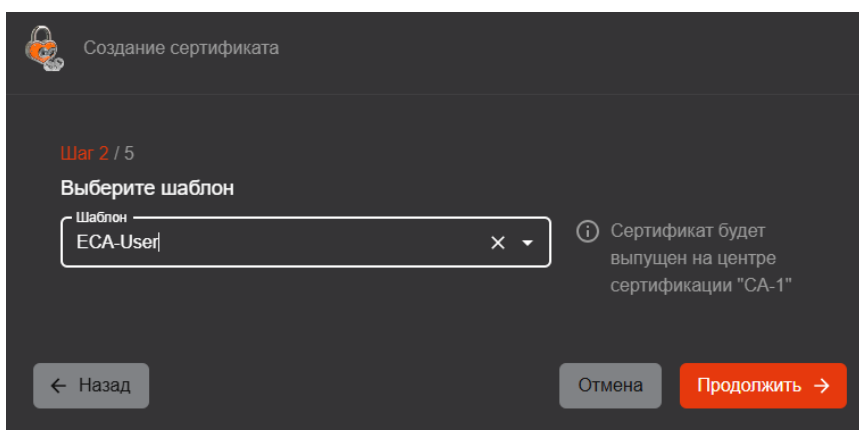




Рисунок 238 – Окно создания сертификата PKCS#12. Шаг 2. Выбор шаблона сертификата

- В окне Шага 3 указаны атрибуты в соответствии с выбранным (на предыдущем шаге) шаблоном сертификата (подробное описание полей предустановленных шаблонов см. в Приложении 2 «Описание полей предустановленных шаблонов сертификатов»). Значение атрибутов заполняется автоматически в соответствии с данными в карточке субъекта (см. раздел 9.8.4 настоящего руководства) и изменению не подлежит.

В случае если в атрибуте указано несколько значений, в выпадающем меню будет предложен выбор значения из существующих или возможно добавление значения атрибута по нажатию кнопки **<Добавить>**  справа от соответствующего поля (если атрибут содержит несколько значений, то при наведении мышки на кнопку **<Добавить>**, она становится активной – красного цвета). Также дополнительно добавленное значение атрибута можно удалить по кнопке  справа от соответствующего поля атрибута (см. Рисунок 239).

- Если данные атрибутов отсутствуют, то необходимо ввести значения в соответствующие поля в карточке субъекта (см. раздел 9.8.4 настоящего руководства).
- Необязательные поля могут оставаться незаполненными.
- Нажмите ставшую активной кнопку **<Продолжить>** для перехода к следующему шагу.

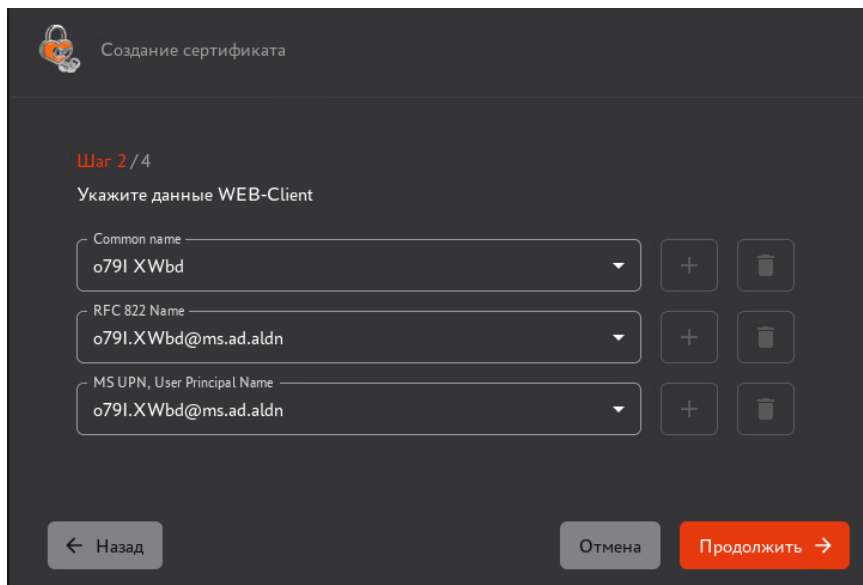


Рисунок 239 – Окно создания сертификата PKCS#12. Шаг 3. Атрибуты сертификата

- Далее необходимо создать пароль с подтверждением (см. Рисунок 240) в соответствии с правилами ввода пароля:

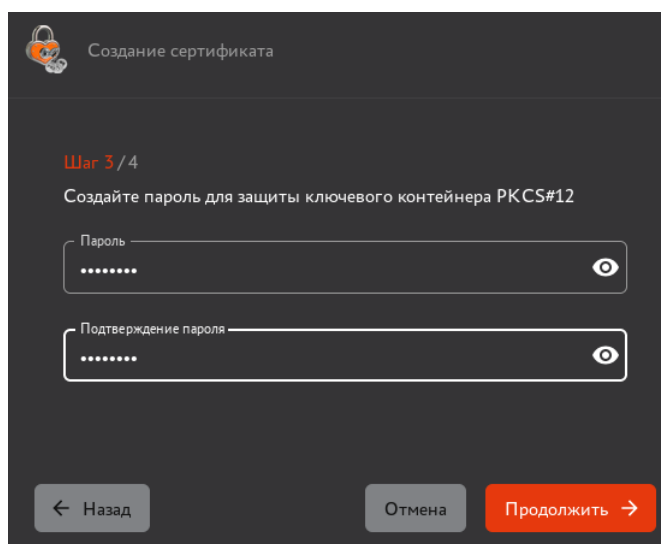



Рисунок 240 – Окно создания сертификата PKCS#12. Шаг 4. Ввод пароля контейнера

- для просмотра вводимых символов необходимо нажать кнопку  на текущей строке;
- пароль должен содержать не менее 8 символов с использованием цифр, заглавных и прописных букв, ввод осуществляется на латинице;

- если в пароле используются запрещенные символы, то рамка поля ввода приобретает красный цвет;
- если пароли не совпадают, то рамка поля подтверждения окрашивается в красный цвет.

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

- Далее необходимо выбрать параметры криптографии из выпадающего списка значений алгоритма ключа (см. Рисунок 241). По умолчанию выбрано значение «RSA–2048».

Внимание! Доступные алгоритмы определяются выбранным шаблоном (если криптопровайдер алгоритма не заявлен в шаблоне, его выбор будет недоступен), а также зависят от криптопровайдеров Центра сертификации ¹, указанного в выбранном шаблоне (если в шаблоне в качестве Центра сертификации установлено значение «любой», доступные алгоритмы будут зависеть от криптопровайдеров активного центра сертификации).

- После выбора алгоритма нажмите кнопку **<Создать сертификат>**.

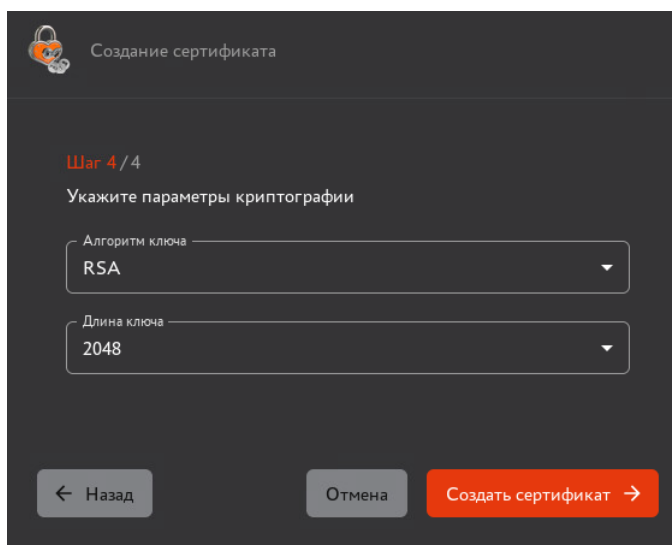


Рисунок 241 – Окно создания сертификата PKCS#12. Шаг 5. Выбор параметров криптографии

- Далее по нажатию кнопки **<Создать сертификат>** открывается финальное окно создания сертификата и отображается краткая информация о созданном сертификате (см. Рисунок 259).

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.

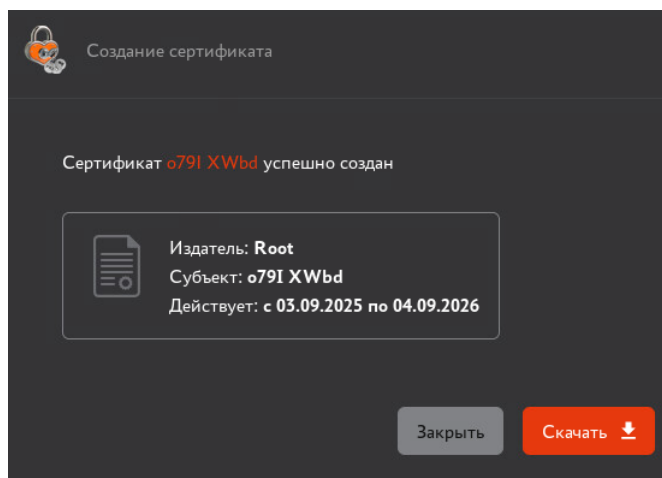


Рисунок 242 – Окно создания сертификата PKCS#12. Информирование об успешном создании сертификата

¹ Выбор криптопровайдеров осуществляется при создании центра сертификации.

В результате выпуска сертификата с закрытым ключом PKCS#12 для существующего субъекта сгенерирована ключевая пара в соответствии с заданными параметрами криптографии.

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

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

1.5 Создание сертификата субъекта по запросу

Внимание! Создание сертификата возможно как для существующего предварительно созданного локального субъекта (см. раздел 9.8.5.1 настоящего руководства) или субъекта внешней ресурсной системы (см. раздел 9.8.6 настоящего руководства), так и субъекта, создаваемого в процессе выпуска сертификата. При этом субъект на основании запроса будет создан только при успешном создании для него сертификата.

Предварительные условия выполнения сценария:

- файл-запрос для субъекта должен быть подготовлен заранее в стороннем центре сертификации (например, при помощи ПО «Единый клиент JaCarta»);
- расширение файл-запроса должно быть `.csr` или `.req`;
- файл-запрос должен быть сформирован с учетом известных данных выбранного шаблона Центра сертификации Aladdin eCA. 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 243) загрузите файл-запрос (загружается по кнопке **<Выбрать файл>**) и нажмите кнопку **<Продолжить>**.

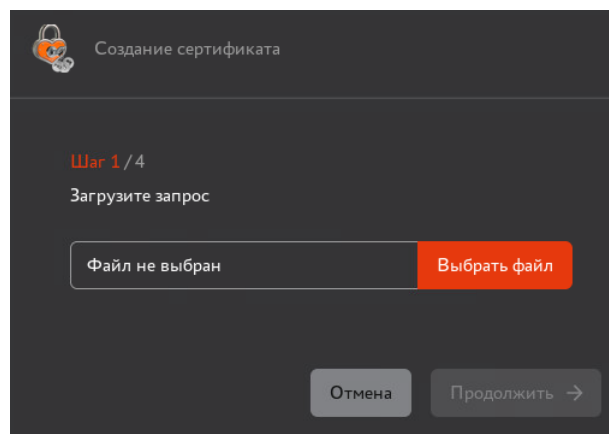


Рисунок 243 – Окно создания сертификата по запросу в разделе «Сертификаты». Шаг 1. Загрузка запроса

- 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 244):

- «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.

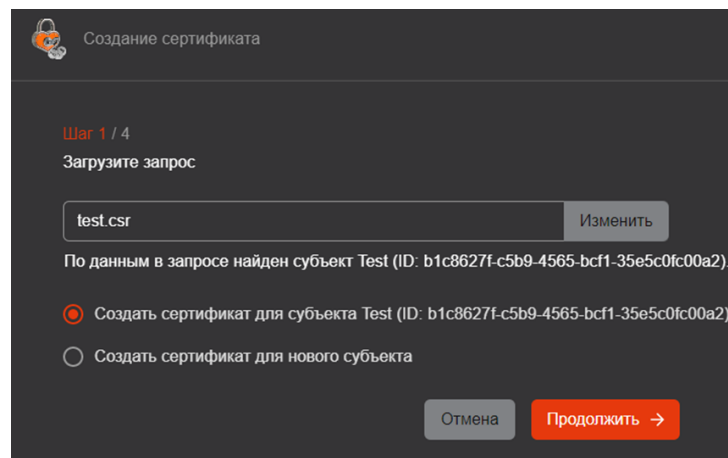


Рисунок 244 – Окно создания сертификата по запросу в разделе «Сертификаты». Шаг 1. Загрузка запроса.

- 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 245):
 - «Выбрать субъект на следующем шаге». Данная опция выбрана по умолчанию. Выберите данную опцию, чтобы на следующем шаге выбрать субъект, для которого будет создан сертификат¹;
 - «Создать сертификат для нового субъекта». Выберите данную опцию, чтобы создать сертификат для нового субъекта, который будет создан на основании данных запроса.

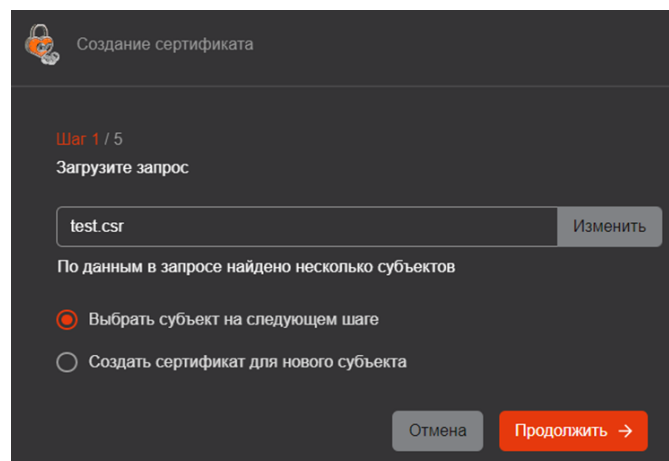


Рисунок 245 – Окно создания сертификата по запросу в разделе «Сертификаты». Шаг 1. Загрузка запроса.

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 246). Далее по сценарию сертификат будет создаваться для нового субъекта, который будет создан на основании данных запроса;

¹ 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.

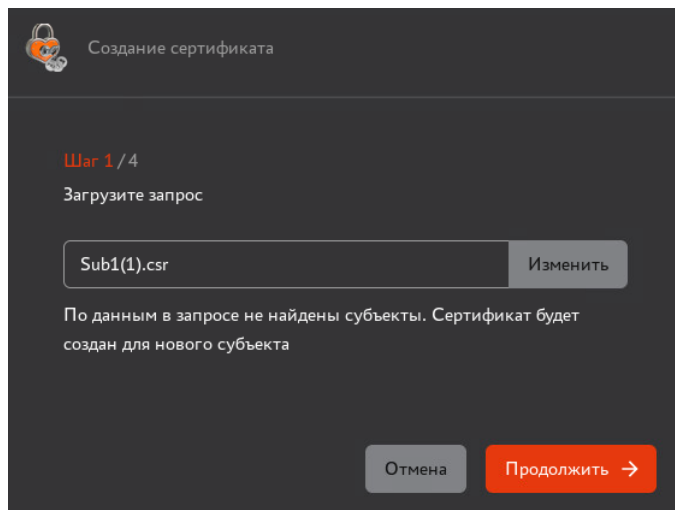


Рисунок 246 – Окно создания сертификата по запросу в разделе «Сертификаты». Шаг 1. Загрузка запроса. Не найден ни один субъект

- 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 3¹. Нажмите кнопку **<Продолжить>** для перехода к следующему шагу.
- (Шаг 2/5) В появившемся окне (см. Рисунок 247):
 - 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;

¹ 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.

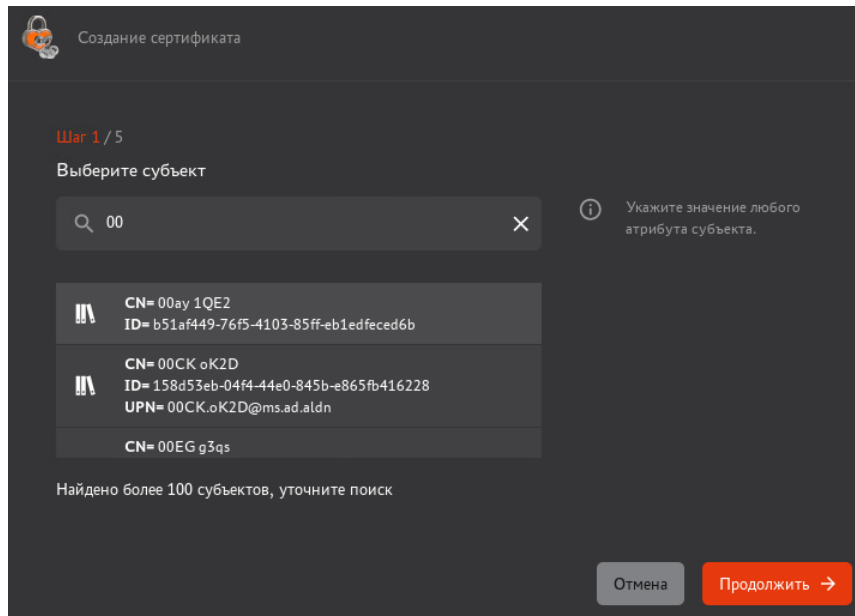


Рисунок 247 – Окно создания сертификата по запросу в разделе «Сертификаты». Шаг 2. Выбор субъекта

- (Шаг 2/4 или 3/5) В появившемся окне (см. Рисунок 248) выберите шаблон, на основании которого будет создан сертификат (предполагается, что администратор заранее знает какой шаблон необходимо выбрать). После выбора шаблона в окне отображается информация о Центре сертификации, в котором будет выпущен сертификат. Центр сертификации, в котором будет выпущен сертификат, определяется при создании шаблона (см. раздел 7.12 настоящего руководства). Если в шаблоне в качестве Центра сертификации выбрано значение «Любой», то выпуск сертификатов по данному шаблону доступен в любом Центре сертификации. При этом для выпуска сертификатов будет использован активный в данный момент Центр сертификации.

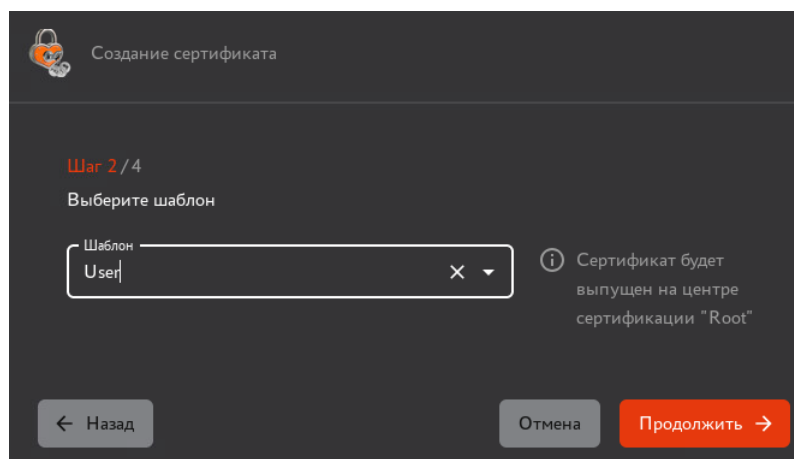


Рисунок 248 – Окно создания сертификата по запросу в разделе «Сертификаты». Шаг 3. Выбор шаблона

- 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 28. Проверка является регистронезависимой. При этом в случае, если в процессе выпуска сертификата по запросу создается новый субъект, то валидация значений из полей запроса на соответствие атрибутам субъекта не 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 249 и Рисунок 250).

Перечень возможных ошибок представлен в таблице 29.

Таблица 28 – Соответствие полей запроса шаблону выпускаемого сертификата

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

Поле в шаблоне	Значение поля в запросе	Атрибут субъекта	Возможность создания сертификата	Поле в сертификате	Возможные ошибки*
Есть, обязательное	Нет	Есть	Да	Присутствует	Ошибка №1 Исправление указанной ошибки доступно на этапе переопределения SAN (путем выбора значения для поля из атрибута субъекта).
Есть, необязательное	Есть	Нет	Да	Отсутствует	1) Ошибка №2, если значение в запросе не проходит валидацию по шаблону 2) Ошибка №4
Есть, необязательное	Нет	Нет	Да	Отсутствует	–
Есть, необязательное	Есть	Есть	Да	Присутствует, если поле не было удалено на этапе переопределения значений для полей SAN, указанных в шаблоне или отсутствует, если поле было удалено на этапе переопределения значений для полей SAN, указанных в шаблоне	1) Ошибка №2, если значение в запросе не проходит валидацию по шаблону 2) Ошибка 4, если значение в запросе не соответствует значению атрибута
Есть, необязательное	Нет	Есть	Да	Присутствует, если поле не было удалено на этапе переопределения значений для полей SAN, указанных в шаблоне или отсутствует, если поле было удалено на этапе переопределения значений для полей SAN, указанных в шаблоне	–
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 29 – Перечень возможных ошибок обработки запроса

Ошибка	Сообщение
Ошибка №1	«Отсутствует обязательное поле» ¹
Ошибка №2	«Значение в поле не соответствует регулярному выражению: \»%s\», где \»%s\» ²
Ошибка №3	«Поле отсутствует в шаблоне»
Ошибка №4	«Значение в поле не соответствует значению атрибута субъекта»

Если создание сертификата невозможно, то существует две возможности:

- вернуться на предыдущий шаг и сменить шаблон на подходящий;
- пересоздать файл–запрос с учетом выявленных при сверке ошибок и перезагрузить файл–запрос, вернувшись на предыдущие шаги по нажатию кнопки **<Назад>**.

¹ Описание полей предустановленных шаблонов см. в Приложении 2 «Описание полей предустановленных шаблонов сертификатов».

² Правила валидации значений полей предустановленных шаблонов см. в Приложении 3 «Правила валидации значений полей по умолчанию предустановленных шаблонов сертификатов».

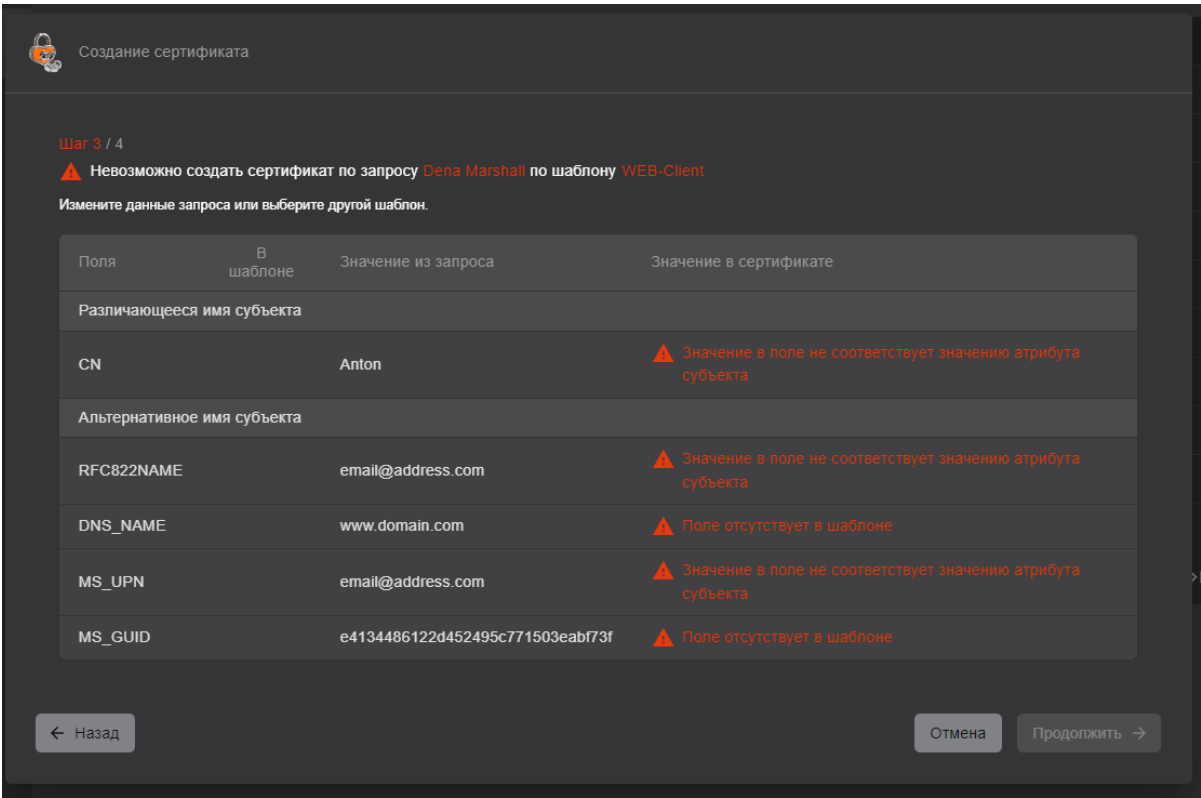


Рисунок 249 – Окно создания сертификата по запросу в разделе «Сертификаты». Шаг 4. Результат обработки запроса с ошибкой в поле различающегося имени субъекта

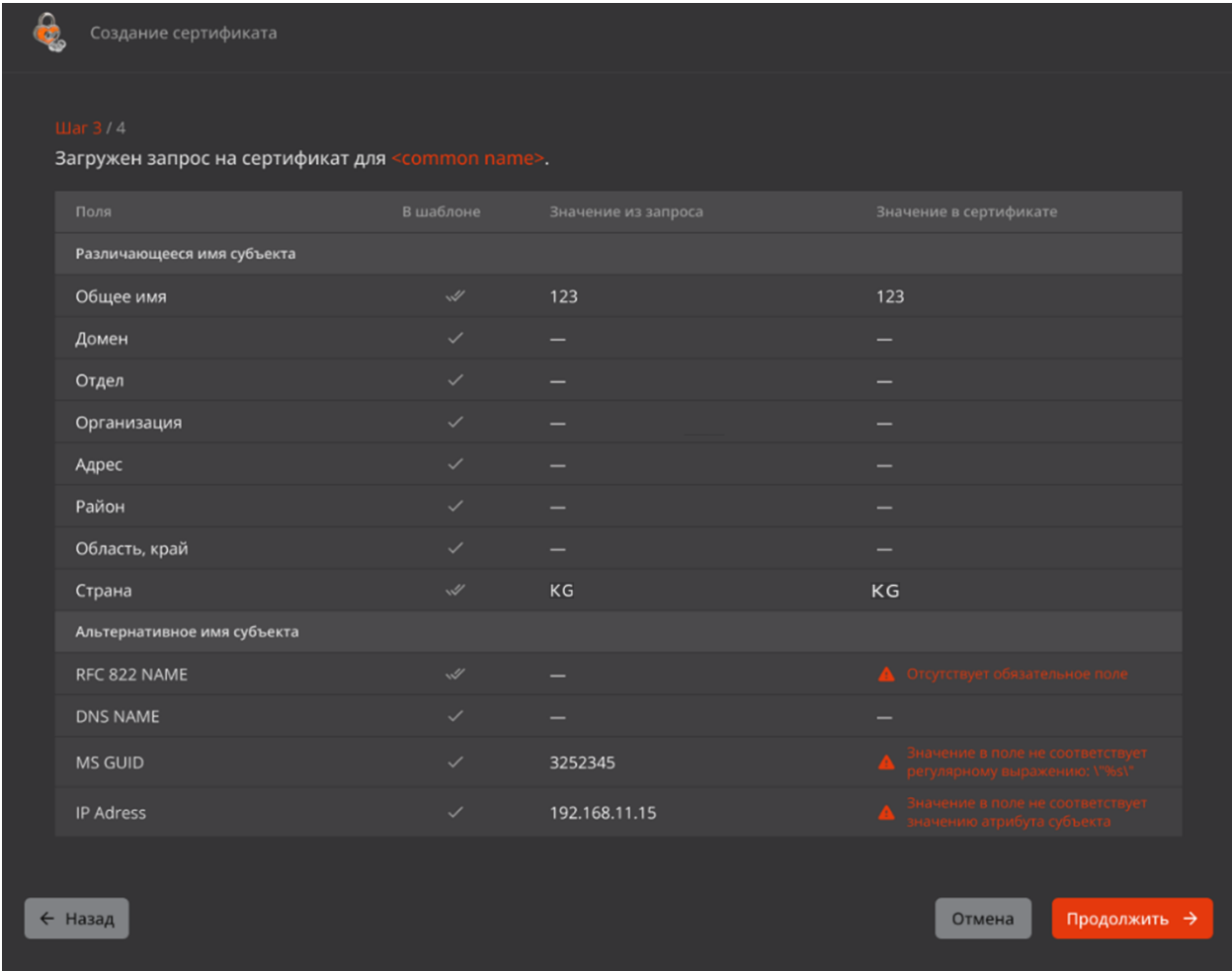


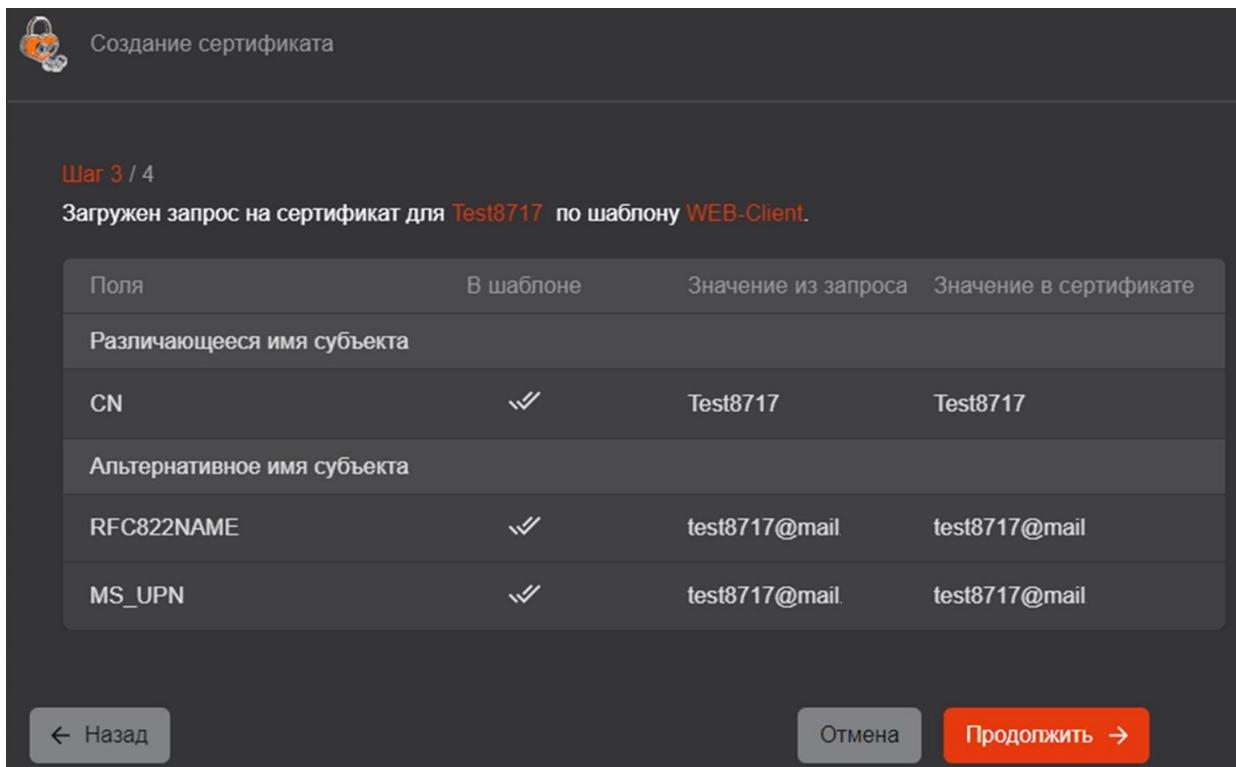


Рисунок 250 – Окно создания сертификата по запросу в разделе «Сертификаты». Шаг 4. Результат обработки запроса с ошибками в полях альтернативного имени субъекта

В результате успешной обработки запроса на сертификат субъекта на следующем шаге отображается (см. Рисунок 251):

- 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 реализации¹, 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		Test8717	Test8717
Альтернативное имя субъекта			
RFC822NAME		test8717@mail	test8717@mail
MS_UPN		test8717@mail	test8717@mail


← Назад Отмена Продолжить →

Рисунок 251 – 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.


¹ 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 сертификата¹. Значение атрибутов заполняется автоматически в соответствии с данными в карточке субъекта² 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 252).

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.

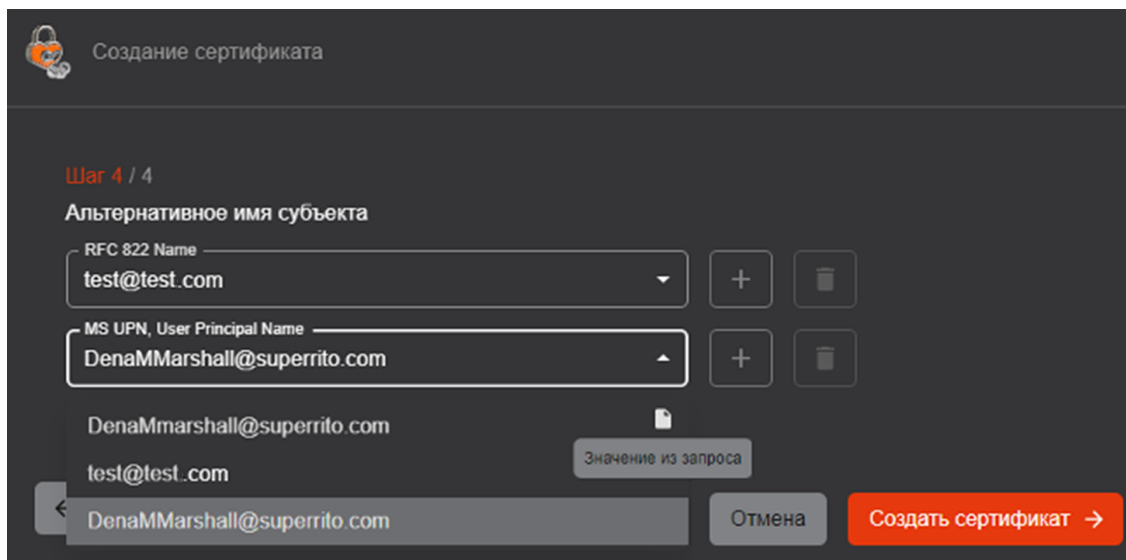


Рисунок 252 – Окно создания сертификата по запросу в разделе «Сертификаты». Шаг 5. Атрибуты сертификата

- Далее по нажатию кнопки **<Создать сертификат>** открывается финальное окно создания сертификата и отображается краткая информация о созданном сертификате (см. Рисунок 253). 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.

¹ Подробное описание полей предустановленных шаблонов см. в Приложении 2 «Описание полей предустановленных шаблонов сертификатов».

² Подробнее см. раздел 9.8.4 настоящего руководства.

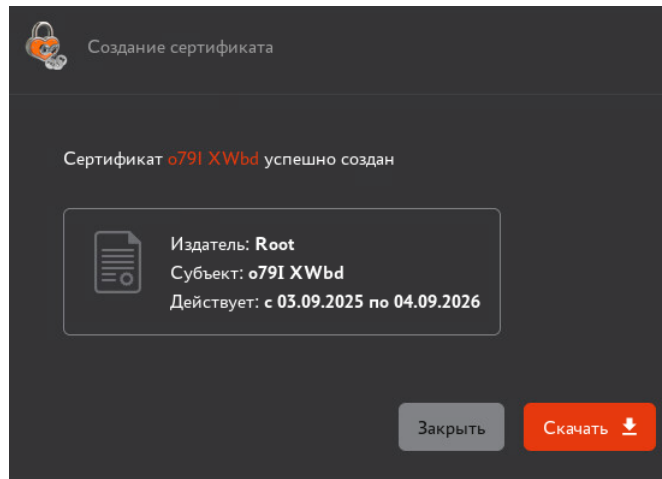


Рисунок 253 – Окно создания сертификата по запросу в разделе «Сертификаты».

Результат успешного создания сертификата

- При успешном создании сертификата и выполнении всех условий ниже происходит его публикация в ресурсную систему:
 - сертификат был создан для субъекта, подключенного 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 9.12 настоящего руководства). Если в шаблоне в качестве Центра сертификации выбрано значение «Любой», то выпуск сертификатов по данному шаблону доступен в любом Центре сертификации. При этом для выпуска сертификатов будет использован активный в данный момент Центр сертификации. По файлу запроса возможен только одноразовый выпуск сертификата.

При необходимости, возможно перезагрузить файл–запрос в мастере создания сертификата без сброса текущего прогресса по кнопке **<Изменить>**.

После загрузки файла запроса и выбора шаблона нажмите активировавшуюся кнопку **<Продолжить>**.

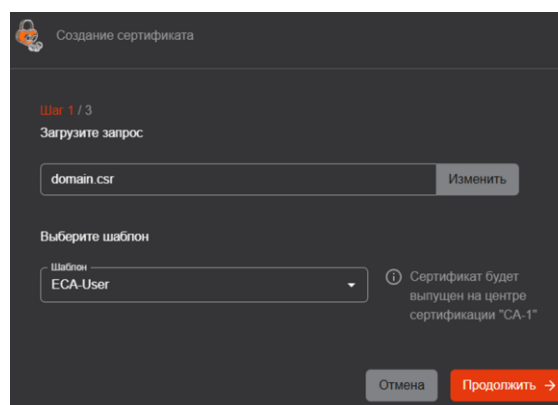


Рисунок 254 – Окно создания сертификата по запросу в разделе «Субъекты». Шаг 1.

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 255 и Рисунок 256).

Перечень возможных ошибок представлен в таблице 29.

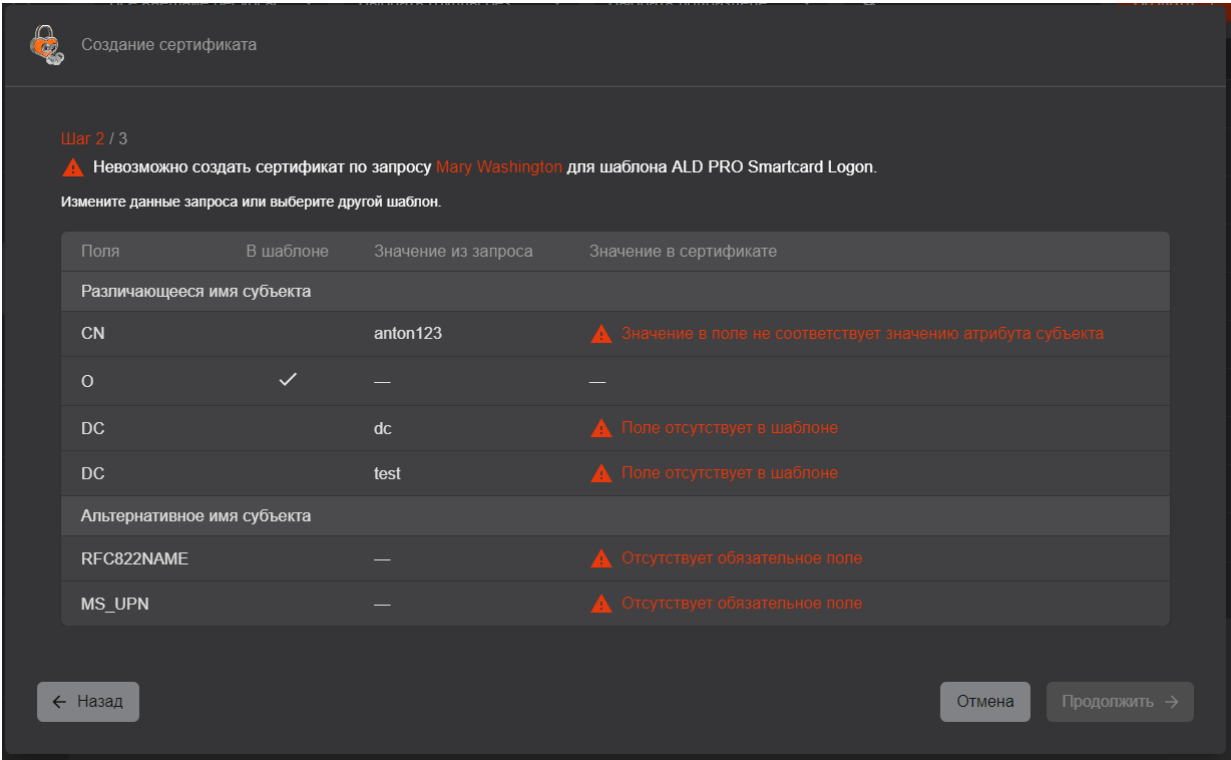


Рисунок 255 – Окно создания сертификата по запросу в разделе «Субъекты». Шаг 2. Результат обработки запроса с ошибкой в поле различающегося имени субъекта

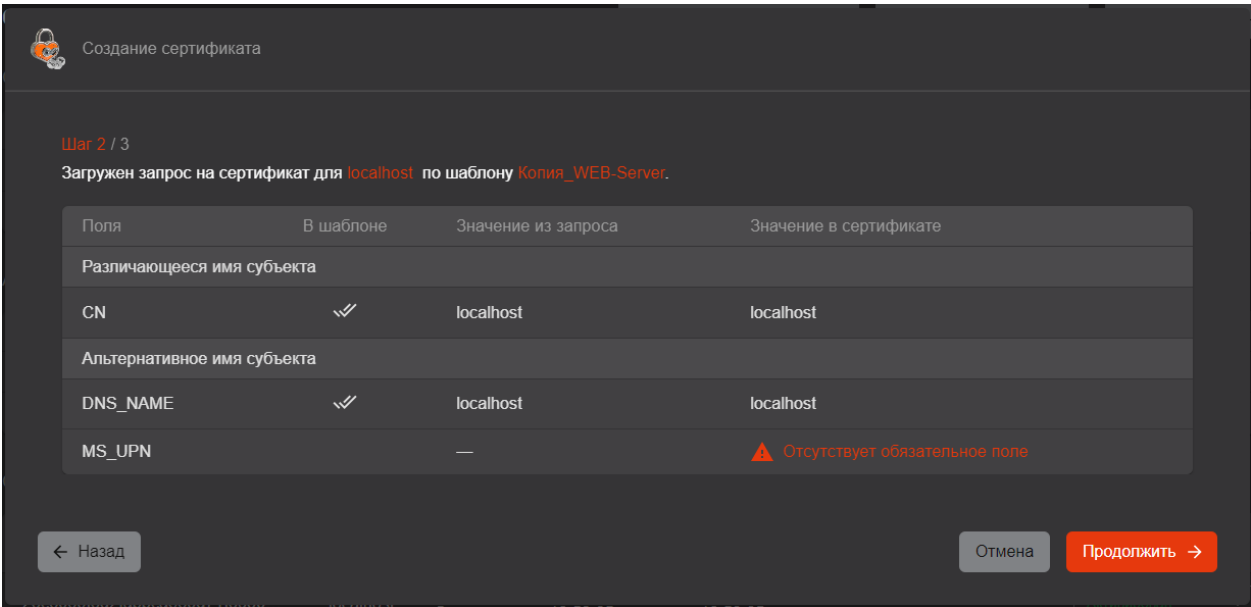


Рисунок 256 – Окно создания сертификата по запросу в разделе «Субъекты». Шаг 2. Результат обработки запроса с ошибками в полях альтернативного имени субъекта

Если создание сертификата невозможно, то существует две возможности:

- вернуться на предыдущий шаг и сменить шаблон на подходящий;

- пересоздать файл–запрос с учетом выявленных при сверке ошибок и перезагрузить файл–запрос, вернувшись на предыдущие шаги по нажатию кнопки **<Назад>**.
- В результате успешной обработки запроса на сертификат субъекта на следующем шаге отображается (см. Рисунок 257):
 - 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 реализации¹, то они идентифицируются по параметру OID.

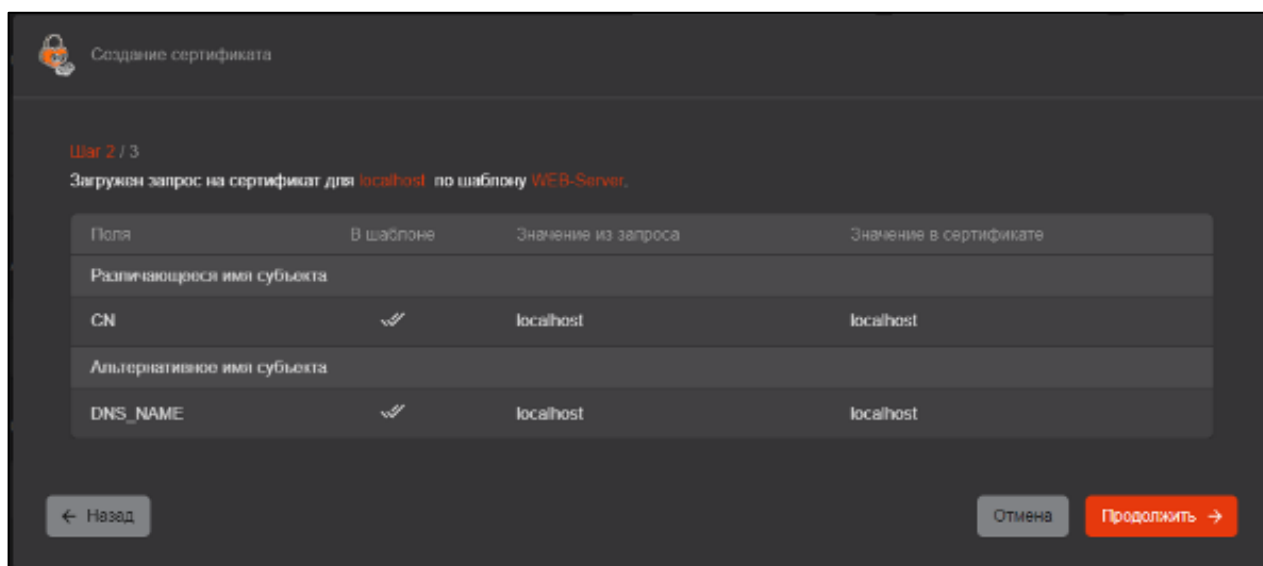





Рисунок 257 – Окно создания сертификата по запросу в разделе «Субъекты». Шаг 2. Результат успешной обработки запроса

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.

¹ 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 9.8.4 настоящего руководства) и изменению не подлежит. В случае если в атрибуте указано несколько значений, в выпадающем меню будет предложен выбор значения из существующих или возможно добавление значения атрибута по нажатию кнопки **<Добавить>**  справа от соответствующего поля (если атрибут содержит несколько значений, то при наведении мышки на кнопку **<Добавить>**, она становится активной – красного цвета). Также дополнительно добавленное значение атрибута можно удалить по кнопке  справа от соответствующего поля атрибута (см. Рисунок 258).

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.

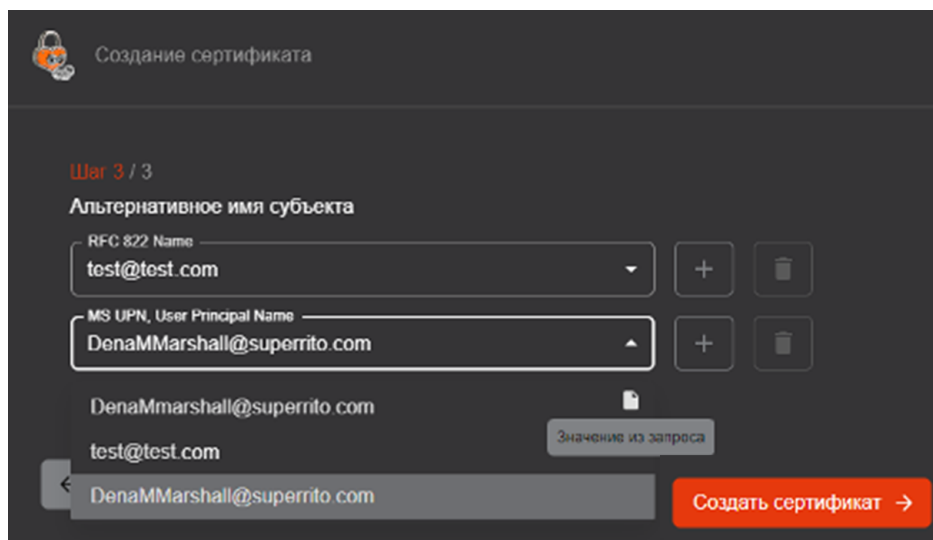


Рисунок 258 – Окно создания сертификата по запросу в разделе «Субъекты». Шаг 4. Атрибуты сертификата

- Далее по нажатию кнопки **<Создать сертификат>** открывается финальное окно создания сертификата и отображается краткая информация о созданном сертификате (см. Рисунок 259). 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.

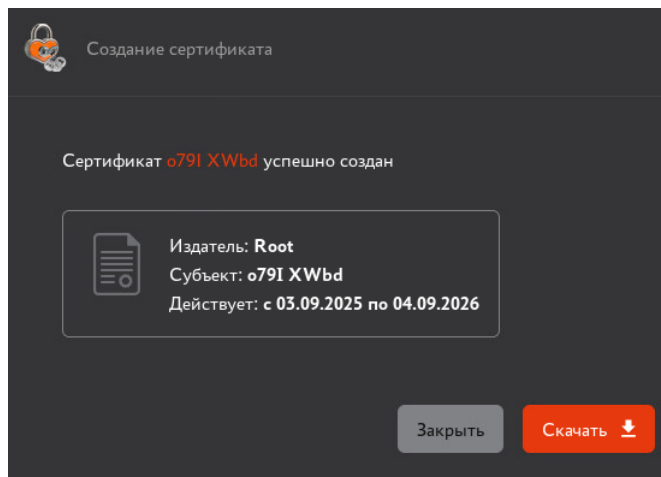


Рисунок 259 – Окно создания сертификата по запросу в разделе «Субъекты». Шаг 4. Информирование об успешном создании сертификата

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

- сертификат был создан для субъекта, подключенного 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 9.8.5.1 настоящего руководства) или выберите субъект внешней ресурсной системы (см. раздел 9.8.6 настоящего руководства).

Центр сертификации Aladdin eCA поддерживает следующие виды ключевых носителей для создания сертификата:

- JaCarta:
 - JaCarta PKI.
 - JaCarta PRO.
 - JaCarta-2 PKI/ГОСТ.
 - JaCarta-2 ГОСТ.
 - JaCarta-3.
- Рутокен¹:
 - 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 приведен 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.

¹ 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 Центра регистрации Aladdin eRA, 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 260):

- «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 261).

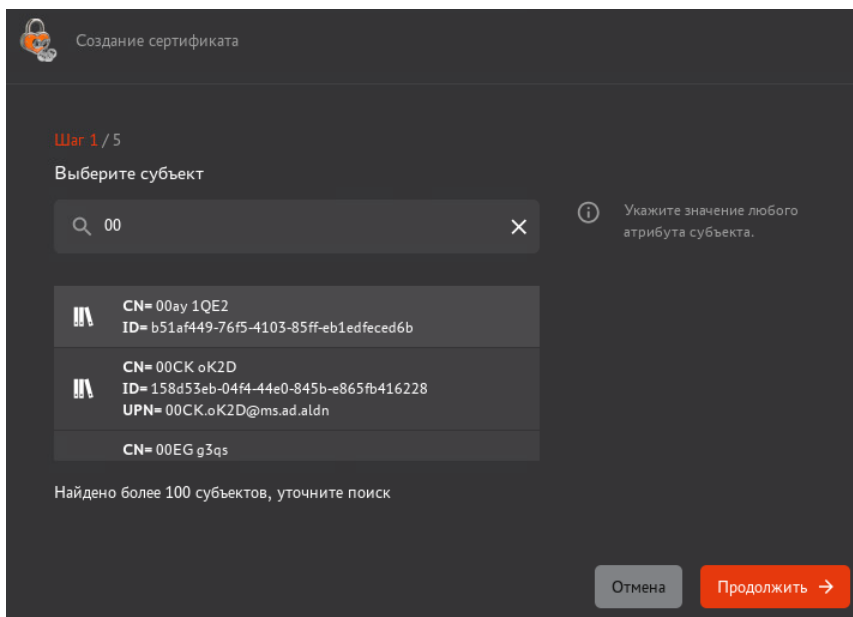


Рисунок 260 – Окно создания сертификата на электронном ключе в разделе «Сертификаты». Шаг 1

- В открывшемся окне (см. Рисунок 261) 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 9.12 настоящего руководства). Если в шаблоне в качестве Центра сертификации выбрано значение «Любой», то выпуск сертификатов по данному шаблону доступен в любом Центре сертификации. При этом для выпуска сертификатов будет использован активный в данный момент Центр сертификации. Переход на следующий шаг осуществляется по ставшей активной кнопке **<Продолжить>** в случае ввода корректного PIN-кода электронного ключа и заполнении всех полей.

Рисунок 261 – 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 9.8.4 настоящего руководства) и изменению не подлежит. В случае если в атрибуте указано несколько значений, в выпадающем меню будет предложен выбор значения из существующих или возможно добавление значения атрибута по нажатию кнопки **<Добавить>**  справа от соответствующего поля (если атрибут содержит несколько значений, то при наведении мышки на кнопку **<Добавить>**, она становится активной – красного цвета). Также дополнительно добавленное значение атрибута можно удалить по кнопке  справа от соответствующего поля атрибута (см. Рисунок 262). Необязательные поля могут оставаться незаполненными.

Рисунок 262 – 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 262).

- Далее необходимо выбрать параметры криптографии (см. Рисунок 263):
 - 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>**.

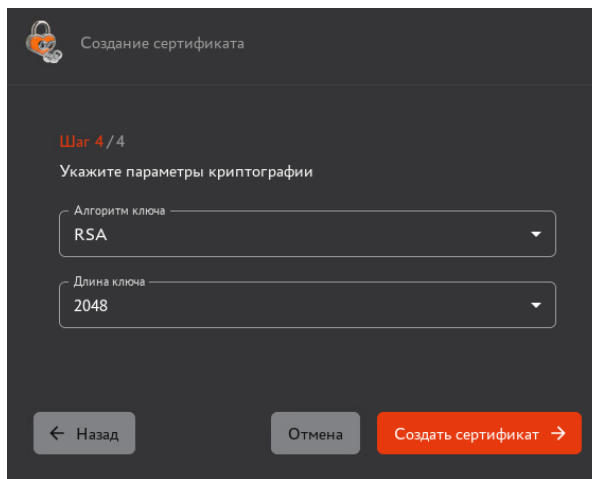


Рисунок 263 – Окно создания сертификата на электронном ключе. Шаг 4

- 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>**.

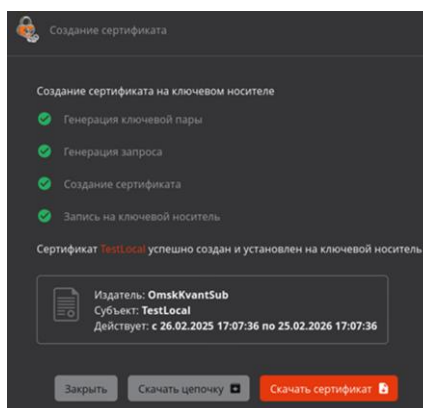


Рисунок 264 – Окно успешного создания сертификата субъекта на электронном ключе

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

- сертификат был создан для субъекта, подключенного 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 265). Для выпуска сертификата на электронном ключе установите ПО JC–WebClient или «Рутокен Плагин».

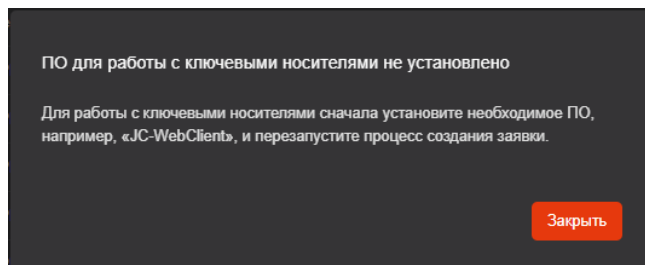


Рисунок 265 – ПО для работы с ключевыми носителями не установлено

- В случае, если электронный носитель не подключен, то администратор будет уведомлен об этом информационным сообщением (см. Рисунок 266). Для выпуска сертификата подключите электронный ключ и перезапустите мастер создания сертификата.

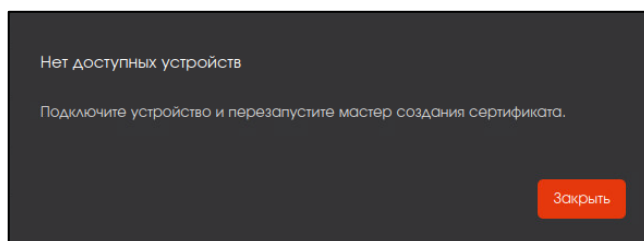


Рисунок 266 – Окно информационного сообщения «Нет доступных устройств»

- В случае, если выбранный для выпуска сертификата алгоритм не поддерживается выбранной моделью ключевого носителя, администратор будет уведомлён об этом информационным сообщением.

ПРИЛОЖЕНИЕ 2. ОПИСАНИЕ ПОЛЕЙ ПРЕДУСТАНОВЛЕННЫХ ШАБЛОНОВ СЕРТИФИКАТОВ

Примечания:

- Для всех предустановленных шаблонов запись в сертификат SID субъекта (при наличие данного атрибута у субъекта) отключена.
- Для всех предустановленных шаблонов автоматическая публикация сертификатов в ресурсную систему после их выпуска отключена.
- Для всех предустановленных шаблонов контроль соответствия значений отличительного и альтернативного имен значениям аналогичных атрибутов у субъекта при выпуске сертификата включен.

Имя шаблона	Идентификатор	Период действия сертификата	Шифрование		Использование ключа		Расширенное использование ключа		Компоненты имени сертификата					
			Алгоритм	Минимальная длина ключа	Значения	Крит.	Значения	Крит.	Отличительное имя субъекта			Альтернативное имя субъекта		
									Поле	Обязат.	Валидац.	Поле	Обязат.	Валидац.
[Deprecated] ECA – Auth	8ecba810–7f48–4c4e–b803–99a97146e2ba	2y	RSA	1024	– Цифровая подпись – Подтверждение подлинности – Шифрование ключей	+	– Аутентификация клиента – Защита электронной почты	–	Common name	+	+	–		
			ECDSA	256										
			ГОСТ Р 34.10–2012	Выключен										
[Deprecated] ECA – User	2d58b30c-3965-4555-9af4-fec4552af21e	2y	RSA	1024	– Цифровая подпись – Подтверждение подлинности – Шифрование ключей	+	– Аутентификация клиент – Защита электронной почты	–	Common name	+	+	–		
			ECDSA	256										
			ГОСТ Р 34.10–2012	256										
[Deprecated] ECA – WEB – Server	25bbd733-4d8c-43ce-ba5a-e9826eb7b16c	2y	RSA	1024	– Цифровая подпись – Шифрование ключей	+	– Аутентификация сервера	–	Common name	+	+	DNS name	+	+
			ECDSA	256										
			ГОСТ Р 34.10–2012	256										
[Deprecated] Domain Controller	bf2dac0a–f05f–49dd–95b4–e50691489b6a	2y	RSA	1024	– Цифровая подпись – Подтверждение подлинности – Шифрование ключей	+	– Аутентификация клиента – Центр распространения ключей Kerberos – SSH сервер	–	Common name ¹	+	+	DNS name ²	+	+
			ECDSA	256								MS GUID ³	+	+
			ГОСТ Р 34.10–2012	Выключен										

¹ Имя контроллера домена.

² FQDN – полное доменное имя вашего сервера.

³ Глобальный уникальный идентификатор контроллера домена, данные должны быть получены из контроллера домена. Для получения значения идентификатора в среде РЕД ОС и SberLinux OS Server выполните команду: `samba-tool computer show <hostname> | grep objectGUID`. Для получения значения идентификатора в среде Astra Linux Special Edition выполните команду: `ipa host-show <hostname> --all | grep ipauniqueid`, где `hostname` – короткое имя контроллера домена.

Имя шаблона	Идентификатор	Период действия сертификата	Шифрование		Использование ключа		Расширенное использование ключа		Компоненты имени сертификата					
			Алгоритм	Минимальная длина ключа	Значения	Крит.	Значения	Крит.	Отличительное имя субъекта			Альтернативное имя субъекта		
									Поле	Обязат.	Валидац.	Поле	Обязат.	Валидац.
[Deprecated] Smartcard Logon	aa03e458-50cd-46b8-82cd-d5612ed3b647	2y	RSA	1024	– Цифровая подпись – Подтверждение подлинности – Шифрование ключей – Шифрование данных	+	– Аутентификация клиента – Защита электронной почты – Вход с MS смарт-картой	–	Common name ¹	+	+	MS UPN ²	+	+
			ECDSA	256								RFC 822 Name ³	+	+
			ГОСТ Р 34.10-2012	Выключен										
[Deprecated] WEB-Client	059a38f5-f345-4275-b79f-e7e6cc3cbb68	2y	RSA	1024	– Цифровая подпись – Подтверждение подлинности – Шифрование ключей	+	– Аутентификация клиента – Защита электронной почты	–	Common name ⁴	+	+	MS UPN ⁵	+	+
			ECDSA	256								RFC 822 Name ⁶	+	+
			ГОСТ Р 34.10-2012	Выключен										
[Deprecated] WEB-Server	08c66f99-218a-46ef-bdee-6a2b3b26a4f1	2y	RSA	1024	– Цифровая подпись – Шифрование ключей	+	Аутентификация сервера	–	Common name ⁷	+	+	DNS name ⁸	+	+
			ECDSA	256										
			ГОСТ Р 34.10-2012	Выключен										
[Deprecated] S/MIME	0c234243-18cf-4c05-b699-537731b2436f	2y	RSA	1024	– Цифровая подпись – Подтверждение подлинности – Шифрование ключей – Шифрование данных	+	– Аутентификация клиента – Защита электронной почты – Вход с MS смарт-картой	–	Common name ⁹	+	+	RFC 822 Name ¹⁰	+	+
			ECDSA	256										
			ГОСТ Р 34.10-2012	Выключен										

¹ Имя пользователя.

² Имя входа пользователя в формате e-mail адреса.

³ Почтовый адрес пользователя, может совпадать с MS UPN.

⁴ Имя веб-клиента.

⁵ Имя входа пользователя в формате e-mail адреса.

⁶ Почтовый адрес пользователя, может совпадать с MS UPN.

⁷ Имя веб-сервера.

⁸ FQDN – полное доменное имя вашего сервера.

⁹ Имя пользователя.

¹⁰ почтовый адрес пользователя, может совпадать с MS UPN.

Имя шаблона	Идентификатор	Период действия сертификата	Шифрование		Использование ключа		Расширенное использование ключа		Компоненты имени сертификата					
			Алгоритм	Минимальная длина ключа	Значения	Крит.	Значения	Крит.	Отличительное имя субъекта			Альтернативное имя субъекта		
									Поле	Обязат.	Валидац.	Поле	Обязат.	Валидац.
[Deprecated] ALD PRO Domain Controller	11ec34a4-d03e-4059-92f0-9c09b08bffa	2y	RSA	1024	– Цифровая подпись – Подтверждение подлинности – Шифрование ключей – Шифрование данных	+	– Центр распространения ключей Kerberos – Аутентификация сервера	–	Common name ¹	+	+	MS UPN ²	+	+
			ECDSA	256					Organization ³	–	+	Kerberos KPN ⁴	+	+
			ГОСТ Р 34.10-2012	Выключен										
[Deprecated] ALD PRO Smartcard Logon	18d9bd4e-6f15-423f-8137-ac8416ad6874	2y	RSA	1024	– Цифровая подпись – Подтверждение подлинности – Шифрование ключей – Шифрование данных	+	– Аутентификация клиента – Центр распространения ключей Kerberos – Аутентификация сервера	–	Common name ⁵	+	+	MS UPN ⁶	+	+
			ECDSA	256					Organization ⁷	–	+	RFC 822 Name ⁸	+	+
			ГОСТ Р 34.10-2012	Выключен										
[Deprecated] OCSP Signer	aac2e49b-9c8e-4869-80c1-eef526ba75ab	2y	RSA	1024	Цифровая подпись	+	OCSP подписант	–	Common name	+	+	–		
			ECDSA	256										
			ГОСТ Р 34.10-2012	Выключен										
[Deprecated] Root CA	9129245a-eaad-4ebc-a2a4-8845ac0336fb	7d24y	RSA	1024	– Цифровая подпись – Подпись сертификата – Подпись списка отзыва	+	– Любое расширенное использование ключа – Аутентификация клиента – Аутентификация сервера	–	Common name	+	+	RFC 822 Name	–	+
			ECDSA	256					Unique Identifier (UID)	–	+	DNS name	–	+
			ГОСТ Р 34.10-2012	256					Given name	–	+	MS UPN	–	+
									Initials	–	+	MS GUID	–	+

¹ Имя контроллера домена ALD PRO.
² Данные в формате «krbtgt/полное имя домена@полное имя домена».
³ Организация.
⁴ Данные в формате «krbtgt/полное имя домена@полное имя домена».
⁵ Имя пользователя ALD PRO.
⁶ Имя входа пользователя в формате e-mail адреса.
⁷ Организация.
⁸ Почтовый адрес пользователя, может совпадать с MS UPN.

Имя шаблона	Идентификатор	Период действия сертификата	Шифрование		Использование ключа		Расширенное использование ключа		Компоненты имени сертификата					
			Алгоритм	Минимальная длина ключа	Значения	Крит.	Значения	Крит.	Отличительное имя субъекта			Альтернативное имя субъекта		
									Поле	Обязат.	Валидац.	Поле	Обязат.	Валидац.
									Surname	-	+	IP address	-	+
									Organizational unit	-	+	Directory Name	-	+
									Locality	-	+	Uniform resource identifier	-	+
									State or province	-	+	Registered Identifier (OID)	-	+
									Domain component	-	+	Permanent identifier	-	+
									Country	-	+	Xmpp address	-	+
									Postal code	-	+	Service Name	-	+
									Business category	-	+	Subject Identification Method	-	+
									Telephone number	-	+	Kerberos KPN	-	+
									Pseudonym	-	+			
									Postal address	-	+			
									Street	-	+			
									Name	-	+			
									Title	-	+			
									Domain qualifier	-	+			
									Description	-	+			
									Unstructured address	-	+			
									Unstructured name	-	+			
									Email Address (E)	-	+			
									Serial number	-	+			
									Organization	-	+			
									ИНН	-	+			
									ОГРН	-	+			
									ОГРНИП	-	+			
									СНИЛС	-	+			
									ИНН юл	-	+			

Имя шаблона	Идентификатор	Период действия сертификата	Шифрование		Использование ключа		Расширенное использование ключа		Компоненты имени сертификата					
			Алгоритм	Минимальная длина ключа	Значения	Крит.	Значения	Крит.	Отличительное имя субъекта			Альтернативное имя субъекта		
									Поле	Обязат.	Валидац.	Поле	Обязат.	Валидац.
[Deprecated] Sub CA	af3b0355-1798-4c64-98f7-a9c70407db1c	7d24y	RSA	1024	– Цифровая подпись – Подпись сертификата – Подпись списка отзыва	+	– Любое расширенное использование ключа – Аутентификация клиента – Аутентификация сервера	-	Common name	+	+	RFC 822 Name	-	+
									Unique Identifier (UID)	-	+	DNS name	-	+
			ECDSA	256					Given name	-	+	MS UPN	-	+
									Initials	-	+	MS GUID	-	+
									Surname	-	+	IP address	-	+
									Organizational unit	-	+	Directory Name	-	+
									Locality	-	+	Uniform resource identifier	-	+
									State or province	-	+	Registered Identifier (OID)	-	+
									Domain component	-	+	Permanent identifier	-	+
									Country	-	+	Xmpp address	-	+
									Postal code	-	+	Service Name	-	+
									Business category	-	+	Subject Identification Method	-	+
									Telephone number	-	+	Kerberos KPN	-	+
									Pseudonym	-	+			
									Postal address	-	+			
									Street	-	+			
									Name	-	+			
									Title	-	+			
									Domain qualifier	-	+			
									Description	-	+			
									Unstructured address	-	+			
									Unstructured name	-	+			
									Email Address (E)	-	+			
									Serial number	-	+			
									Organization	-	+			
									ИНН	-	+			
									ОГРН	-	+			

Имя шаблона	Идентификатор	Период действия сертификата	Шифрование		Использование ключа		Расширенное использование ключа		Компоненты имени сертификата					
			Алгоритм	Минимальная длина ключа	Значения	Крит.	Значения	Крит.	Отличительное имя субъекта			Альтернативное имя субъекта		
									ОГРНИП	–	+			
									СНИЛС	–	+			
									ИНН ЮЛ	–	+			
[Deprecated] SCEP Management	3e5df3d4–683c–4252–b862–467589c2225b	25y	RSA	1024	– Цифровая подпись – Шифрование ключей – Шифрование данных	+	–	–	Common name	+	–	–		
			ECDSA	256										
			ГОСТ P 34.10–2012	256										
User	f215f72f-9a9a-45c8-83e8-25879d52dcf6	1y	RSA	2048	– Цифровая подпись – Подтверждение подлинности – Шифрование ключей	+	– Аутентификация клиент – Защита электронной почты	–	Common name	+	+	–		
			ECDSA	256										
			ГОСТ P 34.10–2012	256										
Domain Controller	eca2ad3d-944e-48ce-ba7b-114f16ad8fd4	1y	RSA	2048	– Цифровая подпись – Подтверждение подлинности – Шифрование ключей	+	– Аутентификация клиента – Центр распространения ключей Kerberos – SSH сервер	–	Common name ¹	+	+	DNS name ²	+	+
			ECDSA	256								MS GUID ³	+	+
			ГОСТ P 34.10–2012	256										

¹ Имя контроллера домена.

² FQDN –полное доменное имя вашего сервера.

³ Глобальный уникальный идентификатор контроллера домена, данные должны быть получены из контроллера домена. Для получения значения идентификатора в среде РЕД ОС и SberLinux OS Server выполните команду: `samba-tool computer show <hostname> | grep objectGUID`. Для получения значения идентификатора в среде Astra Linux Special Edition выполните команду: `ipa host-show <hostname> --all | grep ipauniqueid`, где `hostname` – короткое имя контроллера домена.

Имя шаблона	Идентификатор	Период действия сертификата	Шифрование		Использование ключа		Расширенное использование ключа		Компоненты имени сертификата					
			Алгоритм	Минимальная длина ключа	Значения	Крит.	Значения	Крит.	Отличительное имя субъекта			Альтернативное имя субъекта		
Smartcard Logon	682225f6-f189-412f-a456-c480d42efaa8	1y	RSA	2048	– Цифровая подпись – Подтверждение подлинности – Шифрование ключей – Шифрование данных	+	– Аутентификация клиента – Защита электронной почты – Вход с MS смарт-картой	–	Common name ¹	+	+	MS UPN ²	+	+
			ECDSA	256								RFC 822 Name ³	+	+
			ГОСТ P 34.10–2012	256										
WEB–Client	18ecaacc-43d6-4aaa-afcc-1bc8e547e6f5	1y	RSA	2048	– Цифровая подпись – Подтверждение подлинности – Шифрование ключей	+	– Аутентификация клиента – Защита электронной почты	–	Common name ⁴	+	+	MS UPN ⁵	+	+
			ECDSA	256								RFC 822 Name ⁶	+	+
			ГОСТ P 34.10–2012	256										
WEB–Server	61c901fa-c823-4899-87a0-df4035291fa0	1y	RSA	2048	– Цифровая подпись – Шифрование ключей	+	Аутентификация сервера	–	Common name ⁷	+	+	DNS name ⁸	+	+
			ECDSA	256										
			ГОСТ P 34.10–2012	256										
S/MIME	0a7c4a9f-b260-46c5-94c5-58de5e977678	1y	RSA	2048	– Цифровая подпись – Подтверждение подлинности – Шифрование ключей – Шифрование данных	+	– Аутентификация клиента – Защита электронной почты – Вход с MS смарт-картой	–	Common name ⁹	+	+	RFC 822 Name ¹⁰	+	+
			ECDSA	256										
			ГОСТ P 34.10–2012	256										

¹ Имя пользователя.

² Имя входа пользователя в формате e-mail адреса.

³ Почтовый адрес пользователя, может совпадать с MS UPN.

⁴ Имя веб-клиента.

⁵ Имя входа пользователя в формате e-mail адреса.

⁶ Почтовый адрес пользователя, может совпадать с MS UPN.

⁷ Имя веб-сервера.

⁸ FQDN – полное доменное имя вашего сервера.

⁹ Имя пользователя.

¹⁰ почтовый адрес пользователя, может совпадать с MS UPN.

Имя шаблона	Идентификатор	Период действия сертификата	Шифрование		Использование ключа		Расширенное использование ключа		Компоненты имени сертификата					
			Алгоритм	Минимальная длина ключа	Значения	Криг.	Значения	Криг.	Отличительное имя субъекта			Альтернативное имя субъекта		
ALD PRO Domain Controller	83afddde-5729-4562-a7ed-260f1c0f73d7	1y	RSA	2048	– Цифровая подпись – Подтверждение подлинности – Шифрование ключей – Шифрование данных	+	– Центр распространения ключей Kerberos – Аутентификация сервера	–	Common name ¹	+	+	MS UPN ²	+	+
			ECDSA	256					Organization ³	–	+	Kerberos KPN ⁴	+	+
			ГОСТ Р 34.10–2012	256										
ALD PRO Smartcard Logon	85e99e47-479f-407e-98f8-ad13d51435a7	1y	RSA	2048	– Цифровая подпись – Подтверждение подлинности – Шифрование ключей – Шифрование данных	+	– Аутентификация клиента – Центр распространения ключей Kerberos – Аутентификация сервера	–	Common name ⁵	+	+	MS UPN ⁶	+	+
			ECDSA	256					Organization ⁷	–	+	RFC 822 Name ⁸	+	+
			ГОСТ Р 34.10–2012	256										
OCSP Signer	eeb625cb-861e-458c-94ae-79b2e05090e5	1y	RSA	2048	Цифровая подпись	+	OCSP подписант	–	Common name	+	+	–		
			ECDSA	256										
			ГОСТ Р 34.10–2012	256										

¹ Имя контроллера домена ALD PRO.

² Данные в формате «krbtgt/полное имя домена@полное имя домена».

³ Организация.

⁴ Данные в формате «krbtgt/полное имя домена@полное имя домена».

⁵ Имя пользователя ALD PRO.

⁶ Имя входа пользователя в формате e-mail адреса.

⁷ Организация.

⁸ Почтовый адрес пользователя, может совпадать с MS UPN.

Имя шаблона	Идентификатор	Период действия сертификата	Шифрование		Использование ключа		Расширенное использование ключа		Компоненты имени сертификата					
			Алгоритм	Минимальная длина ключа	Значения	Крит.	Значения	Крит.	Отличительное имя субъекта			Альтернативное имя субъекта		
									Поле	Обязат.	Валидац.	Поле	Обязат.	Валидац.
Root CA	a1eb9d3a-b9b5-4e6d-8f2d-587ca9cc6554	15y	RSA	4096	– Цифровая подпись – Подпись сертификата – Подпись списка отзыва	+	– Любое расширенное использование ключа – Аутентификация клиента – Аутентификация сервера	–	Common name	+	+	RFC 822 Name	–	+
			ECDSA	384					Unique Identifier (UID)	–	+	DNS name	–	+
			ГОСТ Р 34.10–2012	512					Given name	–	+	MS UPN	–	+
									Initials	–	+	MS GUID	–	+
									Surname	–	+	IP address	–	+
									Organizational unit	–	+	Directory Name	–	+
									Locality	–	+	Uniform resource identifier	–	+
									State or province	–	+	Registered Identifier (OID)	–	+
									Domain component	–	+	Permanent identifier	–	+
									Country	–	+	Xmpp address	–	+
									Postal code	–	+	Service Name	–	+
									Business category	–	+	Subject Identification Method	–	+
									Telephone number	–	+	Kerberos KPN	–	+
									Pseudonym	–	+			
									Postal address	–	+			
									Street	–	+			
									Name	–	+			
									Title	–	+			
									Domain qualifier	–	+			
									Description	–	+			
									Unstructured address	–	+			
									Unstructured name	–	+			
									Email Address (E)	–	+			
									Serial number	–	+			
									Organization	–	+			
									Дата рождения	–	+			

Имя шаблона	Идентификатор	Период действия сертификата	Шифрование		Использование ключа		Расширенное использование ключа		Компоненты имени сертификата					
			Алгоритм	Минимальная длина ключа	Значения	Крит.	Значения	Крит.	Отличительное имя субъекта			Альтернативное имя субъекта		
									Поле	Обязат.	Валидац.	Поле	Обязат.	Валидац.
									Место рождения	–	+			
									ИНН	–	+			
									ОГРН	–	+			
									ОГРНИП	–	+			
									СНИЛС	–	+			
									ИНН ЮЛ	–	+			
Sub CA	4f56589e-7e80-4fbe-b49f-662c9ba9a335	7y	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	–	+
			ECDSA	256					Given name	–	+	MS UPN	–	+
			ГОСТ Р 34.10–2012	256					Initials	–	+	MS GUID	–	+
									Surname	–	+	IP address	–	+
									Organizational unit	–	+	Directory Name	–	+
									Locality	–	+	Uniform resource identifier	–	+
									State or province	–	+	Registered Identifier (OID)	–	+
									Domain component	–	+	Permanent identifier	–	+
									Country	–	+	Xmpp address	–	+
									Postal code	–	+	Service Name	–	+
									Business category	–	+	Subject Identification Method	–	+
									Telephone number	–	+	Kerberos KPN	–	+
									Pseudonym	–	+			
									Postal address	–	+			
									Street	–	+			
									Name	–	+			
									Title	–	+			
									Domain qualifier	–	+			
									Description	–	+			

Имя шаблона	Идентификатор	Период действия сертификата	Шифрование		Использование ключа		Расширенное использование ключа		Компоненты имени сертификата					
			Алгоритм	Минимальная длина ключа	Значения	Крит.	Значения	Крит.	Отличительное имя субъекта			Альтернативное имя субъекта		
									Поле	Обязат.	Валидац.	Поле	Обязат.	Валидац.
									Unstructured address	–	+			
									Unstructured name	–	+			
									Email Address (E)	–	+			
									Serial number	–	+			
									Organization	–	+			
									Дата рождения	–	+			
									Место рождения	–	+			
									ИНН	–	+			
									ОГРН	–	+			
									ОГРНИП	–	+			
									СНИЛС	–	+			
									ИНН юЛ	–	+			
SCEP Management	77004b9d-e195-40a3-aea0-dca5ad403f49	25y	RSA	2048	– Цифровая подпись – Шифрование ключей – Шифрование данных	+	–	–	Common name	+	–	–		
			ECDSA	256										
			ГОСТ Р 34.10–2012	256										

ПРИЛОЖЕНИЕ 3. ПРАВИЛА ВАЛИДАЦИИ ЗНАЧЕНИЙ ПОЛЕЙ ПО УМОЛЧАНИЮ ПРЕДУСТАНОВЛЕННЫХ ШАБЛОНОВ СЕРТИФИКАТОВ

Поле	Правило валидации
Поля SDN	
Country	Допустимые символы: "A"–"Z", "a"–"z". Длина значения должна составлять 2 символа.
Domain qualifier	Допустимые символы: "A"–"Z", "a"–"z", "0"–"9", "'", "(", ")", "+", ",", "-", ".", "/", ":", "=", "?", пробел.
Email Address (E)	Допустимые символы: "A"–"Z", "a"–"z", "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».
Поля SAN	
RFC 822 Name	Допустимые символы: "A"–"Z", "a"–"z", "0"–"9", ".", "@", "_", "-". Формат значения: "text@text". Пример заполнения: «ivanova@example.com».
DNS Name	Допустимые символы: "A"–"Z", "a"–"z", "0"–"9", "-", ".", "*", ".". Пример значения: «dc1.presale.aeca».
IP address	Допустимые символы: "A"–"F", "a"–"f", "0"–"9", ".", ":". Формат значения: IPv4–адрес или IPv6–адрес.
Directory Name	Формат значения: последовательность идентификаторов относительных отличительных имен (RDN) и их значений, отделенных запятой или запятой с пробелом (например, O=organization, OU=Department, L=City, DC=Component.). 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».

Поле	Правило валидации
MS GUID, Globally Unique Identifier	Допустимые символы: "A"–"F", "a"–"f", "0"–"9". Длина значения должна составлять 32 символа. Пример значения: «92625ee510e248479554779d1f43f751».
Kerberos KPN, Kerberos 5 Principal Name	Допустимые символы: "A"–"Z", "a"–"z", "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.

Имя	OID	Описание
OCSF подписант	1.3.6.1.5.5.7.3.9	Сертификат может использоваться для формирования электронной подписи OCSF-запросов.
Подписание Adobe PDF	1.2.840.113583.1.1.5	Сертификат может использоваться для подписания документов Adobe PDF.
Аутентификация PIV карты	2.16.840.1.101.3.6.8	Сертификат может использоваться для аутентификации карты PIV.
SCVP клиент	1.3.6.1.5.5.7.3.16	Сертификат может использоваться как сертификат клиента при использовании протокола Server-Based Certificate Validation Protocol (SCVP).
SCVP сервер	1.3.6.1.5.5.7.3.15	Сертификат может использоваться как сертификат сервера при использовании протокола Server-Based Certificate Validation Protocol (SCVP).
Домен SIP	1.3.6.1.5.5.7.3.20	Сертификат может использоваться как сертификат Session Initiation Protocol (SIP) доменов.
SSH клиент	1.3.6.1.5.5.7.3.21	Сертификат может использоваться как сертификат SSH клиента.
SSH сервер	1.3.6.1.5.5.7.3.22	Сертификат может использоваться как сертификат SSH сервера.
Аутентификация сервера	1.3.6.1.5.5.7.3.1	Сертификат может использоваться при установлении защищенного соединения по протоколу TLS для подтверждения подлинности сервера.
Отметка времени	1.3.6.1.5.5.7.3.8	Сертификат может использоваться для привязки хеша объекта ко времени из доверенного источника времени.
ICAO подписание основного списка	2.23.136.1.1.3	Сертификат может использоваться для подписания основного списка ICAO.

ПРИЛОЖЕНИЕ 5. ФОРМАТ И ПРАВИЛА ЗАПИСИ ЗНАЧЕНИЙ В ПОЛЯ СЕРТИФИКАТА НА БУМАЖНОМ НОСИТЕЛЕ

5.1 Формат сертификата на бумажном носителе для физического лица

Сертификат ключа проверки электронной подписи	
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

Сертификат ключа проверки электронной подписи	
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	
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»: <Название алгоритма> (<длина ключа>) 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 «СТ» 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 «СТ» 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

Поле	Значение
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»: <Название алгоритма> (<длина ключа>) 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
 - Фамилия, имя, отчество: Иванов Иван Иванович
 - ПИН: 01234567891234
4. Сведения об издателе квалифицированного сертификата
 - Наименование УЦ: Root
 - Место нахождения УЦ: Страна, Область, Город, Ул. Тест 3, 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 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 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 Aladdin Enterprise Certificate Authority в Центре сертификации в разделе и на вкладке «Центры валидации».

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

Активированный ЦС – это экземпляр центра сертификации в информационной системе, который используется в настоящий момент для выпуска сертификатов на основании запроса и сертификатов доступа субъектов.

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

Кластер – это группа точек распространения определенного типа (CRL, Delta CRL и AIA) или служб OCSP, доступ к которым осуществляется по единому URL (путем использования внешних средств балансирования нагрузки).

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

Корневой ЦС – экземпляр центра сертификации в информационной системе, имеющий абсолютное доверие со стороны всех участников процесса строгой аутентификации. С точки зрения службы безопасности предприятия должен быть обеспечен максимальным уровнем защиты (отдельный ПК, отключённый от сети, с доступом ограниченного круга лиц). Корневой ЦС владеет само подписанным сертификатом, который должен распространяться доверенным способом в информационной системе.

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

Пагинация – это постраничный вывод информации на экране разделов. Ссылочный блок для разграничения содержимого размещен внизу экранной страницы и представляет цифровой диапазон, отображающий:

- количество элементов на одной странице – возможно выбрать из выпадающего списка – выводить 5, 10 или 25 элементов на одну страницу;
- нумерацию элементов страницы, которая в настоящее время открыта у пользователя, из общего количества созданных элементов;
- указатели для навигации по страницам.

Подчиненный ЦС – экземпляр центра сертификации в информационной системе, обладающий функцией управления политиками строгой аутентификации или функцией управления жизненным циклом сертификатов субъектов информационной системы. Подчиненный ЦС владеет сертификатом, выданным вышестоящим ЦС (Корневым или другим Подчиненным), который используется для проверки всей цепочки доверия сертификатов.

Пользовательская точка – это запись URL–адреса, созданная администратором с целью регистрации сторонней точки распространения CRL, Delta CRL или AIA, существующей или развёртываемой на сервере в информационной системе.

Приоритет – это очерёдность записи URL–адреса точки распространения или службы OCSP в сертификате и, соответственно, в списках, отображаемом на вкладках «Точки распространения» и «Службы OCSP».

Разрешённые издатели – это список Центров сертификации, сертификаты которых клиент может использовать для авторизации на сервере, на котором развёрнут Центр сертификации с актуальным списком разрешённых издателей.

Ресурсная система (внешняя) – это подключаемая служба каталогов, которая предоставляет информацию об имеющихся субъектах.

Ресурсная система (локальная) – это ресурсная система, создаваемая автоматически при установке программного средства «Центр сертификатов доступа Aladdin Enterprise Certificate Authority Certified Edition», представляющая собой базу данных субъектов и формируемая из сведений, вводимых при выпуске сертификата для нового субъекта.

Сервис регистрации – служба, составная часть Центра сертификации, отвечающая за обработку запросов на выдачу сертификатов от субъектов информационной системы.

Сервис сертификатов – служба, составная часть Центра сертификации, непосредственно отвечающая за жизненный цикл сертификатов (выдача, отзыв).

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

Сертификат веб-сервера – это сертификат, с помощью которого сервер, на котором развёрнут программный компонент «Центр сертификации Aladdin Enterprise Certification Authority», устанавливает с клиентом tls-соединение.

Событие безопасности – идентифицированное возникновение состояния системы, сервиса или сети, указывающего на возможное нарушение политики информационной безопасности, или сбой средств контроля, или ранее неизвестную ситуацию, которая может быть значимой для безопасности.

Список отозванных сертификатов (Certificate Revocation List – **CRL**) – список аннулированных (отозванных) сертификатов, издается центром сертификации по запросу или с заданной периодичностью на основании запросов об отзыве сертификатов.

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

Технологический ЦС – экземпляр центра сертификации в информационной системе, обладающий функцией первичной настройки программного компонента «Центр сертификации Aladdin Enterprise Certification Authority».

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

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

ЛИСТ РЕГИСТРАЦИИ ИЗМЕНЕНИЙ

[illegible]